Reducció de l'equivalència inicial visible a teoremes inductius

Vicent-Ramon Palasí Lallana

Report LSI–96–39–R

Reducció de l'equivalència inicial visible a teoremes inductius.

Vicent-Ramon Palasí Lallana*
Departament de Llenguatges i Sistemes Informàtics
Universitat Politècnica de Catalunya
e-mail: vicent@goliat.upc.es

Abstract

Es demostra que la comprovació de l'equivalència inicial visible de dues especificacions algebraiques visibles es pot reduir a la demostració de certs teoremes inductius sobre una certa àlgebra inicial.

1 Introducció

A [Pal95] es va demostrar que determinar si dues especificacions són equivalents en comportament (suposant semàntica inicial) es pot reduir a comprovar si es compleixen uns certs teoremes inductius en una àlgebra inicial donada. És més: es va veure que tant aquesta àlgebra inicial com els teoremes inductius es poden construir algorísmicament a partir de les dades inicials (les dues especificacions l'equivalència de les quals volem determinar). Així obteníem un algorisme per resoldre el problema de l'equivalència de comportament entre dues especificacions.

A [Pal96a] es va definir una nova semàntica, anomenada "inicial visible" basant-se en la semàntica de comportament. La semàntica inicial visible té les característiques adients per tractar el problema de la correcció d'un programa respecte a una especificació algebraica. De fet, a [Pal96b] es descriu un sistema automàtic de verificació de programes respecte una especificació algebraica, basant-se en la semàntica inicial visible.

Al present report, es demostra que la comprovació de l'equivalència inicial visible es pot reduir a la deducció de teoremes inductius, permetent que el sistema descrit a [Pal96b] sigui possible[1]. La demostració que en fem segueix les línies de la que es troba a [Pal95] sobre la semàntica de comportament. De fet, el nom dels diversos apartats del present report són els mateixos. A més, tan sols s'han inclòs les proves que són diferents (ni que

[1] De fet, per dir-ho amb paraules de [Pal96], el que es fa aquí és demostrar la correcció de l'algorisme β

sigui lleugerament) a les que es troben a [Pal95].

Tampoc es fa una descripció de les idees intuïtives que sotgen darrere de la demostració formal. Es deixa aquesta feina per al futur. Mentrestant, el lector interessat pot deduir-les fàcilment a partir de [Pal95], [Pal96a] i el present report.

Per acabar, una qüestió de notació. Quan, en aquest report usem propietats enunciades o demostrades en [Pal95] o [Pal96a], usarem la notació [Pal95].X o [Pal96a].X, on X és el número que la propietat tenia al report original.

2 V-reunions.

En aquest apartat, s'introdueix el concepte de reunió visible (a partir d'ara, V-reunions). Intuïtivament, una V-reunió de dues especificacions SP_1 i SP_2 és aquella especificació SP_3 l'àlgebra inicial de la qual conté tota la informació que tenen les àlgebres inicials de SP_1 i SP_2 per separat.

De fet, la diferència entre T-Reunions i V-Reunions rau en les equacions d'E_{new}. Mentre que, a les T-Reunions, les operacions $trans_s$ estaven definides sobre tots els símbols de funció possibles, aquí les operacions $trans_s$ només estan definides sobre els símbols *observables.*

La raó d'aquesta diferència és que, mentre que les T-Reunions s'aplicaven a la semàntica de comportament, les V-Reunions s'apliquen a la semàntica visible. Aquesta darrera té un nivell d'observabilitat més que la primera (el que distingeix entre gèneres i operacions observables i no observables) i això s'ha de reflectir en la definició de V-reunió.

Dit amb unes altres paraules, la T-reunió és un cas especial de la V-reunió quan $\Sigma_{Obs} = \Sigma_{All}$ (quan tots els gèneres i operacions són observables).

Definició 1. Siguin $SP_1 = (Vis, \Sigma_{Obs}, (\Sigma_{All})_1, E_1)$ i $SP_2 = (Vis, \Sigma_{Obs}, (\Sigma_{All})_2, E_2)$ dues especificacions visibles amb la mateixa signatura observable.

Sigui una especificació $SP_4 = (Vis_4, (\Sigma_{Obs})_4, (\Sigma_{All})_4, E_4)$, tal que SP_4 és un T-Renomenament de SP_2 via les bijeccions de T-renomenament θ i ϕ.

Diem que una especificació simple $SP_3 = (\Sigma_3, E_3)$ és una V-reunió de SP_1 i SP_2 via SP_4 si:

- $sorts(\Sigma_3) = sorts((\Sigma_{All})_1) \cup (sorts(\Sigma_{All})_4) \cup \gamma$ on $\gamma \notin (sorts((\Sigma_{All})_1) \cup sorts((\Sigma_{All})_4))$.
- $opns(\Sigma_3) = opns((\Sigma_{All})_1) \cup (opns(\Sigma_{All})_4) \cup F_{new}$ on F_{new} conté el següents símbols de funció:

  - $yes : \longrightarrow \gamma$
  - $plus : \gamma \times \gamma \longrightarrow \gamma$
  - Per a tot $s \in sorts(\Sigma_{Obs})$
    $trans_s : s \times \theta(s) \longrightarrow \gamma$

  on $yes, plus, trans \notin (opns((\Sigma_{All})_1) \cup opns((\Sigma_{All})_4))$

- $E_3 = E_1 \cup E_4 \cup E_{new}$ on E_{new} conté les següents equacions:

  - $plus(yes, yes) = yes$
  - $\forall s \in sorts(\Sigma_{Obs}) \quad \forall \sigma \in opns(\Sigma_{Obs})_{\lambda,s}$
    $trans_s(\sigma, \phi(\sigma)) = yes$
  - $\forall w1, .., wn, s \in sorts(\Sigma_{Obs}) \quad \forall \sigma \in opns(\Sigma_{Obs})_{w1..wn,s}$
    $trans_s(\sigma(t_1, t_2, ..., t_n), \phi(\sigma)(u_1, u_2, ..., u_n)) =$
    $plus(trans_{w_1}(t_1, u_1), plus(trans_{w_2}(t_2, u_2), ..., trans_{w_n}(t_n, u_n)...))$

  on $E_{new} \cap (E_1 \cup E_4) = \varnothing$

Les bijeccions θ i ϕ s'anomenen bijeccions de V-reunió.

Observacions

- En aquesta definició s'han utilitzat els noms $\gamma, yes, plus$ i $trans$ per significar els nou gènere i les noves funcions que s'introdueixen en una V-reunió. Pot haver-hi un petit problema si les especificacions originals ja feien ús d'aquests noms (ja que, com s'ha dit, $\gamma \notin S$ i $yes, plus, trans \notin (F \cup F_3)$) . Aquesta col.lisió de noms s'evita fàcilment utilitzant uns altres noms per a $\gamma, yes, plus$ i $trans$.

- Es pot veure fàcilment que l'algorisme que crea una V-reunió a partir de dues especificacions preexistents té una complexitat lineal respecte a l'entrada.

Sobre les V-reunions tal com les hem definides, podem enunciar el següent lema:

Lema 2. Sigui $SP_3 = SP_1 \uplus SP_2$ *via* SP_4. Es compleixen les següents afirmacions:

- $\forall t, u \in T_{\Sigma_{SP_1}}, \quad t \equiv_{SP_1} u$ si i només si $t \equiv_{SP_3} u$.

- $\forall t, u \in T_{\Sigma_{SP_4}}, \quad t \equiv_{SP_4} u$ si i només si $t \equiv_{SP_3} u$.

Prova És la mateixa que la del teorema [Pal95].46, que és el mateix teorema que aquest però enunciat sobre T-reunions. Per als propòsits d'aquesta prova, la diferència entre T-reunions i V-reunions no és rellevant. □

3 Raó de l'existència d'E_{new}

3.1 Implicació cap a la dreta

Per demostrar l'implicació cap a la dreta, ens ajudarem amb el concepte de termes V-I.

