

# Esercizi esame Linguaggi per il Global Computing

F.

July 2019

## 1 Esercizio B

### 1.1 Testo

Dimostrare che ogni processo del CCS finito termina in un numero finito di passi.

$$P, Q = 0 \mid \alpha.P \mid P + Q \mid P|Q \mid P \setminus L \mid P[f]$$

### 1.2 Dimostrazione con somme finite

Voglio dimostrare che  $\forall S \in CCS$  se  $S \xrightarrow{\alpha} S'$ ,  $S'$  finito  $\implies S$  termina in un numero finito di passi, definisco  $size(S)$  come limite superiore al numero di passi del processo S:

$$\begin{aligned} size(0) &= 0 \\ size(\alpha.P) &= 1 + size(P) \\ size(P|Q) &= size(P) + size(Q) \\ size(P + Q) &= \max\{size(P), size(Q)\} \\ size(P \setminus L) &= size(P) \\ size(P[f]) &= size(P) \end{aligned}$$

E' anche possibile dimostrare che il numero di stati raggiungibili da S è finito, per fare questo definisco B come il bound superiore al numero di stati raggiungibili da P:

$$\begin{aligned} B(0) &= 1 \\ B(\alpha.P) &= 1 + B(P) \\ B(P|Q) &= B(P) * B(Q) \\ B(P + Q) &= B(P) + B(Q) \\ B(P \setminus L) &= B(P) \\ B(p[f]) &= B(P) \end{aligned}$$

**Dimostrazione** Dimostro che dati processi con altezza di derivazione (albero di generazione dato dalla grammatica) finita allora la loro esecuzione è finita, questo perchè il numero di passi è superiormente limitato dall'atezza dell'albero e quindi è finito.

Dimostro che se  $S \xrightarrow{\alpha} S' \implies size(S) > size(S')$  e che dato che l'albero di derivazione di  $S$  è finito per ipotesi allora anche i suoi sottoalberi sono finiti e se per ogni processo che fa un passo vale che  $size(S) > size(S')$ , allora  $S$  termina.

Inoltre è possibile dimostrare che anche il numero di stati raggiungibili è finito, l'ipotesi è che se il numero di stati stati raggiungibili dai sottoprocessi di  $S$  è finito, allora anche gli stati raggiungibili da  $S$  sono finiti.

Procedo per induzione sulla lunghezza della derivazione della grammatica sopra riportata:

**Caso Base  $S = 0$  :**

$S$  ha lunghezza di derivazione 0, ovvero  $S = 0$ , non esegue nessun passo,  $S$  termina in un numero finito di passi. Inoltre  $B(0) = 1$  e  $size(0) = 0$  quindi entrambi sono finiti.

**Casi Induttivi** In questi casi la lunghezza della derivazione è  $n + 1$  e so che fino a lunghezza  $n$  l'ipotesi induttiva è vera, ovvero l'albero di derivazione di  $S$  ha altezza finita e che se  $S \xrightarrow{\alpha} S' \implies size(S) > size(S')$ . Ora procedo sull'altezza  $n + 1$  in base all'ultimo passo di derivazione applicato.

**Caso Induttivo Prefix  $S = \alpha.P$  :**

Per la regola ACT  $\alpha.P \xrightarrow{\alpha} P$ , quindi  $size(S) = 1 + size(P)$  ovvero  $size(S) > size(P)$  e per ipotesi è vero che  $size(P)$  è finita perchè l'altezza dell'albero di derivazione è  $1 -$  altezza di  $S$  e altezza di  $S$  è finita, per ipotesi induttiva quindi  $P$  termina in un numero finito di passi allora anche  $S$  termina in un numero finito di passi.

Inoltre è possibile dimostrare che anche il bound al numero di stati raggiungibili è finito dato che  $B(P)$  è finito per ipotesi induttiva è  $B(S) = B(P) + 1$  e quindi finito.

**Caso Induttivo Parallelo  $S = P|Q$  :**

È vero che  $size(S) = size(P) + size(Q)$  e  $B(S) = B(P) * B(Q)$ . Ci sono tre casi in base alle regole PAR:

$PAR_{\setminus L}$   $S = P|Q \xrightarrow{\alpha} P'|Q$  e  $S' = P'|Q$ , so per ipotesi che  $S$  ha altezza dell'albero di derivazione finita, gli alberi di derivazione di  $P$  e  $Q$  sono quindi finiti anch'essi e si ha che:

$$size(S) = size(P) + size(Q) \text{ e } size(S') = size(P') + size(Q)$$

Per la premessa alla regola  $P \xrightarrow{\alpha} P'$ , quindi applico l'ipotesi induttiva che dice che  $size(P) > size(P')$ , allora è vero che  $size(S) > size(S')$ .

