

Lecture Notes on Denotational Semantics

Jeremy G. Siek

November 5, 2017

Contents

<i>Binary Arithmetic</i>	2
<i>An Imperative Language</i>	4
<i>Recursive Definitions via Least Fixed Points</i>	5
<i>A Functional Language</i>	9

Binary Arithmetic

Borrowing and combining elements from Chapter 4 of ?, we consider the language of binary arithmetic specified in Figure 1. The Syntax defines the form of the programs and the Semantics specifies the behavior of running the program. In this case, the behavior is simply to output a number (in decimal). Our grammar for binary numerals departs slightly from ?, with ϵ representing the empty string of digits.

The main purpose of a semantics is communicate in a precise way with other people, primarily language implementers and programmers. Thus, it is incredibly important for the semantics to be written in a way that will make it most easily understood, while still being completely precise. Here we have chosen to give the semantics of binary arithmetic in terms of decimal numbers because people are generally much more familiar with decimal numbers.

When writing down a semantics, one is often tempted to consider the efficiency of a semantics, as if it were an implementation. Indeed, it would be straightforward to transcribe the definitions of E and N in Figure 1 into your favorite programming language and thereby obtain an interpreter. All other things being equal, it is fine to prefer a semantics that is suggestive of an implementation, but one should prioritize ease of understanding first. As a result, some semantics that we study may be more declarative in nature. This is not to say that one should not consider the efficiency of implementations when designing a language. Indeed, the semantics should be co-designed with implementations to avoid accidental designs that preclude the desired level of efficiency. Thus, a recurring theme of these notes will be to consider implementations of languages alongside their semantics.

Figure 2 presents an interpreter for binary arithmetic. This interpreter, in a way reminiscent of real computers, operates on the binary numbers directly. The auxiliary functions *add* and *mult* implement the algorithms you learned in grade school, but for binary instead of decimals.

Exercise 1 Prove that $N(\text{add3}(d_1, d_2, d_3)) = d_1 + d_2 + d_3$.

Exercise 2 Prove that $N(\text{add}(n_1, n_2, c)) = N(n_1) + N(n_2) + c$.

Exercise 3 Prove that $N(\text{mult}(n_1, n_2)) = N(n_1)N(n_2)$.

Exercise 4 Prove that the interpreter is correct. That is

$$N(I(e)) = E(e)$$

Reading: ? Chapter 4
Exercises: 4.2, 4.6

Syntax

digit	$d ::=$	$0 \mid 1$
binary numeral	$n ::=$	$\epsilon \mid nd$
expression	$e ::=$	$n \mid e + e \mid e \times e$

Semantics

$$\begin{aligned} N(\epsilon) &= 0 \\ N(nd) &= 2N(n) + d \\ E(n) &= N(n) \\ E(e_1 + e_2) &= E(e_1) + E(e_2) \\ E(e_1 \times e_2) &= E(e_1)E(e_2) \end{aligned}$$

Figure 1: Language of binary arithmetic

Interpreter

$$\begin{aligned}
 I(n) &= n \\
 I(e_1 + e_2) &= \text{add}(I(e_1), I(e_2), 0) \\
 I(e_1 \times e_2) &= \text{mult}(I(e_1), I(e_2))
 \end{aligned}$$

Figure 2: Binary arithmetic interpreter.

Auxiliary Functions

$$\text{add3}(d_1, d_2, d_3) = \begin{cases} 00 & \text{if } n = 0 \\ 01 & \text{if } n = 1 \\ 10 & \text{if } n = 2 \\ 11 & \text{if } n = 3 \end{cases} \quad \text{where } n = d_1 + d_2 + d_3$$

$$\text{add}(\epsilon, \epsilon, c) = \begin{cases} \epsilon & \text{if } c = 0 \\ \epsilon 1 & \text{otherwise} \end{cases}$$

$$\text{add}(n_1 d_1, n_2 d_2, c) = \text{add}(n_1, n_2, c') d_3 \quad \text{if } \text{add3}(d_1, d_2, c) = c' d_3$$

