universität innsbruck

26W lecture 7



Computability Theory

Aart Middeldorp

Outline

1. **Summary of Previous Lecture**
2. **Combinatory Logic**
3. **Combinators**
4. **Church Numerals**
5. **Combinatorial Completeness**
6. **CL–Representability**
7. **Confluence**
8. **Summary**

Definitions

- set $A \subseteq \mathbb{N}$ is recursive if its characteristic function χ_A is recursive
- disjoint sets $A, B \subseteq \mathbb{N}$ are recursively separable if there exists $f : \mathbb{N} \to \{0, 1\} \in \mathsf{R}$ such that

$$x \in A \implies f(x) = 0 \qquad x \in B \implies f(x) = 1$$

- set $A \subseteq \mathbb{N}$ is recursively enumerable if $A = \varnothing$ or A is range of unary recursive function
- set $A \subseteq \mathbb{N}$ is index set if $d \in A \wedge \varphi_e \simeq \varphi_d \implies e \in A$ for all $d, e \in \mathbb{N}$

Lemmata

- if A and B are recursively inseparable then A and B are not recursive
- set A is recursive if and only if A and $\mathbb{N} \setminus A$ are recursively enumerable

Rice's Theorem

non–trivial index sets are not recursive

Theorem

- sets $A = \{x \mid \varphi_x(x) = 0\}$ and $B = \{x \mid \varphi_x(x) = 1\}$ are recursively inseparable
- following statements are equivalent for any set $A \subseteq \mathbb{N}$:
  1. A is recursively enumerable
  2. A is range of unary partial recursive function
  3. A is domain of unary partial recursive function

Definition

set $A \subseteq \mathbb{N}$ is diophantine if $\exists$ polynomial $P(x, y_1, \ldots, y_n)$ with integer coefficients such that

$$x \in A \iff \exists\, y_1 \cdots \exists\, y_n \quad P(x, y_1, \ldots, y_n) = 0$$

Lemma

A is diophantine $\iff$ $A = \{P(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in \mathbb{N} \text{ and } P(x_1, \ldots, x_n) \geqslant 0\}$
for some polynomial $P(x_1, \ldots, x_n)$ with integer coefficients

Lemma

diophantine sets are recursively enumerable

Theorem (Matiyasevich)

recursively enumerable sets are diophantine

Corollary (MRDP Theorem)

Hilbert's 10th problem is unsolvable

Theorem (Jones 1975)

- $P(x, y) = 2x + 2y^3x^2 + y^2x^3 - 2yx^4 - x^5 - y^4x$ generates set of all Fibonacci numbers
- there exists no polynomial $Q(x_1, \ldots, x_n)$ such that

$$\{Q(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \geqslant 0\}$$

is set of all Fibonacci numbers

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

abstraction, arithmetization, CL–representability, combinators, combinatorial completeness, Church numerals, Church–Rosser theorem, Curry–Howard isomorphism, fixed point theorem, intuitionistic propositional logic, normalization theorem, termination, typing, undecidability, Z property

Outline

1. Summary of Previous Lecture
2. **Combinatory Logic**
3. Combinators
4. Church Numerals
5. Combinatorial Completeness
6. CL–Representability
7. Confluence
8. Summary

Definition

CL–terms are built from

- infinite set of variables $\mathcal{V} = \{x, y, z, \ldots\}$
- constants $\mathsf{I} \quad \mathsf{K} \quad \mathsf{S}$
- application $(s \cdot t)$ for CL–terms s and t

Examples

y	S	$(\mathsf{I} \cdot \mathsf{K})$	$(x \cdot (\mathsf{S} \cdot y))$	$((\mathsf{S} \cdot \mathsf{I}) \cdot \mathsf{I})$	functional notation
y	S	IK	$x(\mathsf{S}y)$	SII	applicative notation

Notational Conventions

- juxtaposition for application
- association to the left to reduce number of parentheses

