3/15/15

Proof Theory

What is a formal proof? (Formal proofs are rare, even in Math!)

Huge variety of formal proof systems. But they all generally (?) have:

- logical axioms (e.g. $P \to (Q \to P)$) — true in all models
- rules of inference. (e.g. Modus Ponens)

Logical axioms typically include/consist in logical tautologies.

(Hilbert style) (In Theory T of 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 ℓ_i is either

(1) a logical axiom

or (2) an axiom of Theory T

or (3) ℓ_i follows from earlier ℓ_j's by rules of inference

and ℓ is one of the ℓ_i's.

Natural deduction style: proof takes the form of a tree:

$$\dfrac{\dfrac{\cdots}{\ell} \quad \dfrac{\cdots}{\ell \to \psi}}{\psi}$$

("Fitch style") nags a bell.

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

$T \vdash \ell$: "T proves ℓ"
: There's a proof of ℓ from T.

"tautologically implies" (my notation)

Desirable features in a proof system

- Soundness: if $T \vdash \varphi$, then $T \Vdash \varphi$.
  If the logical axioms are valid (true in all models?) and the rules of inference are truth-preserving, then the system is sound.
- completeness: if $T \Vdash \varphi$, then $T \vdash \varphi$.
  (~~we~~ means we can capture logical consequence with just the tools of proof — incredible! Possible? [yes])
- decidability — we want to be able to determine in a purely mechanistic way ~~what~~ whether something is a proof (proofs should be checkable).
  — we should be able to recognize whether something is an axiom and whether some particular φ follows from some other formulas $\varphi_1, \varphi_2 \ldots$ by rules of inference.

for decidable theories - ??

$\boxed{\text{Ex1}}$ (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) " " "
that is sound and complete, but not decidable.

Hints: These are not technical / keep it simple.

Gödel proved completeness from completeness in his system. But in MM we can deduce completeness from compactness (but it's objectionable, so...)

("Micky Mouse")

The MM proof system (A. Miller)

<u>AXIOMS</u>: ALL Logical validities, i.e. if $\models \ell$ (ℓ holds in all Models) then ℓ is an axiom.

<u>rules of inference</u>: $\ell, \ell \to \psi$, deduce ψ.

Theorem: MM is sound and complete, i.e. $T \vdash \sigma \leftrightarrow T \models \sigma$

<u>proof</u>: (Soundness): we want to verify that
- $T \vdash \sigma \to T \models \sigma$.
- if $T \vdash \sigma$ then there is a proof $\ell_0 \dots \ell_n, \sigma$.
- let's verify that $T \models \ell_i$ for all ℓ_i
  - if ℓ_i is an axiom of T, then $T \models \ell_i$
  - if ℓ_i is a logical axiom, then $T \models \ell_i$
  - otherwise, ℓ_i is deduced from other earlier ℓ_J, and $\ell_J \to \ell_i$, since $T \models \ell_J$ and $T \models \ell_J \to \ell_i$
- so $T \models \ell_i$.

(completeness) want: $T \models \sigma$ implies $T \vdash \sigma$

Suppose $T \models \sigma$. By compactness, there is a finite subtheory $(\sigma_0, \sigma_1, \dots \sigma_k) \in T$ such that $\sigma_0 \sigma_1 \dots \sigma_k \models \sigma$.

- So every model of $\sigma_0 \wedge \sigma_1 \wedge \dots \sigma_k$ is a model of σ.

- So $(\sigma_0 \wedge \sigma_1 \wedge \dots \sigma_k) \to \sigma$ is valid

instead of:
$(A \wedge B) \to C$
$= A \to (B \to C)$

- This is logically eq. to:

$\star\ \sigma_0 \to (\sigma_1 \to (\sigma_2 \to \dots (\sigma_k \to \sigma))))$

So it's an axiom of T.

now, proof:

$\star$ is a logical axiom in MM.
$\sigma_0, \sigma_1, \sigma_2 \dots \sigma_k$ are axioms in T.

Use Modus ponens k times to get σ.

So $T \vdash \sigma$.

What's wrong with MM?
That the axioms are all logical validities.
What's wrong with this?

So it's not decidable

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 ($\mathcal{B}$)

Logical axioms:

(1) all formulas in the form of a propositional tautology universally quantified.

e.g. $\forall x(\varphi \to (\psi \to \varphi))$ $\quad \forall x(\varphi \to \neg\varphi)$

(2) quantified axioms - universally quantified instances of:

$\forall z(\forall x\, \varphi(x) \to \varphi(z))$ $\quad z$ is any term

$\forall x(\varphi \to \psi) \to (\forall x\, \varphi \to \forall x\, \psi)$

$\forall x(\varphi(x) \to \exists x\, \varphi(y))$

$\psi \to \forall x\, \psi$, if x does not appear free in ψ.

$\exists x\, \varphi(x) \to \neg\forall x\, \neg\varphi(x)$

(3) equality axioms

$\forall x\, x = x$

$\forall x_0 \ldots x_k, x_0' \ldots x_k',$

$(x_0 = x_0' \wedge x_k = x_k', \ldots) \to$

$\varphi(x_0', x_1' \ldots x_k')$.

rules of inference:

Modus ponens.

$\mathcal{B}$ is decidable.

Every proof system has its own concept of proof (but it's always based on def of formal proof, right?)

Get a concept of $T \vdash \varphi$.

Eg. $\exists x \neg \varphi(x) \vdash \neg \forall x\, \varphi(x)$

? is this T?