$$\text{add}(n_1 d_1, \epsilon, c) = \text{add}(n_1 d_1, \epsilon 0, c)$$

$$\text{add}(\epsilon, n_2 d_2, c) = \text{add}(\epsilon 0, n_2 d_2, c)$$

$$\text{mult}(n_1, \epsilon) = \epsilon$$

$$\text{mult}(n_1, n_2 0) = \text{mult}(n_1, n_2) 0$$

$$\text{mult}(n_1, n_2 1) = \text{add}(n_1, \text{mult}(n_1, n_2) 0, 0)$$

An Imperative Language

Figure 3 defines a language with mutable variables, a variant of the IMP [??] and WHILE [?] languages that often appear in textbooks on programming languages. As a bonus, we include the while loop, even though ? does not cover loops until Chapter 6. The reason for his delayed treatment of while loops is that their semantics is typically expressed in terms of fixed points of continuous functions, which takes some time to explain. However, it turns out that the semantics of while loops can be defined more simply.

To give meaning to mutable variables, we use a *Store* which is partial function from variables (identifiers) to numbers.

$$\text{Store} = \text{Id} \rightarrow \text{Nat}$$

We write $[x \mapsto n]s$ for $\{x \mapsto n\} \cup (s|_{\text{dom}(s) - \{x\}})$.

The syntax of expressions is extended to include variables, so the meaning of expressions must be parameterized on the store. The meaning of a variable x is the associated number in the store s .

$$E x s = s x$$

A program takes a number as input and it may produce a number or it might diverge. Traditional denotational semantics model this behavior with a partial function $\text{Nat} \rightarrow \text{Nat}$. Here we shall use the alternate, but equivalent, approach of using a relation $\text{Nat} \times \text{Nat}$.

We define the while loop using an auxiliary relation named *loop*, which we define inductively in Figure 3. Its two parameters are for the meaning of the condition b and the body c of the loop. If the meaning of the condition m_b is false, then the loop is already finished so the starting and finishing stores are the same. If the condition m_b is true, then the loop executes the body, relating the starting store s_1 to an intermediate store s_2 , and then the loop continues, relating s_2 to the finishing store s_3 .

We define an implementation of the imperative language, in terms of an abstract machine, in Figure 4. The machine executes one command at a time, similar to how a debugger such as gdb can be used to view the execution of a C program one statement at a time. Each command causes the machine to transition from one state to the next, where a state is represented by a control component and the store. The control component is the sequence of commands that need to be executed, which is convenient to represent as a command of the following form.

$$\text{control } k ::= \text{skip} \mid c ; k$$

The partial function *eval*, also defined in Figure 4 in the main entry point for the abstract machine.

Reading: ? Chapter 5
Exercises: 5.4, 5.5 a, 5.9

Syntax

variables	$x \in \mathbb{X}$
expressions	$e ::= \dots \mid x$
conditions	$b ::= \text{true} \mid \text{false} \mid e = e \mid \neg b \mid b \vee b \mid b \wedge b$
commands	$c ::= \text{skip} \mid x := e \mid c ; c \mid \text{if } b \text{ then } c \text{ else } c \mid \text{while } b \text{ do } c$

Semantics

$$P c = \{(n, s' Z) \mid (\{A \mapsto n\}, s') \in C c\}$$

$$C \text{ skip} = \text{id}$$

$$C(x := e) = \{(s, [x \mapsto E e s]s) \mid s \in \text{Store}\}$$

$$C(c_1 ; c_2) = C c_2 \circ C c_1$$

$$C \left(\begin{array}{l} \text{if } b \text{ then } c_1 \\ \text{else } c_2 \end{array} \right) = \begin{cases} C c_1 & \text{if } B b s = \text{true} \\ C c_2 & \text{if } B b s = \text{false} \end{cases}$$

$$C(\text{while } b \text{ do } c) = \text{loop}(B b, C c)$$

$$\frac{m_b s = \text{false}}{(s, s) \in \text{loop}(m_b, m_c)}$$

$$\frac{m_b s_1 = \text{true} \quad (s_1, s_2) \in m_c \quad (s_2, s_3) \in \text{loop}(m_b, m_c)}{(s_1, s_3) \in \text{loop}(m_b, m_c)}$$

