Languages for Concurrency and Distribution Exam

Exercises on Calculus of Communicating Systems and Hennessy-Milner Logic

Filippo Fantinato mat. 2041620

filippo.fantinato.2@studenti.unipd.it

July 10, 2023

Contents

1 Exercise B

Prove that each process in the finite fragment of CCS with finite sums terminates in a finite number of steps and prove also that the number of reachable states is finite. Discuss the case of infinite sums.

More formally, given the finite fragment of CCS defined by the following syntax and operational rules:

Definition 1.1 (CCS syntax with finite non deterministic choice)**.**

$$P, Q ::= \alpha.P \mid \sum_{\substack{i \in I \\ |I|=n \in \mathbb{N}}} P_i \mid P|Q \mid P\backslash L \mid P[f]$$

Definition 1.2 (CCS semantic rules)**.**

$$\frac{}{\alpha.P \xrightarrow{\alpha} P} \quad \text{(act)}$$

$$\frac{P_j \xrightarrow{\alpha} P'_j \quad j \in I}{\sum_{\substack{i \in I \\ |I|=n \in \mathbb{N}}} P_i \xrightarrow{\alpha} P'_j} \quad \text{(sum)}$$

$$\frac{P \xrightarrow{\alpha} P'}{P|Q \xrightarrow{\alpha} P'|Q} \quad \text{(par-1)}$$

$$\frac{Q \xrightarrow{\alpha} Q'}{P|Q \xrightarrow{\alpha} P|Q'} \quad \text{(par-2)}$$

$$\frac{P \xrightarrow{\alpha} P' \quad Q \xrightarrow{\bar{\alpha}} Q'}{P|Q \xrightarrow{\tau} P'|Q'} \quad \text{(par)}$$

$$\frac{P \xrightarrow{\alpha} P'}{P\backslash L \xrightarrow{\alpha} P'\backslash L} \quad \text{(res)}$$

$$\frac{P \xrightarrow{\alpha} P'}{P[f] \xrightarrow{f(\alpha)} P'[f]} \quad \text{(red)}$$

I need to prove:

- given a process P, if $P \xrightarrow{\alpha} P'$ then $\|P\| > \|P'\|$;
- given a process P, $|states(P)| \leqslant \#P$ where states is the set of states that P can reach and $\#P$ the upper bound to that set.

1.1 CCS processes always terminate with finite non deterministic choice

Definition 1.3 (Process depth)**.** *Given a process P, the depth $\|\cdot\| : \mathcal{L}_{CCS} \to \mathbb{N}$ of the process P is defined recursively in the following way:*

$$
\begin{aligned}
&\|P\| \triangleq \\
&\qquad \|\alpha.P\| \triangleq 1 + \|P\| \\
&\qquad \left\| \sum_{i \in I, |I| = n \in \mathbb{N}} P_i \right\| \triangleq \max_{i \in I, |I| = n \in \mathbb{N}} \|P_i\| \\
&\qquad \|P|Q\| \triangleq \|P\| + \|Q\| \\
&\qquad \|P \backslash L\| \triangleq \|P\| \\
&\qquad \|P[f]\| \triangleq \|P\|
\end{aligned}
$$

Theorem 1.1. *Given a process P, $P \xrightarrow{\alpha} P' \implies \|P\| > \|P'\|$*

Proof. By induction on the height of the derivation tree $P \xrightarrow{\alpha} P'$:

- (base case, $h = 1$)
  - the process is an instance of the rule (act)

$$\frac{}{\alpha.P_1 \xrightarrow{\alpha} P_1}$$

    (1) by hypothesis, $P = \alpha.P_1$ and $P' = P_1'$

    (2) by definition 1.3, $\|P\| = 1 + \|P_1\|$ and $\|P'\| = \|P_1\|$

    (3) by (2) $1 + \|P_1\| > \|P_1\|$

    $\implies \|P\| > \|P'\|$

- (inductive cases, $h > 1$)

  Inductive hypothesis: Given a process P, if $P \xrightarrow{\alpha} P'$ and it's derivated with height $k < h$ then $\|P\| > \|P'\|$.

  - the process is an instance of the rule (sum)

$$\frac{Q_j \xrightarrow{\alpha} Q_j' \quad j \in I}{\sum_{|I| = n \in \mathbb{N}}^{i \in I} Q_i \xrightarrow{\alpha} Q_j'}$$

    (1) by hypothesis, $P = \sum_{|I| = n \in \mathbb{N}}^{i \in I} Q_i$ and $P' = Q_j'$

    (2) since $Q_j \xrightarrow{\alpha} Q_j'$ it's derivated with height $< h$, by inductive hypothesis $\|Q_j\| > \left\|Q_j'\right\|$

    (3) by definition 1.3, $\|P\| = \max_{|I| = n \in \mathbb{N}}^{i \in I} \|Q_i\|$ and $\|P'\| = \left\|Q_j'\right\|$

    (4) by (3) and (2), I can deduce

$$\max_{\substack{i \in I \\ |I| = n \in \mathbb{N}}} \|Q_i\| > \left\|Q_j'\right\|$$

    $\implies \|P\| > \|P'\|$

– the process is an instance of the rule (par-1)

$$\frac{P_1 \xrightarrow{\alpha} P_1'}{P_1|P_2 \xrightarrow{\alpha} P_1'|P_2}$$

(1) by hypothesis, $P = P_1|P_2$ and $P' = P_1'|P_2$

(2) since $P_1 \xrightarrow{\alpha} P_1'$ it's derivated with height $< h$, by inductive hypothesis $\|P_1\| > \|P_1'\|$

(3) by definition 1.3, $\|P\| = \|P_1\| + \|P_2\|$ and $\|P'\| = \|P_1'\| + \|P_2\|$

(4) by (2) and (3), $\|P\| = \|P_1\| + \|P_2\| > \|P_1'\| + \|P_2\| = \|P'\|$

$\implies \|P\| > \|P'\|$

– the process is an instance of the rule (par-2)

$$\frac{P_2 \xrightarrow{\alpha} P_2'}{P_1|P_2 \xrightarrow{\alpha} P_1|P_2'}$$

(1) by hypothesis $P = P_1|P_2$ and $P' = P_1|P_2'$

(2) since $P_2 \xrightarrow{\alpha} P_2'$ is derivated with height $< h$, by inductive hypothesis $\|P_2\| > \|P_2'\|$

(3) by definition 1.3, $\|P\| = \|P_1\| + \|P_2\|$ and $\|P'\| = \|P_1\| + \|P_2'\|$

(4) by (2) and (3), $\|P\| = \|P_1\| + \|P_2\| > \|P_1\| + \|P_2'\| = \|P'\|$

$\implies \|P\| > \|P'\|$

– the process is an instance of the rule (par)

$$\frac{P_1 \xrightarrow{\alpha} P_1' \quad P_2 \xrightarrow{\bar{\alpha}} P_2'}{P_1|P_2 \xrightarrow{\tau} P_1'|P_2'}$$

