Introduction to Formal Proof

Bernard Sufrin

Trinity Term 2018

1: Formal Proofs in Propositional Calculus

Introduction

▷ A calculus by which the *validity* (correctness) of propositional conjectures is judged

▷ A propositional conjecture has some *premisses* and a *conclusion*

▷ Example 1:

It is raining
If *I wear a hat* **and** *it is raining* **then** *my head stays dry*
My head is not dry
I therefore conclude that
I am not wearing a hat

▷ Question: is this conjecture valid?

▷ Example 2:

It is raining

If *I wear a hat* **and** *it is raining* **then** *my head stays dry*

My head is dry

I therefore conclude that

I am wearing a hat

Question: is this conjecture valid?

▷ Example 3:

I conclude (without premisses) that

If *today is Tuesday* **then** *we are in Paris*

Question: is this conjecture valid?

Propositional Language: propositions

- ▷ A *proposition* is a meaningful declarative sentence that may be true or false in a situation.
- ▷ Examples:
  - ◦ "Socrates is mortal"
  - ◦ "The King's Arms is at the junction of Cornmarket with High Street"
  - ◦ "I am hungry"
  - ◦ "Tony Blair is a war-criminal"
  - ◦ "It is raining and my head is wet"
  - ◦ "If I wear a hat and it is raining then my head stays dry"
- ▷ But not
  - ◦ "Do you like green eggs and ham?"
  - ◦ "Can you catch it in your hat?"
  - ◦ "Let's go!"
  - ◦ "Don't mention the war."

Propositional Language: atomic propositions

▷ An *atomic proposition* is a proposition with no logical connectives in it.

▷ Examples:

- "Socrates is mortal"
- "The King's Arms is at the junction of Cornmarket with High Street"
- "I am hungry"
- "Tony Blair is a war-criminal"

▷ But not

- "It is raining and my head is wet" ("... and ...")
- "If I wear a hat and it is raining then my head stays dry" ("if ... and ... then ...")

Symbolic representation

- ▷ Atomic propositions denoted by letters/identifiers
- ▷ Propositional connectives written in symbols

It is raining	R
If *I wear a hat* **and** *it is raining* **then** *my head stays dry*	$(H \wedge R) \rightarrow D$
My head is not dry	$\neg D$
I therefore conclude that	———
I am not wearing a hat	$\neg H$

- ▷ **... therefore ...** separates the premisses of a conjecture from its conclusion

  It is not a propositional connective

Composing Propositions with Logical Connectives

$$\left.\begin{array}{ll} \triangleright \text{ not } \ldots & \neg\phi \\ \triangleright \ldots \text{ and } \ldots & \phi \wedge \psi \\ \triangleright \ldots \text{ or } \ldots & \phi \vee \psi \\ \triangleright \text{ if } \ldots \text{ then } \ldots & \phi \to \psi \\ \triangleright \ldots \text{ if and only if } \ldots & \phi \leftrightarrow \psi \end{array}\right\} \text{ where } \phi \text{ and } \psi \text{ are propositions}$$

- ▷ The connectives are not independent of each other
- ▷ There are other connectives, but these are the most common
- ▷ Sometimes other symbols are used for connectives (typically $\Rightarrow, \Leftrightarrow$ for $\to, \leftrightarrow$)

Parsing

▷ Priority of connectives is (in descending order) $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$

- $\rightarrow$ has slightly higher priority on its right than on its left
- Some texts give $\wedge$ the same priority as $\vee$
- (Jape gives $\wedge$ and $\vee$ slightly higher priority on their left)

▷ If in doubt, parenthesize!

▷ Examples:

- $\underline{(\underline{A \wedge B} \rightarrow \underline{C \vee D})} \leftrightarrow \overline{A \rightarrow \overline{B \rightarrow \overline{C \vee D}}}$
- $\underline{\neg \underline{\neg A}} \rightarrow A$
- $\overline{\overline{A \vee B} \vee C} \vee \underline{\underline{D \wedge E} \wedge F}$

Presenting a conjecture

- ▷ Informal: "if you accept *these premisses*[1] then you should accept *this conclusion*"
- ▷ Formal: "from *these premisses* we may validly infer *this conclusion*."
  - ∘ In horizontal form: $premiss, premiss, premiss, \ldots \vdash conclusion$
  - ∘ In vertical form:

$$\frac{premiss \qquad premiss \qquad premiss \qquad \ldots}{conclusion}$$

- ▷ *e.g.* the conjecture:

$$R, H \wedge R \rightarrow D, D \vdash H \qquad\qquad \frac{R \qquad H \wedge R \rightarrow D \qquad D}{H}$$

- ▷ *e.g.* the conjecture:

$$R, H \wedge R \rightarrow D, \neg D \vdash \neg H \qquad\qquad \frac{R \qquad H \wedge R \rightarrow D \qquad \neg D}{\neg H}$$

[1] i.e. their truth

What is the nature of a valid conjecture?

