CL 2002:

Computational Logic

(*Lecture 2*)

Sergei N. Artemov

`September 10, 2002`

Computer Science Program
CUNY Graduate Center

This lecture plan

1. Truth tables and tautologies

2. Hilbert style systems, completeness of the classical propositional logic.

3. Brouwer-Heyting-Kolmogorov semantics – ”truth tables” for intuitionistic logic.

4. Heyting proof systems, deduction theorem.

5. Possible world semantics, soundness. Monotonicity principle.

6. Soundness and completeness w.r.t. Kripke semantics.

7. Properties of **Int**.

Propositional formulas

Language: connectives $\wedge, \vee, \rightarrow$, boolean constant $\bot$ (for *falsum*), variables $p_0, p_1, p_2, \ldots$.

Formulas (inductive definition):
1. $\bot$ and $p_0, p_1, p_2, \ldots$ are formulas
2. If A, B are formulas then $(A \wedge B)$, $(A \vee B)$,$(A \rightarrow B)$ are formulas.

Defined connectives: $\neg A$ is $A \rightarrow \bot$, $A \leftrightarrow B$ is $(A \rightarrow B) \wedge (B \rightarrow A)$, $\top$ is $\bot \rightarrow \bot$.

Excessive), (are omitted using the following precedence convention: $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$. For example, $A \wedge B \rightarrow \neg C \vee D \wedge A$ should be read as $(A \wedge B) \rightarrow ((\neg C) \vee (D \wedge A))$. Similar connectives are right associative: $A \rightarrow B \rightarrow C$ means $A \rightarrow (B \rightarrow C)$.

Classical truth tables. We postulate two truth values `true` and `false` (a.k.a. 1 and 0) and assume the following tables:

- $\bot$ is always false
- $A \wedge B$ is true iff A is true *and* B is true
- $A \vee B$ is true iff A is true *or* B is true
- $A \rightarrow B$ is true iff B is true *or* A is false ("material implication")

The (defined) truth tables:

- $\neg A$ is true iff A is false
- $\top$ is true
- $A \leftrightarrow B$ is true iff ...

Inductive definition of truth values of a compound formula given truth values of atomic formulas, not a definition of connectives!

A given formula F is a *tautology* iff F is true under all interpretations. F is *satisfiable* is F is true under at least one interpretation. An interpretation which makes F true is called a *model* of F.

Lemma F is a tautology iff $\neg F$ is not satisfiable

Detecting a tautology and finding a satisfying interpretation are dual approaches to the same problem.

Proof Systems are algorithms that generate tautologies. A *sound* proof system generates only tautology. A *complete* proof system generates all of them.

Components of Hilbert style proof systems

Axioms is a designated set of formulas.

Rules of inference are designated rules having format

$$\frac{A_1, A_2, \ldots, A_n}{C}$$

where $A_1, A_2, \ldots, A_n$ are called *premises* (*antecedent*) and C the conclusion (*succedent*) of that rule.

Theorems are generated from axioms by the rules of inference.

Hilbert proof systems have many axioms and minimal set of rules. They are good for specification purposes, but are not very proof friendly. Here we consider a typical Hilbert proof system.

Propositional axioms of classical logic **Cl**

1. $A \to (B \to A)$
2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$
3. $A \wedge B \to A$
4. $A \wedge B \to B$
5. $A \to (B \to (A \wedge B))$
6. $A \to (A \vee B)$
7. $B \to (A \vee B)$
8. $(A \to C) \to ((B \to C) \to (A \vee B \to C))$
9. $\bot \to A$
10. $\neg\neg A \to A$

Rule of inference: *Modus Ponens (MP)*

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

Example of a derivation (a formal proof)

1. $(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A))$ (axiom 2)
2. $A \to ((A \to A) \to A)$ (axiom 1)
3. $(A \to (A \to A)) \to (A \to A)$ (from 1., 2., by MP)
4. $A \to (A \to A)$ (axiom 1)
5. $A \to A$ (from 3. and 4., by MP)

What an effort to establish such a trivial fact! Are all formal proof systems that bad? Fortunately, it is not the case. There are very efficient and natural proof systems at our disposal.

Notation: $\vdash F$ denotes F *is derivable*, i.e. there is a formal derivation of F in a given proof system.

