Introduction to Formal Proof

Bernard Sufrin

Trinity Term 2018



## 1: Formal Proofs in Propositional Calculus

[01-intro]

| Introduction  | Propositional Language: propositions  |  |  |
|---|---|--|--|
|   | ▷ A <i>proposition</i> is a meaningful declarative sentence that may be true or false in a situation.               |  |  |
| ho A calculus by which the <i>validity</i> (correctness) of propositional conjectures is judged | $\triangleright$ Examples:  |  |  |
|   | ∘ "Socrates is mortal"  |  |  |
| $\triangleright$ A propositional conjecture has some <i>premisses</i> and a <i>conclusion</i>   | $\circ$ "The King's Arms is at the junction of Cornmarket with High Street"   |  |  |
|   | ∘ "I am hungry"   |  |  |
| ⊳ Example 1:  | <ul> <li>"Tony Blair is a war-criminal"</li> </ul>  |  |  |
| It is raining   | <ul> <li>"It is raining and my head is wet"</li> </ul>  |  |  |
| If I wear a hat and it is raining then my head stays dry  | $\circ$ "If I wear a hat and it is raining then my head stays dry"  |  |  |
| My head is not dry  | $\triangleright$ But not  |  |  |
| I therefore conclude that   | ◦ "Do you like green eggs and ham?"   |  |  |
| I am not wearing a hat  | <ul> <li>"Can you catch it in your hat?"</li> </ul>   |  |  |
| ▷ Question: is this conjecture valid?   | ◦ "Let's go!"   |  |  |
|   | <ul> <li>"Don't mention the war."</li> </ul>  |  |  |
|   |   |  |  |
| تا 11 – 1 – 13 <sup>th</sup> April, 2017@13:42 [712]  | - 3 - 13 <sup>th</sup> April, 2017@13:42 [712   |  |  |
| troduction to Formal Proof 1: Formal Proofs in Propositional Calculus Introduction              | Introduction to Formal Proof 1: Formal Proofs in Propositional Calculus Propositional Language: atomic propositions |  |  |
| ⊳ Example 2:  | Propositional Language: atomic propositions   |  |  |
| It is raining   |   |  |  |
| If I wear a hat and it is raining then my head stays dry<br>My head is dry                      | $\triangleright$ An <i>atomic proposition</i> is a proposition with no logical connectives in it.                   |  |  |
| I therefore conclude that   | ⊳ Examples:   |  |  |
| l am wearing a hat  | ∘ "Socrates is mortal"  |  |  |
| Question: is this conjecture valid?   | <ul> <li>"The King's Arms is at the junction of Cornmarket with High Street"</li> </ul>                             |  |  |
|   | ∘ "I am hungry"   |  |  |
|   | <ul> <li>"Tony Blair is a war-criminal"</li> </ul>  |  |  |
| ⊳ Example 3:  |   |  |  |
| I conclude (without premisses) that   | $\triangleright$ But not  |  |  |
| If today is Tuesday then we are in Paris  | <ul> <li>"It is raining and my head is wet" (" and")</li> </ul>   |  |  |
| Question: is this conjecture valid?   | <ul> <li>"If I wear a hat and it is raining then my head stays dry" ("if and then")</li> </ul>                      |  |  |
|   |   |  |  |
| - 2 - 13 <sup>th</sup> April, 2017@13:42 [712]  | - 4 - 13 <sup>th</sup> April, 2017@13:42 [712]  |  |  |

13th April, 2017@13:42 [712]

Presenting a conjecture

### 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 | $(H \land R) \rightarrow D$ |
| My head is not dry                                       | $\neg D$                    |
| I therefore conclude that                                |                             |
| l am not wearing a hat                                   | $\neg H$                    |

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

It is not a propositional connective

| -0-  | - 5 -    | 13th April, 2017@13:42 [712] |
|--|----------|------------------------------|
| Introduction to Formal Proof 1: Formal Proofs in Propositional C | Calculus | Symbolic representation      |

### **Composing Propositions with Logical Connectives**

| ⊳ not   | $\neg\phi$ `  | )   |
|---|---|---|
| $\triangleright \dots$ and $\dots$            | $\phi \wedge \psi$  | $\}$ where $\phi$ and $\psi$ are propositions |
| ▷ or  | $\phi \lor \psi$  | $\}$ where $\phi$ and $\psi$ are propositions |
| $\triangleright$ if then                      | $\begin{array}{l} \phi \to \psi \\ \phi \leftrightarrow \psi \end{array}$ |   |
| $\triangleright \dots$ if and only if $\dots$ | $\phi \leftrightarrow \psi$ ,   | ļ   |

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

Parsing

 $\triangleright$  Priority of connectives is (in descending order)  $\neg, \land, \lor, \rightarrow, \leftrightarrow$ 

- $\circ \rightarrow$  has slightly higher priority on its right than on its left
- $\circ$  Some texts give  $\wedge$  the same priority as  $\vee$
- $\circ$  (Jape gives  $\land$  and  $\lor$  slightly higher priority on their left)
- $\triangleright$  If in doubt, parenthesize!

