Automated theorem proving
The Semi-decidability

Given a tree $\pi$ and a proposition $A$, can decide if $\pi$ proof of $A$

Enumerate all trees (La biblioteca de Babel)
If a proof of $A$ exists, it will eventually show up
Otherwise, enumeration does not terminate

Cannot avoid non termination: provability undecidable
A useless algorithm

Slow (library of Babel very big)

But the idea of enumerating and testing is practically useful
I. Proof search in Natural deduction
Enumerate, bottom up, the rules that can apply to each node

\[ P \vdash Q \Rightarrow (P \land Q) \]

Let us start with an introduction rule
How many possibilities?
Enumerate, bottom up, the rules that can apply to each node

\[
\frac{P, Q \vdash P \land Q}{\frac{P \vdash Q \Rightarrow (P \land Q)}{P \Rightarrow Q \Rightarrow (P \land Q)}} \Rightarrow\text{-intro}
\]

Again: an introduction rule
How many possibilities?
Enumerating rules

Enumerate, bottom up, the rules that can apply to each node

\[
\frac{P, Q \vdash P}{} \quad \frac{P, Q \vdash Q}{P, Q \vdash P \land Q} \quad \frac{P, Q \vdash Q}{P \vdash Q \Rightarrow (P \land Q)} \quad \frac{P, Q \vdash P \land Q}{\Rightarrow\text{-intro}}
\]
Enumerate, bottom up, the rules that can apply to each node:

\[
\begin{align*}
\frac{P, Q \vdash P}{P, Q \vdash P \land Q} & \quad \text{axiom} \\
\frac{P, Q \vdash Q}{P, Q \vdash P \land Q} & \quad \text{\&-intro} \\
\frac{P \vdash Q \Rightarrow (P \land Q)}{P, Q \vdash P \land Q} & \quad \Rightarrow\text{-intro}
\end{align*}
\]
Enumerating rules

Enumerate, bottom up, the rules that can apply to each node

\[
\frac{P, Q \vdash P}{P \vdash Q \Rightarrow (P \land Q)} \quad \Rightarrow\text{-intro}
\]

\[
\frac{P, Q \vdash Q}{P, Q \vdash P \land Q} \quad \land\text{-intro}
\]

\[
\frac{P, Q \vdash P \land Q}{P, Q \vdash P} \quad \text{axiom}
\]

\[
\frac{P, Q \vdash Q}{P, Q \vdash Q} \quad \text{axiom}
\]
Elimination rules

Not as nice

\[ \Gamma \vdash A \land B \]
\[ \frac{}{\Gamma \vdash A} \quad \land\text{-elim} \]

Always applies

Need to guess $B$ that does not appear in the conclusion (that is, enumerate all possible $B$)
Elimination rules

\[
P \land Q \vdash P \quad \text{?}-\text{elim}
\]
Elimination rules

\[
\frac{P \land Q}{P \land Q \vdash P} \quad \land\text{-elim}
\]

How did you guess $\land$ and $Q$?
An asymmetry

In Natural deduction

The form of the conclusion of the sequent guides the choice of introductions

The form of the hypotheses of the sequent does not guide the choice of eliminations
II. Sequent calculus
The idea

Keep introduction rules (that work): right rules
Replace elimination rules with introduction rules applied to hypotheses: left rules

For instance

\[ \Gamma, A \land B \vdash C \quad \land\text{-left} \]

What can we do with this hypothesis
The idea

Keep introduction rules (that work): right rules
Replace elimination rules with introduction rules applied to hypotheses: left rules

For instance

\[
\Gamma, A, B \vdash C \\
\Gamma, A \land B \vdash C \quad \land\text{-left}
\]
Back to our example

\[ P \land Q \vdash P \]
Back to our example

$$\frac{P \land Q \vdash P}{P \land Q \vdash P} \land\text{-left}$$
More rules

\[\Gamma \vdash A \quad \Gamma, B \vdash C \quad \frac{}{\Gamma, A \Rightarrow B \vdash C} \Rightarrow\text{-left}\]

\[\Gamma \vdash A \quad \frac{}{\Gamma, \neg A \vdash B} \neg\text{-left}\]

\[\Gamma, \bot \vdash A \quad \frac{}{\bot\text{-left}}\]

\[\Gamma, (t/x)A \vdash B \quad \frac{}{\Gamma, \forall x \ A \vdash B} \forall\text{-left}\]
The contraction rule