Figure 3: An Imperative Language

$$k, s \longrightarrow k', s'$$

$$\begin{array}{ll}
\text{skip} ; k, s \longrightarrow k, s & \\
(x := e) ; k, s \longrightarrow k, [x \mapsto E(e)(s)]s & \\
(c_1 ; c_2) ; k, s \longrightarrow c_1 ; (c_2 ; k), s & \\
(\text{if } b \text{ then } c_1 \text{ else } c_2) ; k, s \longrightarrow c_1 ; k, s & \text{if } Bbs = \text{true} \\
(\text{if } b \text{ then } c_1 \text{ else } c_2) ; k, s \longrightarrow c_2 ; k, s & \text{if } Bbs = \text{false} \\
(\text{while } b \text{ do } c) ; k, s \longrightarrow c ; ((\text{while } b \text{ do } c) ; k), s & \text{if } Bbs = \text{true} \\
(\text{while } b \text{ do } c) ; k, s \longrightarrow k, s & \text{if } Bbs = \text{false} \\
\text{eval}(c) = \{(n, n') \mid (c ; \text{skip}), \{A \mapsto n\} \longrightarrow^* \text{skip}, s' \text{ and } n' = s'(Z)\} &
\end{array}$$

Figure 4: An Abstract Machine for an Imperative Language

Notation: given a relation R , we write $R(a)$ for the image of $\{a\}$ under R . For example, if $R = \{(0, 4), (1, 2), (1, 3), (2, 5)\}$, then $R(1) = \{2, 3\}$ and $R(0) = \{4\}$.

Exercise 5 Prove that if $k, s \longrightarrow k', s'$, then $Cks = Ck's'$.

Exercise 6 Prove that $P(c) = \text{eval}(c)$.

Recursive Definitions via Least Fixed Points

We shall revisit the semantics of the imperative language, this time taking the traditional but more complex approach of defining `while` with a recursive equation and using least fixed points to solve it. Recall that the meaning of a command is a partial function from stores to stores, or more precisely,

$$C(c) : \text{Store} \rightarrow \text{Store}$$

The meaning of a loop `(while b do c)` is a solution to the equation

$$w = \lambda s. \text{if } Bbs \text{ then } w(Ccs) \text{ else } s \quad (1)$$

In general, one can write down recursive equations that do not have solutions, so how do we know whether this one does? When is there a unique solution? The theory of least fixed points provides answers to these questions.

Definition 1. A fixed point of a function is an element that gets mapped to itself, e.g. $x = f(x)$.

In this case, the element that we're interested in is w , which is itself a function, so our f will be higher-order function. We reformulate Equation 1 as a fixed point equation by abstracting away the

Reading: ? Chapter 6
Exercises: 6.2 a, 6.6, 8

recursion into a parameter r .

$$w = F_{b,c}(w) \quad \text{where } F_{b,c} r s = \text{if } B b s \text{ then } r(C c s) \text{ else } s \quad (2)$$

There are quite a few theorems in the literature that guarantee the existence of fixed points, but with different assumptions about the function and its domain. For our purposes, the CPO Fixed-Point Theorem will do the job. The idea of this theorem is to construct an infinite sequence that provides increasingly better approximations of the least fixed point. The union of this sequence will turn out to be the least fixed point.

The CPO Fixed-Point Theorem is quite general; it is stated in terms of a function F over partially ordered sets with a few mild conditions. The ordering captures the notion of approximation, that is, we write $x \sqsubseteq y$ if x approximates y .

Definition 2. A **partially ordered set** (poset) is a pair (L, \sqsubseteq) that consists of a set L and a partial order \sqsubseteq on L .

For example, consider the poset $(\mathbb{N} \rightarrow \mathbb{N}, \sqsubseteq)$ of partial functions on natural numbers. Some partial function f is a better approximation than another partial function g if it is defined on more inputs, that is, if the graph of f is a subset of the graph of g . Two partial functions are incomparable if neither is a subset of the other.

The sequence of approximations will start with the worst approximation, a bottom element, written \perp , that contains no information. (For example, \emptyset is the \perp for the poset of partial functions.) The sequence proceeds to by applying F over and over again, that is,

$$\perp \quad F(\perp) \quad F(F(\perp)) \quad F(F(F(\perp))) \quad \dots \quad F^i(\perp) \quad \dots$$

But how do we know that this sequence will produce increasingly better approximations? How do we know that

$$F^i(\perp) \sqsubseteq F^{i+1}(\perp)$$

We can ensure this by requiring the output of F to improve when the input improves, that is, require F to be monotonic.

