WS 2023 lecture 10

Computability Theory

Aart Middeldorp

Outline

Definitions

- (many-step) strategy $\mathcal{S}$ for ARS $\mathcal{A} = \langle A, \to \rangle$ is relation $\to_{\mathcal{S}}$ on A such that $\to_{\mathcal{S}} \subseteq \to^{+}$ and $\mathrm{NF}(\to_{\mathcal{S}}) = \mathrm{NF}(\mathcal{A})$
- one-step strategy satisfies $\to_{\mathcal{S}} \subseteq \to$
- strategy $\mathcal{S}$ is deterministic if $a = b$ whenever $a \;{}_{\mathcal{S}}\!\leftarrow \cdot \to_{\mathcal{S}} b$
- strategy $\mathcal{S}$ for ARS $\mathcal{A}$ is normalizing if every normalizing element is $\mathcal{S}$–terminating
- strategy $\mathcal{S}$ for ARS $\mathcal{A}$ is hyper–normalizing if every normalizing element is terminating with respect to $\to^{*} \cdot \to_{\mathcal{S}} \cdot \to^{*}$
- strategy $\mathcal{S}_{\bullet}$ for ARS $\mathcal{A}$ with Z property for $\bullet$: $a \to_{\bullet} b$ if $a \notin \mathrm{NF}(\mathcal{A})$ and $b = a^{\bullet}$
- root reduction $\xrightarrow{\epsilon}$: $\mathsf{I}\,t \xrightarrow{\epsilon} t$ $\quad \mathsf{K}\,t\,u \xrightarrow{\epsilon} t$ $\quad \mathsf{S}\,t\,u\,v \xrightarrow{\epsilon} t\,v\,(u\,v)$
- leftmost outermost reduction $\xrightarrow{\mathsf{lo}}$:

$$\frac{t \xrightarrow{\epsilon} u}{t \xrightarrow{\mathsf{lo}} u} \qquad \frac{t \xrightarrow{\mathsf{lo}} u \quad t\,v \in \mathrm{NF}(\xrightarrow{\epsilon})}{t\,v \xrightarrow{\mathsf{lo}} u\,v} \qquad \frac{t \xrightarrow{\mathsf{lo}} u \quad v\,t \in \mathrm{NF}(\xrightarrow{\epsilon}) \quad v \in \mathrm{NF}(\to)}{v\,t \xrightarrow{\mathsf{lo}} v\,u}$$

- $t \xrightarrow{\neg\mathsf{lo}} u$ if $t \to u$ but not $t \xrightarrow{\mathsf{lo}} u$

Theorem

$\mathcal{S}_{\bullet}$ is hyper–normalizing for every ARS with Z property for $\bullet$

Theorem (Factorization)

$\to^{*} \subseteq \xrightarrow{\mathsf{lo}}{}^{*} \cdot \xrightarrow{\neg\mathsf{lo}}{}^{*}$

Normalization Theorem

leftmost outermost reduction is hyper–normalizing

Theorem

partial recursive functions are CL–representable by combinators in normal form

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

Theorem

function φ is partial recursive $\iff$ φ is CL–representable

Remark (Hindley and Seldin, CUP 2008)

> *The main theorem of this chapter will be that every partial recursive function can be represented in both λ and CL.*
>
> *The converse is also true, that every function representable in λ or CL is partial recursive. But its proof is too boring to include in this book.*

Definition

Gödel number of CL–term is defined inductively:

$$\mathfrak{g}(\mathsf{I}) = \langle 0 \rangle \qquad \mathfrak{g}(\mathsf{K}) = \langle 1 \rangle \qquad \mathfrak{g}(\mathsf{S}) = \langle 2 \rangle \qquad \mathfrak{g}(t\,u) = \langle 3, \mathfrak{g}(t), \mathfrak{g}(u) \rangle \qquad \mathfrak{g}(x_i) = \langle 4, i \rangle$$