 $\triangleright$  Examples:  $\circ (\underline{A \land B} \to \underline{C \lor D}) \leftrightarrow \overline{A \to \overline{B \to \overline{C \lor D}}}$  $\circ \neg \underline{\neg A} \to A$  $\circ \overline{\overline{A \vee B} \vee C} \vee \underline{D} \wedge \underline{E} \wedge F$ 

Introduction to Formal Proof 1: Formal Proofs in Propositional Calculus

 $R, H \land R \rightarrow$ 

### Presenting a conjecture

- 7 -

- $\triangleright$  Informal: "if you accept these premisses<sup>1</sup> then you should accept this conclusion"
- ▷ Formal: "from *these premisses* we may validly infer *this conclusion*."
  - $\circ$  In horizontal form: *premiss*, *premiss*, *premiss*, ...  $\vdash$  *conclusion*
  - In vertical form:

 $\triangleright$  *e.g.* the conjecture:

$$D, D \vdash H$$
  $\frac{R \quad H \land R \to D \quad D}{H}$ 

 $\triangleright$  *e.g.* the conjecture:

i.e. their truth

$$R, H \land R \to D, \neg D \vdash \neg H \qquad \qquad \frac{R \quad H \land R \to D \quad \neg D}{\neg H}$$

$$\neg H$$

- 6 -

- 8 -

What is the nature of a valid conjecture?

Introduction to Formal Proof 1: Formal Proofs in Propositional Calculus

|  |  | -  | ▷ Example conjecture: co                      | mmutativity of conjunction: (f   | for any propositions $\phi$ and $\psi)$   |
|--|--|--|---|--|---|
| ▷ The validity of a conj   | s is a formal system that we use to j<br>ecture is judged <i>solely from its form</i><br>ons of the atomic propositions. |  | $rac{\psi}{\phi}$                            | $\frac{\psi \wedge \phi}{\wedge \psi}$   | $\psi \wedge \phi \vdash \phi \wedge \psi$  |
| <ul> <li>▷ The validity of R, H ∧ R → D, ¬D ⊢ ¬H</li> <li>○ is independent of the interpretation H, R, D in the real world.</li> <li>○ does not establish the truth of the premisses.</li> </ul>   |  | $\circ \ ``from \ \psi \land \phi \ we \ can \ infer \ \phi \land \psi''$ $\circ \ ``if \ we \ have \ established \ \psi \land \phi \ then \ we \ can \ infer \ \phi \land \psi''$ |   | $\wedge \psi$ "  |   |
| <ul> <li>o so should not, on a should not an alternative interpreter a should be "there as a should be should be a should be a should be a should be a should be</li></ul> | my garden"   |  | 3. Since we have establ                       | lished (by premiss) $\psi \land \phi$ we c<br>lished (by premiss) $\psi \land \phi$ we c |   |
| Introduction to Formal Proof 1: Formal Pro   | – 9 –<br>pofs in Propositional Calculus  | 13 <sup>th</sup> April, 2017@13:42 [712]<br>What is the purpose of a proof system?   | Introduction to Formal Proof 1: Formal Proofs | – 11 –<br>; in Propositional Calculus  | 13 <sup>th</sup> April, 2017@13:42 [712]<br>What is the purpose of a proof system?          |
| V  | What is the purpose of a proof   | system?  |   |  |   |
| • When the premisse  | hat a particular conjecture has<br>es are all true then you should accep<br>premisses are untrue then you need           | t the conclusion   | $\triangleright$ Here we use the words        | <i>infer, conclude,</i> and <i>deduce</i> m  | ore or less interchangeably.  |
|  | <b>hat a conjecture has not (yet)</b><br>t (yet) accept the conclusion, even i   | -  | or has been inferred / c                      |  | roof of a conjecture if it is a premiss<br>or indirectly) from the premisses of<br>e using. |

What is the nature of a valid conjecture?

What is the purpose of a proof system?

What is the purpose of a proof system?

