PSC 2023/24 (375AA, 9CFU)

Principles for Software Composition

Roberto Bruni
http://www.di.unipi.it/~bruni/

http://didawiki.di.unipi.it/doku.php/magistraleinformatica/psc/start

07 - Recursion

Notation

$$f : X \to (Y \to Z) \qquad f : X \to Y \to Z$$

$$\forall x \in X.\ f(x) : Y \to Z \qquad \forall x \in X.\ f\ x : Y \to Z$$

$$\forall x \in X.\ \forall y \in Y.\ (f(x))(y) \in Z \qquad \forall x \in X.\ \forall y \in Y.\ f\ x\ y \in Z$$

$$g : (X \to Y) \to Z \qquad g\ x$$

$$\forall h \in (X \to Y).\ g(h) \in Z \qquad f\ h$$

Notation

$$f : X_1 \to X_2 \to \cdots \to X_n$$

$$f : X_1 \to (X_2 \to (\cdots \to X_n))$$

$$f \ x_1 \ x_2 \ \cdots \ x_n$$

$$(((f \ x_1) \ x_2) \ \cdots) \ x_n$$

Notation

$$f : X_1 \times X_2 \to Y$$

$$f : (X_1 \times X_2) \to Y$$

$$\forall x_1 \in X_1.\ \forall x_2 \in X_2.\ f(x_1, x_2) \in Y$$

$$f\ x_1$$

Notation

$$f : X \to Y$$

$$A \subseteq X$$

$$f_{|A} : A \to Y$$

$$\forall a \in A.\ f_{|A}(a) \triangleq f(a)$$

Predecessors

$$A, \prec$$

$$a \in A$$

$$\lfloor a \rfloor \triangleq \{x \in A \mid x \prec a\}$$

Well-founded recursion

Recursive definitions

$$\mathcal{A}[\![\cdot]\!] : \mathsf{Aexp} \to \mathbb{M} \to \mathbb{Z}$$

$\mathcal{A}[\![a]\!]\sigma$ denotes the value associated to a in σ

$$\begin{aligned} \mathcal{A}[\![n]\!]\sigma &\triangleq n \\ \mathcal{A}[\![x]\!]\sigma &\triangleq \sigma(x) \\ \mathcal{A}[\![a_0 \,\mathsf{op}\, a_1]\!]\sigma &\triangleq \mathcal{A}[\![a_0]\!]\sigma \; op \; \mathcal{A}[\![a_1]\!]\sigma \end{aligned}$$

The function is defined recursively:
how do we know one and exactly one value is associated to each expression? (true)

Recursive definitions

$$\mathsf{N} ::= 0 \mid \mathsf{s}(\mathsf{N})$$

$$\mathcal{N}[\![\cdot]\!] : \mathsf{Nexp} \to \mathbb{N}$$

$$\begin{aligned} \mathcal{N}[\![0]\!] &\triangleq 0 \\ \mathcal{N}[\![\mathsf{s}(\mathsf{N})]\!] &\triangleq 1 + \mathcal{N}[\![\mathsf{s}(\mathsf{s}(\mathsf{N}))]\!] \end{aligned}$$

The function is defined recursively:
how do we know one and exactly one value is associated to each expression? (false)

Well founded recursion

$$A, \prec \text{ w.f.}$$

$$F \triangleq \{F_a : (\lfloor a \rfloor \to B) \to B\}_{a \in A}$$

$$\forall a \in A.\ \forall h \in \lfloor a \rfloor \to B.\ F_a(h) \in B$$

TH. There exists a unique function $f : A \to B$ such that

$$\forall a \in A.\ f(a) = F_a(f_{|\lfloor a \rfloor})$$

Example

$$\mathbb{N}, <$$

$$F \triangleq \{F_n : (\lfloor n \rfloor \to \mathbb{N}) \to \mathbb{N}\}_{n \in \mathbb{N}}$$

$$F_0 : (\emptyset \to \mathbb{N}) \to \mathbb{N}$$

$$F_0 \; h \triangleq 1$$

$$F_{n+1} : (\{n\} \to \mathbb{N}) \to \mathbb{N}$$

$$F_{n+1} \; h \triangleq (n+1) \cdot h(n)$$

$$f(0) = F_0 f_{|\emptyset} = 1$$

$$f(n+1) = F_{n+1} \; f_{|\{n\}} = (n+1) \cdot f(n)$$

$$f(n) = n!$$

Example

$$\mathbb{N}, < \qquad\qquad m \in \mathbb{N}$$

$$F^m \triangleq \{F^m_n : (\lfloor n \rfloor \to \mathbb{N}) \to \mathbb{N}\}_{n \in \mathbb{N}}$$

