# cs4004/cs4504: FORMAL VERIFICATION Lecture 5: Propositional Logic

Vasileios Koutavas



School of Computer Science and Statistics Trinity College Dublin

# Last lecture:

→ Syntactic entailment:  $A_1 ... A_n \vdash B$ 

Meaning: from  $A_1 ... A_n$  we can derive B using the inference rules of propositional logic

Different than semantic entailment  $A_1 ... A_n \models B$  and syntactic entailment  $A \rightarrow B$ . (there is a connection between these entailments)

→ Inference rules are defined using the system of natural deduction Conjuction introduction and elimination rules:

$$\frac{A_1}{B}$$
 RULE NAME

These are simple natural deduction rules

#### NATURAL DEDUCTION

Simple inference rules: "given formulas derive a formula," e.g.:

$$\frac{A_1}{A_1 \wedge A_2} \wedge i \qquad \frac{A_1 \wedge A_2}{A_1} \wedge e_1 \qquad \frac{A_1 \wedge A_2}{A_2} \wedge e_2$$

**Proof of**  $(p \land q) \land r$ ,  $s \land t \vdash q \land s$ .

1	$(p \land q) \land r$	premise
2	$s \wedge t$	premise
3	$p \wedge q$	∧e <sub>1</sub> 1
4	q	$\wedge e_2$ 3
5	S	∧ <i>e</i> <sub>1</sub> 2
6	$q \wedge s$	∧i 4,5

#### NATURAL DEDUCTION

Simple inference rules: "given formulas derive a formula," e.g.:

$$\frac{A_1}{A_1 \wedge A_2} \wedge i \qquad \frac{A_1 \wedge A_2}{A_1} \wedge e_1 \qquad \frac{A_1 \wedge A_2}{A_2} \wedge e_2$$

**Proof of**  $(p \land q) \land r$ ,  $s \land t \vdash q \land s$ .

1	$(p \wedge q) \wedge r$	premise
2	$s \wedge t$	premise
3	$b \lor d$	$\wedge e_1$ <sup>1</sup>
4	q	$\wedge e_2$ 3
5	S	∧e <sub>1</sub> 2
6	$q \wedge s$	$\wedge i$ 4, 5

\_

Simple inference rules: "given formulas derive a formula," e.g.:

$$\frac{A_1}{A_1 \wedge A_2} \wedge i \qquad \frac{A_1 \wedge A_2}{A_1} \wedge e_1 \qquad \frac{A_1 \wedge A_2}{A_2} \wedge e_2$$

**Proof of**  $(p \land q) \land r$ ,  $s \land t \vdash q \land s$ .

1	$(p \land q) \land r$	premise
2	$s \wedge t$	premise
3	$b \lor d$	$\lambda e_1 1$
4	q	$\wedge e_2$ 3
5	S	∧e <sub>1</sub> 2
6	$q \wedge s$	∧ <i>i</i> 4,5

#### NATURAL DEDUCTION

Simple inference rules: "given formulas derive a formula," e.g.:

$$\frac{A_1}{A_1 \wedge A_2} \wedge i \qquad \frac{A_1 \wedge A_2}{A_1} \wedge e_1 \qquad \frac{A_1 \wedge A_2}{A_2} \wedge e_2$$

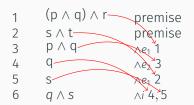
**Proof of**  $(p \land q) \land r$ ,  $s \land t \vdash q \land s$ .

1 
$$(p \land q) \land r$$
 premise  
2  $s \land t$  premise  
3  $p \land q$   $e_1 1$   
4  $q$   $he_2 3$   
5  $s$   $he_1 2$   
6  $q \land s$   $hi \ 4, 5$ 

Simple inference rules: "given formulas derive a formula," e.g.:

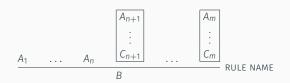
$$\frac{A_1}{A_1 \wedge A_2} \wedge i \qquad \frac{A_1 \wedge A_2}{A_1} \wedge e_1 \qquad \frac{A_1 \wedge A_2}{A_2} \wedge e_2$$

**Proof of**  $(p \land q) \land r$ ,  $s \land t \vdash q \land s$ .



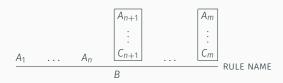
# NATURAL DEDUCTION

**Complex** inference rules: "given proofs and formulas derive a formula"



#### NATURAL DEDUCTION

Complex inference rules: "given proofs and formulas derive a formula"



Meaning of  $C_i$ : "assume  $A_i$  has been established in your proof and prove  $C_i$ ."