Definició 3 Sigui $SP_3 = SP_1 \uplus SP_2$ *via* SP_4, tal com estan definits al teorema 17. Sigui $l \in T_{\Sigma_{SP_3}}$. Direm que l és V-I si conté un subterme $trans_m(s,t)$ (amb $m \in$ S) tal que $\forall\, w \in T_{\Sigma_{Obs}}$ es compleix que, o bé, *no* $w \equiv_{SP_3} s$ o bé *no* $\phi^*(w) \equiv_{SP_3} t$

Dit d'una altra manera, un terme l no és V-I, si per a tots els seus subtermes de la forma $trans_m(s,t)$ (amb $m \in$ S), $\exists\, w \in T_{\Sigma_{Obs}}$ tal que $w \equiv_{SP_3} s$ i $\phi^*(w) \equiv_{SP_3} t$

Observació. Per augmentar la claredat de lectura, s'ha decidit que d'ara en endavant es notarà $trans(s,t)$ per expressar $trans_m(s,t)$, perquè el subíndex de trans és fàcilment deduïble del context (ja que m és el gènere que tenen s i t).

Sublema 4 Sigui $SP_3 = SP_1 \uplus SP_2$ *via* SP_4, tal com estan definits al teorema 17. Sigui $l \in T_{\Sigma_{SP_3}}$ un terme V-I i sigui u el resultat d'aplicar-li una equació $e \in E_3$ a l. Llavors u és V-I.

Prova. Com que l és V-I, hi haurà un subterme $trans(s,t)$ tal que $\forall\, w \in T_{\Sigma_{Obs}}$ es compleix que, o bé, *no* $w \equiv_{SP_3} s$ o bé *no* $\phi^*(w) \equiv_{SP_3} t$.

Distingim els següents cassos:

- Si e s'aplica en qualsevol subterme que no sigui $trans(s,t)$, u conservarà el mateix subterme $trans(s,t)$ i, per tant, u també serà V-I.
- Si e s'aplica sobre $trans(s,t)$ es poden donar els següents tres subcassos:
  - S'aplica sobre t. Llavors u contindrà un subterme de la forma $trans(s,t')$ on $t' \equiv_{SP_3} t$. Com que l és V-I, per a cada w que pertanyi a $T_{\Sigma_{Obs}}$ ha de passar una de les dues condicions següents:
    * *no* $w \equiv_{SP_3} s$.
    * *no* $\phi^*(w) \equiv_{SP_3} t$. Si es complís que $\phi^*(w) \equiv_{SP_3} t'$, llavors, com que $t' \equiv_{SP_3} t$, es compliria $\phi^*(w) \equiv_{SP_3} t$ per transitivitat. Com que això és absurd, queda demostrat que *no* $\phi^*(w) \equiv_{SP_3} t'$

    És a dir, u és V-I, ja que conté un subterme de la forma $trans(s,t')$ tal que $\forall\, w \in T_{\Sigma_{Obs}}$ es compleix que, o bé, *no* $w \equiv_{SP_3} s$ o bé *no* $\phi^*(w) \equiv_{SP_3} t'$.

– S'aplica sobre s. Llavors u contindrà un subterme de la forma $trans(s', t)$ on $s' \equiv_{SP_3} s$. Com que l és V-I, per a cada w que pertanyi a $T_{\Sigma_{Obs}}$ ha de passar una de les dues condicions següents:

  * $no \quad w \equiv_{SP_3} s$. Si es complís que $w \equiv_{SP_3} s'$, llavors, com que $s' \equiv_{SP_3} s$, es compliria $w \equiv_{SP_3} s$ per transitivitat. Com que això és absurd, queda demostrat que $no \quad w \equiv_{SP_3} s'$
  * $no \quad \phi^*(w) \equiv_{SP_3} t$.

  És a dir, u és V-I, ja que conté un subterme de la forma $trans(s', t)$ tal que $\forall\, w \in T_{\Sigma_{Obs}}$ es compleix que, o bé, $no \quad w \equiv_{SP_3} s'$ o bé $no \quad \phi^*(w) \equiv_{SP_3} t$.

– S'aplica sobre el subterme complet $trans(s, t)$. Com que el subterme comença per *trans*, només dues equacions poden aplicar-se.

  * $trans(\sigma, \phi(\sigma)) = yes$ Aquesta és impossible que s'apliqui, ja que pressuposaria que $\exists\, w \in T_{\Sigma_{Obs}}$ tal que $w \equiv_{SP_3} s$ i que $\phi^*(w) \equiv_{SP_3} t$ (en aquest cas, $w = s = \sigma$). Ara bé, hem triat $trans(s, t)$ com aquell subterme de l tal que $no \ \exists\, w \in T_{\Sigma_{Obs}}$ que compleix $w \equiv_{SP_3} s$ i que $\phi^*(w) \equiv_{SP_3} t$. Per tant, aquest cas no es pot donar.

  * $trans(\sigma(s_1, ..., s_n), \phi(\sigma)(t_1, ..., t_n)) = plus(trans(s_1, t_1), plus(trans(s_2, t_2)... trans(s_n, t_n)...))$. Llavors el subterme de l sobre el qual s'aplica l'equació és de la forma $trans(\sigma(v^*(s_1), ..., v^*(s_n)), \phi(\sigma)(v^*(t_1), ..., v^*(t_n))$ i el subterme de u resultant és de la forma $plus(trans(v^*(s_1), v^*(t_1)), plus(trans(v^*(s_2), v^*(t_2))... trans(v^*(s_n), v^*(t_n))...))$

    Suposem que, per a tot i, $\exists\, w_i \in T_{\Sigma_{Obs}}$ tal que $w_i \equiv_{SP_3} v^*(s_i)$ i $\phi^*(w_i) \equiv_{SP_3} v^*(t_i)$. Llavors, resulta que $\sigma(w_1, ..., w_n) \equiv_{SP_3} \sigma(v^*(s_1), ..., v^*(s_n))$ i $\phi(\sigma(w_1, ..., w_n)) = \phi(\sigma)(\phi^*(w_1), ..., \phi^*(w_n)) \equiv_{SP_3} \phi(\sigma)(v^*(t_1), ..., v^*(t_n))$. És a dir, si fem que w sigui $\sigma(w_1, ..., w_n)$, llavors $\exists\, w \in T_{\Sigma_{Obs}}$ tal que $w \equiv_{SP_3} s$ i $\phi^*(w) \equiv_{SP_3} t$. Però això és absurd, ja que havíem triat el terme trans(s,t) com aquell que complia que no $\exists\, w$ tal que $w \equiv_{SP_3} s$ i $\phi^*(w) \equiv_{SP_3} t$.

    Per tant, concloem que existeix un i tal que, o bé $no \quad w_i \equiv_{SP_3} v^*(s_i)$ o bé $no \quad \phi^*(w_i) \equiv_{SP_3} v^*(t_i)$. Ara bé, com que $trans(v^*(s_i), v^*(t_i))$ és un subterme de u, resulta que u és V-I, que és el que volíem demostrar.□

Sublema 5 Sigui $SP_3 = SP_1 \uplus SP_2$ *via* SP_4, tal com estan definits al teorema 17. Sigui $l \in T_{\Sigma_{SP_3}}$ un terme i sigui u el resultat d'aplicar-li una equació $e \in E_3$ a t. Llavors si l no és V-I, u tampoc ho és.

Prova. Ho farem per reducció a l'absurd. Suposem que l no és V-I i u sí que ho és. Per tant, quan apliquem l'equació e hem d'introduïr un subterme $trans(s, t)$ tal que

$\forall\, w \in T_{\Sigma_{Obs}}$ es compleix que, o bé, *no* $w \equiv_{SP_3} s$ o bé *no* $\phi^*(w) \equiv_{SP_3} t$. Però només hi han dues equacions que poden introduïr un subterme *trans*:

1. $trans(\sigma, \phi(\sigma)) = yes$, en sentit invers. Si s'aplica aquesta equació, fent que w sigui σ, es compleix que $\exists\, w \in T_{\Sigma_{Obs}}$ tal que $w \equiv_{SP_3} s$ i, a més, $\phi^*(w) \equiv_{SP_3} t$. És a dir, el subterme introduït no compleix les condicions que havia de complir i, per tant, u no és V-I.