Definition

predicates $\mathsf{I}(x)$, $\mathsf{K}(x)$, $\mathsf{S}(x)$, $\mathsf{A}(x)$, $\mathsf{V}(x)$, $\mathsf{term}(x)$ are defined inductively:

$$\begin{aligned}
\mathsf{I}(x) &\iff \mathsf{seq}(x) \wedge \mathsf{len}(x) = 1 \wedge (x)_1 = 0 \\
\mathsf{K}(x) &\iff \mathsf{seq}(x) \wedge \mathsf{len}(x) = 1 \wedge (x)_1 = 1 \\
\mathsf{S}(x) &\iff \mathsf{seq}(x) \wedge \mathsf{len}(x) = 1 \wedge (x)_1 = 2 \\
\mathsf{A}(x) &\iff \mathsf{triple}(x) \wedge (x)_1 = 3 \wedge \mathsf{term}((x)_2) \wedge \mathsf{term}((x)_3) \\
\mathsf{V}(x) &\iff \mathsf{seq}(x) \wedge \mathsf{len}(x) = 2 \wedge (x)_1 = 4 \\
\mathsf{term}(x) &\iff \mathsf{I}(x) \vee \mathsf{K}(x) \vee \mathsf{S}(x) \vee \mathsf{A}(x) \vee \mathsf{V}(x)
\end{aligned}$$

$$\frac{}{\mathsf{I}\,t \to t} \qquad \frac{}{\mathsf{K}\,t\,u \to t} \qquad \frac{}{\mathsf{S}\,t\,u\,v \to t\,v\,(u\,v)} \qquad \frac{t \to u}{t\,v \to u\,v} \qquad \frac{t \to u}{v\,t \to v\,u}$$

Definition

predicate $\mathsf{step}(x,y)$ is inductively defined:

$$\begin{aligned}\mathsf{step}(x,y) \iff\ & \mathsf{term}(x) \wedge \mathsf{term}(y) \wedge \mathsf{A}(x) \wedge \\ & \Big[\ \big[\mathsf{I}((x)_2) \wedge (x)_3 = y\big] \\ & \vee \big[\mathsf{A}((x)_2) \wedge \mathsf{K}((x)_{2,2}) \wedge (x)_{2,3} = y\big] \\ & \vee \big[\mathsf{A}((x)_2) \wedge \mathsf{A}((x)_{2,2}) \wedge \mathsf{S}((x)_{2,2,2}) \wedge \mathsf{A}(y) \wedge \mathsf{A}((y)_2) \wedge \mathsf{A}((y)_3) \wedge \\ & \quad (x)_{2,2,3} = (y)_{2,2} \wedge (x)_{2,3} = (y)_{3,2} \wedge (x)_3 = (y)_{2,3} \wedge (x)_3 = (y)_{3,3}\big] \\ & \vee \big[\mathsf{A}(y) \wedge \mathsf{step}((x)_2,(y)_2) \wedge (x)_3 = (y)_3\big] \\ & \vee \big[\mathsf{A}(y) \wedge (x)_2 = (y)_2 \wedge \mathsf{step}((x)_3,(y)_3)\big]\ \Big]\end{aligned}$$

Definitions

- predicates $\mathsf{reduction}(x)$ and $\mathsf{conversion}(x)$

$$\begin{aligned}\mathsf{reduction}(x) &\iff \mathsf{seq}(x) \wedge (\forall\, i < \mathsf{len}(x) \dot{-} 1)\ [\ \mathsf{step}((x)_i,(x)_{i+1})\ ] \\ \mathsf{conversion}(x) &\iff \mathsf{seq}(x) \wedge (\forall\, i < \mathsf{len}(x) \dot{-} 1)\ [\ \mathsf{step}((x)_i,(x)_{i+1}) \vee \mathsf{step}((x)_{i+1},(x)_i)\ ]\end{aligned}$$

- predicates $\mathsf{zero}(x)$ and $\mathsf{numeral}(x)$

$$\begin{aligned}\mathsf{zero}(x) &\iff \mathsf{A}(x) \wedge \mathsf{K}((x)_2) \wedge \mathsf{I}((x)_3) \\ \mathsf{numeral}(x) &\iff \mathsf{zero}(x) \vee \big[\mathsf{A}(x) \wedge \mathsf{A}((x)_2) \wedge \mathsf{S}((x)_{2,2}) \wedge \mathsf{B}((x)_{2,3}) \wedge \mathsf{numeral}((x)_3)\big]\end{aligned}$$