- Propositional calculus is a formal system that we use to judge the validity of conjectures.
- The validity of a conjecture is judged *solely from its form*, not on the meanings/interpretations of the atomic propositions.
- The validity of $R, H \wedge R \rightarrow D, \neg D \vdash \neg H$
  - is independent of the interpretation H, R, D in the real world.
  - *does not* establish the truth of the premisses.
  - *so should not, on its own,* convince you that $\neg H$
- An alternative interpretation

  R "there are roses in my garden"

  H "there's a hedgehog in my garden"

  D "I am depressed"

What is the purpose of a proof system?

- ▷ **If you know only that a particular conjecture has been proven:**
  - ∘ When the premisses are all true then you should accept the conclusion
  - ∘ When some of the premisses are untrue then you need not accept the conclusion
- ▷ **If you know only that a conjecture has not (yet) been proven:**
  - ∘ Then you need not (yet) accept the conclusion, even if all the premisses are true

▷ Example conjecture: commutativity of conjunction: (for any propositions ϕ and ψ)

$$\frac{\psi \wedge \phi}{\phi \wedge \psi} \qquad\qquad \psi \wedge \phi \vdash \phi \wedge \psi$$

- "from $\psi \wedge \phi$ we can infer $\phi \wedge \psi$"
- "if we have established $\psi \wedge \phi$ then we can infer $\phi \wedge \psi$"

▷ Intuitive argument

1. Take $\psi \wedge \phi$ as a premiss
2. Since we have established (by premiss) $\psi \wedge \phi$ we can infer ϕ
3. Since we have established (by premiss) $\psi \wedge \phi$ we can infer ψ
4. Since we established (on the previous two lines) both ϕ and ψ we can infer $\phi \wedge \psi$

▷ Here we use the words *infer*, *conclude*, and *deduce* more or less interchangeably.

▷ We say that a proposition has been *established* in a proof of a conjecture if it is a premiss or has been inferred / concluded / deduced (directly or indirectly) from the premisses of the conjecture by means of the proof rules that we are using.

Proof Rules for conjunction

▷ "and introduction":

- In a proof in which we have established ϕ and established ψ, we can conclude $\phi \wedge \psi$

$$\frac{\phi \qquad \psi}{\phi \wedge \psi}\ \wedge\text{-intro}$$

▷ "and elimination"

- In a proof in which we have established $\phi \wedge \psi$, we can conclude ϕ

$$\frac{\phi \wedge \psi}{\phi}\ \wedge\text{-elim-L}$$

- In a proof where we have established $\phi \wedge \psi$, we can conclude ψ

$$\frac{\phi \wedge \psi}{\psi}\ \wedge\text{-elim-R}$$

- Formal presentations of the proof
  - In linear form

1:	$\psi \wedge \phi$	premiss
2:	ϕ	$\wedge$-elim-R 1
3:	ψ	$\wedge$-elim-L 1
4:	$\phi \wedge \psi$	$\wedge$-intro 2, 3

  - As a tree

$$\dfrac{\dfrac{\dfrac{}{\psi \wedge \phi}\ \text{premiss}}{\phi}\ \wedge\text{-elim-R} \qquad \dfrac{\dfrac{}{\psi \wedge \phi}\ \text{premiss}}{\psi}\ \wedge\text{-elim-L}}{\phi \wedge \psi}\ \wedge\text{-intro}$$

- The proof tree is complete because its root is the conclusion of the conjecture and each leaf is a premiss of the conjecture.

