CS4004/CS4504: FORMAL VERIFICATION

Lecture 6: Propositional Logic

Vasileios Koutavas

School of Computer Science and Statistics
Trinity College Dublin

We are working with natural deduction proofs $A_1 \ldots A_n \vdash B$ in propositional logic. Deduction rules so far:

- **Conjunction:** $\dfrac{A_1 \qquad A_2}{A_1 \wedge A_2} \wedge i \qquad \dfrac{A_1 \wedge A_2}{A_1} \wedge e_1 \qquad \dfrac{A_1 \wedge A_2}{A_2} \wedge e_2$

- **Disjunction:** $\dfrac{A_1}{A_1 \vee A_2} \vee i_1 \qquad \dfrac{A_2}{A_1 \vee A_2} \vee i_2 \qquad \dfrac{A_1 \vee A_2 \qquad \boxed{\begin{matrix} A_1 \\ \cdots \\ B \end{matrix}} \qquad \boxed{\begin{matrix} A_2 \\ \cdots \\ B \end{matrix}}}{B} \vee e$

- **Implication:** $\dfrac{\boxed{\begin{matrix} A \\ \cdots \\ B \end{matrix}}}{A \to B} \to i \qquad \dfrac{A \qquad A \to B}{B} \to e$

and the derived: $\dfrac{A_1 \to A_2 \qquad \neg A_2}{\neg A_1} \text{MT}$

Notice the introduction rule of implication:

$$\frac{\boxed{\begin{array}{c} A \\ \cdots \\ B \end{array}}}{A \rightarrow B} \rightarrow i$$

It contains only one premise: $\boxed{\begin{array}{c} A \\ \cdots \\ B \end{array}}$

Notice the introduction rule of implication:

$$\frac{\boxed{\begin{array}{c} A \\ \cdots \\ B \end{array}}}{A \to B} \to i$$

It contains only one premise: $\boxed{\begin{array}{c} A \\ \cdots \\ B \end{array}}$

This means that we can think of premises of the form $\boxed{\begin{array}{c} A \\ \cdots \\ B \end{array}}$ as premises of the form $A \to B$

Notice the introduction rule of implication:

$$\frac{\boxed{\begin{array}{c} A \\ \cdots \\ B \end{array}}}{A \to B} \to i$$

It contains only one premise: $\boxed{\begin{array}{c} A \\ \cdots \\ B \end{array}}$

This means that we can think of premises of the form $\boxed{\begin{array}{c} A \\ \cdots \\ B \end{array}}$

as premises of the form $A \to B$

We would have exactly the same logic if we replaced all box-premises with implication-premises, except for the premise in ($\to i$).

We have seen how to prove $p \to q \vdash \neg q \to \neg p$

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

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

$$\frac{\boxed{\begin{array}{c} A \\ \cdots \\ B \end{array}}}{A \to B} \to i \qquad \frac{A \qquad A \to B}{B} \to e \qquad \frac{A_1 \to A_2 \qquad \neg A_2}{\neg A_1}\ \mathrm{MT}$$

IMPLICATION PROOFS

Is this entailment correct? $(p \vee q) \to r \vdash (p \to r) \wedge (q \to r)$

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

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

$$\frac{\boxed{\begin{array}{c} A \\ \cdots \\ B \end{array}}}{A \to B}\ \to i \qquad \frac{A \qquad A \to B}{B}\ \to e \qquad \frac{A_1 \to A_2 \qquad \neg A_2}{\neg A_1}\ \mathrm{MT}$$

The following derivable rule has a trivial proof. Sometimes this is useful to prove the goals of inner proofs using the established facts before these proofs.

$$\frac{A}{A}\ \text{COPY}$$

Show the following theorem: $\vdash p \to q \to p$.

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

Negation

Writing contradictions in the logic:

- $p \wedge \neg p$
- $(p \wedge q) \wedge \neg(p \wedge q)$
- $(p \to \neg q \vee r) \wedge \neg(p \to \neg q \vee r)$
- ...

Writing contradictions in the logic:

- $p \wedge \neg p$
- $(p \wedge q) \wedge \neg(p \wedge q)$
- $(p \rightarrow \neg q \vee r) \wedge \neg(p \rightarrow \neg q \vee r)$
- ...

Contradictions are formulas whose semantics returns F for all models.

Writing contradictions in the logic:

- $p \land \neg p$
- $(p \land q) \land \neg(p \land q)$
- $(p \to \neg q \lor r) \land \neg(p \to \neg q \lor r)$
- ...

Contradictions are formulas whose semantics returns F for all models. They are unsatisfiable.

Formulas of the form $A \land \neg A$ are unsatisfiable.

Writing contradictions in the logic:

- $p \land \neg p$
- $(p \land q) \land \neg(p \land q)$
- $(p \to \neg q \lor r) \land \neg(p \to \neg q \lor r)$
- ...

Contradictions are formulas whose semantics returns F for all models. They are unsatisfiable.

Formulas of the form $A \land \neg A$ are unsatisfiable.

They are all semantically equivalent: $A \land \neg A \equiv B \land \neg B$, for all A, B. [1]

[1] $A \equiv B$ means $A \models B$ and $B \models A$

Writing contradictions in the logic:

- $p \wedge \neg p$
- $(p \wedge q) \wedge \neg(p \wedge q)$
- $(p \to \neg q \vee r) \wedge \neg(p \to \neg q \vee r)$
- ...

