Formalisms Every Computer Scientist Should Know

Contents

Class 1 **3**
- 0.1 Tools . . . 3
- 0.2 Syllabus . . . 3
- 0.3 Math . . . 4

Class 2 **7**
- 0.4 Lattices and Fixpoints . . . 7

Class 3 **9**

Class 6 **11**
- 0.5 Hilbert formal system for propositional logic . . . 12

Class 7 **13**
- 0.6 Natural Deduction for Propositional Logic . . . 13
  - 0.6.1 Judgements in Natural Deduction . . . 13
- 0.7 Kripke Semantics . . . 15
- 0.8 Sequent (Gentzen) Calculus and LK . . . 16
  - 0.8.1 Judgements in LK . . . 16

Class 8 **17**
  - 0.8.2 Metatheorems . . . 18
    - Compactness . . . 18
    - Craig's interpolation . . . 18
    - Cut elimination . . . 18
- 0.9 First-order logic . . . 18
  - 0.9.1 Syntax . . . 18
    - Nonlogical symbols ("signature") . . . 18
    - Logical symbols . . . 19
    - Grammar . . . 19
    - Safe substitution . . . 19

First Order Logic (FOL) **21**
  - 0.9.2 Small Detour . . . 21
  - 0.9.3 Back to Work . . . 22
  - 0.9.4 Three Sound and Complete Proof Systems . . . 22
    - Hilbert . . . 22

0.9.5 Gentzen 22
0.9.6 Natural Deduction 23

Class 1

0.1 Tools

- Lean or Coq
- CVC5 or Z3
- possibly a model checker
- professional version of ChatGPT

0.2 Syllabus

1. MATH ("Informalism")
   - proofs (natural deduction)
   - fixpoints (induction, coinduction)
2. DECLARATIVE LOGIC
   - syntax (rules) vs. semantics (models)
   - propositional, predicate, modal logic
   - decision procedures (SAT, SMT)
3. FUNCTIONS
   - λ calculus, typed λ
   - SOS (structured operational semantics), rewriting
   - "propositions-as-types" (connection to logic)
4. PROCESSES (CONCURRENT)*
   - CCS, Petri nets
   - (bi-) simulation
5. CIRCUITS*
   - boolean, sequential, dataflow (Kahn nets)
   - interfaces

6. STATE TRANSITION SYSTEMS*
   - (ω-) automata, games, timed, probabilistic, pushdown
   - programs, Turing machines
   - grammars (Chomsky hierarchy)
7. DECLARATIVE SPECIFICATION
   - Hoare logics, separation logic
   - temporal logics (LTL, CTL, ATL)
   - partial correctness vs. termination, safety vs. liveness

*: Operational.

0.3 Math

Definition 1. *A real b is a bound of a function f from $\mathbb{R}$ to $\mathbb{R}$ if for all x in $\mathbb{R}$, we have $f(x) \leq b$.*

Definition 2. *Given two functions f and g from $\mathbb{R}$ to $\mathbb{R}$, their sum is the function $f+g$ such that for all x in $\mathbb{R}$, we have $(f+g)(x) = f(x)+g(x)$.*

Theorem 1. *For all functions f and g from $\mathbb{R}$ to $\mathbb{R}$, if f and g are bounded, then $f+g$ is bounded.*

Proof.

1. Consider arbitrary functions $\hat{f}$ and $\hat{g}$ from $\mathbb{R}$ to $\mathbb{R}$.
2. Assume $\hat{f}$ and $\hat{g}$ are bounded.
3. Show that $\hat{f}+\hat{g}$ is bounded.
4. (2 $\rightarrow$) Let $\hat{a}$ be a bound for $\hat{f}$, and $\hat{b}$ be a bound for $\hat{g}$.
5. We show that $\hat{a}+\hat{b}$ is a bound for $\hat{f}+\hat{g}$.
6. Consider an arbitrary real $\hat{x}$.
7. Show $(\hat{f}+\hat{g})(x) \leq \hat{a}+\hat{b}$.
8. (Definition of sum) $(\hat{f}+\hat{g})(\hat{x}) = \hat{f}(\hat{x})+\hat{g}(\hat{x})$.
9. (Definition of bound) $\hat{f}(\hat{x}) \leq \hat{a}$ and $\hat{g}(\hat{x}) \leq \hat{b}$.
10. The rest follows from "arithmetic".

□

Homework. Prove the Schröder-Bernstein theorem "in this style".

Definition 3. *Two sets A and B are equipollent ("have the same size") if there is a bijection from A to B.*

Definition 4. *A function f from A to B is*

1. *one-to-one if for all x and y in A, if $x \neq y$, then $f(x) \neq f(y)$.*
2. *onto if for all z in B, there exists x in A such that $f(x) = z$.*

3. *bijective if f is one-to-one and onto.*

Goals	Knowledge	Outermost symbol
Show for all x, $G(x)$. Consider arbitrary $\hat{x}$. Show $G(\hat{x})$.	We know for all x, $K(x)$. In particular, we know $K(\hat{t})$. $\hat{t}$: term containing only constants.	$\forall$
Show there exists x s.t. $G(x)$. We show that $G(\hat{t})$. $\hat{t}$: term containing only constants.	We know there exists x s.t. $K(x)$. Let $\hat{x}$ be s.t. $K(\hat{x})$.	$\exists$

