Modely konkurentných systémov
Formálne metódy tvorby softvéru

Damas Gruska

Katedra aplikovanej informatiky, I20, gruska@fmph.uniba.sk

Prednáška 4.

o-kongruencia (Observational congruence)

Theorem

$P \sim Q$ *implikuje* $P = Q$
$P = Q$ *implikuje* $P \approx Q$

Úlohy:
- dokážte predchádzajúcu vetu,
- nájdite P, Q také, že
$P = Q$ ale $P \not\sim Q$,
$P \approx Q$ ale $P \neq Q$.

Theorem

$=$ *je ekvivalencia*

Úloha: dokážte predchádzajúcu vetu.

o-kongruencia (Observational congruence)

Theorem

Ak $P_1 \approx P_2$ *tak* $x.P_1 = x.P_2$

Úloha: dokážte predchádzajúcu vetu.

Theorem

Nech $P_1 = P_2$. *Potom*

$$\begin{aligned} x.P_1 &= x.P_2 \\ P_1 + Q &= P_2 + Q \\ P_1 | Q &= P_2 | Q \\ P_1 \setminus L &= P_2 \setminus L \\ P_1[f] &= P_2[f] \end{aligned}$$

Úloha: dokážte predchádzajúcu vetu.

o-kongruencia (Observational congruence)

Theorem

Nech $E = F$, *potom* $\mu XE = \mu XF$

Úloha: dokážte predchádzajúcu vetu.

Theorem

Nech $P_1 = P_2$. *Potom*

$$\begin{aligned} x.\tau.P &= x.P \\ P + \tau.P &= \tau.P \\ x.(P + \tau.Q) + x.Q &= x.(P + \tau.Q) \end{aligned}$$

Úloha: dokážte predchádzajúcu vetu.

o-kongruencia (Observational congruence)

Úloha: dokážte nasledujúce tvrdenia:

$$
\begin{array}{rcl}
P|\tau.Q & \approx & P|Q \\
P|\tau.Q & \neq & P|Q \\
P|\tau.Q & = & \tau.(P|Q)
\end{array}
$$

o-kongruencia (Observational congruence)

Definition

P je stabilný ak $P \overset{\tau}{\nrightarrow}$.

Theorem

Ak P, Q sú stabilné a $P \approx Q$ tak $P = Q$.

Úloha: dokážte predchádzajúcu vetu.

Theorem

$P \approx Q$ iff $P = Q$ alebo $P = \tau.Q$ alebo $\tau.P = Q$.

Dôkaz.

$\Leftarrow$

triviálne

$\Rightarrow$

Nech $P \approx Q$. Máme tri prípady:
1. $P \xrightarrow{\tau} P', P' \approx Q$ pre nejaké P'. Potom $P = \tau.Q$,
2. $Q \xrightarrow{\tau} Q', P \approx Q'$ pre nejaké Q'. Potom $\tau.P = Q$,
3. $P \xrightarrow{a} P'$ potom keďže $P \approx Q$ máme $Q \overset{\hat{a}}{\Rightarrow} Q'$ a $P' \approx Q'$ t.j. $Q \overset{a}{\Rightarrow} Q'$ a $P = Q$.

o-kongruencia (Observational congruence)

Definition

X je sekvenčné v E ak každý subterm termu E obsahujúci X (okrem X samotného) je tvaru $y.F$ alebo $\sum P_i$.

Definition

X je silne strážené v E ak každý výskyt X je vnútri nejakého podtermu tvaru $a.F$ $(a \neq \tau)$.

$\tau.X + a.Nil$
sekvenčné ale nie silne strážené
$a.X|b.Nil$
silne strážené ale nie sekvenčné
$\tau(a.(b.Nil|c.Nil) + b.X)$
silne strážené a sekvenčné

o-kongruencia (Observational congruence)

Theorem

Nech X je v E silne strážené a sekvenčné a $P = E[P/x], Q = E[Q/X]$. Potom $P = Q$.

