Proof Theory

What is a formal proof? (Formal proofs are rare, even in Math!)
Huge variety of formal proof systems, but only all generally (?) have:
- logical axioms (e.g., \( P \rightarrow (Q \rightarrow P) \))
- rules of inference (e.g., modus ponens)

Logical axioms typically include / consist in logical axiomatics.

(Thibert style) \( \forall \) (in Theory \( T \) of \( \mathcal{L} \))

Define a (formal) proof in such a system -- is a finite list of formulas \( \ell_1, \ell_2, \ldots, \ell_n \)
Such that each \( \ell_i \) is either
(1) a logical axiom
or (2) an axiom of Theory \( T \)
or (3) \( \ell_i \) follows from each \( \ell_j \)

by rules of inference
and \( \mathcal{L} \) is one of the \( \ell_i \) is.

Natural deduction style:

```
\[ \begin{array}{c}
\text{Proof tree}\end{array} \]
```

(Fitch style)

\[ \begin{array}{c}
\text{Proof tree}\end{array} \]

The rule Modus ponens tells you the proof-theoretic meaning of implication.

\( \text{T : } \Gamma \vdash \phi \text{ : Then \phi is a proof of } \phi \text{ from } \Gamma \)
Desirable features in a proof system:

- Soundness: if $T \vdash \phi$, then $T \models \phi$.
- Completeness: if $T \models \phi$, then $T \vdash \phi$.

If the logical axioms are valid (or models?) and the rules of inference are truth-preserving, then the system is sound.

For decidability, we want to be able to determine in a purely mechanistic way whether something is a proof (proofs should be checkable).

- We should be able to recognize whether something is an axiom and whether some particular $\phi$ follows from some other formulas $\psi_1, \ldots, \psi_n$ by rules of inference.

**Exercise:**

(a) Construct a formal proof system that is sound but not complete.

(b) Construct a formal proof system that is complete but not sound.

(c) Construct a formal proof system that is sound and complete, but not decidable.

Hints: These are not technical, keep it simple.
So \( (a, \lambda x. a \rightarrow a) \rightarrow a \) is a model of \( \mathbf{M} \).

Suppose \( \mathbf{M} \) is a model of \( \mathbf{M} \). By completeness, there is a finite subset of \( \mathbf{M} \) such that \( \mathbf{M} \) is a model of \( \mathbf{M} \).

So every model of \( \mathbf{M} \) is a model of \( \mathbf{M} \).

Theorem: \( \mathbf{M} \) is sound and complete.

Proof: (Soundness): If \( \mathbf{M} \) is a model of \( \mathbf{M} \), then \( \mathbf{M} \) is a model of \( \mathbf{M} \).

- Let's verify that \( \mathbf{M} \) is a model of \( \mathbf{M} \).

- If \( \mathbf{M} \) is an axiom, \( \mathbf{M} \) is a model of \( \mathbf{M} \).

- Otherwise, \( \mathbf{M} \) is deduced from \( \mathbf{M} \) and \( \mathbf{M} \), and \( \mathbf{M} \) is a model of \( \mathbf{M} \).

So if \( \mathbf{M} \) is a model of \( \mathbf{M} \), then \( \mathbf{M} \) is a model of \( \mathbf{M} \).

Conversely, \( \mathbf{M} \) is deduced from \( \mathbf{M} \) and \( \mathbf{M} \), and \( \mathbf{M} \) is a model of \( \mathbf{M} \).

- Therefore, \( \mathbf{M} \) is an axiom, \( \mathbf{M} \) is a model of \( \mathbf{M} \).

Thus, \( \mathbf{M} \) is a model of \( \mathbf{M} \).

Rules of inference: \( \otimes, \rightarrow, \land \).

Axioms: \( \mathbf{M} \).

Gold: Axiom

Formal completeness (Gold's completeness theorem)

(\( \mathbf{M} \) is a complete formal system)

The \( \mathbf{M} \) proof system

(A. Miller)
Instead of:

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

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

This is logically connect to:

\[ \sigma_1 \rightarrow (\sigma_2 \rightarrow (\sigma_3 \rightarrow \ldots (\sigma_n \rightarrow \sigma_i))) \]

So, it's an axiom of \( T \).

