CSU44004/CSU55004: FORMAL VERIFICATION

Lecture 4: Propositional Logic

Vasileios Koutavas

School of Computer Science and Statistics
Trinity College Dublin

RECAP

- Propositional logic formulas are syntax:

$$A ::= p \mid (\neg A) \mid (A \wedge A) \mid (A \vee A) \mid (A \to A)$$

- A valuation/model of A is an assignment of T or F to *(at least)* the atomic propositions in A.
- Given a model $\mathcal{M}$ of A, the semantics of A for this model is either T or F
  - "$\mathcal{M}$ makes A T (or F)"
  - we construct the truth table of A to see which one it is
  - A can be satisfiable/falsifiable/valid/invalid
- Semantic entailment: $A_1, \ldots, A_n \models B$ is the statement
  - Any model $\mathcal{M}$ making all A_i $(1 \leq i \leq n)$ T, also makes B T.

SEMANTIC ENTAILMENT

To check whether the following is a correct entailment

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

we need to construct and check 16 lines in a truth table ($2^{\#\text{atomic propositions}}$).

→ **Brute force algorithm for checking semantic entailment is exponential to the number of atomic propositions.**

SEMANTIC ENTAILMENT

To check whether the following is a correct entailment

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

we need to construct and check 16 lines in a truth table ($2^{\#\text{atomic propositions}}$).

- → **Brute force algorithm for checking semantic entailment is exponential to the number of atomic propositions**.
- → an indirect proof can be quicker.

INDIRECT PROOFS OF SEMANTIC ENTAILMENT

Indirect proof:

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

Incorrect iff there is a model 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 **incorrect**
2. check if that's possible

Incorrect iff there is a model 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:

$$\begin{array}{ccccccccccccccc} (p & \rightarrow & (q & \vee & r)) & , & (q & \rightarrow & s) & , & p & \models & \neg & r & \rightarrow & s \\ & \mathsf{T} & & & & & & & & & & & & \mathsf{F} & \end{array}$$

INDIRECT PROOFS OF SEMANTIC ENTAILMENT

Indirect proof:

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

Incorrect iff there is a model 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 **incorrect**
2. check if that's possible

Incorrect iff there is a model 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.

INDIRECT PROOFS OF SEMANTIC ENTAILMENT

Check the following:

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

INDIRECT PROOFS OF SEMANTIC ENTAILMENT

Check the following:

$$\begin{array}{cccccccccccccccc} (\neg p & \rightarrow & q) & , & (q & \rightarrow & p) & , & (p & \rightarrow & \neg q) & \models & p & \wedge & \neg q \\ & \mathsf{T} & & & & \mathsf{T} & & & & \mathsf{T} & & & & \mathsf{F} & \end{array}$$

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

propagation of F inside the subformulas of $p \wedge \neg q$ gives us 3 possible ways to falsify the statement.

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	T			T	F		F	T			F	F	T F
F	T	T				T	T		T	T	T F		T	F	F T
T	F	T			F	T	F		F	T			F	F	F T

Contradiction in all possible assignments (q must have both T and F value). Therefore not falisfiable. Therefore valid!

INDIRECT PROOFS OF SEMANTIC ENTAILMENT

Check whether the following are valid:

1. $p \to q \to r \models p \to r \to q$
2. $p \to q \to r \models q \to p \to r$
3. $((p \to q) \to s), (r \to q), p \models q \land (r \to s)$

Syntactic logical proofs

THREE DIFFERENT ENTAILMENTS (IMPLICATIONS)

- $\rightarrow$ $A \rightarrow B$
  This is **merely syntax**, although we have assigned a meaning to this syntax via sem($A \rightarrow B$).

Three different entailments (implications)

→ $A \to B$
This is **merely syntax**, although we have assigned a meaning to this syntax via sem($A \to B$).

→ $A_1 \ldots A_n \models B$
"Any model $\mathcal{M}$ making all A_i T, also makes B T"
"$A_1 \ldots A_n$ model B"
We can show as a lemma that $\models A \to B$ iff $A \models B$.

THREE DIFFERENT ENTAILMENTS (IMPLICATIONS)

→ $A \rightarrow B$
This is **merely syntax**, although we have assigned a meaning to this syntax via sem($A \rightarrow B$).

→ $A_1 \ldots A_n \models B$
"Any model $\mathcal{M}$ making all A_i T, also makes B T"
"$A_1 \ldots A_n$ model B"
We can show as a lemma that $\models A \rightarrow B$ iff $A \models B$.

one more:

→ $A_1 \ldots A_n \vdash B$
"from $A_1 \ldots A_n$ we can syntactically prove B"
"$A_1 \ldots A_n$ proves B"
i.e., there is a way to start from the formulas $A_1 \ldots A_n$ and derive B using the inference rules of propositional logic (stay tuned)

Inference rules are essentially axioms of the form:

Axiom (stucture of an inference rule)
If we have formulas $A_1 \ldots A_n$ then we can derive formula B.

Inference rules are essentially axioms of the form:

Axiom (stucture of an inference rule)
If we have formulas $A_1 \dots A_n$ then we can derive formula B.

Examples:

Axiom ($\wedge i$)
If we have any formulas A_1 and A_2 then we can derive the formula $A_1 \wedge A_2$

Axiom ($\wedge e_1$)
If we have formula $A_1 \wedge A_2$ then we can derive the formula A_1

Axiom ($\wedge e_2$)
If we have formula $A_1 \wedge A_2$ then we can derive the formula A_2

NATURAL DEDUCTION

There is a standard calculus for axioms of this form called Natural Deduction

Structure of inference axioms:

$$\frac{A_1 \qquad \ldots \qquad A_n}{B}\ \text{RULE NAME}$$

NATURAL DEDUCTION

There is a standard calculus for axioms of this form called Natural Deduction

Structure of inference axioms:

$$\frac{A_1 \qquad \ldots \qquad A_n}{B}\ \text{RULE NAME}$$

Examples:

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

NATURAL DEDUCTION

There is a standard calculus for axioms of this form called Natural Deduction

Structure of inference axioms:

$$\frac{A_1 \qquad \ldots \qquad A_n}{B}\ \text{RULE NAME}$$

Examples:

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

- → variables (As) in these rules can "pattern-match" to arbitrary formulas
- → constructors ($\wedge, \vee, \rightarrow, \neg$) can only "pattern-match" the same constructors

NATURAL DEDUCTION PROOFS

Suppose we need to prove $p \wedge q,\ r \vdash q \wedge r$.

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

Suppose we need to prove $p \wedge q,\ r \vdash q \wedge r$.

Proof.

1	$p \wedge q$	premise
2	r	premise
3	q	$\wedge e_2$ 1
4	$q \wedge r$	$\wedge i$ 3, 2

□

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

Suppose we need to prove $p \wedge q,\ r \vdash q \wedge r$.

Proof.

1	$p \wedge q$	premise
2	r	premise
3	q	$\wedge e_2$ 1
4	$q \wedge r$	$\wedge i$ 3, 2

□

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

Similar to calculus or to constructing a syntax-transforming program

NATURAL DEDUCTION PROOFS

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

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

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

Proof.

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

□

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