- ▷ The proof rules are parameterized by ϕ and ψ
- ▷ View them as functions that construct proofs from proofs
- ▷ Example: proof that $\phi \wedge (\psi \wedge \kappa) \vdash (\phi \wedge \psi) \wedge \kappa$

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{premiss}
\UnaryInfC{$\phi \wedge (\psi \wedge \kappa)$}
\RightLabel{$\wedge$-elim-L}
\UnaryInfC{ϕ}
\AxiomC{}
\RightLabel{premiss}
\UnaryInfC{$\phi \wedge (\psi \wedge \kappa)$}
\RightLabel{$\wedge$-elim-R}
\UnaryInfC{$\psi \wedge \kappa$}
\RightLabel{$\wedge$-elim-L}
\UnaryInfC{ψ}
\RightLabel{$\wedge$-intro}
\BinaryInfC{$\phi \wedge \psi$}
\AxiomC{}
\RightLabel{premiss}
\UnaryInfC{$\phi \wedge (\psi \wedge \kappa)$}
\RightLabel{$\wedge$-elim-R}
\UnaryInfC{$\psi \wedge \kappa$}
\RightLabel{$\wedge$-elim-R}
\UnaryInfC{κ}
\RightLabel{$\wedge$-intro}
\BinaryInfC{$(\phi \wedge \psi) \wedge \kappa$}
\end{prooftree}
$$

- ▷ The proof tree is complete because its root is the conclusion of the conjecture and each leaf is a premiss of the conjecture.

▷ Same proof (linear presentation)

1:	$\phi \wedge (\psi \wedge \kappa)$	premiss
2:	ϕ	$\wedge$-elim-L 1
3:	$\psi \wedge \kappa$	$\wedge$-elim-R 1
4:	ψ	$\wedge$-elim-L 3
5:	$\phi \wedge \psi$	$\wedge$-intro 2 4
6:	κ	$\wedge$-elim-R 3
7:	$(\phi \wedge \psi) \wedge \kappa$	$\wedge$-intro 5, 6

▷ In this proof the pattern for each rule is matched in more than one way

Proof Rules for disjunction

▷ Introduction rules are straightforward

$$\frac{\phi}{\phi \vee \psi}\ \vee\text{-intro-L}$$

$$\frac{\psi}{\phi \vee \psi}\ \vee\text{-intro-R}$$

▷ Elimination rule captures the idea of case analysis

$$\frac{(\phi \vee \psi) \quad \boxed{\begin{array}{c}\phi\\ \vdots\\ \kappa\end{array}} \quad \boxed{\begin{array}{c}\psi\\ \vdots\\ \kappa\end{array}}}{\kappa}\ \vee\text{-elim}$$

▷ We can conclude κ in a proof in which we have established $\phi \vee \psi$ and in which we have

(a) established κ by assuming ϕ, and

(b) established κ by assuming ψ

▷ We have established $(\phi \vee \psi)$, *i.e.* that at least one of ϕ and ψ hold, but not which of them

▷ Having *both* proof (a) and proof (b) means it doesn't matter which

▷ $\boxed{\begin{array}{c}\alpha\\ \vdots\\ \kappa\end{array}}$ means: *this particular instance of* α cannot be referenced outside the supbroof of κ

▷ Case study: proof of $E \vee (F \wedge G) \vdash (E \vee F) \wedge (E \vee G)$

1:	$E \vee F \wedge G$	premise
2:	E	assumption
3:	$E \vee F$	$\vee$ intro 2
4:	$E \vee G$	$\vee$ intro 2
5:	$(E \vee F) \wedge (E \vee G)$	$\wedge$ intro 3,4
6:	$F \wedge G$	assumption
7:	G	$\wedge$ elim 6
8:	F	$\wedge$ elim 6
9:	$E \vee F$	$\vee$ intro 8
10:	$E \vee G$	$\vee$ intro 7
11:	$(E \vee F) \wedge (E \vee G)$	$\wedge$ intro 9,10
12:	$(E \vee F) \wedge (E \vee G)$	$\vee$ elim 1,2-5,6-11

What makes this proof **formal** is that it doesn't depend on the **meanings** of E, F, or G or of the premiss or the conclusion, it just depends on the **syntactic forms** of the premiss and the conclusion and the propositions (formulæ) that arise in the course of the proof.

Proof rules as "conjecture transformers"

▷ Q: But how did I go about *finding* the proof of $E \vee (F \wedge G) \vdash (E \vee F) \wedge (E \vee G)$?

▷ A: At each stage I used a proof rule to transform a conjecture (the goal) to the set of conjectures that need to be proved in order for it to hold (the subgoals).

A subgoal that's an assumption (or premiss) requires no further work.

