Automated theorem proving

The Semi-decidability

Given a tree π and a proposition A, can decide if π proof of A

Enumerate all trees (La biblioteca de Babel)
If a proof of A exists, it will eventualy 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

Enumerating rules

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

$$\frac{}{P \vdash Q \Rightarrow (P \wedge Q)}\ ?$$

Let us stat with an introduction rule
How many possibilities?

Enumerating rules

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

$$\dfrac{\dfrac{\dfrac{}{P, Q \vdash P \wedge Q}\,?}{P \vdash Q \Rightarrow (P \wedge Q)}\,\Rightarrow\text{-intro}}$$

Again: an introduction rule

How many possibilities?

Enumerating rules

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

$$\dfrac{\dfrac{\overline{P, Q \vdash P}\ ? \qquad \overline{P, Q \vdash Q}}{P, Q \vdash P \wedge Q}\ \wedge\text{-intro}}{P \vdash Q \Rightarrow (P \wedge Q)}\ \Rightarrow\text{-intro}$$

Enumerating rules

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

$$\dfrac{\dfrac{\dfrac{}{P, Q \vdash P}\ \text{axiom} \qquad \dfrac{}{P, Q \vdash Q}\ ?}{P, Q \vdash P \wedge Q}\ \wedge\text{-intro}}{P \vdash Q \Rightarrow (P \wedge Q)}\ \Rightarrow\text{-intro}$$

Enumerating rules

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

$$\dfrac{\dfrac{\dfrac{}{P, Q \vdash P}\ \text{axiom} \qquad \dfrac{}{P, Q \vdash Q}\ \text{axiom}}{P, Q \vdash P \wedge Q}\ \wedge\text{-intro}}{P \vdash Q \Rightarrow (P \wedge Q)}\ \Rightarrow\text{-intro}$$

Elimination rules

Not as nice

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge\text{-elim}$$

Always applies

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

Elimination rules

$$\frac{}{P \wedge Q \vdash P}\ ?\text{-elim}$$

Elimination rules

$$\frac{\overline{P \wedge Q \vdash P \wedge Q}}{P \wedge Q \vdash P}\ \wedge\text{-elim}$$

How did you guess $\wedge$ 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

$$\frac{}{\Gamma, A \wedge B \vdash C}\ \wedge\text{-left}$$

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

$$\frac{\Gamma, A, B \vdash C}{\Gamma, A \wedge B \vdash C} \wedge\text{-left}$$

Back to our example

$$\frac{}{P \wedge Q \vdash P}\ ?$$

Back to our example

$$\dfrac{\dfrac{}{P, Q \vdash P}}{P \wedge Q \vdash P} \wedge\text{-left}$$

More rules

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

$$\frac{\Gamma \vdash A}{\Gamma, \neg A \vdash B} \neg\text{-left}$$

$$\frac{}{\Gamma, \bot \vdash A} \bot\text{-left}$$

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

The contraction rule

Natural deduction: hypotheses remain: mutiple use
In Sequent calculus

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

the hypothesis $\forall x\ A$ disapears

Need to save the hypothese

$$\frac{\Gamma, A, A \vdash B}{\Gamma, A \vdash B}\ \text{contraction-left}$$

multiset

The cut rule

Translating a proof of the form

$$\dfrac{\dfrac{\pi}{\Gamma \vdash A \wedge B}}{\Gamma \vdash A}\ \wedge\text{-elim}$$

A proof π' of $\Gamma \vdash A \wedge B$

$$\dfrac{\dfrac{\pi'}{\Gamma \vdash A \wedge B} \quad \dfrac{\dfrac{}{\Gamma, A, B \vdash A}\ \text{axiom}}{\Gamma, A \wedge B \vdash A}\ \wedge\text{-left}}{}$$

The cut rule

Translating a proof of the form

$$\dfrac{\dfrac{\pi}{\Gamma \vdash A \wedge B}}{\Gamma \vdash A}\ \wedge\text{-elim}$$

A proof π' of $\Gamma \vdash A \wedge B$

$$\dfrac{\dfrac{\pi'}{\Gamma \vdash A \wedge B} \quad \dfrac{\dfrac{}{\Gamma, A, B \vdash A}\ \text{axiom}}{\Gamma, A \wedge B \vdash A}\ \wedge\text{-left}}{\Gamma \vdash A}\ \text{cut}$$

The cut rule

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

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

$$\frac{}{\Gamma \vdash A \vee \neg A}$$

A special rule

$$\frac{\Gamma \vdash \neg\neg A}{\Gamma \vdash A}$$

Or ...