Počítadlo

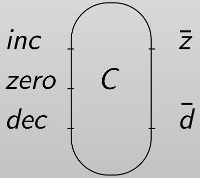
$$
\begin{aligned}
Count_0 &\stackrel{def}{=} inc.Count_1 + zero.Count_0 \\
Count_n &\stackrel{def}{=} inc.Count_{n+1} + dec.Count_{n-1} \quad (n > 0)
\end{aligned}
$$

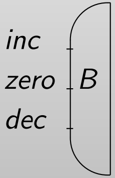
Počítadlo

$$
\begin{aligned}
C &\stackrel{def}{=} inc.(C \frown C) + dec.D \\
D &\stackrel{def}{=} \bar{d}.C + \bar{z}.B \\
B &\stackrel{def}{=} inc.(C \frown B) + zero.B
\end{aligned}
$$

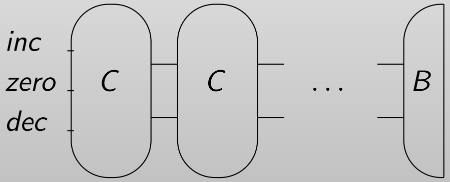
$$P \frown Q \stackrel{def}{=} (P[i'/i, z'/z, d'/d] | Q[i'/inc, z'/zero, d'/dec]) \setminus \{i', z', d'\}$$

Počítadlo





$C^{(n)} = C^\frown C^\frown \ldots^\frown C^\frown B$



Počítadlo

$$C^{(n)} = \overbrace{C^\frown C^\frown \ldots ^\frown C}^{n\times}{}^\frown B$$

Musíme ukázať, že:

$$\begin{aligned} C^{(0)} &= inc.C^{(1)} + zero.C^{(0)} \\ C^{(n)} &= inc.C^{(n+1)} + dec.C^{(n-1)} \quad (n > 0) \end{aligned}$$

Pre $n > 0$

$$\begin{aligned} C^{(n)} &= C^\frown C^{(n-1)} \\ &= inc.((C^\frown C)^\frown C^{(n-1)}) + dec.(D^\frown C^{(n-1)}) \\ &= inc.C^{(n+1)} + dec.(D^\frown C^{(n-1)}) \end{aligned}$$

Počítadlo

Úloha:
ukázať, že platí

$$\begin{aligned} D^\frown C &\approx C^\frown D \\ D^\frown B &\approx B^\frown B \\ B^\frown B &= B \end{aligned}$$

Prepisvací systém

Majme množinu rovností (axióm, prepisovacích pravidiel) $\mathcal{A}$.

To, že term t sa dá prepísať na term t' použitím $\mathcal{A}$ budeme označovať $\mathcal{A} \vdash t = t'$.

$\mathcal{A} \vdash x = x$

Ak $\mathcal{A} \vdash x = y$ potom $\mathcal{A} \vdash y = x$.

Ak $\mathcal{A} \vdash x = y$ a $\mathcal{A} \vdash y = z$ potom $\mathcal{A} \vdash x = z$.

Ak $\mathcal{A} \vdash x_i = y_i$ pre $i \in \{1, \ldots, n\}$ tak
$\mathcal{A} \vdash f(x_1, \ldots, , x_n) = f(y_1, \ldots, y_n)$

Axiomatizácia

Definition

Proces je konečný ak neobsahuje rekurziu. Proces je sériový, ak neobsahuje operátory $|, \backslash, [f]$.

Každý konečný proces je bisimulárny nejakému konečnému sériovému procesu.

V ďalšom sa budeme zaoberať len konečnými sériovými procesmi.

Axiomatizácia

$P = Q$ znamená, že P a Q sú o-kongruentné
$\mathcal{A} \vdash P = Q$ znamená, že rovnosť môže byť odvodená pomocou axióm $\mathcal{A}$

$\mathcal{A}_1$:

$$\begin{array}{rcll} P + Q & = & Q + P & A1 \\ P + (Q + R) & = & (Q + P) + R & A2 \\ P + P & = & P & A3 \\ P + Nil & = & P & A4 \end{array}$$

$\mathcal{A}_2$:

$$\begin{array}{rcll} x.\tau.P & = & x.P & A5 \\ P + \tau.P & = & \tau.P & A6 \\ x.(P + \tau.Q) + x.Q & = & x.(P + \tau.Q) & A7 \end{array}$$

Definition

P je v štandardnej forme ak $P \equiv \sum_{i=1}^{n} x_i.P_i$ kde každé P_i je opäť v štandardnej forme.