$$F^m_0 : (\emptyset \to \mathbb{N}) \to \mathbb{N}$$

$$F^m_0 \ h \triangleq 0$$

$$F^m_{n+1} : (\{n\} \to \mathbb{N}) \to \mathbb{N}$$

$$F^m_{n+1} \ h \triangleq m + h(n)$$

$$f^m(0) = 0$$

$$f^m(n+1) = m + f^m(n)$$

$$f^m(n) = m \cdot n$$

Ackermann function

a computable function that is total but not primitive recursive

$$m \in \mathbb{N} \qquad ack_m : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$

$$\begin{aligned}
ack_m(0,0) &\triangleq m \\
ack_m(0,n+1) &\triangleq ack_m(0,n)+1 \\
ack_m(1,0) &\triangleq 0 \\
ack_m(k+1,n+1) &\triangleq ack_m(k, ack_m(k+1,n)) \\
ack_m(k+2,0) &\triangleq 1
\end{aligned}$$

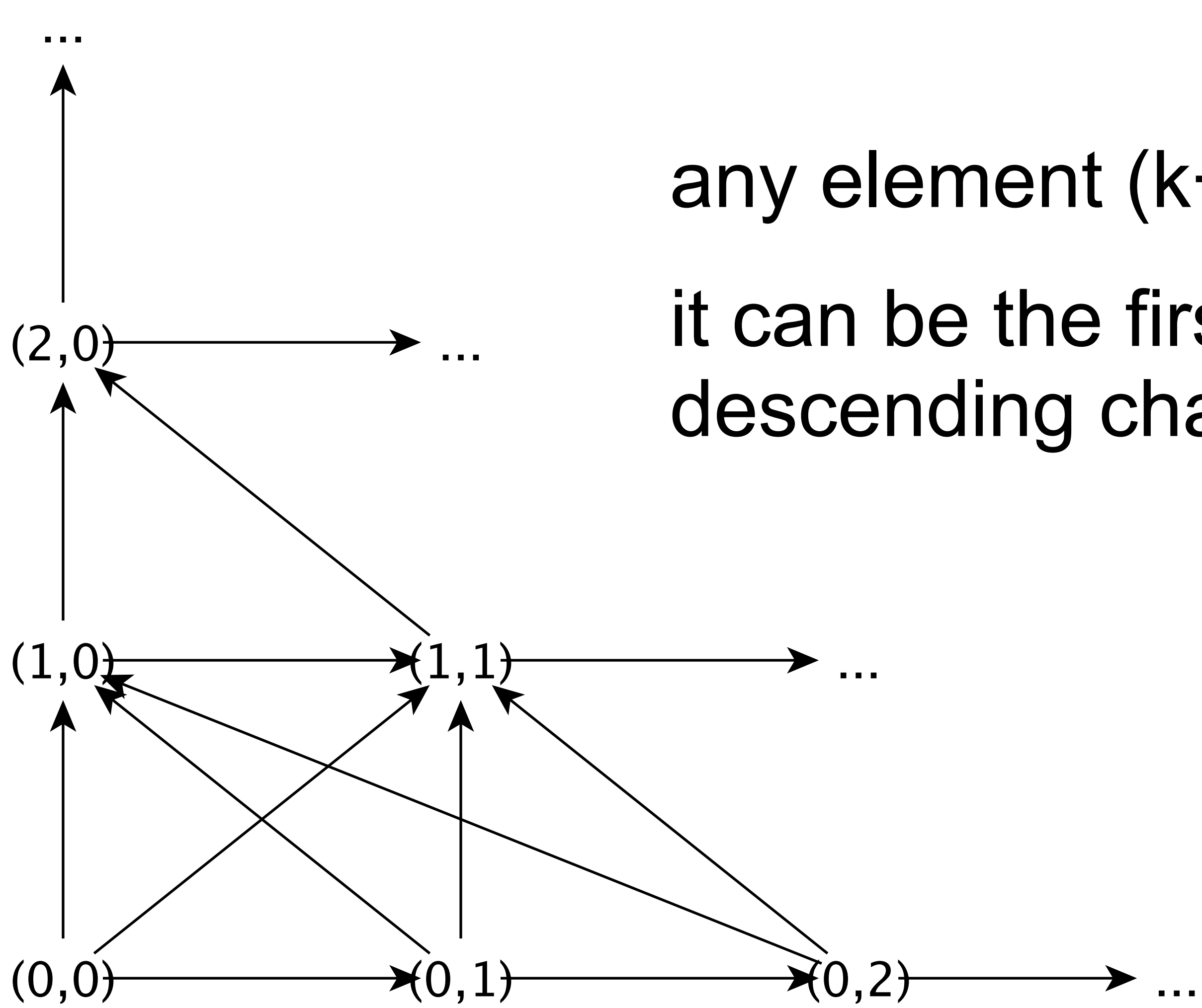
$\mathbb{N} \times \mathbb{N}, \prec$ lexicographic precedence relation