- $\mathsf{enc}(n) = \mathfrak{g}(\underline{n})$

Example

$\mathsf{enc}(0) = \mathfrak{g}(\mathsf{KI}) = \langle 3, \langle 1 \rangle, \langle 0 \rangle \rangle = 18375000$

Definition

- function $\mathsf{dec}\colon \mathbb{N} \to \mathbb{N}$

$$\mathsf{dec}(x) = \begin{cases} 0 & \text{if } \mathsf{zero}(x) \\ \mathsf{dec}((x)_3) + 1 & \text{if } \mathsf{numeral}(x) \wedge \neg\mathsf{zero}(x) \\ 0 & \text{otherwise} \end{cases}$$

Theorem

CL–representable functions are partial recursive

Proof

$$\mathsf{first}(x) = (x)_1 \quad \mathsf{last}(x) = (x)_{\mathsf{len}(x)} \quad \mathfrak{g}(F\,\underline{x_1}\cdots\underline{x_n}) = \langle 3, \dots \langle 3, \mathfrak{g}(F), \mathsf{enc}(x_1)\rangle, \dots \mathsf{enc}(x_n)\rangle$$

$$f(x_1,\dots,x_n) \simeq \mathsf{dec}(\mathsf{last}((\mu\, i)\ [\mathsf{reduction}(i) \wedge \mathsf{first}(i) = \mathfrak{g}(F\,\underline{x_1}\cdots\underline{x_n}) \wedge \mathsf{numeral}(\mathsf{last}(i))]))$$

Outline

Notation

$\ulcorner t \urcorner = \mathfrak{g}(t)$ is Church numeral of Gödel number of CL–term t

Theorem

$\forall$ CL–term F $\exists$ CL–term X such that $F \ulcorner X \urcorner \leftrightarrow^* X$

Proof

- primitive recursive function $a(x, y) = \langle 3, x, y \rangle$ is represented by combinator A
- $\mathsf{A} \ulcorner t \urcorner \ulcorner u \urcorner \leftrightarrow^* \langle 3, \mathfrak{g}(t), \mathfrak{g}(u) \rangle = \mathfrak{g}(t\,u) = \ulcorner t\,u \urcorner$
- primitive recursive function $\mathrm{enc}(x) = \mathfrak{g}(x)$ is represented by combinator E
- $\mathsf{E} \ulcorner t \urcorner \leftrightarrow^* \mathfrak{g}(\mathfrak{g}(t)) = \ulcorner\ulcorner t \urcorner\urcorner$
- $Y = \langle x \rangle (F\,(\mathsf{A}\,x\,(\mathsf{E}\,x)))$ and $X = Y \ulcorner Y \urcorner$
- $X \leftrightarrow^* F\,(\mathsf{A} \ulcorner Y \urcorner (\mathsf{E} \ulcorner Y \urcorner)) \leftrightarrow^* F\,(\mathsf{A} \ulcorner Y \urcorner \ulcorner\ulcorner Y \urcorner\urcorner) \leftrightarrow^* F \ulcorner Y \ulcorner Y \urcorner\urcorner = F \ulcorner X \urcorner$

Outline

Definitions

- sets T and U of CL–terms are recursively separable if $\{\mathfrak{g}(t) \mid t \in T\}$ and $\{\mathfrak{g}(u) \mid u \in U\}$ are recursively separable
- set T of CL–terms is conversion–closed if $u \in T$ whenever $t \in T$ and $t \leftrightarrow^* u$

Theorem

non-empty conversion–closed sets of CL–terms are recursively inseparable

Proof (by contradiction)

- non-empty conversion–closed sets T and U of CL–terms
- $\exists$ recursive function $f \colon \mathbb{N} \to \{0, 1\}$ such that

$$t \in T \implies f(\mathfrak{g}(t)) = 0 \qquad t \in U \implies f(\mathfrak{g}(t)) = 1$$

- $V = \{t \mid f(\mathfrak{g}(t)) = 0\}$

Proof (cont'd)

- $T \subseteq V$ and $U \cap V = \varnothing$
- f is represented by F

$$t \in V \implies F \ulcorner t \urcorner \leftrightarrow^* \underline{0} \qquad t \notin V \implies F \ulcorner t \urcorner \leftrightarrow^* \underline{1}$$