Class 2

Goal	Knowledge	Outermost symbol
Show for all x, $G(x)$. Consider arbitrary $\hat{x}$. Show $G(\hat{x})$	We know for all x, $K(x)$ In particular we know $K(\hat{t})$ for constant $\hat{t}$	$\forall$
Show: exists x s.t. $G(x)$. We show $G(\hat{t})$	We know exists x s.t. $K(x)$ Let $\hat{x}$ be s.t. $K(x)$	$\exists$
Show G_1 iff G_2 1. Show if G_1 then G_2 2. Show if G_2 then G_1	We know K_1 iff K_2 In particular we know if K_1 then K_2 and if K_2 then K_1	$\Longleftrightarrow$
Show if G_1 then G_2 Assume G_1 Show G_2	We know if K_1 then K_2 1. To show K_2 it suffices to show K_2 2. Know K_1, Also know K_2	$\Rightarrow$
Show G_1 and G_2 1. Show G_1 2. Show G_2	Know K_1 and K_2 1. Also Know K_1 2. Also Know K_2	$\wedge$
Show G_1 or G_2 1. Assume $\neg G_1$, show G_2 2. Assume $\neg G_2$, show G_1	We know K_1 or K_2. Show G. 1. Assume K_1, Show G 2. Assume K_2, Show G Case split ↑	$\vee$
Move Negation Inside, as far as possible		$\neg$

0.4 Lattices and Fixpoints

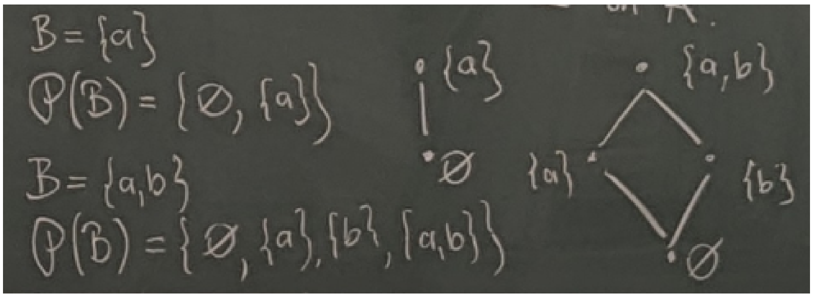
We begin by defining relations and their properties.

Definition 5. *A binary **relation** R on a set A is a subset $R \subset A \times A$.*
*The relation R is **reflexive** if for all x in A, we have $R(x,x)$.*
*The relation R is **Antisymmetric** if for all x and y in A, if $R(x,y)$ and $R(y,x)$ then $x = y$.*
*The relation R is **transitive** if for all x,y and z in A, if $R(x,y)$ and $R(y,z)$ then $R(x,z)$.*
*The relation R is a **partial order** if R is reflexive, antisymmetric and transitive.*
*A **Poset** $(A, \sqsubseteq)$ is a set A and a partial order $\sqsubseteq$ on A.*

Example 1. *The pair $(\mathbb{N}, \leq)$ where $\mathbb{N}$ is the set of natural numbers, is a poset.*
For every set B, we have $(\mathscr{P}(B), \subseteq)$ where $\mathscr{P}(B)$ is the powerset of B, is a poset.

Definition 6.

- *Let $(A, \sqsubseteq)$ be a poset. A function F from A to A is **monotone** (order-preserving, homomorphism) if for all x and y in A, if $x \sqsubseteq y$, then $F(x) \sqsubseteq F(y)$.*
- *F has a fixpoint x in A if there exists x in A such that $F(x) = x$.*



- *x in A is a pre-fixpoint of F if $x \sqsubseteq F(x)$ and is a post-fixpoint of F, if $F(x) \sqsubseteq x$.*

Definition 7. *Let $(A, \sqsubseteq)$ be a poset.*

- *x in A is an* ***upper bound****(lower bound) on a subset B of A if for all y in B, it holds that $y \sqsubseteq x$ ($x \sqsubseteq y$).*
- *x is the least upper bound of B if (i) x is an upper bound of B and (ii) for all upper bounds y of B, we have $x \sqsubseteq y$. We denote such x by $\bigsqcup B$.*
- *x is the greatest lower bound of B if (i) x is a lower bound of B and (ii) for all lower bounds y of B, we have $y \sqsubseteq x$. We denote such x by $\bigsqcap B$.*

Example 2.

- *Consider the poset $(\mathbb{N}, \leq)$. Then for any $B \subseteq \mathbb{N}$, if B is finite, $\bigsqcup B$ is well-defined and equal to $\max B$. If B is infinite, then $\bigsqcup B$ does not exist.*
- *Consider the poset $(\mathbb{N} \cup \{\infty\}, \leq)$ where for all x in $\mathbb{N}$, it holds that $x \leq \infty$. Then for all $B \subseteq \mathbb{N}$, the least upper bound $\bigsqcup B$ is well-define.*
- *Let A be any set and consider the poset $(\mathscr{P}(A), \subseteq)$. For any subset B of $\mathscr{P}(A)$, it holds that $\bigsqcup B = \bigcup B$ and $\bigsqcap B = \bigcap B$.*

Definition 8. *Poset $(A, \sqsubseteq)$ is a* ***complete-lattice*** *if for all $B \subseteq A$, both $\bigsqcap B$ and $\bigsqcup B$ exist.*

Example 3. *Let $(A, \sqsubseteq)$ be a complete-lattice.*

- $\bigsqcup A = \top$
- $\bigsqcap A = \bot$
- $\bigsqcup \varnothing = \bot$
- $\bigsqcap \varnothing = \top$

Theorem 2 (Knaster-Tarski)**.** *For every complete lattice $(A, \sqsubseteq)$ and monotone function F on A, it holds that*

