

CSU44004/CSU55004: FORMAL VERIFICATION

Lecture 5: Propositional Logic

Vasileios Koutavas



School of Computer Science and Statistics
Trinity College Dublin

Last lecture:

→ **Syntactic entailment**: $A_1 \dots A_n \vdash B$

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

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

→ Inference rules are defined using the system of **natural deduction**

Conjunction introduction and elimination rules:

$$\frac{A_1 \quad \dots \quad A_n}{B} \text{ RULE NAME}$$

These are **simple natural deduction rules**

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

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

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

| | | |
|---|-------------------------|-----------------|
| 1 | $(p \wedge q) \wedge r$ | premise |
| 2 | $s \wedge t$ | premise |
| 3 | $p \wedge q$ | $\wedge e_1$ 1 |
| 4 | q | $\wedge e_2$ 3 |
| 5 | s | $\wedge e_1$ 2 |
| 6 | $q \wedge s$ | $\wedge i$ 4, 5 |



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

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

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

| | | |
|---|-------------------------|-----------------|
| 1 | $(p \wedge q) \wedge r$ | premise |
| 2 | $s \wedge t$ | premise |
| 3 | $p \wedge q$ | $\wedge e_1$ 1 |
| 4 | q | $\wedge e_2$ 3 |
| 5 | s | $\wedge e_1$ 2 |
| 6 | $q \wedge s$ | $\wedge i$ 4, 5 |

□

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

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

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

| | | |
|---|-------------------------|-----------------|
| 1 | $(p \wedge q) \wedge r$ | premise |
| 2 | $s \wedge t$ | premise |
| 3 | $p \wedge q$ | $\wedge e_1$ 1 |
| 4 | q | $\wedge e_2$ 3 |
| 5 | s | $\wedge e_1$ 2 |
| 6 | $q \wedge s$ | $\wedge i$ 4, 5 |

□

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

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

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

| | | |
|---|-------------------------|-----------------|
| 1 | $(p \wedge q) \wedge r$ | premise |
| 2 | $s \wedge t$ | premise |
| 3 | $p \wedge q$ | $\wedge e_1$ 1 |
| 4 | q | $\wedge e_2$ 3 |
| 5 | s | $\wedge e_1$ 2 |
| 6 | $q \wedge s$ | $\wedge i$ 4, 5 |

□

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

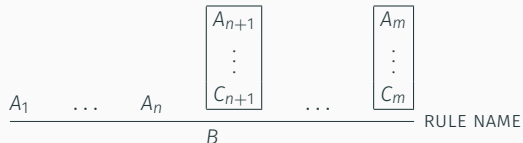
$$\frac{A_1 \quad A_2}{A_1 \wedge A_2} \wedge i \qquad \frac{A_1 \wedge A_2}{A_1} \wedge e_1 \qquad \frac{A_1 \wedge A_2}{A_2} \wedge e_2$$

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

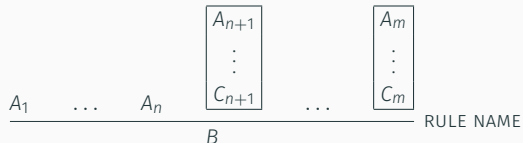
| | | |
|---|-------------------------|-----------------|
| 1 | $(p \wedge q) \wedge r$ | premise |
| 2 | $s \wedge t$ | premise |
| 3 | $p \wedge q$ | $\wedge e_1$ 1 |
| 4 | q | $\wedge e_2$ 3 |
| 5 | s | $\wedge e_1$ 2 |
| 6 | $q \wedge s$ | $\wedge i$ 4, 5 |



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



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



Meaning of $\boxed{\begin{array}{c} A_i \\ \vdots \\ C_i \end{array}}$: “assume A_i has been established in your proof and prove C_i .”

Example: disjunction rules.

DISJUNCTION

The introduction rules of \vee are simple rules.

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

The introduction rules of \vee are simple rules.

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

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

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

The introduction rules of \vee are simple rules.

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

The elimination rules of \vee are complex rules.

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

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

DISJUNCTION RULES

The introduction rules of \vee are simple rules.

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

The elimination rules of \vee are complex rules.

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

$$\frac{A_1}{A_1 \vee A_2} \vee i_1 \qquad \frac{A_2}{A_1 \vee A_2} \vee i_2 \qquad \frac{A_1 \vee A_2 \quad \boxed{\begin{array}{c} A_1 \\ \vdots \\ B \end{array}} \quad \boxed{\begin{array}{c} A_2 \\ \vdots \\ B \end{array}}}{B} \vee e$$

PROOF WITH DISJUNCTION

Prove $p \vee q \vdash q \vee p$

Proof.



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

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

$$\frac{A_1 \vee A_2 \quad \boxed{\begin{array}{c} A_1 \\ \vdots \\ B \end{array}} \quad \boxed{\begin{array}{c} A_2 \\ \vdots \\ B \end{array}}}{B} \wedge e$$

PROOF WITH DISJUNCTION

Prove $p \vee q \vdash q \vee p$

Proof.