Natural deduction: hypotheses remain: multiple use

In Sequent calculus

\[ \Gamma, (t/x)A \vdash B \]

\[ \frac{\Gamma, (t/x)A \vdash B}{\Gamma, \forall x A \vdash B} \] \ \forall\text{-left} 

the hypothesis \( \forall x A \) disappears

Need to save the hypothesis

\[ \Gamma, A, A \vdash B \]

\[ \frac{\Gamma, A, A \vdash B}{\Gamma, A \vdash B} \] \ contraction-left

multiset
The cut rule

Translating a proof of the form

\[
\begin{array}{c}
\pi \\
\hline
\Gamma \vdash A \land B \\
\hline
\Gamma \vdash A \\
\end{array}
\] \quad \land\text{-elim}

A proof \( \pi' \) of \( \Gamma \vdash A \land B \)

\[
\begin{array}{c}
\pi' \\
\hline
\Gamma \vdash A \land B \\
\end{array}
\] \quad \land\text{-left}

\[
\begin{array}{c}
\hline
\Gamma, A, B \vdash A \\
\end{array}
\] \quad \text{axiom}

\[
\begin{array}{c}
\hline
\Gamma, A \land B \vdash A \\
\end{array}
\] \quad \land\text{-left}
The cut rule

Translating a proof of the form

\[ \pi \]

\[ \frac{\Gamma \vdash A \land B}{\Gamma \vdash A} \quad \land\text{-elim} \]

A proof \( \pi' \) of \( \Gamma \vdash A \land B \)

\[ \pi' \]

\[ \frac{\Gamma, A, B \vdash A}{\Gamma \vdash A} \quad \text{axiom} \]

\[ \frac{\Gamma \vdash A \land B \quad \frac{\Gamma, A \land B \vdash A}{\Gamma, A \land B \vdash A}}{\Gamma \vdash A} \quad \land\text{-left} \]

\[ \frac{\Gamma, A \land B \vdash A}{\Gamma \vdash A} \quad \text{cut} \]
The cut rule

\[
\frac{\Gamma \vdash A \quad \Gamma, A \vdash B}{\Gamma \vdash B} \quad \text{cut}
\]

Translation of Natural deduction into Sequent calculus: in a first step with the cut cut rule

In a second step: prove that this rule can be eliminated cut elimination
Works for *constructive* logic

What about *classical* logic?
III. The excluded middle in Sequent calculus
Three solutions:
A special rule
\[ \Gamma \vdash A \lor \neg A \]

A special rule
\[ \Gamma \vdash \neg \neg A \]
\[ \Gamma \vdash A \]

Or ...
An example

\[\frac{P \vdash \neg(P \Rightarrow Q)}{\neg \neg(P \Rightarrow Q), P \vdash Q}\]
A better idea

\[
\begin{align*}
\neg\neg (P \Rightarrow Q), P, \neg Q & \vdash \bot \\
\neg\neg (P \Rightarrow Q), P & \vdash \neg \neg Q \\
\neg\neg (P \Rightarrow Q), P & \vdash Q
\end{align*}
\]
A better idea

\[
\begin{align*}
&\frac{P \vdash P}{\text{axiom}} & &\frac{P, Q \vdash Q}{\text{axiom}} & &\frac{}{\Rightarrow\text{-left}} \\
&\frac{P, P \Rightarrow Q \vdash Q}{\Rightarrow\text{-left}} & &\frac{P, \neg Q, P \Rightarrow Q \vdash \bot}{\neg\text{-left}} & &\frac{P, \neg Q \vdash \neg (P \Rightarrow Q)}{\neg\text{-right}} \\
&\frac{P, \neg Q \vdash \neg (P \Rightarrow Q)}{\neg\text{-left}} & &\frac{\neg\neg (P \Rightarrow Q), P, \neg Q \vdash \bot}{\neg\text{-right}} & &\frac{\neg\neg (P \Rightarrow Q), P \vdash \neg \neg Q}{\text{excluded middle}} & &\frac{\neg\neg (P \Rightarrow Q), P \vdash Q}{\text{excluded middle}}
\end{align*}
\]
Saving $Q$ on the left

$\vdash P$ axiom $\quad P, Q \vdash Q$ axiom

$\frac{P, P \Rightarrow Q \vdash Q}{P, P \Rightarrow Q \vdash Q}$ $\Rightarrow$-left

