# Esercizi esame Linguaggi per il Global Computing

Francesca Del Nin

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 il 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 se $S \xrightarrow{\alpha} S' \implies size(S) > size(S')$ e che se i sottoprocessi di S sono finiti (size S' è finita) allora S termina. Dimostrazione per induzione sulla struttura di S,
l'ipotesi è che

se i sottoprocessi di S terminano in un numero finito di passi allora anche S termina in un numero finito di passi.

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.

**Caso Base S = 0** :

S non esegue nessun passo per cui $S \stackrel{\alpha}{\not\to} \implies$ S termina in un numero finito di passi. Inoltre $B(0) = 1$ e $size(0) = 0$

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

Per la regola ACT $\alpha.P \xrightarrow{\alpha} P$ e per ipotesi induttiva so che P termina in un numero finito di passi (size(P) è finita). $size(S) = 1 + size(P)$ quindi anch'essa finita perche si aggiunge un passo ai passi (finiti) di P.

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 quidi finito.

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

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

$PAR_{\backslash L}$ $S = P|Q \xrightarrow{\alpha} P'|Q$ e $S' = P'|Q$, so per ipotesi induttiva che $P$ e $Q$ sono finiti e terminano in un numero finito di passi, e so che $size(S') = size(P') + size(Q)$ e so che la premessa alla regola SUM1 $P \xrightarrow{\alpha} P'$ vale. Quindi $size(P) = 1 + size(P')$ (perche fa un passo da P a P') e si ha che $size(S) = size(P) + size(Q) = 1 + size(P') + size(Q) > size(P') + size(Q) = size(S')$.

Per ipotesi induttiva $P$ e $Q$ terminano per cui anche $S$ termina.

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

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

$SINC$ $S = P|Q \xrightarrow{\alpha} P'|Q'$ e $S' = P'|Q'$, so per ipotesi induttiva che P' e Q' sono finiti. In questo caso i due processi si sincronizzano eseguendo un passo, quindi $size(S) = 1 + size(S') > size(S')$ e S termina in un numero finito di passi.

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:

$SUM_{\backslash L}$ 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 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 fatto un passo per arrivare in P' è vero anche che $size(P) = 1 + size(P')$ e quindi $size(S) = size(P) > size(P') = size(S')$.

Inoltre per ipotesi induttiva $Q$ e $P$ terminano per cui anche $S$ termina.

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'. Si deduce che $size(S) = size(Q) > size(P) > size(P') = size(S')$. Inoltre per ipotesi induttiva $Q$ e $P$ terminano per cui anche $S$ termina.

$SUM_{\backslash R}$ 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.

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

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

Per la regola RES $P_{\backslash L} \xrightarrow{\alpha} P'_{\backslash L}$ quindi $size(S') = size(P'_{\backslash L}) = size(P')$. Sappiamo che P fa un passo ($\alpha \notin L$) e va in P', per cui $size(P) = 1 + size(P') > size(P') \implies size(S) > size(S')$. Per ipotesi induttiva $size(P')$ è finita per cui S termina.

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', per cui si ha che $size(P) = 1 + size(P')$ quindi $size(S) > size(S')$, inoltre per ipotesi induttiva $P'$ termina in un numero finito di passi per cui anche $S$ 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 lunghezza finita (indipendentemente dalla presenza di somme infinite) allora termina in un numero finito di passi.

Procedo per induzione sula lunghezza della derivazione:

### 1.3.1 Caso Base

In questo caso la lunghezza è 0, l'unico processo di lunghezza 0 è 0, che non ha passi possibili e $size(0) = 0$.

### 1.3.2 Casi Indittuvi

in questo caso la lunghezza della dervazione è $n + 1$ e per ipotesi sappiamo che fino alla lunghezza $n$ è vero che il processo termina in un numero finito di passi, ovvero $size(\text{derivaizone fino ad } n) = k$ con $k$ finito.

**Caso** $S = \alpha.P$ In questo caso alla derivazione di $P$ stiamo "aggiungendo" $\alpha$ e quindi $size(S) = 1 + size(P)$ e siccome $size(P)$ è finita per ipotesi induttiva anche $size(S)$ lo è.

**Caso** $S = P|Q$ $P$ e $Q$ sono processi che terminano in un numero finito di passi, ovvero la loro funzione $size$ è finita. Sappiamo che $size(P + Q) = size(P) + size(Q)$ quindi è finita.

