Lingua Project

(9) A relational model of program correctness

(Sec. 8)

The book "**Denotational Engineering**" may be downloaded from:
https://moznainaczej.com.pl/what-has-been-done/the-book

Andrzej Jacek Blikle

March 29th, 2025

Chain-complete partially ordered sets

$\sqsubseteq$: Rel(A,A) = {R | R $\subseteq$ A x A}   ordering relation in A

DEF. partial order:

a $\sqsubseteq$ a   reflexivity

if a $\sqsubseteq$ b and b $\sqsubseteq$ c then a $\sqsubseteq$ c   transitivity

if a $\sqsubseteq$ b and b $\sqsubseteq$ a then a = b   weak antisymmetricity

b : B is called the least element in B $\subseteq$ A if ($\forall$ b' : B) b $\sqsubseteq$ b'

a : A is called the upper bound of B $\subseteq$ A, if ($\forall$ b : B) b $\sqsubseteq$ a

$a_1 \sqsubseteq a_2 \sqsubseteq a_3 \sqsubseteq \ldots$ a chain

$\lim(a_i \mid i = 1,2,\ldots)$ (def) least upper bound (if exists)

DEF. (A, $\sqsubseteq$, Φ) is called a chain-complete partially ordered set (CPO) if:

1. every chain in A has a limit,
2. Φ is the least element of A

Continuous functions in CPO's

$(A, \sqsubseteq, \Phi)$ — CPO

DEF. $f : A \longmapsto A$ is continuous if

1. if $a_1 \sqsubseteq a_2 \sqsubseteq \ldots$ then $f.a_1 \sqsubseteq f.a_2 \sqsubseteq \ldots$,
2. if $a_1 \sqsubseteq a_2 \sqsubseteq \ldots$ has a limit then $f.a_1 \sqsubseteq f.a_2 \sqsubseteq \ldots$ has a limit,
3. $\lim(f.a_1 \sqsubseteq f.a_2 \sqsubseteq \ldots) = f.[\lim(a_1 \sqsubseteq a_2 \sqsubseteq \ldots)]$.

A composition of continuous functions is continuous.

Kleene's fixed-point theorem

If $f : A \longmapsto A$ is continuous, then the least solution of

$x = f.x$

exists and equals $\lim(f^n.\Phi \mid n = 0,1,2,\ldots)$.

A fundament for recursive definitions of languages, functions and domains

Cartesian CPO's

$(A, \sqsubseteq, \Phi)$ — a CPO

$(A^{cn}, \sqsubseteq^{cn}, \Phi^{cn})$ — a Cartesian CPO of tuples

(a-1,…a-n) $\sqsubseteq^{cn}$ (b-1,…,b-n) iff(def) a-i $\sqsubseteq$ b-i for i = 1;n

f : $A^{cn} \longmapsto A$ is continuous in first argument iff(def)

f.(x, a-2,…,a-n) : $A \longmapsto A$ is continuous for any tuple (a-2,…,a-n)

f : $A^{cn} \longmapsto A$ is continuous iff(def) is continuous in all arguments

Lemma

if f-i : $A^{cn} \longmapsto A$ for i = 1;n are continuous then

f(a-1,…,a-n) = (f-1(a-1,…,a-n),…,f-n(a-1,…,a-n)) is continuous

A CPO of formal languages

$A = \{a_1,\ldots,a_n\}$ — an alphabet
$Lan(A) = \{L \mid L \subseteq A^*\}$ — the set of all languages over A
$(Lan(A), \subseteq, \{\ \})$ — CPO of formal languages over A

P, Q : Lan(A)

P © Q	= {p © q | p : P and q : Q}	— concatenation
P Q	= {p q | p : P and q : Q}	— (an alternative notation)
P^0	= {ε}	
P^n	= P $P^{(n-1)}$ for n > 0	— n-th power
P^+	= P^1 | P^2 | …	— plus-power
P^*	= P^+ | P^0	— star-power
P^{c*}	= {$(p_1,\ldots,p_n)$ | n ≥ 0 and p_i : P}	— Cartesian power

All function defined above, and union, are <u>continuous</u>

<u>Associativity</u> and <u>distributivity</u>
(P Q) L = P (Q L) will be written P Q L
(P | Q) L = (P L) | (Q L) will be written PL | QL

Equational grammars (example)

car : Character = {a,…,z,0,…,9}
ide : Identifier = Character | Character © Identifier
exp : Expression = Identifier | {(} © Expression © {+} © Expression © {)}

Theorem
Equational (polynomial) grammars are equivalent to Chomsky's context-free grammars and Backus-Naur grammars.

