Esercizi esame Linguaggi per il Global Computing

Francesca Del Nin

June 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 e 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 = α.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 $size(P) = 1 + size(P') > size(P') \Rightarrow size(S) > size(S')$. 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" α 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.

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. reticoli completi : un insieme parzialmente ordinato in cui ogni sottoinsieme ha *lub* e *glb*

2.2 Dimostrazione

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

- il *lub* di P $= gfp$ (greatest fixed point) di f e quindi $\in L$
- il *glb* di P $= lfp$ (least fixed point) di fe quindi $\in L$
- ogni sottoinsieme dei punti fissi di f in L ha *lub* e *glb* ed essi $\in L$

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

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

Si ha che $\forall x \in P_1$ vale $x \leq f(x)$ per definizione, per monotonia di f si ha che $f(x) \leq f(f(x))$ e quindi $f(x) \in P_1$

Sia $u = \vee P_1$ allora $\forall x \in P_1 . x \leq u$ e per monotonia di f vale anche che $\forall x \in P_1 . f(x) \leq f(u)$, questo indica che $f(u)$ è un upper bound dell'insieme P_1 (perché $x \leq f(x) \leq f(u)$). Ma u è il least upper bound quindi $u \leq f(u) \Rightarrow u \in P_1$.

Dato che $u \in P_1$ per monotonia di f si ha che $f(u) \leq f(f(u)) \Rightarrow f(u) \in P_1$, quindi $f(u) \leq u$ Allora:

- $u \leq f(u)$
- $f(u) \leq u$

$\Rightarrow u = f(u) = \vee P_1$ Siccome ogni fixed point appartiene all'insieme P_1 e $u = f(u)$ è il *lub* di tale insieme, allora $f(u)$ è il lub per tutti i fixed point e quindi è il greatest fixed point, ed appartiene all'insieme.

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

E' vero che $\forall x \in P_2 x \geq f(x)$ e per monotonia di f: $f(x) \geq f(f(x)) \Rightarrow f(x) \in P_2$.

Sia $g = \wedge P_2$ allora $g \leq x.\forall x \in P_2$. Per monotonia di f è vero che $\forall x \in P_2.f(g) \leq f(x)$ ovvero $f(g)$ è un lower bound di P_2.

g è il greatest lower bound di P_2 quindi $g \geq f(g)$, allora $g \in P_2$

Per monotonia di f $f(g) \geq f(f(g)) \Rightarrow f(g) \in P_2$ e quindi $g \leq f(g)$ in quanto g è greatest lower bound di P_2. Quindi:

- $g \geq f(g)$
- $f(g) \geq g$

$\Rightarrow g = f(g) = \wedge P_2$. g è chiaramente un fixed point, e siccome tutti i fixed point appartengono a P_2 e $f(g)$ è il greatest lower bound di $P_2 \Rightarrow f(g)$ è il least fixed point, ed appartiene a L.

Punto 3 Devo dimostrare che per ogni sottoinsieme di P esistono *lub* e *glb* e cha appartengono a P.

Sia $S \subseteq P$ e $s = \vee S$ (least upper bound di S), dimostro che esiste un elemento di P che è maggiore di tutti gli elementi di S, e che tale elemento è il più piccolo elemento di P (comunque più grande di S).

Definisco $U = \{x \in P | s \leq x\}$ ovvero l'insieme degli elementi più grandi di s in P (upper closure). U è quindi l'intervallo degli elementi da s al Top element di L: $U = [s....\top]$. Si ha che $s \in U$.

Ora dimostro che U è chiuso rispetto a f, ovvero:

Definizione di chiusura sia $f : S \to T$, e $S' \subseteq S$, allora si dice che S' è chiuso rispetto ad f se e solo se: $f[S'] \subseteq S'$, dove $f[S']$ è l'immagine di f in S.

Quindi voglio dimostrare che $f[U] \subseteq U$. Dimostro che:

a $s \leq f(s)$

b $\forall x \in U$ $s \leq f(x)$

a $\forall e \in S$ vale che $e \leq s$ per definizione di lub. Dato che S è un sottoinsieme dei punti fissi vale che $e = f(e)$ e per monotonia di f vale che $f(e) \leq f(s) \Rightarrow \forall e \in S.e \leq f(s)$, ovvero $f(s)$ è un upper bound di S, ma per definizione di least upper bound si ha che $s \leq f(s)$.

b $\forall x \in U \; s \leq x$ per definizione di U. Per monotonia di f: $f(s) \leq f(x)$, per **a** $s \leq f(s) \Rightarrow s \leq f(x) \forall x \in U$.

Per **a** e **b** $\Rightarrow \forall x \in U \; f(x) \in U$. Ovvero U è chiuso rispetto ad f.

Siccome $f : U \to U$ e U è un reticolo completo in quanto intervallo di un reticolo completo (L), e per **Punto 1** e **Punto 2** vale che $f : U \to U$ con U reticolo completo ha lub e glb in U $\Rightarrow$ f ha lub e glb in U e lub=greatest fixed point e glb=least fixed point di f in U.

Siccome $s \leq x \forall x \in U$ allora s è il greatest lower bound di U, quindi s = least fixed point di f in U. Allora S ha lub in F perchè il lub di $S = s =$ least fixed point di f in U e quindi $\in F$.

Analogamente i può dimostrare che S ha glb in F, e siccome questo vale $\forall S \subseteq P \Rightarrow P$ è un reticolo completo

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 $(P, Q) \in R \Rightarrow (P, Q) \in F(R)$, 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 $\leq$ 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).