2. $trans(\sigma(s_1, ..., s_n), \phi(\sigma)(t_1, ..., t_n)) = plus(trans(s_1, t_1), plus(trans(s_2, t_2)... \, trans(s_n, t_n)...))$, en sentit invers. Llavors el subterme que introdueix la equació és de la forma $trans(\sigma(v^*(s_1), \, ..., v^*(s_n)), \phi(\sigma)(v^*(t_1), ..., v^*(t_n))$ i el subterme corresponent de l és de la forma
$plus(trans(v^*(s_1), v^*(t_1)), plus(trans(v^*(s_2), v^*(t_2))... trans(v^*(s_n), v^*(t_n))...))$

   Ara bé, l no és V-I És a dir, per a tots els i, $\exists\, w_i \in T_{\Sigma_{Obs}}$ tal que $w_i \equiv_{SP_3} v^*(s_i)$ i $\phi^*(w_i) \equiv_{SP_3} v^*(t_i)$. Llavors, tenim que, si fem que w sigui $\sigma(w_1, ..., w_n)$ es compleix que $\exists\, w \in T_{\Sigma_{Obs}}$ tal que $w \equiv_{SP_3} \sigma(v^*(s_1), ..., v^*(s_n))$ i $\phi^*(w) \equiv_{SP_3} \phi(\sigma)(v^*(t_1), ..., v^*(t_n))$. Per tant u no seria V-I. □

Corol.lari 6 Sigui $SP_3 = SP_1 \uplus SP_2$ *via* SP_4, tal com estan definits al teorema 17. Sigui $l \in T_{\Sigma_{SP_3}}$ i sigui u el resultat d'aplicar-li una equació $e \in E_3$ a t. Llavors, l és V-I si i només si u és V-I.

Prova. És la conseqüència directa del sublema 4 i del contrarrecíproc del sublema 5. □

Sublema 7 Sigui $SP_3 = SP_1 \uplus SP_2$ *via* SP_4, tal com estan definits al teorema 17. Sigui $t, u \in T_{\Sigma_{SP_3}}$ tal que $t \equiv_{SP_3} u$. Llavors es compleix que t és V-I si i només si u és V-I.

Prova. Si $t \equiv_{SP_3} u$, per definició de $\equiv_{SP_3}$, pot passar un d'aquests quatre casos:

1. Aquest cas es produeix quan $t = u$. El sublema queda reduït en aquest cas a "t és V-I si i només si t és V-I", que és trivial.

2. En aquest segon cas, $t \equiv_{SP_3} u$ perquè $u \equiv_{SP_3} t$. Com que la demostració d'aquesta darrera relació de congrüència és més curta (en passos) que la primera, podem aplicar-hi la hipòtesi d'inducció. Així obtenim que "u és V-I si i només si t és V-I". Aplicant la simetria de la doble implicació ja tenim el que buscàvem

3. En aquest tercer cas, $t \equiv_{SP_3} u$ perquè $t \equiv_{SP_3} v$ i $v \equiv_{SP_3} u$. Com que les subdemostracions de $t \equiv_{SP_3} v$ i $v \equiv_{SP_3} u$ són més curtes (en passos) que la demostració inicial, podem aplicar la hipòtesi d'inducció. Tenim, doncs, que "t és V-I si i només si v és V-I" i "v és V-I si i només si u és V-I". Aplicant la transitivitat de la doble implicació ja tenim el que buscàvem.

4. En aquest quart cas, $t \equiv_{SP_3} u$ perquè u resulta d'aplicar una equació e a t. Però, pel corol.lari 6, obtenim que, si passa això "t és V-I si i només si u és V-I". $\square$

Lema 8. Sigui $SP_3 = SP_1 \uplus SP_2$ *via* SP_4, tal com estan definits al teorema 17. Siguin $s, t \in T_{\Sigma_{SP_3}}$. Es compleix que:

$$trans(s,t) \equiv_{SP_3} yes \text{ implica que } \exists\, w \in T_{\Sigma_{Obs}} \text{ tal que } w \equiv_{SP_3} s \text{ i } \phi^*(w) \equiv_{SP_3} t.$$

Prova. Suposem que $trans(s,t) \equiv_{SP_3} yes$. Com que yes no és V-I (ja que no conté cap subterme de la forma $trans(s',t')$), llavors $trans(s,t)$ tampoc no ho serà, pel sublema 7. Però, com que aquest darrer subterme no és V-I, , per definició 3, ha d'existir un $w \in T_{\Sigma_{Obs}}$ tal que $w \equiv_{SP_3} s$ i $\phi^*(w) \equiv_{SP_3} t$. $\square$

3.2 Implicació cap a l'esquerra.

Ara demostrem la implicació cap a l'esquerra de l'afirmació que enunciàvem al començament de l'apartat.

Sublema 9 Sigui $SP_3 = SP_1 \uplus SP_2$ *via* SP_4, tal com estan definits al teorema 17. Llavors es compleix:

$$plus(yes, plus(yes, ..., yes)...) \equiv_{SP_3} yes.$$

Prova. La prova és la mateixa que la del sublema 9. Als efectes d'aquesta prova, les diferències entre T-reunions i V-reunions no són rellevants. $\square$

Lema 10. Sigui $SP_3 = SP_1 \uplus SP_2$ *via* SP_4, tal com estan definits al teorema 17. Sigui $t \in T_{\Sigma_{Obs}}$. Es compleix que

$$u \equiv_{SP_3} \phi^*(t) \text{ implica } trans(t,u) \equiv_{SP_3} yes$$

Prova. Demostrem-ho per inducció estructural sobre t. Anomeno F_{Obs} a $opns(\Sigma_{Obs})$.

<u>Base de la inducció.</u> És el cas en què $t \in (F_{Obs})_{\lambda,s}$, llavors $\phi^*(t) = \phi(t)$ i, per tant, $u \equiv_{SP_3} \phi(t)$. Però, com que existeix l'equació $trans(t, \phi(t)) = yes$ (per a qualsevol t que pertanyi a F_{Obs}) , trivialment, $trans(t, \phi(t)) \equiv_{SP_3} yes$. Com que $u \equiv_{SP_3} \phi(t)$ i $\equiv_{SP_3}$ és una congrüència, llavors tenim que $trans(t,u) \equiv_{SP_3} yes$.

<u>Pas de la inducció.</u> És el cas en què t és de la forma $\sigma(t_1, ..., t_n)$, on $\sigma \in F_{Obs}$; $t_1, ..., t_n \in T_{\Sigma_{Obs}}$. Conseqüentment, $\phi^*(t)$ és de la forma $\phi(\sigma)(\phi^*(t_1), ..., \phi^*(t_n))$. Per tant, $trans(t, \phi^*(t))$ és[2] el següent terme $plus(trans(t_1, \phi^*(t_1)), plus(trans(t_2, \phi^*(t_2))...trans(t_n, \phi^*(t_n))...))$. Com

[2]Aplicant l'equació

$$trans(\sigma(x_1, ..., x_n), \phi(\sigma)(y_1, ..., y_n)) = plus(trans(x_1, y_1), plus(trans(x_2, y_2)...trans(x_n, y_n)...))$$

que $t_1, ..., t_n \in T_{\Sigma_{Obs}}$, podem aplicar la hipòtesi d'inducció i obtenim que, per a tots els i, es compleix que $trans(t_i, \phi^*(t_i)) \equiv_{SP_3} yes$. Llavors $trans(t, \phi^*(t)) \equiv_{SP_3} plus(yes, plus(yes, ..., yes)...)$. Pel sublema 9, $trans(t, \phi^*(t)) \equiv_{SP_3} yes$. I com que $u \equiv \phi^*(t)$, llavors $trans(t, u) \equiv_{SP_3} yes$.
□

4 Demostració de la robustesa

En aquest apartat, demostrem la robustesa del nostre mètode. És a dir, demostrem que si es compleixen uns certs teoremes inductius en l'àlgebra inicial de SP_3 llavors SP_1 i SP_2 són inicialment visiblement equivalents. Aquesta propietat és enunciada en el teorema 12.

4.1 Propietats útils

Però primer demostrem algunes propietats que ens serviran per a demostrar el teorema 12.