Definition 3. Given two partial orders (A, \sqsubseteq) and (B, \sqsubseteq) , $F : A \rightarrow B$ is **monotonic** iff for any $x, y \in A$, $x \sqsubseteq y$ implies $F(x) \sqsubseteq F(y)$.

Proposition 1. The functional $F_{b,c}$ for *while* loops (2) is monotonic.

Proof. Let $f, g : \text{Store} \rightarrow \text{Store}$ such that $f \sqsubseteq g$. We need to show that $F_{b,c}(f) \sqsubseteq F_{b,c}(g)$. Let s be an arbitrary state. Suppose $B b s = \text{true}$.

$$F_{b,c} f s = f(C c s) \sqsubseteq g(C c s) = g(C c s) = F_{b,c} g s$$

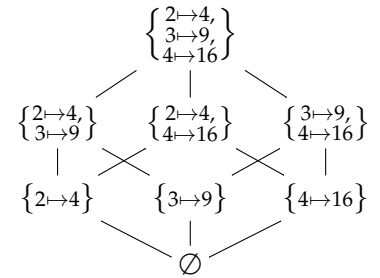


Figure 5: A poset of partial functions.

So we have $F_{b,c}(f) \subseteq F_{b,c}(g)$. Next suppose $Bbs = \text{false}$.

$$F_{b,c}fs = s = F_{b,c}gs$$

So again we have $F_{b,c}(f) \subseteq F_{b,c}(g)$. Having completed both cases, we conclude that $F_{b,c}(f) \subseteq F_{b,c}(g)$. \square

We have $\perp \sqsubseteq F(\perp)$ because \perp is less or equal to everything. Then we apply monotonicity to obtain $F(\perp) \sqsubseteq F(F(\perp))$. Continuing in this way we obtain the sequence of increasingly better approximations in Figure 6. If at some point the approximation stops improving, but instead F produces an element that is merely equal to the last one, then we have found a fixed point. However, because we are interested in elements that are partial functions, which are infinite, the sequences of approximations will also be infinite. So we'll need some other way to go from the sequences of approximations to the actual fixed point.

The solution is to take the union of all the approximations. The analogue of union for an arbitrary partial order is least upper bound.

Definition 4. Given a subset S of a partial order (L, \sqsubseteq) , an **upper bound** of S is an element y such that for all $x \in S$ we have $x \sqsubseteq y$. The **least upper bound (lub)** of S , written $\sqcup S$, is the least of all the upper bounds of S , that is, given any upper bound z of S , we have $\sqcup S \sqsubseteq z$.

In arbitrary posets, a least upper bound may not exist for an arbitrary subset. In particular, for the poset $(\mathbb{N} \rightarrow \mathbb{N}, \subseteq)$, two partial functions do not have a lub if they are inconsistent, that is, if they map the same input to different outputs, such as $\{3 \mapsto 8\}$ and $\{3 \mapsto 9\}$. However, the CPO Fixed-Point Theorem will only need to consider totally ordered subsets, i.e., chains, and all the elements in a chain are consistent.

Definition 5. A **chain** is a totally ordered subset of a poset. A **chain-complete partial order (cpo)** has a least upper bound for every chain.

Proposition 2. The poset of partial functions $(A \rightarrow B, \subseteq)$ is a cpo.

Proof. Let S be a chain in $(A \rightarrow B, \subseteq)$. We claim that the lub of S is just the union of all the elements of S , that is $\sqcup S$. Recall that $\forall xy, (x, y) \in \sqcup S$ iff $\exists f \in S, (x, y) \in f$. We first need to show that $\sqcup S$ is an upper bound of S . Suppose $f \in S$. We need to show that $f \subseteq \sqcup S$. Consider $(x, y) \in f$. Then $(x, y) \in \sqcup S$. So indeed, $\sqcup S$ is an upper bound of S . Second, consider another upper bound g of S . We need to show that $\sqcup S \subseteq g$. Suppose $(x, y) \in \sqcup S$. Then $(x, y) \in h$ for some $h \in S$. Because g is an upper bound of S , we have $h \subseteq g$ and therefore $(x, y) \in g$. So we conclude that $\sqcup S \subseteq g$. \square

$$\perp \sqsubseteq F(\perp) \sqsubseteq F^2(\perp) \sqsubseteq F^3(\perp) \sqsubseteq \dots$$