A CPO of binary relations

$Rel.(A, A) = \{R \mid R \subseteq A \times A\}$

$(Rel(A, A), \subseteq, \{\ \})$ — CPO of binary relations

$[B] = \{(b, b) \mid b:B\}$; $B \subseteq A$ — identity relations (function)

$(a, b) : R$ will be written as $a\ R\ b$

$P, R : Rel(A,A)$

$P \bullet R = \{(a, c) \mid (\exists b:B)\ (a\ P\ b\ \&\ b\ R\ c)\}$ — composition

$R^0 = [A]$

$R^n = R \bullet R^{n-1}$ for $n > 0$

$R^+ = R^1 \mid R^2 \mid \ldots$

$R^* = R^+ \mid R^0$

All function defined above, and union, are <u>continuous</u>

<u>Associativity</u> and <u>distributivity</u> over union

$(P\ R)\ Q = P\ (R\ Q)$ will be written $P\ R\ Q$

$(P \mid R)\ Q = (P\ Q) \mid (R\ Q)$ will be written $P\ Q \mid R\ Q$

If P, R – functions, then $P \bullet R$ – function

A CPO of domains

(Domain, ⊆, { }) — the Cohn's CPO of domains

DEF (M.P. Cohn)
(1) { }, Identifier, Integer, Character, … belong to Domain
(2) Domain is closed under all our domain operations (see below)
(2) Domain is closed under enumerable unions of sets

A | B	— set-theoretic union
$A \cap B$	— set-theoretic intersection
A x B	— Cartesian product
A^{cn}	— Cartesian n-th power
A^{c+}	— Cartesian plus-iteration
A^{c*}	— Cartesian star-iteration
FinSub.A	— the set of all finite subsets
$A \Longrightarrow B$	— the set of all mappings including the empty mapping
A – B	— set-theoretic difference
Sub.A	— the set of all subsets
$A \rightarrow B$	— the set of all functions from A to B
$A \longmapsto B$	— the set of all total functions from A to B
Rel.(A,B)	— the set of all relations between A and B

continuous and noncontinuous domain constructors

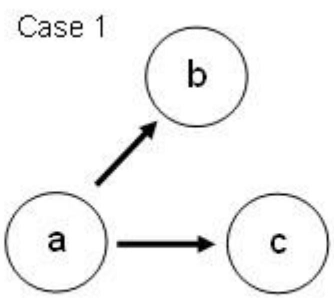
red indicates non-continuity

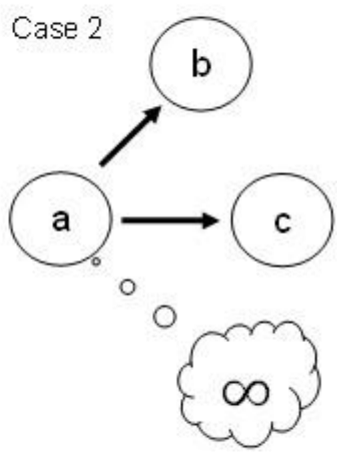
Binary relations

S – a set of states
Rel.(S, S) = {R | R ⊆ S x S}
a R b means (a,b) : R

A ⊆ S
[A] = {(s, s) | s : A} – a subset of identity

Two interpretations of a R b & a R c





In this model we can't distinguish between these two situations

We can describe abortion if states may carry errors.

p : S ⟼ {tt, ff, ee}   a 3-valued predicate; ee – error or ?
  C = {s | p.s = tt}
¬C = {s | p.s = ff}
(C, ¬C) represents p unambiguously

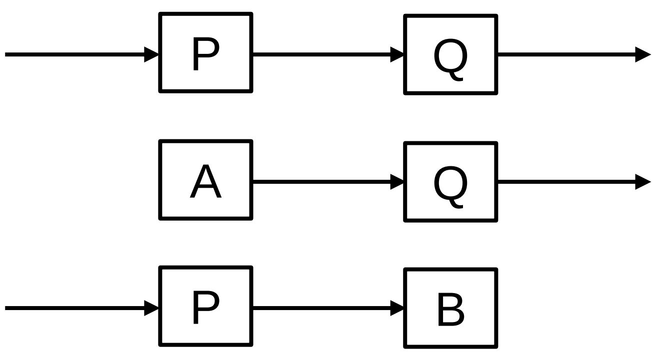
Three composition operations

(definitions)