- $A \in T$ and $B \in U$
- $G = \langle x \rangle (\text{zero?}\,(F\,x)\,B\,A))$

$$t \in V \implies G \ulcorner t \urcorner \leftrightarrow^* B \qquad t \notin V \implies G \ulcorner t \urcorner \leftrightarrow^* A$$

- $\exists X$ such that $G \ulcorner X \urcorner \leftrightarrow^* X$ by fixed point theorem

$$X \in V \implies X \leftrightarrow^* G \ulcorner X \urcorner \leftrightarrow^* B \implies X \in U \implies X \notin V$$
$$X \notin V \implies X \leftrightarrow^* G \ulcorner X \urcorner \leftrightarrow^* A \implies X \in T \implies X \in V \qquad \lightning$$

Theorem

non-trivial conversion–closed sets of CL–terms are not recursive

Proof

- non-trivial conversion–closed set T of CL–terms
- $\sim T = \{t \mid t \notin T\}$ is non-empty conversion–closed set of CL–terms
- T and $\sim T$ are recursively inseparable $\implies$ T is not recursive

Corollary

set of normalizing CL–terms is not recursive: decision problem

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

is undecidable

Outline

Definition (Types)

- infinite set $\mathbb{V}$ of type variables
- set $\mathbb{C}$ of type constants
- set $\mathbb{T}$ of types is defined inductively:
  - $\mathbb{V} \subseteq \mathbb{T}$
  - $\mathbb{C} \subseteq \mathbb{T}$
  - if $\sigma, \tau \in \mathbb{T}$ then $(\sigma \to \tau) \in \mathbb{T}$

Notation

- outermost parentheses are omitted
- $\to$ is right-associative: $\rho \to \sigma \to \tau$ stands for $\rho \to (\sigma \to \tau)$

Definition (Type Assignment, Curry-style)

- type assignment formula $t : \tau$ with CL–term t and type τ
- type assignment system TA

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

$$\frac{t : \sigma \to \tau \qquad u : \sigma}{t\,u : \tau}$$

for all types σ, τ, ρ and CL–terms t and u

Notation

$\Gamma \vdash t : \tau$ if $t : \tau$ can be derived in TA from assumptions in Γ

Example ①

$\vdash \mathsf{SKK} : \sigma \to \sigma$ for all types σ

$$\dfrac{\dfrac{\dfrac{}{\mathsf{S} : (\sigma \to (\sigma \to \sigma) \to \sigma) \to (\sigma \to \sigma \to \sigma) \to \sigma \to \sigma} \qquad \dfrac{}{\mathsf{K} : \sigma \to (\sigma \to \sigma) \to \sigma}}{\mathsf{SK} : (\sigma \to \sigma \to \sigma) \to \sigma \to \sigma} \qquad \dfrac{}{\mathsf{K} : \sigma \to \sigma \to \sigma}}{\mathsf{SKK} : \sigma \to \sigma}$$

Example ②

$x : \sigma \to \tau,\ y : \sigma \vdash \mathsf{K}x\mathsf{I}y : \tau$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\mathsf{K} : (\sigma \to \tau) \to (\rho \to \rho) \to \sigma \to \tau} \qquad x : \sigma \to \tau}{\mathsf{K}x : (\rho \to \rho) \to \sigma \to \tau} \qquad \dfrac{}{\mathsf{I} : \rho \to \rho}}{\mathsf{K}x\mathsf{I} : \sigma \to \tau} \qquad y : \sigma}{\mathsf{K}x\mathsf{I}y : \tau}$$

Theorem

if $\Gamma, x : \sigma \vdash t : \tau$ and $x \notin \mathcal{V}\mathrm{ar}(\Gamma)$ then $\Gamma \vdash [x]t : \sigma \to \tau$

Proof

induction on definition of $[x]t$

① $t = x \implies [x]t = \mathsf{I}$ and $\sigma = \tau \implies \vdash \mathsf{I} : \sigma \to \tau \implies \Gamma \vdash \mathsf{I} : \sigma \to \tau$

② $x \notin \mathcal{V}\mathrm{ar}(t) \implies [x]t = \mathsf{K}t$ and $\Gamma \vdash t : \tau$

