Estonian Winter School in Computer Science, 2004

Proof Polynomilas

"For it is far better to know something about everything than to know all about one thing. This universality is the best."

Blaise Pascal, *Penses*

(*Lectures 1-2*)

Sergei Artemov
Graduate Center of the City University of New York

Reading

1. D. van Dalen, *Logic and Structure*, Springer-Verlag, third-fourth edition.

2. A. Troelstra & H. Schwichtenberg, *Basic Proof Theory*, Cambridge University Press, 1996.

3. J.-Y. Girard, Y. Lafont & P. Taylor, *Proofs and Types*, Cambridge University Press, Cambridge 1989.

4. S. Artemov, "Explicit provability and constructive semantics", *Bulletin of Symbolic Logic*, volume 7, No.1, pp. 1-36, 2001

TIME100 project: "The greatest scientists of the century" (20 positions):

- Technology - 6 (airplane, rocket, TV, transistor, plastic, WWW)
- Biology & Medicine - 4 (psychoanalysis, penicillin, DNA, polio)
- Physics & Astronomy - 3 (Einstein, Fermi, Hubble)
- Anthropology - 1 (The Leakeys)
- Economy - 1 (Keynes)

bullet Environment - 1 (Rachel Carson)

- Psychology - 1 (Piaget)

- Computer Science - 1 (Turing, a logician)
- Mathematics - 1 (Gödel, a logician)
- Philosophy - 1 (Wittgenstein, who began as a logician)

Three traditions in Logic

1. *Classical*: Frege, Hilbert, Gödel, Tarski

2. *Constructive*: Brouwer, Heyting, Kolmogorov, Gödel

3. *Explicit*: Skolem, Curry, Gödel, Church – *bridge to computing!*

Fundamental results in Logic make their way from foundational topics to real applications within one lifetime

Propositional Logic: *consistent, decidable, not feasible (if $P \neq NP$). Many practical methods reduce to this level*

Boole (1854), Post (1920): boolean circuits, boolean values in programming, duality of proof search and model checking

Gentzen (1933): normalization of proofs basis for "all" modern provers, proof checkers

Downside: limited expressive power!

First order logic: *one sort of objects, quantifiers* $\forall$, $\exists$. *Consistent, undecidable but recursively enumerable, formalizes all "usual" mathematical reasoning. First order theories are typically not categorical. Formal arithmetic, set theory, theory of reals, theory of groups, rings, fields, etc. can be presented as FO theories.*

Frege (1879): proofs in first order systems as positive tests of validness

Downside: not "object oriented" ", no direct representation of dynamic features (time, actions, etc.) hence excessive coding, computationally unfriendly! Another trouble: $\exists$-sickness (later).

Higher order logic: *Higher sorts of quantified variables. "Very" undecidable, not axiomatizable, not compact. HO theories: second order arithmetic (analysis), type theories. Close to the natural language, widely used for proof checking in verification.*

Milner (late '70s): Edinburgh LCF prover
Andrews (1982): classical HOL prover
etc.

Downside: No efficient proof search, no complete proof systems possible, difficulties with semantics and consistency.

Intuitionism: constructive approach to mathematics

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."

Constructive semantics problem

BHK problem: find the intended provability semantics of intuitionistic logic satisfying *BHK* conditions:

- 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 $A \to B$ is a construction which, given a proof of A returns a proof of B,
- absurdity $\bot$ is a proposition which has no proof, $\neg A$ is $A \to \bot$.

Crucial for understanding connections between computations and derivations!

Major models for intuitionistic logic

1. Algebraic semantics (Birkhoff, 1935)
2. Topological semantics (Stone, 1937; Tarski, 1938)
3. Realizability semantics (Kleene, 1945)
4. Beth models (1956)
5. Dialectica Interpretation (Gödel, 1958)
6. Curry - Howard isomorphism (1958)
7. Medvedev's logic of problems (1962)
8. Kripke models (1965)
9. Kuznetsov-Muravitsky-Goldblatt provability interpretation (1976)
10. Categorical semantics (Goldblatt, 1979)

None captures the original **BHK**-semantics!

