CHAPTER 2 DEDUCTIONS

2.2 Deductions

What do we mean by proof?

Rough Idea:

using some axioms/assumptions, we continue to infer new true statements, until we arrive at what we wanted to prove.

So,

- a proof will be a string of true statements
- each statement should either be
  - an axiom or assumption, or
  - be infered from earlier statements

e.g. $P, P \to Q, Q$

want extra properties like decidability

Defined and fixed later

Def Let

- Λ be a set of $\mathcal{L}$-formulas (the logical axioms)
- Σ be a set of $\mathcal{L}$-formulas (the non-log. axioms)
- D be a finite sequence $(\phi_1, \ldots, \phi_n)$ of $\mathcal{L}$-formulas.

Then we call <u>D a deduction from Σ</u> if for all $1 \le i \le n$, either

1. $\phi_i \in \Lambda$,
2. $\phi_i \in \Sigma$, or
3. there is a rule of inference (Γ, ϕ_i) with $\Gamma \subseteq \{\phi_1, \ldots, \phi_{i-1}\}$.

RI

Defined and fixed later

Compare with Prop. 2.2.4

* We say <u>D is a deduction from Σ of ϕ_n</u> and write $\Sigma \vdash \phi_n$

About Λ and (Γ, ϕ)... among other things we will want

- every $\alpha \in \Lambda$ is valid, i.e. $\models \alpha$.
- RIs preserve truth, i.e. $\Gamma \models \phi$

<u>Ex</u>

Let $\Lambda = \emptyset$

Let rules of inference be $\{ \underbrace{(\{\alpha, \alpha \to \beta\}, \beta)}_{\text{modus ponens}} \mid \alpha, \beta \text{ are } \mathcal{L}\text{-form.} \}$

Let $\Sigma = \{ \forall x\, P(x,x),\ P(u,v),$
$P(v,u) \to P(u,u),\ P(v,u) \to P(v,v),$
$P(u,v) \to P(v,u) \}$.

① Show $\Sigma \vdash P(u,u)$.

Σ	$P(u,v)$	Incorrect Ded.
Σ	$P(u,v) \to P(v,u)$	$\forall x\, P(x,x)$
RofI	$P(v,u)$	$P(u,u)$
Σ	$P(v,u) \to P(u,u)$	
RofI	$P(u,u)$	

② Explain why $\Sigma \nvdash P(v,v)$.

<u>Def</u> Assuming Λ, Σ, and the RofI are fixed, we define $Thm_\Sigma = \{ \phi \mid \Sigma \vdash \phi \}$

all formulas deducible from Σ
<u>OR</u>
the theorems generated by Σ via deductions

<u>Ex</u> In last example

$Thm_\Sigma = \Sigma \cup \{ P(v,u), P(u,u) \}$.

Prop. 2.2.4 Thm_Σ is the smallest set C of $\mathcal{L}$-formulas such that

1. $\Sigma \subseteq C$,
2. $\Lambda \subseteq C$, and
3. if (Γ, θ) is a R of I with $\Gamma \subseteq C$, then $\theta \in C$.

pf

① Show Thm_Σ satisfies 1–3.

- If $\alpha \in \Sigma \cup \Lambda$ then (α) is a deduction of α, so $\alpha \in Thm_\Sigma$. Thus $\Sigma \cup \Lambda \subseteq Thm_\Sigma$.
- Let (Γ, ϕ) be a R of I with $\Gamma \subseteq Thm_\Sigma$. Rember: Γ is finite, so $\Gamma = \{\alpha_1, \dots, \alpha_m\} \subseteq Thm_\Sigma$. Thus, there is a deduction D_i of α_i from Σ. Then $D_1 \cup \dots \cup D_m \cup \{\phi\}$ (with obvious meaning) is a deduction of ϕ from Σ.

② Show that if C satisfies 1–3, then $Thm_\Sigma \subseteq C$.

