universität innsbruck

Computability Theory

Aart Middeldorp

Outline

Definition (Parallel Reduction)

- $t \twoheadrightarrow\!\!\!\!\!\!\!+\; t$ for all $t \in \{\mathsf{S}, \mathsf{K}, \mathsf{I}\} \cup \mathcal{V}$
- $\mathsf{I}\, t \twoheadrightarrow\!\!\!\!\!\!\!+\; t \quad \mathsf{K}\, t\, u \twoheadrightarrow\!\!\!\!\!\!\!+\; t \quad \mathsf{S}\, t\, u\, v \twoheadrightarrow\!\!\!\!\!\!\!+\; t\, v\, (u\, v)$ for all CL–terms t, u, v
- $t_1\, t_2 \twoheadrightarrow\!\!\!\!\!\!\!+\; u_1\, u_2$ if $t_1 \twoheadrightarrow\!\!\!\!\!\!\!+\; u_1$ and $t_2 \twoheadrightarrow\!\!\!\!\!\!\!+\; u_2$ for all CL–terms t_1, t_2, u_1, u_2

Lemmata

- $\rightarrow \;\subseteq\; \twoheadrightarrow\!\!\!\!\!\!\!+ \;\subseteq\; \rightarrow^*$
- $\twoheadrightarrow\!\!\!\!\!\!\!+$ has diamond property

Corollary

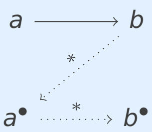
CL is confluent

Definition

ARS $\mathcal{A} = \langle A, \rightarrow \rangle$ has Z property if

$$a \rightarrow b \quad \Longrightarrow \quad b \rightarrow^* \bullet(a) \rightarrow^* \bullet(b)$$

for some function $\bullet$ on A



Lemma (Monotonicity)

$a \rightarrow^* b \quad \Longrightarrow \quad a^\bullet \rightarrow^* b^\bullet$ for every ARS $\langle A, \rightarrow \rangle$ with Z property for $\bullet$

Definition

functions $\diamond$ and $\star$ on CL–terms:

$$t^\diamond = \begin{cases} u^\diamond \star v^\diamond & \text{if } t = u\,v \\ t & \text{otherwise} \end{cases}$$

$$s \star t = \begin{cases} u\,t\,(v\,t) & \text{if } s = \mathsf{S}\,u\,v \\ u & \text{if } s = \mathsf{K}\,u \\ t & \text{if } s = \mathsf{I} \\ s\,t & \text{otherwise} \end{cases}$$

Lemma

every ARS with Z property is confluent

Theorem

CL has Z property for $\diamond$

Definition

recursion combinator is combinator R such that

$$R\ x\ y\ \underline{0} \leftrightarrow^* x \qquad\qquad R\ x\ y\ \underline{n+1} \leftrightarrow^* y\ \underline{n}\ (R\ x\ y\ \underline{n})$$

Lemma

if R is recursion combinator then

$$F = \langle z\, y_1\, \dots\, y_n \rangle (R\ (G\, y_1 \cdots y_n)\ \langle u\, v \rangle (H\, v\, u\, y_1 \cdots y_n)\ z)$$

represents primitive recursive function f based on g and h

Definitions

$$\mathsf{D} = \langle x\,y\,z\rangle(z\,(\mathsf{K}\,y)\,x) = \mathsf{C}(\mathsf{BC}(\mathsf{B}(\mathsf{CI})\mathsf{K})) \qquad \text{(pairing combinator)}$$

$$\mathsf{Q} = \langle x\,y\rangle(\mathsf{D}\,(\mathsf{succ}\,(y\,\underline{0}))\,(x\,(y\,\underline{0})\,(y\,\underline{1})))$$

$$\mathsf{R} = \langle x\,y\,z\rangle(z\,(\mathsf{Q}\,y)\,(\mathsf{D}\,\underline{0}\,x)\,\underline{1})$$

Lemmata

- $\mathsf{D}\,x\,y\,\underline{0} \to^+ x$
- $\mathsf{D}\,x\,y\,\underline{n} \to^+ y$ for all $n > 0$
- $\mathsf{Q}\,x\,(\mathsf{D}\,\underline{n}\,y) \to^+ \mathsf{D}\,\underline{n+1}\,(x\,\underline{n}\,y)$
- R is recursion combinator