Introduction to Formal Proof 1: Formal Proofs in Propositional Calculus

### **Proof Rules for conjunction**

 $\triangleright$  "and introduction":

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

$$\frac{\phi \quad \psi}{\phi \land \psi} \land \text{-intro}$$

 $\triangleright$  "and elimination"

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

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

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

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

- 13 − 13<sup>th</sup> April, 2017@13:42 [712]

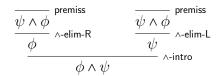
Introduction to Formal Proof 1: Formal Proofs in Propositional Calculus

### ▷ Formal presentations of the proof

• In linear form

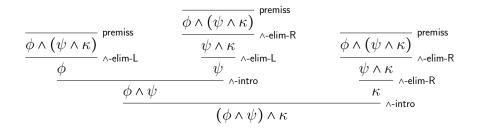
1: 
$$\psi \land \phi$$
 premiss  
2:  $\phi$   $\land$ -elim-R 1  
3:  $\psi$   $\land$ -elim-L 1  
4:  $\phi \land \psi$   $\land$ -intro 2, 3

 $\circ$  As a tree



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

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



▷ 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: | $\phi \land (\psi \land \kappa)$   | premiss      |
|----|------------------------------------|--------------|
| 2: | $\phi$                             | ∧-elim-L 1   |
| 3: | $\psi \wedge \kappa$               | ∧-elim-R 1   |
| 4: | $\psi$                             | ∧-elim-L 3   |
| 5: | $\phi \wedge \psi$                 | ∧-intro 2 4  |
| 6: | $\kappa$                           | ∧-elim-R 3   |
| 7: | $(\phi \wedge \psi) \wedge \kappa$ | ∧-intro 5, 6 |

 $\triangleright$  In this proof the pattern for each rule is matched in more than one way

Proof Rules for disjunction

Introduction to Formal Proof 1: Formal Proofs in Propositional Calculus

 $\triangleright$  Case study: proof of  $E \lor (F \land G) \vdash (E \lor F) \land (E \lor G)$ 

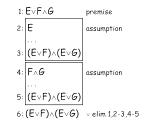
| I   | Proof Rules for disjunction   |  |                                     | 1: $E \lor F \land G$ premise   |   |
|---|---|--|-------------------------------------|---|---|
|   |   |  |                                     | 2: E assumption   |   |
|   |   |  |                                     | 3: EVF v intro 2  |   |
|   |   |  |                                     | 4: E∨G v intro 2  |   |
|   |   |  |                                     | 5: $(E \lor F) \land (E \lor G)$ $\land$ intro 3,4  |   |
|   |   |  |                                     | 6: F∧G assumption   |   |
| $\triangleright$ Introduction rules are straigh   | tforward  |  |                                     | 7: $G$ $\wedge$ elim 6  |   |
|   | $\phi$  |  |                                     | 8: <b>F</b> A elim 6  |   |
|   | $\frac{\tau}{\phi \lor \psi}$ v-intro-L   |  |                                     | 9: E∨F v intro 8  |   |
|   |   |  |                                     | 10: $E \lor G$ $\lor$ intro 7   |   |
|   | $\frac{\phi}{\phi\lor\psi}\lor-intro-L$ $\frac{\psi}{\phi\lor\psi}\lor-intro-R$   |  |                                     | 11: (E∨F)∧(E∨G) ∧ intro 9,10  |   |
|   | $\overline{\phi \lor \psi}$ V-Intro-R   |  |                                     | 12: (E∨F)∧(E∨G) velim 1,2-5,6-1   | 1   |
|   | - 17 -  | 13 <sup>th</sup> April, 2017@13:42 [712] |                                     | or the conclusion, it just depends on the on and the propositions (formulæ) that ar       |   |
| Introduction to Formal Proof 1: Formal Proofs in Propo                                    | ositional Calculus  | Proof Rules for disjunction              | Introduction to Formal Proof 1: For | rmal Proofs in Propositional Calculus   | Proof rules as "conjecture transformers"                |
| ▷ Elimination rule captures the   | idea of case analysis<br>$\begin{array}{c} \phi \\ (\phi \lor \psi) \\ \kappa \\ \nu \\ \nu - elim \end{array}$ |  |                                     | Proof rules as "conjecture transf   | ormers"   |
|   | f in which we have established $\phi \lor$  | $\boldsymbol{\psi}$ and in which we have | $\triangleright$ Q: But how did I   | go about finding the proof of $E \lor (F \land$   | $G) \vdash (E \lor F) \land (E \lor G)?$                |
| (a) established $\kappa$ by assuming (b) established $\kappa$ by assuming                 |   |  |                                     |   |   |
|   | , <i>i.e.</i> that at least one of $\phi$ and $\psi$  |  | conjectures that                    | I used a proof rule to transform a conject<br>need to be proved in order for it to hold ( |   |
| ▷ Having <i>both</i> proof (a) and proof $\begin{bmatrix} \alpha \\ \vdots \end{bmatrix}$ | roof (b) means it doesn't matter w  | nich                                     | A subgoal that's                    | an assumption (or premiss) requires no fu   | rther work.   |
| $\left[ \begin{array}{c} \alpha \\ \vdots \end{array} \right]$                            | roof (b) means it doesn't matter w $t$  |  | A subgoal that's                    | an assumption (or premiss) requires no fu   | rther work.   |
| $\left[ \begin{array}{c} \alpha \\ \vdots \end{array} \right]$                            |   |  | A subgoal that's                    | an assumption (or premiss) requires no fu   | rther work.   |
| $\begin{bmatrix} \alpha \\ \vdots \end{bmatrix}$  |   |  | A subgoal that's                    | an assumption (or premiss) requires no fu   | rther work.<br>13 <sup>th</sup> April, 2017@13:42 [712] |