1. *$\bigsqcup \{x \in A | x \sqsubseteq F(x)\}$ is the unique greatest fixpoint of F.*
2. *$\bigsqcap \{x \in A | F(x) \sqsubseteq x\}$ is the unique least fixpoint of F.*

Homework 1. *Prove the Knaster Tarski Theorem.*

Class 3

Definition 9 (Prefixpoint). *Consider a lattice $(A, \sqsubseteq)$ and a function $f\colon A \to A$. The set of prefixes is*

$$\{x \in A : x \sqsubseteq f(x)\}\,.$$

Definition 10 (Postfixpoint). *Consider a lattice $(A, \sqsubseteq)$ and a function $f\colon A \to A$. The set of postfixes is*

$$\{x \in A : f(x) \sqsubseteq x\}\,.$$

Definition 11 (gfp and lfp). *Consider a complete lattice $(A, \sqsubseteq)$ and a function $f\colon A \to A$. Then,*

$$\begin{aligned} \mathrm{gfp} f &:= \bigsqcup \{x \in A : x \sqsubseteq f(x)\} \\ \mathrm{lfp} f &:= \bigsqcap \{x \in A : f(x) \sqsubseteq x\}\,. \end{aligned}$$

Theorem 3 (Fixpoints). *Consider a complete lattice $(A, \sqsubseteq)$ and a monotonic function $f\colon A \to A$. Then,* $\mathrm{gfp} f$ *and* $\mathrm{lfp} f$ *are fixpoints of f and, for all fixpoints x of f, we have* $\mathrm{lfp} f \sqsubseteq x \sqsubseteq \mathrm{gfp} f$.

Definition 12 ($\bigsqcup$-continuous). *Consider a complete lattice $(A, \sqsubseteq)$. A function $f\colon A \to A$ is $\bigsqcup$-continuous if, for all increasing sequences $x_0 \sqsubseteq x_1 \sqsubseteq x_2 \sqsubseteq x_2 \sqsubseteq \ldots$, we have*

$$f\left(\bigsqcup \{x_n : n \in \mathbb{N}\}\right) = \bigsqcup \{f(x_n) : n \in \mathbb{N}\}\,.$$

Definition 13 ($\bigsqcap$-continuous). *Consider a complete lattice $(A, \sqsubseteq)$. A function $f\colon A \to A$ is $\bigsqcap$-continuous if, for all increasing sequences $x_0 \sqsupseteq x_1 \sqsupseteq x_2 \sqsupseteq x_2 \sqsupseteq \ldots$, we have*

$$f\left(\bigsqcap \{x_n : n \in \mathbb{N}\}\right) = \bigsqcap \{f(x_n) : n \in \mathbb{N}\}\,.$$

Lemma 1. *$\bigsqcup$-continuous implies monotonicity and $\bigsqcap$-continuous implies monotonicity.*

Theorem 4 (Constructive fixpoints). *Consider a complete lattice $(A, \sqsubseteq)$ and a monotonic function $f\colon A \to A$. Then,*

$$\begin{aligned} \mathrm{lfp} f &= \bigsqcup \{f^n(\bot) : n \in \mathbb{N}\} \\ \mathrm{gfp} f &= \bigsqcap \{f^n(\top) : n \in \mathbb{N}\}\,. \end{aligned}$$

Homework 2. *Prove this theorem.*

Definition 14 ($\mathbb{N}$). *Define $\mathbb{N}$ as the smallest set X such that*

1. $0 \in X$

2. *if $n \in X$, then $Sn \in X$*

In the definition of $\mathbb{N}$, we consider a universal set U sufficiently big, the complete lattice $(2^U, \subseteq)$ and the function on sets given by $f(Y) := \{0\} \cup \{Sn : n \in Y\}$. Then, $\mathrm{lfp} f = \mathbb{N}$.

Definition 15 (Set of words)**.** *Consider a finite alphabet Σ. Define Σ^* as the smallest set X such that*

1. $\varepsilon \in X$
2. *for all $a \in \Sigma$, we have $aX \subseteq X$.*

A few remarks are in place.

- Inductively defined sets are countable and consist of finite elements.
- Inductively defined sets can be written as rules $x \Rightarrow f(x)$ meaning that, if $x \in X$, then $f(x) \in X$.
- Inductively defined sets allow proof by induction. Consider proving that for all $x \in X$ we have $G(x)$. This can be proven by showing
  1. $G(\perp)$
  2. For all $x \in X$, if $G(x)$, then $G(f(x))$

Definition 16 (Balanced binary sequences)**.** *Define the set S as the largest set X such that*

1. $X \subseteq 01X \cup 10X$.

In the definition of balanced binary sequences, we consider the complete lattice $(\Sigma^\omega, \subseteq)$ and the function on sets given by $f(X) := 01X \cup 10X$. Then, balanced binary sequences correspond to $\mathrm{gfp} f$.

Definition 17 (Interval $[0,1]$)**.** *Define the set S as the largest set X such that*

1. $X \subseteq 0X \cup 1X \cup \ldots \cup 9X$.

A few remarks are in place.

- Coinductively defined sets are uncountable and consist of infinite elements.
- Coinductively defined sets can be written as rules $x \Leftarrow f(x)$ meaning that, for all $y \in X$, there exists x such that $y = f(x)$ and $x \in X$.
- Coinductively defined sets allow proof by coinduction. Consider proving that for all x, if $G(x)$, then $x \in X$. This can be proven by showing
  1. For all x and i, if $G(f_i(x))$, then $G(x)$,

  where $\{f_1, \ldots, f_n\}$ is the set of rules that define the set X.