Intuitionistic system = classical system + effective $\vee$ *and* $\exists$*.*

Existential property of intuitionistic systems:
a constructive proof of $\forall x \exists y A(x, y)$ *yields computable term (program)* $f(x)$ *such that* $\forall x A(x, f(x))$ *holds.*

Corollary: *intuitionistic correctness proof = program + correctness proof = verified program*

Downside: produces correct but computationally not optimal programs

Explicit tradition: Functions vs. Quantifiers:

Skolem (1920), Herbrand (1930), Gödel (1930):

quantifiers $\forall$, $\exists$ *are ghosts of functions, a precursor to automated reasoning!*:

logic	explicit logic
$\forall x \exists y A(x,y)$	$A(x, f(x))$
$\exists x A(x) \rightarrow \exists y B(y)$	$A(x) \rightarrow B(f(x))$

By its nature the closest to Computer Science. Addresses the right set of questions: whether $f(x)$ is computable, feasible, etc.

Downside: Too many Skolem functions, unification problems.

Shönfinkel (1924), Church (1929, 1930):

λ-calculus = universal functional language, foundational motivations.

Normal form = the result of a computation,

normalization process = computation

McCarthy (1960): λ-calculus implemented in *LISP*,

universal machine = *LISP*-compiler in *LISP*.

Functional programming languages.

Curry (1934), Howard (1969):

typed λ-calculus, implemented in ML

$t{:}F$ $\sim$ *term* t *has type* F $\sim$ t *is a proof of the proposition* F

proofs $\sim$ *functional programs*

assumptions $\sim$ *initial data*

deduction $\sim$ *execution sequence*

Girard (1971): Higher order λ-calculus, yields the consistency of the second order arithmetic, is implemented in the prover *Coq* and *Lego*

Martin-Löf (1982): type theory with intuitionistic logic, is implemented in *NuPRL*, *MetaPRL* and *Alf* provers.

Constructive quantifiers = computable Skolem functions

Good news: *intuitionistic correctness proof =*
= program + correctness proof = verified program

Bad news: *the above scheme is not efficient. Too long detour:*
formal specs $S(x,y) \mapsto$ *constructive proof of* $\forall x \exists y S(x,y) \mapsto$
$\mapsto$ *computable Skolem function* $y = f(x)$

Compromise: *reverse engineering of proofs, write a proof of* $\forall x \exists y S(x,y)$ *targeting a specific algorithm* $y = f(x)$

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
- $A \to B$ 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 more 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. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$ (axiom 2)
6. $(A \to B) \to (A \to C)$ (from 4 and 5, by MP)
7. $A \to C$ (from 1 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 $A \to B$, A produces B which is thus also true under I (truth tables for $\to$)

Some additional rules and facts

Deduction Theorem (DT) $\quad \Gamma, A \vdash B$ 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 "$\Gamma \vdash A \to B$ yields $\Gamma, A \vdash B$" is trivial, by MP.

We establish "$\Gamma, A \vdash B$ yields $\Gamma \vdash A \to B$" 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 $\Gamma \vdash A \to B$ since $\Gamma \vdash B$
2. If B is an axiom - likewise
3. If B is A, then $\Gamma \vdash A \to B$, since $\Gamma \vdash A \to A$
4. If B follows from earlier sentences $C \to B$ and C in this derivation by MP. By the induction hypothesis, $\Gamma \vdash A \to (C \to B)$ and $\Gamma \vdash A \to C$. Using axiom (2) $(A \to (C \to B)) \to ((A \to C) \to (A \to B))$ by MP twice, we get the desired $\Gamma \vdash A \to B$.

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

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: 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 $A \to B$ is a construction which, given a proof of A returns a proof of B,
- absurdity $\bot$ is a proposition which has no proof, $\neg A$ is $A \to \bot$.

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

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

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:

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!