Lemma

CL–representable functions are closed under minimization

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

Definitions

- (many-step) strategy $\mathcal{S}$ for ARS $\mathcal{A} = \langle A, \to \rangle$ is relation $\to_{\mathcal{S}}$ such that
  1. $\to_{\mathcal{S}} \subseteq \to^+$
  2. $\mathrm{NF}(\to_{\mathcal{S}}) = \mathrm{NF}(\mathcal{A})$
- 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 $\to^* \cdot \to_{\mathcal{S}} \cdot \to^*$

Lemma

hyper–normalization $\implies$ normalization

Definition

strategy $\mathcal{S}_{\bullet}$ for ARS $\mathcal{A}$ with Z property for $\bullet$: $a \xrightarrow{\bullet} b$ if $a \notin \mathrm{NF}(\mathcal{A})$ and $b = a^{\bullet}$

Theorem

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

Proof

① $a \to^n b$ and $n > 0 \implies b \to^* \bullet^n(a)$ by induction on n:

$a \to c \to^{n-1} b \implies c \to^* \bullet(a)$ (Z property)

- $n = 1 \implies b = c$
- $n > 1 \implies b \to^* \bullet^{n-1}(c)$ (induction hypothesis)

$\bullet^{n-1}(c) \to^* \bullet^n(a) \implies b \to^* \bullet^n(a)$ ($n - 1$ applications of monotonicity)

Theorem

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

Proof (cont'd)

① $a \to^n b$ and $n > 0 \quad \Longrightarrow \quad b \to^* \bullet^n(a)$

② $a \twoheadrightarrow_\bullet^{\leqslant n} \bullet^n(a)$ for all $n \geqslant 0$ by induction on n

- $n = 0 \quad \Longrightarrow \quad a = \bullet^n(a)$
- $n > 0 \quad \Longrightarrow \quad a \twoheadrightarrow_\bullet^{\leqslant n-1} \bullet^{n-1}(a) \twoheadrightarrow_\bullet^{=} \bullet^{n-1}(a)^\bullet = \bullet^n(a)$ (induction hypothesis)

③ $a \to^n b$ with $n > 0$ and $b \in \mathrm{NF}(\to)$

$a \twoheadrightarrow_\bullet^{\leqslant n} \bullet^n(a) \;{}^*\!\!\leftarrow b \quad \Longrightarrow \quad a \twoheadrightarrow_\bullet^{\leqslant n} b \quad \Longrightarrow \quad \mathcal{S}_\bullet$ is normalizing

Theorem

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

Theorem

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

Proof (sketch)

① $\to^* \cdot \xrightarrow{\bullet} \subseteq \xrightarrow{\bullet} \cdot \to^*$

- suppose $a \to^* b \xrightarrow{\bullet} c$
- $b \notin \mathsf{NF} \implies a \notin \mathsf{NF} \implies a \xrightarrow{\bullet} \bullet(a) \to^* \bullet(b) = c$ (monotonicity)

② $\mathcal{S}_\bullet$ is normalizing strategy $\implies$ $\mathcal{S}_\bullet$ is hyper−normalizing strategy

Outline

Definition

- root reduction $\xrightarrow{\epsilon}$: $\quad \mathsf{I}\,t \xrightarrow{\epsilon} t \quad \mathsf{K}\,t\,u \xrightarrow{\epsilon} t \quad \mathsf{S}\,t\,u\,v \xrightarrow{\epsilon} t\,v\,(u\,v)$
- leftmost outermost reduction $\xrightarrow{\text{lo}}$:

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

for all CL–terms t, u, v

Example

$$\cfrac{\cfrac{\cfrac{}{\mathsf{KI}(\mathsf{IS}) \xrightarrow{\epsilon} \mathsf{I}}}{\mathsf{KI}(\mathsf{IS}) \xrightarrow{\text{lo}} \mathsf{I}} \qquad \cfrac{}{\mathsf{KI}(\mathsf{IS})\mathsf{I} \in \mathsf{NF}(\xrightarrow{\epsilon})}}{\mathsf{KI}(\mathsf{IS})\mathsf{I} \xrightarrow{\text{lo}} \mathsf{II}} \qquad \cfrac{}{\mathsf{K}(\mathsf{KI}(\mathsf{IS})\mathsf{I}) \in \mathsf{NF}(\xrightarrow{\epsilon})} \qquad \cfrac{}{\mathsf{K} \in \mathsf{NF}(\to)}$$
$$\overline{\mathsf{K}(\mathsf{KI}(\mathsf{IS})\mathsf{I}) \xrightarrow{\text{lo}} \mathsf{K}(\mathsf{II})}$$