Homework 3 (Prove balanced binary sequences)**.** *Consider S generated by the rules $X \Leftarrow 01X$ and $X \Leftarrow 10X$. Prove that, for all binary words x, we have that x inS if and only if every finite prefix of even length of x has the same number of* 0*s and* 1*s.*

Hints.

1. The direction $\Leftarrow$ can be proven by coinduction.
2. The direction $\Rightarrow$ can be proven by induction on the length of the prefix.

Class 6

Formal system F is a set of rules. Rule is a finite set of (formulas) premises $p_0, \ldots, p_k$ and (a formula called) conclusion c. We usually have infinitely many rules but only finitely many different rule schemata. For example, schema $\phi \to \phi$ gives infinitely many rules like $p_3 \to p_3$. Axiom is a rule without premises.

Proof (derivation) is a finite sequence of formulas $\phi_0, \ldots, \phi_n$ such that every formula in the sequence is

- either an axiom (which can be viewed as a special case of the following);
- or the conclusion of a rule whose premises occur earlier in the sequence.

This is a linear view.

Linear view is usually easier for proving meta theorems. Tree view (inductive definition) is usually better in practice.

Theorem is a formula that occurs in a proof. We distinguish the following:

- $\vdash \phi$ ... "ϕ is a theorem (of the formal system F)" (has a proof) [syntax]
- $\vDash \phi$ ... "ϕ is valid (ϕ is tautology)" (is true in all models) [semantics]

Formal system equipped with semantics is called a logic. Most of logic is about establishing $\vdash \phi$ iff $\vDash \phi$.

Rule R is sound iff [if all premises of R are valid, then the conclusion of R is valid]. Formal system F is sound iff all rules are sound (or equivalently, every theorem is valid). Formal system F is complete iff every valid formula is a theorem. Formal system F is consistent unless $\vdash \bot$ (or equivalently, there exists a formula that is not a theorem). Rule R is derivable in F iff [for all formulas ϕ, $\underset{F \cup \{R\}}{\vdash} \phi$ iff $\underset{F}{\vdash} \phi$]. Rule R is admissible in F iff $F \cup \{R\}$ is still consistent. Formula ϕ is expressible in a logic L iff [there exists a formula ψ of L such that, for all interpretations v, $[[\phi]]_v = [[\psi]]_v$. For example $\phi_1 \wedge \phi_2$ is expressible using only $\neg$ and $\vee$ (de Morgan) as $\psi = \neg(\neg\phi_1 \wedge \neg\phi_2)$.

We can enumerate all theorems by systematically enumerating all possible proofs. The proof is a witness for validity. Sound formal system gives a sound procedure for validity (but not necessarily complete). Sound complete formal system gives a sound semi-complete procedure for validity (may not terminate on inputs that represent a formula that is not valid). To get a decision procedure (sound and complete procedure for validity), we need both (1) sound complete formal system for validity, and (2) sound complete formal system for satisfiability (to define a formal system for satisfiability, replace "formulas" (ϕ is valid) by "judgements" (ϕ is satisfiable); all axioms are satisfiable, all rules go from satisfiables to satisfiable). For every input ϕ, one of them will eventually terminate. Conclude; either ϕ is valid, or $\neg\phi$ is satisfiable (which means that ϕ is not valid). Recall that, if both a set and its complement are recursively-enumerable, the set is recursive (decidable).

Example (formal system for unsatisfiability):

$$\frac{\Gamma[\bot] \qquad\qquad \Gamma[\top]}{\Gamma[p]}$$

0.5 Hilbert formal system for propositional logic

Hilbert system uses connectives → and ¬ only. Hilbert system has three axioms and one rule – modus ponens (MP):

$$\frac{\phi \qquad\qquad \phi \to \psi}{\psi}$$

Axioms:

- (K): $\phi \to \psi \to \phi$
- (S): $(\phi \to \psi \to \chi) \to ((\phi \to \psi) \to (\phi \to \chi))$
- (em): $(\neg\phi \to \neg\psi) \to (\psi \to \phi)$

Example (prove $\phi \to \phi$ in Hilbert system):
(K) $\phi \to (\psi \to \phi) \to \phi$
(S) $(\phi \to (\psi \to \phi) \to \phi) \to ((\phi \to \psi \to \phi) \to (\phi \to \phi))$
(MP) $(\phi \to \psi \to \phi) \to (\phi \to \phi)$
(K) $\phi \to \psi \to \phi$
(MP) $\phi \to \phi$

Notation: $\Gamma \vdash \phi$ means $\underset{F \cup \Gamma}{\vdash} \phi$ (the set of formulas Γ is used as added axioms)
Metatheorem ("deduction theorem"): $\Gamma \vdash \phi \to \psi$ iff $\Gamma, \phi \vdash \psi$
Metaproof:
" $\Longrightarrow$ ": One application of modus ponens.
" $\Longleftarrow$ ": Assume ψ has a proof π using axioms Γ, ϕ, (K), (S), (em). Show that $\phi \to \psi$ has a proof π' using Γ, (K), (S), (em) — induction on length n of π.
Case $n = 1$: ψ must be an axiom. Either $\psi \in \Gamma \cup \{\mathrm{K}, \mathrm{S}, \mathrm{em}\}$ so we prove it by (K), or $\psi = \phi$ so we use $\vdash \phi \to \phi$ as derived above.
Case $n > 1$: ψ is the result of an application of modus ponens. We have χ and $\chi \to \psi$, both of which were derived from Γ, ϕ in fewer steps. Induction hypothesis gives us $\Gamma \vdash \phi \to \chi$ and $\Gamma \vdash \phi \to \chi \to \psi$. We use (S) in the form $(\phi \to \chi \to \psi) \to (\phi \to \chi) \to (\phi \to \psi)$ and apply modus ponens twice, resulting in $\phi \to \psi$ derived from Γ only.