Lema 11 L'afirmació

$$\begin{array}{l} \forall s \in Vis,\ \forall s_1, s_2 \in (T_{\Sigma_{SP_3}})_s;\ t_1, t_2 \in (T_{\Sigma_{SP_3}})_{\theta(s)} \text{ es compleix que} \\ (trans_s(s_1, t_1) \equiv_{SP_3} yes \ \wedge\ trans_s(s_1, t_2) \equiv_{SP_3} yes \text{ implica } t_1 \equiv_{SP_3} t_2) \ \wedge \\ (trans_s(s_1, t_1) \equiv_{SP_3} yes \ \wedge\ trans_s(s_2, t_1) \equiv_{SP_3} yes \text{ implica } s_1 \equiv_{SP_3} s_2) \end{array}$$

implica l'afirmació

$$\begin{array}{l} \forall s \in Vis,\ \forall s_1, s_2 \in (T_{\Sigma_{SP_3}})_s;\ t_1, t_2 \in (T_{\Sigma_{SP_3}})_{\theta(s)} \text{ es compleix que} \\ (trans_s(s_1, t_1) \equiv_{SP_3} yes \ \wedge\ trans_s(s_2, t_2) \equiv_{SP_3} yes \ \wedge\ s_1 \equiv_{SP_3} s_2 \text{ implica } t_1 \equiv_{SP_3} t_2) \ \wedge \\ (trans_s(s_1, t_1) \equiv_{SP_3} yes \ \wedge\ trans_s(s_2, t_2) \equiv_{SP_3} yes \ \wedge\ t_1 \equiv_{SP_3} t_2 \text{ implica } s_1 \equiv_{SP_3} s_2) \end{array}$$

Prova. Abans de tot, demostrem el següent sublema:

$$\begin{array}{l} \forall s \in Vis,\ \forall s_1, s_2 \in (T_{\Sigma_{SP_3}})_s;\ t_2 \in (T_{\Sigma_{SP_3}})_{\theta(s)} \text{ es compleix que} \\ s_1 \equiv_{SP_3} s_2 \ \wedge\ trans_s(s_2, t_2) \equiv_{SP_3} yes \text{ implica } trans(s_1, t_2) \equiv_{SP_3} yes \end{array}$$

Suposem que la premissa es compleix. Com que es compleix que $s_1 \equiv_{SP_3} s_2$ (per la premissa) i, a més, $t_2 \equiv_{SP_3} t_2$, per la propietat de congrüència s'ha de complir que

$$trans_s(s_1, t_2) \equiv_{SP_3} trans_s(s_2, t_2)$$

I, com que segons la premissa $trans_s(s_2, t_2) \equiv_{SP_3} yes$, obtenim:

$$trans_s(s_1, t_2) \equiv_{SP_3} yes$$

I el sublema queda demostrat.

Demostrem ara el lema, que és una implicació. Per fer-ho, suposem que la primera afirmació enunciada en aquesta implicació es compleix i hem de demostrar que la segona també ho fa. De fet, només demostrarem que es compleix el primer conjuntand de la segona afirmació (el segon conjuntand es demostra anàlogament).

Com que el primer conjuntand de la segona afirmació és, de nou, una implicació, la forma de demostrar-lo és suposar que la premisa és certa i demostrar que si es així la conclusió també ho és.

Per tant, suposem que és cert

$$trans_s(s_1, t_1) \equiv_{SP_3} yes \ \wedge \ trans_s(s_2, t_2) \equiv_{SP_3} yes \ \wedge \ s_1 \equiv_{SP_3} s_2$$

Pel sublema que acaben de demostrar això implica:

$$trans_s(s_1, t_1) \equiv_{SP_3} yes \ \wedge \ trans_s(s_1, t_2) \equiv_{SP_3} yes$$

I, com que la primera afirmació es compleix, això implica:

$$t_1 \equiv_{SP_3} t_2$$

Per tant, hem demostrat el primer conjuntand de la segona afirmació. El segon conjuntand es demostra anàlogament. Així demostrem que la segona afirmació es compleix si ho fa la primera. En altres paraules, hem demostrat el lema. □

4.2 Nucli de la demostració de la robustesa

Demostrem ara el teorema que enuncia la robustesa del nostre mètode.

Teorema 12 Siguin dues especificacions $SP_1 = (\Sigma_1, E_1)$ i $SP_2 = (\Sigma_2, E_2)$, on $\Sigma_1 = (Vis, \Sigma_{Obs}, (\Sigma_{All})_1)$ i $\Sigma_2 = (Vis, \Sigma_{Obs}, (\Sigma_{All})_2)$ són dues signatures visibles. Sigui SP_3, la V-reunió de SP_1 i SP_2 via qualsevol especificació $SP_4 = (Vis_4, \Sigma_{Obs_4}, (\Sigma_{All})_4, E_4)$. Llavors, l'afirmació

$$\begin{array}{l}\forall\, s \in Vis,\ \forall\, x_1, x_2 \in vars(s);\ y_1, y_2 \in vars(\theta(s)) \text{ es compleix que} \\ (T_{SP_3} \models trans_s(x_1, y_1) = yes \ \&\ trans_s(x_1, y_2) = yes \ \Rightarrow y_1 = y_2) \wedge \\ (T_{SP_3} \models trans_s(x_1, y_1) = yes \ \&\ trans_s(x_2, y_1) = yes \ \Rightarrow x_1 = x_2)\end{array}$$

implica l'afirmació

SP_1 i SP_2 són inicialment visiblement equivalents.

Prova. Comencem amb la primera afirmació

$$\forall s \in Vis,\ \forall x_1, x_2 \in vars(s);\ y_1, y_2 \in vars(\theta(s)) \text{ es compleix que}$$
$$(T_{SP_3} \models trans_s(x_1, y_1) = yes \ \&\ trans_s(x_1, y_2) = yes \ \Rightarrow y_1 = y_2) \wedge$$
$$(T_{SP_3} \models trans_s(x_1, y_1) = yes \ \&\ trans_s(x_2, y_1) = yes \ \Rightarrow x_1 = x_2)$$

Per definició de satisfacció d'una equació en una àlgebra donada, aquesta afirmació és equivalent a:

$$\forall s \in Vis,\ \forall x_1, x_2 \in vars(s);\ y_1, y_2 \in vars(\theta(s)),\ \forall v : X \longrightarrow T_{\Sigma_{SP_3}} \text{ es compleix que}$$
$$(v^*(trans_s(x_1, y_1)) \equiv_{SP_3} v^*(yes) \ \wedge\ v^*(trans_s(x_1, y_2)) \equiv_{SP_3} v^*(yes) \text{ implica } v^*(y_1) \equiv_{SP_3} v^*(y_2$$
$$\wedge$$
$$(v^*(trans_s(x_1, y_1)) \equiv_{SP_3} v^*(yes) \ \wedge\ v^*(trans_s(x_2, y_1)) \equiv_{SP_3} v^*(yes) \text{ implica } v^*(x_1) \equiv_{SP_3} v^*(x_2$$

Però, com que les úniques variables que hi ha a l'afirmació són x_1, x_2, y_1 i y_2, podem aplicar la definició de v^* i obtenim:

$$\forall s \in Vis,\ \forall s_1, s_2 \in (T_{\Sigma_{SP_3}})_s;\ t_1, t_2 \in (T_{\Sigma_{SP_3}})_{\theta(s)} \text{ es compleix que}$$
$$(trans_s(s_1, t_1) \equiv_{SP_3} yes \ \wedge\ trans_s(s_1, t_2) \equiv_{SP_3} yes \ \text{ implica } t_1 \equiv_{SP_3} t_2) \ \wedge$$
$$(trans_s(s_1, t_1) \equiv_{SP_3} yes \ \wedge\ trans_s(s_2, t_1) \equiv_{SP_3} yes \ \text{ implica } s_1 \equiv_{SP_3} s_2)$$

Aplicant el lema 11, aquesta afirmació implica la següent:

$$\forall s \in Vis,\ \forall s_1, s_2 \in (T_{\Sigma_{SP_3}})_s;\ t_1, t_2 \in (T_{\Sigma_{SP_3}})_{\theta(s)} \text{ es compleix que}$$
$$(trans_s(s_1, t_1) \equiv_{SP_3} yes \ \wedge\ trans_s(s_2, t_2) \equiv_{SP_3} yes \ \wedge\ s_1 \equiv_{SP_3} s_2 \text{ implica } t_1 \equiv_{SP_3} t_2) \ \wedge$$
$$(trans_s(s_1, t_1) \equiv_{SP_3} yes \ \wedge\ trans_s(s_2, t_2) \equiv_{SP_3} yes \ \wedge\ t_1 \equiv_{SP_3} t_2 \text{ implica } s_1 \equiv_{SP_3} s_2)$$

