



**PSC 2022/23** (375AA, 9CFU)

Principles for Software Composition

Roberto Bruni

<http://www.di.unipi.it/~bruni/>

[http://didawiki.di.unipi.it/doku.php/  
magistraleinformatica/psc/start](http://didawiki.di.unipi.it/doku.php/magistraleinformatica/psc/start)

**07 - Recursion**

# Notation

$$f : X \rightarrow (Y \rightarrow Z)$$

$$f : X \rightarrow Y \rightarrow Z$$

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

$$\forall x \in X. f\ x : Y \rightarrow Z$$

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

$$\forall x \in X. \forall y \in Y. f\ x\ y \in Z$$

$$g : (X \rightarrow Y) \rightarrow Z$$

$$g\ x$$

$$\forall h \in (X \rightarrow Y). g(h) \in Z$$

$$f\ h$$

# Notation

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

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

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

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

# Notation

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

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

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

$$f \ x_1$$

# Notation

$$f : X \rightarrow Y$$

$$A \subseteq X$$

$$f|_A : A \rightarrow Y$$

$$\forall a \in A. f|_A(a) \stackrel{\Delta}{=} f(a)$$

# Predecessors

$A, \prec$

$a \in A$

$[a] \triangleq \{x \in A \mid x \prec a\}$

# Well-founded recursion

# Recursive definitions

$$\mathcal{A}[\cdot] : \text{Aexp} \rightarrow \mathbb{M} \rightarrow \mathbb{Z}$$

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

$$\mathcal{A}[n]\sigma \triangleq n$$

$$\mathcal{A}[x]\sigma \triangleq \sigma(x)$$

$$\mathcal{A}[a_0 \text{ op } a_1]\sigma \triangleq \mathcal{A}[a_0]\sigma \text{ op } \mathcal{A}[a_1]\sigma$$

The function is defined recursively:

how do we know one and exactly one value is associated to each expression? (true)



# Recursive definitions

$$N ::= 0 \mid s(N)$$

$$\mathcal{N}[\cdot] : \text{Nexp} \rightarrow \mathbb{N}$$

$$\mathcal{N}[0] \triangleq 0$$

$$\mathcal{N}[s(N)] \triangleq 1 + \mathcal{N}[s(s(N))]$$

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

# Well founded recursion

$A, \prec$  w.f.

$$F \triangleq \{F_a : ([a] \rightarrow B) \rightarrow B\}_{a \in A}$$

$$\forall a \in A. \forall h \in [a] \rightarrow B. F_a(h) \in B$$

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

$$\forall a \in A. f(a) = F_a(f|_{[a]})$$

# Example

$\mathbb{N}, <$

$$F \triangleq \{F_n : ([n] \rightarrow \mathbb{N}) \rightarrow \mathbb{N}\}_{n \in \mathbb{N}}$$

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

$$F_0 h \triangleq 1$$

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

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

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

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

$$f(n) = n!$$

# Example

$\mathbb{N}, <$

$m \in \mathbb{N}$

$$F^m \triangleq \{F_n^m : ([n] \rightarrow \mathbb{N}) \rightarrow \mathbb{N}\}_{n \in \mathbb{N}}$$

$$F_0^m : (\emptyset \rightarrow \mathbb{N}) \rightarrow \mathbb{N}$$

$$F_{n+1}^m : (\{n\} \rightarrow \mathbb{N}) \rightarrow \mathbb{N}$$

$$F_0^m h \triangleq 0$$

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

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

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

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

# Ackermann function

a computable function that is total but not primitive recursive

$$m \in \mathbb{N} \quad \text{ack}_m : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$$

$$\text{ack}_m(0, 0) \stackrel{\Delta}{=} m$$

$$\text{ack}_m(0, n + 1) \stackrel{\Delta}{=} \text{ack}_m(0, n) + 1$$

$$\text{ack}_m(1, 0) \stackrel{\Delta}{=} 0$$

$$\text{ack}_m(k + 1, n + 1) \stackrel{\Delta}{=} \text{ack}_m(k, \text{ack}_m(k + 1, n))$$