$\frac{P, \neg Q, P \Rightarrow Q \vdash \bot}{P, \neg Q \vdash \neg (P \Rightarrow Q)}$ $\neg$-left

$\frac{P, \neg Q \vdash \neg (P \Rightarrow Q)}{\neg \neg (P \Rightarrow Q), P, \neg Q \vdash \bot}$ $\neg$-right

$\frac{\neg \neg (P \Rightarrow Q), P \vdash \neg \neg Q}{\neg \neg (P \Rightarrow Q), P \vdash Q}$ excluded middle
Or keep it in the right hand side

\[
\begin{align*}
&P \vdash P \quad \text{axiom} \\
&P, Q \vdash Q \quad \text{axiom} \\
&P, P \Rightarrow Q \vdash Q \quad \Rightarrow\text{-left} \\
&P, P \Rightarrow Q \vdash (\bot, )Q \quad (\neg\text{-left}) \\
&P \vdash \neg( P \Rightarrow Q), Q \quad \neg\text{-right} \\
&\neg\neg( P \Rightarrow Q), P \vdash (\bot, )Q \quad (\neg\text{-left}) \\
&\neg\neg( P \Rightarrow Q), P \vdash Q \quad (\neg\text{-right}) \\
&\neg\neg( P \Rightarrow Q), P \vdash Q \quad \text{(excluded middle)}
\end{align*}
\]

Sequents with several propositions in the right hand side
Sequents with several propositions in the right hand side

\[ \begin{align*}
P \vdash P, Q & \quad \text{axiom} \\
 P, P \Rightarrow Q \vdash Q & \quad \Rightarrow \text{-left} \\
 P \vdash \neg (P \Rightarrow Q), Q & \quad \neg \text{-right} \\
 \neg \neg (P \Rightarrow Q), P \vdash Q & \quad \neg \text{-left}
\end{align*} \]
IV. Cut elimination in Sequent calculus
The cut rule

\[ \Gamma \vdash A, \Delta \quad \Gamma, A \vdash \Delta \]
\[ \frac{}{\Gamma \vdash \Delta} \text{cut} \]

ruins all the benefit of Sequent calculus

A second theorem
\( \Gamma \vdash \Delta \) has a proof in Sequent calculus if and only if it has a cut free proof
thus
\( \Gamma \vdash A \) has a proof in Natural Deduction if and only if it has a cut free proof in Sequent Calculus
Eliminating the cut rule step by step

A typical case

\[
\begin{align*}
\sigma &\quad \frac{}{\Gamma, B, C \vdash \Delta} \\
\frac{}{\Gamma, B \land C \vdash \Delta} \quad \text{^\-left} \\
\Gamma &\vdash \Delta
\end{align*}
\]

\[
\begin{align*}
\sigma' &\quad \frac{\sigma_1'}{\Gamma \vdash B, \Delta} \\
\frac{}{\Gamma \vdash B \land C, \Delta} \quad \text{^\-right} \\
\sigma_2' &\quad \frac{\sigma_2'}{\Gamma \vdash C, \Delta}
\end{align*}
\]
Eliminating the cut rule step by step

First eliminate cuts in (the smaller) \( \sigma, \sigma'_1, \sigma'_2 \)

\[
\begin{align*}
\frac{\rho}{\Gamma, B, C \vdash \Delta} \quad \text{\( \land \)-left} & \quad \frac{\rho'_1}{\Gamma \vdash B, \Delta} \quad \frac{\rho'_2}{\Gamma \vdash C, \Delta} \quad \text{\( \land \)-right} \\
\frac{\Gamma, B \land C \vdash \Delta}{\Gamma \vdash B \land C, \Delta} \quad \text{\( \land \)-right} & \quad \frac{\Gamma \vdash B \land C, \Delta}{\Gamma \vdash \Delta} \quad \text{cut}
\end{align*}
\]
Eliminating the cut rule step by step

Cut on smaller propositions (and iterate)

\[
\begin{align*}
\frac{\rho}{\Gamma, B, C \vdash \Delta} & \quad \text{and iterate} \\
\Gamma & \vdash \Delta \\
\frac{\rho'}{\Gamma \vdash B, \Delta} & \quad \text{and iterate} \\
\frac{\rho'_1}{\Gamma \vdash C, \Delta} & \quad \text{and iterate} \\
\end{align*}
\]
V. Proof search in cut free Sequent calculus
Choices

