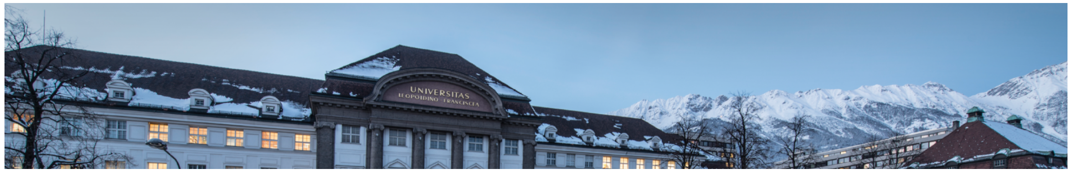
WS 2023 lecture 12



Computability Theory

Aart Middeldorp

Outline

Theorem (Strong Normalization)

typable CL–terms are terminating (SN)

Definition

typable CL–term t is strongly computable (SC) if

- t has atomic type $\tau \in \mathbb{V} \cup \mathbb{C}$ and is SN
- t has type $\sigma \to \tau$ and $t\,u$ is SC whenever $u : \sigma$ is SC

Lemma

every typable term is SC and every SC term is terminating

Theorem

problem

instance: CL–term t
question: is t typable ?

is decidable

Definition

principal type of combinator t is any type σ such that

① $\vdash t : \sigma$

② if $\vdash t : \tau$ then τ is substitution instance of σ

Theorem

every typable combinator has principal type

Type Inference

principle types can be computed by typing rules of TA (with type variables σ, τ, ρ)

$$\frac{}{\mathsf{I} : \sigma \to \sigma} \qquad \frac{}{\mathsf{K} : \sigma \to \tau \to \sigma} \qquad \frac{}{\mathsf{S} : (\rho \to \sigma \to \tau) \to (\rho \to \sigma) \to \rho \to \tau} \qquad \frac{t : \sigma \to \tau \qquad u : \sigma}{t\,u : \tau}$$

and unification algorithm

Definition

type τ is inhabited if $\vdash t : \tau$ for some combinator t

Theorem

problem

instance: type τ
question: is τ inhabited ?

is decidable

Intuitionistic Propositional Logic

- basic connectives $\to$ $\wedge$ $\vee$ $\bot$
- derived connectives
  - $\neg\varphi$ abbreviates $\varphi \to \bot$
  - $\top$ abbreviates $\bot \to \bot$
  - $\varphi \leftrightarrow \psi$ abbreviates $(\varphi \to \psi) \wedge (\psi \to \varphi)$
- implication fragment contains only $\to$

Definition

Kripke model is triple $\mathcal{C} = \langle C, \leqslant, \Vdash \rangle$ with

- non-empty set C of states
- partial order $\leqslant$ on C
- binary relation $\Vdash$ between elements of C and propositional atoms

such that $d \Vdash p$ whenever $c \Vdash p$ and $c \leqslant d$

Definition

Kripke model $\mathcal{C} = \langle C, \leqslant, \Vdash \rangle$, $c \in C$

- $c \Vdash \varphi \wedge \psi$ if and only if $c \Vdash \varphi$ and $c \Vdash \psi$
- $c \Vdash \varphi \vee \psi$ if and only if $c \Vdash \varphi$ or $c \Vdash \psi$
- $c \Vdash \varphi \to \psi$ if and only if $d \Vdash \psi$ for all $d \geqslant c$ with $d \Vdash \varphi$
- $c \nVdash \bot$

Terminology

c forces p if $c \Vdash p$

Definition

Kripke model $\mathcal{C} = \langle C, \leqslant, \Vdash \rangle$, $c \in C$

- $c \Vdash \Gamma$ if $c \Vdash \varphi$ for all $\varphi \in \Gamma$
- $\mathcal{C} \Vdash \varphi$ if $c \Vdash \varphi$ for all $c \in C$

Definition

$\Gamma \Vdash \varphi$ if $c \Vdash \varphi$ whenever $c \Vdash \Gamma$ for all Kripke models $\mathcal{C} = \langle C, \leqslant, \Vdash \rangle$ and $c \in C$

Lemma (Monotonicity)

if $c \leqslant d$ and $c \Vdash \varphi$ then $d \Vdash \varphi$

Lemma

if $\Vdash \varphi \vee \psi$ then $\Vdash \varphi$ or $\Vdash \psi$

Part I: Recursive Function Theory

Ackermann function, bounded minimization, bounded recursion, course–of–values recursion, diagonalization, diophantine sets, elementary functions, fixed point theorem, Fibonacci numbers, Gödel numbering, Gödel's β function, Grzegorczyk hierarchy, loop programs, minimization, normal form theorem, partial recursive functions, primitive recursion, recursive enumerability, recursive inseparability, s–m–n theorem, total recursive functions, undecidability, while programs, ...