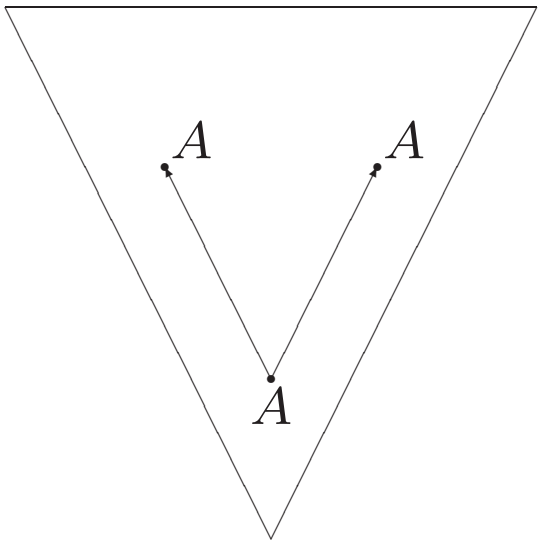
Topological semantics

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: $t(\bot) = \emptyset$, $t(A \wedge B) = t(A) \cap t(B)$, $t(A \vee B) = t(A) \cup t(B)$, $t(A \to B)$ 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:
$t(A \to A)$= *interior* $(\overline{t(A)} \cup t(A))$ = *interior*(T) = 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 $x \models B$"

$x \models A \to B$ iff "$y \models B$ or $y \not\models A$" for all y such that $x \preceq y$ (i.e. if $x \models A \to B$ 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.

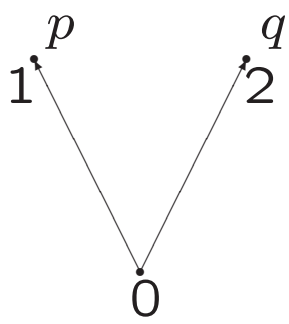
The important feature of Kripke models for **Int** is the monotonicity property of truth assignments:
for any formula F if $x \models F$ and $x \preceq y$ then $y \models F$.

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 $1 \preceq 2$, $2 \preceq 1$, $1 \preceq 0$, ... holds.

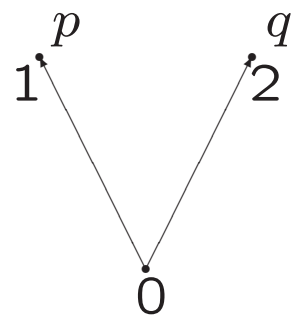
Notational convention: we label the nodes with propositional variables true at a given node. By default, all variables not listed next to a node are assumed false at this node. In particular, $1 \models p$, $2 \models q$, $1 \not\models q$, $2 \not\models p$, $0 \not\models p$, $0 \not\models q$, and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



Question: for each of the formulas $p \wedge q$, $p \vee q$, $p \to q$, $\neg p$, 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 $\mathbf{Int} \vdash F$ 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 $\neg\neg p \to p$ 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 $0 \not\models p$, $0 \not\models \neg\neg p \to p$.

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**.

Sequents. In a general setting a sequent is a figure $\Gamma \Rightarrow \Delta$, where Γ, Δ are finite multisets of formulas, i.e. the number of occurrences of a formula in a multiset counts, but not the order.

Example: $\{p, p, \bot, \bot, \bot, q, q, q\}$ and $\{p, \bot, q\}$ are equal as sets but different as multisets.

The idea behind an intuitionistic sequent (i.e. Gentzen style) calculus is that a sequent $\Gamma \Rightarrow F$ represents a derivation from hypothesis $\Gamma \vdash F$ in the traditional Hilbert style system. The case of empty Δ is covered by a convention: a sequent $\Gamma \Rightarrow$ represents a derivation from hypothesis $\Gamma \vdash \bot$.

Intuitionistis sequent is a sequent $\Gamma \Rightarrow \Delta$, where Δ contains not more than one formula (i.e. $|\Delta| \leq 1$).

Gentzen proof systems have few simple axioms and plenty of rules. They are not good for specification purposes, but are very proof friendly and constitute basis for practically all automated deduction systems. Right now we will introduce a Gentzen style system **IntG** for propositional intuitionistic logic. This system essentially coincides with **G1i** from "Basic Proof Theory".

Axioms: all sequents of form $A \Rightarrow A$ and $\bot \Rightarrow$. It even suffices to consider *atomic* axioms only, i.e. when A is a propositional variable.