Definitions

- set $\mathcal{V}\mathrm{ar}(t)$ of variables of CL–term t is inductively defined:

$$\mathcal{V}\mathrm{ar}(t) = \begin{cases} \varnothing & \text{if } t \in \{\mathsf{I}, \mathsf{K}, \mathsf{S}\} \\ \{t\} & \text{if } t \in \mathcal{V} \\ \mathcal{V}\mathrm{ar}(t_1) \cup \mathcal{V}\mathrm{ar}(t_2) & \text{if } t = t_1 t_2 \end{cases}$$

- combinator is CL–term t such that $\mathcal{V}\mathrm{ar}(t) = \varnothing$

Definition

(weak) reduction is smallest relation $\to$ on CL–terms such that

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

for all CL–terms t, u, v

Definitions

- normal form is CL–term t such that $t \to u$ for no CL–term u
- $\to^+$ is transitive closure of $\to$
- $\to^*$ is transitive and reflexive closure of $\to$
- $t \to^! u$ if $t \to^* u$ for normal form u
- CL–term t is normalizing if $t \to^! u$ for some CL–term u
- infinite reduction is sequence $(t_i)_{i \geqslant 0}$ such that $t_i \to t_{i+1}$ for all $i \geqslant 0$
- CL–term t is terminating if there are no infinite reductions starting at t

Example

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

$$\mathsf{SII}(\mathsf{SII}) \to \mathsf{I}(\mathsf{SII})(\mathsf{I}(\mathsf{SII})) \to \mathsf{SII}(\mathsf{I}(\mathsf{SII})) \to \mathsf{SII}(\mathsf{SII})$$

Outline

1. Summary of Previous Lecture
2. Combinatory Logic
3. **Combinators**
4. Church Numerals
5. Combinatorial Completeness
6. CL–Representability
7. Confluence
8. Summary

Definition

$$\mathsf{B} = \mathsf{S}(\mathsf{KS})\mathsf{K} \qquad \mathsf{C} = \mathsf{S}(\mathsf{BBS})(\mathsf{KK}) \qquad \mathsf{Y} = \mathsf{B}(\mathsf{SI})(\mathsf{SII})(\mathsf{B}(\mathsf{SI})(\mathsf{SII}))$$

Lemma

$$\mathsf{B}\,xyz \;\to^+ x(yz) \qquad \mathsf{C}\,xyz \;\to^+ xzy \qquad \mathsf{Y}\,x \;\to^+ x(\mathsf{Y}\,x)$$

Proof

$$\mathsf{B}\,xyz \to \mathsf{KS}x(\mathsf{K}x)yz \to \mathsf{S}(\mathsf{K}x)yz \to \mathsf{K}xz(yz) \to x(yz)$$

$$\mathsf{C}\,xyz \to \mathsf{BBS}x(\mathsf{KK}x)yz \to \mathsf{BBS}\,x\mathsf{K}yz \to^+ \mathsf{B}(\mathsf{S}\,x)\mathsf{K}yz \to^+ \mathsf{S}x(\mathsf{K}y)z \to xz(\mathsf{K}yz) \to xzy$$

$$\begin{aligned}\mathsf{Y}\,x &\to^+ \mathsf{SI}(\mathsf{SII}(\mathsf{B}(\mathsf{SI})(\mathsf{SII})))x \to \mathsf{I}\,x(\mathsf{SII}(\mathsf{B}(\mathsf{SI})(\mathsf{SII}))x) \to^+ x(\mathsf{I}(\mathsf{B}(\mathsf{SI})(\mathsf{SII}))(\mathsf{I}(\mathsf{B}(\mathsf{SI})(\mathsf{SII})))x)\\ &\to^+ x(\mathsf{B}(\mathsf{SI})(\mathsf{SII})(\mathsf{B}(\mathsf{SI})(\mathsf{SII}))x) = x(\mathsf{Y}\,x)\end{aligned}$$

Outline

1. Summary of Previous Lecture
2. Combinatory Logic
3. Combinators
4. **Church Numerals**
5. Combinatorial Completeness
6. CL–Representability
7. Confluence
8. Summary