Derivations from hypotheses

Let Γ be a set of formulas. By $\Gamma \vdash F$ we denote the fact that F can be derived from hypotheses Γ. Note that here formulas from Γ are not necessarily tautologies!. This is a formalization of *hypothetical reasoning* when an agent makes assumptions "for the sake of argument" without insisting on its validity.

Example of a derivation from hypotheses $A \to B,\ B \to C\ \vdash A \to C$

1. $A \to B$ (a hypothesis)
2. $B \to C$ (a hypothesis)
3. $(B \to C) \to (A \to (B \to C))$ (axiom 1)
4. $A \to (B \to C)$ (from 2 and 3, by MP)
5. $(A \to B) \to ((A \to (B \to C)) \to (A \to C))$ (axiom 2)
6. $(A \to (B \to C)) \to (A \to C)$ (from 1 and 5, by MP)
7. $A \to C$ (from 4 and 6, by MP)

Soundness of formal proofs

Theorem If $\vdash F$ then F is a tautology (i.e. F is true under any interpretation).

General Theorem If $\Gamma \vdash F$ then F is true in any model of Γ.

Proof. Let interpretation I be a model of Γ. Suppose also that there is a derivation of F from hypotheses Γ. Each sentence in such a derivation is either an axiom, or from Γ, or follows from some other formulas occurring in this derivation earlier. We claim that every sentence in the derivation is true under interpretation I. Indeed, a sentence from Γ is true under I, every axiom is also true under I since the axiom is a tautology (check it by yourself). The rule of inference Modus Ponens when applied to true premises $A \rightarrow B$, A produces B which is thus also true under I (truth tables for $\rightarrow$!)

Some additional rules and facts

Deduction Theorem (DT) $\Gamma, A \vdash B$ iff $\Gamma \vdash A \to B$.

Before we produce a proof of this theorem, let us try to use it. It improves the efficiency of derivations immensely.

1. $A \vdash A$ (by definition of derivations from hypotheses)
2. $\vdash A \to A$ (by DT)

1. $A \to B,\ B \to C,\ A \vdash C$ (MP twice)
2. $A \to B,\ B \to C \vdash A \to C$ (by DT, from 1)

More examples: de Morgan principle $(\neg A \vee \neg B) \leftrightarrow \neg(A \wedge B)$

1. $A, \neg A \vdash \bot$ (by MP, since $\neg A$ is $A \to \bot$)
2. $B, \neg B \vdash \bot$ (likewise)
3. $A, B, \neg A \vdash \bot$ (from 1)
4. $A, B, \neg B \vdash \bot$ (from 2)
5. $A \wedge B, \neg A \vdash \bot$ (given $A \wedge B$ derive A, B first)
6. $A \wedge B, \neg B \vdash \bot$ (likewise)
7. $A \wedge B, \neg A \vee \neg B \vdash \bot$ (by axiom 8)
8. $\neg A \vee \neg B \vdash (A \wedge B) \to \bot$ (by DT)
9. $\vdash (\neg A \vee \neg B) \to ((A \wedge B) \to \bot)$ (by DT)
10. $\vdash (\neg A \vee \neg B) \to \neg(A \wedge B)$ (1/2 of de Morgan)

Proof of the Deduction Theorem.

Direction "$\Gamma \vdash A \rightarrow B$ yields $\Gamma, A \vdash B$" is trivial, by MP.

We establish "$\Gamma, A \vdash B$ yields $\Gamma \vdash A \rightarrow B$" by induction on (the length of) a proof of B in Γ, A. There are four possible cases: 1) $B \in \Gamma$, 2) B is an axiom, 3) B is A, and 4) B follows from earlier sentences in this derivation by MP.

1. If $B \in \Gamma$, then $\Gamma \vdash A \rightarrow B$ since $\Gamma \vdash B$
2. If B is an axiom - likewise
3. If B is A, then $\Gamma \vdash A \rightarrow B$, since $\Gamma \vdash A \rightarrow A$

4. If B follows from earlier sentences $C \rightarrow B$ and C in this derivation by MP. By the induction hypothesis, $\Gamma \vdash A \rightarrow (C \rightarrow B)$ and $\Gamma \vdash A \rightarrow C$. Using axiom (2) $(A \rightarrow (C \rightarrow B)) \rightarrow ((A \rightarrow C) \rightarrow (A \rightarrow B))$ by MP twice, we get the desired $\Gamma \vdash A \rightarrow B$.