An example

$$\dfrac{\dfrac{?}{P \vdash \neg(P \Rightarrow Q)}}{\neg\neg(P \Rightarrow Q), P \vdash Q}\ \neg\text{-left}$$

A better idea

$$\dfrac{\dfrac{\dfrac{}{\neg\neg(P \Rightarrow Q), P, \neg Q \vdash \bot}\ \neg\text{-left}}{\neg\neg(P \Rightarrow Q), P \vdash \neg\neg Q}\ \neg\text{-right}}{\neg\neg(P \Rightarrow Q), P \vdash Q}\ \text{excluded middle}$$

A better idea

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{P \vdash P}\,\text{axiom} \quad \dfrac{}{P, Q \vdash Q}\,\text{axiom}}{P, P \Rightarrow Q \vdash Q}\,\Rightarrow\text{-left}}{P, \neg Q, P \Rightarrow Q \vdash \bot}\,\neg\text{-left}}{P, \neg Q \vdash \neg(P \Rightarrow Q)}\,\neg\text{-right}}{\neg\neg(P \Rightarrow Q), P, \neg Q \vdash \bot}\,\neg\text{-left}}{\neg\neg(P \Rightarrow Q), P \vdash \neg\neg Q}\,\neg\text{-right}}{\neg\neg(P \Rightarrow Q), P \vdash Q}\,\text{excluded middle}$$

Saving Q on the left

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{P \vdash P}\,\text{axiom} \quad \dfrac{}{P, Q \vdash Q}\,\text{axiom}}{P, P \Rightarrow Q \vdash Q}\,\Rightarrow\text{-left}}{P, \neg Q, P \Rightarrow Q \vdash \bot}\,\neg\text{-left}}{P, \neg Q \vdash \neg(P \Rightarrow Q)}\,\neg\text{-right}}{\neg\neg(P \Rightarrow Q), P, \neg Q \vdash \bot}\,\neg\text{-left}}{\neg\neg(P \Rightarrow Q), P \vdash \neg\neg Q}\,\neg\text{-right}}{\neg\neg(P \Rightarrow Q), P \vdash Q}\,\text{excluded middle}$$

Or keep it in the right hand side

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{P \vdash P}\,\text{axiom} \quad \dfrac{}{P, Q \vdash Q}\,\text{axiom}}{P, P \Rightarrow Q \vdash Q}\,\Rightarrow\text{-left}}{P, P \Rightarrow Q \vdash (\bot,)Q}\,(\neg\text{-left})}{P \vdash \neg(P \Rightarrow Q), Q}\,\neg\text{-right}}{\neg\neg(P \Rightarrow Q), P \vdash (\bot,)Q}\,\neg\text{-left}}{\neg\neg(P \Rightarrow Q), P \vdash Q}\,(\neg\text{-right})}{\neg\neg(P \Rightarrow Q), P \vdash Q}\,(\text{excluded middle})$$

Sequents with several propositions in the right hand side

Sequents with several propositions in the right hand side

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{P \vdash P, Q}\,\text{axiom} \qquad \dfrac{}{P, Q \vdash Q}\,\text{axiom}}{P, P \Rightarrow Q \vdash Q}\,\Rightarrow\text{-left}}{P \vdash \neg(P \Rightarrow Q), Q}\,\neg\text{-right}}{\neg\neg(P \Rightarrow Q), P \vdash Q}\,\neg\text{-left}$$

IV. Cut elimination in Sequent calculus

The cut rule

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

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

$$\dfrac{\dfrac{\dfrac{\sigma}{\Gamma, B, C \vdash \Delta}}{\Gamma, B \wedge C \vdash \Delta}\,\wedge\text{-left} \qquad \dfrac{\dfrac{\sigma_1'}{\Gamma \vdash B, \Delta} \quad \dfrac{\sigma_2'}{\Gamma \vdash C, \Delta}}{\Gamma \vdash B \wedge C, \Delta}\,\wedge\text{-right}}{\Gamma \vdash \Delta}\,\text{cut}$$