Let $\phi \in Thm_\Sigma$. Proceed by induction on the length of the shortest deduction of ϕ from Σ. If $\phi \in \Sigma \cup \Lambda \subseteq C$ then $\phi \in C$. Otherwise, we may assume there is a R of I (Γ, ϕ) s.t. $\Gamma \subseteq C$ (by induction). Thus, by 3, $\phi \in C$.

$\square$

2.3 Logical Axioms

These will be about equality and quantifiers.

<u>Def</u> The set of logical axioms, Λ, is defined as follows:

- For every variable x in $\mathcal{L}$,

(E1) $\underline{x = x}$ is in Λ

- For all variables $x_1, \ldots, x_n, y_1, \ldots, y_n$ and all function symbols f and all relation symbols R,

(E2) $\underline{\left[(x_1 = y_1) \wedge \cdots \wedge (x_n = y_n)\right] \to f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)}$

and

(E3) $\underline{\left[(x_1 = y_1) \wedge \cdots \wedge (x_n = y_n)\right] \to \left[R(x_1, \ldots, x_n) \to R(y_1, \ldots, y_n)\right]}$

are in Λ

- For every variable x in $\mathcal{L}$, every $\mathcal{L}$-term t, and every $\mathcal{L}$-formula ϕ, <u>if</u> <u>t is subtitutable for x in ϕ</u>, then

(Q1) $\underline{(\forall x)(\phi) \to \phi^x_t}$

and

(Q2) $\underline{\phi^x_t \to (\exists x)(\phi)}$

are in Λ

- There are no other formulas in Λ

Q: how many formulas are in Λ?

2.4 Rules of Inference

I. Propositional Consequence

Remember logic from 108? we had things like

$$\neg(A \vee B) \approx (\neg A) \wedge (\neg B) \qquad \text{(DeMorgan)}$$

↑ logically equivalent

Here, $A, B, \ldots$ were propositional variables and were always assigned values of T or F. Then we could prove things like the one above with a truth table

A	B	$A \vee B$	$\neg(A \vee B)$	$\neg A$	$\neg B$	$(\neg A) \wedge (\neg B)$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

Same!

Also, a propositional formula is a tautology if it is always true, e.g. $A \vee (\neg A)$

A	$\neg A$	$A \vee \neg A$
T	F	T
F	T	T

← always true!

We now define a function to convert first-order formulas to proposital formulas.

Running Example Let

$$\beta :\equiv \left[(\forall u)(P(u)) \wedge f(y)=z\right] \to \left[(\forall z)\left[(\exists y)(f(y)=z)\right] \vee (\forall u)P(u)\right]$$

1. Find all subformulas of β of the form $(\forall x)(\alpha)$ that are NOT in the scope of another quantifier and systematically replace them with a prop. variable. (Repeat for all such subformulas)

2. Systematically replace all remaining atomic formulas with new prop. variables.

$$\beta_p :\equiv (A \wedge B) \to (C \vee A)$$

Notice that β_p is a tautology since

A	B	C	$A \wedge B$	β_p
T	T		T	T
T	F		F	T
F	T		F	T
F	F		F	T

Does not depend on C — o/w need 8 rows

Fact β_p a tautology $\Longrightarrow$ β_p is valid, i.e. $\models \beta$

converse is not (always) true.

using Lemma 2.4.2

Def Let $\Gamma = \{\alpha_1, \dots, \alpha_n\}$ be a finite set of $\mathcal{L}$-formulas, and ϕ another $\mathcal{L}$-formua. Let $\Gamma_p = \{\alpha_{1p}, \dots, \alpha_{np}\}$, ϕ_p be the results of applying the above conversion procedure uniformly to all of the $\mathcal{L}$-formulas. We say that ϕ is a propositional consequence of Γ if

$$[\alpha_{1p} \wedge \alpha_{2p} \wedge \dots \wedge \alpha_{np}] \rightarrow \phi_p$$

is a tautology.