(1) by hypothesis $P = P_1|P_2$ and $P' = P_1'|P_2'$

(2) since $P_1 \xrightarrow{\alpha} P_1'$ and $P_2 \xrightarrow{\alpha} P_2'$ are derivated with height $< h$, by inductive hypothesis $\|P_1\| > \|P_1'\|$ and $\|P_2\| > \|P_2'\|$

(3) by definition 1.3, $\|P\| = \|P_1\| + \|P_2\|$ and $\|P'\| = \|P_1'\| + \|P_2'\|$

(4) by (2) and (3) $\|P\| = \|P_1\| + \|P_2\| > \|P_1'\| + \|P_2'\| = \|P'\|$

$\implies \|P\| > \|P'\|$

– the process is an instance of the rule (res)

$$\frac{P_1 \xrightarrow{\alpha} P_1'}{P_1\backslash L \xrightarrow{\alpha} P_1'\backslash L}$$

(1) by hypothesis $P = P_1\backslash L$ and $P' = P_1'\backslash L$

(2) since $P_1 \xrightarrow{\alpha} P_1'$ it's derivated with height $< h$, by inductive hypothesis $\|P_1\| > \|P_1'\|$

(3) by definition 1.3, $\|P\| = \|P_1\|$ and $\|P'\| = \|P_1'\|$

(4) by (2) and (3), $\|P\| = \|P_1\| > \|P_1'\| = \|P'\|$

$\implies \|P\| > \|P'\|$

– the process is an instance of the rule (red)

$$\frac{P_1 \xrightarrow{\alpha} P_1'}{P_1[f] \xrightarrow{f(\alpha)} P_1'[f]}$$

(1) by hypothesis $P = P_1[f]$ and $P' = P_1'[f]$

(2) since $P_1 \xrightarrow{\alpha} P_1'$ it's derivated with height $< h$, by inductive hypothesis $\|P_1\| > \|P_1'\|$

(3) by definition 1.3, $\|P\| = \|P_1\|$ and $\|P'\| = \|P_1'\|$

(4) by (2) and (3), $\|P\| = \|P_1\| > \|P_1'\| = \|P'\|$

$\implies \|P\| > \|P'\|$

□

1.2 CCS processes have finite states with finite non deterministic choice

Definition 1.4 (Process derivation length)**.** *Given a process P, the length of P can be recursively defined as follows:*

$$l(P) = \begin{cases} 0 & \text{if } P \nrightarrow \\ 1 + l(P') & \text{if } P \xrightarrow{\alpha} P' \end{cases}$$

Definition 1.5 (States of a process)**.** *Given a process P and annotating the set of all the states that P can reach via the function $S^n(P)\colon \mathcal{L}_{CCS} \to 2^{\mathcal{P}}$, then*

$$S^n(P) = \bigcup_{\substack{0 \leqslant k \leqslant n \\ k \in \mathbb{N}}} \{P' \mid P \xrightarrow{k} P'\}$$

just for the sake of clarity, by $S(P)$ I mean $S^{l(P)}(P)$.

Definition 1.6 (States upper bound)**.** *Given a process P, the upper bound $\#(\cdot)\colon \mathcal{L}_{CCS} \to \mathbb{N}$ to $|S(\cdot)|$ is defined recursively as*

$$\begin{aligned} \#(P) \triangleq & \\ & \#(\alpha.P) \triangleq 1 + \#(P_1) \\ & \#(\sum_{i \in I, |I| = n \in \mathbb{N}} P_i) \triangleq 1 + \sum_{i \in I, |I| = n \in \mathbb{N}} \#(P_i) \\ & \#(P|Q) \triangleq \#(P) \cdot \#(Q) \\ & \#(P \backslash L) \triangleq \#(P) \\ & \#(P[f]) \triangleq \#(P) \end{aligned}$$

Theorem 1.2. *Given a process P, $|S(P)| \leqslant \#(P)$*

Proof. By induction on the structure of P

- (inductive cases)

  Inductive hypothesis: Given a process Q sub-process of P, then $|S(Q)| \leqslant \#(Q)$.

  - $P = \alpha.P_1$

    (1) since P_1 is a sub-process of P, by inductive hypothesis $|S(P_1)| \leqslant \#(P_1)$

    (2) by (1) and the definition 1.5, we have that

    $$|S(P)| = |\{\alpha.P_1\} \cup S(P_1)| = 1 + |S(P_1)| \leqslant 1 + \#(P_1) = \#(P)$$

    $\implies |S(P)| \leqslant \#(P)$

  - $P = P_1|P_2$

    (1) since P_1 and P_2 are sub-process of P, by inductive hypothesis $|S(P_1)| \leqslant \#(P_1)$ and $|S(P_2)| \leqslant \#(P_2)$

    (2) by lemma 1.1 and (1), we have that

    $$\begin{aligned} |S(P_1|P_2)| &= |\{P_1'|P_2' \mid P_1' \in S(P_1), P_2' \in S(P_2)\}| \\ &= |S(P_1)| \cdot |S(P_2)| \\ &\leqslant \#(P_1) \cdot \#(P_2) \\ &= \#(P) \end{aligned}$$

    $\implies |S(P)| \leqslant \#(P)$

  - $P = \sum_{\substack{i \in I \\ |I| = n \in \mathbb{N}}} P_i$

    (1) since P_i is a sub-process of P, by inductive hypothesis $|S(P_i)| \leqslant \#(P_i), \forall i \in I$

    (2) by lemma 1.2 and (1), we have that

    $$\begin{aligned} |S(\sum_{\substack{i \in I \\ |I| = n \in \mathbb{N}}} P_i)| &\leqslant |\{\sum_{\substack{i \in I \\ |I| = n \in \mathbb{N}}} P_i\} \cup \bigcup_{\substack{i \in I \\ |I| = n \in \mathbb{N}}} S(P_i)| \\ &= 1 + \sum_{\substack{i \in I \\ |I| = n \in \mathbb{N}}} |S(P_i)| \\ &\leqslant 1 + \sum_{\substack{i \in I \\ |I| = n \in \mathbb{N}}} \#(P_i) \\ &= \#(P) \end{aligned}$$

    $\implies |S(P)| \leqslant \#(P)$

  - $P = P_1 \backslash L$

(1) since P_1 is a sub-process of P, by inductive hypothesis $|S^{|}(P_1) \leqslant \#(P_1)$

(2) by (1) and the definition 1.5, we have that

$$|S(P_1 \backslash L)| = |S(P_1)| \leqslant \#(P_1) = \#(P)$$

$\implies |S(P)| \leqslant \#(P)$

– $P = P_1[f]$

(1) since P_1 is a sub-process of P, by inductive hypothesis $|S^{|}(P_1) \leqslant \#(P_1)$

(2) by (1) and the definition 1.5, we have that

$$|S(P_1[f])| = |S(P_1)| \leqslant \#(P_1) = \#(P)$$

$\implies |S(P)| \leqslant \#(P)$

□

Lemma 1.1. *Given a process* $P = Q|T$, *then* $S(P) = \mathcal{P}_{par} = \{Q'|T' \mid Q' \in S(Q), T' \in S(T)\}$, *i.e.* $\forall Z \in \mathcal{P}.Z \in S(Q|T) \implies Z \in \mathcal{P}_{par}$

Proof. By induction on the length l of the derivation

- (base case, $l = 0$)
  if $l = 0$, then $Z = P_1|P_2$, which belongs to $\mathcal{P}_{par}$ by definition.