Definition

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

Example

$$
\begin{aligned}
\mathsf{SSSSSSSS} &\xrightarrow{\mathsf{lo}} \mathsf{SS(SS)SSSS} \xrightarrow{\mathsf{lo}} \mathsf{SS(SSS)SSS} \xrightarrow{\mathsf{lo}} \mathsf{SS(SSSS)SS} \\
&\xrightarrow{\neg\mathsf{lo}} \mathsf{SS(SS(SS))SS} \xrightarrow{\mathsf{lo}} \mathsf{SS(SS(SS)S)S} \xrightarrow{\neg\mathsf{lo}} \mathsf{SS(SS(SSS))S} \\
&\xrightarrow{\mathsf{lo}} \mathsf{SS(SS(SSS)S)} \xrightarrow{\mathsf{lo}} \mathsf{SS(SS(SSSS))} \xrightarrow{\mathsf{lo}} \mathsf{SS(SS(SS(SS)))}
\end{aligned}
$$

Theorem (Factorization)

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

Theorem

leftmost outermost reduction is normalizing

Proof

- assume $t \to^! u \implies t \xrightarrow{\text{lo}}^* \cdot \xrightarrow{\neg\text{lo}}^* u$ by factorization
- u is normal form $\implies v \xrightarrow{\neg\text{lo}} u$ is impossible $\implies t \xrightarrow{\text{lo}}^* u$

Theorem

leftmost outermost reduction is hyper−normalizing

Proof

infinite reduction

$$t \xrightarrow{\neg\text{lo}}^* \cdot \xrightarrow{\text{lo}} \cdot \xrightarrow{\neg\text{lo}}^* \cdot \xrightarrow{\text{lo}} \cdot \xrightarrow{\neg\text{lo}}^* \cdots$$

gives rise to infinite $\xrightarrow{\text{lo}}$ reduction starting from t by factorization

Example

combinator $\mathsf{SII}(\mathsf{SII})$ is not normalizing:

$$\mathsf{SII}(\mathsf{SII}) \xrightarrow{\text{lo}} \mathsf{I}(\mathsf{SII})(\mathsf{I}(\mathsf{SII})) \xrightarrow{\text{lo}} \mathsf{SII}(\mathsf{I}(\mathsf{SII})) \longrightarrow \mathsf{SII}(\mathsf{SII})$$

Outline

Definition

$$T = \langle x \rangle (\mathsf{D}\ \underline{0}\ (\langle u\,v \rangle (u\ (x\ (\mathsf{succ}\ v))\ u\ (\mathsf{succ}\ v)))) \qquad P = \langle x\,y \rangle (T\ x\ (x\ y)\ (T\ x)\ y)$$

Lemma

$$P\ x\ y \leftrightarrow^* \begin{cases} y & \text{if } x\ y \to^* \underline{0} \\ P\ x\ (\mathsf{succ}\ y) & \text{if } x\ y \to^* \underline{n+1} \end{cases}$$

Proof

- $P\ x\ y \to^* \mathsf{D}\ \underline{0}\ (\langle u\,v \rangle (u\ (x\ (\mathsf{succ}\ v))\ u\ (\mathsf{succ}\ v)))\ (x\ y)\ (T\ x)\ y$
- $x\ y \to^* \underline{0} \implies P\ x\ y \to^* \underline{0}\ (T\ x)\ y \to^* y$
- $x\ y \to^* \underline{n+1} \implies P\ x\ y \to^* (\langle u\,v \rangle (u\ (x\ (\mathsf{succ}\ v))\ u\ (\mathsf{succ}\ v)))\ (T\ x)\ y$
  $\to^* T\ x\ (x\ (\mathsf{succ}\ y))\ (T\ x)\ (\mathsf{succ}\ y) \leftrightarrow^* P\ x\ (\mathsf{succ}\ y)$

Theorem

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

Proof

partial recursive function $\varphi(x_1,\ldots,x_n) \simeq \mathrm{u}((\mu\, i)\,(g(x_1,\ldots,x_n,i) = 0))$

with primitive recursive functions u and g that are represented by combinators U and G