Structural rules: weakening

$$\frac{\Gamma \Rightarrow \Delta}{A, \Gamma \Rightarrow \Delta}\ , \qquad \frac{\Gamma \Rightarrow}{\Gamma \Rightarrow A}$$

contraction

$$\frac{A, A, \Gamma \Rightarrow \Delta}{A, \Gamma \Rightarrow \Delta}$$

Logical rules:

$$\frac{A, \Gamma \Rightarrow \Delta}{A \wedge B, \Gamma \Rightarrow \Delta}\,(\wedge, \Rightarrow) \qquad \frac{B, \Gamma \Rightarrow \Delta}{A \wedge B, \Gamma \Rightarrow \Delta}\,(\wedge, \Rightarrow) \qquad \frac{\Gamma \Rightarrow A \qquad \Gamma \Rightarrow B}{\Gamma \Rightarrow A \wedge B}\,(\Rightarrow, \wedge)$$

$$\frac{\Gamma \Rightarrow A}{\Gamma \Rightarrow A \vee B}\,(\Rightarrow, \vee) \qquad \frac{\Gamma \Rightarrow B}{\Gamma \Rightarrow A \vee B}\,(\Rightarrow, \vee) \qquad \frac{A, \Gamma \Rightarrow \Delta \qquad B, \Gamma \Rightarrow \Delta}{A \vee B, \Gamma \Rightarrow \Delta}\,(\vee, \Rightarrow)$$

$$\frac{A, \Gamma \Rightarrow B}{\Gamma \Rightarrow A \to B}\,(\Rightarrow, \to) \qquad \frac{\Gamma \Rightarrow A \qquad B, \Gamma \Rightarrow \Delta}{A \to B, \Gamma \Rightarrow \Delta}\,(\to, \Rightarrow)$$

Cut rule

$$\frac{\Gamma \Rightarrow A \qquad A, \Gamma' \Rightarrow \Delta}{\Gamma, \Gamma' \Rightarrow \Delta}\,\text{Cut}$$

Some additional rules which can be derived in **IntG**

Negation

$$\frac{A, \Gamma \Rightarrow}{\Gamma \Rightarrow \neg A} \qquad \frac{\Gamma \Rightarrow A}{\neg A, \Gamma \Rightarrow}$$

Proof:

$$\dfrac{\dfrac{\dfrac{A, \Gamma \Rightarrow}{A, \Gamma \Rightarrow \bot}\ \text{weakening}}{\Gamma \Rightarrow A \to \bot}\ (\Rightarrow,\to)} \qquad \dfrac{\Gamma \Rightarrow A \qquad \dfrac{\dfrac{\bot \Rightarrow}{\bot, \Gamma \Rightarrow}\ \text{weakenings}}{A \to \bot, \Gamma \Rightarrow}}{}$$

Additive Cut

$$\frac{\Gamma \Rightarrow A \qquad A, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta}$$

Proof: exercise!

More examples: de Morgan principle in **IntG**

$$\dfrac{\dfrac{\dfrac{\dfrac{A \Rightarrow A}{A \wedge B \Rightarrow A}}{\neg A, A \wedge B \Rightarrow}}{\neg A \Rightarrow \neg(A \wedge B)} \qquad \dfrac{\dfrac{\dfrac{B \Rightarrow B}{A \wedge B \Rightarrow B}}{\neg B, A \wedge B}}{\neg B \Rightarrow \neg(A \wedge B)}}{\dfrac{(\neg A \vee \neg B) \Rightarrow \neg(A \wedge B)}{\Rightarrow (\neg A \vee \neg B) \rightarrow \neg(A \wedge B)}}$$

Other cases of de Morgan Laws: $(\neg A \wedge \neg B) \leftrightarrow \neg(A \vee B)$ – exercise.