Part II: Combinatory Logic and Lambda Calculus

α–equivalence, abstraction, arithmetization, β–reduction, CL–representability, combinators, combinatorial completeness, Church numerals, Church–Rosser theorem, Curry–Howard isomorphism, de Bruijn notation, η–reduction, fixed point theorem, intuitionistic propositional logic, λ–definability, normalization theorem, termination, typing, undecidability, Z property, ...

Outline

Online Evaluation in Presence

https://lv-analyse.uibk.ac.at/evasys/public/online/index

Definition

Hilbert system (for implication fragment) consists of two axioms and modus ponens:

$$\frac{}{\varphi \to \psi \to \varphi} \qquad \frac{}{(\varphi \to \psi \to \chi) \to (\varphi \to \psi) \to \varphi \to \chi} \qquad \frac{\varphi \quad \varphi \to \psi}{\psi}$$

Definitions

- derivation in Hilbert system from set Γ of formulas is finite sequence of formulas such that each formula is
  - axiom or
  - member of Γ or
  - follows from earlier formulas by modus ponens
- φ is consequence of set Γ ($\Gamma \vdash_h \varphi$) if φ is last line of derivation from Γ
- proof in Hilbert system is derivation from $\varnothing$
- formula φ is theorem ($\vdash_h \varphi$) if φ is consequence of $\varnothing$

Example

$\varphi \to \varphi$ is theorem:

1	$(\varphi \to (\varphi \to \varphi) \to \varphi) \to (\varphi \to \varphi \to \varphi) \to \varphi \to \varphi$	axiom
2	$\varphi \to (\varphi \to \varphi) \to \varphi$	axiom
3	$(\varphi \to \varphi \to \varphi) \to \varphi \to \varphi$	modus ponens 1, 2
4	$\varphi \to \varphi \to \varphi$	axiom
5	$\varphi \to \varphi$	modus ponens 3, 4

Deduction Theorem

$\Gamma \cup \{\varphi\} \vdash_h \psi \iff \Gamma \vdash_h \varphi \to \psi$

Proof ($\Longleftarrow$)

- suppose $\Gamma \vdash_h \varphi \to \psi$
- $\Gamma \cup \{\varphi\} \vdash_h \varphi \to \psi$ and $\Gamma \cup \{\varphi\} \vdash_h \varphi \implies \Gamma \cup \{\varphi\} \vdash_h \psi$ by modus ponens

Example

$(\varphi \to \psi \to \chi) \to \psi \to \varphi \to \chi$ is theorem:

- $\{\varphi \to \psi \to \chi, \psi, \varphi\} \vdash_h \chi$

1	$\varphi \to \psi \to \chi$	
2	φ	
3	$\psi \to \chi$	modus ponens 1, 2
4	ψ	
5	χ	modus ponens 3, 4

- $\{\varphi \to \psi \to \chi, \psi\} \vdash_h \varphi \to \chi$ by deduction theorem
- $\{\varphi \to \psi \to \chi\} \vdash_h \psi \to \varphi \to \chi$ by deduction theorem
- $\vdash_h (\varphi \to \psi \to \chi) \to \psi \to \varphi \to \chi$ by deduction theorem

Proof ($\Longrightarrow$)

