CS4004/CS4504: FORMAL VERIFICATION

Lecture 5: Propositional Logic

Vasileios Koutavas

School of Computer Science and Statistics
Trinity College Dublin

Last lecture:

- Syntactic entailment: $A_1 \dots A_n \vdash B$

  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
  Conjuction introduction and elimination rules:

$$\frac{A_1 \qquad \dots \qquad A_n}{B}\ \textsc{rule name}$$

  These are **simple natural deduction rules**

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

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

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

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

$\square$

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

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

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

$\square$

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

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

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

$\square$

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

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

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

$\square$

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

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

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

$\square$

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

$$\cfrac{A_1 \qquad \dots \qquad A_n \qquad \boxed{\begin{matrix} A_{n+1} \\ \vdots \\ C_{n+1} \end{matrix}} \qquad \dots \qquad \boxed{\begin{matrix} A_m \\ \vdots \\ C_m \end{matrix}}}{B}\ \text{RULE NAME}$$

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

$$\dfrac{A_1 \quad \ldots \quad A_n \quad \boxed{\begin{matrix} A_{n+1} \\ \vdots \\ C_{n+1} \end{matrix}} \quad \ldots \quad \boxed{\begin{matrix} A_m \\ \vdots \\ C_m \end{matrix}}}{B}\ \textsc{Rule name}$$

Meaning of $\boxed{\begin{matrix} A_i \\ \vdots \\ C_i \end{matrix}}$: “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 $A_1 \vee A_2$.

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

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

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

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

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

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

Proof.

$\square$

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

PROOF WITH DISJUNCTION

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

Proof.

1	p ∨ q	premise

□

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

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

Proof.

1	p ∨ q	premise
2	p	assumption
3	$q \vee p$	$\vee i_2$ 2

□

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

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

Proof.

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

□

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

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

□

$$\frac{A_1}{A_1 \vee A_2}\ \vee i_1 \qquad \frac{A_2}{A_1 \vee A_2}\ \vee i_2 \qquad \frac{A_1 \vee A_2 \qquad \boxed{\begin{matrix} A_1 \\ \vdots \\ B \end{matrix}} \qquad \boxed{\begin{matrix} A_2 \\ \vdots \\ B \end{matrix}}}{B}\ \wedge e$$

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

Proof.

1	p ∨ 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

□

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

PROOF WITH DISJUNCTION

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

$\square$

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))

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

PROOF WITH DISJUNCTION

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

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

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

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

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

Implication

First: elimination of $\to$ (aka **modus ponens**)

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

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

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

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**)

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

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 $p \to q \to r,\ p,\ q \vdash r$

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

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

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

$$\frac{A_1 \qquad \ldots \qquad A_n}{B}$$

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

$$\frac{A_1 \qquad \ldots \qquad A_n}{B}$$

The following is a derivable rule:

$$\frac{A_1 \to A_2 \qquad \neg A_2}{\neg A_1}\ \mathrm{MT}$$

this is called **modus tollens**.

Introduction of $\rightarrow$:

$$\frac{\boxed{\begin{matrix} A \\ \vdots \\ B \end{matrix}}}{A \rightarrow B} \rightarrow i$$

"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.

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