▷ The starting goal (the original conjecture) is:

1: 
$$E \lor (F \land G)$$
 premiss  
...  
2:  $(E \lor F) \land (E \lor G)$ 

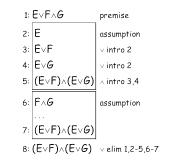
 $\circ$  We guess from the form of the premiss that we can finish the proof with  ${\scriptstyle \lor-elim}$ 

• Using this rule transforms the starting goal into two subgoals



### (alternate guess is that we can finish the proof with *^*-intro)

### $\triangleright$ After two v-intro steps we have completed the first subgoal





### $\triangleright$ Working on the first subgoal: we guess we can finish with $\land$ -intro

| 1: | E∨F∧G                    | premise          |
|----|--------------------------|------------------|
| 2: | E                        | assumption       |
| 3: | …<br>E∨F                 |                  |
| 4: | <br>E∨G<br>(E∨F)∧(E∨G)   |                  |
| 5: | (EvF)^(EvG)              | ∧ intro 3,4      |
| 6: | F∧G                      | assumption       |
| 7: | <br>(E∨F)∧(E∨ <i>G</i> ) |                  |
| 8: | (E∨F)∧(E∨ <i>G</i> )     | v elim 1,2-5,6-7 |

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

▷ Working on the second subgoal (the bottom box)

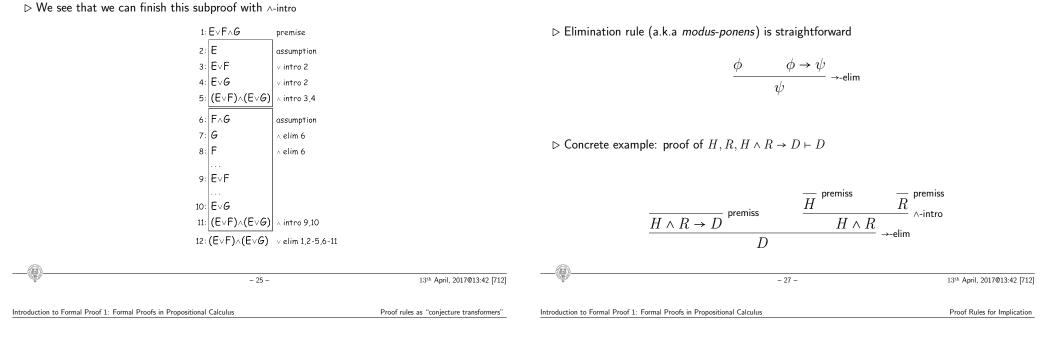
 $\circ$  we can see we are going to need both conjuncts so we take two  $\wedge\text{-elim}$  steps

| 1:  | E∨F∧G                | premise         |
|-----|----------------------|-----------------|
| 2:  |                      | assumption      |
| 3:  | E∨F<br>E∨ <i>G</i>   | v intro 2       |
| 4:  | E∨G                  | v intro 2       |
| 5:  | (E∨F)∧(E∨ <i>G</i> ) | ∧ intro 3,4     |
| 6:  | F∧ <i>G</i>          | assumption      |
| 7:  | G                    | ∧ elim 6        |
| 8:  |                      | ∧elim 6         |
|     |                      |                 |
| 9:  | (E∨F)∧(E∨ <i>G</i> ) |                 |
| 10: | (E∨F)∧(E∨G)          | velim 1,2-5,6-9 |