Note: the above induction provides an efficient algorithm transforming the proof $\Gamma, A \vdash B$ to a proof $\Gamma \vdash A \rightarrow B$

More rules

- $A, B \vdash A \wedge B$, by axiom 5 and DT
- $\bot \vdash B$. Easy, from axiom 9: $\bot \rightarrow B$, by MP.
- $A, \neg A \vdash B$. Indeed, $A, A \rightarrow \bot \vdash \bot$, by MP, $\bot \vdash B$, above, thus $A, A \rightarrow \bot \vdash B$
- $B \vee C, \neg B, \neg C \vdash \bot$. Read $\neg X$ as $X \rightarrow \bot$, use axiom $(B \rightarrow \bot) \rightarrow ((C \rightarrow \bot) \rightarrow (B \vee C \rightarrow \bot))$ and MP three times.

Intuitionism: constructive approach to mathematics and logic

Brouwer (1900s):

> "It does not make sense to think of truth or falsity of a mathematical statement independently of our knowledge concerning the statement. A statement is *true* if we have a proof of it, and *false* if we can show that the assumption that there is a proof for the statement leads to a contradiction."

Intended "truth tables" for intuitionistic logic (a.k.a. *BHK* conditions), an attempt to define implication

- a proof of $A \wedge B$ consists of a proof of A and a proof of B,
- a proof of $A \vee B$ is given by presenting either a proof of A or a proof of B,
- a proof of $A \rightarrow B$ is a construction which, given a proof of A returns a proof of B,
- absurdity $\perp$ is a proposition which has no proof, $\neg A$ is $A \rightarrow \perp$.

Uses unspecified notions of "proof" and "construction"!

Intuitionistic tautology = a formula which is provable regardless of the provability of its atoms: $A \rightarrow A$, $A \wedge B \rightarrow A$, $A \rightarrow A \vee B$, $A \rightarrow \neg\neg A$, etc. Heyting (1931): an axiom system **Int** for propositional intuitionistic logic on basis of this vague intuition only: skip the double negation principle (axiom 10).

Propositional axioms of classical logic **Cl**

1. $A \to (B \to A)$
2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$
3. $A \wedge B \to A$
4. $A \wedge B \to B$
5. $A \to (B \to (A \wedge B))$
6. $A \to (A \vee B)$
7. $B \to (A \vee B)$
8. $(A \to C) \to ((B \to C) \to (A \vee B \to C))$
9. $\bot \to A$
10. $\neg\neg A \to A$

Rule of inference: *Modus Ponens (MP)*

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

Propositional axioms of classical logic **Int**

1. $A \to (B \to A)$
2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$
3. $A \wedge B \to A$
4. $A \wedge B \to B$
5. $A \to (B \to (A \wedge B))$
6. $A \to (A \vee B)$
7. $B \to (A \vee B)$
8. $(A \to C) \to ((B \to C) \to (A \vee B \to C))$
9. $\bot \to A$

Rule of inference: *Modus Ponens (MP)*

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

What is left? Proof theoretically: Deduction Theorem survives, as does every fact which is independent of axiom 10.

Int gives some positive test of the desired ”constructive” meaning. Completeness issue cannot be even stated properly before semantics is made rigid.

Two artificial but very useful semantics, each living its own life now:

1. Topological semantics (Stone, 1937; Tarski, 1938)
2. Possible worlds semantics (Kripke, 1965).

Int is known to be complete with respect to each of them!

Topological semantics

Universe is a topological space T (think real space $\mathbf{R}^n$). Propositional letters are evaluated by open subsets of T. Each formula F is thus assigned an open subset $t(F)$ of T according to the inductive rule: $t(\bot) = \emptyset$, $t(A \wedge B) = t(A) \cap t(B)$, $t(A \vee B) = t(A) \cup t(B)$, $t(A \rightarrow B)$ is *interior* $(\overline{t(A)} \cup t(B))$ (here $\overline{X}$ denotes the complement of X). In particular, $t(\neg A)$ is *interior* $(\overline{t(A)})$.