Com que $\Sigma_{Obs} \subsetneq (\Sigma_{All})_1$ i $(\Sigma_{All})_1 \subset \Sigma_{SP_3}$, tenim que $T_{\Sigma_{Obs}} \subset T_{\Sigma_{SP_3}}$. Per tant, l'afirmació anterior implica la següent:

$$\forall s \in Vis,\ \forall s_1, s_2 \in (T_{\Sigma_{Obs}})_s;\ t_1, t_2 \in (T_{\Sigma_{SP_3}})_{\theta(s)} \text{ es compleix que}$$
$$(trans_s(s_1, t_1) \equiv_{SP_3} yes \ \wedge\ trans_s(s_2, t_2) \equiv_{SP_3} yes \ \wedge\ s_1 \equiv_{SP_3} s_2 \text{ implica } t_1 \equiv_{SP_3} t_2) \ \wedge$$
$$(trans_s(s_1, t_1) \equiv_{SP_3} yes \ \wedge\ trans_s(s_2, t_2) \equiv_{SP_3} yes \ \wedge\ t_1 \equiv_{SP_3} t_2 \text{ implica } s_1 \equiv_{SP_3} s_2)$$

Ara bé, sabem que $\Sigma_{Obs} \subsetneq (\Sigma_{All})_2$ i, per tant, $T_{\Sigma_{Obs}} \subsetneq T_{\Sigma_{SP_2}}$. Llavors, com que $s_1, s_2 \in (T_{\Sigma_{SP_2}})_s$, es compleix que $\phi^*(s_1), \phi^*(s_2) \in (T_{\Sigma_{SP_4}})_{\theta(s)}$, pel sublema [Pal95].38. Com que $T_{\Sigma_{SP_4}} \subset T_{\Sigma_{SP_3}}$, vol dir que $\phi^*(s_1), \phi^*(s_2) \in (T_{\Sigma_{SP_3}})_{\theta(s)}$. Per tant, com que la darrera afirmació es compleix per a tots els valors de t_i que pertanyin a $(T_{\Sigma_{SP_3}})_{\theta(s)}$, es complirà en particular quan $t_i = \phi^*(s_i)$:

$$\forall s \in Vis,\ \forall s_1, s_2 \in (T_{\Sigma_{Obs}})_s \text{ es compleix que}$$
$$(trans_s(s_1, \phi^*(s_1)) \equiv_{SP_3} yes \ \wedge\ trans_s(s_2, \phi^*(s_2)) \equiv_{SP_3} yes \ \wedge$$
$$s_1 \equiv_{SP_3} s_2 \text{ implica } \phi^*(s_1) \equiv_{SP_3} \phi^*(s_2) \ \wedge$$
$$(trans_s(s_1, \phi^*(s_1)) \equiv_{SP_3} yes \ \wedge\ trans_s(s_2, \phi^*(s_2)) \equiv_{SP_3} yes \ \wedge$$
$$\phi^*(s_1) \equiv_{SP_3} \phi^*(s_2) \text{ implica } s_1 \equiv_{SP_3} s_2)$$

Obtenim pel lema 10:

$\forall\, s \in Vis,\ \forall\, s_1, s_2 \in (T_{\Sigma_{Obs}})_s$ es compleix que
$(cert\ \wedge\ cert\ \wedge\ s_1 \equiv_{SP_3} s_2$ implica $\phi^*(s_1) \equiv_{SP_3} \phi^*(s_2))\ \wedge$
$(cert\ \wedge\ cert\ \wedge\ \phi^*(s_1) \equiv_{SP_3} \phi^*(s_2)$ implica $s_1 \equiv_{SP_3} s_2)$

Que, per les regles de la lògica, és equivalent a:

$\forall\, s \in Vis,\ \forall\, s_1, s_2 \in (T_{\Sigma_{Obs}})_s$ es compleix que
$(s_1 \equiv_{SP_3} s_2)$ si i només si $(\phi^*(s_1) \equiv_{SP_3} \phi^*(s_2))$

Per definició [Pal96a].18, això és equivalent a:

$\forall\, s_1, s_2 \in TVis_{\Sigma_1}$ es compleix que
$(s_1 \equiv_{SP_3} s_2)$ si i només si $(\phi^*(s_1) \equiv_{SP_3} \phi^*(s_2))$

Com que $TVis_{\Sigma_1} \subseteq T_{\Sigma_{SP_1}}$, llavors podem aplicar la primera part del lema 2 a la banda esquerra de la doble implicació. Si ho fem, obtenim que:

$\forall\, s_1, s_2 \in TVis_{\Sigma_1}$ es compleix que
$(s_1 \equiv_{SP_1} s_2)$ si i només si $(\phi^*(s_1) \equiv_{SP_3} \phi^*(s_2))$

Com que $TVis_{\Sigma_1} = TVis_{\Sigma_2}$, ja que les dues especificacions comparteixen la mateixa signatura observable, llavors $s_1, s_2 \in TVis_{\Sigma_2}$. Per tant, $s_1, s_2 \in T_{\Sigma_{SP_2}}$. Ara bé, com que $SP_4 \in T - Renam(SP_2)$, per la definició [Pal95].37, resulta que $\phi^*(s_1), \phi^*(s_2) \in T_{\Sigma_{SP_4}}$. Per tant, podem aplicar la segona part del lema 2 a la banda dreta de la doble implicació i el resultat és:

$\forall\, s_1, s_2 \in TVis_{\Sigma_1}$ es compleix que
$(s_1 \equiv_{SP_1} s_2)$ si i només si $(\phi^*(s_1) \equiv_{SP_4} \phi^*(s_2))$

Com que $SP_4 \in T - Renam(SP_2)$, aplicant el lema [Pal95].40:

$\forall\, s_1, s_2 \in TVis_{\Sigma_1}$ es compleix que
$(s_1 \equiv_{SP_1} s_2)$ si i només si $(s_1 \equiv_{SP_2} s_2)$

O, el que és el mateix:

$\forall\, s_1, s_2 \in TVis_{\Sigma_1}$ es compleix que
$(T_{SP_1} \models s_1 = s_2)$ si i només si $(T_{SP_2} \models s_1 = s_2)$

Pel lema [Pal96a].24, això és el mateix que dir

T_{SP_1} i T_{SP_2} són visiblement equivalents

És a dir, segons la definició [Pal96a].36,

SP_1 i SP_2 són inicialment visiblement equivalents

Que és el que volíem demostrar. $\square$

5 Demostració de la completesa

En aquest apartat, demostrem la completesa del nostre mètode. És a dir, demostrem que si SP_1 i SP_2 són inicialment visiblement equivalents llavors es compleixen uns certs teoremes inductius en l'àlgebra inicial de SP_3 . Aquesta propietat és enunciada en el teorema 16.

5.1 Propietats útils

Però primer demostrem algunes propietats que ens serviran per a demostrar el teorema 16.

Lema 13 L'afirmació

$\forall s \in Vis;\ \ \forall s_1, s_2 \in (T_{\Sigma_{Obs}})_s;\ t_1, t_2 \in (T_{\Sigma_{SP_3}})_{\theta(s)}$ es compleix que
$t_1 \equiv_{SP_3} \phi^*(s_1) \wedge t_2 \equiv_{SP_3} \phi^*(s_2)$ implica
$(s_1 \equiv_{SP_3} s_2)$ si i només si $(t_1 \equiv_{SP_3} t_2)$

implica l'afirmació

$\forall s \in Vis;\ \ \forall s_1, s_2 \in (T_{\Sigma_{SP_3}})_s;\ t_1, t_2 \in (T_{\Sigma_{SP_3}})_{\theta(s)}$ es compleix que
$trans_s(s_1, t_1) \equiv_{SP_3} yes \wedge trans_s(s_2, t_2) \equiv_{SP_3} yes$ implica
$(s_1 \equiv_{SP_3} s_2)$ si i només si $(t_1 \equiv_{SP_3} t_2)$

Prova. Suposem que es compleix la primera afirmació. Suposem que es compleix també que $trans_s(s_1, t_1) \equiv_{SP_3} yes \wedge trans_s(s_2, t_2) \equiv_{SP_3} yes$. Volem demostrar que es compleix que $(s_1 \equiv_{SP_3} s_2)$ si i només si $(t_1 \equiv_{SP_3} t_2)$.