Inoltre  $B(S) = B(P) * B(Q)$  e per ipotesi  $B(P)$  e  $B(Q)$  sono finiti per cui anche il limite superiore al numero di stati raggiungibili da  $S$  è finito.

$PAR_{\setminus R}$  Analogo con  $P$  e  $Q$  scambiati

$SINC$   $S = P|Q \xrightarrow{\alpha} P'|Q'$  e  $S' = P'|Q'$ , so per ipotesi che altezza di  $S$  è finita, per cui anche l'altezza di  $P$  e  $Q$  sono finite.

Per la premessa alla regola sia  $P$  che  $Q$  fanno un passo per andare in  $P'$  e  $Q'$ , quindi posso applicare l'ipotesi induttiva e so che:  $size(P) > size(P')$  e  $size(Q) > size(Q')$ , quindi  $size(S) > size(S')$ .

Inoltre  $B(S) = B(P) * B(Q)$  e per ipotesi  $B(P)$  e  $B(Q)$  sono finiti per cui anche  $B(S)$  lo è.

**Caso Induttivo Non Determinismo  $S = P+Q$  :**

$size(S) = \max\{size(P), size(Q)\}$  e  $B(S) = B(P) + B(Q)$ , ci sono due casi in base alle regole SUM:

$SUM_{\setminus L}$  in questo caso  $S = P + Q \xrightarrow{\alpha} P' = S'$ , ovvero  $S$  fa un passo e va in  $P'$ , in questo caso si ha  $size(S) = \max\{size(P), size(Q)\}$  e  $size(S') = \max\{size(P'), size(Q)\}$  a sua volta ci sono due casi:

Max= $P$  in questo caso  $size(S) = size(P)$  e  $S \xrightarrow{\alpha} S' = P'$  quindi  $size(S') = size(P')$  e siccome  $P$  ha come sottoprocesso  $P'$ , ovvero l'albero di derivazione di  $P'$  è di altezza finita in quando minore di  $P$  (che è finito per ipotesi), posso applicare l'ipotesi induttiva che dice che  $size(P) > size(P')$  quindi  $size(S) = size(P) > size(P') = size(S')$ .

Max= $Q$  in questo caso  $size(S) = size(Q)$  e  $S \xrightarrow{\alpha} S' = P'$  quindi  $size(S') = size(P')$ . Sappiamo che  $size(Q) > size(P)$  e che  $P$  fa un passo per andare in  $P'$ , l'albero di derivazione di  $P'$  è quindi minore dell'albero di derivazione di  $P$ , quindi posso applicare l'ipotesi induttiva che dice che  $size(P) > size(P') \implies size(Q) > size(P) > size(P') \implies size(S) > size(S')$ .

$SUM_{\setminus R}$  analogo con  $P$  e  $Q$  scambiati.

In tutti i casi si ha che  $B(S) = B(P) + B(Q)$  e per ipotesi sappiamo che  $B(P)$  e  $B(Q)$  sono finiti, per cui anche  $B(S)$  è finito.

In tutti i casi so anche che  $B(S) = B(P) + B(Q)$  e per ipotesi  $B(P)$  e  $B(Q)$  sono finiti per ipotesi per cui anche  $B(S)$  è finito.

**Caso Induttivo Restriction  $S=P_{\setminus L}$  :**

In questo caso  $size(S) = size(P)$  e  $B(S) = B(P)$ .

Per la regola RES  $P_{\setminus L} \xrightarrow{\alpha} P'_{\setminus L}$  quindi  $size(S') = size(P'_{\setminus L}) = size(P')$ . Sappiamo che  $P$  fa un passo ( $\alpha \notin L$ ) e va in  $P'$ , e l'albero di derivazione di  $P'$

è minore di quello di  $P$  e quindi è finito, posso applicare l'ipotesi induttiva che  $size(P) > size(P') \implies size(S) > size(S')$ .

Inoltre  $B(S) = B(P)$  e  $B(S') = B(P')$  per ipotesi si ha che  $B(P')$  è finito (in quanto sottoprocesso di  $S$ ) per cui anche  $B(S)$  lo è.

#### Caso Induttivo Relabeling $S=P[f]$ :

Anche in questo caso  $size(S) = size(P)$  e  $B(S) = B(P)$ .