Proof rules as "conjecture transformers"

Introduction to Formal Proof 1: Formal Proofs in Propositional Calculus

### **Proof Rules for Implication**



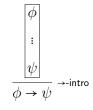
### $\triangleright$ The two resulting subgoals are closed by v-intro rules

| 1:  | E∨F∧G                | premise           |
|-----|----------------------|-------------------|
| 2:  | E                    | assumption        |
| 3:  | E∨F                  | v intro 2         |
| 4:  | E∨G                  | v intro 2         |
| 5:  | (E∨F)∧(E∨ <i>G</i> ) | ∧ intro 3,4       |
| 6:  | F∧G                  | assumption        |
| 7:  | G                    | ∧elim 6           |
| 8:  | F                    | ∧ elim 6          |
| 9:  | E∨F                  | v intro 8         |
| 10: | E∨G                  | v intro 7         |
| 11: | (E∨F)∧(E∨ <i>G</i> ) | ∧ intro 9,10      |
| 12: | (E∨F)∧(E∨G)          | ∨ elim 1,2-5,6-11 |

 $\triangleright$  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?

▷ Introduction rule



To prove  $\phi \rightarrow \psi$  assume  $\phi$  and prove  $\psi$  from it.

The box means "don't refer to the assumed occurrence of  $\phi$  outside of the nested subproof"

Proof Rules for Implication

Introduction to Formal Proof 1: Formal Proofs in Propositional Calculus

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

 $\triangleright$  We know that the proof is eventually going to look like this

1: 
$$E \to (F \to G)$$
 premiss  
...  $(E \to F) \to (E \to G)$ 

 $\triangleright$  We cannot do anything immediately with the premiss ( $\rightarrow$ -elim is not applicable)

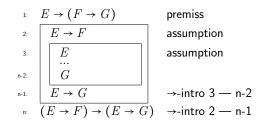
But we *could* start a new hypothetical subproof using  $\rightarrow$ -intro

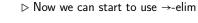
1: 
$$E \rightarrow (F \rightarrow G)$$
 premiss  
2:  $E \rightarrow F$  assumption  
(n-1):  $E \rightarrow G$   
n:  $(E \rightarrow F) \rightarrow (E \rightarrow G)$   $\rightarrow$ -intro 2 — n-1

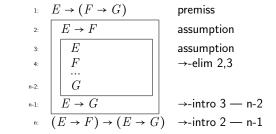
In fact we were *forced* to do this! (Why?)

|   | - 29 -                        | 13 <sup>th</sup> April, 2017@13:42 [712] |                                     | - 31 -                               | 13 <sup>th</sup> April, 2017@13:42 [712] |
|---|-------------------------------|--|-------------------------------------|--------------------------------------|--|
| Introduction to Formal Proof 1: Formal Proc | ofs in Propositional Calculus | Proof Rules for Implication              | Introduction to Formal Proof 1: For | mal Proofs in Propositional Calculus | Proof Rules for Implication              |

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









1:  $E \rightarrow (F \rightarrow G)$ premiss  $E \rightarrow F$ assumption 2: Eassumption 3: F $\rightarrow$ -elim 2.3 4:  $F \rightarrow G$  $\rightarrow$ -elim 1.3 5: ••• Gn-2:  $E \rightarrow G$  $\rightarrow$ -intro 3 — n-2 n-1:  $(E \to F) \to (E \to G) \to -intro 2 - n-1$ 

 $\triangleright$  and it just takes one more  $\rightarrow$ -elim to close the (gap in the) proof

Proof Rules for Implication

### A Paradox?

 $\triangleright$  One consequence of accepting the  $\rightarrow$ -intro rule is the theorem  $F \vdash E \rightarrow F$ 

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

- We have proved that if F holds anyway, then (for any proposition E) that  $E \rightarrow F$ , the natural language interpretation of which is: "if E then F"
- $\circ$  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.
- $\circ$  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

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

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

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

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



13th April, 2017@13:42 [712]

1:  $E \rightarrow (F \rightarrow G)$ premiss  $E \rightarrow F$ 2: assumption Eassumption 3: F $\rightarrow$ -elim 2.3 4:  $F \rightarrow G$ 5:  $\rightarrow$ -elim 1.3 G→-elim 5,4 6:  $E \rightarrow G$  $\rightarrow$ -intro 3 — 6 7: \*  $(E \to F) \to (E \to G) \to -intro 2 - 7$ 

 $\triangleright$  EXERCISE: Use this sequence to explain why the "boxed assumption" restriction of  $\rightarrow$ -intro is satisfied by this proof.