Figure 6: Ascending chain of F .

$$\sqcup \left\{ \begin{array}{l} \{2 \mapsto 4, 3 \mapsto 9\}, \\ \{3 \mapsto 9, 4 \mapsto 16\} \end{array} \right\} = \left\{ \begin{array}{l} 2 \mapsto 4, \\ 3 \mapsto 9, \\ 4 \mapsto 16 \end{array} \right\}$$

Figure 7: The lub of partial functions.

The last ingredient required in the proof of the fixed point theorem is that the output of F should only depend on a finite amount of information from the input, that is, it should be continuous. For example, if the input to F is itself a function g , F should only need to apply g to a finite number of different values. This requirement is at the core of what it means for a function to be computable [?]. So applying F to the lub of a directed set X (an infinite thing) should be the same as taking the lub of the set obtained by mapping F over the elements of X (finite things).

Definition 6. A monotonic function $F : A \rightarrow B$ on a cpo is **continuous** iff for all chains X of A

$$F(\bigsqcup X) = \bigsqcup \{F(x) \mid x \in X\}$$

Proposition 3. The functional $F_{b,c}$ for *while* loops (2) is continuous.

Proof. Let S be a chain in $(A \rightarrow B, \subseteq)$. We need to show that

$$F_{b,c}(\bigcup S) = \bigcup \{F_{b,c}(f) \mid f \in S\}$$

We shall prove this equality by showing that each graph is a subset of the other. We assume $(s, s'') \in F_{b,c}(\bigcup S)$. Suppose $Bbs = \text{true}$. Then $(s, s'') \in (\bigcup S) \circ (Cc)$, so $(s, s') \in Cc$ and $(s', s'') \in g$ for some s' and $g \in S$. So $(s, s'') \in g \circ (Cc)$. Therefore $(s, s'') \in \bigcup \{F_{b,c}(f) \mid f \in S\}$. So we have shown that $F_{b,c}(\bigcup S) \subseteq \bigcup \{F_{b,c}(f) \mid f \in S\}$. Next suppose $Bbs = \text{false}$. Then $F_{b,c}(\bigcup S) = id = \bigcup \{F_{b,c}(f) \mid f \in S\}$.

For the other direction, we assume $(s, s'') \in \bigcup \{F_{b,c}(f) \mid f \in S\}$. So $(s, s'') \in F_{b,c}(g)$ for some $g \in S$. Suppose $Bbs = \text{true}$. Then $(s, s') \in Cc$ and $(s', s'') \in g$ for some s' . So $(s', s'') \in \bigcup S$ and therefore $(s, s'') \in F_{b,c}(\bigcup S)$. So we have shown that $\bigcup \{F_{b,c}(f) \mid f \in S\} \subseteq F_{b,c}(\bigcup S)$. Next suppose $Bbs = \text{false}$. Then again we have both graphs equal to the identity relation. \square

We now state the fixed point theorem for cpos.

Theorem 4 (CPO Fixed-Point Theorem). Suppose (L, \sqsubseteq) is a cpo and let $F : L \rightarrow L$ be a continuous function. Then F has a least fixed point, written $\text{fix } F$, which is the least upper bound of the ascending chain of F :

$$\text{fix } F = \bigsqcup \{F^n(\perp) \mid n \in \text{Nat}\}$$

Proof. Note that \perp is an element of L because it is the lub of the

empty chain. We first prove that $\text{fix } F$ is a fixed point of F .

$$\begin{aligned}
 F(\text{fix } F) &= F(\bigsqcup \{F^n(\perp) \mid n \in \text{Nat}\}) \\
 &= \bigsqcup \{F(F^n(\perp)) \mid n \in \text{Nat}\} && \text{by continuity} \\
 &= \bigsqcup \{F^{n+1}(\perp) \mid n \in \text{Nat}\} \\
 &= \bigsqcup \{F^n(\perp) \mid n \in \text{Nat}\} && \text{because } F^0(\perp) = \perp \sqsubseteq F^1(\perp) \\
 &= \text{fix } F
 \end{aligned}$$