See Ex 2.4.4

II. The Rules of inference

- Whenever ϕ is a propositional cons. of Γ,

(PC) (Γ, ϕ) is a rule of inference

- For all formulas ϕ and ψ and all variables x that are NOT free in ψ

(QR) $(\{\psi \rightarrow \phi\}, \psi \rightarrow (\forall x \phi))$ and

$(\{\phi \rightarrow \psi\}, (\exists x \phi) \rightarrow \psi)$

are rules of inference.

- There are no other rules.

To clarify

- If you prove α and β and

$$[\alpha \wedge \beta \to \phi]_p$$

is a tautology, then you can conclude ϕ.

- Provided x is NOT free in ψ,
  - from $\psi \to \phi$ you can deduce $\psi \to \forall x\, \phi$
  - from $\phi \to \psi$ " " " $\exists x\, \phi \to \psi$

Important Note

- The set of RofIs is decidable: there is algorithm (think comp. prog.) that given a finite set of $\mathcal{L}$-formulas Γ and $\mathcal{L}$-form. ϕ can decide (in a finite amount of time) if (Γ, ϕ) is a RofI or not.

- Also, Λ is decideable

2.5 Soundness

The goal of this section is to prove:

<u>Theorem 2.5.3.</u> (Soundness) If $\Sigma \vdash \phi$, then $\Sigma \models \phi$.

of our deductive system (Λ and RofI)

* Σ is a set of formulas. Soundness says

"if assuming Σ, we can prove ϕ, then any structure that thinks Σ is true, will also think ϕ is true."

OR

"if we can prove it, it's true."

OR

"proofs preserve truth."

Recap of requirements for our deductive system:

exercises
1. ✓ an algorithm can decide if $\theta \in \Lambda$ or not
2. ✓ an algorithm can decide, given finite Γ, if (Γ, θ) is a RofI.
3. ✓ Γ is finite for every RofI (Γ, θ)
4. $\models \Lambda$
5. RofIs preserve truth: if (Γ, θ) is an RofI, then $\Gamma \models \theta$

Theorem 2.5.1 $\models \Lambda$

pf Let $\alpha \in \Lambda$ and let s be any vaf. We show $\mathfrak{M} \models \alpha[s]$. Note: is of type E1, E2, E3, Q1, or Q2.

Claim: If α has type E3, then $\mathfrak{M} \models \alpha[s]$.

pf of claim.

- α has the form

$$(x_1 = y_1) \wedge \cdots \wedge (x_n = y_n) \to (R(x_1, \ldots, x_n) \to R(y_1, \ldots, y_n))$$

- Assume

$\mathfrak{M} \models s(x_1) = s(y_1) \wedge \cdots \wedge s(x_n) = s(y_n)$

and

$\mathfrak{M} \models (s(x_1), \ldots, s(x_n)) \in R^{\mathfrak{M}}$

- Thus

$\mathfrak{M} \models (s(y_1), \ldots, s(y_n)) \in R^{\mathfrak{M}}$, so $\mathfrak{M} \models \alpha[s]$.

Claim: If α has type Q1, then $\mathfrak{M} \models \alpha[s]$

- α has the form $(\forall x\, \phi) \to \phi^x_t$ where t is sub. for x.

- Assume $\mathfrak{M} \models (\forall x\, \phi)[s]$, so $\mathfrak{M} \models \phi[s[x|m]]$ for all $m \in M$.

- Thus, $\mathfrak{M} \models \phi[s[x|\bar{s}(t)]]$

- $\boxed{\text{Need Thm 2.6.2: } \mathfrak{M} \models \phi[s[x|\bar{s}(t)]] \leftrightarrow \mathfrak{M} \models \phi^x_t[s]}$

- Thus $\mathfrak{M} \models \phi^x_t[s]$, so $\mathfrak{M} \models \alpha[s]$.

<u>Claim</u>: If α has type E1, E2, Q2, Then $\mathfrak{M} \models \alpha[s]$.

pf of claim: book + exercises.