No need to enumerate all possible propositions

But... a few choices remain
1. Choosing the sequent

\[
\frac{P, Q \vdash P}{P, Q \vdash P \land Q} \land\text{-right}
\]

\[
\frac{P, Q \vdash Q}{P, Q \vdash P \land Q} \land\text{-right}
\]

2. Choosing the proposition

\[P \land Q \vdash Q \lor R\]

3. Choosing the rule: logic, contraction (or axiom)

4. Choosing the term

\[
\frac{\Gamma, (t/x)A \vdash B}{\Gamma, \forall x A \vdash B} \forall\text{-left}
\]
Don’t know choices
Either $A$ or $B$: chose $A$, if $A$ fails then chose $B$ (general case)

Don’t care choices
Either $A$ or $B$: no matter what you chose, the resultat will be the same (sequentialization of independent tasks)
1. Choosing the sequent

\[
\frac{P, Q \vdash P \quad P, Q \vdash Q}{P, Q \vdash P \land Q} \quad \text{\textsuperscript{\wedge}-right}
\]

2. Choosing the proposition

\[\forall x (P(x) \land Q(x)) \vdash \forall x (P(x))\]

3. Choosing the rule: logic, contraction (or axiom)

\[\forall x (P(x) \land \neg P(S(x))) \vdash \]

4. Choosing the term

\[P(f(f(c))) \vdash \exists x P(f(x))\]
Finite and infinite don’t know choices

Choosing the proposition: finite

Choosing the rule: finite

Choosing the term: infinite
Avoiding choosing the term

\[
\begin{align*}
? & \quad P(f(f(c))) \vdash \exists x \ P(f(x)) \quad \exists\text{-right} \\
\text{try } c, \ f(c), \ f(f(c)), \ ... \\
\text{Which term to chose? How did you guess?}
\end{align*}
\]
Delaying the choice of the term

\[
\frac{P(f(f(c)))) \vdash P(f(X))}{P(f(f(c)))) \vdash \exists x \ P(f(x)) \quad \exists\text{-right}
\]
Delaying the choice of the term

\[
\frac{P(f(f(c)))) \vdash P(f(X))}{P(f(f(c))) \vdash \exists x \ P(f(x))} \quad \text{axiom}
\]

\[
\frac{P(f(f(c))) \vdash \exists x \ P(f(x))}{\exists \text{-right}}
\]

Proof scheme:

- \(\exists\)-right et \(\forall\)-left restricted to (meta)-variables
- the \textit{axiom} rule permits to prove any sequent
In a second step

\[
\begin{align*}
P(f(f(c))) & \vdash P(f(X)) & \text{axiom} \\
\end{align*}
\]

\[
\begin{align*}
P(f(f(c))) & \vdash \exists x \ P(f(x)) & \exists\text{-right} \\
\end{align*}
\]

Look for a substitution of \( X \) that completes thus proof scheme (that is transforms it into a proof)

Comparing \( P(f(f(c))) \) and \( P(f(X)) \)
Completing a proof scheme

In each sequent proved with the (pseudo) axiom rule

Chose an atomic proposition in the left hand side and in the right hand side

Look for a substitution that makes all pairs identical: the unification algorithm

(then check the conditions $x$ not free in $\Gamma\Delta$)
The unification algorithm: an example

The solutions of the problem

\[ P(f(X)) = P(f(f(c))) \]

are the same as those of the problem

\[ f(X) = f(f(c)) \]

that are the same as those of the problem

\[ X = f(c) \]

and this problem has a solution: the substitution \( f(c)/X \).
The unification algorithm: the general case

Chose an equation in the system

- \( f(t_1, \ldots, t_n) = f(u_1, \ldots, u_n) \rightarrow \) replace it with \( t_1 = u_1, \ldots, t_n = u_n \)
- \( f(t_1, \ldots, t_n) = g(u_1, \ldots, u_m) \rightarrow \) fail
- \( X = X \rightarrow \) delete
- \( X = t \) (or \( t = X \)), if \( X \) occurs in \( t \), \( t \) different from \( X \), fail
- \( X = t \) (or \( t = X \)) \( X \) does not occur in \( t \), substitute \( t \) for \( A \) in the rest of the system solve \( \rightarrow \) substitution \( \sigma \), return \( \sigma \cup \{ \sigma t/X \} \).
Computers can build proofs (sometimes)

Computers are truth judgment machines
Computers can check proofs and build proofs,
Proofs, theories... are algorithms
Algorithms and programs can be proved correct
Language is a unifying notion