Per la regola REL  $P[f] \xrightarrow{f(\alpha)} P'[f] = S'$ , e  $size(S') = size(P')$ . Per la premessa alla regola sappiamo che  $P$  fa un passo e va in  $P'$ , e l'albero di derivazione è più piccolo e quindi finito, per l'ipotesi induttiva è quindi vero che  $size(P) > size(P')$  quindi  $size(S) > size(S')$  e quindi  $S$  termina.

Anche il numero di stati raggiungibili è finito perché per ipotesi  $B(P')$  è finito in quanto sottoprocesso di  $P(=S)$  e  $B(S) = B(P) = B(P')$  per cui è finito.

### 1.3 Dimostrazione con somme infinite

In questo caso non è possibile dimostrare che il numero di stati raggiungibili è finito perché il bound superiore al numero di stati è definito come la somma tra tutti i bound dei processi sommati, ovvero  $B(P+Q) = B(P) + B(Q)$ , quindi nel caso di una scelta tra un numero infinito di processi la somma sarebbe infinita.

Si può comunque dimostrare che i processi che contengono scelte non deterministiche tra un numero infinito di processi terminano.

Per fare ciò utilizzo la struttura della grammatica che genera CCS, l'ipotesi induttiva è quindi che se il processo generato ha altezza di derivazione finita (indipendentemente dalla presenza di somme infinite) allora termina in un numero finito di passi.

Procedo per induzione sulla lunghezza della derivazione, la dimostrazione è analoga a quella delle somme finite tranne nel caso della regola sum infinita:

**Caso**  $S = \sum_{i \in I} P_i$  in questo caso la somma è infinita, ci sono quindi infiniti  $P_i$  che vengono sommati e  $size(S) = \max\{size(P_i) | i \in I\}$ . Sappiamo che la regola dice che  $S \xrightarrow{\alpha} P'_i$  per un qualche  $i \in I$ . Per ipotesi  $S$  ha albero di derivazione finito e quindi ognuno dei  $P_i$  ha altezza finita, posso quindi applicare l'ipotesi induttiva che per ogni  $P_i$ , se  $P_i \xrightarrow{\alpha} P'_i$  allora  $size(P_i) > size(P'_i)$  ovvero  $size(S) = \max\{size(P_i) | i \in I\} > size(S')$  per ogni  $S'$ .

Abbiamo quindi dimostrato che sia nel caso finito che nel caso infinito i processi CCS terminano in un numero finito di passi.

## 2 Esercizio Q

### 2.1 Testo

Dimostrare il teorema di Knaster-Tarski nel caso di reticoli completi

**Enunciato Teorema** Sia  $L$  un reticolo completo e  $f : L \rightarrow L$  una funzione monotona  $\Rightarrow$  l'insieme dei punti fissi di  $f$  in  $L$  è un reticolo completo.

**Def. Upper Bound** : sia  $S$  un insieme di numeri reali,  $x$  è un upper bound di  $S$  se  $x \geq s \forall s \in S$

**Def. Least Upper Bound** :  $x$  è un Least Upper Bound di  $S$  se  $x \leq y \forall y$  upper bounds di  $S$

**Def. Insieme Parzialmente Ordinato** : è un insieme  $I$  su cui per ogni sua coppia di elementi vale una relazione binaria  $\sqsubseteq$  che soddisfa i seguenti assiomi:

- riflessività (ogni elemento è in relazione con sè stesso)
- antisimmetria ( $a \leq b, b \leq a \implies a = b$ )
- transitività ( $a \leq b, b \leq c \implies a \leq c$ )

**Def. Reticoli Complet** : un insieme parzialmente ordinato  $L$  in cui ogni sottoinsieme ha  $\text{lub}$  e  $\text{glb}$  in  $L$ .

### 2.2 Dimostrazione

Per dimostrare che l'insieme dei punti fissi di  $f$  in  $L$  è un reticolo completo dimostro che dato  $\langle P, \sqsubseteq \rangle$  l'insieme dei punti fissi di  $f$ :

- sia  $P_1 = \{x \in L \mid x \sqsubseteq f(x)\}$ , il  $\text{lub}$  di  $P_1 = \text{gfp}$  (greatest fixed point) di  $f$  e quindi  $\in P$
- sia  $P_2 = \{x \in L \mid f(x) \sqsubseteq x\}$ , il  $\text{glb}$  di  $P_2 = \text{lfp}$  (least fixed point) di  $f$  quindi  $\in P$
- ogni sottoinsieme dei punti fissi di  $f$  in  $L$  ha  $\text{lub}$  e  $\text{glb}$  ed essi  $\in P$

I primi due punti dimostrano il Lemma di Knaster Tarski e il terzo dimostra che è un complete lattice.