Next we prove that $\text{fix } F$ is the least of the fixed points of F . Suppose e is an arbitrary fixed point of F . By the monotonicity of F we have $F^i(\perp) \sqsubseteq F^i(e)$ for all i . And because e is a fixed point, we also have $F^i(e) = e$, so e is an upper bound of the ascending chain, and therefore $\text{fix } F \sqsubseteq e$. \square

Returning to the semantics of the while loop, we give the least fixed-point semantics of an imperative language in Figure 8. We have already seen that the poset of partial functions is a cpo and that $F_{b,c}$ is continuous, so $\text{fix}(F_{b,c})$ is well defined and is the least fixed-point of $F_{b,c}$. Thus, we can define the meaning of the while loop as follows.

$$C(\text{while } b \text{ do } c) s = \text{fix}(F_{b,c}) s$$

Exercise 7 Prove that the semantics in Figure 3 is equivalent to the least fixed-point semantics in Figure 8, i.e., $(n, n') \in Pc$ iff $Pcn = n'$.

In the literature there are two schools of thought regarding how to define complete partial orders. There is the one presented above, that requires lubs to exist for all chains [???]. The other requires that the poset be directed complete, that is, lubs exist for all directed sets [???]. The two schools of thought are equivalent, i.e., a poset P with a least element is directed-complete iff every chain in P has a lub [?] (Theorem 8.11).

A Functional Language

Figure 9

$$\begin{aligned}
 P'cn &= (C'c \{A \mapsto n\}) Z \\
 C' \text{skip} s &= s \\
 C'(x := e) s &= [x \mapsto Ees]s \\
 C'(c_1 ; c_2) s &= C'c_2(C'c_1 s) \\
 C' \left(\begin{array}{l} \text{if } b \text{ then } c_1 \\ \text{else } c_2 \end{array} \right) s &= \begin{cases} C'c_1 s & \text{if } Bbs = \text{true} \\ C'c_2 s & \text{if } Bbs = \text{false} \end{cases} \\
 C'(\text{while } b \text{ do } c) s &= \text{fix}(F_{b,c}) s
 \end{aligned}$$

Figure 8: Least Fixed-Point Semantics of an Imperative Language

Syntax

$$\begin{array}{ll}
 \text{variables} & x \in \mathbb{X} \\
 \text{expression} & e ::= \dots \mid x \mid \lambda x. e \mid e e
 \end{array}$$

Domain

$$\text{elements } d ::= n \mid \{(d_1, d'_1), \dots, (d_n, d'_n)\}$$

Ordering

$$n \sqsubseteq n \quad \frac{t \subseteq t'}{t \sqsubseteq t'}$$

Semantics

$$\begin{aligned}
 Exs &= \{sx\} \\
 E(\lambda x. e) s &= \{t \mid \forall (d, d') \in t, d' \in Ee[x \mapsto d]s\} \\
 E(e_1 e_2) s &= (Ee_1 s) \cdot (Ee_2 s) \\
 D_1 \cdot D_2 &\stackrel{\text{def}}{=} \left\{ d' \mid \begin{array}{l} \exists t d d'. t \in D_1, d_2 \in D_2, \\ (d, d') \in t, d \sqsubseteq d_2 \end{array} \right\}
 \end{aligned}$$

Figure 9: A Functional Language

*Answers to Exercises***Answer of Exercise 1**

d_1, d_2, d_3	$add3(d_1, d_2, d_3)$	$d_1 + d_2 + d_3$
0,0,0	00	0
0,0,1	01	1
0,1,0	01	1
0,1,1	10	2
1,0,0	01	1
1,0,1	10	2
1,1,0	10	2
1,1,1	11	3

Answer of Exercise 2

The proof is by induction on add .