Class 7

For this chapter, we replace the word *formula* in rules and proofs of a formal system by the word *judgement*.

0.6 Natural Deduction for Propositional Logic

Judgements in Natural Deduction have the form $\Gamma \vdash \phi$, where Γ is a set of formulas and ϕ is a formula. Semantically, for all interpretations v, if all formulas in Γ are true in v, then ϕ is true in v. Formal system for natural deduction defines a meta-symbol $\vdash_{\text{meta}}$ such that $\vdash_{\text{meta}} (\Gamma \vdash \phi)$.

0.6.1 Judgements in Natural Deduction

We use the notation Γ, ϕ to show $\Gamma \cup \{\phi\}$.

1. Axioms

$$\frac{}{\Gamma, \phi \vdash \phi}\ \textsc{ax} \qquad\qquad \frac{}{\Gamma \vdash \top}\ \top\textsc{-intro}$$

2. False-elimination: if $\bot$ can be derived, then anything can be derived.

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash \phi}\ \bot\textsc{-elim}$$

3. Conjunction elimination and introduction

$$\frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \phi}\ \wedge\textsc{-elim} \qquad\qquad \frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \psi}\ \wedge\textsc{-elim} \qquad\qquad \frac{\Gamma \vdash \phi \qquad \Gamma \vdash \psi}{\Gamma \vdash \phi \wedge \psi}\ \wedge\textsc{-intro}$$

4. Disjunction elimination and introduction

$$\frac{\Gamma \vdash \phi \vee \psi \qquad \Gamma, \phi \vdash \chi \qquad \Gamma, \psi \vdash \chi}{\Gamma \vdash \chi}\ \vee\textsc{-elim} \qquad\qquad \frac{\Gamma \vdash \phi}{\Gamma \vdash \phi \wedge \psi}\ \vee\textsc{-intro} \qquad\qquad \frac{\Gamma \vdash \phi}{\Gamma \vdash \psi \wedge \phi}\ \wedge\textsc{-intro}$$

5. Negation elimination and introduction

$$\frac{\Gamma \vdash \phi \qquad \Gamma \vdash \neg\phi}{\Gamma \vdash \bot}\ \neg\textsc{-elim} \qquad\qquad \frac{\Gamma, \phi \vdash \bot}{\Gamma \vdash \neg\phi}\ \neg\textsc{-intro}$$

6. Implication elimination and introduction

$$\dfrac{\Gamma\vdash\phi \qquad \Gamma\vdash\phi\to\psi}{\Gamma\vdash\psi}\ \to\text{-ELIM} \qquad\qquad \dfrac{\Gamma,\phi\vdash\psi}{\Gamma\vdash\phi\to\psi}\ \to\text{-INTRO}$$

Observe how →-elim is similar to modus ponens.

Homework 4. *Prove implication transitivity using Natural Deduction.*

Example 4. *Show* $(\phi\to\psi)\to(\neg\psi\to\neg\phi)$.

Proof.

$$\dfrac{\dfrac{\dfrac{\dfrac{\phi\to\psi,\neg\psi,\phi\vdash\psi \qquad \phi\to\psi,\neg\psi,\phi\vdash\neg\psi}{\phi\to\psi,\neg\psi,\phi\vdash\bot}\ \neg\text{-ELIM}}{\phi\to\psi,\neg\psi\vdash\neg\phi}\ \neg\text{-INTRO}}{(\phi\to\psi)\vdash(\neg\psi\to\neg\phi)}\ \to\text{-INTRO}}{\vdash(\phi\to\psi)\to(\neg\psi\to\neg\phi)}\ \to\text{-INTRO}$$

Now we have two goals to prove.

$$\dfrac{\dfrac{}{\phi\to\psi,\neg\psi,\phi\vdash\phi}\ \text{AX} \qquad \dfrac{}{\phi\to\psi,\neg\psi,\phi\vdash\phi\to\psi}\ \text{AX}}{\phi\to\psi,\neg\psi,\phi\vdash\psi}\ \to\text{-ELIM} \qquad\qquad \dfrac{}{\phi\to\psi,\neg\psi,\phi\vdash\neg\psi}\ \text{AX}$$

□

Observe how this method of writing proofs in Natural Deduction requires us to rewrite the context for every step. We can use a slightly different notation to avoid this repetition.

We can draw boxes to introduce *contexts* in a proof. Every formula written inside a box is assumed to hold only within that box. The following "proofs" are examples of using this notation.

$$\dfrac{\boxed{\begin{array}{c}\phi\\ \vdots\\ \psi\end{array}}}{\phi\to\psi} \qquad \dfrac{\boxed{\begin{array}{c}\phi\\ \vdots\\ \bot\end{array}}}{\neg\phi} \qquad\qquad \dfrac{\phi\lor\psi \qquad \boxed{\begin{array}{c}\phi\\ \vdots\\ \chi\end{array}} \qquad \boxed{\begin{array}{c}\phi\\ \vdots\\ \chi\end{array}}}{\chi}$$

Using this notation, we can rewrite the proof for example 4:

$$\dfrac{\boxed{\begin{array}{c}1.\ \phi\to\psi\\ \dfrac{\boxed{\begin{array}{c}2.\ \neg\psi\\ \dfrac{\boxed{\begin{array}{c}3.\ \phi\\ 4.\ \psi\ (\to\text{-elim, 1, 3})\\ 5.\ \bot\ (\neg\text{-elim, 2, 4})\end{array}}}{\neg\phi}\end{array}}}{\neg\psi\to\neg\phi}\end{array}}}{(\phi\to\psi)\to(\neg\psi\to\neg\phi)}$$

The system defined above is in fact the NJ (Intuitionistic Natural Deduction) system. The following rule, namely the law of excluded middle, cannot be derived in NJ:

$$\frac{}{\Gamma \vdash \phi \vee \neg\phi}\ \text{EX-MIDDLE}$$

The NK system (Classical Natural Deduction) is NJ with the addition of the law of excluded middle. The NK system is sound and complete for propositional logic.