- (inductive case, $l \implies l + 1$)
  Inductive hypothesis: Given a state $Z_l \in S(Q|T)$ derivated with length $k = l$, then $Z_l \in \mathcal{P}_{par}$.

  We have that $Z = Q|T \xrightarrow{l} (Z_l = Q^l|T^l \in \mathcal{P}_{par})$ and we need to prove that if $Z_l \xrightarrow{\alpha} Z_{l+1}$ then $Z_{l+1} \in \mathcal{P}_{par}$.

  We can distinguish three cases:

  – if Q^l and T^l cannot perform any further step, then Z_l cannot perform it either and so the statement I want to prove is vacuously true.

  – if Q^l cannot perform a further step and $T^l \xrightarrow{\alpha} T^{l+1}$, then by applying the rule (par-2) $Z^{l+1} = Q^l|T^{l+1}$. Since by inductive hypothesis $Q^l|T^l \in \mathcal{P}_{par}$, where $T^l \in S(T)$ and $Q^l \in S(Q)$, I can claim $T^{l+1} \in S(T)$, from which I deduce $Z_{l+1} = Q^l|T^{l+1} \in \mathcal{P}_{par}$.

  – if $Q^l \xrightarrow{\alpha} Q^{l+1}$, then by applying the rule (par-1) $Z_{l+1} = Q^{l+1}|T^l$. Since by inductive hypothesis $Q^l|T^l \in \mathcal{P}_{par}$, where $T^l \in S(T)$ and $Q^l \in S(Q)$, I can claim $Q^{l+1} \in S(Q)$, from which I deduce $Z_{l+1} = Q^{l+1}|T^l \in \mathcal{P}_{par}$.

□

Lemma 1.2. *Given a process* $P = \sum_{|I|=n\in\mathbb{N}}^{i\in I} Q_i$, *then* $S(P) \subseteq \mathcal{P}_{sum} = \{P\} \cup \bigcup_{|I|=n\in\mathbb{N}}^{i\in I} S(Q_i)$, *i.e.* $\forall Z \in \mathcal{P}.Z \in S(\sum_{|I|=n\in\mathbb{N}}^{i\in I} Q_i) \implies Z \in \mathcal{P}_{sum}$

Proof. By induction on the length l of the derivation

- (base case, $l = 0$)
  if $l = 0$, then $Z = \sum_{|I|=n\in\mathbb{N}}^{i\in I} Q_i$, which belongs to $\mathcal{P}_{sum}$ by definition.
- (inductive case, $l \implies l + 1$)
  Inductive hypothesis: Given a state $Z_l \in S(\sum_{|I|=n\in\mathbb{N}}^{i\in I} Q_i)$ derivated with length $k = l$, then $Z_l \in \mathcal{P}_{sum}$.
  We have that $Z = \sum_{|I|=n\in\mathbb{N}}^{i\in I} Q_i \xrightarrow{l} (Z_l = Q_j^l \in \mathcal{P}_{sum})$ and we need to prove that if $Z_l \xrightarrow{\alpha} Z_{l+1}$ then $Z_{l+1} \in \mathcal{P}_{sum}$.
  We can distinguish two cases:
  - if Q_j^l cannot perform any further step, then Z_l cannot perform it either and so the statement I want to prove is vacuously true.
  - if $Q_j^l \xrightarrow{\alpha} Q_j^{l+1}$, then $Z_{l+1} = Q_j^{l+1}$. Since by inductive hypothesis $Z_l \in \mathcal{P}_{sum}$, where $Q_j^l \in S(Q_j)$, I can claim $Q_j^{l+1} \in S(Q_j)$ by the definition 1.5, from which I deduce $Z_{l+1} = Q_j^{l+1} \in \mathcal{P}_{sum}$.

□

1.3 CCS processes have finite states with finite non deterministic choice Variant

Corollary 1.1 (Process derivation length is finite)**.** *By Theorem 1.1, given a process* P *then* $l(P)$ *is a finite number.*

Theorem 1.3. *Given a process* P, $S^{l(P)}(P)$ *is finite.*

Proof. We can rewrite the definition of the set of all states 1.5 as:

$$S^0(P) = \{P\}$$
$$S^{n+1}(P) = \{P^{n+1} \mid P^n \xrightarrow{1} P^{n+1}\} \cup S^n(P)$$

By lemma 1.3, we know that the set of states obtained by performing at most 1 step from a generic process P is finite and by 1.1, $S^{l(P)}(P)$ is the union of $(l(P) + 1)$-th sets each of which is finite.
Therefore, I can claim $S^{l(P)}(P)$ is finite since is the union of finite sets.

□

Lemma 1.3. *Given a process* P, $S^1(P)$ *is finite.*

Proof. By induction on the structure of P.

- (inductive cases)

  Inductive hypothesis: Given a process Q sub-process of P, then $S^1(P)$ is finite.

  - $P = \alpha.P_1$

    The set of states that P can reach by performing at most 1 step is P itself and the one obtained applying the rule (act), that is

    $$S^1(\alpha.P_1) = \{\alpha.P_1, P_1\}$$

    $\implies S^1(P)$ is finite.

  - $P = \sum_{|I|=n\in\mathbb{N}}^{i\in I} P_i$

    The set of states that P can reach by performing at most 1 step is P itself and the one obtained applying the rule (sum), i.e.

    $$S^1(\sum_{\substack{i\in I\\ |I|=n\in\mathbb{N}}} P_i) = \{\sum_{\substack{i\in I\\ |I|=n\in\mathbb{N}}} P_i, P_1 \dots P_n\}$$

    $\implies S^1(P)$ is finite.

  - $P = P_1|P_2$

    The set of states that P can reach by performing at most 1 step is P itself and the one obtained applying the rules (par-1) or (par-2), i.e.

    $$S^1(P_1|P_2) = \{P_1|P_2, P_1'|P_2, P_1|P_2'\}$$

    $\implies S^1(P)$ is finite.

  - $P = P_1\backslash L$

    The set of states that P can reach by performing at most 1 step is P itself and the one obtained applying the rule (res), that is

    $$S^1(P_1\backslash L) = \{P_1\backslash L, P_1'\backslash L\}$$

    $\implies S^1(P)$ is finite.