- Case $N(add(\epsilon, \epsilon, 0)) = N(\epsilon) = 0 = N(\epsilon) + N(\epsilon) + 0$
- Case $N(add(\epsilon, \epsilon, 1)) = N(\epsilon 1) = 1 = N(\epsilon) + N(\epsilon) + 1$
- Case $add(n'_1 d_1, n'_2 d_2, c) = add(n_1, n_2, c') d_3$
where $add3(d_1, d_2, c) = c' d_3$.

$$\begin{aligned}
N(add(n'_1 d_1, n'_2 d_2, c)) &= N(add(n'_1, n'_2, c') d_3) \\
&= N(add(n'_1, n'_2, c')) \times 2 + d_3 \\
&= (N(n'_1) + N(n'_2) + c') \times 2 + d_3 \\
&= 2N(n'_1) + 2N(n'_2) + c' \times 2 + d_3 \\
&= 2N(n'_1) + 2N(n'_2) + N(c' d_3) \\
&= 2N(n'_1) + d_1 + 2N(n'_2) + d_2 + c \quad \text{by Ex. 1} \\
&= N(n'_1 d_1) + N(n'_2 d_2) + c
\end{aligned}$$

- Case $add(n_1 d_1, \epsilon, c) = add(n_1 d_1, \epsilon 0, c)$

$$\begin{aligned}
N(add(n_1 d_1, \epsilon, c)) &= N(add(n_1 d_1, \epsilon 0, c)) \\
&= N(n_1 d_1) + N(\epsilon 0) + c \quad \text{by I.H.} \\
&= N(n_1 d_1) + N(\epsilon) + c
\end{aligned}$$

- Case $add(\epsilon, n_2 d_2, c) = add(\epsilon 0, n_2 d_2, c)$

$$\begin{aligned}
N(add(\epsilon, n_2 d_2, c)) &= N(add(\epsilon 0, n_2 d_2, c)) \\
&= N(\epsilon 0) + N(n_2 d_2) + c \\
&= N(\epsilon) + N(n_2 d_2) + c
\end{aligned}$$

Answer of Exercise 3

By induction on $mult$.

- Case $mult(n_1, \epsilon) = \epsilon$:

$$N(mult(n_1, \epsilon)) = N(\epsilon) = 0 = N(n_1)N(\epsilon)$$

- Case $mult(n_1, n'_2 0) = mult(n_1, n'_2)0$:

$$\begin{aligned} N(mult(n_1, n'_2 0)) &= N(mult(n_1, n'_2)0) \\ &= 2N(mult(n_1, n'_2)) \\ &= 2N(n_1)N(n'_2) && \text{by I.H.} \\ &= N(n_1)N(n'_2 0) \end{aligned}$$

- Case $mult(n_1, n'_2 1) = add(n_1, mult(n_1, n'_2)0)$:

$$\begin{aligned} N(mult(n_1, n'_2 1)) &= N(add(n_1, mult(n_1, n'_2)0, 0)) \\ &= N(n_1) + N(mult(n_1, n'_2)0) + 0 && \text{by Ex. 2} \\ &= N(n_1) + 2N(mult(n_1, n'_2)) \\ &= N(n_1) + 2N(n_1)N(n'_2) && \text{by I.H.} \\ &= N(n_1)(2N(n'_2) + 1) \\ &= N(n_1)N(n'_2 1) \end{aligned}$$

Answer of Exercise 4

The proof is by induction on e .

- Case $e = n$: $N(I(n)) = N(n) = E(n)$.
- Case $e = e_1 + e_2$:

$$\begin{aligned} N(I(e_1 + e_2)) &= N(add(I(e_1), I(e_2), 0)) \\ &= N(I(e_1)) + N(I(e_2)) && \text{by Ex. 2} \\ &= E(e_1) + E(e_2) && \text{by the I.H.} \\ &= E(e_1 + e_2) \end{aligned}$$

- Case $e = e_1 \times e_2$:

$$\begin{aligned} N(I(e_1 \times e_2)) &= N(mult(I(e_1), I(e_2))) \\ &= N(I(e_1)) \times N(I(e_2)) && \text{by Ex. 3} \\ &= E(e_1) \times E(e_2) && \text{by the I.H.} \\ &= E(e_1 \times e_2) \end{aligned}$$

Answer of Exercise 5

The proof is by cases on $k, s \longrightarrow k', s'$.