Example: disjunction rules.



The introduction rules of  $\lor$  are simple rules.

- → given a number of formulas as premises...(?)
- $\rightarrow$  produce a formula  $A_1 \lor A_2$ .

The introduction rules of  $\lor$  are simple rules.

- → given a number of formulas as premises...(?)
- → produce a formula  $A_1 \lor A_2$ .

$$\frac{A_1}{A_1 \vee A_2} \vee i_1 \qquad \frac{A_2}{A_1 \vee A_2} \vee i_2$$

The introduction rules of  $\lor$  are simple rules.

- → given a number of formulas as premises...(?)
- $\rightarrow$  produce a formula  $A_1 \lor A_2$ .

The elimination rules of  $\lor$  are complex rules.

- → given a formula  $A_1 \lor A_2$
- → and given some proofs... (?)
- → produce a formula B

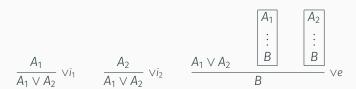
$$\frac{A_1}{A_1 \vee A_2} \vee i_1 \qquad \frac{A_2}{A_1 \vee A_2} \vee i_2$$

The introduction rules of  $\lor$  are simple rules.

- → given a number of formulas as premises...(?)
- $\rightarrow$  produce a formula  $A_1 \lor A_2$ .

The elimination rules of  $\lor$  are complex rules.

- $\rightarrow$  given a formula  $A_1 \lor A_2$
- → and given some proofs... (?)
- $\rightarrow$  produce a formula B



Prove  $p \lor q \vdash q \lor p$ 

Proof.

$$\frac{A_1}{A_1 \vee A_2} \vee i_1 \qquad \frac{A_2}{A_1 \vee A_2} \vee i_2 \qquad \frac{A_1 \vee A_2}{B} \wedge \epsilon$$

Prove  $p \lor q \vdash q \lor p$ 

Proof.

1 
$$p \lor q$$
 premise

$$\frac{A_1}{A_1 \vee A_2} \vee i_1 \qquad \frac{A_2}{A_1 \vee A_2} \vee i_2 \qquad \frac{A_1 \vee A_2}{B} \qquad \frac{\vdots}{B} \qquad Ae$$

Prove 
$$p \lor q \vdash q \lor p$$

Proof.

$$\begin{array}{cccc} 1 & p \lor q & premise \\ 2 & p & assumption \\ 3 & q \lor p & \lor i_2 2 \end{array}$$

$$\frac{A_1}{A_1 \vee A_2} \vee i_1 \qquad \frac{A_2}{A_1 \vee A_2} \vee i_2 \qquad \frac{A_1 \vee A_2}{B} \qquad \frac{A_1}{B} \wedge e$$

Prove  $p \lor q \vdash q \lor p$ 

Proof.

1	$p \vee q$	premise
2	р	assumption
3	$q \lor p$	$\vee i_2$ 2
4	9	assumption
5	$q \lor p$	∨i₁ 4

$$\frac{A_1}{A_1 \vee A_2} \vee i_1 \qquad \frac{A_2}{A_1 \vee A_2} \vee i_2 \qquad \frac{A_1 \vee A_2}{B} \qquad \frac{A_2}{B} \wedge e$$

Prove  $p \lor q \vdash q \lor p$ 

Proof.

1 
$$p \lor q$$
 premise  
2  $p$  assumption  
3  $q \lor p$   $\lor i_2$  2  
4  $q$  assumption  
5  $q \lor p$   $\lor i_1$  4  
6  $q \lor p$   $\lor e$  1, 2-3, 4-5

$$\frac{A_1}{A_1 \vee A_2} \vee i_1 \qquad \frac{A_2}{A_1 \vee A_2} \vee i_2 \qquad \frac{A_1 \vee A_2}{B} \qquad \frac{A_2}{B} \wedge e$$

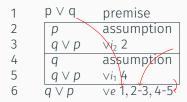
Prove  $p \lor q \vdash q \lor p$ 

Proof.

$$\frac{A_1}{A_1 \vee A_2} \vee i_1 \qquad \frac{A_2}{A_1 \vee A_2} \vee i_2 \qquad \frac{A_1 \vee A_2}{B} \qquad \frac{A_2}{B} \wedge e$$

Prove  $p \lor q \vdash q \lor p$ 

Proof.