▷ The starting goal (the original conjecture) is:

$$\begin{array}{lll} \text{1:} & E \vee (F \wedge G) & \text{premiss} \\ & \cdots & \\ \text{2:} & (E \vee F) \wedge (E \vee G) & \end{array}$$

- We guess from the form of the premiss that we can finish the proof with ∨-elim
- Using this rule transforms the starting goal into two subgoals

1:	E∨F∧G	premise
2:	E	assumption
	. . .	
3:	(E∨F)∧(E∨G)	
4:	F∧G	assumption
	. . .	
5:	(E∨F)∧(E∨G)	
6:	(E∨F)∧(E∨G)	∨ elim 1,2-3,4-5

(alternate guess is that we can finish the proof with ∧-intro)

▷ Working on the first subgoal: we guess we can finish with ∧-intro

1:	$E \vee F \wedge G$	premise
2:	E	assumption
	$\ldots$	
3:	$E \vee F$	
	$\ldots$	
4:	$E \vee G$	
5:	$(E \vee F) \wedge (E \vee G)$	∧ intro 3,4
6:	$F \wedge G$	assumption
	$\ldots$	
7:	$(E \vee F) \wedge (E \vee G)$	
8:	$(E \vee F) \wedge (E \vee G)$	∨ elim 1,2-5,6-7

This yields two nested subgoals (2...3) and (2...4) – one for each conjunct

▷ After two ∨-intro steps we have completed the first subgoal

1:	$E \vee F \wedge G$	premise
2:	E	assumption
3:	$E \vee F$	∨ intro 2
4:	$E \vee G$	∨ intro 2
5:	$(E \vee F) \wedge (E \vee G)$	∧ intro 3,4
6:	$F \wedge G$	assumption
	...	
7:	$(E \vee F) \wedge (E \vee G)$	
8:	$(E \vee F) \wedge (E \vee G)$	∨ elim 1,2-5,6-7

▷ Working on the second subgoal (the bottom box)

- we can see we are going to need both conjuncts so we take two $\wedge$-elim steps

1:	$E \vee F \wedge G$	premise
2:	E	assumption
3:	$E \vee F$	$\vee$ intro 2
4:	$E \vee G$	$\vee$ intro 2
5:	$(E \vee F) \wedge (E \vee G)$	$\wedge$ intro 3,4
6:	$F \wedge G$	assumption
7:	G	$\wedge$ elim 6
8:	F	$\wedge$ elim 6
	...	
9:	$(E \vee F) \wedge (E \vee G)$	
10:	$(E \vee F) \wedge (E \vee G)$	$\vee$ elim 1,2-5,6-9

▷ We see that we can finish this subproof with $\wedge$-intro

1:	$E \vee F \wedge G$	premise
2:	E	assumption
3:	$E \vee F$	$\vee$ intro 2
4:	$E \vee G$	$\vee$ intro 2
5:	$(E \vee F) \wedge (E \vee G)$	$\wedge$ intro 3,4
6:	$F \wedge G$	assumption
7:	G	$\wedge$ elim 6
8:	F	$\wedge$ elim 6
	...	
9:	$E \vee F$	
	...	
10:	$E \vee G$	
11:	$(E \vee F) \wedge (E \vee G)$	$\wedge$ intro 9,10
12:	$(E \vee F) \wedge (E \vee G)$	$\vee$ elim 1,2-5,6-11

▷ The two resulting subgoals are closed by ∨-intro rules

1:	$E \lor F \land G$	premise
2:	E	assumption
3:	$E \lor F$	∨ intro 2
4:	$E \lor G$	∨ intro 2
5:	$(E \lor F) \land (E \lor G)$	∧ intro 3,4
6:	$F \land G$	assumption
7:	G	∧ elim 6
8:	F	∧ elim 6
9:	$E \lor F$	∨ intro 8
10:	$E \lor G$	∨ intro 7
11:	$(E \lor F) \land (E \lor G)$	∧ intro 9,10
12:	$(E \lor F) \land (E \lor G)$	∨ elim 1,2-5,6-11

▷ Notice that assumption 2 is not used outside of 2-5, nor is 6 used outside of 6-11.

Exercise: Could we have started the proof search by using ∧-intro?

Proof Rules for Implication

▷ Elimination rule (a.k.a *modus-ponens*) is straightforward

$$\dfrac{\phi \qquad\qquad \phi \to \psi}{\psi}\ \to\text{-elim}$$

▷ Concrete example: proof of $H, R, H \wedge R \to D \vdash D$

$$\dfrac{\dfrac{}{H \wedge R \to D}\ \text{premiss} \qquad \dfrac{\dfrac{}{H}\ \text{premiss} \qquad \dfrac{}{R}\ \text{premiss}}{H \wedge R}\ \wedge\text{-intro}}{D}\ \to\text{-elim}$$

▷ Introduction rule

$$\frac{\boxed{\begin{array}{c}\phi \\ \vdots \\ \psi\end{array}}}{\phi \to \psi} \to\text{-intro}$$

To prove $\phi \to \psi$ assume ϕ and prove ψ from it.

