

# CS4004/CS4504: FORMAL VERIFICATION

## Lecture 3: Propositional Logic

---

Vasileios Koutavas



School of Computer Science and Statistics  
Trinity College Dublin

## Definition

A is **satisfiable** when it has **a model** which makes it true.

A is **falsifiable** when it has **a model** which makes it false.

A is **valid** or **a tautology** when **all models** make it true.

A is **invalid** or **a contradiction** when **all models** make it false.

## Definition

A is **satisfiable** when it has **a model** which makes it true.

A is **falsifiable** when it has **a model** which makes it false.

A is **valid** or **a tautology** when **all models** make it true.

A is **invalid** or **a contradiction** when **all models** make it false.

Q: which of the above are properties of

$$(p \rightarrow \neg q) \rightarrow (q \vee \neg p)$$

## Definition

A is **satisfiable** when it has **a model** which makes it true.

A is **falsifiable** when it has **a model** which makes it false.

A is **valid** or **a tautology** when **all models** make it true.

A is **invalid** or **a contradiction** when **all models** make it false.

Q: which of the above are properties of

$$(p \rightarrow \neg q) \rightarrow (q \vee \neg p)$$

Q: show that if  $A_1 \wedge (A_2 \wedge A_3)$  is satisfiable then  $(A_1 \wedge A_2) \wedge A_3$  is satisfiable.

### Definition

A is **satisfiable** when it has **a model** which makes it true.

A is **falsifiable** when it has **a model** which makes it false.

A is **valid** or **a tautology** when **all models** make it true.

A is **invalid** or **a contradiction** when **all models** make it false.

Q: which of the above are properties of

$$(p \rightarrow \neg q) \rightarrow (q \vee \neg p)$$

Q: show that if  $A_1 \wedge (A_2 \wedge A_3)$  is satisfiable then  $(A_1 \wedge A_2) \wedge A_3$  is satisfiable.

Q: Let  $(A_1 \wedge A_2) \rightarrow A_3$  be valid. Is it necessary that  $A_3$  is satisfiable?

Our goal is to use the logic to derive logical **conclusions** from logical **premises** (assumptions).

Two ways to do this:

- **Syntactic reasoning**: using syntactic axioms and derivation rules. **The preferred way** because it's easier. We'll see this in the next lecture.

Our goal is to use the logic to derive logical **conclusions** from logical **premises** (assumptions).

Two ways to do this:

- **Syntactic reasoning**: using syntactic axioms and derivation rules.  
**The preferred way** because it's easier. We'll see this in the next lecture.
- **Semantic reasoning**: using the truth values.  
We already did this in the associativity questions.

## Definition

We write  $A_1, \dots, A_n \models B$  to mean that any valuation giving to all  $A_1, \dots, A_n$  the value T also gives  $B$  the value T.

This is called **semantic entailment**.

We call  $A_1, \dots, A_n$  the **premises** or **antecedents**.

We call  $B$  the **conclusion** or **consequent**.

We assume that *any valuation* makes the **empty premises** T.

We will write  $A \equiv B$  when  $A \models B$  and  $B \models A$ . This is called **semantic equivalence**.



## Definition

We write  $A_1, \dots, A_n \models B$  to mean that any valuation giving to all  $A_1, \dots, A_n$  the value T also gives  $B$  the value T.

This is called **semantic entailment**.

We call  $A_1, \dots, A_n$  the **premises** or **antecedents**.

We call  $B$  the **conclusion** or **consequent**.

We assume that *any valuation* makes the **empty premises** T.

We will write  $A \equiv B$  when  $A \models B$  and  $B \models A$ . This is called **semantic equivalence**.

Q: show that  $p \rightarrow q \models \neg q \rightarrow \neg p$

Q: show that  $\neg(p \wedge q) \equiv \neg p \vee \neg q$  and  $\neg(p \vee q) \equiv \neg p \wedge \neg q$  (De Morgan laws)

Q: show that  $A \rightarrow B \equiv \neg A \vee B$

Explain the following

**Lemma**

*A is valid if and only if  $\models A$ .*

**Lemma**

*A is invalid if and only if  $\models \neg A$ .*

We will write<sup>1</sup>

*(something) iff (something else)*

To mean

If *(something)* is true **then** *(something else)* is true, **and**  
If *(something else)* is true **then** *(something)* is true

---

<sup>1</sup>We are using a meta-logic to state and prove our lemmas about Propositional Logic. Leibniz would not approve! But we have no other choice...

Prove the following using the semantics

**Lemma**

$\models A \rightarrow B$  iff  $A \models B$ .

**Lemma**

$A_1 \wedge A_2 \models B$  iff  $A_1, A_2 \models B$ .

**Lemma**

$A \models B_1 \vee B_2$  iff  $A \models B_1$  or  $A \models B_2$ .

## INDIRECT PROOFS OF SEMANTIC ENTAILMENT

Example: check if the following holds:

$$(p \rightarrow (q \vee r)) , (q \rightarrow r) , p \models \neg r \rightarrow s$$

There are **4 atomic propositions**. How many lines in the truth table?