- suppose $\Gamma \cup \{\varphi\} \vdash_h \psi$
- let $\Pi_1 \colon \chi_1, \dots, \chi_n$ be derivation of ψ from $\Gamma \cup \{\varphi\}$, so $\chi_n = \psi$
- consider new sequence $\Pi_2 \colon \varphi \to \chi_1, \dots, \varphi \to \chi_n$
- insert extra lines into Π_2 and use modus ponens, as follows:
  1. if χ_i is axiom or member of Γ
     insert χ_i and $\chi_i \to \varphi \to \chi_i$ before $\varphi \to \chi_i$
  2. if $\chi_i = \varphi$
     insert steps of proof of $\varphi \to \varphi$ before it
  3. if χ_i is derived with modus ponens from χ_j and χ_k with $j, k < i$ then $\chi_k = (\chi_j \to \chi_i)$
     insert $(\varphi \to \chi_j \to \chi_i) \to (\varphi \to \chi_j) \to \varphi \to \chi_i$ and $(\varphi \to \chi_j) \to \varphi \to \chi_i$ before $\varphi \to \chi_i$
- resulting sequence is derivation of $\varphi \to \psi$ from Γ

Theorem

Hilbert system is sound and complete with respect to Kripke models for implication fragment:

$$\Gamma \vdash_h \varphi \iff \Gamma \Vdash \varphi$$

Proof ($\Longrightarrow$)

suppose $\Gamma \vdash_h \varphi$, we prove $\Gamma \Vdash \varphi$ by induction on length of derivation of $\Gamma \vdash_h \varphi$:

- $\varphi \in \Gamma$

  $\Gamma \Vdash \varphi$ holds trivially
- $\varphi = (\psi_1 \to \psi_2 \to \psi_1)$

  $\Vdash \varphi$ by definition of $\Vdash$ and thus also $\Gamma \Vdash \varphi$
- $\varphi = ((\psi_1 \to \psi_2 \to \psi_3) \to (\psi_1 \to \psi_2) \to \psi_1 \to \psi_3)$

  $\Vdash \varphi$ by definition of $\Vdash$ and thus also $\Gamma \Vdash \varphi$
- φ is obtained by modus ponens

  $\Gamma \vdash_h \psi$ and $\Gamma \vdash_h \psi \to \varphi$ are shorter derivations

  $\Gamma \Vdash \psi$ and $\Gamma \Vdash \psi \to \varphi$ by induction hypothesis

  $\Gamma \Vdash \varphi$ by definition of $\Vdash$

Proof ($\Longleftarrow$)

suppose $\Gamma \vdash_h \varphi$ does not hold

define Kripke model $\mathcal{C} = \langle C, \subseteq, \Vdash \rangle$ with

- $C = \{\Delta \mid \Gamma \subseteq \Delta$ and $\Delta = \{\psi \mid \Delta \vdash_h \psi\}\}$
- $\Delta \Vdash p$ if $p \in \Delta$ for propositional atoms p

claim: $\Delta \Vdash \psi \iff \psi \in \Delta$ for all $\Delta \in C$ and implicational formulas ψ

proof of claim (induction on ψ): consider $\psi = (\psi_1 \to \psi_2)$

$\Longrightarrow$ let $\Delta \Vdash \psi$ and define $\Delta' = \{\chi \mid \Delta, \psi_1 \vdash_h \chi\}$

$\psi_1 \in \Delta' \in C$ and thus $\Delta' \Vdash \psi_1$ by induction hypothesis

$\Delta' \Vdash \psi_2$ because $\Delta \subseteq \Delta'$ and thus $\psi_2 \in \Delta'$ by induction hypothesis

$\Delta, \psi_1 \vdash_h \psi_2$

$\Delta \vdash_h \psi$ by deduction theorem

Proof ($\Longleftarrow$, cont'd)

suppose $\Gamma \vdash_h \varphi$ does not hold

define Kripke model $\mathcal{C} = \langle C, \subseteq, \Vdash \rangle$ with

- $C = \{\Delta \mid \Gamma \subseteq \Delta$ and $\Delta = \{\psi \mid \Delta \vdash_h \psi\}\}$
- $\Delta \Vdash p$ if $p \in \Delta$ for propositional atoms p

claim: $\Delta \Vdash \psi \iff \psi \in \Delta$ for all $\Delta \in C$ and implicational formulas ψ

proof of claim: consider $\psi = (\psi_1 \to \psi_2)$

$\Longleftarrow$ let $\psi \in \Delta$ and consider state $\Delta' \supseteq \Delta$ with $\Delta' \Vdash \psi_1$