The box means "don't refer to the assumed occurence of ϕ outside of the nested subproof"

▷ Concrete example: "discovering" a proof of $E \to (F \to G) \vdash (E \to F) \to (E \to G)$

▷ We know that the proof is eventually going to look like this

1:	$E \to (F \to G)$	premiss
	$\dots$	
n:	$(E \to F) \to (E \to G)$	

▷ We cannot do anything immediately with the premiss (→-elim is not applicable)

But we *could* start a new hypothetical subproof using →-intro

1:	$E \to (F \to G)$	premiss
2:	$E \to F$	assumption
	$\dots$	
(n-1):	$E \to G$	
n:	$(E \to F) \to (E \to G)$	→-intro 2 — n-1

In fact we were *forced* to do this! (Why?)

▷ Exactly the same consideration holds for the subproof 2 — $(n-1)$, leaving us with

1:	$E \rightarrow (F \rightarrow G)$	premiss
2:	$E \rightarrow F$	assumption
3:	E	assumption
	$\cdots$	
n-2:	G	
n-1:	$E \rightarrow G$	→-intro 3 — n-2
n:	$(E \rightarrow F) \rightarrow (E \rightarrow G)$	→-intro 2 — n-1

▷ Now we can start to use →-elim

1:	$E \to (F \to G)$	premiss
2:	$\quad E \to F$	assumption
3:	$\qquad E$	assumption
4:	$\qquad F$	→-elim 2,3
	$\qquad \cdots$	
n-2:	$\qquad G$	
n-1:	$\quad E \to G$	→-intro 3 — n-2
n:	$(E \to F) \to (E \to G)$	→-intro 2 — n-1

▷ and again ...

1:	$E \to (F \to G)$	premiss
2:	$E \to F$	assumption
3:	E	assumption
4:	F	→-elim 2,3
5:	$F \to G$	→-elim 1,3
	$\cdots$	
n-2:	G	
n-1:	$E \to G$	→-intro 3 — n-2
n:	$(E \to F) \to (E \to G)$	→-intro 2 — n-1

▷ and it just takes one more →-elim to close the (gap in the) proof

1:	$E \to (F \to G)$	premiss
2:	$E \to F$	assumption
3:	E	assumption
4:	F	→-elim 2,3
5:	$F \to G$	→-elim 1,3
6:	G	→-elim 5,4
7:	$E \to G$	→-intro 3 — 6
8:	$(E \to F) \to (E \to G)$	→-intro 2 — 7

▷ EXERCISE: Use this sequence to explain why the "boxed assumption" restriction of →-intro is satisfied by this proof.

▷ Here's the proof in tree form (with the origins of assumptions labelled):

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{E \to (F \to G)}\,\text{premiss} \qquad \dfrac{}{E}\,\text{hyp}_3}{F \to G}\,\to\text{-elim} \qquad \dfrac{\dfrac{}{E \to F}\,\text{hyp}_2 \qquad \dfrac{}{E}\,\text{hyp}_3}{F}\,\to\text{-elim}}{G}\,\to\text{-elim}}{E \to G}\,\to\text{-intro}_3}{(E \to F) \to (E \to G)}\,\to\text{-intro}_2$$

▷ EXERCISE: Use this tree to explain why the "boxed assumption" restriction of →-intro is satisfied by this proof.

▷ ASIDE: it can be quite challenging to keep track of assumptions made during the process of discovering a proof that you are recording in tree form.

A Paradox?

▷ One consequence of accepting the →-intro rule is the theorem $F \vdash E \to F$

1:	F	premiss
2:	$\boxed{E}$	hyp
3:	$\boxed{F}$	copy 1
4:	$E \to F$	→-intro

- We have proved that if F holds anyway, then (for any proposition E) that $E \to F$, the natural language interpretation of which is: "if E then F"
- But in natural language "if E then F" is sometimes taken to suggest that E is, in some sense, *relevant to*, or a *causal factor* in F.
- There is no real paradox here: just take $E \to F$ to mean "F holds in every situation in which E holds."