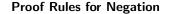


 $\triangleright$  Here's the proof in tree form (with the origins of assumptions labelled):

$$\frac{\overline{E \to (F \to G)}^{\text{premiss}} \overline{E}^{\text{hyp}_3}}{F \to G} \xrightarrow{\overline{E} \text{ hyp}_3}{F \to -\text{elim}} \xrightarrow{\overline{E} \to F} \xrightarrow{\text{hyp}_2} \overline{E}^{\text{hyp}_3} \xrightarrow{\text{-elim}} \xrightarrow{F \to -\text{elim}} \xrightarrow{$$

- $\triangleright$  EXERCISE: Use this tree to explain why the "boxed assumption" restriction of  $\rightarrow$ -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.

Proof Rules for Negation

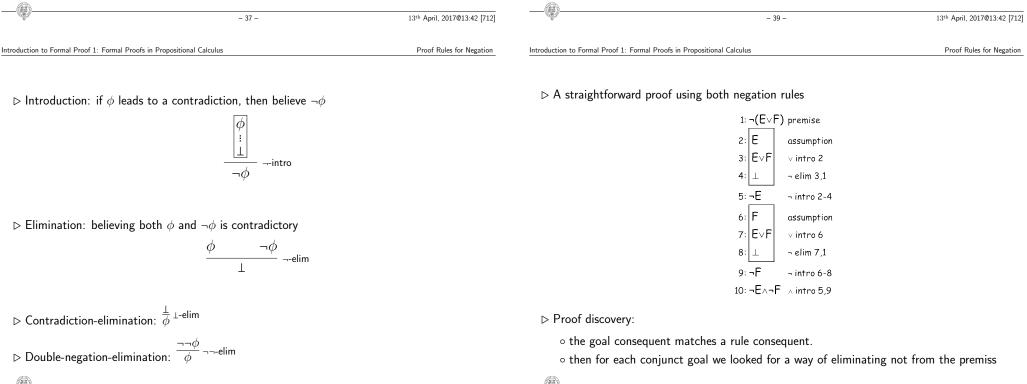


 $\triangleright$  An important consequence of these rules – called classical contradiction or *reductio ad absurdam* (RAA) – is: if  $\neg \phi$  leads to a contradiction, then believe  $\phi$ 

- $\triangleright$  Informal meaning of  $\neg$  is captured by
  - $\circ$  "If you believe  $\phi$  then you shouldn't believe  $\neg\phi$  "
  - $\circ$  "If you believe  $\neg\phi$  then you shouldn't believe  $\phi$  "
- $\triangleright$  The rules for  $\neg$  must demonstrate that  $\phi$  and  $\neg \phi$  contradict each other.
- $\triangleright$  We use the symbol  $\perp$  to mean *contradiction*.



 $\triangleright$  Exercise: "prove" the classical contradiction rule



13th April, 2017@13:42 [712]

- 40 -

Proof Rules for Negation

 $\triangleright$  Denying the Consequent: (a.k.a *Modus Tollens*)

 $\triangleright$  Law of the Excluded Middle:  $\vdash \phi \lor \neg \phi$ 

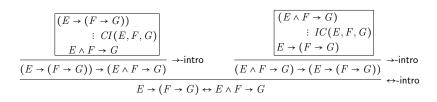
- $\triangleright$  This theorem has no premisses.
  - $\neg(\phi \lor \neg \phi)$ assumption 1 2:  $\neg \phi \land \neg \neg \phi$ Theorem  $\neg(\phi \lor \psi) \vdash \neg \phi \land \neg \psi$ ∧-elim 2 3:  $\neg \neg \phi$ ∧-elim 2 4:  $\neg \phi$ ¬elim 4.3 5:  $\perp$ contra (classical) 1-5  $(\phi \vee \neg \phi)$
- ▷ Proof discovery:
  - $\circ$  the goal consequent is a disjunction, but
  - $\circ$  using an  $\lor\text{-intro}$  rule would require us to choose one of the disjuncts to prove
  - $\circ$  so we structure the proof as a proof by contradiction
- $\triangleright$  Exercise: prove the theorem cited on line 2

|   | - 41 -                    | 13th April, 2017@13:42 [712] |                                | - 43 -                                    | 13 <sup>th</sup> April, 2017@13:42 [712]     |
|---|---------------------------|------------------------------|--------------------------------|---|--|
| Introduction to Formal Proof 1: Formal Proofs i | in Propositional Calculus | Derived Rules                | Introduction to Formal Proof 1 | : Formal Proofs in Propositional Calculus | A first glance at soundness and completeness |