**Punto 1** Dimostro che dato  $P_1 = \{x \in L \mid x \sqsubseteq f(x)\}$  ovvero l'insieme di tutti i postfix points, il *lub* di tale insieme è il greatest fixed point di  $f$  (ed appartiene a  $P_1$ ).

Sia

$$u = \sqcup P_1 \implies \forall x \in P_1 \ x \sqsubseteq u$$

e per monotonia di  $f$  vale anche che

$$\forall x \in P_1 \ f(x) \sqsubseteq f(u)$$

e per definizione di  $P_1$   $x \sqsubseteq f(x)$ , questo indica che  $f(u)$  è un **upper bound** dell'insieme  $P_1$  (perché  $x \sqsubseteq f(x) \sqsubseteq f(u)$ ). Ma  $u$  è il least upper bound quindi

$$u \sqsubseteq f(u) \implies u \in P_1$$

Dato che  $u \in P_1$  per monotonia di  $f$  si ha che

$$f(u) \sqsubseteq f(f(u)) \implies f(u) \in P_1$$

quindi  $f(u) \sqsubseteq u$  Allora:

- $u \sqsubseteq f(u)$
- $f(u) \sqsubseteq u$

$$\implies u = f(u) = \sqcup P_1 \text{ e } \in P_1.$$

Siccome ogni fixed point appartiene all'insieme  $P_1$ , perché

$$\forall n \in P \ f(n) = n \text{ ovvero } n \sqsubseteq f(n) \implies n \in P_1$$

e  $u = f(u) = \sqcup P_1$  è il *lub* di tale insieme, allora  $\forall n \in P \ n \in P_1$  e

$$n = f(n) \sqsubseteq u = f(u) = \sqcup P_1$$

Ovvero  $u = f(u)$  è il più grande fixed point di  $f$  ed è il *least upper bound* di  $P_1$  ed  $\in P$  in quanto è un fixed point.

**Punto 2** Dimostro che dato  $P_2 = \{x \in L \mid x \sqsupseteq f(x)\}$  ovvero l'insieme dei prefixed point di  $f$  in  $L$ , il *glb* di tale insieme è uguale al least fixed point di  $f$ .

Sia

$$l = glb(P_2) = \sqcap P_2 \implies l \sqsubseteq x \ \forall x \in P_2$$

. Per monotonia di  $f$  è vero che

$$\forall x \in P_2 \ f(l) \sqsubseteq f(x)$$

ovvero  $f(l)$  è un **lower bound** di  $P_2$ .

$l$  è il greatest lower bound di  $P_2$  quindi

$$l \sqsupseteq f(l) \implies l \in P_2$$

( $l$  è in  $L$  perché  $f : L \rightarrow L$ ).

Per monotonia di  $f$ :

$$f(l) \supseteq f(f(l)) \Rightarrow f(l) \in P_2$$

e quindi  $l \subseteq f(l)$  in quanto  $l$  è greatest lower bound di  $P_2$ , ovvero è minore o uguale a tutti gli elementi di  $P_2$ . Quindi:

- $l \supseteq f(l)$
- $f(l) \supseteq l$

$\Rightarrow l = f(l) = \sqcap P_2$ .  $l$  è chiaramente un fixed point, e siccome tutti i fixed point appartengono a  $P_2$  (perché  $\forall n \in P \ f(n) = n$  è vero anche che  $n \supseteq f(n) \Rightarrow n \in P_2$ ) e  $l = f(l)$  è il greatest lower bound di  $P_2$

$$\Rightarrow f(l) \subseteq x \ \forall x \in P_2$$

quindi è più piccolo di tutti gli elementi in  $P_2$  quindi anche di tutti i fixed point, ovvero è il least fixed point di  $f$  in  $L$  ed appartiene a  $L$  perché  $f$  ha dominio in  $L$ .

**Punto 3** Devo dimostrare che per ogni sottoinsieme di  $P$  esistono  $\text{lub}$  e  $\text{glb}$  e che appartengono a  $P$ , ovvero che sono punti fissi.

Sia  $S \subseteq P$  e  $q = \sqcup S$  (least upper bound di  $S$ ),  $q$  esiste perché  $S \subseteq P \subseteq L$  e  $L$  è un complete lattice, quindi per definizione di complete lattice ogni suo sottoinsieme ha  $\text{lub}$  e  $\text{glb}$  in  $L$ .