  - $P = P_1[f]$

    The set of states that P can reach by performing at most 1 step is P itself and the one obtained applying the rule (red), that is

    $$S^1(P_1[f]) = \{P_1[f], P_1'[f]\}$$

    $\implies S^1(P)$ is finite.

□

1.4 CCS processes always terminate with infinity non deterministic choice

Now let's take in account the CCS language with non finite states, that is the variant defined here below:

Definition 1.7 (CCS syntax with infinity non deterministic choice)**.**

$$P, Q ::= \varnothing \mid \alpha.P \mid \sum_{\substack{i \in I \\ |I|=\infty}} P_i \mid P|Q \mid P\backslash L \mid P[f]$$

When we consider such language, we cannot apply induction since there is no bound on the height of the derivation tree. Therefore, we need to assume a finite number of application of production rules, in order to deal with only finite height tree.

Definition 1.8 (Height of a process tree)**.**

$$\begin{aligned} h(P) = & \\ & h(\varnothing) = 1 \\ & h(\alpha.P) = 1 + h(P) \\ & h(\sum_{\substack{i \in I \\ |I|=\infty}} P_i) = \sup_{i \in I}\{h(P_i)\} + 1 \\ & h(P|Q) = 1 + \max\{h(P), h(Q)\} \\ & h(P\backslash L) = 1 + h(P) \\ & h(P[f]) = 1 + h(P) \end{aligned}$$

Lemma 1.4. *Given a process P, $P \xrightarrow{\alpha} P' \implies h(P) > h(P')$*

Proof. By induction on the height of the derivation tree $P \xrightarrow{\alpha} P'$.

- (base case, $h = 1$)
  - the process is an instance of the rule (act)

$$\frac{}{\alpha.P_1 \xrightarrow{\alpha} P_1}$$

    (1) by hypothesis $P = \alpha.P_1$ and $P' = P_1'$

    (2) by definition 1.8, $h(P) = 1 + h(P_1)$ and $h(P') = h(P_1)$

    (3) by (2), $1 + h(P_1) > h(P_1)$

    $\implies h(P) > h(P')$

- (inductive case, $h > 1$) *Inductive hypothesis*: Given a process P, if $P \xrightarrow{\alpha} P'$ and it's derivated with height $k < h$ then $h(P) > h(P')$.

– the process is an instance of the rule (sum)

$$\frac{Q_j \xrightarrow{\alpha} Q'_j \quad j \in I}{\sum_{|I|=\infty}^{i \in I} Q_i \xrightarrow{\alpha} Q'_j}$$

(1) by hypothesis $P = \sum_{|I|=n \in \mathbb{N}}^{i \in I} Q_i$ and $P' = Q'_j$

(2) since $Q_j \xrightarrow{\alpha} Q'_j$ it's derivated with height $< h$, by inductive hypothesis $h(Q_j) > h(Q'_j)$

(3) by definition 1.8, $h(P) = \sup_{i \in I}\{h(Q_i)\} + 1$ and $h(P') = h(Q'_j)$

(4) by (2) and (3), $h(P) = \sup_{i \in I}\{h(Q_i)\} + 1 > \sup_{i \in I}\{h(Q_i)\} \geqslant h(Q'_j) = h(P')$

$\implies h(P) > h(P')$

– the process is an instance of the rule (par-1)

$$\frac{P_1 \xrightarrow{\alpha} P'_1}{P_1|P_2 \xrightarrow{\alpha} P'_1|P_2}$$

In order to make everything work, we need to assume $h(P_1) > h(P_2)$ since otherwise the derivation tree wouldn't decrease.

(1) by hypothesis $P = P_1|P_2$ and $P' = P'_1|P_2$

(2) since $P_1 \xrightarrow{\alpha} P'_1$ it's derivated with height $< h$, by inductive hypothesis $h(P_1) > h(P'_1)$

(3) by definition 1.8, $h(P) = 1 + \max\{h(P_1), h(P_2)\}$ and $h(P') = 1 + \max\{h(P'_1), h(P_2)\}$

(4) since we assumed $h(P_1) > h(P_2)$ we know that also this state $h(P'_1) \geqslant h(P_2)$, so

$$h(P) = 1 + h(P_1) > 1 + h(P'_1) = h(P')$$

$\implies h(P) > h(P')$

– the process is an instance of the rule (par-2)

$$\frac{P_2 \xrightarrow{\alpha} P'_2}{P_1|P_2 \xrightarrow{\alpha} P_1|P'_2}$$

In order to make everything work, we need to assume $h(P_2) > h(P_1)$ since otherwise the derivation tree wouldn't decrease.

(1) same as the above case

$\implies h(P) > h(P')$

– the process is an instance of the rule (par)

$$\frac{P_1 \xrightarrow{\alpha} P'_1 \quad P_2 \xrightarrow{\bar{\alpha}} P'_2}{P_1|P_2 \xrightarrow{\tau} P'_1|P'_2}$$

(1) by hypothesis $P = P_1|P_2$ and $P' = P'_1|P'_2$

(2) since $P_1 \xrightarrow{\alpha} P_1'$ it's derivated with height $< h$, by inductive hypothesis $h(P_1) > h(P_1')$ and $h(P_2) > h(P_2')$

(3) by definition 1.8, $h(P) = 1 + \max\{h(P_1), h(P_2)\}$ and $h(P') = 1 + \max\{h(P_1'), h(P_2')\}$

(4) by (2) and (3), $h(P) = 1 + \max\{h(P_1), h(P_2)\} > 1 + \max\{h(P_1'), h(P_2')\} = h(P')$

$\implies h(P) > h(P')$

– the process is an instance of the rule (red)

$$\frac{P_1 \xrightarrow{\alpha} P_1'}{P_1[f] \xrightarrow{f(\alpha)} P_1'[f]}$$

(1) by hypothesis $P = P_1[f]$ and $P' = P_1'[f]$

(2) since $P_1 \xrightarrow{\alpha} P_1'$ it's derivated with height $< h$, by inductive hypothesis $h(P_1) > h(P_1')$

(3) by definition 1.8, $h(P) = 1 + h(P_1)$ and $h(P') = 1 + h(P_1')$

(4) by (2) and (3), $h(P) = 1 + h(P_1) > 1 + h(P_1') = h(P')$

$\implies h(P) > h(P')$

– the process is an instance of the rule (res)

$$\frac{P_1 \xrightarrow{\alpha} P_1'}{P_1 \backslash L \xrightarrow{\alpha} P_1' \backslash L}$$

The proof is analogous to the (red) case

$\implies h(P) > h(P')$

□

1.5 CCS processes have no finite states with infinity non deterministic choice

With no limitation to the height of a derivation tree, it's quite easy to see that there exists some processes with no finite number of states. Regarding processes with a finite height derivation tree, it's less obvious the existence of processes with no finite number of states and below you can see an example. Let's consider the following process

$$P = \sum_{i \in \{1,2,\dots\}} \alpha_i.\alpha_i.\varnothing \tag{2}$$

we can notice that such process has an infinite number of states even if it has a finite height derivation tree. Therefore, I state that under the constraints I have imposed on the derivation tree height, there exists processes with no finite number of states.