Poznámka: Nil je v štandardnej forme ak zobereme $n = 0$.

$a.Nil$
$a.Nil + b.(c.Nil + \tau.Nil)$
sú v štandardnej forme

$Nil + b.Nil$
$a.(Nil + b.Nil)$
nie sú v štandardnej forme

Axiomatizácia

Theorem

Pre každé P existuje P' v štandardnej forme, také že $\mathcal{A}_1 \vdash P = P'$.

Nil môžeme povyhadzovať a výsledok je v štandardnej forme.

Theorem

$P \sim Q$ iff $\mathcal{A}_1 \vdash P = Q$.

Dôkaz:
$\Leftarrow$ (bezospornosť)
toto už bolo dokázané pre $\sim$
$\Rightarrow$ (úplnosť)
Predpokladajme $P \sim Q$ a že P a Q sú v štandardnej forme
$P \equiv \sum_{i=1}^{n} x_i.P_i$ a $Q \equiv \sum_{i=1}^{m} x_i.Q_i$
Indukciou podľa hĺbky P a Q
- ak maximálna hĺbka P a Q je 0 tak P a Q sú rovné Nil.
- inak nech $x.P'$ je sumand P tak $P \xrightarrow{x} P'$ a keďže $P \sim Q$ tak existuje Q' $Q \xrightarrow{x} Q'$, $P' \sim Q'$ t.j. $x.Q'$ je sumand Q a podľa indukcie $\mathcal{A}_1 \vdash P' = Q'$.

Axiomatizácia

Ideme dokázať obdobné tvrdenie pre $=$.
$P \equiv a.(b.Nil + \tau.Nil)$, $Q \equiv a.(b.Nil + \tau.Nil) + a.Nil$
P a Q majú rôzne štandardné formy ale $P = Q$.

Definition

P je v plne štandardnej forme ak
(i) $P \equiv \sum_{i=1}^{n} x_i.P_i$ kde každé P_i je opäť v plne štandardnej forme,
(ii) ak $P \stackrel{x}{\Rightarrow} P_i$ tak $P \stackrel{x}{\rightarrow} P_i$.

$P \equiv \tau.(a.(\tau.Nil + b.Nil))$
$P' \equiv a.(\tau.Nil + b.Nil)$
P, P' nie sú v plne štandardnej forme.

Theorem

Ak $P \overset{x}{\Rightarrow} P'$ *tak* $\mathcal{A}_1 \cup \mathcal{A}_2 \vdash P = P + x.P'$.

Dôkaz:
Indukciou podľa hĺbky štruktúry P.
$P \overset{x}{\Rightarrow} P'$
1. prípad $x.P'$ je sumand P (A3)
2. prípad $x.Q$ je sumand P a $Q \overset{\tau}{\Rightarrow} P'$ potom podľa indukcie

$\mathcal{A}_1 \cup \mathcal{A}_2 \vdash Q = Q + \tau.P'$ a
$\mathcal{A}_1 \cup \mathcal{A}_2 \vdash P = P + x.Q$ (A3)
$\mathcal{A}_1 \cup \mathcal{A}_2 \vdash P = P + x.(Q + \tau.P')$ (podľa predchádzajúcich dvoch)
$\mathcal{A}_1 \cup \mathcal{A}_2 \vdash P = P + x.(Q + \tau.P') + x.P'$ (A7)
$\mathcal{A}_1 \cup \mathcal{A}_2 \vdash P = P + x.Q + x.P'$ (z $\mathcal{A}_1 \cup \mathcal{A}_2 \vdash Q = Q + \tau.P'$)
$\mathcal{A}_1 \cup \mathcal{A}_2 \vdash P = P + x.P'$ (z $\mathcal{A}_1 \cup \mathcal{A}_2 \vdash P = P + x.Q$)

3. prípad $\tau.Q$ je sumand P a $Q \stackrel{x}{\Rightarrow} P'$ potom podľa indukcie

$\mathcal{A}_1 \cup \mathcal{A}_2 \vdash Q = Q + x.P'$ a

$\mathcal{A}_1 \cup \mathcal{A}_2 \vdash P = P + \tau.Q$ (A3)