Eliminating the cut rule step by step

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

$$\dfrac{\dfrac{\dfrac{\rho}{\Gamma, B, C \vdash \Delta}}{\Gamma, B \wedge C \vdash \Delta}\,\wedge\text{-left} \qquad \dfrac{\dfrac{\rho'_1}{\Gamma \vdash B, \Delta} \quad \dfrac{\rho'_2}{\Gamma \vdash C, \Delta}}{\Gamma \vdash B \wedge C, \Delta}\,\wedge\text{-right}}{\Gamma \vdash \Delta}\,\text{cut}$$

Eliminating the cut rule step by step

Cut on smaller propositions (and iterate)

$$\dfrac{\dfrac{\dfrac{\rho}{\Gamma, B, C \vdash \Delta}}{\Gamma, B \wedge C \vdash \Delta}\,\wedge\text{-left} \qquad \dfrac{\dfrac{\rho_1'}{\Gamma \vdash B, \Delta} \quad \dfrac{\rho_2'}{\Gamma \vdash C, \Delta}}{\Gamma \vdash B \wedge C, \Delta}\,\wedge\text{-right}}{\Gamma \vdash \Delta}\,\text{cut}$$

$$\dfrac{\dfrac{\dfrac{\rho}{\Gamma, B, C \vdash \Delta} \quad \dfrac{\rho_1'}{\Gamma, C \vdash B, \Delta}}{\Gamma, C \vdash \Delta}\,\text{cut} \qquad \dfrac{\rho_2'}{\Gamma \vdash C, \Delta}}{\Gamma \vdash \Delta}\,\text{cut}$$

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

$$\dfrac{\dfrac{}{P, Q \vdash P}\,? \qquad \dfrac{}{P, Q \vdash Q}\,?}{P, Q \vdash P \wedge Q}\,\wedge\text{-right}$$

2. Choosing the proposition

$$P \wedge Q \vdash Q \vee R$$

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

$$\dfrac{\Gamma, (t/x)A \vdash B}{\Gamma, \forall x\ A \vdash B}\,\forall\text{-left}$$

Mazes and *œufs mimosa*

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

$$\dfrac{\dfrac{}{P, Q \vdash P}\,? \qquad \dfrac{}{P, Q \vdash Q}\,?}{P, Q \vdash P \wedge Q}\,\wedge\text{-right}$$

2. Choosing the proposition

$$\forall x\ (P(x) \wedge Q(x)) \vdash \forall x\ (P(x))$$

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

$$\forall x\ (P(x) \wedge \neg P(S(x))) \vdash$$

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

$$\frac{?}{P(f(f(c))) \vdash \exists x\ P(f(x))}\ \exists\text{-right}$$

try c, $f(c)$, $f(f(c))$, ...
Which term to chose? How did you guess?

Delaying the choice of the term

$$\frac{P(f(f(c))) \vdash P(f(X))}{P(f(f(c))) \vdash \exists x\ P(f(x))}\ \exists\text{-right}$$

Delaying the choice of the term

$$\dfrac{\dfrac{}{P(f(f(c))) \vdash P(f(X))}\ \text{axiom}}{P(f(f(c))) \vdash \exists x\ P(f(x))}\ \exists\text{-right}$$

Proof scheme:

- $\exists$-right et $\forall$-left restricted to (meta)-variables
- the *axiom* rule permits to prove any sequent

In a second step

$$\dfrac{\dfrac{}{P(f(f(c))) \vdash P(f(X))}\ \text{axiom}}{P(f(f(c))) \vdash \exists x\ P(f(x))}\ \exists\text{-right}$$

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

- $f(t_1, ..., t_n) = f(u_1, ..., u_n) \longrightarrow$ replace it with $t_1 = u_1, ..., t_n = u_n$
- $f(t_1, ..., t_n) = g(u_1, ..., u_m) \longrightarrow$ fail
- $X = X \longrightarrow$ 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 $\longrightarrow$ substitution σ, return $\sigma \cup \{\sigma t/X\}$.

Message to take home

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