Com que es compleix que $trans_s(s_1, t_1) \equiv_{SP_3} yes \wedge trans_s(s_2, t_2) \equiv_{SP_3} yes$, tenim pel lema 8, que $\exists\, w_1, w_2 \in T_{\Sigma_{Obs}}$ tal que $w_1 \equiv_{SP_3} s_1 \wedge \phi^*(w_1) \equiv_{SP_3} t_1$ $\wedge\ w_2 \equiv_{SP_3} s_2 \wedge \phi^*(w_2) \equiv_{SP_3} t_2$. D'una banda, com que $w_1 \equiv_{SP_3} s_1 \wedge w_2 \equiv_{SP_3} s_2$, es compleix que $(s_1 \equiv_{SP_3} s_2)$ si i només si $(w_1 \equiv_{SP_3} w_2)$.

D'altra banda, com que es compleix la primera afirmació i que $w_1, w_2 \in T_{\Sigma_{Obs}}$ i, a més, que $\phi^*(w_1) \equiv_{SP_3} t_1 \wedge \phi^*(w_2) \equiv_{SP_3} t_2$, podem aplicar la primera afirmació i obtenim $(w_1 \equiv_{SP_3} w_2)$ si i només si $(t_1 \equiv_{SP_3} t_2)$. Combinant aquesta doble implicació amb la que resulta del darrer paràgraf, tenim que: $(s_1 \equiv_{SP_3} s_2)$ si i només si $(t_1 \equiv_{SP_3} t_2)$. I això és el que volíem demostrar. □

Lema 14. L'afirmació

$\forall s_1, s_2 \in TVis_{\Sigma_1}$ es compleix que
$(s_1 \equiv_{SP_3} s_2)$ si i només si $(\phi^*(s_1) \equiv_{SP_3} \phi^*(s_2))$

implica l'afirmació:

$$\forall\, s_1, s_2 \in TVis_{\Sigma_1};\; t_1, t_2 \in T_{\Sigma_{SP_3}} \text{ es compleix que}$$
$$t_1 \equiv_{SP_3} \phi^*(s_1) \wedge t_2 \equiv_{SP_3} \phi^*(s_2) \text{ implica}$$
$$(s_1 \equiv_{SP_3} s_2) \text{ si i només si } (t_1 \equiv_{SP_3} t_2)$$

Prova. Suposem que es compleix la primera afirmació. Suposem que es compleix que $t_1 \equiv_{SP_3} \phi^*(s_1) \wedge t_2 \equiv_{SP_3} \phi^*(s_2)$. Volem veure que es compleix que $(s_1 \equiv_{SP_3} s_2)$ si i només si $(t_1 \equiv_{SP_3} t_2)$.

Com que es compleix que $t_1 \equiv_{SP_3} \phi^*(s_1) \wedge t_2 \equiv_{SP_3} \phi^*(s_2)$, tenim que $(t_1 \equiv_{SP_3} t_2)$ si i només si $(\phi^*(s_1) \equiv_{SP_3} \phi^*(s_2))$.

D'altra banda, com que es compleix la primera afirmació, tenim que $(s_1 \equiv_{SP_3} s_2)$ si i només si $(\phi^*(s_1) \equiv_{SP_3} \phi^*(s_2)$. Aplicant aquesta doble implicació a la que resulta en el paràgraf anterior, obtenim que $(s_1 \equiv_{SP_3} s_2)$ si i només si $(t_1 \equiv_{SP_3} t_2)$, que és el que volíem demostrar. □

Lema 15 L'afirmació

$$\forall\, s \in Vis,\; \forall\, s_1, s_2 \in (T_{\Sigma_{SP_3}})_s;\; t_1, t_2 \in (T_{\Sigma_{SP_3}})_{\theta(s)} \text{ es compleix que}$$
$$(trans_s(s_1, t_1) \equiv_{SP_3} yes \;\wedge\; trans_s(s_2, t_2) \equiv_{SP_3} yes \;\wedge\; s_1 \equiv_{SP_3} s_2 \text{ implica } t_1 \equiv_{SP_3} t_2) \;\wedge$$
$$(trans_s(s_1, t_1) \equiv_{SP_3} yes \;\wedge\; trans_s(s_2, t_2) \equiv_{SP_3} yes \;\wedge\; t_1 \equiv_{SP_3} t_2 \text{ implica } s_1 \equiv_{SP_3} s_2)$$

implica l'afirmació

$$\forall\, s \in Vis,\; \forall\, s_1, s_2 \in (T_{\Sigma_{SP_3}})_s;\; t_1, t_2 \in (T_{\Sigma_{SP_3}})_{\theta(s)} \text{ es compleix que}$$
$$(trans_s(s_1, t_1) \equiv_{SP_3} yes \;\wedge\; trans_s(s_1, t_2) \equiv_{SP_3} yes \text{ implica } t_1 \equiv_{SP_3} t_2) \;\wedge$$
$$(trans_s(s_1, t_1) \equiv_{SP_3} yes \;\wedge\; trans_s(s_2, t_1) \equiv_{SP_3} yes \text{ implica } s_1 \equiv_{SP_3} s_2)$$

Prova. Suposem la primera afirmació i hem de demostrar la segona. En concret, començarem per demostrar el primer conjuntand de la segona afirmació.

Com que aquest conjuntand és, de nou, una implicació, suposarem la premissa i hem de demostrar la conclusió. Suposem, doncs, que és certa la premissa.

$$trans_s(s_1, t_1) \equiv_{SP_3} yes \;\wedge\; trans_s(s_1, t_2) \equiv_{SP_3} yes$$

Això és equivalent a dir

$$trans_s(s_1, t_1) \equiv_{SP_3} yes \;\wedge\; trans_s(s_1, t_2) \equiv_{SP_3} yes \;\wedge\; s_1 \equiv_{SP_3} s_1)$$

Hem suposat que la primera afirmació es compleix. En concret es compleix la seva instància quan $s_1 = s_2$, és a dir, la implicació que diu que $(trans_s(s_1, t_1) \equiv_{SP_3} yes \;\wedge$

$trans_s(s_1, t_1) \equiv_{SP_3} yes \ \wedge \ s_1 \equiv_{SP_3} s_1$ implica $t_1 \equiv_{SP_3} t_2$). Aplicant aquesta instància, obtenim que l'afirmació anterior implica que :

$$t_1 \equiv_{SP_3} t_2$$

Per tant, resumint, ($trans_s(s_1, t_1) \equiv_{SP_3} yes \ \wedge \ trans_s(s_2, t_2) \equiv_{SP_3} yes$ implica $t_1 \equiv_{SP_3} t_2$) i el primer conjuntand de la segona afirmació queda demostrat. El segon conjuntand es demostra anàlogament (usant la instància de la primera afirmació en qué $t_1 = t_2$). $\square$

5.2 Nucli de la demostració de la completesa

Demostrem ara el teorema que enuncia la completesa del nostre mètode.

Teorema 16 Siguin dues especificacions $SP_1 = (\Sigma_1, E_1)$ i $SP_2 = (\Sigma_2, E_2)$, on $\Sigma_1 = (Vis, \Sigma_{Obs}, (\Sigma_{All})_1)$ i $\Sigma_2 = (Vis, \Sigma_{Obs}, (\Sigma_{All})_2)$ són dues signatures visibles. Sigui SP_3, la V-reunió de SP_1 i SP_2 via qualsevol especificació $SP_4 = (Vis_4, \Sigma_{Obs_4}, (\Sigma_{All})_4, E_4)$. Llavors, l'afirmació

SP_1 i SP_2 són inicialment visiblement equivalents

implica l'afirmació

$\forall s \in Vis, \ \forall x_1, x_2 \in vars(s); \ y_1, y_2 \in vars(\theta(s))$ es compleix que
$(T_{SP_3} \models trans_s(x_1, y_1) = yes \ \& \ trans_s(x_1, y_2) = yes \ \Rightarrow y_1 = y_2) \wedge$
$(T_{SP_3} \models trans_s(x_1, y_1) = yes \ \& \ trans_s(x_2, y_1) = yes \ \Rightarrow x_1 = x_2)$

Prova. Suposem que SP_1 i SP_2 són inicialment visiblement equivalents. Pel lema [Pal96a].36, això és el mateix que dir:

T_{SP_1} i T_{SP_2} són visiblement equivalents

És a dir, segons el lema [Pal96a].24,

$\forall s_1, s_2 \in TVis_{\Sigma_1}$ es compleix que
$(T_{SP_1} \models s_1 = s_2)$ si i només si $(T_{SP_2} \models s_1 = s_2)$