Definition

for all $n \geqslant 0$ Church numeral $\underline{n}$ is combinator

$$\underline{n} = \begin{cases} \mathsf{KI} & \text{if } n = 0 \\ \mathsf{SB}\,\underline{n-1} & \text{if } n > 0 \end{cases} \qquad\qquad \underline{n} = (\mathsf{SB})^n(\mathsf{KI})$$

Definition

function $f\colon \mathbb{N}^n \to \mathbb{N}$ is CL–representable if there exists combinator F such that

$$\begin{aligned} f(x_1, \ldots, x_n) = y \quad &\Longrightarrow \quad F\,\underline{x_1} \cdots \underline{x_n} \to^* \underline{y} \\ f(x_1, \ldots, x_n) \text{ is undefined} \quad &\Longrightarrow \quad F\,\underline{x_1} \cdots \underline{x_n} \text{ is not normalizing} \end{aligned}$$

for all $x_1, \ldots, x_n, y \in \mathbb{N}$

$$\underline{n} = (\mathsf{SB})^n(\mathsf{KI})$$

Lemma

$\underline{n}\,x\,y \to^+ x^n\,y$

Proof

induction on $n \geqslant 0$

$$\underline{0}\,x\,y = \mathsf{KI}\,x\,y \to \mathsf{I}\,y \to y = x^0\,y$$

$$\underline{n+1}\,x\,y = \mathsf{SB}\,\underline{n}\,x\,y \to \mathsf{B}\,x\,(\underline{n}\,x)\,y \to^+ x\,(\underline{n}\,x\,y) \to^+ x\,(x^n\,y) = x^{n+1}\,y$$

$$\underline{n} = (\mathsf{SB})^n(\mathsf{KI})$$

Lemma

initial functions are CL−representable

Proof

$$\mathsf{zero} = \mathsf{K}(\mathsf{KI}):$$

$$\mathsf{zero}\ \underline{x} \to \mathsf{KI} = \underline{0}$$

$$\mathsf{succ} = \mathsf{SB}:$$

$$\mathsf{succ}\ \underline{x} = \mathsf{SB}\,\underline{x} = \underline{x+1}$$

$$\pi_i^n = \begin{cases} \mathsf{K}^{i-1}((\mathsf{BK})^{n-i-1}\,\mathsf{K}) & \text{if } 1 \leqslant i < n \\ \mathsf{K}^{i-1}\,\mathsf{I} & \text{if } 1 \leqslant i = n \end{cases}$$

Outline

1. Summary of Previous Lecture
2. Combinatory Logic
3. Combinators
4. Church Numerals
5. **Combinatorial Completeness**
6. CL–Representability
7. Confluence
8. Summary

Definition (Bracket Abstraction)

- CL–term $[x]t$ is defined for all CL–terms t and variables x:

$$[x]t = \begin{cases} \mathsf{I} & \text{if } t = x \\ \mathsf{K}\,t & \text{if } x \notin \mathcal{V}\mathrm{ar}(t) \\ \mathsf{S}\,([x]t_1)([x]t_2) & \text{if } t = t_1 t_2 \text{ and } x \in \mathcal{V}\mathrm{ar}(t) \end{cases}$$