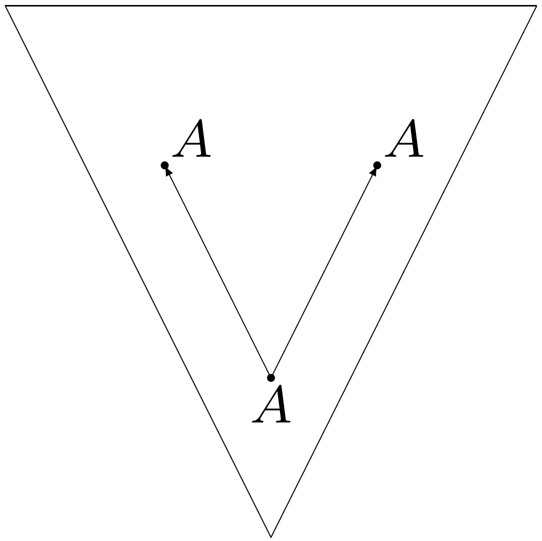
A tautology is a formula which is always evaluated T regardless to an evaluation of its atoms. Examples:

$t(A \rightarrow A) =$ *interior* $(\overline{t(A)} \cup t(A)) =$ *interior*$(\mathrm{T}) = \mathrm{T}$.

$t(\neg A \vee A) = \{$*interior* $(\overline{t(A)})\} \cup t(A)$ which not necessarily equals T: take T=$\mathbf{R}$, $t(A) = (0, 1)$. Then $t(\neg A \vee A) = \mathbf{R} - \{0, 1\}$, i.e. a line without two points. Thus $\neg A \vee A$ is not an intuitionistic tautology.

Possible Worlds Semantics by Saul Kripke.

Classical logic, propositional and quantified alike, gives a static picture of the world. A classical interpretation (model) is an assignment of truth values to atoms of the language. Intuitionistic logic can be explained on the basis of the idea of "possible worlds" which can be traced back to Leibniz. The possible worlds universe consists of a collection of classical models W connected by a binary accessibility relation $a \preceq b$ "world b is accessible from world a". In other worlds, the possible worlds constitute a graph, not necessarily finite. Whereas classical connectives operate within individual worlds (i.e. nodes in W), intuitionstic connectives reach out to all the worlds accessible from a given one (possible worlds).



Intuitionistic Kripke model is a triple $K = (W, \preceq, \models)$, where W is a nonempty set (elements of which are called "possible worlds"), $\preceq$ a partial order on W (in particular, reflexive, transitive), and $\models$ a monotone truth assignment having form: "world$\models$formula" such that each propositional letter p gets some truth value in any world from W respecting the *monotonicity* property: if $x \models p$ and $x \preceq y$ then $y \models p$.

The definition of $x \models F$ (read as *a formula* F *is true in a world* x, or x *forces* F) goes by induction on F: $x \not\models \bot$

$x \models A \wedge B$ iff "$x \models A$ and $x \models B$"

$x \models A \vee B$ iff "$x \models A$ or $x \models B$"

$x \models A \rightarrow B$ iff "$y \models B$ or $y \not\models A$" for all y such that $x \preceq y$

(i.e. if $x \models A \rightarrow B$ holds classically in all accessible worlds).

As in the case of the topological semantics, connectives $\wedge, \vee$ behave like in the usual classical semantics in any given world, whereas $\rightarrow$ (and thus $\neg$) refer to all the worlds accessible from a given one.

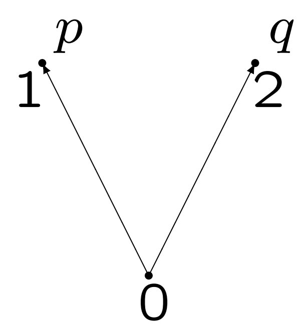
The important feature of Kripke models for **Int** is the monotonicity property of truth assignments:
for any formula F if $x \models F$ and $x \preceq y$ then $y \models F$.

Proof: an easy induction on the complexity of F.

Example

Consider a three-element "V-shaped" model with $W = \{0, 1, 2\}$ given by an oriented graph below. According to this graph, $0 \preceq 1$, $0 \preceq 2$, and neither of $1 \preceq 2$, $2 \preceq 1$, $1 \preceq 0$, $\ldots$ holds.