$$\text{ack}_m(k + 2, 0) \stackrel{\Delta}{=} 1$$

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

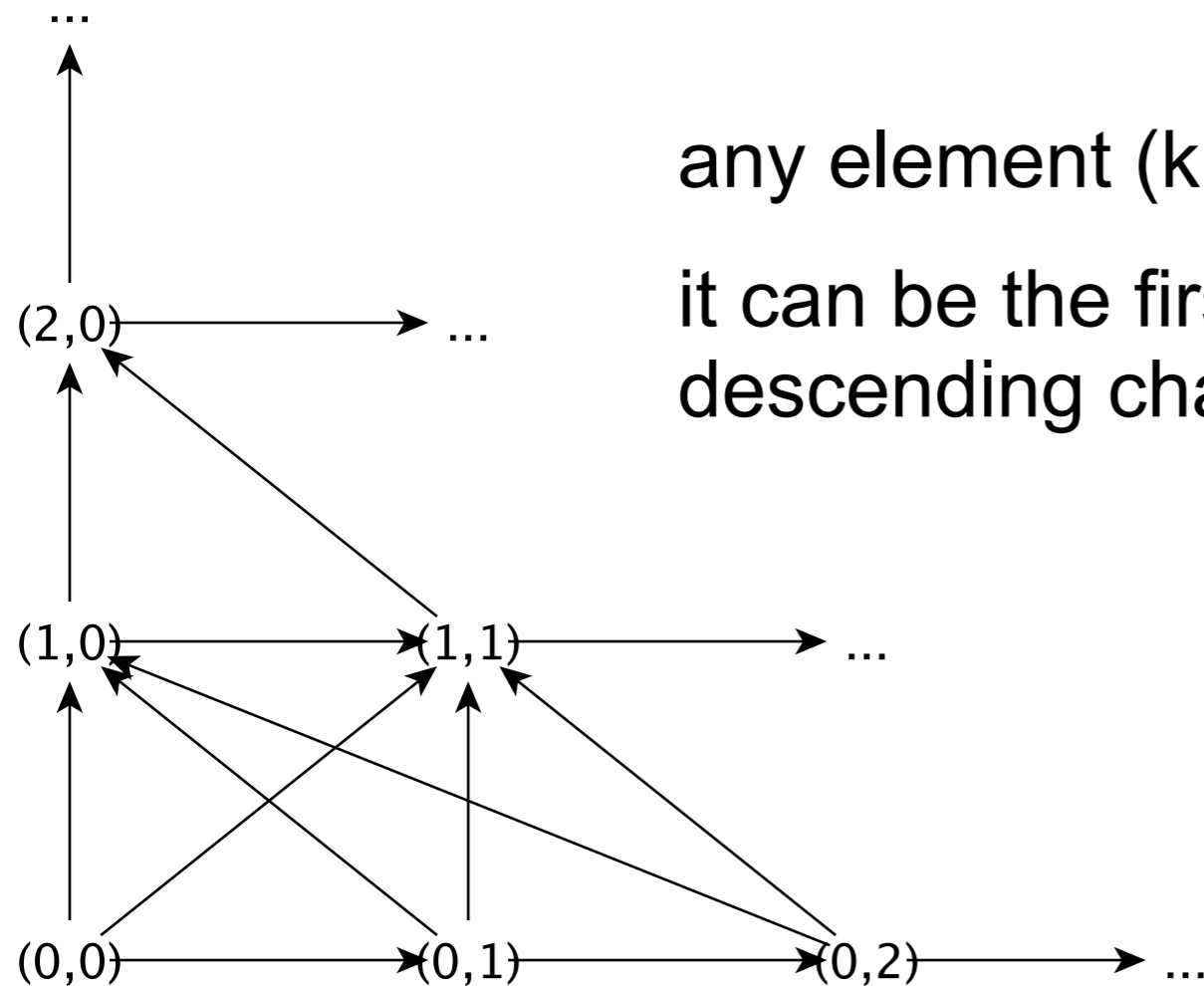
$$(k, n) \prec (k + 1, n')$$

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

# 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

$$\begin{aligned}(k, n) &< (k + 1, n') \\ (k, n) &< (k, n + 1)\end{aligned}\quad \prec^+ \text{ is w.f.}$$

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

can we find  $m$  minimal in  $Q$ ?

$$\hat{k} \triangleq \min \{k \mid (k, n) \in Q\} \text{ (non-empty because } Q \neq \emptyset)$$

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

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

# Ackermann function

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

$$ack_m(0, n + 1) \triangleq ack_m(0, n) + 1$$

$n$  increments of base case  $m$

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



# Ackermann function

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

add  $m$  for  $n$  times to the base case 0

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

# Ackermann function

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

$$ack_m(k + 2, 0) \triangleq 1$$

$$ack_m(2, 0) \triangleq 1$$

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

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

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

multiplies by  $m$  for  $n$  times the base case 1

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

# Ackermann function

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

$$ack_m(k + 2, 0) \triangleq 1$$

$$ack_m(3, 0) \triangleq 1$$

$$ack_m(3, n + 1) \triangleq ack_m(2, ack_m(3, n))$$

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

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

$n$  times exponentiation

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

# Ackermann function

it grows faster than any primitive recursive function

$$ack_3(0, 3) \stackrel{\triangle}{=} 3 + 3 = 6$$

$$ack_3(1, 3) \stackrel{\triangle}{=} 3 \cdot 3 = 9$$

$$ack_3(2, 3) \stackrel{\triangle}{=} 3^3 = 27$$

$$ack_3(3, 3) \stackrel{\triangle}{=} 3^{3^3} = 3^{27} \simeq 7.6 \cdot 10^{12}$$