$\vdash \mathsf{K} : \tau \to \sigma \to \tau \implies \Gamma \vdash \mathsf{K}t : \sigma \to \tau$

③ $t = t_1 t_2 \implies [x]t = \mathsf{S}([x]t_1)([x]t_2)$ and $\Gamma, x : \sigma \vdash t_1 : \tau_1 \to \tau$ and $\Gamma, x : \sigma \vdash t_2 : \tau_1$

$\Gamma \vdash [x]t_1 : \sigma \to \tau_1 \to \tau$ and $\Gamma \vdash [x]t_2 : \sigma \to \tau_1$ by induction hypothesis

$\vdash \mathsf{S} : (\sigma \to \tau_1 \to \tau) \to (\sigma \to \tau_1) \to \sigma \to \tau \implies \Gamma \vdash \mathsf{S}([x]t_1)([x]t_2) : \sigma \to \tau$

Theorem (Subject Reduction)

if $\Gamma \vdash t : \tau$ and $t \to u$ then $\Gamma \vdash u : \tau$

Proof

① $t = \mathsf{I}t_1 \to t_1 = u \implies \vdash \mathsf{I} : \sigma \to \tau$ and $\Gamma \vdash t_1 : \sigma \implies \sigma = \tau \implies \Gamma \vdash u : \tau$

② $t = \mathsf{K}t_1t_2 \to t_1 = u \implies \Gamma \vdash \mathsf{K}t_1 : \sigma \to \tau$ and $\Gamma \vdash t_2 : \sigma$

$\implies \vdash \mathsf{K} : \rho \to \sigma \to \tau$ and $\Gamma \vdash t_1 : \rho \implies \rho = \tau \implies \Gamma \vdash u : \tau$

③ $t = \mathsf{S}t_1t_2t_3 \to t_1t_3(t_2t_3) = u \implies \Gamma \vdash \mathsf{S}t_1t_2 : \sigma \to \tau$ and $\Gamma \vdash t_3 : \sigma$

$\implies \Gamma \vdash \mathsf{S}t_1 : \rho \to \sigma \to \tau$ and $\Gamma \vdash t_2 : \rho \implies \vdash \mathsf{S} : \mu \to \rho \to \sigma \to \tau$ and $\Gamma \vdash t_1 : \mu$

$\implies \rho = \sigma \to \rho_1$ and $\mu = \sigma \to \rho_1 \to \tau \implies \Gamma \vdash t_1t_3 : \rho_1 \to \tau$ and $\Gamma \vdash t_2t_3 : \rho_1$

$\implies \Gamma \vdash u : \tau$

④ $t = t_1t_2 \to u_1t_2 = u$ with $t_1 \to u_1 \implies \Gamma \vdash t_1 : \sigma \to \tau$ and $\Gamma \vdash t_2 : \sigma$

$\implies \Gamma \vdash u_1 : \sigma \to \tau$ by induction hypothesis $\implies \Gamma \vdash u : \tau$

Theorem (Subject Reduction)

if $\Gamma \vdash t : \tau$ and $t \to u$ then $\Gamma \vdash u : \tau$

Proof (cont'd)

⑤ $t = t_1t_2 \to t_1u_2 = u$ with $t_2 \to u_2 \implies \Gamma \vdash t_1 : \sigma \to \tau$ and $\Gamma \vdash t_2 : \sigma$

$\implies \Gamma \vdash u_2 : \sigma$ by induction hypothesis $\implies \Gamma \vdash u : \tau$

Definition

CL–term t with $\mathcal{V}\mathrm{ar}(t) = \{x_1, \ldots, x_n\}$ is typable if

$$x_1 : \rho_1, \ldots, x_n : \rho_n \vdash t : \tau$$

for some types $\rho_1, \ldots, \rho_n, \tau$

Outline

Important Concepts

- $\ulcorner t \urcorner$
- arithmetization
- $\mathbb{C}$
- conversion–closed
- dec(n)
- enc(n)
- $\Gamma \vdash t : \tau$
- $\mathfrak{g}(t)$
- Gödel number
- recursive separability
- SN
- subject reduction
- $\mathbb{T}$
- TA
- type
- type assignment
- type constant
- $\mathbb{V}$

homework for December 11