Now, proof:

\[ \sigma \text{ is a logical axiom in } M. \]

\[ \sigma_0, \sigma_1, \sigma_2, \ldots, \sigma_n \] are axioms in \( T \).

Use Modus ponens \( K \) times to get \( \sigma_i \).

So \( T \vdash \sigma_i \).

What's wrong with \( M.M \)?
That the axioms are all logical validities.

What's wrong with this?

We can't recognize the axioms - how do we know whether something is true in all models? (Incompleteness theorem will show us that it's impossible to get an algorithm to decide whether something is a logical validity.)

So we need to cut down our axioms, but we still want to be able to prove all logical validities.
another proof system (ð)

Logical axioms:
1. all formulas in the form of a propositional tautology universally quantified.
   e.g. \( \forall x (\phi \rightarrow (\psi \rightarrow \theta)) \)

2. quantified axioms - universally quantified instances:
   \( \forall x (\exists y (\chi)) \rightarrow (\exists y (\exists \gamma \rightarrow \chi)) \)
   \( \forall x (\epsilon (x) \rightarrow \exists x (\beta (x))) \)
   \( \forall x (\epsilon (x) \rightarrow \forall x (\beta (x))) \)
   \( \forall x (\epsilon (x) \rightarrow \forall x (\beta (x))) \)
   \( \forall x (\epsilon (x)) \rightarrow \forall x (\beta) \)

3. equality axioms
   \( \forall x (x = x) \)
   \( \forall x (\epsilon (x_0 = x_1 = x_2 = x_3 = \ldots) \rightarrow ) \)
   \( \epsilon (x_0', x_1', \ldots, x_n') \).

Rules of inference:

Modal powers.

\( \beta \) is decidable.
Every proof system has its own concept of proof (but it's always based on the formal proof, right?)

Get a concept of T

\[ \exists x \rightarrow \neg(x) \rightarrow \forall x \rightarrow x(x) \]

1. \[ \exists x \rightarrow x(x) \] 2. \[ \exists x \rightarrow x(x) \rightarrow \forall x \rightarrow x(x) \] by MP from 1, 2
3. \[ \forall x \rightarrow x(x) \]
4. \[ \forall x \rightarrow x(x) \rightarrow \neg x(x) \] by MP from 1, 2
5. \[ \forall x \rightarrow x(x) \rightarrow (\forall x \rightarrow x(x)) \rightarrow (\forall x \rightarrow x(x)) \]
6. \[ \forall x \rightarrow x(x) \rightarrow (\forall x \rightarrow x(x)) \] by MP from 1, 5
7. \[ (\forall x \rightarrow x(x)) \rightarrow (\forall x \rightarrow x(x)) \] by MP from 1, 2
8. \[ (\forall x \rightarrow x(x)) \rightarrow (\forall x \rightarrow x(x)) \] by MP from 1, 5
9. \[ (\forall x \rightarrow x(x)) \]

The name exists of a proof = the existence of a model where \( T \) is satisfied by \( \sigma \) is not satisfied by \( \sigma \).

4-color theorem: Say you have a map with touching areas to be different colors. For any map, you can 4-color it.

Haken finally proved this theorem by writing a computer program to check 50,000 cases (reduced for 600). Is that a proof? Doesn't tell us it's true! Thay, 10 yrs ago, computer proved 4,048,057,630 5-color maps, 70 miles long, checked by other computers.
Proof of Decidability in \( \mathfrak{B} \):
\[
(\vdash t \rightarrow \mathcal{Y}) \leftrightarrow (\top, t \vdash \mathcal{Y})
\]

proof:

\[
\begin{align*}
\vdash & \; \mathcal{T} \vdash \mathcal{T} \rightarrow \mathcal{Y} \\
\text{Then} \quad & \; \mathcal{T} \wedge \mathcal{L} \vdash \mathcal{L} \rightarrow \mathcal{Y} \\
& \quad \mathcal{T} \vdash \mathcal{T} \wedge \mathcal{L} \rightarrow \mathcal{L} \rightarrow \mathcal{Y} \\
& \quad \mathcal{T} \vdash \mathcal{T} \rightarrow \mathcal{Y}
\end{align*}
\]

\[
\begin{align*}
\vdash & \; \mathcal{T} \wedge \mathcal{L} \rightarrow \mathcal{Y} \\
& \quad \text{so this is a proof} \; \Theta_1, \ldots, \Theta_n
\end{align*}
\]