$\psi_1 \in \Delta'$ by induction hypothesis and thus $\Delta' \vdash_h \psi_1$

$\Delta' \vdash_h \psi$ because $\Delta \vdash_h \psi$ and $\Delta \subseteq \Delta'$

$\Delta' \vdash_h \psi_2$ by modus ponens and thus $\psi_2 \in \Delta'$

$\Delta' \Vdash \psi_2$ by induction hypothesis and thus $\Delta' \Vdash \psi$ by definition of $\Vdash$

Proof ($\Longleftarrow$, cont'd)

suppose $\Gamma \vdash_h \varphi$ does not hold

define Kripke model $\mathcal{C} = \langle C, \subseteq, \Vdash \rangle$ with

- $C = \{\Delta \mid \Gamma \subseteq \Delta$ and $\Delta = \{\psi \mid \Delta \vdash_h \psi\}\}$
- $\Delta \Vdash p$ if $p \in \Delta$ for propositional atoms p

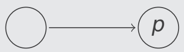
claim: $\Delta \Vdash \psi \iff \psi \in \Delta$ for all $\Delta \in C$ and implicational formulas ψ

define $\Delta = \{\psi \mid \Gamma \vdash_h \psi\}$

$\Delta \in C$ and $\varphi \notin \Delta$ and thus $\Gamma \subseteq \Delta$ and $\Delta \nVdash \varphi$

$\Gamma \nVdash \varphi$ by definition of $\Vdash$

Example (Peirce's Law)

$\nvdash_h ((p \to q) \to p) \to p$ because of Kripke model 

Outline

1. Summary of Previous Lecture
2. Evaluation
3. Hilbert Systems
4. **Curry–Howard Isomorphism**
5. Intuitionistic Propositional Logic
6. Summary

type assignment	Hilbert system
$\Gamma, x : \tau \vdash x : \tau$	$\Gamma, \varphi \vdash \varphi$
$\Gamma \vdash \mathsf{K} : \sigma \to \tau \to \sigma$	$\Gamma \vdash \varphi \to \psi \to \varphi$
$\Gamma \vdash \mathsf{S} : (\sigma \to \tau \to \rho) \to (\sigma \to \tau) \to \sigma \to \rho$	$\Gamma \vdash (\varphi \to \psi \to \chi) \to (\varphi \to \psi) \to \varphi \to \chi$
$\dfrac{\Gamma \vdash t : \sigma \to \tau \qquad \Gamma \vdash u : \sigma}{\Gamma \vdash t\,u : \tau}$	$\dfrac{\Gamma \vdash \varphi \to \psi \qquad \Gamma \vdash \varphi}{\Gamma \vdash \psi}$

Theorem (Curry–Howard)

1. if $\Gamma \vdash t : \tau$ then $\text{types}(\Gamma) \vdash_{\mathsf{h}} \tau$
2. if $\Gamma \vdash_{\mathsf{h}} \varphi$ then $\Delta \vdash t : \varphi$ for some t and Δ with $\text{types}(\Delta) = \Gamma$

Theorem (Curry–Howard)

1. if $\Gamma \vdash t : \tau$ then $\text{types}(\Gamma) \vdash_{\mathsf{h}} \tau$

Proof

induction on derivation of judgement $\Gamma \vdash t : \tau$

- $t = x$ and $\Gamma = \Gamma', x : \tau \implies \text{types}(\Gamma) = \text{types}(\Gamma'), \tau$ and thus $\text{types}(\Gamma) \vdash_{\mathsf{h}} \tau$
- $t = \mathsf{K}$ and $\tau = (\sigma \to \rho \to \sigma) \implies \text{types}(\Gamma) \vdash_{\mathsf{h}} \tau$ by axiom K
- $t = \mathsf{S}$ and $\tau = ((\sigma \to \rho \to \chi) \to (\sigma \to \rho) \to \sigma \to \chi \implies \text{types}(\Gamma) \vdash_{\mathsf{h}} \tau$ by axiom S
- $t = u\,v$ and $\Gamma \vdash u : \sigma \to \tau$ and $\Gamma \vdash v : \sigma$

  $\implies \text{types}(\Gamma) \vdash_{\mathsf{h}} \sigma \to \tau$ and $\text{types}(\Gamma) \vdash_{\mathsf{h}} \sigma$ by induction hypothesis