**Caso** $S = P_{\setminus L}$ In questo caso sappiamo che $P$ è finito e applichiamo una restrizione a P, il processo $S$ termina quindi in un numero finito di passi perchè $P$ termina per ipotesi e $size(S) = size(P)$.

**Caso** $S = S[f]$ $P$ termina per ipotesi induttiva e stiamo applicando una funzione di relabeling ai canali di $P$, $size(S) = size(P)$ e quindi termina in un numero finito di passi dato che $P$ termina in un numero finito di passi per ipotesi.

**Caso** $S = \sum_{i \in I} P_i$ in questo caso la somma è infinta, ci sono quindi infiniti $P_i$ che vengono sommati, per ipotesi induttiva ognuno dei $P_i$ termina in un numero finito passi ovvero $size(P_i) = k$ con $k$ finito. $size(S) = max\{size(P_i)|i \in I\}$, ma sappiamo che ogni $size(P_i)$ è finita per cui anche $size(S)$ è finita.

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 $f : L \to L$ 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 Completi** : un insieme parzialmente ordinato L in cui ogni sottoinsieme ha *lub* e *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 $P_1 = \{x \in L | x \sqsubseteq f(x)\}$, il *lub* di $P_1 = gfp$ (greatest fixed point) di $f$ e quindi $\in P$
- sia $P_2 = \{x \in L | f(x) \sqsubseteq x\}$, il *glb* di $P_2 = lfp$ (least fixed point) di $f$ quindi $\in P$

- ogni sottoinsieme dei punti fissi di $f$ in $L$ ha *lub* e *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 $P_1 = \{x \in L | x \sqsubseteq f(x)\}$ ovvero l'insieme di tutti i postfix points, il *lub* di tale insieme è il greatest fixed point di $f$ (ed appartiene a $P1$).

Sia $u = \sqcup P_1$ allora $\forall x \in P_1$ $x \sqsubseteq u$ 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:

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

$\implies u = f(u) = \sqcup P_1$ 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 $P_2 = \{x \in L | x \sqsupseteq f(x)\}$ ovvero l'insieme dei prefixed point di $f$ in $L$, il *glb* di tale insieme è uguale al least fixed point di $f$.

Sia $l = \sqcap P_2$ allora $l \sqsubseteq x$ $\forall x \in P_2$. 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 $l \sqsupseteq f(l)$, allora $l \in P_2$ ($l$ è in L perché $f : L \to L$).

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

- $l \sqsupseteq f(l)$
- $f(l) \sqsupseteq l$

$\implies l = f(l) = \sqcap P_2$. $l$ è chiaramente un fixed point, e siccome tutti i fixed point appartengono a $P_2$ perchè $\forall n \in P\ f(n) = n$ è vero anche che $n \sqsupseteq f(n) \implies n \in P_2$ e $l = f(l)$ è il greatest lower bound di $P_2 \implies f(l) \sqsubseteq x\ \forall x \in P_2$ 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 $lub$ e $glb$ e cha 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 lub e glb in $L$.

Sia inoltre

$$I = \{x \in L | q \sqsubseteq x\}$$

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

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

Per defizione $q$ è il glb dell'insieme $I$, in quanto è il più grande elemento che è più piccolo di ogni elemento appartente all'insieme,

$$q = glb(I) = \sqcap I \implies glb(I) \in I$$

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

$$\forall x \in I\ x \sqsubseteq lub(I)$$

ma sappiamo anche che

$$\forall x \in I\ q \sqsubseteq x$$

Allora

$$\implies q \sqsubseteq x \sqsubseteq lub(I) \implies lub(I) \in I$$

**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 $q \sqsubseteq f(x) \forall x \in I$. ovver

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

Ora so che: $I$ è un complete lattice in quanto intervallo in un complete lattice, $\forall x \in I \; f(x) : I \to I$, 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, ma siccome $q'$ è il least fixed point è in P, ma è il più piccolo elemento in P $\implies$ è least upper bound.

## 2.3 Knaster Tarski in CCS

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

- $\forall P \xrightarrow{\alpha} P' \exists Q \xrightarrow{\alpha} Q'$ tc $(P', Q') \in R$
- $\forall Q \xrightarrow{\alpha} Q' \exists P \xrightarrow{\alpha} P'$ 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 $\sim = \cup\{R | R$ è bisimulazione$\} = \cup\{R | R \subseteq F(R)\}$ quindi $\sim =$ max Fixed Point$(F)$.