

CS/IS F214 Logic in Computer Science

### MODULE: PROPOSITIONAL LOGIC

#### **Proof of Soundness**

# **Proving Soundness**

#### • Theorem:

• Let  $\phi_1$ ,  $\phi_2$ , ...,  $\phi_n$  and  $\psi$  be propositional logic formulas: If  $\phi_1$ ,  $\phi_2$ , ...,  $\phi_n$  |-  $\psi$  holds then  $\phi_1$ ,  $\phi_2$ , ...,  $\phi_n$  |=  $\psi$  holds.



# **Proving Soundness**

#### • Theorem:

• Let  $\phi_1$ ,  $\phi_2$ , ...,  $\phi_n$  and  $\psi$  be propositional logic formulas. If  $\phi_1$ ,  $\phi_2$ , ...,  $\phi_n$  |-  $\psi$  holds then  $\phi_1$ ,  $\phi_2$ , ...,  $\phi_n$  |=  $\psi$  holds.

## • Proof Outline:

- If  $\phi_1$ ,  $\phi_2$ , ...,  $\phi_n$  |-  $\psi$  holds <u>then there is a proof</u> of  $\psi$  from the premises  $\phi_1$ ,  $\phi_2$ , ...,  $\phi_n$
- We show <u>by mathematical induction on the length of this</u> proof that  $\varphi_1, \varphi_2, ..., \varphi_n = \psi$  must hold.
  - Length of the proof is the number of lines (i.e. steps).
- To be precise, by induction on k, we show M(k):
  - For all sequents  $\phi_1$ ,  $\phi_2$ , ...,  $\phi_n$  |  $\psi$  which have a proof of length k,
    - $\varphi_1, \varphi_2, ..., \varphi_n = \psi$  holds.

## Induction on the length of a Proof

### Consider the following sequent

$$p \land q \longrightarrow r \mid -p \longrightarrow (q \longrightarrow r)$$
  
and the following proof of it:

1	p∧q>r	Premise
2	р	Assumption
3	q	Assumption
4	p∧q	∧i 2,3
5	r	>e1,4
6	q>r	>i3-5
7	p>(q>r)	>i2-6

- •Suppose we remove the last line:
  - we don't get a complete proof (of anything).
    - Why?

### Induction on the length of a Proof - Example

## A proof of:

$$p \land q --> r \mid -p --> (q --> r)$$

1	p∧q>r	Premise
2	p	Assumption
3	q	Assumption
4	p∧q	∧i 2,3
5	r	>e1,4
6	q>r	>i3-5_
7	p>(q>r)	>i2-6

 Removing the last line results in an incomplete proof.

#### •We can fix this:

- by <u>changing the assumption in</u> line 2 <u>into a premise</u>
- •Then we get a (shorter) proof of

$$p \wedge q \longrightarrow r, p \mid - (q \longrightarrow r)$$

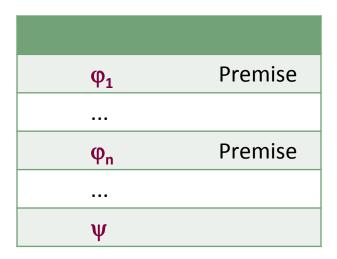
1	p∧q>r	Premise
2	р	Premise
3	q	Assumption
4	p∧q	∧i 2,3
5	r	>e1,4
6	q>r	>i3-5

# Proving Soundness (by induction on *proof length*):

- Let M(k) be :
  - For all sequents  $\varphi_1$ ,  $\varphi_2$ , ...,  $\varphi_n$  |-  $\psi$  that have a proof of length k,  $\varphi_1$ ,  $\varphi_2$ , ...,  $\varphi_n$  |=  $\psi$  holds.
- Base Case: (k=1)
  - Then the proof must only have a premise, say  $\psi$ . Why?
  - i.e. this is a proof of  $\psi$  |-  $\psi$ .
    - But trivially,  $\psi \mid = \psi$ .
      - Why?
- Induction Step:
  - **Hypothesis**: Assume M(k') to be true for all k' < k.



Consider the proof of the sequent  $\phi_1$ ,  $\phi_2$ , ...,  $\phi_n$  |-  $\psi$  of length k:



What was the last rule applied? Consider case by case:

Consider the proof of the sequent  $\phi_1$ ,  $\phi_2$ , ...,  $\phi_n$  |-  $\psi$  of length k:



What was the last rule applied? Consider case by case:

case ∧i: (see opposite column)

- If the last rule were ∧i:
  - then  $\psi$  is of the form  $\psi_1 \wedge \psi_2$
- •in which case there were sub-proofs for  $\psi_1$  and  $\psi_2$ 
  - i.e. we have proofs of

• 
$$\phi_1, \phi_2, ..., \phi_n \mid -\psi_1$$
 and

• 
$$\phi_1, \phi_2, ..., \phi_n \mid -\psi_2$$

- each of length < k.
- By hypothesis,

• 
$$\phi_1$$
,  $\phi_2$ , ...,  $\phi_n | = \psi_1$  and

• 
$$\phi_1, \phi_2, ..., \phi_n = \psi_2$$

- and so
  - $\varphi_1, \varphi_2, ..., \varphi_n \mid = \psi_1 \wedge \psi_2$  (by semantics)

Consider the proof of the sequent  $\phi_1$ ,  $\phi_2$ , ...,  $\phi_n$  |-  $\psi$  of length k:

$\phi_1$	Premise
$\varphi_{n}$	Premise
Ψ	

What was the last rule applied? case -->i: (see opposite column)

- <u>If the last rule were -->i</u>:
  - then  $\psi$  is of the form  $\psi_1 \longrightarrow \psi_2$
- •in which case there was a subproof for  $\psi_2$  assuming  $\psi_1$ 
  - i.e. we have a proof of

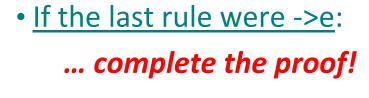
• 
$$\phi_1$$
,  $\phi_2$ , ...,  $\phi_n$ ,  $\psi_1 | - \psi_2$ 

- of length < k.</li>
- By hypothesis,

• 
$$\phi_1, \phi_2, ..., \phi_n, \psi_1 = \psi_2$$

- and so
  - $\phi_1, \phi_2, ..., \phi_n \mid = \psi_1 --> \psi_2$  (by truth table)

Consider the proof of the sequent  $\phi_1$ ,  $\phi_2$ , ...,  $\phi_n$  |-  $\psi$  of length k:



$\phi_1$	Premise
$\varphi_{n}$	Premise
•••	
Ψ	

Other cases are similar – do the following case:

case -->e:

# **Proving Soundness**

- Thus we have proven that, for all k,
  - For all sequents  $\phi_1$ ,  $\phi_2$ , ...,  $\phi_n$  |  $\psi$  which have a proof of length k,
    - $\varphi_1, \varphi_2, ..., \varphi_n = \psi$  holds
- by assuming that
  - for all sub-proofs deriving an intermediate  $\psi'$ , which are of length less than k,
    - $\phi_1, \phi_2, ..., \phi_n = \psi'$  holds.

Q.E.D.