# Arithmetic expressions

$A_{\text{exp}}, \prec$

$a_i \prec a_0 \text{ op } a_1$

$\mathcal{A}[\cdot] : A_{\text{exp}} \rightarrow \mathbb{M} \rightarrow \mathbb{Z}$

$\mathcal{A}[n]\sigma \stackrel{\Delta}{=} n$

$\mathcal{A}[x]\sigma \stackrel{\Delta}{=} \sigma(x)$

$\mathcal{A}[a_0 \text{ op } a_1]\sigma \stackrel{\Delta}{=} \mathcal{A}[a_0]\sigma \text{ op } \mathcal{A}[a_1]\sigma$

# Boolean expressions

$\text{Bexp}, <$

$b_i < b_0 \text{ bop } b_1$

$b < \neg b$

$\mathcal{B}[\cdot] : \text{Bexp} \rightarrow \mathbb{M} \rightarrow \mathbb{Z}$

$\mathcal{B}[v]\sigma \triangleq v$

$\mathcal{B}[a_0 \text{ cmp } a_1]\sigma \triangleq \mathcal{A}[a_0]\sigma \text{ cmp } \mathcal{A}[a_1]\sigma$

$\mathcal{B}[\neg b]\sigma \triangleq \neg \mathcal{B}[b]\sigma$

$\mathcal{B}[b_0 \text{ bop } b_1]\sigma \triangleq \mathcal{B}[b_0]\sigma \text{ bop } \mathcal{B}[b_1]\sigma$

# Consistency of expressions

# Consistency?

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

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

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

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

**structural induction!**

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

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

$$\forall a_0, a_1. P(a_0) \wedge P(a_1) \Rightarrow P(a_0 \text{ op } a_1)$$

---

$$\forall a. P(a)$$



# Base cases

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

take  $x \in \text{Ide}$

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

taken a generic  $\sigma$  we conclude by rule

$$\frac{}{\langle x, \sigma \rangle \longrightarrow \sigma(x)}$$

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

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  $\sigma$  we conclude by rule

$$\frac{}{\langle n, \sigma \rangle \longrightarrow n}$$

# Inductive case

$\forall a_0, a_1. P(a_0) \wedge P(a_1) \Rightarrow P(a_0 \text{ op } a_1)$  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  $P(a_0 \text{ op } a_1) \triangleq \forall \sigma. \langle a_0 \text{ op } a_1, \sigma \rangle \longrightarrow \mathcal{A}[[a_0 \text{ op } a_1]]\sigma$   
 $= \mathcal{A}[[a_0]]\sigma \text{ op } \mathcal{A}[[a_1]]\sigma$

take a generic  $\sigma$

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

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

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

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

# Denotational semantics of commands?

# Recursive definitions

for divergence

$$\mathcal{C}[\cdot] : \text{Com} \rightarrow \mathbb{M} \rightarrow \mathbb{M} \cup \{\perp\}$$

$$\mathcal{C}[\text{skip}]\sigma \stackrel{\Delta}{=} \sigma$$

$$\mathcal{C}[x := a]\sigma \stackrel{\Delta}{=} \sigma[\mathcal{A}[a]\sigma / x]$$

$$\mathcal{C}[c_0; c_1]\sigma \stackrel{\Delta}{=} \mathcal{C}[c_1](\mathcal{C}[c_0]\sigma) \text{ almost...}$$

$$\mathcal{C}[\text{if } b \text{ then } c_0 \text{ else } c_1]\sigma \stackrel{\Delta}{=} \begin{cases} \mathcal{C}[c_0]\sigma & \text{if } \mathcal{B}[b]\sigma \\ \mathcal{C}[c_1]\sigma & \text{otherwise} \end{cases}$$

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

almost...

not well-founded recursion!

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

# The general problem

$$f : D \rightarrow D$$

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

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

three questions:

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

# Example

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

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

# Example

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

# Ingredients

a partial order (to compare elements)

order preserving functions

iterative approximations

a base case

a limit solution