- Case $\boxed{\text{skip} ; k, s \longrightarrow k, s}$

$$C(\text{skip} ; k)(s) = (C(k) \circ C(\text{skip}))(s) = (C(k) \circ id)(s) = C(k)(s)$$

- Case $\boxed{x := e ; k, s \longrightarrow k, [x \mapsto E(e)(s)]s}$

$$\begin{aligned} C((x := e) ; k)(s) &= (C(k) \circ C(x := e))(s) \\ &= C(k)(C(x := e)(s)) \\ &= C(k)([x \mapsto E(e)(s)]s) \end{aligned}$$

- Case $\boxed{(c_1 ; c_2) ; k, s \longrightarrow c_1 ; (c_2 ; k), s}$

$$\begin{aligned} C((c_1 ; c_2) ; k)(s) &= (C(k) \circ (C(c_2) \circ C(c_1)))(s) \\ &= ((C(k) \circ C(c_2)) \circ C(c_1))(s) \\ &= C(c_1 ; (c_2 ; k))(s) \end{aligned}$$

- Case $\boxed{(\text{if } b \text{ then } c_1 \text{ else } c_2) ; k, s \longrightarrow c_1 ; k, s \text{ and } Bbs = \text{true}}$

$$\begin{aligned} C((\text{if } b \text{ then } c_1 \text{ else } c_2) ; k)(s) &= (C(k) \circ C(\text{if } b \text{ then } c_1 \text{ else } c_2))(s) \\ &= (C(k) \circ C(c_1))(s) \\ &= C(c_1 ; k)(s) \end{aligned}$$

- Case $\boxed{(\text{if } b \text{ then } c_1 \text{ else } c_2) ; k, s \longrightarrow c_2 ; k, s \text{ and } Bbs = \text{false}}$

$$\begin{aligned} C((\text{if } b \text{ then } c_1 \text{ else } c_2) ; k)(s) &= (C(k) \circ C(\text{if } b \text{ then } c_1 \text{ else } c_2))(s) \\ &= (C(k) \circ C(c_2))(s) \\ &= C(c_2 ; k)(s) \end{aligned}$$

- Case $\boxed{(\text{while } b \text{ do } c) ; k, s \longrightarrow c ; ((\text{while } b \text{ do } c) ; k), s \text{ and } Bbs = \text{true}}$

$$\begin{aligned} C((\text{while } b \text{ do } c) ; k)(s) &= (C(k) \circ C(\text{while } b \text{ do } c))(s) \\ &= (C(k) \circ (C(\text{while } b \text{ do } c) \circ C(c)))(s) \\ &= ((C(k) \circ C(\text{while } b \text{ do } c)) \circ C(c))(s) \\ &= C(c ; ((\text{while } b \text{ do } c) ; k))(s) \end{aligned}$$

- Case $\boxed{(\text{while } b \text{ do } c) ; k, s \longrightarrow k, s \text{ and } Bbs = \text{false}}$

$$\begin{aligned} C((\text{while } b \text{ do } c) ; k)(s) &= (C(k) \circ C(\text{while } b \text{ do } c))(s) \\ &= (C(k) \circ id)(s) \\ &= C(k)(s) \end{aligned}$$

Answer of Exercise 6

TODO

Answer of Exercise 7

TODO

References

- Roberto M. Amadio and Curien Pierre-Louis. *Domains and Lambda-Calculi*. Cambridge University Press, 1998.
- B.A. Davey and H.A. Priestley. *Introduction to Lattices and Order*. Cambridge University Press, 2nd edition, 2002.
- Carl A. Gunter, Peter D. Mosses, and Dana S. Scott. Semantic domains. In *Handbook of Theoretical Computer Science, Volume B: Formal Models and Semantics (B)*, pages 633–674. 1990.
- C. A. R. Hoare. An axiomatic basis for computer programming. *Commun. ACM*, 12(10):576–580, 1969. ISSN 0001-0782.
- John C. Mitchell. *Foundations of programming languages*. MIT Press, Cambridge, MA, USA, 1996. ISBN 0-262-13321-0.
- Gordon D. Plotkin. Domains. course notes, 1983.
- David A. Schmidt. *Denotational semantics: a methodology for language development*. William C. Brown Publishers, Dubuque, IA, USA, 1986. ISBN 0-697-06849-2.
- Glynn Winskel. *The Formal Semantics of Programming Languages*. Foundations of Computing. MIT Press, 1993.