⊳ Proof

### **Derived Rules**

- $\triangleright$  Exercise: prove  $\phi \land \psi \rightarrow \theta \vdash \phi \rightarrow (\psi \rightarrow \theta)$  (call this proof IC( $\phi, \psi, \kappa$ ))
- $\triangleright$  Exercise: prove  $\phi \rightarrow (\psi \rightarrow \theta) \vdash \phi \land \psi \rightarrow \theta$  (call this proof  $Cl(\phi, \psi, \kappa)$ )
- Q: Can these proofs become part of the proof of  $\vdash E \rightarrow (F \rightarrow G) \leftrightarrow E \wedge F \rightarrow G$ ?
- A: Imagine just substituting the proof trees at the appropriate point



 $\triangleright$  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*.

- 44 -

13th April, 2017@13:42 [712]

### A first glance at soundness and completeness

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

premiss

premiss assumption

→-elim 1, 3

¬-elim 4, 2

¬-intro 3-5

 $\phi \rightarrow \psi$ 

 $\phi$ 

 $\psi \ \perp$ 

4:

5:

 $\neg \psi$ 

 $\triangleright$  If I find a proof of  $R, H \land R \rightarrow D, \neg D \vdash \neg H$ 

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

 $\triangleright$  If I find a proof of  $R, H \land R \to D, D \vdash H$ 

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

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

- is it because the conjecture is invalid?
- is it because we are insufficiently clever?
- $\circ$  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 " $P_1, P_2, ..., P_n \vdash Q$ "?

- 45 -

- Soundness: if we can find a proof for " $P_1, P_2, ..., P_n \vdash Q$ " then is it valid?
- $\triangleright$  But to answer these questions we need
  - $\circ$  an independent characterization of the notion of validity.
  - a way of conducting rigorous proofs *about proofs*!

13th April, 2017@13:42 [712]

# Contents

| Propositional Calculus                           |
|--|
| Introduction1                                    |
| Propositional Language: propositions             |
| Propositional Language: atomic propositions4     |
| Symbolic representation5                         |
| Composing Propositions with Logical Connectives6 |
| Parsing7   |
| Natural Deduction in the Propositional Calculus  |
| Presenting a conjecture8                         |
| What is the nature of a valid conjecture?        |
| What is the purpose of a proof system?10         |

|      | - 46 - |
|------|--------|
|      | I      |
|      |        |
|      |        |
|      |        |
|      |        |
|      |        |
|      |        |
|      |        |
|      |        |
|      |        |
|      |        |
|      |        |
|      |        |
| (III | ~      |
|      |        |
|      |        |

13<sup>th</sup> April, 2017@13:42 [712]

| <b>Note 1:</b> "Calculus" used in this logical context signifies a systematic ( <i>i.e.</i> rule-based rather than intuitive) method of reasoning by calculation.   |       |
|---|-------|
|   | 1     |
| <b>Note 2:</b><br>We use "rules of inference", "inference rules", and "proof rules" interchangeably in this course.   | 13 17 |
| <b>Note 3: Linear Proofs represent DAGs</b><br>We emphasise that the tree and linear presentations are <i>presentations of the same underlying proof structure</i> . They are not different proofs.   | 16 🕼  |
| The correspondence between the linear presentation<br>1: $\phi \land (\psi \land \kappa)$ premiss<br>2: $\phi$ $\land -\text{elim-L 1}$<br>3: $\psi \land \kappa$ $\land -\text{elim-R 1}$<br>4: $\psi$ $\land -\text{elim-R 3}$<br>5: $\phi \land \psi$ $\land -\text{intro 2 4}$<br>6: $\kappa$ $\land -\text{elim-R 3}$<br>7: $(\phi \land \psi) \land \kappa$ $\land -\text{intro 5, 6}$  |       |
| and the tree presentation $\frac{\phi \wedge (\psi \wedge \kappa)}{\phi}$ 1. premiss $3. \wedge -\text{elim-R}$ 3. $-\sqrt{-\text{elim-R}}$ 5. $--\text{$ |       |
| 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: L

|          | -                       | V-elim  |
|----------|-------------------------|---------|
| (u) ppo  | even(2n)                |         |
| even(n): | even(2n)                | ven(2n) |
|          | $(even(n) \lor odd(n))$ | ever    |