2 Exercise I

Show that the semantics of Hennessy-Milner's logic discussed during the lectures is well defined, that is, when we consider least and greatest fixed points, the corresponding functions are monotone on a complete lattice. Discuss whether and how negation might be included in the logic.

More formally, given the the Hennessy-Milner's logic defined by the following syntax and semantic $f^{\eta}_{\cdot,X} := [\![\cdot]\!]_\eta \colon \mathcal{L}_{HML} \to 2^{\mathcal{P}}$:

Definition 2.1 (Hennessy-Milner's logic syntax)**.**

$$\phi, \psi ::= T \mid F \mid \phi \wedge \psi \mid \phi \vee \psi \mid < \alpha > \phi \mid [\alpha]\phi \mid X \mid \nu X.\phi \mid \mu X.\phi$$

Definition 2.2 (Hennessy-Milner's logic semantic)**.**

$$\begin{aligned}
&[\![\phi]\!]_\eta \triangleq \\
&\quad [\![T]\!]_\eta \triangleq \mathcal{P} \\
&\quad [\![F]\!]_\eta \triangleq \varnothing \\
&\quad [\![X]\!]_\eta \triangleq \eta(X) \\
&\quad [\![\phi \wedge \psi]\!]_\eta \triangleq [\![\phi]\!]_\eta \cap [\![\psi]\!]_\eta \\
&\quad [\![\phi \vee \psi]\!]_\eta \triangleq [\![\phi]\!]_\eta \cup [\![\psi]\!]_\eta \\
&\quad [\![< \alpha > \phi]\!]_\eta \triangleq < \alpha > [\![\phi]\!]_\eta \triangleq \{P \mid \exists P'.P \xrightarrow{\alpha} P' \wedge P' \in [\![\phi]\!]_\eta\} \\
&\quad [\![[\alpha]\phi]\!]_\eta \triangleq [\alpha][\![\phi]\!]_\eta \triangleq \{P \mid \forall P'.P \xrightarrow{\alpha} P' \wedge P' \in [\![\phi]\!]_\eta\} \\
&\quad [\![\nu Y.\phi_1]\!]_\eta \triangleq FIX(f^{\eta}_{\phi,X}) \triangleq \bigcup\{z \mid z \subseteq f^{\eta_{[X \to \cdot]}}_{\phi_1,Y}(z)\} \\
&\quad [\![\mu Y.\phi_1]\!]_\eta \triangleq fix(f^{\eta}_{\phi,X}) \triangleq \bigcap\{z \mid f^{\eta_{[X \to \cdot]}}_{\phi_1,Y}(z) \subseteq z\}
\end{aligned}$$

where $\eta \colon \mathcal{V} \to \mathcal{P}$ is defined as follows:

$$\eta_{[X \to S]}(Y) \begin{cases} \mathrm{S} & \text{if } Y = X \\ \eta(Y) & \text{if } Y \neq X \end{cases}$$

Note I'm assuming that for alpha conversion each new variable introduced by the last two operators is always different from each other variable already bounded in that scope.

2.1 Hennessy-Milner Logic without negation is well defined

Theorem 2.1. *The semantics of Hennessy-Milner's logic is well defined.*

Proof. By Knaster–Tarski theorem and lemma 2.1, then Hennessy-Milner's logic is well defined. □

Lemma 2.1 (HML semantic is monotone)**.** *Given a formula* ϕ, $f^{\eta}_{\phi,X}\colon (2^{\mathcal{P}},\subseteq) \to (2^{\mathcal{P}},\subseteq)$ *is monotone, i.e.*

$$\forall x, y \in 2^{\mathcal{P}}, x \subseteq y \implies f^{\eta}_{\phi,X}(x) \subseteq f^{\eta}_{\phi,X}(y)$$

Proof. By induction on the structure of ϕ.

- (base cases)
  - $\phi = T$
    (1) by the definition 2.2, $f^{\eta}_{\phi,X}(x) = f^{\eta}_{\phi,X}(y) = \mathcal{P}$
    (2) by (1), we can trivially deduce $f^{\eta}_{\phi,X}(x) \subseteq f^{\eta}_{\phi,X}(y)$
    $\implies f^{\eta}_{\phi,X}(x) \subseteq f^{\eta}_{\phi,X}(y)$
  - $\phi = F$
    (1) by the definition 2.2, $f^{\eta}_{\phi,X}(x) = f^{\eta}_{\phi,X}(y) = \varnothing$
    (2) by (1), we can trivially deduce $f^{\eta}_{\phi,X}(x) \subseteq f^{\eta}_{\phi,X}(y)$
    $\implies f^{\eta}_{\phi,X}(x) \subseteq f^{\eta}_{\phi,X}(y)$
  - $\phi = X$
    (1) by hypothesis, $x \subseteq y$
    (2) by the definition 2.2, $f^{\eta}_{\phi,X}(x) = [\![X]\!]_{\eta[X\to x]} = \eta_{[X\to x]}(X) = x$ and $f^{\eta}_{\phi,X}(y) = [\![X]\!]_{\eta[X\to y]} = \eta_{[X\to y]}(X) = y$
    (3) by (1) and (2), we can trivially deduce $f^{\eta}_{\phi,X}(x) \subseteq f^{\eta}_{\phi,X}(y)$
    $\implies f^{\eta}_{\phi,X}(x) \subseteq f^{\eta}_{\phi,X}(y)$
- (inductive cases)
  Inductive hypothesis: Given a formula ψ sub-formula of ϕ, then $f^{\eta}_{\psi,X}\colon (2^{\mathcal{P}},\subseteq) \to (2^{\mathcal{P}},\subseteq)$ is monotone.
  - $\phi = \phi_1 \wedge \phi_2$
    (1) by hypothesis, $x \subseteq y$
    (2) by the definition 2.2, $f^{\eta}_{\phi_1\wedge\phi_2,X}(s) = f^{\eta}_{\phi_1,X}(s) \cap f^{\eta}_{\phi_2,X}(s),\ \forall s \in 2^{\mathcal{P}}$
    (3) since ϕ_1 and ϕ_2 are sub formulas of ϕ, by inductive hypothesis $f^{\eta}_{\phi_1,X}(x) \subseteq f^{\eta}_{\phi_1,X}(y)$ and $f^{\eta}_{\phi_2,X}(x) \subseteq f^{\eta}_{\phi_2,X}(y)$
    (4) by all the above steps I can deduce $(f^{\eta}_{\phi_1,X}(x) \cap f^{\eta}_{\phi_2,X}(x)) \subseteq (f^{\eta}_{\phi_1,X}(y) \cap f^{\eta}_{\phi_2,X}(y))$
    $\implies f^{\eta}_{\phi,X}(x) \subseteq f^{\eta}_{\phi,X}(y)$
  - $\phi = \phi_1 \vee \phi_2$
    (1) by hypothesis, $x \subseteq y$
    (2) by the definition 2.2, $f^{\eta}_{\phi_1\vee\phi_2,X}(s) = f^{\eta}_{\phi_1,X}(s) \cup f^{\eta}_{\phi_2,X}(s),\ \forall s \in 2^{\mathcal{P}}$