Claim: \( \vdash \; \mathcal{T} \vdash \mathcal{L} \rightarrow \Theta_i \) for each \( i \);

proof:

\[
\begin{align*}
(1) & \; \text{if } \Theta_i \text{ is a tautology, then} \\
& \quad \mathcal{L} \rightarrow \Theta_i \text{ is also a tautology,} \\
& \quad \mathcal{T} \vdash \mathcal{L} \rightarrow \Theta_i
\end{align*}
\]

\[
\begin{align*}
(2) & \; \text{if } \Theta_i \text{ arises from a quantifier} \\
& \quad \text{ axiom, then check that } \mathcal{T} \vdash \mathcal{L} \rightarrow \Theta_i \\
& \quad \text{(use } \mathcal{L} \Theta_i \rightarrow (\mathcal{L} \rightarrow Q_i))
\end{align*}
\]

thus \( \mathcal{T} \vdash \mathcal{L} \rightarrow \mathcal{Y} \)

Proof of the Completeness theorem (1929)

In \( \mathfrak{B} = \vdash \top \text{ iff } \vdash \mathcal{Y} \).

Define: \( \mathcal{T} \) is consistent iff \( \mathcal{T} \) does not prove \( \mathcal{L} \wedge \mathcal{L} \) for any \( \mathcal{L} \). Otherwise \( \mathcal{T} \) is "blown up".

\( \mathcal{E} \mathcal{L} \) \( \mathcal{T} \) is inconsistent iff \( \mathcal{T} \vdash \mathcal{L} \) for all \( \mathcal{L} \).

\( \vdash \mathcal{T} \) is strong} 

\( \rightarrow \) \text{ if } \mathcal{T} \vdash \mathcal{L}, \text{ it proves anything.}

\( \text{Recursively Tautology) } \) in \( \mathfrak{B} \)
Lemma: Every consistent theory is satisfiable.

Now, given this lemma, let's prove completeness:

$(\rightarrow)$ (Soundness) if you can prove it's right

$(\leftarrow)$ (Completeness) if it's right you can prove it.

Soundness is easy - axioms and rules are valid in our proof system.

$(\leftarrow)$ (Completeness):

Assume $T \vdash \Theta$

So $T \vdash \Theta$ is not satisfiable.

So $T \vdash \neg \Theta$ is inconsistent.

So $T, \neg \Theta \vdash \bot$

So by Deduction Theorem

$T \vdash \neg \Theta \rightarrow \bot$

$T \vdash (\neg \Theta \rightarrow (\bot \bot)) \rightarrow \bot$ (tautology)

So $T \vdash \bot$. Yay.

Now let's prove the Lemma.

Give Haukás proof:

Claim: If $T$ is consistent, any formula $\phi$, either $T \vdash \phi$ is consistent or $T, \neg \phi$ is consistent.

Proof: if $T \vdash \phi$ is not consistent, then

$T \vdash \bot$.

But then $T \vdash \phi \rightarrow \bot$, so $T \vdash \bot$ (taut).
So $T + \neg C$ has all cases of $T$,
So $T + \neg C$ is consistent

(\textit{vice versa})

Claim: if $T$ is consistent, $C(x)$ is any
particular, $C$ is any new constant, then
$T + \exists x. C(x) \rightarrow C(c)$ is consistent.
(Here in assertion) (Hence consis.)

Theorem on constants: $T + C(x)$ where
$C = \text{a constant not appearing in}$ $T$, then $T + \forall x. C(x)$.

\textit{allows the generic result to be generalised}

Proof: assume $T + C(c)$.
So $\exists \text{ proof } \Theta_0, \ldots, \Theta_k$, $C(c)$
Show that $T + \forall x. \Theta_0 \land \Theta_k$
\[ \forall x (c \rightarrow \Theta_0) \rightarrow \forall x. C(x \rightarrow \forall x. \Theta_0) \]

Proof: If $T + C(c)$, not consistent, then $T + \exists x. \neg C(x)$
By the theorem on (constants), $T + \exists x. C(x) \land$
\[ \forall x \neg C(x) \quad \text{allure or } + \text{ in } T. \]
So $T$ is inconsistent.

Every consistent theory can be
extended to one a complete consistent
Haken. Any such theory is satisfiable.

(but model only (constant constants))