| Note 5: Natural Deduction   |   | 20                                |
|---|---|-----------------------------------|
| $\triangleright$ The rules we have presented so far arguably formalize "natural" way, advance about the relationship between these two connectives  | ▷ The rules we have presented so far arguably formalize "natural" ways of reasoning about propositions formed with ∧ and ∨ without taking a position in advance about the relationship between these two connectives  | sition in                         |
| ▷ The natural deduction style of presenting a logical system or a calculus characterizes each construct by  | lus characterizes each construct by   |                                   |
| <ul> <li>an introduction rule (or rules)</li> <li>(channed how to octablish composite availants from simpler and</li> </ul>   |   |                                   |
| <ul> <li>an elimination rule (or rules)</li> <li>an elimination rule (or rules)</li> <li>(showing how to use parts of composite predicates)</li> </ul>  |   |                                   |
| Natural Deduction is one of many systems used in the formalization of logic. It arose out of dissatisfaction with 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 int Systems and Natural Deduction systems. | one of many systems used in the formalization of logic. It arose out of dissatisfaction with more austere forms of formalizing logic, such<br>ipedia article on Natural Deduction is a good place to follow the story if you are interested.<br>nal programming then you may also be interested in the work I did with James J. Leifer intended to build a bridge between Hilbert<br>Deduction systems. | ic, such<br>art                   |
| I nese two papers are available on the web.<br>1. Deduction for functional programmers by James J. Leifer and Bernar  | ese two papers are available on the web.<br>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 19<br>JFP paper.  | functional programming by James J. Leifer (June 1995). Was James Leifer's final year dissertation: a greatly expanded version of the  | of the                            |
| <b>Note 6:</b><br>Here's an outline of the proof of $E \lor (F \land G) \vdash (E \lor F) \land (E \lor G)$ that we would have ended up with if we had decided to use $\land$ -intro as our first goal-transforming step.   |   | 21 🕼                              |
|   |   |                                   |
|   | – 48 – 13th April, 2017@13:42 [712]   | 3:42 [712]                        |
| Introduction to Formal Proof 1: Formal Proofs in Propositional Calculus   |   | Notes                             |
| $1: \frac{E \vee F \land G}{G}$   | premise   |                                   |
| 2:  | assumption  |                                   |
| 3: E <f< td=""><td></td><td></td></f<>  |   |                                   |
| 4: F>6  | assumption  |                                   |
| 5: EVF  |   |                                   |
| ي<br>ق<br>ق   | v elim 1,2-3,4-5  |                                   |
| 7: E  | assumption  |                                   |
| 8: Ev6  |   |                                   |
| 9: F>6  | assumption  |                                   |
| 10: EVG   |   |                                   |
| 11: EVG<br>12: (FVF) <sub>2</sub> (FVG)   | ∨ elim 1,7-8,9-10<br>∑v(5) ∧ intro 6 11   |                                   |
| In this case the v-elim rule is used twice: once to establish the conjunct on line 6, and once to establish the conju<br>uses of a jattor in our original arrore in each of the colored submonds required by the feindrab use of violim   | 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<br>virginal proof once in each of the coloreral subvoords required by the (sindle) use of (value).   | ie two                            |
| Note 7: Equivalent logical power<br>When we say that two (collections) of rules are of equivalent logical power<br>of rules can also be constructed using the other collection. This does not r   | constructed using only one of the c<br>using one collection will be identica  | 36 11<br>ollections<br>  to those |
| using the other collection.<br>To convince ourselves that two collections are of equivalent power (in the<br>collection from the second (and the otherwise-fixed set of rules), and vice-   | using the other collection.<br>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<br>collection from the second (and the otherwise-fixed set of rules), and vice-versa.  | he first                          |
|   |   |                                   |

Notes

Introduction to Formal Proof 1: Formal Proofs in Propositional Calculus

| Calculus         |  |
|------------------|--|
| in Propositional |  |
| .⊑               |  |
| roofs            |  |
| Formal P         |  |
| ÷                |  |
| Proof            |  |
| Formal Proo      |  |
| to F             |  |
| Introduction to  |  |

# Notes

41 🕼

# Note 8: Typographical conventions

- ▷ 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.  $\triangle$
- ▷ For example: earlier we showed part of a proof that ∨ distributes through ∧ 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.

| assumption            | Theorem ¬(E · F) $\vdash$ ¬E ^ F 1 | > elim 2 | > elim 2 | - elim 4,3 |
|-----------------------|------------------------------------|----------|----------|------------|
| 1: -(Ev-E) assumption | ב: שרר∧שר                          | 3:E      | 4:<br>JE | T          |
| ÷                     | .∷                                 | ŝ        | 4        | ä          |

contra (classical) 1-5

6: Ev-E

 $13^{\rm th}$  April, 2017@13:42 [712]

- 50 -