- $[x_1 \ldots x_n]t$ abbreviates $[x_1](\ldots[x_n]t\ldots)$

Example

$$\begin{aligned}
[x\,y\,z](xzy) &= [x\,y](\mathsf{S}([z](xz))([z]y)) = [x\,y](\mathsf{S}(\mathsf{S}([z]x)([z]z))(\mathsf{K}y)) = [x\,y](\mathsf{S}(\mathsf{S}(\mathsf{K}x)\mathsf{I})(\mathsf{K}y)) \\
&= [x](\mathsf{S}([y](\mathsf{S}(\mathsf{S}(\mathsf{K}x)\mathsf{I})))([y](\mathsf{K}y))) = [x](\mathsf{S}(\mathsf{K}(\mathsf{S}(\mathsf{S}(\mathsf{K}x)\mathsf{I})))(\mathsf{S}([y]\mathsf{K})([y]y))) \\
&= [x](\mathsf{S}(\mathsf{K}(\mathsf{S}(\mathsf{S}(\mathsf{K}x)\mathsf{I})))(\mathsf{S}(\mathsf{K}\mathsf{K})\mathsf{I})) = \cdots \\
&= \mathsf{S}(\mathsf{S}(\mathsf{K}\mathsf{S})(\mathsf{S}(\mathsf{K}\mathsf{K})(\mathsf{S}(\mathsf{K}\mathsf{S})(\mathsf{S}(\mathsf{S}(\mathsf{K}\mathsf{S})(\mathsf{S}(\mathsf{K}\mathsf{K})\mathsf{I}))(\mathsf{K}\mathsf{I})))))(\mathsf{K}(\mathsf{S}(\mathsf{K}\mathsf{K})\mathsf{I}))
\end{aligned}$$

Lemma

$x \notin \mathcal{V}\mathrm{ar}([x]t)$

Lemma

$([x]t)\,x \to^* t$ for all CL–terms t and variables x

Proof

induction on t

- $t = x \quad \Longrightarrow \quad ([x]t)\,x = \mathsf{I}x \to x = t$
- $x \notin \mathcal{V}\mathrm{ar}(t) \quad \Longrightarrow \quad ([x]t)\,x = \mathsf{K}tx \to t$
- $t = t_1 t_2$ and $x \in \mathcal{V}\mathrm{ar}(t) \quad \Longrightarrow \quad ([x]t_1)x \to^* t_1$ and $([x]t_2)x \to^* t_2$ by induction hypothesis

  $\Longrightarrow \quad ([x]t)\,x = \mathsf{S}([x]t_1)([x]t_2)x \to ([x]t_1)x(([x]t_2)x) \to^* t_1 t_2 = t$

Corollary (Combinatorial Completeness)

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

1. $\exists$ combinator C such that $C\,x_1 \cdots x_n \to^* t$
2. $\exists$ combinator D such that $D\,x_2 \cdots x_n \to^* t\,[D/x_1]$

Proof

① $C = [x_1 \ldots x_n]t$: $\quad C\,x_1 \cdots x_n \to^+ ([x_2 \ldots x_n]t)\,x_2 \cdots x_n \to^+ \cdots \to^+ t$

② $D = \mathsf{Y}C$: $\quad D\,x_2 \cdots x_n \to^+ C\,D\,x_2 \cdots x_n \to^+ t\,[D/x_1]$

Definition (Bracket Abstraction, Optimized)

- CL–term $\langle x \rangle t$ is defined for all CL–terms t and variables x:

$$\langle x \rangle t = \begin{cases} \mathsf{I} & \text{if } t = x \\ \mathsf{K}\, t & \text{if } x \notin \mathcal{V}\mathrm{ar}(t) \end{cases} \qquad \langle x \rangle t = \begin{cases} u & \text{if } t = u\, x \text{ and } x \notin \mathcal{V}\mathrm{ar}(u) \\ \mathsf{B}\, u\, (\langle x \rangle v) & \text{if } t = u\, v \text{ and } x \notin \mathcal{V}\mathrm{ar}(u) \\ \mathsf{C}\, (\langle x \rangle u)\, v & \text{if } t = u\, v \text{ and } x \notin \mathcal{V}\mathrm{ar}(v) \\ \mathsf{S}\, (\langle x \rangle u)\, (\langle x \rangle v) & \text{if } t = u\, v \text{ and } x \in \mathcal{V}\mathrm{ar}(u) \cap \mathcal{V}\mathrm{ar}(v) \end{cases}$$

- $\langle x_1 \ldots x_n \rangle t$ abbreviates $\langle x_1 \rangle (\ldots \langle x_n \rangle t \ldots)$

