I217E: Functional Programming

Nao Hirokawa

JAIST

Term 2-1, 2022

`http://www.jaist.ac.jp/~hirokawa/lectures/fp/`

Schedule

10/12	introduction	11/9	interpreters
10/14	algebraic data types I	11/11	compilers
10/19	algebraic data types II	11/16	termination
10/21	applications	11/18	confluence
10/26	program reasoning	11/25	verification
10/28	data structures I	11/30	review
11/2	data structures II	12/5	exam
11/4	computational models		

Evaluation

exam (60) + reports (40)

Is Mathematics Correct?

Theorem (?)

$-1 = 1$

Proof.

using Euler's formula $e^{i\theta} = \cos\theta + i\sin\theta$

$$-1 \;=\; e^{i\pi} \;=\; e^{i2\pi\cdot\frac{1}{2}} \;=\; (e^{i2\pi})^{\frac{1}{2}} \;=\; 1^{\frac{1}{2}} \;=\; 1$$

□

Functions

Definition

function from A to B is relation $f \subseteq A \times B$ such that

- for every $x \in A$ there exists $y \in B$ with $(x, y) \in f$ **totality**
- $y = z$ whenever $(x, y) \in f$ and $(x, z) \in f$ **uniqueness of images**

Example

which are functions from $\mathbb{N}$ to $\mathbb{N}$?

1. $\{(x + 1, x) \mid x \in \mathbb{N}\}$
2. $\{(x, y) \mid x \in \mathbb{N} \text{ and } y = x^2\}$
3. $\{(x, y) \mid x, y \in \mathbb{N} \text{ and } y \leqslant x\}$

Well-Definedness

Terminology

function definition is **well-defined** if it really defines function

Example

which of function definitions are well-defined for $\mathbb{N} \to \mathbb{N}$?

$\boxed{1}$ $\mathtt{f}_1(x) = \begin{cases} 0 & \text{if } x = 0 \\ x + \mathtt{f}_1(x-1) & \text{if } x > 0 \end{cases}$

$\boxed{2}$ $\mathtt{f}_2(x) = x + \mathtt{f}_2(x-1)$ if $x \geqslant 1$

$\boxed{3}$ $\mathtt{f}_3(x) = \mathtt{f}_3(x)$

$\boxed{4}$ $\mathtt{f}_4(x) = 0 \times \mathtt{f}_3(x)$

$\boxed{5}$ $\mathtt{f}_5(x) = \begin{cases} 0 & \text{if } x \leqslant 5 \\ 10 & \text{if } x \geqslant 5 \end{cases}$

Are Functions Well-Defined?

- definition for $+$:

$$\begin{aligned} 0 + y &\to y \\ \mathsf{s}(x) + y &\to \mathsf{s}(x+y) \\ (x+y)+z &\to x + (y+z) \end{aligned}$$

- definition for f:

$$\begin{aligned} \mathsf{f}(\mathsf{true}, y) &\to \mathsf{true} \\ \mathsf{f}(x, \mathsf{false}) &\to \mathsf{true} \\ \mathsf{f}(x, x) &\to x \end{aligned}$$

how to ensure uniqueness of normal forms? — confluence

Confluence

Definition

$\mathcal{R}$ is confluent if for every s, t, u there is v such that

$t \mathrel{{}^{*}_{\mathcal{R}}{\leftarrow}} s \to^{*}_{\mathcal{R}} u$ implies $t \to^{*}_{\mathcal{R}} v \mathrel{{}^{*}_{\mathcal{R}}{\leftarrow}} u$

$$\begin{tikzcd} & s \arrow[dl, "*"', "\mathcal{R}"] \arrow[dr, "*", "\mathcal{R}"'] & \\ t \arrow[dr, dashed, "\mathcal{R}"', "*"] & & u \arrow[dl, dashed, "\mathcal{R}", "*"'] \\ & v & \end{tikzcd}$$

Lemma

for every confluent TRS $\mathcal{R}$

if $t \mathrel{{}^{*}_{\mathcal{R}}{\leftarrow}} s \to^{*}_{\mathcal{R}} u$ and $t, u \in \mathsf{NF}(\mathcal{R})$ then $t = u$