Playing with negation: prove $A \to \neg\neg A$, $\neg\neg\neg A \to \neg A$

$$\dfrac{\dfrac{\dfrac{A \Rightarrow A}{A, \neg A \Rightarrow}}{A \Rightarrow \neg\neg A}}{\Rightarrow A \to \neg\neg A} \qquad \dfrac{\dfrac{\dfrac{\text{as before}}{A \Rightarrow \neg\neg A}}{\neg\neg\neg A, A \Rightarrow}}{\neg\neg\neg A \Rightarrow \neg A} \Rightarrow \neg\neg\neg A \Rightarrow \neg A$$

A failed attempt to prove $\neg\neg p \rightarrow p$

$$\dfrac{\dfrac{\dfrac{p \Rightarrow p}{\Rightarrow p, \neg p}}{\neg\neg p \Rightarrow p}}{\Rightarrow \neg\neg p \rightarrow p}$$

The sequent in red is not an intuitionistic one. The proof above is OK from the classical standpoint (classical sequents admit multiple formulas in Δ), but is not acceptable in **IntG**.

Exercises: Try and fail to prove $p \vee \neg p$ in **IntG**. Try and succeed in proving $\neg\neg(p \vee \neg p)$ in **IntG**.

Equivalence of **Int** and **IntG**

Theorem.
A sequent $\Gamma \Rightarrow F$ *is derivable in* **IntG** *if and only if* $\Gamma \vdash F$ *in* **Int**.

Proof. Induction on derivations in **IntG** and in **Int** respectively. Details were given in class, cf. also "BPT" (Basic Proof Theory book). Note that the rule Cut is needed to imitate the Modus Ponens Step in **IntG**.

Cut rule and automated proof search.

The rule Cut is the only one in **IntG** which violates the *subformula property*: each formula occurring in the premises of a given rule is a subformula of some formula in the concluding sequent. The subformula property is essential for backward search methods in automated proving. An stunning fact first discovered by Gentzen in the early 1930s is that the Cut rule can be eliminated from any classical and intuitionistic derivation. We will establish this important fact later.

Need of Cut? As we have noticed, a Cut Rule has been used in emulating Modus Ponens in **IntG**. On the other hand, observations demonstrate that Cuts can be eliminated from particular proofs in **IntG**.

$$\dfrac{\dfrac{A \Rightarrow A}{A \wedge B \Rightarrow A} \qquad \dfrac{A \Rightarrow A}{A \Rightarrow A \vee B}}{A \wedge B \Rightarrow A \vee B}\ \text{Cut}$$

$$\dfrac{\dfrac{A \Rightarrow A}{A \wedge B \Rightarrow A}}{A \wedge B \Rightarrow A \vee B}$$

No Cuts

Another example where Cut is present:

$$\dfrac{\dfrac{\dfrac{A \Rightarrow A}{A \Rightarrow A \vee B} \qquad \dfrac{C \Rightarrow C}{A, C \Rightarrow C}}{A \vee B \rightarrow C, A \Rightarrow C}}{A \vee B \rightarrow C \Rightarrow A \rightarrow C} \qquad \dfrac{\dfrac{A \Rightarrow A \qquad \dfrac{C \Rightarrow C}{A, C \Rightarrow C}}{A \rightarrow C, A \Rightarrow C}}{A \rightarrow C, A \wedge B \Rightarrow C}}{A \rightarrow C \Rightarrow A \wedge B \rightarrow C} \text{ Cut}$$

$$A \vee B \rightarrow C \Rightarrow A \wedge B \rightarrow C$$

but can be eliminated:

$$\dfrac{\dfrac{\dfrac{\dfrac{A \Rightarrow A}{A \Rightarrow A \vee B} \qquad \dfrac{C \Rightarrow C}{A, C \Rightarrow C}}{A \vee B \rightarrow C, A \Rightarrow C}}{A \vee B \rightarrow C, A \wedge B \Rightarrow C}}{A \vee B \rightarrow C \Rightarrow A \wedge B \rightarrow C}$$

No Cuts

Why would one need to eliminate Cuts? Here is a nice corollary of the Cut Elimination Theorem, much more are yet to come.