- $F_1 = \langle x_1 \cdots x_n \rangle (\mathrm{U}\ (P\ (G\ x_1 \cdots x_n)\ \underline{0}))$
- $F_2 = \langle x_1 \cdots x_n \rangle (P\ (G\ x_1 \cdots x_n)\ \underline{0}\ \mathsf{I}\ (F_1\ x_1 \cdots x_n))$ represents φ
- $A = G\ \underline{x_1} \cdots \underline{x_n}$ and $B = F_1\ \underline{x_1} \cdots \underline{x_n}$
- case 1: $\varphi(x_1,\ldots,x_n){\downarrow}$

  $\varphi(x_1,\ldots,x_n) = \mathrm{u}(y)$ for $y = (\mu\, i)\,(g(x_1,\ldots,x_n,i) = 0)$

$$F_2\ \underline{x_1} \cdots \underline{x_n} \to^* P\ A\ \underline{0}\ \mathsf{I}\ B \leftrightarrow^* P\ A\ \underline{y}\ \mathsf{I}\ B \leftrightarrow^* \underline{y}\ \mathsf{I}\ B \to^* \mathsf{I}^y\ B \to^* B$$
$$\to^* \mathrm{U}\ (P\ A\ \underline{0}) \leftrightarrow^* \mathrm{U}\ \underline{y} \to^* \underline{\mathrm{u}(y)} = \underline{\varphi(x_1,\ldots,x_n)}$$

Proof (cont'd)

partial recursive function $\varphi(x_1,\ldots,x_n) \simeq \mathsf{u}((\mu\, i)\,(g(x_1,\ldots,x_n,i) = 0))$

with primitive recursive functions u and g that are represented by U and G

- $F_1 = \langle x_1 \cdots x_n \rangle (\mathsf{U}\,(P\,(G\,x_1 \cdots x_n)\,\underline{0}))$
- $F_2 = \langle x_1 \cdots x_n \rangle (P\,(G\,x_1 \cdots x_n)\,\underline{0}\;\mathsf{I}\;(F_1\,x_1 \cdots x_n))$ represents φ
- $A = G\,\underline{x_1} \cdots \underline{x_n}$ and $B = F_1\,\underline{x_1} \cdots \underline{x_n}$
- case 2: $\varphi(x_1,\ldots,x_n)\uparrow$

$$\begin{aligned} F_2\,\underline{x_1} \cdots \underline{x_n} &\to^* P\,A\,\underline{0}\;\mathsf{I}\;B \to^* T\,A\,(A\,\underline{0})\,(T\,A)\,\underline{0}\;\mathsf{I}\;B \to^* T\,A\,\underline{m+1}\,(T\,A)\,\underline{0}\;\mathsf{I}\;B \\ &\to^* \mathsf{D}\,\underline{0}\,(\langle u\,v\rangle(u\,(A\,(\mathsf{succ}\,v))\,u\,(\mathsf{succ}\,v)))\,\underline{m+1}\,(T\,A)\,\underline{0}\;\mathsf{I}\;B \\ &\to^* \langle u\,v\rangle(u\,(A\,(\mathsf{succ}\,v))\,u\,(\mathsf{succ}\,v))\,(T\,A)\,\underline{0}\;\mathsf{I}\;B \\ &\to^* T\,A\,(A\,(\mathsf{succ}\,\underline{0}))\,(T\,A)\,(\mathsf{succ}\,\underline{0})\;\mathsf{I}\;B \\ &\to^* T\,A\,(A\,\underline{1})\,(T\,A)\,\underline{1}\;\mathsf{I}\;B \to^* \cdots \to^* T\,A\,(A\,\underline{2})\,(T\,A)\,\underline{2}\;\mathsf{I}\;B \to^* \cdots \end{aligned}$$

contains $\xrightarrow{\mathsf{lo}}$ step $\implies$ $F_2\,\underline{x_1} \cdots \underline{x_n}$ has no normal form by hyper-normalization of $\xrightarrow{\mathsf{lo}}$

Outline

Important Concepts

- $\xrightarrow{\epsilon}$
- $\xrightarrow{\mathsf{lo}}$
- $\xrightarrow{\neg\mathsf{lo}}$
- deterministic
- factorization
- hyper–normalization
- normalization
- leftmost outermost reduction
- normalization theorem
- P
- root reduction
- $\mathcal{S}_\bullet$
- strategy
- T

homework for December 4