Composition of Substitutions and Subsumption

Definition

$\sigma\tau = \{x \mapsto (x\sigma)\tau \mid x \in \mathcal{V}\}$

Example

$\sigma = \{x \mapsto \mathsf{s}(y), y \mapsto x + \mathsf{s}(0)\}$ $\quad \tau = \{x \mapsto \mathsf{s}(0), z \mapsto \mathsf{s}(\mathsf{s}(y))\}$

- $\sigma\tau = \{x \mapsto \mathsf{s}(y), y \mapsto \mathsf{s}(0) + \mathsf{s}(0), z \mapsto \mathsf{s}(\mathsf{s}(y))\}$
- $\tau\sigma = \{x \mapsto \mathsf{s}(0), y \mapsto x + \mathsf{s}(0), z \mapsto \mathsf{s}(\mathsf{s}(x + \mathsf{s}(0)))\}$

Definition

$\sigma \leq \tau \iff \exists \rho : \sigma\rho = \tau$

Unification Problem

Definition (Unification Problem)

instance: terms s, t
question: $s\sigma = t\sigma$ for some substitution σ (σ is **unifier** of s and t)

Definition

$\leqslant$-minimal unifier is called most general unifier (mgu)

Example

for $x + (0 + \mathsf{s}(y))$ and $\mathsf{s}(z) + (0 + x)$

- $\{x \mapsto \mathsf{s}(z)\}$ is not unifier
- $\{x \mapsto \mathsf{s}(z),\ y \mapsto z\}$ is mgu
- $\{x \mapsto \mathsf{s}(0),\ y \mapsto 0,\ z \mapsto 0\}$ is unifier but not mgu

Unification Algorithm

let $s \approx t$ denote unordered pair of s and t

Definition (unification rules, $E \Rightarrow_\sigma E'$)

- $\dfrac{\{f(s_1,\ldots,s_n) \approx f(t_1,\ldots,t_n)\} \uplus E}{\{s_1 \approx t_1,\ \ldots,\ s_n \approx t_n\} \cup E}$
- $\dfrac{\{x \approx x\} \uplus E}{E}$ if $x \in \mathcal{V}$
- $\dfrac{\{x \approx t\} \uplus E}{E\{x \mapsto t\}}\ \{x \mapsto t\}$ if $x \notin \mathcal{V}\mathsf{ar}(t)$ (occurs check)

Theorem

- *s and t are unifiable if and only if $\{s \approx t\} \Rightarrow^* \varnothing$*
- *$\sigma_1\sigma_2\cdots\sigma_n$ is mgu of s and t if $\{s \approx t\} \Rightarrow_{\sigma_1} \cdots \Rightarrow_{\sigma_n} \varnothing$*

$$\{x + (0 + \mathsf{s}(y)) \approx \mathsf{s}(z) + (0 + x)\}$$
$$\Downarrow$$
$$\{x \approx \mathsf{s}(z),\ 0 + \mathsf{s}(y) \approx 0 + x\}$$
$$\Downarrow \{x \mapsto \mathsf{s}(z)\}$$
$$\{0 + \mathsf{s}(y) \approx 0 + \mathsf{s}(z)\}$$
$$\Downarrow$$
$$\{0 \approx 0,\ \mathsf{s}(y) \approx \mathsf{s}(z)\}$$
$$\Downarrow$$
$$\{\mathsf{s}(y) \approx \mathsf{s}(z)\}$$
$$\Downarrow$$
$$\{y \approx z\}$$
$$\Downarrow \{y \mapsto z\}$$
$$\varnothing$$

mgu

$$\{x \mapsto \mathsf{s}(z)\}\{y \mapsto z\}$$
$$= \{x \mapsto \mathsf{s}(z), y \mapsto z\}$$

Knuth-Bendix' Confluence Criterion

Definition

$(C[r_1]\sigma, r_2\sigma)$ is critical pair of $\mathcal{R}$ if

1. $\ell_1 \to r_1$ and $\ell_2 \to r_2$ are renamed rules in $\mathcal{R}$ having no common variables
2. $\ell_2 = C[\ell_2']$ and ℓ_2' is non-variable
3. σ is mgu of ℓ_1 and ℓ_2'
4. if $C = \Box$ then $\ell_1 \to r_1$ and $\ell_2 \to r_2$ are not same