Example

$$\langle x\, y\, z \rangle (x z y) = \langle x\, y \rangle (\mathsf{C} (\langle z \rangle (x z)) y) = \langle x\, y \rangle (\mathsf{C} x y) = \langle x \rangle (\mathsf{C} x) = \mathsf{C}$$

Lemma

$(\langle x \rangle t)\, x \to^* t$ for all CL–terms t and variables x

Outline

1. Summary of Previous Lecture
2. Combinatory Logic
3. Combinators
4. Church Numerals
5. Combinatorial Completeness
6. **CL–Representability**
7. Confluence
8. Summary

Lemma

CL−representable functions are closed under composition

Proof

$$f(x_1, \ldots, x_n) = g(h_1(x_1, \ldots, x_n), \ldots, h_m(x_1, \ldots, x_n))$$

with $G, H_1, \ldots, H_m$ representing $g, h_1, \ldots, h_m$

$$F = \langle x_1 \ldots x_n \rangle (G\,(H_1\,x_1 \cdots x_n) \cdots (H_m\,x_1 \cdots x_n))$$

Lemma

CL−representable functions are closed under primitive recursion

$$f(0, y_1, \ldots, y_n) = g(y_1, \ldots, y_n)$$
$$f(x+1, y_1, \ldots, y_n) = h(f(x, y_1, \ldots, y_n), x, y_1, \ldots, y_n)$$

$$f(x, y_1, \ldots, y_n) = \begin{cases} g(y_1, \ldots, y_n) & \text{if } x = 0 \\ h(f(x-1, y_1, \ldots, y_n), x-1, y_1, \ldots, y_n) & \text{otherwise} \end{cases}$$

Booleans

$\mathsf{T} = \mathsf{K}$ $\quad$ $\mathsf{F} = \mathsf{KI}$ $\quad$ $\mathsf{T}xy \to x$ $\quad$ $\mathsf{F}xy \to \mathsf{I}y \to y$

Test for Zero

$$\text{zero?} = \mathsf{C}(\mathsf{B}(\mathsf{CIK}))(\mathsf{K}(\mathsf{KI}))$$

$$\begin{aligned} \text{zero? } \underline{0} &\to^* \mathsf{B}(\mathsf{CIK})\,\underline{0}\,(\mathsf{K}(\mathsf{KI})) \to^* \mathsf{CIK}(\underline{0}\,(\mathsf{K}(\mathsf{KI}))) \to \mathsf{CIKI} \to^* \mathsf{IIK} \to^* \mathsf{K} = \mathsf{T} \\ \text{zero? } \underline{n+1} &\to^* \mathsf{B}(\mathsf{CIK})\,\underline{n+1}\,(\mathsf{K}(\mathsf{KI})) \to^* \mathsf{CIK}(\mathsf{SB}\,\underline{n}\,(\mathsf{K}(\mathsf{KI}))) \to^* \mathsf{CIK}(\mathsf{B}(\mathsf{K}(\mathsf{KI}))(\underline{n}\,(\mathsf{K}(\mathsf{KI})))) \\ &\to^* \mathsf{I}(\mathsf{B}(\mathsf{K}(\mathsf{KI}))(\underline{n}\,(\mathsf{K}(\mathsf{KI}))))\mathsf{K} \to \mathsf{B}(\mathsf{K}(\mathsf{KI}))(\underline{n}\,(\mathsf{K}(\mathsf{KI})))\mathsf{K} \\ &\to^* \mathsf{K}(\mathsf{KI})(\underline{n}\,(\mathsf{K}(\mathsf{KI}))\mathsf{K}) \to \mathsf{KI} = \mathsf{F} \end{aligned}$$

$$f(x, y_1, \ldots, y_n) = \begin{cases} g(y_1, \ldots, y_n) & \text{if } x = 0 \\ h(f(x-1, y_1, \ldots, y_n), x-1, y_1, \ldots, y_n) & \text{otherwise} \end{cases}$$