1) $\exists x \neg \varphi(x)$ axiom of theory

2) $\exists x \neg \varphi(x) \to \neg \forall x \neg\neg \varphi(x)$ ← one of axiom (2)

3) $\neg \forall x \neg\neg \varphi(x)$ by MP from 1, 2

4) $\forall x\, \varphi(x) \to \neg\neg \varphi(x)$ ← tautology axiom (of (1)).

5) $\forall x (\varphi(x) \to \neg\neg \varphi(x)) \to (\forall x\, \varphi(x) \to \forall x \neg\neg \varphi(x))$

← axiom (quantifier axiom)

6) $\forall x\, \varphi(x) \to \forall x \neg\neg \varphi(x)$ MP 4, 5

7) $[\forall x\, \varphi(x) \to \forall x \neg\neg \varphi(x)] \to [\neg \forall x \neg\neg \varphi(x) \to \neg \forall x\, \varphi(x)]$ ← axiom (tautology axiom)

8) $\neg \forall x \neg\neg \varphi(x) \to \neg \forall x\, \varphi(x)$ MP 6, 7

9) $\neg \forall x\, \varphi(x)$ MP, 8, 3

The nonexistence of a proof of σ = the existence of a model where T is satisfied but σ is not

4-color theorem. Say you have a map, want touching areas to be diff 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 from ∞). Is that a proof? Doesn't tell us why it's true! Thus, 10 yrs ago, computer proof turned into formal deduction ⇒ none of us can minute proof, miles long, checked by other computers.

Proof of Deductive thm in $\mathcal{B}$:

$(T \vdash \varphi \to \psi) \longleftrightarrow (T, \varphi \vdash \psi)$

proof:

$\to$ $T \vdash \varphi \to \psi$

Then $T \wedge \varphi \vdash \varphi \to \psi$

Th $T \wedge \varphi \vdash \varphi$, $T \wedge \varphi \vdash \varphi \to \psi$.

Th $T \wedge \varphi \vdash \psi$

$\leftarrow$ $T \wedge \varphi \vdash \psi$

So there's a proof $\theta_0, \theta_1, \ldots \theta_n$

Claim: $T \vdash \varphi \to \theta_i$ for each i

proof: (1) if θ_i is a tautology, Then $\varphi \to \theta_i$ is also a tautology, So $T \vdash \varphi \to \theta_i$

(2) if θ_i is φ itself, then $T \vdash \varphi \to \theta_i$, since it's a tautology

(3) If θ_i arises from a quantifier axiom, Then check that $T \vdash \varphi \to \theta_i$, (use $\theta_i \to (\varphi \to \theta_i)$)

$\vdots$

Thus $T \vdash \varphi \to \psi$

Proof of The Completeness Theorem (Gödel 1929) in $\mathcal{B}$: $T \vdash \sigma$ iff $T \models \sigma$.

Define: T is consistent iff T does not prove $\varphi \wedge \neg\varphi$ for any φ. Otherwise T is inconsistent.

$\boxed{\text{Ex2}}$ T is inconsistent iff $T \vdash \varphi$ for all φ.

"Blow up"

$\leftarrow$ is easy

$\to$ if it proves a $\perp$, it proves anything (need a certain tautology) in $\mathcal{B}$

<u>Lemma</u>: every consistent theory is satisfiable.

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

($\longrightarrow$) (soundness) if you can prove it it's right
($\longleftarrow$) (completeness) if it's right you can prove it.

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

($\longleftarrow$ completeness):

assume $T \not\vdash \sigma$

So $T + \neg\sigma$ is not satisfiable.

So $T + \neg\sigma$ is inconsistent

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

So by deduction theorem

$T \vdash \neg\sigma \longrightarrow \bot$

$T \vdash (\neg\sigma \to (\bot)) \to \sigma$ (tautology)

So $T \vdash \sigma$. yay.

Now let's prove the <u>lemma</u>.
Gene Hahn's proof:

Claim: if T is consistent, for any formula ℓ, either $T + \ell$ is consistent or $T + \neg\ell$ is consistent

Proof if $T + \ell$ is not consistent, then
$T, \ell \vdash \bot$.
But then $T \vdash \ell \to \bot$, so $T \vdash \neg\ell$ (tautology)

So $T + \neg \ell$ has same consequences of T,
So $T + \neg \ell$ is consistent

(+ vice versa)

Claim: if T is consistent, $\ell(x)$ is any formula, c is any new constant, then $T + \exists x\, \ell(x) \to \ell(c)$ is consistent.
(Henkin assertion) (lemma constant.)

Theorem on constants: $T \vdash \ell(x)$ where c = a constant not appearing in T, then $T \vdash \forall x\, \ell(x)$.

allows generic results to be generalized.

:(Proof: assume $T \vdash \ell(c)$.
So $\exists$ proof $\theta_0 \ldots \theta_k$, $\ell(c)$
Show that $T \vdash \forall x\, \theta_i(x)$ for each θ_i
$\forall x\, (\ell \to \psi) \to (\forall x\, \ell \to \forall x\, \psi)$

:(proof: If (T is) inconsistent, then $T \vdash \exists x\, \ell(x) \wedge \neg \ell(c)$

By the Theorem on constants, $T \vdash \exists x\, \ell(x) \wedge \forall x\, \neg \ell(x)$ derive a $\perp$ in T.
So T is consistent.

:(Every consistent theory can be extended to a complete consistent Henkin theory. Every such theory is satisfiable.
(buildModel for Henkin constants)