Rules for iff

▷ If we take $\phi \leftrightarrow \psi$ as an abbreviation for "$\phi \to \psi$ and $\psi \to \phi$" we get the rules:

$$\frac{\phi \to \psi \quad \psi \to \phi}{\phi \leftrightarrow \psi}\ \text{abb-}\leftrightarrow\text{-intro} \qquad \frac{\phi \leftrightarrow \psi}{\phi \to \psi}\ \text{abb-}\leftrightarrow\text{-elim-r} \qquad \frac{\phi \leftrightarrow \psi}{\psi \to \phi}\ \text{abb-}\leftrightarrow\text{-elim-l}$$

which capture the essence of the abbreviation; but mention an additional connective ($\to$)

▷ The following rules are of equivalent logical power; and they mention *only* $\leftrightarrow$

$$\frac{\boxed{\begin{array}{c}\psi\\ \vdots\\ \phi\end{array}} \quad \boxed{\begin{array}{c}\phi\\ \vdots\\ \psi\end{array}}}{\phi \leftrightarrow \psi}\ \leftrightarrow\text{-intro} \qquad \frac{\phi \quad \phi \leftrightarrow \psi}{\psi}\ \leftrightarrow\text{-elim-r} \qquad \frac{\psi \quad \phi \leftrightarrow \psi}{\phi}\ \leftrightarrow\text{-elim-l}$$

Proof Rules for Negation

- Informal meaning of $\neg$ is captured by
  - "If you believe ϕ then you shouldn't believe $\neg\phi$"
  - "If you believe $\neg\phi$ then you shouldn't believe ϕ"

- The rules for $\neg$ must demonstrate that ϕ and $\neg\phi$ contradict each other.
- We use the symbol $\perp$ to mean *contradiction*.

▷ Introduction: if ϕ leads to a contradiction, then believe $\neg\phi$

$$\frac{\boxed{\begin{array}{c}\phi\\ \vdots\\ \bot\end{array}}}{\neg\phi}\ \neg\text{-intro}$$

▷ Elimination: believing both ϕ and $\neg\phi$ is contradictory

$$\frac{\phi \qquad \neg\phi}{\bot}\ \neg\text{-elim}$$

▷ Contradiction-elimination: $\frac{\bot}{\phi}\ \bot\text{-elim}$

▷ Double-negation-elimination: $\frac{\neg\neg\phi}{\phi}\ \neg\neg\text{-elim}$

▷ An important consequence of these rules – called classical contradiction or *reductio ad absurdam* (RAA) – is: if $\neg\phi$ leads to a contradiction, then believe ϕ

$$\dfrac{\boxed{\begin{array}{c}\neg\phi\\ \vdots\\ \bot\end{array}}}{\phi}\ \text{contradiction(classical)}$$

▷ Exercise: "prove" the classical contradiction rule

▷ A straightforward proof using both negation rules

1:	$\neg(E \vee F)$	premise
2:	E	assumption
3:	$E \vee F$	$\vee$ intro 2
4:	$\perp$	$\neg$ elim 3,1
5:	$\neg E$	$\neg$ intro 2-4
6:	F	assumption
7:	$E \vee F$	$\vee$ intro 6
8:	$\perp$	$\neg$ elim 7,1
9:	$\neg F$	$\neg$ intro 6-8
10:	$\neg E \wedge \neg F$	$\wedge$ intro 5,9

▷ Proof discovery:

- the goal consequent matches a rule consequent.
- then for each conjunct goal we looked for a way of eliminating not from the premiss

▷ Law of the Excluded Middle: $\vdash \phi \vee \neg\phi$

▷ This theorem has no premisses.

1:	$\neg(\phi \vee \neg\phi)$	assumption
2:	$\neg\phi \wedge \neg\neg\phi$	Theorem $\neg(\phi \vee \psi) \vdash \neg\phi \wedge \neg\psi$
3:	$\neg\neg\phi$	$\wedge$-elim 2
4:	$\neg\phi$	$\wedge$-elim 2
5:	$\bot$	$\neg$elim 4,3
6:	$(\phi \vee \neg\phi)$	contra (classical) 1—5

▷ Proof discovery:

- the goal consequent is a disjunction, but
- using an $\vee$-intro rule would require us to choose one of the disjuncts to prove
- so we structure the proof as a proof by contradiction

▷ Exercise: prove the theorem cited on line 2

Derived Rules

- ▷ Exercise: prove $\phi \land \psi \to \theta \vdash \phi \to (\psi \to \theta)$ (call this proof IC(ϕ, ψ, κ))
- ▷ Exercise: prove $\phi \to (\psi \to \theta) \vdash \phi \land \psi \to \theta$ (call this proof CI(ϕ, ψ, κ))

Q: Can these proofs become part of the proof of $\vdash E \to (F \to G) \leftrightarrow E \land F \to G$?