Predecessor

$$\mathsf{P} = \mathsf{C}(\mathsf{C}(\mathsf{CI}(\mathsf{B}(\mathsf{CI})(\mathsf{CI}(\mathsf{SB}))))(\mathsf{K}(\mathsf{KI})))\mathsf{I}$$

Lemma

P represents predecessor function

Lemma

CL−representable functions are closed under primitive recursion

Proof

$$f(0, y_1, \ldots, y_n) = g(y_1, \ldots, y_n)$$
$$f(x+1, y_1, \ldots, y_n) = h(f(x, y_1, \ldots, y_n), x, y_1, \ldots, y_n)$$

with G, H representing g, h

$$F\,x\,y_1 \cdots y_n = (\text{zero?}\ x)\,(G\,y_1 \cdots y_n)\,(H\,(F\,(\mathsf{P}\,x)\,y_1 \cdots y_n)\,(\mathsf{P}\,x)\,y_1 \cdots y_n)$$
$$F = \langle x\,y_1 \ldots y_n\rangle\,((\text{zero?}\ x)\,(G\,y_1 \cdots y_n)\,(H\,(F\,(\mathsf{P}\,x)\,y_1 \cdots y_n)\,(\mathsf{P}\,x)\,y_1 \cdots y_n))$$
$$F = \mathsf{Y}\,(\langle f\,x\,y_1 \ldots y_n\rangle\,((\text{zero?}\ x)\,(G\,y_1 \cdots y_n)\,(H\,(f\,(\mathsf{P}\,x)\,y_1 \cdots y_n)\,(\mathsf{P}\,x)\,y_1 \cdots y_n)))$$

Corollary

primitive recursive functions are CL−representable

Outline

1. Summary of Previous Lecture
2. Combinatory Logic
3. Combinators
4. Church Numerals
5. Combinatorial Completeness
6. CL–Representability
7. **Confluence**
8. Summary

Definition

function $f\colon \mathbb{N}^n \to \mathbb{N}$ is CL–representable if there exists combinator F such that

$$f(x_1, \ldots, x_n) = y \quad \Longrightarrow \quad F\,\underline{x_1} \cdots \underline{x_n} \to^* \underline{y}$$
$$f(x_1, \ldots, x_n) \text{ is undefined} \quad \Longrightarrow \quad F\,\underline{x_1} \cdots \underline{x_n} \text{ is not normalizing}$$

for all $x_1, \ldots, x_n, y \in \mathbb{N}$

Question

is it possible that both $F\,\underline{x_1} \cdots \underline{x_n} \to^* \underline{y}$ and $F\,\underline{x_1} \cdots \underline{x_n} \to^* \underline{z}$ with $y \neq z$?

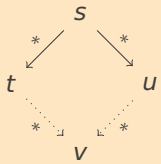
Answer

no, because CL has unique normal forms: $\forall$ term t $\forall$ normal forms n_1 and n_2

$$t \to^* n_1 \quad \wedge \quad t \to^* n_2 \quad \Longrightarrow \quad n_1 = n_2$$

Theorem

CL is confluent: $\forall s \forall t \forall u \left[s \to^* t \wedge s \to^* u \implies \exists v \left(t \to^* v \wedge u \to^* v \right) \right]$



Corollary

CL has unique normal forms

Outline

1. Summary of Previous Lecture
2. Combinatory Logic
3. Combinators
4. Church Numerals
5. Combinatorial Completeness
6. CL–Representability
7. Confluence
8. **Summary**

Important Concepts

- $\rightarrow$
- $\rightarrow^+$
- $\rightarrow^*$
- $\rightarrow^!$
- B
- $[x]t$
- $\langle x \rangle t$
- bracket abstraction
- C
- Church numeral
- CL–representable function
- CL–term
- combinator
- combinatorial completeness
- combinatory logic
- confluence
- I
- F
- K
- normal form
- normalization
- P
- π_i^n
- S
- succ
- T
- termination
- unique normal forms
- (weak) reduction
- Y
- zero
- zero?

homework for December 7