$\square$

<u>Thm 2.52</u> If (Γ, Θ) is a R of I, then $\Gamma \models \Theta$

<u>pf</u> Let $\mathfrak{M}$ be an structure. Assume $\mathfrak{M} \models \Gamma[s]$ for every va f s; we must show $\mathfrak{M} \models \Theta[r]$ for every r.

Let r be an arbitrary va f.

<u>Claim</u>: If (Γ, Θ) has type PC, then $\mathfrak{M} \models \Theta[r]$.

<u>pf</u> see the book.

<u>Claim</u>: If (Γ, Θ) has type QR, then $\mathfrak{M} \models \Theta[r]$.

<u>pf</u>

- (Γ, Θ) has the form

  1. $(\{\psi \to \phi\}, \psi \to (\forall x \phi))$ OR
  2. $(\{\phi \to \psi\}, (\exists x \phi) \to \psi)$

  with x <u>not free in ψ</u>.

- we only treat 1; 2 is an exercise.
- So, assume $\mathfrak{M} \models (\psi \to \phi)[s]$ for every va f s. $*$
- Also, assume $\mathfrak{M} \models \psi[r]$; WTS $\mathfrak{M} \models (\forall x \phi)[r]$ $**$

To show $\mathfrak{M} \models \forall x \phi[r]$, let $m \in M$; we will show $\mathfrak{M} \models \phi[r[x|m]]$.

Observe,

$$\mathcal{M} \models \psi[r] \qquad \text{by } \star\star$$

$$\Longrightarrow \underline{\mathcal{M} \models \psi[r[x|m]]} \qquad \text{since } x \text{ is } \underline{\text{not}} \text{ free in } \psi \quad (\text{Prop } 1.7.7)$$

Also, $\underline{\mathcal{M} \not\models \psi[r[x|m]] \text{ or } \mathcal{M} \models \phi[r[x|m]]}$ by $\star$

(with $s = r[x|m]$). Thus, $\mathcal{M} \models \phi[r[x|m]]$. $\square$

<u>Theorem 2.5.3.</u> (Soundness) If $\Sigma \vdash \phi$, then $\Sigma \models \phi$.

<u>pf</u>

formulas provable from Σ.

formulas logically implied by ϕ

Let $Thm_\Sigma = \{\phi \mid \Sigma \vdash \phi\}$; let $X = \{\phi \mid \Sigma \models \phi\}$.

WTS $Thm_\Sigma \subseteq X$; we use Prop 2.2.4, which says that <u>if</u>

1. $\Sigma \subseteq X$,
2. $\Lambda \subseteq X$, and
3. if (Γ, θ) is a R of I with $\Gamma \subseteq X$, then $\theta \in X$

<u>then</u> $Thm_\Sigma \subseteq X$. Let's check the list.

1. Certainly $\mathcal{M} \models \Sigma \Rightarrow \mathcal{M} \models \Sigma$, so $\Sigma \subseteq X$.
2. Since $\models \Lambda$ (Thm 2.5.1), it's certainly true that $\mathcal{M} \models \Sigma \Rightarrow \mathcal{M} \models \Lambda$, so $\Lambda \subseteq X$.
3. Let (Γ, θ) be an R of I with $\Gamma \subseteq X$. Assume $\mathcal{M} \models \Sigma$; WTS $\mathcal{M} \models \theta$. Now, $\Gamma \subseteq X$, so $\mathcal{M} \models \Sigma \Rightarrow \mathcal{M} \models \Gamma$. Thus $\mathcal{M} \models \Gamma$, so by Thm 2.5.2, $\mathcal{M} \models \theta$. $\square$

2.7 Properties of our deductive system

Thm 2.7.1 Our ded. system can prove that $=$ is an equiv. relation. That is,

1. $\vdash x = x$
2. $\vdash x = y \to y = x$
3. $\vdash (x = y \wedge y = z) \to x = z$

pf

See book.

Lem 2.7.2 $\Sigma \vdash \theta$ iff $\Sigma \vdash \forall x\, \theta$

pf

($\Longrightarrow$) Assume $\Sigma \vdash \theta$. Let y be a var. diff. than x.