P, Q : Rel.(S, S)
A ⊆ S

Sequential compositions

P ● Q = { (a,b) | (∃ c) a P c and c Q b}   is continuous in (Rel.(S, S), ⊆, Φ)
A ● Q = { b | (∃ a : A) a Q b}   - outputs of Q for inputs in A
P ● B = { a | (∃ b : B) a P b}   - inputs of P with outputs in B



P ● Q to be written PQ

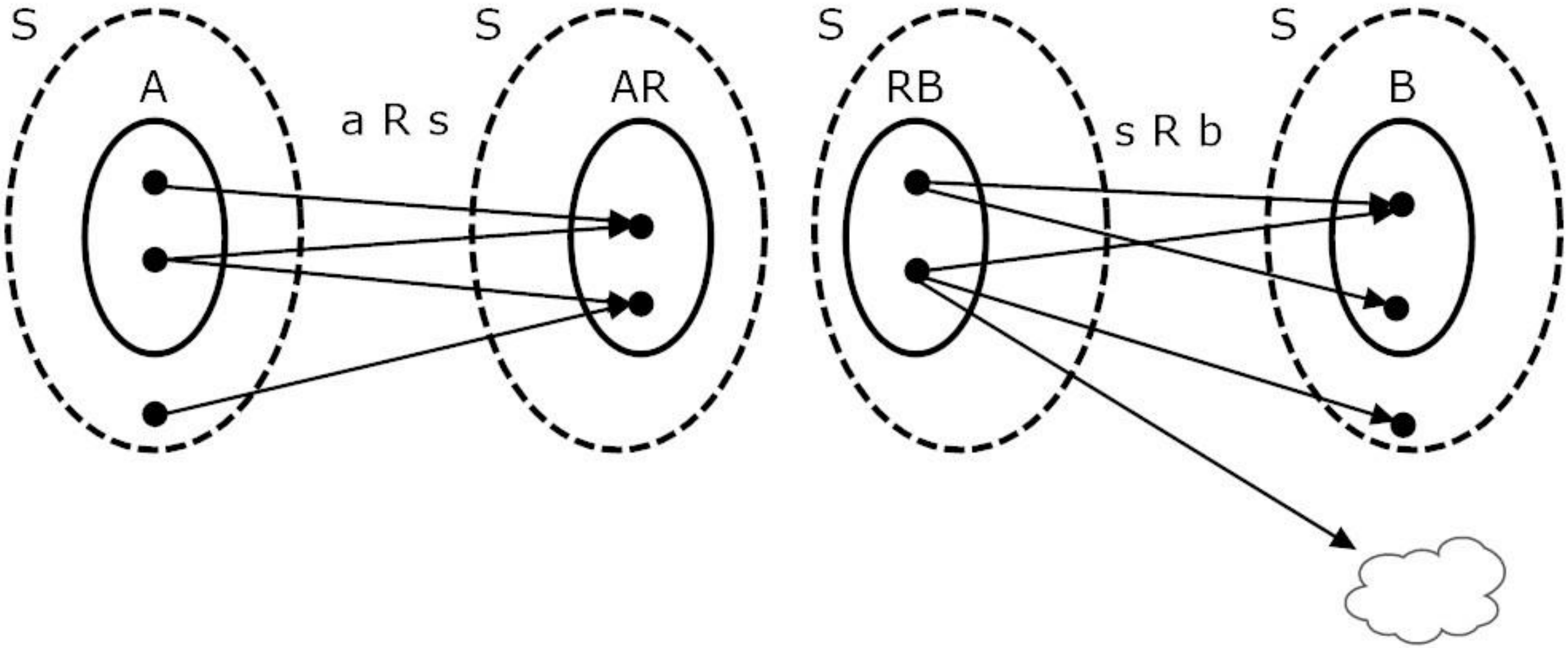
A ● Q to be written AQ

P ● B to be written PB

(AR) | (BR) to be written AR | BR

Composition operations

(interpretations)



Composition operations

(basic properties)