Disjunctive Property for intuitionistic logic

If **Int** $\vdash A \vee B$, *then* **Int** $\vdash A$ *or* **Int** $\vdash B$

Proof. Work in **IntG**. Suppose **IntG** proves $\Rightarrow A \vee B$ without Cuts. Consider the very last rule in this derivation. A direct inspection of rules of **IntG** leaves only three possibilities

$$\frac{\Rightarrow}{\Rightarrow A \vee B}\ \text{Weakening}, \qquad \frac{\Rightarrow A}{\Rightarrow A \vee B}\ (\Rightarrow, \vee), \qquad \frac{\Rightarrow B}{\Rightarrow A \vee B}\ (\Rightarrow, \vee),$$

first of which is impossible since the empty sequent $\Rightarrow$ is not derivable without Cut (answer, why).

Cut Elimination Theorem

Any proof in **IntG** *possibly containing Cuts can be reduces by a proper sequence of proof transformations to a Cut-free proof of the same sequent.*

Proof. Given in class, see also "Basic Proof Theory" book, Chapter 4.

Kripke Completeness Theorem for intuitionistic logic.

$$\Gamma \vdash F \quad \textit{iff} \quad \Gamma \models F$$

Proof. Soundness:

$$\textit{If } \Gamma \vdash F \quad \textit{then} \quad \Gamma \models F$$

has already been established in Lecture 2. Completeness:

$$\textit{If } \Gamma \models F \quad \textit{then} \quad \Gamma \vdash F$$

is an easy corollary of the following

Finite Model Property of **Int**:

If $\Gamma \not\vdash F$, *then there is a finite Kripke countermodel for* F.

Exercise 1. Suppose a derivation $\Gamma, A \vdash B$ has n lines, i.e. n steps each of which is either invoking and axiom or a hypothesis from Γ, invoking A, or using the rule Modus Ponens once. Give a reasonable upper bound of the number of steps in the derivation $\Gamma \vdash A \to B$ obtained by applying the proof of the Deduction Theorem above.

Exercise 2. Prove that $p \vee \neg p$ is not valid in the topological semantics for intuitionistic logic.

Exercise 3. Prove that $p \to \neg\neg p$ is valid in the topological semantics for intuitionistic logic.

Exercise 4 Prove that $p \to \neg\neg p$ is valid in Kripke semantics for intuitionistic logic.

Exercise 5. Show that **Int** $\nvdash p \vee \neg p$ by finding a countermodel Kripke for this formula (i.e. find a Kripke model K such that this formula is not forced at some node of K).

Exercise 6. Establish the disjunctive property of **Int**: $\vdash A \vee B$ yields ($\vdash A$ or $\vdash B$).

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

Exercise 7. Show that **Int** is not a three valued logic. In particular, show that the formula $(p \leftrightarrow q) \vee (p \leftrightarrow r) \vee (p \leftrightarrow s) \vee (q \leftrightarrow r) \vee (q \leftrightarrow s) \vee (r \leftrightarrow s)$ is not derivable in **Int**.

Hint: note, that the fact that **Cl** is two valued is reflected by the fact that $(p \leftrightarrow q) \vee (q \leftrightarrow r) \vee (p \leftrightarrow r)$ 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 $(p \leftrightarrow q) \vee (q \leftrightarrow r) \vee \ldots \vee (p \leftrightarrow s)$ (for all six pairs of p, q, r, s). Show now that the latter formula is not provable in **Int**.

Exercise 8. Prove 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**).

Exercise 9. In what follows by "derive a formula F in **IntG**" we mean "derive in **IntG** sequent $\Rightarrow F$". Derive in **IntG** formulas
a) $(A \wedge B) \rightarrow (B \wedge A)$
b) $(A \vee B) \rightarrow (B \vee A)$
c) $((A \wedge B) \rightarrow C) \leftrightarrow (A \rightarrow (B \rightarrow C))$
d) $\neg(A \wedge \neg A)$
e) $(A \vee B) \rightarrow (\neg A \rightarrow B)$. Is the converse $(\neg A \rightarrow B) \rightarrow (A \vee B)$ derivable?
f) $(A \rightarrow B) \rightarrow (\neg B \rightarrow \neg A)$. Is the converse $(\neg B \rightarrow \neg A) \rightarrow (A \rightarrow B)$ derivable?

Exercise 10. Is the Pierce Law $((A \rightarrow B) \rightarrow A) \rightarrow A$ (a classical tautology which does not look like the law of excluded middle at all) derivable in intuitionistic logic? Try to find its derivation in **IntG**.