Contradictions are formulas whose semantics returns F for all models. They are unsatisfiable.

Formulas of the form $A \wedge \neg A$ are unsatisfiable.

They are all semantically equivalent: $A \wedge \neg A \equiv B \wedge \neg B$, for all A, B. [1]

We should be able to prove $A \wedge \neg A \dashv\vdash B \wedge \neg B$, for all A, B. [2]

[1] $A \equiv B$ means $A \models B$ and $B \models A$

[2] $A \dashv\vdash B$ means $A \vdash B$ and $B \vdash A$

Writing contradictions in the logic:

- $p \wedge \neg p$
- $(p \wedge q) \wedge \neg(p \wedge q)$
- $(p \rightarrow \neg q \vee r) \wedge \neg(p \rightarrow \neg q \vee r)$
- ...

Contradictions are formulas whose semantics returns F for all models. They are unsatisfiable.

Formulas of the form $A \wedge \neg A$ are unsatisfiable.

They are all semantically equivalent: $A \wedge \neg A \equiv B \wedge \neg B$, for all A, B. [1]

We should be able to prove $A \wedge \neg A \dashv\vdash B \wedge \neg B$, for all A, B. [2]

In fact we will show $A \wedge \neg A \vdash B$, for all A, B!
Intuition: if something as absurd as $A \wedge \neg A$ is considered true then any B can be shown to be true.

[1] $A \equiv B$ means $A \models B$ and $B \models A$
[2] $A \dashv\vdash B$ means $A \vdash B$ and $B \vdash A$

We will pick an atomic proposition (say p) and name the following:

- we write $\bot$ (pronounced “bottom”) to represent $p \wedge \neg p$
- we also write $\top$ (pronounced “top”) to represent $\neg(p \wedge \neg p)$
  (we don’t need the latter here but it will be useful to have later on)

We will pick an atomic proposition (say p) and name the following:

- we write $\perp$ (pronounced "bottom") to represent $p \wedge \neg p$
- we also write $\top$ (pronounced "top") to represent $\neg(p \wedge \neg p)$
  (we don't need the latter here but it will be useful to have later on)

We will allow to introduce $\perp$ from any contradiction (not just $p \wedge \neg p$). This rule **eliminates** $\neg$:

$$\frac{A \qquad \neg A}{\perp}\ \neg e$$

We will pick an atomic proposition (say p) and name the following:

- we write $\bot$ (pronounced “bottom”) to represent $p \wedge \neg p$
- we also write $\top$ (pronounced “top”) to represent $\neg(p \wedge \neg p)$
  (we don’t need the latter here but it will be useful to have later on)

We will allow to introduce $\bot$ from any contradiction (not just $p \wedge \neg p$). This rule **eliminates** $\neg$:

$$\frac{A \qquad \neg A}{\bot} \neg e$$

To introduce a negation $\neg A$ we must show that from A we can derive bottom (a contradiction).

We will pick an atomic proposition (say p) and name the following:

- we write $\bot$ (pronounced "bottom") to represent $p \land \neg p$
- we also write $\top$ (pronounced "top") to represent $\neg(p \land \neg p)$
  (we don't need the latter here but it will be useful to have later on)

We will allow to introduce $\bot$ from any contradiction (not just $p \land \neg p$). This rule **eliminates** $\neg$:

$$\frac{A \qquad \neg A}{\bot}\ \neg e$$

To introduce a negation $\neg A$ we must show that from A we can derive bottom (a contradiction).

$$\frac{\boxed{\begin{array}{c} A \\ \cdots \\ \bot \end{array}}}{\neg A}\ \neg i$$

We will pick an atomic proposition (say p) and name the following:

- we write $\bot$ (pronounced "bottom") to represent $p \land \neg p$
- we also write $\top$ (pronounced "top") to represent $\neg(p \land \neg p)$
  (we don't need the latter here but it will be useful to have later on)

We will allow to introduce $\bot$ from any contradiction (not just $p \land \neg p$). This rule **eliminates** $\neg$:

$$\frac{A \qquad \neg A}{\bot}\ \neg e$$

To introduce a negation $\neg A$ we must show that from A we can derive bottom (a contradiction).

$$\frac{\boxed{\begin{array}{c} A \\ \cdots \\ \bot \end{array}}}{\neg A}\ \neg i$$

Finally, from bottom we are allowed to derive anything: $\dfrac{\bot}{A}\ \bot e$

Show: $(p \to \neg q \lor r) \land \neg(p \to \neg q \lor r) \ \vdash \ s$

$$\frac{A \qquad \neg A}{\perp}\ \neg e \qquad \frac{\boxed{\begin{array}{c} A \\ \cdots \\ \perp \end{array}}}{\neg A}\ \neg i \qquad \frac{\perp}{A}\ \perp e$$

Show: $p, \neg q \vdash \neg(p \rightarrow q)$

$$\frac{A \qquad \neg A}{\bot}\ \neg e \qquad \frac{\boxed{\begin{array}{c} A \\ \cdots \\ \bot \end{array}}}{\neg A}\ \neg i \qquad \frac{\bot}{A}\ \bot e \qquad \frac{A \qquad A \rightarrow B}{B} \rightarrow e$$