(3) since ϕ_1 and ϕ_2 are sub formulas of ϕ, by inductive hypothesis $f^{\eta}_{\phi_1,X}(x) \subseteq f^{\eta}_{\phi_1,X}(y)$ and $f^{\eta}_{\phi_2,X}(x) \subseteq f^{\eta}_{\phi_2,X}(y)$

(4) by all the above steps, I can deduce $(f^{\eta}_{\phi_1,X}(x) \cup f^{\eta}_{\phi_2,X}(x)) \subseteq (f^{\eta}_{\phi_1,X}(y) \cup f^{\eta}_{\phi_2,X}(y))$

$\implies f^{\eta}_{\phi,X}(x) \subseteq f^{\eta}_{\phi,X}(y)$

- $\phi =< \alpha > \phi_1$

(1) by hypothesis, $x \subseteq y$

(2) by the definition 2.2, $f^{\eta}_{<\alpha>\phi_1,X}(s) =< \alpha > f^{\eta}_{\phi_1,X}(s),\ \forall s \in 2^{\mathcal{P}}$

(3) since ϕ_1 is a sub formula of ϕ, by inductive hypothesis $f^{\eta}_{\phi_1,X}(x) \subseteq f^{\eta}_{\phi_1,X}(y)$

(4) by all the above steps, I can deduce $f^{\eta}_{<\alpha>\phi_1,X}(x) \subseteq f^{\eta}_{<\alpha>\phi_1,X}(y)$ since all the processes that can perform a step α towards a state where ϕ holds, are both in $f^{\eta}_{\phi_1,X}(x)$ and $f^{\eta}_{\phi_1,X}(y)$ by inductive hypothesis

$\implies f^{\eta}_{\phi,X}(x) \subseteq f^{\eta}_{\phi,X}(y)$

- $\phi = [\alpha]\phi_1$

(1) by hypothesis, $x \subseteq y$

(2) by the definition 2.2, $f^{\eta}_{[\alpha]\phi_1,X}(s) = [\alpha] f^{\eta}_{\phi_1,X}(s),\ \forall s \in 2^{\mathcal{P}}$

(3) since ϕ_1 is a sub formula of ϕ, by inductive hypothesis $f^{\eta}_{\phi_1,X}(x) \subseteq f^{\eta}_{\phi_1,X}(y)$

(4) by all the above steps, I can deduce $f^{\eta}_{[\alpha]\phi_1,X}(x) \subseteq f^{\eta}_{[\alpha]\phi_1,X}(y)$ since all the processes that can perform a step α in any way towards a state where ϕ holds, are both in $f^{\eta}_{\phi_1,X}(x)$ and $f^{\eta}_{\phi_1,X}(y)$ by inductive hypothesis

$\implies f^{\eta}_{\phi,X}(x) \subseteq f^{\eta}_{\phi,X}(y)$

- $\phi = \nu Y.\phi_1$

(1) by hypothesis, $x \subseteq y$

(2) by the definition 2.2, $f^{\eta}_{\nu Y.\phi_1,X}(\cdot) = \bigcup\{z \mid z \subseteq f^{\eta[X\to\cdot]}_{\phi_1,Y}(z)\}$

(3) since ϕ_1 is a sub formula of ϕ, by inductive hypothesis $f^{\eta}_{\phi_1,X}(x) \subseteq f^{\eta}_{\phi_1,X}(y)$ that is $f^{\eta[X\to x]}_{\phi_1}(s) \subseteq f^{\eta[X\to y]}_{\phi_1}(s),\ \forall s \in 2^{\mathcal{P}}$

(4) Defining $POST_x = \{z \mid z \subseteq f^{\eta[X\to x]}_{\phi_1,Y}(z)\}$ and $POST_y = \{z \mid z \subseteq f^{\eta[X\to y]}_{\phi_1,Y}(z)\}$ it holds by (3) that $POST_x \subseteq POST_y$ since $POST_y = \{z \mid z \subseteq f^{\eta[X\to x]}_{\phi_1,Y}(z) \subseteq f^{\eta[X\to y]}_{\phi_1,Y}(z)\}$

(5) let's call $X_M \in POST_x$ the greatest fixed point of x and $Y_M \in POST_y$ the greatest fixed point of y, by all the above steps I can deduce $X_M \subseteq Y_M$

$\implies f^{\eta}_{\phi,X}(x) \subseteq f^{\eta}_{\phi,X}(y)$

- $\phi = \mu Y.\phi_1$

(1) by hypothesis, $x \subseteq y$

(2) by the definition 2.2, $f^{\eta}_{\mu Y.\phi_1,X}(\cdot) = \bigcap\{z \mid f^{\eta[X\to\cdot]}_{\phi_1,Y}(z) \subseteq z\}$

(3) since ϕ_1 is a sub formula of ϕ, by inductive hypothesis $f^{\eta}_{\phi_1,X}(x) \subseteq f^{\eta}_{\phi_1,X}(y)$ that is $f^{\eta[X\to x]}_{\phi_1}(s) \subseteq f^{\eta[X\to y]}_{\phi_1}(s),\ \forall s \in 2^{\mathcal{P}}$

(4) Defining $PRE_x = \{z \mid f^{\eta[X\to x]}_{\phi_1,Y}(z) \subseteq z\}$ and $PRE_y = \{z \mid f^{\eta[X\to y]}_{\phi_1,Y}(z) \subseteq z\}$ it holds by (3) that $PRE_x \supseteq PRE_y$ since $PRE_y = \{z \mid f^{\eta[X\to x]}_{\phi_1,Y}(z) \subseteq f^{\eta[X\to y]}_{\phi_1,Y}(z) \subseteq z\}$

(5) let's call $X_m \in PRE_x$ the least fixed point of x and $Y_m \in PRE_y$ the least fixed point of y, by all the above steps I can deduce $X_m \subseteq Y_m$