Sia inoltre

$$I = \{x \in L \mid q \subseteq x\}$$

**3.1** Si ha che (per riflessività della relazione d'ordine)  $q \subseteq q \Rightarrow q \in I$ .

( $I$  è sottoinsieme di  $L$ , quindi ha un  $\text{glb}$ , per assurdo supponiamo che esista un  $q'$  strettamente più grande di  $q$  e che sia il  $\text{glb}$ , ma allora se è strettamente maggiore di  $q$   $q' \in I$  ma quindi  $q$ , che appartiene a  $I$  è più piccolo  $\Rightarrow q'$  NON è il  $\text{glb}$  )

Per definizione  $q$  è il  $\text{glb}$  dell'insieme  $I$ , in quanto è il più grande elemento che è più piccolo di ogni elemento appartenente all'insieme,

$$q = \text{glb}(I) = \sqcap I \Rightarrow \text{glb}(I) \in I$$

**3.2**  $I$  è un sottoinsieme e  $I \subseteq L$  quindi ha un  $\text{lub}$  in  $L$ , inoltre è vero che

$$\forall x \in I \ x \subseteq \text{lub}(I)$$

ma sappiamo anche che

$$\forall x \in I \ q \subseteq x$$

Allora

$$\Rightarrow q \subseteq x \subseteq \text{lub}(I) \Rightarrow \text{lub}(I) \in I$$

**3.3**  $I$  è un intervallo perchè contiene tutti gli elementi da  $q$  a  $Top$  element di  $L$ , inoltre  $I$  è sottoinsieme di  $L$  complete lattice, quindi  $I$  è un complete lattice.

Ora dimostro che  $f$  definita su  $I$  ha codominio  $I$ , ovvero  $f$  è chiusa rispetto a  $I$ , (se questo è vero posso applicare i punti 1 e 2 ecc).

Per definizione di  $I$  e di  $S$  si ha che

$$\forall x \in I, \forall s \in S \ s \sqsubseteq q \text{ e } q \sqsubseteq x$$

Per monotonia di  $f$  vale quindi  $f(s) \sqsubseteq f(q) \sqsubseteq f(x) \ \forall x \in I, \forall s \in S$

$$\implies f(s) \sqsubseteq f(x)$$

Per definizione di  $S$  ogni elemento in  $S$  è un punto fisso (sottoinsieme di  $P$ ), quindi

$$\forall s \in S \ \forall x \in I \ f(s) = s \sqsubseteq f(x)$$

Quindi  $f(x)$  è un upper bound dell'insieme  $S$ ,  $\implies q = lub(S) \sqsubseteq f(x)$  ovvero  $q \sqsubseteq f(x) \ \forall x \in I$ . over

$$\forall x \in I \ q \sqsubseteq f(x) \implies f(x) \in I$$

Ora so che:  $I$  è un complete lattice in quanto intervallo in un complete lattice,  $\forall x \in I \ f(x) : I \rightarrow I$ , posso quindi applicare il punto **2** e vale che

$$q' = lfp \text{ di } f \in I \text{ (e } P)$$

Per definizione di  $q$ ,  $q = glb(I)$ ,  $\implies q \sqsubseteq q'$ , quindi  $q'$  è upper bound di  $I$ , ma siccome  $q'$  è il least fixed point è in  $P$ , ma è il più piccolo elemento in  $I$  (e  $P$ )  $\implies$  è least upper bound di  $S$ . Allora  $q = \sqcup S \in P$ .

## 2.3 Knaster Tarski in CCS

Sia  $R \subseteq Proc \times Proc$  tc se  $(P, Q) \in R$  allora:

- $\forall P \xrightarrow{\alpha} P' \exists Q \xrightarrow{\alpha} Q' \text{ tc } (P', Q') \in R$
- $\forall Q \xrightarrow{\alpha} Q' \exists P \xrightarrow{\alpha} P' \text{ tc } (P', Q') \in R$

Definisco

$$F(R) = \{(P, Q) | \text{proprietà sopra}\}$$

Allora se  $(P, Q) \in R \implies (P, Q) \in F(R)$ , ovvero  $R \subseteq F(R)$  cioè  $R$  è bisimulazione.

$F$  è monotona perchè più grande è  $R$  più coppie ci sono in  $F(R)$  (mantiene la relazione di  $\sqsubseteq$  da  $R$  a  $F$ ).

$R$  è bisimulazione sse  $R \subseteq F(R)$ .  $\sim = \cup$  bisimulazioni cioè  $\sim = \cup \{R | R \text{ è bisimulazione}\} = \cup \{R | R \subseteq F(R)\}$  quindi  $\sim = \max \text{ Fixed Point}(F)$ .