A: Imagine just substituting the proof trees at the appropriate point

$$\dfrac{\dfrac{\boxed{\begin{array}{l}(E \to (F \to G)) \\ \qquad\quad \vdots\ CI(E,F,G) \\ \quad E \land F \to G\end{array}}}{(E \to (F \to G)) \to (E \land F \to G)}\ \to\text{-intro} \qquad \dfrac{\boxed{\begin{array}{l}(E \land F \to G) \\ \qquad\quad \vdots\ IC(E,F,G) \\ E \to (F \to G)\end{array}}}{(E \land F \to G) \to (E \to (F \to G))}\ \to\text{-intro}}{E \to (F \to G) \leftrightarrow E \land F \to G}\ \leftrightarrow\text{-intro}$$

- ▷ This justifies the notion that (substitution instance of) a proven conjecture (a.k.a theorem) that has been named can be used within another proof *as if it were a proof rule*.

▷ Denying the Conseqent: (a.k.a *Modus Tollens*)

$$\frac{\phi \to \psi \qquad\qquad \neg\psi}{\neg\phi}\ \mathsf{MT}$$

▷ Proof

1:	$\phi \to \psi$	premiss
2:	$\neg\psi$	premiss
3:	ϕ	assumption
4:	ψ	$\to$-elim 1, 3
5:	$\bot$	$\neg$-elim 4, 2
6:	$\neg\phi$	$\neg$-intro 3-5

A first glance at soundness and completeness

▷ If I find a proof of $R, H \wedge R \rightarrow D, \neg D \vdash \neg H$

... then what should I do if I am wearing a hat and it is raining and my head is wet?

▷ If I find a proof of $R, H \wedge R \rightarrow D, D \vdash H$

... then what should I do if it is raining and my head is dry and I am not wearing a hat?

▷ What if we cannot find a proof of "$R, H \wedge R \rightarrow D, D \vdash H$"?

- is it because the conjecture is invalid?
- is it because we are insufficiently clever?
- is it because the proof rules we have given so far are inadequate or wrong?

▷ More generally, we can ask questions *about the proof rules*:

- Completeness: is there a proof of every valid conjecture of the form "$P_1, P_2, ...P_n \vdash Q$"?
- Soundness: if we can find a proof for "$P_1, P_2, ...P_n \vdash Q$" then is it valid?

▷ But to answer these questions we need

- an independent characterization of the notion of *validity*.
- a way of conducting rigorous proofs *about proofs*!

Contents

Note 1: 1 ☞

"Calculus" used in this logical context signifies a systematic (*i.e.* rule-based rather than intuitive) method of reasoning by calculation.

Note 2: 13 ☞

We use "rules of inference", "inference rules", and "proof rules" interchangeably in this course.

Note 3: Linear Proofs represent DAGs 16 ☞

We emphasise that the tree and linear presentations are *presentations of the same underlying proof structure*. They are not different proofs.

The correspondence between the linear presentation

1:	$\phi \wedge (\psi \wedge \kappa)$	premiss
2:	ϕ	$\wedge$-elim-L 1
3:	$\psi \wedge \kappa$	$\wedge$-elim-R 1
4:	ψ	$\wedge$-elim-L 3
5:	$\phi \wedge \psi$	$\wedge$-intro 2 4
6:	κ	$\wedge$-elim-R 3
7:	$(\phi \wedge \psi) \wedge \kappa$	$\wedge$-intro 5, 6

and the tree presentation

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\phi \wedge (\psi \wedge \kappa)}\text{ 1. premiss}}{\phi}\text{ 2. }\wedge\text{-elim-L} \qquad \dfrac{\dfrac{\dfrac{}{\phi \wedge (\psi \wedge \kappa)}\text{ 1. premiss}}{\psi \wedge \kappa}\text{ 3. }\wedge\text{-elim-R}}{\psi}\text{ 4. }\wedge\text{-elim-L}}{\phi \wedge \psi}\text{ 5. }\wedge\text{-intro} \qquad \dfrac{\dfrac{\dfrac{}{\phi \wedge (\psi \wedge \kappa)}\text{ 1. premiss}}{\psi \wedge \kappa}\text{ 3. }\wedge\text{-elim-R}}{\kappa}\text{ 6. }\wedge\text{-elim-R}}{(\phi \wedge \psi) \wedge \kappa}\text{ 7. }\wedge\text{-intro}$$

is made explicit here by labelling each node of the tree with its corresponding line number.