$$(k,n) \prec (k+1,n')$$

$$(k,n) \prec (k,n+1)$$

Ackermann function

$$(k, n) \prec (k+1, n')$$
$$(k, n) \prec (k, n+1)$$



any element (k+1,n) has infinitely many predecessors

it can be the first element of infinitely many descending chains (of unbounded length, but finite)

Ackermann function

$$(k, n) \prec (k+1, n')$$
$$(k, n) \prec (k, n+1)$$

$\prec^+$ is w.f.

Take a non-empty set $Q \subseteq \mathbb{N} \times \mathbb{N}$

can we find m minimal in Q?

$\widehat{k} \triangleq \min \{k \mid (k, n) \in Q\}$ (non-empty because $Q \neq \varnothing$)

$\widehat{n} \triangleq \min \{n \mid (\widehat{k}, n) \in Q\}$ (non-empty by def of $\widehat{k}$)

clearly $(\widehat{k}, \widehat{n}) \in Q$ is minimal

Ackermann function

$$
\begin{aligned}
ack_m(0,0) &\triangleq m \\
ack_m(0,n+1) &\triangleq ack_m(0,n)+1
\end{aligned}
$$

n increments of base case m

$$ack_m(0,n) \triangleq m+n$$

Ackermann function

$$
\begin{aligned}
ack_m(1,0) &\triangleq 0 \\
ack_m(k+1,n+1) &\triangleq ack_m(k, ack_m(k+1,n)) \\
ack_m(1,n+1) &\triangleq ack_m(0, ack_m(1,n))
\end{aligned}
$$

$$ack_m(0,n) \triangleq m+n$$

$$ack_m(1,n+1) \triangleq m + ack_m(1,n)$$

add m for n times to the base case 0

$$ack_m(1,n) \triangleq m \cdot n$$

Ackermann function

$$
\begin{aligned}
ack_m(k+1, n+1) &\triangleq ack_m(k, ack_m(k+1, n)) \\
ack_m(k+2, 0) &\triangleq 1
\end{aligned}
$$

$$
\begin{aligned}
ack_m(2, 0) &\triangleq 1 \\
ack_m(2, n+1) &\triangleq ack_m(1, ack_m(2, n))
\end{aligned}
$$

$$ack_m(1, n) \triangleq m \cdot n$$

$$ack_m(2, n+1) \triangleq m \cdot ack_m(2, n)$$

multiplies by m for n times the base case 1

$$ack_m(2, n) \triangleq m^n$$

Ackermann function

$$
\begin{aligned}
ack_m(k+1, n+1) &\triangleq ack_m(k, ack_m(k+1, n)) \\
ack_m(k+2, 0) &\triangleq 1
\end{aligned}
$$

$$
\begin{aligned}
ack_m(3, 0) &\triangleq 1 \\
ack_m(3, n+1) &\triangleq ack_m(2, ack_m(3, n))
\end{aligned}
$$

$$ack_m(2, n) \triangleq m^n$$

$$ack_m(3, n+1) \triangleq m^{ack_m(3,n)}$$

n times exponentiation

$$ack_m(3, n) \triangleq m^{m^{m^{\cdots^{m}}}}$$

Ackermann function

it grows faster than any primitive recursive function

$$
\begin{aligned}
ack_3(0,3) &\triangleq 3+3=6 \\
ack_3(1,3) &\triangleq 3\cdot 3=9 \\
ack_3(2,3) &\triangleq 3^3=27 \\
ack_3(3,3) &\triangleq 3^{3^3}=3^{27}\simeq 7.6\cdot 10^{12}
\end{aligned}
$$