Assumption of the law of excluded middle is in fact an important distinction between Intuitionistic and classical logic. In the following is an example which uses excluded middle in its proof.

Example 5. *Show that there exist $a, b \notin \mathbb{Q}$ such that $a^b \in \mathbb{Q}$.*

Proof. Let $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$. We know that $\sqrt{2} \notin \mathbb{Q}$. We do a "classical" case-splitting on $a \in \mathbb{Q}$:

1. $a \notin \mathbb{Q}$. We have
$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2 \in \mathbb{Q}$$

2. $a \in \mathbb{Q}$. We are already done with the proof; let $a_1 = b_1 = \sqrt{2}$. We know $a_1, b_1 \notin \mathbb{Q}$ and, by assumption, ${a_1}^{b_1} \in \mathbb{Q}$.

Observe how this classical-style proof utilizes the law of excluded middle in the case-splitting: $\sqrt{2}^{\sqrt{2}}$ is either in $\mathbb{Q}$ or not in $\mathbb{Q}$; there is no *middle*. □

0.7 Kripke Semantics

Classically, an interpretation $v : P \to \mathbb{B}$ is defined as a mapping from a set of propositions to boolean values $\top$ and $\bot$. For intuitionistic reasoning, we define a new semantics.

Definition 18. *A Kripke model m is defined as a tuple $(W, \leq, w_0, v : W \times P \to \mathbb{B})$, where W is a set of classical worlds, $\leq$ is a pre-order relation on W, w_0 is the initial world, and v is a function from pairs of world and proposition to boolean values such that for any $w, w' \in W$ and any $p \in P$, if $w \leq w'$, then $v(w, p) \leq v(w', p)$.*

Informally, a Kripke model is an interpretation model for intuitionistic proof systems. The following facts hold for any Kripke model m:

1. $m \models \phi$ iff $m \vdash_{w_0} \phi$.

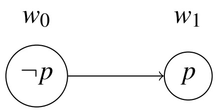
2. $m \not\models_w \bot$ for any world w.

3. $m \models_w p$ iff $v(w, p) = \top$.

4. $m \models_w \phi \to \psi$ iff for any w', if $w \leq w'$ and $m \models_{w'} \phi$, then $m \models_{w'} \psi$.

In NJ, whenever you show $\phi \vee \psi$, you need to show either ϕ, or ψ. As previously stated, the law of excluded middle cannot be derived in NJ. To show this, we need to show that there exists a Kripke model m such that excluded middle is false in a world w of m.

Let us define a Kripke model with only one proposition p and only two worlds w_0 and w_1, where $w_0 \leq w_1$, and p is false in w_0 and true in w_1.



Let us examine what formulas are true (or false) in each world. By definition, p is false in w_0. Let us examine the value of $\neg p$ in w_0. We can safely substitute $\neg p$ with $p \to \bot$. By definition, $p \to \bot$ holds in w_0 iff for any world w, if $w_0 \leq w$ and p is true in w, then $\bot$ is true in w. We know p is true in w_1. We also know that $\bot$ is not true in w_1, as it is not true in any world. So, by definition, $p \to \bot$ is false in w_0. So, both p and $\neg p$ are false in w_0, from which we obtain that $p \vee \neg p$ is also false in w_0.

0.8 Sequent (Gentzen) Calculus and LK

Judgements in the LK proof system have the form $\Gamma \vdash \Delta$, where both Γ and Δ are sets of formulas. Judgement $\Gamma \vdash \Delta$ should be read as "the *conjunction* of the formulas in Γ implies the *disjunction* of the formulas in Δ". Semantically, for a classical interpretation v, $v \models (\Gamma \vdash \Delta)$ if and only if, if all formulas in Γ are true under v, then some fomula in Δ is true under v.

0.8.1 Judgements in LK

Observe how every non-axiom judgement increases the number of logical connectives in the set of formulas.

1. Axioms

$$\frac{}{\Gamma, \phi \vdash \phi, \Delta}\ \text{AX} \qquad \frac{}{\Gamma, \bot \vdash \Delta}\ \bot\text{-ELIM} \qquad \frac{}{\Gamma \vdash \top, \Delta}\ \top\text{-INTRO}$$

2. Conjunction

$$\frac{\Gamma, \phi, \psi \vdash \Delta}{\Gamma, \phi \wedge \psi \vdash \Delta} \qquad \frac{\Gamma \vdash \phi, \Delta \qquad \Gamma \vdash \psi, \Delta}{\Gamma \vdash \phi \wedge \psi, \Delta}$$

3. Disjunction

$$\frac{\Gamma, \phi \vdash \Delta \qquad \Gamma, \psi \vdash \Delta}{\Gamma, \phi \vee \psi \vdash \Delta} \qquad \frac{\Gamma \vdash \phi, \psi, \Delta}{\Gamma \vdash \phi \vee \psi, \Delta}$$

4. Negation

$$\frac{\Gamma, \phi \vdash \Delta}{\Gamma \vdash \neg\phi, \Delta} \qquad \frac{\Gamma \vdash \phi, \Delta}{\Gamma, \neg\phi \vdash \Delta}$$

5. Implication

$$\frac{\Gamma, \phi \vdash \psi, \Delta}{\Gamma \vdash \phi \to \psi, \Delta} \qquad \frac{\Gamma \vdash \phi, \Delta \qquad \Gamma, \psi \vdash \Delta}{\Gamma, \phi \to \psi \vdash \Delta}$$

The LK proof system is sound and complete for propositional logic. This actually means that excluded middle can be derived in LK.