  $\implies \text{types}(\Gamma) \vdash_{\mathsf{h}} \tau$ by modus ponens

Theorem (Curry–Howard)

2. if $\Gamma \vdash_{\mathsf{h}} \varphi$ then $\Delta \vdash t : \varphi$ for some t and Δ with $\text{types}(\Delta) = \Gamma$

Proof

induction on derivation of $\Gamma \vdash_{\mathsf{h}} \varphi$

interesting case: φ is obtained by modus ponens

$\Gamma \vdash_{\mathsf{h}} \psi \to \varphi$ and $\Gamma \vdash_{\mathsf{h}} \psi$

induction hypothesis: $\Delta_1 \vdash t_1 : \psi \to \varphi$ and $\Delta_2 \vdash t_2 : \psi$
for some t_1, Δ_1, t_2, Δ_2 with $\text{types}(\Delta_1) = \text{types}(\Delta_2) = \Gamma$

suppose $\Gamma = \{\chi_1, \dots, \chi_n\}$

$\Delta_1 = \{x_1 : \chi_1, \dots, x_n : \chi_n\}$ and $\Delta_2 = \{y_1 : \chi_1, \dots, y_n : \chi_n\}$

let t_2' be obtained from t_2 by replacing every y_i with x_i

$\Delta_1 \vdash t_2' : \psi$ and thus $\Delta_1 \vdash t_1\,t_2' : \varphi$

Outline

Definition

Hilbert system for intuitionistic propositional logic consists of modus ponens and axioms

① $\varphi \to \psi \to \varphi$

② $(\varphi \to \psi \to \chi) \to (\varphi \to \psi) \to \varphi \to \chi$

③ $\varphi \wedge \psi \to \varphi$

④ $\varphi \wedge \psi \to \psi$

⑤ $\varphi \to \psi \to \varphi \wedge \psi$

⑥ $\varphi \to \varphi \vee \psi$

⑦ $\psi \to \varphi \vee \psi$

⑧ $(\varphi \to \chi) \to (\psi \to \chi) \to \varphi \vee \psi \to \chi$

⑨ $\bot \to \varphi$

Remarks

- $\neg\varphi$ is shortcut for $\varphi \to \bot$
- adding axiom $\varphi \vee \neg\varphi$ (law of excluded middle) gives (classical) propositional logic
- intuitionistic propositional logic is known as IPC in literature

Theorem

Hilbert system for IPC is sound and complete with respect to Kripke models:

$$\Gamma \vdash_{\mathsf{h}} \varphi \iff \Gamma \Vdash \varphi$$

Theorem (Finite Model Property)

$\vdash_{\mathsf{h}} \varphi \iff \mathcal{C} \Vdash \varphi$ for all finite Kripke models $\mathcal{C}$

Theorem

problem

instance: formula φ

question: $\vdash_{\mathsf{h}} \varphi$?

is decidable and PSPACE-complete

Theorem (Glivenko 1929)

$\vdash \varphi \iff \vdash_{\mathsf{h}} \neg\neg\varphi$

Remark

Glivenko's theorem does not extend to predicate logic

Definition (Gödel's Negative Translation)

- $p^{\mathsf{n}} = \neg\neg p$ for propositional atoms p
- $(\varphi \wedge \psi)^{\mathsf{n}} = \varphi^{\mathsf{n}} \wedge \psi^{\mathsf{n}}$
- $(\varphi \vee \psi)^{\mathsf{n}} = \neg(\neg\varphi^{\mathsf{n}} \wedge \neg\psi^{\mathsf{n}})$
- $(\varphi \to \psi)^{\mathsf{n}} = \varphi^{\mathsf{n}} \to \psi^{\mathsf{n}}$
- $\bot^{\mathsf{n}} = \bot$

Theorem

$\vdash \varphi \iff \vdash_{\mathsf{h}} \varphi^{\mathsf{n}}$

Outline

Important Concepts

- φ^{n}
- $\vdash_h$
- Curry–Howard isomorphism
- finite model property
- Glivenko's theorem
- Gödel's negative translation
- Hilbert system
- intuitionistic propositional logic

homework for January 15