$\implies f^{\eta}_{\phi,X}(x) \subseteq f^{\eta}_{\phi,X}(y)$

□

2.2 Hennessy-Milner Logic extented with negation is well defined under some constraints

Definition 2.3 (HML syntax extended with negation)**.**

$$\phi, \psi = \ldots \mid \overline{\phi}$$

-

Definition 2.4 (HML semantic extended with negation)**.**

$$[\![\phi]\!]_\eta \triangleq$$

$$\ldots$$

$$[\![\overline{\phi}]\!]_\eta \triangleq \mathcal{P} \backslash [\![\phi]\!]_\eta$$

Proposition 2.1. *Given a formula ϕ with no negations, $\overline{\phi}$ is anti-monotonic.*

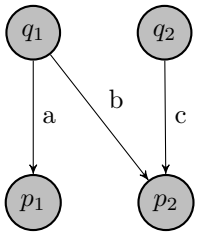
Proof. Since $x \subseteq y$ and by 2.1 $f^{\eta}_{\phi,X}$ is monotone, then

$$[\![\phi_1]\!]_{\eta[X\to x]} = \mathcal{P} \backslash [\![\phi_1]\!]_{\eta[X\to x]} \supseteq \mathcal{P} \backslash [\![\phi_1]\!]_{\eta[X\to y]} = [\![\phi_1]\!]_{\eta[X\to y]}$$

$\implies \phi$ is anti-monotonic against the negation □

Proposition 2.2. *There exists ϕ HML formula extented with negation such that it's non-monotonic.*

Proof. Considering the following transition system



and the formula

$$\phi = (< a > x \wedge < b > \overline{x}) \vee < c > x$$

we can see that by taking $S_1 = \{p_1\}, S_2 = \{p_1, p_2\}$ *s.t.* $S_1 \subseteq S_2$, we can notice that $[\![\phi]\!]_{\eta[x \to S_1]} \neq [\![\phi]\!]_{\eta[x \to S_2]}$

$$[\![\phi]\!]_{\eta[x \to S_1]} = (\{q_1\} \cap \{q_1\}) \cup \varnothing = \{q_1\}$$

$$[\![\phi]\!]_{\eta[x \to S_2]} = (\{q_1\} \cap \varnothing) \cup \{q_2\} = \{q_2\}$$

Therefore, the formula is non monotonic. □

Lemma 2.2 (Odd number of negations implies HML anti-monotonic)**.** *Given a formula ϕ, $f^{\eta}_{\phi,X} \colon 2^{\mathcal{P}} \to 2^{\mathcal{P}}$ extended with negation is anti-monotonic w.r.t X if X is under an odd number of negations in each sub-formula of ϕ.*

Proof. By induction on the structure of ϕ.

- (base cases)
  - $\phi = T$
    (1) by the definition 2.4 $f^{\eta}_{\phi,X}(x) = f^{\eta}_{\phi,X}(y) = \mathcal{P}$
    (2) by (1) we can trivially deduce $f^{\eta}_{\phi,X}(x) \supseteq f^{\eta}_{\phi,X}(y)$
    $\implies f^{\eta}_{\phi,X}(x) \supseteq f^{\eta}_{\phi,X}(y)$
  - $\phi = F$
    (1) by the definition 2.4 $f^{\eta}_{\phi,X}(x) = f^{\eta}_{\phi,X}(y) = \varnothing$
    (2) by (1) we can trivially deduce $f^{\eta}_{\phi,X}(x) \supseteq f^{\eta}_{\phi,X}(y)$
    $\implies f^{\eta}_{\phi,X}(x) \supseteq f^{\eta}_{\phi,X}(y)$
  - $\phi = \overline{X}$
    (1) by hypothesis $x \subseteq y$
    (2) by the definition 2.4 $f^{\eta}_{\phi,X}(x) = [\![\overline{X}]\!]_{\eta[X \to x]} = \mathcal{P} \backslash x$ and $f^{\eta}_{\phi,X}(y) = [\![\overline{X}]\!]_{\eta[X \to y]} = \mathcal{P} \backslash y$
    (3) by (1) and (2) we can trivially deduce $f^{\eta}_{\phi,X}(x) \supseteq f^{\eta}_{\phi,X}(y)$
    $\implies f^{\eta}_{\phi,X}(x) \supseteq f^{\eta}_{\phi,X}(y)$
- (inductive cases)
  Inductive hypothesis: Given a formula ψ sub-formula of ϕ, where the free variable X is under an even number of negations in ψ, then $f^{\eta}_{\psi,:} \, 2^{\mathcal{P}} \to 2^{\mathcal{P}}$ is anti-monotonic.
  - $\phi = \phi_1 \wedge \phi_2$

(1) by hypothesis $x \subseteq y$

(2) by the definition 2.4

$$f^{\eta}_{\phi_1 \wedge \phi_2, X}(s) = f^{\eta}_{\phi_1, X}(s) \cap f^{\eta}_{\phi_2, X}(s) = [\![\phi_1]\!]_{\eta[X \to s]} \cap [\![\phi_2]\!]_{\eta[X \to s]}, \ \forall s \in 2^{\mathcal{P}}$$

(3) since ϕ_1 and ϕ_2 are sub formulas of ϕ, by inductive hypothesis $f^{\eta}_{\phi_1, X}(x) \supseteq f^{\eta}_{\phi_1, X}(y)$ and $f^{\eta}_{\phi_2, X}(x) \supseteq f^{\eta}_{\phi_2, X}(y)$

(4) by all the above steps I can deduce $f^{\eta}_{\phi_1, X}(x) \cap f^{\eta}_{\phi_2, X}(x) \supseteq f^{\eta}_{\phi_1, X}(y) \cap f^{\eta}_{\phi_2, X}(y)$

$\implies f^{\eta}_{\phi, X}(x) \supseteq f^{\eta}_{\phi, X}(y)$

– $\phi = \phi_1 \vee \phi_2$

(1) by hypothesis $x \subseteq y$

(2) by the definition 2.4

$$f^{\eta}_{\phi_1 \vee \phi_2, X}(s) = f^{\eta}_{\phi_1, X}(s) \cup f^{\eta}_{\phi_2, X}(s) = [\![\phi_1]\!]_{\eta[X \to s]} \cup [\![\phi_2]\!]_{\eta[X \to s]}, \ \forall s \in 2^{\mathcal{P}}$$

(3) since ϕ_1 and ϕ_2 are sub formulas of ϕ, by inductive hypothesis $f^{\eta}_{\phi_1, X}(x) \supseteq f^{\eta}_{\phi_1, X}(y)$ and $f^{\eta}_{\phi_2, X}(x) \supseteq f^{\eta}_{\phi_2, X}(y)$

(4) by all the above steps I can deduce $f^{\eta}_{\phi_1, X}(x) \cup f^{\eta}_{\phi_2, X}(x) \supseteq f^{\eta}_{\phi_1, X}(y) \cup f^{\eta}_{\phi_2, X}(y)$