O, el que és el mateix:

$\forall s_1, s_2 \in TVis_{\Sigma_1}$ es compleix que
$(s_1 \equiv_{SP_1} s_2)$ si i només si $(s_1 \equiv_{SP_2} s_2)$

Com que $SP_4 \in T - Renam(SP_2)$, aplicant el lema [Pal95].40:

$\forall s_1, s_2 \in TVis_{\Sigma_1}$ es compleix que
$(s_1 \equiv_{SP_1} s_2)$ si i només si $(\phi^*(s_1) \equiv_{SP_4} \phi^*(s_2))$

Com que $TVis_{\Sigma_1} \subseteq T_{\Sigma_{SP_1}}$, llavors podem aplicar la primera part del lema 2 a la banda esquerra de la doble implicació. Si ho fem, obtenim que:

$\forall\, s_1, s_2 \in TVis_{\Sigma_1}$ es compleix que
$(s_1 \equiv_{SP_3} s_2)$ si i només si $(\phi^*(s_1) \equiv_{SP_4} \phi^*(s_2))$

Com que $TVis_{\Sigma_1} = TVis_{\Sigma_2}$, ja que les dues especificacions comparteixen la mateixa signatura observable, llavors $s_1, s_2 \in TVis_{\Sigma_2}$. Per tant, $s_1, s_2 \in T_{\Sigma_{SP_2}}$. Ara bé, com que $SP_4 \in T - Renam(SP_2)$, per la definició [Pal95].37, resulta que $\phi^*(s_1), \phi^*(s_2) \in T_{\Sigma_{SP_4}}$. Per tant, podem aplicar la segona part del lema 2 a la banda dreta de la doble implicació i el resultat és:

$\forall\, s_1, s_2 \in TVis_{\Sigma_1}$ es compleix que
$(s_1 \equiv_{SP_3} s_2)$ si i només si $(\phi^*(s_1) \equiv_{SP_3} \phi^*(s_2))$

Pel lema 14, això implica:

$\forall\, s_1, s_2 \in TVis_{\Sigma_1};\ t_1, t_2 \in T_{\Sigma_{SP_3}}$ es compleix que
$t_1 \equiv_{SP_3} \phi^*(s_1) \wedge t_2 \equiv_{SP_3} \phi^*(s_2)$ implica
$(s_1 \equiv_{SP_3} s_2)$ si i només si $(t_1 \equiv_{SP_3} t_2)$

Per definició [Pal96a].18, això és el mateix que dir:

$\forall\, s \in Vis;\quad \forall\, s_1, s_2 \in (T_{\Sigma_{Obs}})_s;\ t_1, t_2 \in T_{\Sigma_{SP_3}}$ es compleix que
$t_1 \equiv_{SP_3} \phi^*(s_1) \wedge t_2 \equiv_{SP_3} \phi^*(s_2)$ implica
$(s_1 \equiv_{SP_3} s_2)$ si i només si $(t_1 \equiv_{SP_3} t_2)$

Com que s_1 és de gènere s, $\phi^*(s_1)$ és de gènere $\theta(s)$, pel sublema [Pal95].38. A més a més, $t_1 \equiv_{SP_3} \phi^*(s_1)$, resulta que t_1 és de tipus $\theta(s)$. Anàlogament, es demostra el mateix per a t_2. Per tant, tenim:

$\forall\, s \in Vis;\quad \forall\, s_1, s_2 \in (T_{\Sigma_{Obs}})_s;\ t_1, t_2 \in (T_{\Sigma_{SP_3}})_{\theta(s)}$ es compleix que
$t_1 \equiv_{SP_3} \phi^*(s_1) \wedge t_2 \equiv_{SP_3} \phi^*(s_2)$ implica
$(s_1 \equiv_{SP_3} s_2)$ si i només si $(t_1 \equiv_{SP_3} t_2)$

Aplicant-hi el lema 13, tenim:

$\forall\, s \in Vis;\quad \forall\, s_1, s_2 \in (T_{\Sigma_{SP_3}})_s;\ t_1, t_2 \in (T_{\Sigma_{SP_3}})_{\theta(s)}$ es compleix que
$trans_s(s_1, t_1) \equiv_{SP_3} yes \wedge trans_s(s_2, t_2) \equiv_{SP_3} yes$ implica
$(s_1 \equiv_{SP_3} s_2)$ si i només si $(t_1 \equiv_{SP_3} t_2)$

Per regles de la lògica, això és equivalent a:

$\forall\, s \in Vis;\quad \forall\, s_1, s_2 \in (T_{\Sigma_{SP_3}})_s;\ t_1, t_2 \in (T_{\Sigma_{SP_3}})_{\theta(s)}$ es compleix que
$(trans_s(s_1, t_1) \equiv_{SP_3} yes \wedge trans_s(s_2, t_2) \equiv_{SP_3} yes \wedge (s_1 \equiv_{SP_3} s_2)$ implica $(t_1 \equiv_{SP_3} t_2))$
$\wedge$
$(trans_s(s_1, t_1) \equiv_{SP_3} yes \wedge trans_s(s_2, t_2) \equiv_{SP_3} yes \wedge (t_1 \equiv_{SP_3} t_2)$ implica $(s_1 \equiv_{SP_3} s_2))$

Pel lema 15, això implica:

$\forall s \in Vis$, $\forall s_1, s_2 \in (T_{\Sigma_{SP_3}})_s$; $t_1, t_2 \in (T_{\Sigma_{SP_3}})_{\theta(s)}$ es compleix que
$(trans_s(s_1, t_1) \equiv_{SP_3} yes \ \wedge \ trans_s(s_1, t_2) \equiv_{SP_3} yes$ implica $t_1 \equiv_{SP_3} t_2) \ \wedge$
$(trans_s(s_1, t_1) \equiv_{SP_3} yes \ \wedge \ trans_s(s_2, t_1) \equiv_{SP_3} yes$ implica $s_1 \equiv_{SP_3} s_2)$

És fàcil veure que aquesta afirmació implica que:

$\forall s \in Vis$; $\forall x_1, x_2 \in vars(s)$; $y_1, y_2 \in vars(\theta(s))$, $\forall v : X \longrightarrow T_{\Sigma_{SP_3}}$ es compleix que
$(trans_s(v^*(x_1), v^*(y_1)) \equiv_{SP_3} yes \ \wedge \ trans_s(v^*(x_1), v^*(y_2)) \equiv_{SP_3} yes$ implica $v^*(y_1) \equiv_{SP_3} v^*(y$
$\wedge$
$(trans_s(v^*(x_1), v^*(y_1)) \equiv_{SP_3} yes \ \wedge \ trans_s(v^*(x_2), v^*(y_1)) \equiv_{SP_3} yes$ implica $v^*(x_1) \equiv_{SP_3} v^*(x$

, ja que com que $x_1 \in vars(s)$, $v^*(x_1) = v(x_1)$ i, per tant, $v^*(x_1) \in T_{\Sigma_{SP_3}}$ (i el mateix passa amb la resta de variables). Per la definició de v^*, obtenim:

$\forall s \in Vis$; $\forall x_1, x_2 \in vars(s)$; $y_1, y_2 \in vars(\theta(s))$, $\forall v : X \longrightarrow T_{\Sigma_{SP_3}}$ es compleix que
$(v^*(trans_s(x_1, y_1)) \equiv_{SP_3} v^*(yes) \ \wedge \ v^*(trans_s(x_1, y_2)) \equiv_{SP_3} v^*(yes)$
implica $v^*(y_1) \equiv_{SP_3} v^*(y_2))$
$\wedge$
$(v^*(trans_s(x_1, y_1)) \equiv_{SP_3} v^*(yes) \ \wedge \ v^*(trans_s(x_2, y_1)) \equiv_{SP_3} v^*(yes)$
implica $v^*(x_1) \equiv_{SP_3} v^*(x_2))$

Per definició de satisfacció d'una equació en una àlgebra donada, això és el mateix que dir:

$\forall s \in Vis$; $\forall x_1, x_2 \in vars(s)$; $y_1, y_2 \in vars(\theta(s))$ es compleix que
$(T_{SP_3} \models trans_s(x_1, y_1) = yes \ \& \ trans_s(x_1, y_2) = yes \ \Rightarrow y_1 = y_2) \wedge$
$(T_{SP_3} \models trans_s(x_1, y_1) = yes \ \& \ trans_s(x_2, y_1) = yes \ \Rightarrow x_1 = x_2)$

Que és el que volíem demostrar. $\square$.

