

# 50003 - Models of Computation - Lecture 7

Oliver Killane

02/11/21

## Lecture Recording

Lecture recording is available here

## Note for reader

We will reference to state by set  $State \triangleq (Var \rightarrow \mathbb{N})$ .

## Lemmas

### Lemma

A small proven proposition that can be used in a proof. Used to make the proof smaller.

Also know as an "auxiliary theorem" or "helper theorem".

### Corollary

A theorem connected by a short proof to another existing theorem.

If B is can be easily deduced from A (or is evident in A's proof) then B is a corollary of A.

## Lemmas

1.  $\forall r \in \mathbb{N}. \forall E_1, E'_1, E_2 \in SimpleExp. [E_1 \rightarrow^r E'_1 \Rightarrow (E_1 + E_2) \rightarrow^r (E'_1 + E_2)]$
2.  $\forall r, n \in \mathbb{N}. \forall E_2, E'_2 \in SimpleExp. [E_2 \rightarrow^r E'_2 \Rightarrow (n + E_2) \rightarrow^r (n + E'_2)]$

## Corollaries

1.  $\forall n_1 \in \mathbb{N}. \forall E_1, E_2 \in SimpleExp. [E_1 \rightarrow^* n_1 \Rightarrow (E_1 + E_2) \rightarrow^* (n_1 + E_2)]$
2.  $\forall n_1, n_2 \in \mathbb{N}. \forall E_2 \in SimpleExp. [E_2 \rightarrow^* n_2 \Rightarrow (n_1 + E_2) \rightarrow^* (n_1 + n_2)]$
3.  $\forall n, n_1, n_2, \in \mathbb{N}. \forall E_1, E_2 \in SimpleExp. [E_1 \rightarrow^* n_1 \wedge E_2 \rightarrow^* n_2 \wedge n = n_1 + n_2 \Rightarrow (E_1 + E_2) \rightarrow^* n]$

## Connecting $\Downarrow$ and $\rightarrow^*$ for SimpleExp

$$\forall E \in SimpleExp, n \in \mathbb{N}. [E \Downarrow n \Leftrightarrow E \rightarrow^* n]$$

We prove each direction of implication separately. Fir we prove by induction over  $E$  using the property  $P$ :

$$P(E) =_{def} \forall n \in \mathbb{N}. [E \Downarrow n \Rightarrow E \rightarrow^* n]$$

### Base Case

Take arbitrary  $n \in \mathbb{N}$  to show  $P(n) - n \Downarrow n \Rightarrow n \rightarrow^* n$ .

- (1)  $n \rightarrow^0 n$  ( $n$  is in the normal form)
- (2)  $n \Downarrow n$  ( $n$  is in the normal form)
- (3)  $n \Downarrow n \wedge n \rightarrow^* n$  (By 1 & 2)
- (4)  $n \Downarrow n \Rightarrow n \rightarrow^* n$  (By 3)

### Inductive Step

Take some arbitrary  $E, E_1, E_2$  such that  $E = E_1 + E_2$ .

Inductive Hypothesis

$$\forall n_1 \in \mathbb{N}. [E_1 \Downarrow n_1 \Rightarrow E_1 \rightarrow^* n_1]$$

$$\forall n_2 \in \mathbb{N}. [E_2 \Downarrow n_2 \Rightarrow E_2 \rightarrow^* n_2]$$

To show  $P(E)$ :  $\forall n \in \mathbb{N}. [(E_1 + E_2) \Downarrow n \Rightarrow (E_1 + E_2) \rightarrow^* n]$ .

- (1) Assume  $(E_1 + E_2) \Downarrow n$
- (2)  $\exists n_1, n_2 \in \mathbb{N}. [E_1 \Downarrow n_1 \wedge E_2 \Downarrow n_2]$  (By 1 & definition of B-ADD)
- (3)  $E_1 \rightarrow^* n_1$  (By 2 & IH)
- (4)  $E_2 \rightarrow^* n_2$  (By 2 & IH)
- (5) Chose some  $n \in \mathbb{N}$  such that  $n = n_1 + n_2$
- (6)  $(E_1 + E_2) \rightarrow^* n$  (By 3,4,5 Corollary 3)
- (7)  $E \rightarrow^* n$  (By 6, definition of  $E$ )

Hence assuming  $E \Downarrow n$  implies  $E \rightarrow^* n$ , so  $P(E)$ .