$\implies f^{\eta}_{\phi, X}(x) \supseteq f^{\eta}_{\phi, X}(y)$

– $\phi = < \alpha > \phi_1$

(1) by hypothesis $x \subseteq y$

(2) since ϕ_1 is sub formula of ϕ, by inductive hypothesis $f^{\eta}_{\phi_1, X}(x) \supseteq f^{\eta}_{\phi_1, X}(y)$

(3) by all the above steps, I can deduce $f^{\eta}_{<\alpha>\phi_1, X}(x) \supseteq f^{\eta}_{<\alpha>\phi_1, X}(y)$ since all the processes that can perform a step α in any way towards a state where ϕ holds, are both in $f^{\eta}_{\phi_1, X}(y)$ and $f^{\eta}_{\phi_1, X}(x)$ by inductive hypothesis

$\implies f^{\eta}_{\phi, X}(x) \supseteq f^{\eta}_{\phi, X}(y)$

– $\phi = [\alpha]\phi_1$

(1) by hypothesis $x \subseteq y$

(2) since ϕ_1 is sub formula of ϕ, by inductive hypothesis $f^{\eta}_{\phi_1, X}(x) \supseteq f^{\eta}_{\phi_1, X}(y)$

(3) by all the above steps, I can deduce $f^{\eta}_{[\alpha]\phi_1, X}(x) \supseteq f^{\eta}_{[\alpha]\phi_1, X}(y)$ since all the processes that can perform a step α towards a state where ϕ holds, are both in $f^{\eta}_{\phi_1, X}(y)$ and $f^{\eta}_{\phi_1, X}(x)$ by inductive hypothesis

$\implies f^{\eta}_{\phi, X}(x) \supseteq f^{\eta}_{\phi, X}(y)$

– $\phi = \nu Y.\phi_1$

(1) by hypothesis $x \subseteq y$

(2) since ϕ_1 is sub formula of ϕ, by inductive hypothesis $f^{\eta}_{\phi_1,X}(x) \supseteq f^{\eta}_{\phi_1,X}(y)$

(3) Defining $POST_x = \{z \mid z \subseteq f^{\eta[X\to x]}_{\phi_1,Y}(z)\}$ and $POST_y = \{z \mid z \subseteq f^{\eta[X\to y]}_{\phi_1,Y}(z)\}$ it holds by (3) that $POST_x \supseteq POST_y$ since $POST_y = \{z \mid z \subseteq f^{\eta[X\to y]}_{\phi_1,Y}(z) \subseteq f^{\eta[X\to x]}_{\phi_1,Y}(z)\}$

(4) let's call $X_M \in POST_x$ the greatest fixed point of x and $Y_M \in POST_y$ the greatest fixed point of y, by all the above steps I can deduce $X_M \supseteq Y_M$

$\implies f^{\eta}_{\phi,X}(x) \supseteq f^{\eta}_{\phi,X}(y)$

– $\phi = \mu Y.\phi_1$

(1) by hypothesis $x \subseteq y$

(2) since ϕ_1 is a sub formula of ϕ, by inductive hypothesis $f^{\eta}_{\phi_1,X}(x) \supseteq f^{\eta}_{\phi_1,X}(y)$

(3) Defining $PRE_x = \{z \mid f^{\eta[X\to x]}_{\phi_1,Y}(z) \subseteq z\}$ and $PRE_y = \{z \mid f^{\eta[X\to y]}_{\phi_1,Y}(z) \subseteq z\}$ it holds by (3) that $PRE_x \subseteq PRE_y$ since $PRE_y = \{z \mid f^{\eta[X\to y]}_{\phi_1,Y}(z) \subseteq f^{\eta[X\to x]}_{\phi_1,Y}(z) \subseteq z\}$

(4) let's call $X_m \in PRE_x$ the least fixed point of x and $Y_m \in PRE_y$ the least fixed point of y, by all the above steps I can deduce $X_m \supseteq Y_m$

$\implies f^{\eta}_{\phi,X}(x) \supseteq f^{\eta}_{\phi,X}(y)$

□

Lemma 2.3 (Even number of negations implies HML monotonic)**.** *Given a formula ϕ, $f^{\eta}_{\phi,X}\colon 2^{\mathcal{P}} \to 2^{\mathcal{P}}$ extended with negation is monotonic w.r.t X if X is under an odd number of negations in each sub-formula of ϕ.*

Proof. By induction on the structure of ϕ.

- (base cases)

– $\phi = T$

(1) trivial

$\implies f^{\eta}_{\phi,X}(x) \subseteq f^{\eta}_{\phi,X}(y)$

– $\phi = F$

(1) trivial

$\implies f^{\eta}_{\phi,X}(x) \subseteq f^{\eta}_{\phi,X}(y)$

– $\phi = \overline{\overline{X}}$

(1) by hypothesis $x \subseteq y$

(2) by the definition 2.4, I can conclude $f^{\eta}_{\overline{\overline{X}},X}(x) = \mathcal{P}\backslash(\mathcal{P}\backslash x) = x = f^{\eta}_{X,X}(x)$ and $f^{\eta}_{\overline{\overline{X}},X}(y) = \mathcal{P}\backslash(\mathcal{P}\backslash y) = y = f^{\eta}_{X,X}(y)$

(3) by (1) and (2) we can trivially deduce $f^{\eta}_{\phi,X}(x) \subseteq f^{\eta}_{\phi,X}(y)$

$\implies f^{\eta}_{\phi,X}(x) \subseteq f^{\eta}_{\phi,X}(y)$

- (inductive cases)

  Inductive hypothesis: Given a formula $\overline{\psi}$ sub-formula of ϕ, where the free variable X is under an odd number of negations in ψ, then $f^{\eta}_{\overline{\psi},:}\ 2^{\mathcal{P}} \to 2^{\mathcal{P}}$ is monotonic.

  - $\phi = \phi_1 \wedge \phi_2$

    (1) trivial

    $\implies f^{\eta}_{\phi,X}(x) \subseteq f^{\eta}_{\phi,X}(y)$

  - $\phi = \phi_1 \vee \phi_2$

    (1) trivial

    $\implies f^{\eta}_{\phi,X}(x) \subseteq f^{\eta}_{\phi,X}(y)$

  - $\phi =< \alpha > \phi_1$

    (1) trivial

    $\implies f^{\eta}_{\phi,X}(x) \subseteq f^{\eta}_{\phi,X}(y)$

  - $\phi = [\alpha]\phi_1$

    (1) trivial

    $\implies f^{\eta}_{\phi,X}(x) \subseteq f^{\eta}_{\phi,X}(y)$

  - $\phi = \nu Y.\phi_1$

    (1) trivial

    $\implies f^{\eta}_{\phi,X}(x) \subseteq f^{\eta}_{\phi,X}(y)$

  - $\phi = \mu Y.\phi_1$

    (1) trivial

    $\implies f^{\eta}_{\phi,X}(x) \subseteq f^{\eta}_{\phi,X}(y)$

□