6 Final de la demostració

En aquest apartat, donarem el darrer pas per a la nostra demostració: demostrarem el teorema 17.

Teorema 17. Siguin dues especificacions $SP_1 = (\Sigma_1, E_1)$ i $SP_2 = (\Sigma_2, E_2)$, on $\Sigma_1 = (Vis, \Sigma_{Obs}, (\Sigma_{All})_1)$ i $\Sigma_2 = (Vis, \Sigma_{Obs}, (\Sigma_{All})_2)$ són dues signatures visibles. Sigui SP_3, la V-reunió de SP_1 i SP_2 via qualsevol especificació $SP_4 = (Vis_4, \Sigma_{Obs_4}, (\Sigma_{All})_4, E_4)$. Llavors, les dues afirmacions següents són equivalents:

- $\forall s \in Vis, \forall x_1, x_2 \in vars(s);\ y_1, y_2 \in vars(\theta(s))$ es compleix que $(T_{SP_3} \models trans_s(x_1, y_1) = yes \ \&\ trans_s(x_1, y_2) = yes \ \Rightarrow y_1 = y_2) \wedge$ $(T_{SP_3} \models trans_s(x_1, y_1) = yes \ \&\ trans_s(x_2, y_1) = yes \ \Rightarrow x_1 = x_2)$

- SP_1 i SP_2 són inicialment visiblement equivalents.

Prova. És un corol.lari del teorema 12 i del teorema 16. □

7 Referències

[Pal95] PALASÍ, V.R *Reduction of Behavioural Equivalence to Inductive Theorems.* Research Report LSI-95-56-R. Departament de Llenguatges i Sistemes Informàtics.

[Pal96a] PALASÍ, V.R *Visible Semantics: An Algebraic Semantics for Automatic Verification of Algorithms.* Research Report LSI-96-26-R. Departament de Llenguatges i Sistemes Informàtics. Universitat Politècnica de Catalunya (1996).

[Pal96b] PALASÍ, V.R. *Automatic Verification of Programs: algorithm ALICE.* Research Report LSI-96-34-R. Universitat Politècnica de Catalunya (1996).

Departament de Llenguatges i Sistemes Informàtics
Universitat Politècnica de Catalunya

Research Reports – 1996

LSI–96–1–R "(Pure) Logic out of Probability", Ton Sales.

LSI–96–2–R "Automatic Generation of Multiresolution Boundary Representations", C. Andújar, D. Ayala, P. Brunet, R. Joan-Arinyo, and J. Solé.

LSI–96–3–R "A Frame-Dependent Oracle for Linear Hierarchical Radiosity: A Step towards Frame-to-Frame Coherent Radiosity", Ignacio Martin, Dani Tost, and Xavier Pueyo.

LSI–96–4–R "Skip-Trees, an Alternative Data Structure to Skip-Lists in a Concurrent Approach", Xavier Messeguer.

LSI–96–5–R "Change of Belief in SKL Model Frames (Automatization Based on Analytic Tableaux)", Matías Alvarado and Gustavo Núñez.

LSI–96–6–R "Compressibility of Infinite Binary Sequences", José L. Balcázar, Ricard Gavaldà, and Montserrat Hermo.

LSI–96–7–R "A Proposal for Word Sense Disambiguation using Conceptual Distance", Eneko Agirre and German Rigau.

LSI–96–8–R "Word Sense Disambiguation Using Conceptual Density", Eneko Agirre and German Rigau.

LSI–96–9–R "Towards Learning a Constraint Grammar from Annotated Corpora Using Decision Trees", Lluis Màrquez and Horacio Rodríguez.

LSI–96–10–R "POS Tagging Using Relaxation Labelling", Lluís Padró..

LSI–96–11–R "Hybrid Techniques for Training HMM Part-of-Speech Taggers", Ted Briscoe, Greg Grefenstette, Lluís Padró, and Iskander Serail.

LSI–96–12–R "Using Bidirectional Chart Parsing for Corpus Analysis", A. Ageno and H. Rodríguez.

LSI–96–13–R "Limited Logical Belief Analysis", Antonio Moreno.

LSI–96–14–R "Logic as General Rationality: A Survey", Ton Sales.

LSI–96–15–R "A Syntactic Characterization of Bounded-Rank Decision Trees in Terms of Decision Lists", Nicola Galesi.

LSI–96–16–R "Algebraic Transformation of Unary Partial Algebras I: Double-Pushout Approach", P. Burmeister, F. Rosselló, J. Torrens, and G. Valiente.

LSI-96-17-R "Rewriting in Categories of Spans", Miquel Monserrat, Francesc Rosselló, Joan Torrens, and Gabriel Valiente.

LSI-96-18-R "Strong Law for the Depth of Circuits", Tatsuie Tsukiji and Fatos Xhafa.

LSI-96-19-R "Learning Causal Networks from Data", Ramon Sangüesa i Solé.

LSI-96-20-R "Boundary Generation from Voxel-based Volume Representations", R. Joan-Arinyo and J. Solé.

LSI-96-21-R "Exact Learning of Subclasses of CDNF Formulas with Membership Queries", Carlos Domingo.

LSI-96-22-R "Modeling the Thermal Behavior of Biosphere 2 in a Non-Controlled Environment Using Bond Graphs", Angela Nebot, François E. Cellier, and Francisco Mugica.

LSI-96-23-R "Obtaining Synchronization-Free Code with Maximum Parallelism", Ricard Gavaldá, Eduard Ayguadé, and Jordi Torres.

LSI-96-24-R "Memoisation of Categorial Proof Nets: Parallelism in Categorial Processing", Glyn Morrill.

LSI-96-25-R "Decision Trees Have Approximate Fingerprints", Víctor Lavín and Vijay Raghavan.

LSI-96-26-R "Visible Semantics: An Algebraic Semantics for Automatic Verification of Algorithms", Vicent-Ramon Palasí Lallana.

LSI-96-27-R "Massively Parallel and Distributed Dictionaries on AVL and Brother Trees", Joaquim Gabarró and Xavier Messeguer.

LSI-96-28-R "A Maple package for semidefinite programming", Fatos Xhafa and Gonzalo Navarro.

LSI-96-29-R "Bounding the expected length of longest common subsequences and forests", Ricardo A. Baeza-Yates, Ricard Gavaldà, and Gonzalo Navarro.

LSI-96-30-R "Parallel Computation: Models and Complexity Issues", Raymond Greenlaw and H. James Hoover.

LSI-96-31-R "ParaDict, a Data Parallel Library for Dictionaries (Extended Abstract)", Joaquim Gabarró and Jordi Petit i Silvestre.

LSI-96-32-R "Neural Networks as Pattern Recognition Systems", Lourdes Calderón.

LSI-96-33-R "Semàntica externa: una variant interessant de la semàntica de comportament" (written in Catalan), Vicent-Ramon Palasí Lallana.

LSI-96-34-R "Automatic verification of programs: algorithm ALICE", V.R. Palasí Lallana.

LSI-96-35-R "Multiresolution Approximation of Polyhedral Solids", D. Ayala, P. Brunet, R. Joan-Arinyo, I. Navazo.

LSI-96-36-R "Algebraic Transformation of Unary Partial Algebras II: Single-Pushout Approach", P. Burmeister, M. Montserrat, F. Rosselló, and G. Valiente.

LSI-96-37-R "Probabilistic Conditional Independence: A Similarity-Based Measure and its Application to Causal Network Learning", Ramon Sangüesa Solé, Joan Cabós Fabregat, and Ulises Cortés García.

LSI-96-38-R "Analysing the Process of Enforcing Integrity Constraints", Enric Mayol and Ernest Teniente.

LSI-96-39-R "Reducció de l'equivalència inicial visible a teoremes inductius" (written in Catalan), Vicent-Ramon Palasí Lallana.

Hardcopies of reports can be ordered from:

Nuria Sánchez
Departament de Llenguatges i Sistemes Informàtics
Universitat Politècnica de Catalunya
Pau Gargallo, 5
08028 Barcelona, Spain
secrelsi@lsi.upc.es

See also the Department WWW pages, http://www-lsi.upc.es/www/