Exercise 11. Prove the atomic axioms observation: using axioms $A \Rightarrow A$ with atomic A's only (i.e. when A is just a propositional letter) does not shrink the set of derivable sequents in **IntG**. It suffices to derive all the "old" axioms $A \Rightarrow A$ from the atomic axioms only. Such a proof should go by induction on the complexity of A. The base case when A is atomic is covered by the

atomic axioms. Consider cases corresponding to all three connectives $\wedge, \vee, \rightarrow$ and prove that if both $X \Rightarrow X$ and $Y \Rightarrow Y$ are derivable, then $(X \alpha Y) \Rightarrow (X \alpha Y)$ is also derivable where $\alpha \in \{\wedge, \vee, \rightarrow\}$.

Exercise 12. Show that two rules introducing conjunction

$$\frac{A, \Gamma \Rightarrow \Delta}{A \wedge B, \Gamma \Rightarrow \Delta} \quad \text{and} \quad \frac{B, \Gamma \Rightarrow \Delta}{A \wedge B, \Gamma \Rightarrow \Delta}$$

can be replaced in **IntG** by one rule

$$\frac{A, B, \Gamma \Rightarrow \Delta}{A \wedge B, \Gamma \Rightarrow \Delta}.$$

It suffices to derive each of the "old" rules using the new one and other rules of **IntG**.

Exercise 13. Derive $\neg\neg(A \vee \neg A)$ in **IntG**.

Exercise 14. Show that $\bot$ cannot be expressed in **Int** via other connectives $\wedge, \vee, \rightarrow$. Hint: Suppose there is a formula $F(p)$ without $\bot$ such that **Int** $\vdash F(p) \leftrightarrow (p \rightarrow \bot)$. Find a contradiction.

Exercise 15. Check whether the following is an intuitionsitic tautology:
a) $(p \wedge \neg q) \rightarrow \neg(p \rightarrow q)$
b) $\neg(p \rightarrow q) \rightarrow (p \wedge \neg q)$
c) $((p \vee q) \rightarrow r) \rightarrow [(p \rightarrow r) \wedge (q \rightarrow r)]$

Exercise 16. Let W be a new axiom schema $\neg A \vee \neg\neg A$. Consider logic **IntW** obtained by adding W to the list of axioms of **Int**. Since W is a special case of the law of excluded middle $F \vee \neg F$, logic **IntW** is located somewhere in between **Int** and **Cl**. Show that **Int** $\neq$ **IntW** $\neq$ **Cl**. It clearly suffices to show that **Int** $\nvdash W$ and **IntW** $\nvdash p \vee \neg p$. Hint: the law of excluded middle $p \vee \neg p$ is true in each one node model, but has a two node countermodel. Prove that W is valid in all two node models, regardless of A. This gives you a window of opportunity to distinguish **IntW** and **Cl**.

Exercise 17. Let LC be a new axiom schema $(A \rightarrow B) \vee (B \rightarrow A)$. Consider logic **LC** obtained by adding LC to the list of axioms of **Int**. Since LC is a classical tautology, logic **LC** is located somewhere in between **Int** and **Cl**. Show that **Int** $\neq$ **LC** $\neq$ **Cl**. It clearly suffices to show that **Int** $\nvdash LC$ and **LC** does not prove some classical tautology. Hint: axiom LC is valid in all linear models.

Exercise 18. Show that $\wedge$ cannot be expressed in **Int** via other connectives $\vee, \rightarrow, \bot$. Hint: consider the Kripke model with $W = \{0, 1, 2\}$, $0 < 2$, $1 < 2$ (yes, it is shaped as $\wedge$ itself), with $0 \models p$, $1 \models q$, $2 \models p, q$. By induction on a $\wedge$-free formula F show that the situation when $0 \not\models F$, $1 \not\models F$, and $2 \models F$ is impossible (plenty of cases to be considered, be patient). Note that $p \wedge q$ does just that, i.e. $0 \not\models p \wedge q$, $1 \not\models p \wedge q$, and $2 \models p \wedge q$.