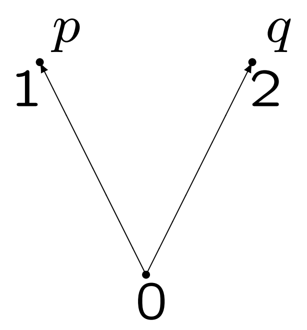
Notational convention: we label the nodes with propositional variables true at a given node. By default, all variables not listed next to a node are assumed false at this node. In particular, $1 \models p$, $2 \models q$, $1 \not\models q$, $2 \not\models p$, $0 \not\models p$, $0 \not\models q$, and all other variables are false at all nodes.



Question: for each of the formulas $p \wedge q$, $p \vee q$, $p \rightarrow q$, $\neg p$, list the nodes where this formula is true.

Answer:

Formula $p \wedge q$ is false at every node. Formula $p \vee q$ is true at 1 and 2, but not at 0. Formula $p \rightarrow q$) is true at 2 and false at 1 (by the usual truth tables). It is false at 0, since it is false at 1, which is accessible from 0. Formula $\neg p$ is false at 1, since $1 \models p$.



On the other hand, $\neg p$ is true at 2, since 2 is the only node accessible from 2 and p is false there. Finally, $\neg p$ is false at 0 since p holds at 1 which is accessible from 0.

Note, that $0 \not\models p$ and $0 \not\models \neg p$!. Hence a classical property that either formula F or its negation $\neg F$ holds at every given world fails: there is the third possibility when neither of those formulas holds. This third option corresponds to the information state when an agent does not have evidences of F neither evidences of $\neg F$.

Definition. A formula F is true in a model K (notation: $K \models F$) if F holds at every node of K. A formula F is valid (in a given class of models) if it is true in every model (of this class).

Soundness Theorem

If **Int** $\vdash F$ then F is valid in all intuitionistic Kripke models.

Proof. A pretty straightforward induction on the length of derivation in a given logic. We first prove that axioms are true in every model. Then we check that rules when applied to formulas true in all models (of a given class) produce a formula true in every such model as well.

To show that $\neg\neg p \rightarrow p$ is not derivable in **Int**, it now suffices to build a countermodel $K = (W, \preceq, \models)$ for this formula. Consider $W = \{0, 1\}$ with $0 \preceq 0$, $0 \preceq 1$, $1 \preceq 1$. Put $0 \not\models p$ and $1 \models p$. Clearly, K is a legitimate **Int** model.

Moreover, $1 \not\models \neg p$, since p holds at 1. Likewise, $0 \not\models \neg p$, since p holds at 1 which is accessible from 0. Therefore $0 \models \neg\neg p$. Since $0 \not\models p$, $0 \not\models \neg\neg p \rightarrow p$.

Exercise: find an intuitionistic countermodel for $\neg p \vee p$.

Completeness Theorem

For intuitionistic logic **Int**
$\vdash F$ iff F is valid in all models.

Completeness Theorem (general form)

For intuitionistic logic **Int**
$\Gamma \vdash F$ iff F is valid in all models of Γ.

The proof of the completeness will be given next time when we will learn more about advanced proof systems for **Int**.

Exercises.

1. Establish the disjunctive property of **Int**:

$$\vdash A \lor B \text{ yields } \vdash A \text{ or } \vdash B.$$

Note that such a property fails for the classical logic where $p \lor \neg p$ is provable, but neither of p nor $\neg p$ is.

2. Show that **Int** is NOT a three valued logic.

Hint: note, that the fact that **Cl** is two valued is reflected by the fact that $(p \leftrightarrow q) \lor (q \leftrightarrow r) \lor (p \leftrightarrow r)$ is a tautology, and thus a theorem of **Cl**). The natural meaning of this formula is that for any three propositions p, q, r at least two of them are equivalent (have the same truth value). In other words, there are no three different truth values to pairwise distinguish three propositions. A natural formal representation of a three valued property of **Int** would be the provability of formula $(p \leftrightarrow q) \lor (q \leftrightarrow r) \lor \ldots \lor (p \leftrightarrow s)$ (for all six pairs of p, q, r, s). Show now that the latter formula is not provable in **Int**.

3. Glivenko's Theorem (embedding the classical logic into **Int**): **Cl**$\vdash A$ iff **Int**$\vdash \neg\neg A$.

In what sense is this an embedding? In the most natural algorithmic sense: given an oracle (a test, if you wish) for **Int** we will get an oracle for **Cl**. The moral here is that intuitionistic logic emulates the classical one (but not the other way around. It takes more than **Cl** to capture **Int**).