## INDIRECT PROOFS OF SEMANTIC ENTAILMENT

Example: check if the following holds:

$$(p \rightarrow (q \vee r)) , (q \rightarrow r) , p \models \neg r \rightarrow s$$

There are **4 atomic propositions**. How many lines in the truth table?

$$2^4 = 16 \text{ lines!}$$

In general, the truth table necessary for checking  $A_1, \dots, A_n \models B$  has  $2^N$  lines, where  $N$  is the number of atomic propositions.

→ Brute force algorithm for checking validity is exponential.

# INDIRECT PROOFS OF SEMANTIC ENTAILMENT

Example: check if the following holds:

$$(p \rightarrow (q \vee r)) , (q \rightarrow r) , p \models \neg r \rightarrow s$$

There are **4 atomic propositions**. How many lines in the truth table?

$$2^4 = 16 \text{ lines!}$$

In general, the truth table necessary for checking  $A_1, \dots, A_n \models B$  has  $2^N$  lines, where  $N$  is the number of atomic propositions.

→ **Brute force algorithm for checking validity is exponential.**

We can do better!

## INDIRECT PROOFS OF SEMANTIC ENTAILMENT

Indirect proof:

1. assume entailment is falsifiable
2. check if that's possible

Falsifiable iff there is a valuation making **all premises** T and the conclusion F.

Example: check if the following entailment holds:

$$(p \rightarrow (q \vee r)) , (q \rightarrow s) , p \models \neg r \rightarrow s$$



# INDIRECT PROOFS OF SEMANTIC ENTAILMENT

Indirect proof:

1. assume entailment is falsifiable
2. check if that's possible

Falsifiable iff there is a valuation making **all premises T** and the conclusion **F**.

- Put a **T** under the **main operator** (remember syntax trees?) of each premise and a **F** under the main operator of the conclusion
- Propagate the truth values.
- Duplicate lines when multiple choices exist.

Example: check if the following entailment holds:

$$(p \xrightarrow{\text{T}} (q \vee r)) , (q \xrightarrow{\text{T}} s) , p \xrightarrow{\text{T}} \neg r \xrightarrow{\text{F}} s$$

# INDIRECT PROOFS OF SEMANTIC ENTAILMENT

Indirect proof:

1. assume entailment is falsifiable
2. check if that's possible

Falsifiable iff there is a valuation making **all premises T** and the conclusion **F**.

- Put a **T** under the **main operator** (remember syntax trees?) of each premise and a **F** under the main operator of the conclusion
- Propagate the truth values.
- Duplicate lines when multiple choices exist.

Example: check if the following entailment holds:

$(p \rightarrow (q \vee r)) , (q \rightarrow s) , p \models \neg r \rightarrow s$

T	T	T	F	T	F	T	T	F	F	F
---	---	---	---	---	---	---	---	---	---	---

# INDIRECT PROOFS OF SEMANTIC ENTAILMENT

Indirect proof:

1. assume entailment is falsifiable
2. check if that's possible

Falsifiable iff there is a valuation making **all premises T** and the conclusion **F**.

- Put a **T** under the **main operator** (remember syntax trees?) of each premise and a **F** under the main operator of the conclusion
- Propagate the truth values.
- Duplicate lines when multiple choices exist.

Example: check if the following entailment holds:

$$(p \rightarrow (q \vee r)) , (q \rightarrow s) , p \models \neg r \rightarrow s$$

T   T   **T**   T   F        **F**   T   F        T        T   F   F   F

**Contradiction:**  $q$  has to be both T and F. Therefore the above is not falsifiable. Therefore the entailment holds.

Check the following:

$$(\neg p \rightarrow q) , (q \rightarrow p) , (p \rightarrow \neg q) \models p \wedge \neg q$$

Check the following:

$$(\neg p \underset{\text{T}}{\rightarrow} q) , (q \underset{\text{T}}{\rightarrow} p) , (p \underset{\text{T}}{\rightarrow} \neg q) \models p \underset{\text{F}}{\wedge} \neg q$$

# INDIRECT PROOFS OF SEMANTIC ENTAILMENT

Check the following:

$(\neg p \rightarrow q)$	,	$(q \rightarrow p)$	,	$(p \rightarrow \neg q)$	$\models$	$p \wedge \neg q$
F T		T F		F T		F F T
T T		T T		T T		T F F
F T		T F		F T		F F F

# INDIRECT PROOFS OF SEMANTIC ENTAILMENT

Check the following:

$(\neg p \rightarrow q)$	,	$(q \rightarrow p)$	,	$(p \rightarrow \neg q)$	$\models$	$p \wedge \neg q$
T F T <b>T</b>		T F		F T		F F T <b>F</b>
F T T		T T		T T T <b>F</b>		T F F <b>T</b>
T F T		<b>F</b> T F		F T		F F F <b>T</b>

**Contradiction in all cases** ( $q$  must have both T and F value).  
Therefore not falsifiable. Therefore valid!

Check whether the following are valid:

1.  $p \rightarrow q \rightarrow r \models p \rightarrow r \rightarrow q$
2.  $p \rightarrow q \rightarrow r \models q \rightarrow p \rightarrow r$
3.  $((p \rightarrow q) \rightarrow s), (r \rightarrow q), p \models q \wedge (r \rightarrow s)$