$\mathcal{A}_1 \cup \mathcal{A}_2 \vdash P = P + \tau.Q + Q$ (A6)

$\mathcal{A}_1 \cup \mathcal{A}_2 \vdash P = P + \tau.Q + Q + x.P'$ (z $\mathcal{A}_1 \cup \mathcal{A}_2 \vdash Q = Q + \tau.P'$)

$\mathcal{A}_1 \cup \mathcal{A}_2 \vdash P = P + \tau.Q + x.P'$ (A6)

$\mathcal{A}_1 \cup \mathcal{A}_2 \vdash P = P + x.P'$ (z $\mathcal{A}_1 \cup \mathcal{A}_2 \vdash P = P + \tau.Q$)

Axiomatizácia

Theorem

Pre každý proces P v štandardnej forme existuje proces P' v plne štandardnej forme rovnakej hĺbky, taký že $\mathcal{A}_1 \cup \mathcal{A}_2 \vdash P = P'$.

Dôkaz.
Indukciou podľa hĺbky P.
Nech $P \equiv Nil$ - tak P je už v plne štandardnej forme. Inak pre každý sumand $y.Q$ procesu P môžeme predpokladať že už je v plne štandardnej forme.
Uvažujme všetky dvojice $x_i.P_i, 1 \leq i \leq k$ také, že $P \stackrel{x_i}{\Rightarrow} P_i$ ale nie $P \stackrel{x_i}{\rightarrow} P_i$.
Potom zobereme
$P' \equiv P + x_1.P_1 + \cdots + x_k.P_k$
a podľa predchádzajúcej vety máme
$\mathcal{A}_1 \cup \mathcal{A}_2 \vdash P = P'$.

Axiomatizácia

Theorem

$P = Q$ *iff* $\mathcal{A}_1 \cup \mathcal{A}_2 \vdash P = Q$.

Dôkaz:
$\Leftarrow$ (bezospornosť)
toto už bolo dokázané pre $=$
$\Rightarrow$ (úplnosť)
Podľa predchádzajúcich viet môžeme predpokladať, že P, Q sú v plne štandardnej forme.
Indukciou podľa hĺbky P a Q.
Ak $P \equiv Q \equiv Nil$ - triviálne.
Nech $P = Q$ a $x.P'$ je sumand P.
Keďže $P \xrightarrow{x} P'$ vieme, že existuje Q', $Q \overset{x}{\Rightarrow} Q'$ a $P' \approx Q'$.
Navyše $Q \xrightarrow{x} Q'$ keďže Q je v plne štandardnej forme a teda $x.Q'$ je sumand Q.

Axiomatizácia

Vieme, že keďže $P' \approx Q'$ tak $P' = Q'$ alebo $P' = \tau.Q'$ alebo $\tau.P' = Q'$

ak platí $P' = Q'$ a keďže oba sú menšej hĺbky

$\mathcal{A}_1 \cup \mathcal{A}_2 \vdash P' = Q'$

a teda

$\mathcal{A}_1 \cup \mathcal{A}_2 \vdash x.P' = x.Q'$

Axiomatizácia

ak platí $P' = \tau.Q'$ musíme $\tau.Q'$ previesť do plne štandardnej formy Q''
$\mathcal{A}_1 \cup \mathcal{A}_2 \vdash \tau.Q' = Q''$.
Suma dĺžok P' a Q''je nižšia a tak môžeme použiť indukčný predpoklad
$\mathcal{A}_1 \cup \mathcal{A}_2 \vdash P' = Q''$
a teda
$\mathcal{A}_1 \cup \mathcal{A}_2 \vdash P' = \tau.Q'$ a podľa A5
$\mathcal{A}_1 \cup \mathcal{A}_2 \vdash x.P' = x.Q'$
Ukázali sme, že každý sumand P "je" ($\mathcal{A}_1 \cup \mathcal{A}_2 \vdash$) aj sumand Q (a naopak).