Deduction of $\forall x\, \theta$

(insert ded. of θ)

θ	
$y = y$	$\wedge$
$y = y \to \theta$	PC: $\theta \to (y = y \to \theta)$
$y = y \to \forall x\, \theta$	QR: x not free in $y = y$
$\forall x\, \theta$	PC: $(y = y \wedge (y = y \to \forall x\, \theta)) \to \forall x\, \theta$

($\Longleftarrow$) Assume $\Sigma \vdash \forall x\, \theta$. Note θ is the same as θ^x_x

Deduction of θ

(insert ded. of $\forall x\, \theta$)

$\forall x\, \theta$	
$\forall x\, \theta \to \theta^x_x$	QI
θ^x_x	PC

$\square$

Lemma 2.7.3 Suppose $\Sigma \vdash \theta$. Let $\alpha \in \Sigma$.

1. Suppose $\alpha :\equiv \forall x \beta$. If Σ' is Σ with α replaced by β, then $\Sigma' \vdash \theta$

2. Let $\gamma :\equiv \forall x \alpha$. If Σ' is Σ with α repl. by γ, then $\Sigma' \vdash \theta$.

pf By the previous lemma $\Sigma' \vdash \Sigma$, so as $\Sigma \vdash \theta$, $\Sigma' \vdash \theta$.

Thm 2.7.4 (Deduction Thm) Let θ be a sentence and Σ a set of formulas. Then for any formula ϕ,

$$\Sigma \cup \theta \vdash \phi \quad \text{iff} \quad \Sigma \vdash (\theta \to \phi)$$

optional

pf
($\Leftarrow$) Assme $\Sigma \vdash (\theta \to \phi)$. Then as $\Sigma \cup \theta \vdash \theta$, $\Sigma \cup \theta \vdash \phi$ (by PC).

($\Rightarrow$) Assue $\Sigma \cup \theta \vdash \phi$. Let $X = \{\psi \mid \Sigma \vdash (\theta \to \psi)\}$. we show $Thm_{\Sigma \cup \theta} \subseteq X$ implying that $\phi \in X$, which is what we want. We use Prop. 2.2.4.

① • $\Sigma \subseteq X$ by PC: $\theta \to$ true is true
• $\theta \subseteq X$ by PC: $\theta \to \theta$ is a tautology

② $\Lambda \subseteq X$ by PC

③ Let (Γ, α) be an RofI with $\Gamma \subseteq X$.
Let $\Gamma = \{\gamma_1, \dots, \gamma_n\}$. So $\Sigma \vdash (\theta \to \gamma_i)$

∘ type PC:

α is a prop. cons. of $\{\gamma_1, \dots, \gamma_n\}$

$\Longrightarrow$ $\theta \to \alpha$ is a " " " $\{\theta \to \gamma_1, \dots, \theta \to \gamma_n\} = \Gamma'$

$\Longrightarrow$ $\Sigma \vdash (\theta \to \alpha)$ since $\Sigma \vdash \Gamma'$

$\Longrightarrow$ $\alpha \in X$

∘ type QR (universal)

$\Gamma = \{\beta \to \delta\}$ $\quad$ $\alpha :\equiv \beta \to \forall x \delta$

with x not free in β.

$$\Gamma \subseteq X \Longrightarrow \Sigma \vdash \theta \to (\beta \to \delta)$$

$$\Longrightarrow \Sigma \vdash (\theta \wedge \beta) \to \delta \qquad \text{by PC}$$

$$\Longrightarrow \Sigma \vdash \theta \wedge \beta \to \forall x \delta$$

θ is a sent. so x not free in θ... nor in β by assump.

$$\Longrightarrow \Sigma \vdash \theta \to (\underbrace{\beta \to \forall x \delta}_{\alpha})$$

$$\Longrightarrow \alpha \in X.$$

∘ type QR (ext.): similar

Thus, Prop 2.2.4 applies. $\square$