Next we work the other way, to show:

$$\forall E \in \text{SimpleExp}. \forall n \in \mathbb{N}. [E \rightarrow^* n \Rightarrow E \Downarrow n]$$

- (1) Take arbitrary  $E \in \text{SimpleExp}$  such that  $E \rightarrow^* n$  (Initial setup)
- (2) Take some  $m \in \mathbb{N}$  such that  $E \Downarrow m$  (By totality of  $\Downarrow$ )
- (3)  $n = m$  (By 1,2 & uniqueness of result for  $\rightarrow$ )
- (4)  $E \Downarrow n$  (By 3)

It is also possible to prove this without using normalisation and determinacy, by induction on  $E$ .

### Multi-Step Reductions

**Lemma:**

$$\forall r \in \mathbb{N}. \forall E_1, E'_1, E_2. [E_1 \rightarrow^r E'_1 \Rightarrow (E_1 + E_2) \rightarrow^r (E'_1 + E_2)]$$

To prove  $\forall r \in \mathbb{N}. [P(r)]$  by induction on  $r$ :

#### Base Case

- Base case is  $r = 0$ .
- Prove that  $P(0)$  holds.

### Inductive Step

- Inductive Case is  $r = k + 1$  for arbitrary  $k \in \mathbb{N}$ .
- Inductive hypothesis is  $P(k)$ .
- Prove  $P(k + 1)$  using inductive hypothesis.

### Proof of the Lemma

By induction on  $r$ : **Base Case:** Take some arbitrary  $E_1, E'_1, E_2 \in \text{SimpleExp}$  such that  $E_1 \rightarrow^0 E'_1$ .

- (1)  $E_1 = E'_1$  (By definition of  $\rightarrow^0$ )
- (2)  $(E_1 + E_2) = (E'_1 + E_2)$  (By 1)
- (3)  $(E_1 + E_2) \rightarrow^0 (E'_1 + E_2)$  (By definition of  $\rightarrow^0$ )

**Inductive Step:** Take arbitrary  $k \in \mathbb{N}$  such that  $P(k)$

- (1) Take arbitrary  $E_1, E'_1, E_2$  such that  $E_1 \rightarrow E'_1$  (Initial setup)
- (2) Take arbitrary  $E''_1$  such that  $E'_1 \rightarrow E''_1$
- (3)  $(E_1 + E_2) \rightarrow^k (E''_1 + E_2)$  (By 2 & IH)
- (4)  $(E''_1 + E_2) \rightarrow (E'_1 + E_2)$  (By 2 & rule S-LEFT)
- (5)  $(E_1 + E_2) \rightarrow^{k+1} (E'_1 + E_2)$  (3,4, definition of  $\rightarrow^{k+1}$ )

### Determinacy of $\rightarrow$ for Exp

We extend simple expressions configurations of the form  $\langle E, s \rangle$ .

$$E \in \text{Exp} ::= n|x|E + E| \dots$$

Determinacy:

$$\forall E, E_1, E_2 \in \text{Exp}. \forall s, s_1, s_2 \in \text{State}. [\langle E, s \rangle \rightarrow \langle E_1, s_1 \rangle \wedge \langle E, s \rangle \rightarrow \langle E_2, s_2 \rangle \Rightarrow \langle E_1, s_1 \rangle = \langle E_2, s_2 \rangle]$$

We prove this using property  $P$ :

$$P(E, s) \triangleq \forall E_1, E_2 \in \text{Exp}. \forall s_1, s_2 \in \text{State}. [\langle E, s \rangle \rightarrow \langle E_1, s_1 \rangle \wedge \langle E, s \rangle \rightarrow \langle E_2, s_2 \rangle \Rightarrow \langle E_1, s_1 \rangle = \langle E_2, s_2 \rangle]$$

**Base Case:**  $E = x$

Take arbitrary  $n \in \mathbb{N}$  and  $s \in \text{State}$  to show  $P(n, s)$