Arithmetic expressions

$\mathsf{Aexp}, \prec$ $\qquad a_i \prec a_0 \,\mathsf{op}\, a_1$

$$\mathcal{A}[\![\cdot]\!] : \mathsf{Aexp} \to \mathbb{M} \to \mathbb{Z}$$

$$\begin{array}{rcl} \mathcal{A}[\![n]\!]\sigma & \triangleq & n \\ \mathcal{A}[\![x]\!]\sigma & \triangleq & \sigma(x) \\ \mathcal{A}[\![a_0 \,\mathsf{op}\, a_1]\!]\sigma & \triangleq & \mathcal{A}[\![a_0]\!]\sigma \; op \; \mathcal{A}[\![a_1]\!]\sigma \end{array}$$

Boolean expressions

$\mathsf{Bexp}, \prec$

$$b_i \prec b_0 \,\mathsf{bop}\, b_1$$

$$b \prec \neg b$$

$$\mathcal{B}[\![\cdot]\!] : \mathsf{Bexp} \to \mathbb{M} \to \mathbb{Z}$$

$$\begin{array}{rcl}
\mathcal{B}[\![v]\!]\sigma & \triangleq & v \\
\mathcal{B}[\![a_0 \,\mathsf{cmp}\, a_1]\!]\sigma & \triangleq & \mathcal{A}[\![a_0]\!]\sigma \; cmp \; \mathcal{A}[\![a_1]\!]\sigma \\
\mathcal{B}[\![\neg b]\!]\sigma & \triangleq & \neg \mathcal{B}[\![b]\!]\sigma \\
\mathcal{B}[\![b_0 \,\mathsf{bop}\, b_1]\!]\sigma & \triangleq & \mathcal{B}[\![b_0]\!]\sigma \; bop \; \mathcal{B}[\![b_1]\!]\sigma
\end{array}$$

Consistency of expressions

Consistency?

$$\forall a, \sigma, n$$

$$\langle a, \sigma \rangle \longrightarrow n \quad \overset{?}{\Leftrightarrow} \quad \mathcal{A}[\![a]\!]\sigma = n$$

$$P(a) \triangleq \forall \sigma.\ \langle a, \sigma \rangle \longrightarrow \mathcal{A}[\![a]\!]\sigma$$

$\forall a \in \mathsf{Aexp}.\ P(a)\,?$

structural induction!

$$\frac{\forall x \in \mathsf{Ide}.\ P(x) \qquad \forall n \in \mathbb{Z}.\ P(n) \qquad \forall a_0, a_1.\ P(a_0) \wedge P(a_1) \Rightarrow P(a_0\ \mathsf{op}\ a_1)}{\forall a.\ P(a)}$$

Base cases

$\forall x \in \mathsf{Ide}.\ P(x)$

take $x \in \mathsf{Ide}$

we need to prove $P(x) \triangleq \forall \sigma.\ \langle x, \sigma \rangle \longrightarrow \mathcal{A}[\![x]\!]\sigma = \sigma(x)$

taken a generic σ we conclude by rule $\dfrac{}{\langle x, \sigma \rangle \longrightarrow \sigma(x)}$

$\forall n \in \mathbb{Z}.\ P(n)$

take $n \in \mathbb{Z}$

we need to prove $P(n) \triangleq \forall \sigma.\ \langle n, \sigma \rangle \longrightarrow \mathcal{A}[\![n]\!]\sigma = n$

taken a generic σ we conclude by rule $\dfrac{}{\langle n, \sigma \rangle \longrightarrow n}$