1 $p \vee q$ premise

□

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

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

$$\frac{A_1 \vee A_2 \quad \boxed{\begin{array}{c} A_1 \\ \vdots \\ B \end{array}} \quad \boxed{\begin{array}{c} A_2 \\ \vdots \\ B \end{array}}}{B} \wedge e$$

PROOF WITH DISJUNCTION

Prove $p \vee q \vdash q \vee p$

Proof.

| | | |
|---|------------|--------------|
| 1 | $p \vee q$ | premise |
| 2 | p | assumption |
| 3 | $q \vee p$ | $\vee i_2$ 2 |

□

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

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

$$\frac{A_1 \vee A_2 \quad \begin{array}{|c|} \hline A_1 \\ \vdots \\ B \\ \hline \end{array} \quad \begin{array}{|c|} \hline A_2 \\ \vdots \\ B \\ \hline \end{array}}{B} \wedge e$$

PROOF WITH DISJUNCTION

Prove $p \vee q \vdash q \vee p$

Proof.

| | | |
|---|------------|--------------|
| 1 | $p \vee q$ | premise |
| 2 | p | assumption |
| 3 | $q \vee p$ | $\vee i_2$ 2 |
| 4 | q | assumption |
| 5 | $q \vee p$ | $\vee i_1$ 4 |

□

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

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

$$\frac{A_1 \vee A_2 \quad \begin{array}{|c|} \hline A_1 \\ \vdots \\ B \\ \hline \end{array} \quad \begin{array}{|c|} \hline A_2 \\ \vdots \\ B \\ \hline \end{array}}{B} \wedge e$$

PROOF WITH DISJUNCTION

Prove $p \vee q \vdash q \vee p$

Proof.

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

□

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

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

$$\frac{A_1 \vee A_2 \quad \begin{array}{|c|} \hline A_1 \\ \vdots \\ B \\ \hline \end{array} \quad \begin{array}{|c|} \hline A_2 \\ \vdots \\ B \\ \hline \end{array}}{B} \wedge e$$

PROOF WITH DISJUNCTION

Prove $p \vee q \vdash q \vee p$

Proof.

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

□

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

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

$$\frac{A_1 \vee A_2 \quad \begin{array}{|c|} \hline A_1 \\ \vdots \\ B \\ \hline \end{array} \quad \begin{array}{|c|} \hline A_2 \\ \vdots \\ B \\ \hline \end{array}}{B} \wedge e$$

PROOF WITH DISJUNCTION

Prove $p \vee q \vdash q \vee p$

Proof.

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

□

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))

$$\begin{array}{c}
 \frac{A_1}{A_1 \vee A_2} \vee i_1 \quad \frac{A_2}{A_1 \vee A_2} \vee i_2 \quad \frac{A_1 \vee A_2 \quad \boxed{\begin{array}{c} \vdots \\ B \end{array}} \quad \boxed{\begin{array}{c} \vdots \\ B \end{array}}}{B} \wedge e
 \end{array}$$

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

$$\begin{array}{c}
 \frac{A_1}{A_1 \vee A_2} \vee i_1 \qquad \frac{A_2}{A_1 \vee A_2} \vee i_2 \qquad \frac{A_1 \vee A_2 \quad \boxed{\begin{array}{c} A_1 \\ \vdots \\ B \end{array}} \quad \boxed{\begin{array}{c} A_2 \\ \vdots \\ B \end{array}}}{B} \vee e
 \end{array}$$

Prove $p \wedge (q \vee r) \vdash (p \wedge q) \vee (p \wedge r)$ and $(p \wedge q) \vee (p \wedge r) \vdash p \wedge (q \vee r)$.

$$\begin{array}{c}
 \frac{A_1 \quad A_2}{A_1 \wedge A_2} \wedge i \qquad \frac{A_1 \wedge A_2}{A_1} \wedge e_1 \qquad \frac{A_1 \wedge A_2}{A_2} \wedge e_2 \\
 \\
 \frac{A_1}{A_1 \vee A_2} \vee i_1 \qquad \frac{A_2}{A_1 \vee A_2} \vee i_2 \qquad \frac{A_1 \vee A_2 \quad \boxed{\begin{array}{c} A_1 \\ \vdots \\ B \end{array}} \quad \boxed{\begin{array}{c} A_2 \\ \vdots \\ B \end{array}}}{B} \vee e
 \end{array}$$

IMPLICATION

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

$$\frac{A \quad A \rightarrow B}{B} \rightarrow e$$

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

$$\frac{A \quad A \rightarrow B}{B} \rightarrow e$$

From:

p : it rained

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

we derive:

q : the street is wet

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

$$\frac{A \quad A \rightarrow B}{B} \rightarrow e$$

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

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

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

$$\frac{A \quad A \rightarrow B}{B} \rightarrow e$$

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

$$\frac{A_1 \quad \dots \quad A_n}{B}$$

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

$$\frac{A_1 \quad \dots \quad A_n}{B}$$

The following is a derivable rule:

$$\frac{A_1 \rightarrow A_2 \quad \neg A_2}{\neg A_1} \text{ MT}$$

this is called **modus tollens**.

Introduction of \rightarrow :

$$\frac{\begin{array}{|c|} A \\ \vdots \\ B \end{array}}{A \rightarrow B} \rightarrow i$$

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

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.

$$\begin{array}{c}
 \frac{A \quad A \rightarrow B}{B} \rightarrow e \qquad \frac{\boxed{\begin{array}{c} A \\ \vdots \\ B \end{array}}}{A \rightarrow B} \rightarrow i \qquad \frac{A_1 \rightarrow A_2 \quad \neg A_2}{\neg A_1} \text{ MT}
 \end{array}$$