$\mathsf{CP}(\mathcal{R})$ is set of all critical pairs of $\mathcal{R}$

Theorem (Knuth and Bendix 1970)

terminating TRS $\mathcal{R}$ is confluent if and only if

$$s \to^*_{\mathcal{R}} \cdot {}^*_{\mathcal{R}}\!\leftarrow t \ \textit{(s and t are joinable)} \quad \textit{for all } (s,t) \in \mathsf{CP}(\mathcal{R})$$

Example of Confluence Proof

consider terminating TRS $\mathcal{R}$

$$0 + y \to y$$
$$\mathsf{s}(x) + y \to \mathsf{s}(x + y)$$
$$(x + y) + z \to x + (y + z)$$

CP($\mathcal{R}$) is red part

$$\begin{array}{rcccl} y + z & {}_{\mathcal{R}}\!\leftarrow & (0 + y) + z & \to_{\mathcal{R}} & 0 + (y + z) \\ \mathsf{s}(x + y) + z & {}_{\mathcal{R}}\!\leftarrow & (\mathsf{s}(x) + y) + z & \to_{\mathcal{R}} & \mathsf{s}(x) + (y + z) \\ (w + (x + y)) + z & {}_{\mathcal{R}}\!\leftarrow & ((w + x) + y) + z & \to_{\mathcal{R}} & (w + x) + (y + z) \end{array}$$

all critical pairs are joinable, and hence $\mathcal{R}$ is confluent

Example of Non-Confluence Proof

consider terminating TRS $\mathcal{R}$

$$\mathsf{f}(\mathsf{true}, y) \to \mathsf{true}$$
$$\mathsf{f}(x, \mathsf{false}) \to \mathsf{true}$$
$$\mathsf{f}(x, x) \to x$$

CP($\mathcal{R}$) is red part

$$\begin{array}{rcccl} \mathsf{true} & {}_{\mathcal{R}}\!\leftarrow & \mathsf{f}(\mathsf{true}, \mathsf{false}) & \to_{\mathcal{R}} & \mathsf{true} \\ \mathsf{true} & {}_{\mathcal{R}}\!\leftarrow & \mathsf{f}(\mathsf{true}, \mathsf{true}) & \to_{\mathcal{R}} & \mathsf{true} \\ \mathsf{true} & {}_{\mathcal{R}}\!\leftarrow & \mathsf{f}(\mathsf{false}, \mathsf{false}) & \to_{\mathcal{R}} & \mathsf{false} \end{array}$$

since last critical pair is not joinable, $\mathcal{R}$ is not confluent

Homework

1. Compute an mgu of s and t if it exists.
   1. $s = x + \mathsf{s}(y)$ and $t = \mathsf{s}(y) + \mathsf{s}(z)$
   2. $s = x + \mathsf{s}(y)$ and $t = \mathsf{s}(y) + \mathsf{s}(x)$
2. Prove or disprove confluence.
   1. $\{\mathsf{f}(\mathsf{f}(x)) \to \mathsf{s}(\mathsf{s}(\mathsf{f}(x)))\}$
   2. $\{\mathsf{b}(\mathsf{a}(x)) \to \mathsf{a}(\mathsf{b}(x))\}$
   3. $\left\{ \begin{array}{c} [\,] \mathbin{+\!\!+} ys \to ys \\ (x : xs) \mathbin{+\!\!+} ys \to x : (xs \mathbin{+\!\!+} ys) \end{array} \right\}$
   4. $\left\{ \begin{array}{c} 0 + y \to y \\ \mathsf{s}(x) + y \to \mathsf{s}(x + y) \\ x + (y + z) \to (x + y) + z \end{array} \right\}$
   5. $\left\{ \begin{array}{ll} \mathsf{max}(0, y) \to y & \mathsf{max}(\mathsf{s}(x), \mathsf{s}(y)) \to \mathsf{s}(\mathsf{max}(x, y)) \\ \mathsf{max}(x, 0) \to x & \mathsf{max}(x, x) \to x \end{array} \right\}$