In general the linear presentation of a proof represents a DAG whose traversal yields a tree presentation.

Note 4: 18 ☞

For a simple concrete example suppose we want to show that $2n$ is always even, we can go about it in this way:

$$\dfrac{\begin{array}{c} \vdots \\ (even(n) \vee odd(n)) \end{array} \quad \boxed{\begin{array}{c} even(n) \\ \vdots \\ even(2n) \end{array}} \quad \boxed{\begin{array}{c} odd(n) \\ \vdots \\ even(2n) \end{array}}}{even(2n)}\ \vee\text{-elim}$$

Note 5: Natural Deduction 20 ☞

- ▷ The rules we have presented so far arguably formalize "natural" ways of reasoning about propositions formed with $\wedge$ and $\vee$ without taking a position in advance about the relationship between these two connectives
- ▷ The *natural deduction* style of presenting a logical system or a calculus characterizes each construct by
  - ∘ an introduction rule (or rules)
    (showing how to establish composite predicates from simpler ones)
  - ∘ an elimination rule (or rules)
    (showing how to *use parts* of composite predicates)

Natural Deduction is one of many systems used in the formalization of logic. It arose out of dissatisfaction with more austere forms of formalizing logic, such as Hilbert's. The Wikipedia article on Natural Deduction is a good place to follow the story if you are interested.

If you enjoyed functional programming then you may also be interested in the work I did with James J. Leifer intended to build a bridge between Hilbert Systems and Natural Deduction systems.

These two papers are available on the web.

1. Deduction for functional programmers by James J. Leifer and Bernard Sufrin. Journal of Functional Programming, volume 6, number 2, 1996.
2. Formal logic via functional programming by James J. Leifer (June 1995). Was James Leifer's final year dissertation: a greatly expanded version of the JFP paper.

Note 6: 21 ☞

Here's an outline of the proof of $E \vee (F \wedge G) \vdash (E \vee F) \wedge (E \vee G)$ that we would have ended up with if we had decided to use $\wedge$-intro as our first goal-transforming step.

1:	$E \vee F \wedge G$	premise
2:	E	assumption
	…	
3:	$E \vee F$	
4:	$F \wedge G$	assumption
	…	
5:	$E \vee F$	
6:	$E \vee F$	$\vee$ elim 1,2-3,4-5
7:	E	assumption
	…	
8:	$E \vee G$	
9:	$F \wedge G$	assumption
	…	
10:	$E \vee G$	
11:	$E \vee G$	$\vee$ elim 1,7-8,9-10
12:	$(E \vee F) \wedge (E \vee G)$	$\wedge$ intro 6,11

In this case the $\vee$-elim rule is used twice: once to establish the conjunct on line 6, and once to establish the conjunct on line 11. Compare this with the two uses of $\wedge$-intro in our original proof, once in each of the colateral subproofs required by the (single) use of $\vee$-elim.

Note 7: Equivalent logical power 36 ☞

When we say that two (collections) of rules are of equivalent logical power, we mean that any proof that can be constructed using only one of the collections of rules can also be constructed using the other collection. This does not mean that the structures of the proofs using one collection will be identical to those using the other collection.

To convince ourselves that two collections are of equivalent power (in the context of an otherwise-fixed set of rules), we need only prove the rules of the first collection from the second (and the otherwise-fixed set of rules), and vice-versa.

Note 8: Typographical conventions

41 ☞

▷ Many texts follow very strict typographical conventions when discussing logic and, in particular, proving general theorems. We are much less meticulous in this part of the course, though we have a mild tendency to use Greek capitals to stand for arbitrary propositions in proof rules and very general theorems, while using Roman capitals to stand for specific atomic propositions.

▷ But because our arguments are strictly formal, and do not depend on the interpretations of atomic propositions, a proof done in our notes using Roman letters is as valid as one that would appear typographically more general if we were enforcing a typographical convention.

▷ For example: earlier we showed part of a proof that $\vee$ distributes through $\wedge$ using Roman capitals to stand for the propositions involved; and here is a proof of the law of the excluded middle that uses a Roman letter for the proposition.

1:	$\neg(E \vee \neg E)$	assumption
2:	$\neg E \wedge \neg\neg E$	Theorem $\neg(E \vee F) \vdash \neg E \wedge \neg F$ 1
3:	$\neg\neg E$	$\wedge$ elim 2
4:	$\neg E$	$\wedge$ elim 2
5:	$\bot$	$\neg$ elim 4,3
6:	$E \vee \neg E$	contra (classical) 1-5