- (1) take  $E_1 \in \text{Exp}, s_1 \in \text{State}$  such that  $\langle n, s \rangle \rightarrow \langle E_1, s_1 \rangle$  (Initial setup)
- (2) take  $E_2 \in \text{Exp}, s_2 \in \text{State}$  such that  $\langle n, s \rangle \rightarrow \langle E_2, s_2 \rangle$  (Initial setup)
- (3)  $n = E_1 \wedge s = s_1$  (By 1 & inversion on definition of E.NUM)
- (4)  $n = E_2 \wedge s = s_2$  (By 2 & inversion on definition of E.NUM)
- (5)  $E_1 = E_2 \wedge s_1 = s_2$  (By 3 & 4)
- (6)  $\langle E_1, s_1 \rangle = \langle E_2, s_2 \rangle$  (By 5 & definition of configurations)

**Base Case:**  $E = x$

Take arbitrary  $x \in Var$  and  $s \in State$  to show  $P(n, s)$

- |     |   |   |
|-----|---|---|
| (1) | take $E_1 \in \mathbb{N}$ , $s_1 \in State$ such that $\langle x, s \rangle \rightarrow \langle E_1, s_1 \rangle$ | (Initial setup)                           |
| (2) | take $E_2 \in \mathbb{N}$ , $s_2 \in State$ such that $\langle x, s \rangle \rightarrow \langle E_2, s_2 \rangle$ | (Initial setup)                           |
| (3) | $E_1 = s(x) \wedge s_1 = s$   | (By 1 & inversion on definition of E.VAR) |
| (3) | $E_2 = s(x) \wedge s_2 = s$   | (By 2 & inversion on definition of E.VAR) |
| (5) | $E_1 = E_2 \wedge s_1 = s_2$  | (By 3 & 4)                                |
| (6) | $\langle E_1, s_1 \rangle = \langle E_2, s_2 \rangle$   | (By 5 & definition of configurations)     |

... Inductive Step ...

## Syntax of Commands

$$C \in Com ::= x := E | \text{if } B \text{ then } C \text{ else } C | C; C | \text{skip} | \text{while } B \text{ do } C$$

- **Determinacy**

$$\forall C, C_1, C_2 \in Com. \forall s, s_1, s_2 \in State. [\langle C, s \rangle \rightarrow_c \langle C_1, s_1 \rangle \wedge \langle C, s \rangle \rightarrow_c \langle C_2, s_2 \rangle \Rightarrow \langle C_1, s_1 \rangle = \langle C_2, s_2 \rangle]$$

- **Confluence**

$$\forall C, C_1, C_2 \in Com. \forall s, s_1, s_2 \in State. [\langle C, s \rangle \rightarrow_c^* \langle C_1, s_1 \rangle \wedge \langle C, s \rangle \rightarrow_c^* \langle C_2, s_2 \rangle \Rightarrow \exists C' \in Com. \exists s' \in State. [\langle C_1, s_1 \rangle \rightarrow C', s'] \wedge \langle C_2, s_2 \rangle \rightarrow C', s']]$$

- **Unique Answer**

$$\forall C \in Com. s_1 s_2 \in State. [\langle C, s \rangle \rightarrow_c^* \langle \text{skip}, s_1 \rangle \wedge \langle C, s \rangle \rightarrow_c^* \langle \text{skip}, s_2 \rangle \Rightarrow s_1 = s_2]$$

- **No Normalisation**

There exist derivations of infinite length for while.

## Connecting $\Downarrow$ and $\rightarrow^*$ for While

1.  $\forall E, n \in Exp. \forall s, s' \in State. [\langle E, s \rangle \Downarrow_e \langle n, s' \rangle \Leftrightarrow \langle E, s \rangle \rightarrow_e^* \langle n, s' \rangle]$
2.  $\forall B, b \in Bool. \forall s, s' \in State. [\langle B, s \rangle \Downarrow_b \langle b, s' \rangle \Leftrightarrow \langle B, s \rangle \rightarrow_b^* \langle b, s' \rangle]$
3.  $\forall C \in Com. \forall s, s' \in State. [\langle C, s \rangle \Downarrow_c \langle s' \rangle \Leftrightarrow \langle C, s \rangle \rightarrow_c^* \langle \text{skip}, s' \rangle]$

For *Exp* and *Bool* we have proofs by induction on the structure of expressions/booleans.

For  $\Downarrow_c$  it is more complex as the  $\Downarrow_c \Leftarrow \rightarrow_c^*$  cannot be proven using totality. Instead **complete/strong induction** on length of  $\rightarrow_c^*$  is used.