Homework 5. *Prove the following in LK:*

1. *The law of excluded middle:* $\vdash p \vee \neg p$*,*
2. *Implication transitivity.*

Class 8

We now talk about three proof systems:

- Hilbert

$$\vdash \phi$$

- Natural deduction

$$\Gamma \vdash \phi$$

- Grentzen

$$\Gamma \vdash \Delta$$

We now talk abou three decision procedures (either for validity or for satisfiability):

- Branching (if we don't derive $\bot$ then it is satisfiable)

$$\frac{\Gamma[\bot] \qquad\qquad \Gamma[\top]}{\Gamma[p]}$$

- Resolution

$$\frac{\Gamma, C_1, C_2, C_1[\bot] \vee C_2[\bot]}{\Gamma, C_1[p], C_2[p]}$$

- Unit resolution, combined with branching of lower priority (DPLL)

$$\frac{\Gamma, C[\bot]}{\Gamma, \ell, C[\neg\ell]}$$

  Example:

$$p \vee q \vee r,\ \neg p \vee \neg q \vee \neg r,\ \neg p \vee q \vee r,\ \neg q \vee r,\ q \vee \neg r$$

  First we branch on r.

  - Case $r = \bot$:

$$p \vee q,\ \neg p \vee q,\ \neg q$$

    We didn't continue this branch.

  - Case $r = \top$:

$$\neg p \vee \neg q,\ q$$

    Then we propagate q. We end up with $\neg p$.
    It is satisfied by $p = \bot,\ q = \top,\ r = \top$.

Horn clause is a clause with at most one positive literal. We can view them as implications where LHS is a conjunction of positive propositions:

$$\begin{aligned} \neg p \vee \neg q &\iff p \wedge q \to \bot \\ \neg p \vee \neg q \vee r &\iff p \wedge q \to r \\ r &\iff \top \to r \end{aligned}$$

0.8.2 Metatheorems

Compactness

Countable set Γ of formulas is satisfiable iff every finite subset of Γ is satisfiable.

Craig's interpolation

We have $\vdash \phi \to \psi$ iff there exists a third formula χ (the "interpolant") which only uses nonlogical symbols (in propositional logic, it is propositions only) that occur in both ϕ and ψ such that $\vdash \phi \to \chi$ and $\vdash \chi \to \psi$.

Cut elimination

Cut rule in NK / NJ:

$$\frac{\Gamma \vdash \phi \qquad\qquad \Gamma, \phi \vdash \psi}{\Gamma \vdash \psi}$$

Cut rule in LK:

$$\frac{\Gamma \vdash \phi, \Delta \qquad\qquad \Gamma, \phi \vdash \Delta}{\Gamma \vdash \Delta}$$

If a judgement can be proved with the cut rule, it can also be proved without the cut rule. In fact, it is "iff"; the other direction is trivial. Of course, the proof may become longer (introducing a lemma ϕ often helps in practice). It is a purely syntactic metatheorem. We cannot use deduction to prove it.

0.9 First-order logic

First-order logic, also called "predicate logic", is propositional logic with quantifiers $\forall$ (for all) and $\exists$ (exists).

0.9.1 Syntax

Nonlogical symbols ("signature")

- finite set of variables $X = \{x, y, z, \dots\}$
- finite set of function symbols $F = \{f, g, h, \dots\}$
- finite set of predicate symbols $P = \{p, q, r, \dots\}$

Each function symbol has a fixed "arity" (number of arguments), which can be zero (arity 0 gives a constant). Each predicate symbol has also a fixed "arity" (number of arguments), which can be zero (arity 0 gives a proposition).

Logical symbols

- connectives $(\bot, \top, \neg, \wedge, \vee, \rightarrow)$
- quantifiers $(\forall, \exists)$
- finite set of predicate symbols $P = \{p, q, r, \dots\}$

We don't add parentheses to the symbols; we will talk about syntax trees; only if we want to write them down as strings, we add parentheses (as few as possible).

Grammar

- Terms: $\phi \ := \ f_0 \mid f_n(t_1, \dots, t_n)$
- Formulas: $\phi \ := \ p_0 \mid p_n(t_1, \dots, t_n) \mid \bot \mid \top \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \phi \rightarrow \phi \mid \forall x.\phi \mid \exists x.\phi$

When we write $\forall x.\phi$, every occurence of x is bound in ϕ. A variable that is not bound is called free. A change of bound variables does not change the abstract syntax tree (same in abstract syntax).