Boxes are subproofs, from (A) given assumptions and (B) the formulas we know before the subproof we derive an intermediate conclusion. (Here we did not have to use (B))

$$\frac{A_1}{A_1 \vee A_2} \vee i_1 \qquad \frac{A_2}{A_1 \vee A_2} \vee i_2 \qquad \frac{A_1 \vee A_2}{B} \qquad \frac{A_1}{B} \wedge \epsilon$$

Prove  $(p \lor q) \lor r \vdash p \lor (q \lor r)$ . (Hint: nested boxes)

$$\frac{A_1}{A_1 \vee A_2} \vee i_1 \qquad \frac{A_2}{A_1 \vee A_2} \vee i_2 \qquad \frac{A_1 \vee A_2}{B} \vee i_2$$

Prove  $p \land (q \lor r) \vdash (p \land q) \lor (p \land r)$  and  $(p \land q) \lor (p \land r) \vdash p \land (q \lor r)$ .

$$\frac{A_1}{A_1 \wedge A_2} \wedge i \qquad \frac{A_1 \wedge A_2}{A_1} \wedge e_1 \qquad \frac{A_1 \wedge A_2}{A_2} \wedge e_2$$

$$\frac{A_1}{A_1 \vee A_2} \vee i_1 \qquad \frac{A_2}{A_1 \vee A_2} \vee i_2 \qquad \frac{A_1 \vee A_2}{B} \qquad B$$



# IMPLICATION ELIMINATION

First: elimination of  $\rightarrow$  (aka modus ponens)

$$\frac{A \qquad A \to B}{B} \to e$$

#### IMPLICATION ELIMINATION

First: elimination of  $\rightarrow$  (aka modus ponens)

$$\frac{A \qquad A \to B}{B} \to e$$

## From:

p: it rained

 $p \rightarrow q$ : if it rained then the street is wet

# we derive:

q: the street is wet

#### IMPLICATION ELIMINATION

First: elimination of  $\rightarrow$  (aka modus ponens)

$$\frac{A \qquad A \to B}{B} \to e$$

## From:

p: it rained

 $p \rightarrow q$ : if it rained then the street is wet

# we derive:

q: the street is wet

## From:

p: the program input is an array

 $p \rightarrow q$ : if the program input is an array then the program output is a sorted array

# we derive:

q: the program output is a sorted array

# PROOF WITH IMPLICATION

Show 
$$p \rightarrow q \rightarrow r$$
,  $p$ ,  $q \vdash r$ 

Show 
$$p \rightarrow q \rightarrow r$$
,  $p$ ,  $p \rightarrow q \vdash r$ 

$$\frac{A \qquad A \to B}{B} \to e$$

## IMPLICATION: MODUS TOLLENS

If we prove  $A_1, ... A_n \vdash B$  then we can use in our proofs a derivable rule (aka a theorem)

$$\frac{A_1}{B}$$
 ...  $\frac{A_n}{B}$ 

If we prove  $A_1, ... A_n \vdash B$  then we can use in our proofs a derivable rule (aka a theorem)

$$\frac{A_1}{B}$$
 ...  $\frac{A_n}{B}$ 

The following is a derivable rule:

this is called modus tollens.

# IMPLICATION INTRODUCTION

Introduction of  $\rightarrow$ :

$$\frac{\begin{vmatrix} A \\ \vdots \\ B \end{vmatrix}}{A \to B} \to i$$

"If we can prove B by assuming A, then A implies B."

#### **IMPLICATION PROOFS**

Prove:  $p \rightarrow q \vdash \neg q \rightarrow \neg p$ 

Example statement: If it rained then the road is wet. Therefore, if the road is not wet then it did not rain.

$$\frac{A \qquad A \to B}{B} \to e \qquad \frac{\stackrel{\stackrel{\longrightarrow}{i}}{\stackrel{:}{B}}}{A \to B} \to i \qquad \frac{A_1 \to A_2 \qquad \neg A_2}{\neg A_1} \text{ MT}$$