For $P, Q, R : Rel.(S, S)$ and $A, B, C \subseteq S$

associativity

$P(QR) = (PQ)R$

$A(RQ) = (AR)Q$

$(RQ)B = R(QB)$

distributivity

$(A \mid B)\, R = (AR) \mid (BR)$

$A\,(R \mid Q) = (AR) \mid (AQ)$

monotonicity

if $A \subseteq B$ then $AR \subseteq BR$

if $R \subseteq Q$ then $AR \subseteq AQ$

$[A]B = A \cap B$

$A[B] = A \cap B$

$(A \cap B)R = A\,[B]\,R$

$R(A \cap B) = R\,[A]\,B$

$(A \cap B)R \subseteq C$ is equivalent to $A[B]R \subseteq C$

if $A \subseteq [B]RC$ then $(A \cap B) \subseteq RC$

The least solution of the fixed-point equation

$$P = [C]\,RP \mid [\neg C]$$

equals $([C]\,R)^*[\neg C]$

while $([C], [\neg C])$ **do** R **od**

Structural constructors of nondeterministic programs

Definitions:

P **;** Q	= P ● Q
if (C, ¬C) **then** P **else** Q **fi**	= [C]P | [¬C]Q
while (C, ¬C) **do** P **od**	= ([C]P)*[¬C]

Partial and total correctness

$AR \subseteq B$ — partial correctness of R for precondition A and postcondition B;
(∀a:A) if (∃ b) aRb, then b:B

$A \subseteq RB$ — weak total correctness of R for precondition A and postcondition B;
(∀a:A) (∃ b) aRb and b:B

but there may exist b1 that a R b1 and b1 /: B (the weakness)

For functions weak total correctness = strong total correctness

For $F : S \rightarrow S$ and $A, B \subseteq S$

termination property

$A \subseteq FB$ implies $AF \subseteq B$

$A \subseteq FB$ iff $AF \subseteq B$ and $A \subseteq FS$

clean termination = termination without error

Non-decidability of termination property

Does the following program terminates for all n (Collatz hypothesis 1937)?

```
x := n;
while x > 1
  do
    if x mod 2 = 0 then x := x/2 else x := 3x + 1 fi
  od
```

It has been proved that it terminates for $n < 5*2^{68}$.

Clean total correctness of while
Auxiliary concepts

ograniczona powtarzalność

$F : S \to S$ has a limited replicability in a set $N \subseteq S$ if there is no infinite sequence

$s, F.s, F.(F.s), \ldots$ in N.

E.g. Sin.[x := x-1] : $S \to S$
has limited replicability in the set of states N = {sta | sta.x > 0}

dobrze ufundowany

A partially ordered set (U, >) is said to be a well-founded set, if there is no infinite decreasing sequence in it, i.e., a sequence $u_1 > u_2 > \ldots$

Lemma 8.7.2-1

If there exists a well founded set (U, <) and a function $K : N \mapsto U$ such that for any a : N, F.a = !, F.a : N and

K.a > K.(F.b)

then F has limited replicability in N.

Proof rules for two structural constructors

Weak total correctness of composition

For any A,D ⊆ S and P,Q : Rel(S,S)
there exist conditions B and C such that

(1) A ⊆ PB
(2) C ⊆ QD
(3) B ⊆ C

---

(4) A ⊆ (PQ)D

Weak total correctness of branching

For any A,B, C ⊆ S and P,Q : Rel(S,S)
if C ∩ ¬C = {} then

(1) A ∩ C ⊆ PB
(2) A ∩ ¬C ⊆ QB
(3) A ⊆ C | ¬C

---

(4) A ⊆ **if** (C, ¬C) **then** P **else** Q **fi** B

in classical logic
this is a tautology

Proof rule for deterministic while-do-od

For any A,B,N ⊆ S and any function F : S → S,
and any disjoint C,¬C ⊆ S

(1) A ⊆ N
(2) N ⊆ C | ¬C
(3) N ∩ ¬C ⊆ B
(4) N ∩ C ⊆ FN (clean total correctness of F)
(5) [C]F has limited replicability in N

---

(6) A ⊆ **while** (C,¬C) **do** F **od** B

Proof rule for simple recursion

If F is the least solution of the equation $X = HXT \mid E$ where H, T, and E are functions and the domains of H and E are disjoint, then the following rule holds:

(1) $(\forall Q)\ (AQ \subseteq B$ implies $A(HQT) \subseteq B)$

(2) $AE \subseteq B$

(3) $A \subseteq FS$

(4) $A \subseteq FB$


Thank you for your attention