Inductive case

$\forall a_0, a_1.\ P(a_0) \wedge P(a_1) \Rightarrow P(a_0 \;\mathsf{op}\; a_1)$ Take generic a_0, a_1

we assume $P(a_i) \triangleq \forall \sigma.\ \langle a_i, \sigma \rangle \longrightarrow \mathcal{A}[\![a_i]\!]\sigma$

we need to prove $P(a_0 \,\mathsf{op}\, a_1) \triangleq \forall \sigma.\ \langle a_0 \,\mathsf{op}\, a_1, \sigma \rangle \longrightarrow \mathcal{A}[\![a_0 \,\mathsf{op}\, a_1]\!]\sigma$

$$= \mathcal{A}[\![a_0]\!]\sigma \; op \; \mathcal{A}[\![a_1]\!]\sigma$$

take a generic σ

$\langle a_0 \,\mathsf{op}\, a_1, \sigma \rangle \longrightarrow n$

$\nwarrow_{n = n_0 \; op \; n_1} \; \langle a_0, \sigma \rangle \longrightarrow n_0, \langle a_1, \sigma \rangle \longrightarrow n_1$

by inductive hypotheses, $n_i = \mathcal{A}[\![a_i]\!]\sigma$

and thus $n = n_0 \; op \; n_1 = \mathcal{A}[\![a_0]\!]\sigma \; op \; \mathcal{A}[\![a_1]\!]\sigma$

Denotational semantics of commands?

Recursive definitions

for divergence

$$\mathcal{C}[\![\cdot]\!] : \mathsf{Com} \to \mathbb{M} \to \mathbb{M} \cup \{\bot\}$$

$$\begin{aligned}
\mathcal{C}[\![\mathbf{skip}]\!]\sigma &\triangleq \sigma \\
\mathcal{C}[\![x := a]\!]\sigma &\triangleq \sigma[\mathcal{A}[\![a]\!]\sigma / x] \\
\mathcal{C}[\![c_0; c_1]\!]\sigma &\triangleq \mathcal{C}[\![c_1]\!](\mathcal{C}[\![c_0]\!]\sigma)
\end{aligned}$$

almost…

$$\mathcal{C}[\![\mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1]\!]\sigma \triangleq \begin{cases} \mathcal{C}[\![c_0]\!]\sigma & \text{if } \mathcal{B}[\![b]\!]\sigma \\ \mathcal{C}[\![c_1]\!]\sigma & \text{otherwise} \end{cases}$$

$$\mathcal{C}[\![\mathbf{while}\ b\ \mathbf{do}\ c]\!]\sigma \triangleq \begin{cases} \sigma & \text{if } \neg\mathcal{B}[\![b]\!]\sigma \\ \mathcal{C}[\![\mathbf{while}\ b\ \mathbf{do}\ c]\!](\mathcal{C}[\![c]\!]\sigma) & \text{otherwise} \end{cases}$$

almost…

not well-founded recursion!

how do we know one solution exists? how do we know it is unique?

The general problem

$$f : D \to D$$

a fixed point of f is $d \in D$ such that $d = f(d)$

let $F_f \triangleq \{d \in D \mid d = f(d)\} \subseteq D$

three questions:

- under which hypotheses $F_f \neq \emptyset$?
- if $F_f \neq \emptyset$, can we select a preferred element $\mathit{fix}(f) \in F_f$?
- and can we compute $\mathit{fix}(f)$?

Example

$D = \mathbb{N}$	F_f	$\mathit{fix}(f)$
$f(n) \triangleq n + 1$	$\varnothing$	
$f(n) \triangleq n/2$	$\{0\}$	0
$f(n) \triangleq n^2 - 5n + 8$	$\{2, 4\}$	2
$f(n) \triangleq n\%5$	$\{0, 1, 2, 3, 4\}$	0
$f(n) \triangleq \sum_{i \in \mathsf{div}(n)} i$	$\{6, 28, 496, ...\}$ perfect numbers	6

where $\mathsf{div}(x) \triangleq \{1\} \cup \{d \mid 1 < d < x, x\%d = 0\}$

Example

$D = \wp(\mathbb{N})$	F_f	$\mathit{fix}(f)$
$f(S) \triangleq S \cap \{1\}$	$\{\,\varnothing\,,\,\{1\}\,\}$	$\varnothing$
$f(S) \triangleq \mathbb{N} \setminus S$	$\varnothing$	
$f(S) \triangleq S \cup \{1\}$	$\{T \mid 1 \in T\}$	$\{1\}$
$f(S) \triangleq \{n \mid \exists m \in S, n \leq m\}$	$\{[0,k] \mid k \in \mathbb{N}\} \cup \{\varnothing, \mathbb{N}\}$	$\varnothing$

Ingredients

a partial order (to compare elements)

order preserving functions

iterative approximations

a base case

a limit solution