Safe substitution

$$\forall x.\ \exists y.\ y \geq x + 1$$

If we want to substitute y^2 for x, we must first rename y to z and then substitute.

$$\forall x.\ \exists z.\ z \geq x + 1$$

$$\exists z.\ z \geq y^2 + 1$$

First Order Logic (FOL)

Definition 19. *Interpretation I in first-order structure:*

1. *Domain D_I*
2. *for each n-ary function symbol $f \in F$, $[f]_I : D_I^n \to D_I$*
3. *for each n-ary predicate symbol $p \in P$, $[p]_I : D_I^n \to B = \{true, false\}$*
4. *"context" (environment) for each (free) variable $x \in X$, $[x]_I \in D_I$*

Formula ϕ is closed if it has no free variables.
Given an interpretation I, a term t and a formula ϕ have the following meaning:

$$[t]_I = \begin{cases} [x]_I & t = x \\ [f]_I([t_1]_I, [t_2]_I, \ldots, [t_n]_I) & t = f(t_1, \ldots, t_n) \end{cases}$$

$$[\phi]_I = \begin{cases} [x]_I & t = x \\ [p]_I([t_1]_I, [t_2]_I, \ldots, [t_n]_I) & \phi = p(t_1, \ldots, t_n) \end{cases}$$

$$[\phi_1 \Rightarrow \phi_2]_I = True \text{ } iff [\phi_1]_I = false \text{ } or \text{ } [\phi_2]_I = true$$

$$[\forall x.\phi]_I = True \text{ } iff \text{ } for \text{ } all \text{ } d \in D_I, [\phi]_{I[x \to d]}$$
$$[\exists x.\phi]_I = True \text{ } iff \text{ } for \text{ } some \text{ } d \in D_I, [\phi]_{I[x \to d]}$$

$$\phi \text{ } valid \text{ } (\vDash \phi) \text{ } iff \text{ } [\phi]_I = True \text{ } for \text{ } all \text{ } interpretations \text{ } I$$

$$\phi \text{ } satisfiable \text{ } iff \text{ } [\phi]_I = True \text{ } for \text{ } some \text{ } interpretations \text{ } I$$

0.9.2 Small Detour

PCP (Post Correspondence Problem): Given a finite set S of dominoes $\frac{s}{t}$ where $s, t \in \{0, 1\}^*$. Is there a finite sequence $\frac{s_1}{t_1}, \ldots \frac{s_n}{t_n}$ of (possibly repeating) dominoes from S such that the

$$s_1 \cdot s_2 \cdot \cdots \cdot s_n = t_1 \cdot t_2 \cdot \cdots \cdot t_n$$

Theorem 5. *The PCP problem is undecidable.*

0.9.3 Back to Work

Metatheorem 1. *1. (Compactness) Set Γ of formulas is satisfiable iff every finite subset of Γ is satisfiable.*

2. (Lowenheim-Skolem). If a set Γ of formulas is satisfiable then Γ is satisfiable by an interpretation with countable domain.

3. Both the validity and satisfiability problems for FOL are undecidable.

Proof. (Proof sketch of undecidability) Let $F = \{e, f_0, f_1\}$ where e is 0-ary and f_0, f_1 are unary. Basically a string 011 of 0,1s is represented as $f_1(f_1(f_0(e)))$.

Let $P = \{p\}$ where p is a binary predicate. Basically a domino $\frac{s}{t}$ is represented by $p(s,t)$.

Given an instance R of PCP, the formula $\phi_R = (\phi_1 \wedge \phi_2) \Rightarrow \phi_3$ is valid iff the answer to R is yes:

$$\begin{aligned}
\phi_1 &= \bigwedge_{1 \le i \le k} P(s_i(e), t_i(e)) \\
\phi_2 &= \forall v, w.(p(v,w) \Rightarrow \bigwedge_{1 \le i \le k} p(s_i(v), t_i(w))) \\
\phi_3 &= \exists z.p(z,z)
\end{aligned}$$

□

0.9.4 Three Sound and Complete Proof Systems

Hilbert

$$\begin{aligned}
&1.(\forall x.\phi) \Rightarrow \phi[x := t] \\
&2.\forall x.(\phi \Rightarrow \psi) \Rightarrow (\forall x.\phi) \Rightarrow (\forall x.\psi) \\
&3.\phi \Rightarrow \forall x.\phi \quad \textit{provided that x is not free in } \phi
\end{aligned}$$

($\phi[x := t]$ means safely replacing each occurrence of x by t)

0.9.5 Gentzen

$$\frac{\Gamma, \phi[x := t] \vdash \Delta}{\Gamma, \forall x.\phi \vdash \Gamma} \forall - elim$$

$$\frac{\Gamma \vdash \Delta, \phi[x := y]}{\Gamma \vdash \Delta, \forall x.\phi} \forall - intro \textit{ y is a new (fresh) variable}$$

$$\frac{\Gamma, \phi[x := y]}{\Gamma, \exists x.\phi \vdash \Delta} \exists - elim$$

$$\frac{\Gamma \vdash \Delta, \phi[x := t]}{\Gamma \vdash \Delta, \exists x.\phi} \exists - intro$$

0.9.6 Natural Deduction

$$\frac{\forall x\phi}{\phi[x := t]}$$

$$\frac{\phi[x := t]}{\exists x.\phi}$$

$$\frac{\begin{bmatrix} y \textit{ new} \\ \dots \\ \phi[x := y] \end{bmatrix}}{\forall x.\phi}$$

$$\frac{\exists x.\phi, \begin{bmatrix} y : \phi[x := y] \\ \dots \\ \psi \end{bmatrix}}{\psi}$$

Homework 6. *Prove de Morgan for quantifiers*

$$\forall x.\phi \Leftrightarrow \nexists x.\ \not\phi$$

in all three systems.

Homework 7. *Use PCP to show satisfiability of FOL is undecidable.*