Axiomatizácia

Theorem

$\mu X(X + E) \sim \mu XE.$ *(B1)*

Theorem

$\mu X(\tau.X + E) = \mu X(\tau.E).$ *(B2)*
$\mu X(\tau.(X + E) + F) = \mu X(\tau.X + E + F).$ *(B3)*

Vieme, že platí
$\mu XE \sim E[\mu XE]$ (B4)

Vieme, že platí (ak X je strážené v E)
Ak $F \sim E[F/X]$ tak $F \sim \mu XE.$ (B5)

Vieme, že platí (ak X je silne strážené a sériové v E)
Ak $F = E[F/X]$ tak $F = \mu XE.$ (B6)

Axiomatizácia

Theorem

$\mathcal{A}_1 \cup \{B1, B4, B5\}$ *tvorí axiomatizáciu silnej bisimulácie pre sériové procesy. (aj nekonečné)*

Theorem

$\mathcal{A}_1 \cup \mathcal{A}_2 \cup \{B2, B3, B4, B6\}$ *tvorí axiomatizáciu o-kongruencie pre sériové procesy. (aj nekonečné)*

Majme prechodvý systém $(CCS, Act, \{\xrightarrow{x}, x \in Act\})$.

Definition

$\mathcal{PL}$ je najmenšia trieda formúl taká, že ak $\phi, \phi_i \in \mathcal{PL}$ tak aj formuly
(i) $< x > \phi$
(ii) $\neg\phi$
(iii) $\wedge_{i\in I}\phi_i$, kde I je indexová množina
sú z $\mathcal{PL}$.

Ak zobereme v $\wedge_{i\in I}\phi_i$ za I prázdnu množinu, výslednú formulu budeme označovať tt (true).

Modálna logika

Neformálne význam formuly $< x > \phi$:

P spĺňa $< x > \phi$ ak P vie vykonať akciu x a výsledný proces Q spĺňa ϕ.

$\phi \equiv < x > tt \wedge \neg < y > tt$
proces môže vykonať akciu x a nemôže vykonať akciu y.

$\phi \equiv < x > (< z > tt \wedge \neg < y > tt)$
proces môže vykonať akciu x a po jej vykonaní dosihne stav (proces), ktorý môže vykonať akciu z a nemôže vykonať akciu y.

Definition

Definujme reláciu splniteľnosti ($\models$)medzi CCS a $\mathcal{PL}$:
(i) $P \models < x > \phi$ ak existuje P' také, že $P \xrightarrow{x} P'$ a $P' \models \phi$
(ii) $P \models \neg\phi$ ak $P \not\models \phi$
(iii) $P \models \wedge_{i \in I} \phi_i$ ak $\forall i, i \in I, P \models \phi_i$

$P \equiv a.(b.Nil + c.Nil), Q \equiv a.b.Nil + a.c.Nil$
$\phi \equiv < a > (< b > tt \wedge < c > tt)$
$P \models \phi$
$Q \not\models \phi$

Modálna logika

$$
\begin{aligned}
ff &\stackrel{def}{=} \neg tt \\
\phi_1 \wedge \phi_2 &\stackrel{def}{=} \bigwedge_{i \in \{1,2\}} \phi_i \\
\bigvee_{i \in I} \phi_i &\stackrel{def}{=} \neg \bigwedge_{i \in I} \neg \phi_i \\
\phi_1 \vee \phi_2 &\stackrel{def}{=} \bigvee_{i \in \{1,2\}} \phi_i \\
\phi_1 \Rightarrow \phi_2 &\stackrel{def}{=} \neg \phi_1 \vee \phi_2 \\
< x_1 \ldots x_n > \phi &\stackrel{def}{=} < x_1 > \cdots < x_n > \phi \\
[s]\phi &\stackrel{def}{=} \neg < s > \neg \phi, s \in Act^*
\end{aligned}
$$

$[s]ff$ - proces nemôže vykonať postupnosť akcii s.

Modálna logika

Theorem

Binárna relácia $S \subseteq CCS \times CCS$ *je (silná) bisimulácia, iff*
$(P, Q) \in S$ *implikuje* $\forall s, s \in Act^*$
1) ak $P \xrightarrow{s} P'$ *tak existuje* Q' *také, že* $Q \xrightarrow{s} Q'$ *a platí* $(P', Q') \in S$
2) ak $Q \xrightarrow{s} Q'$ *tak existuje* P' *také, že* $P \xrightarrow{s} P'$ *a platí* $(P', Q') \in S$

Definition

- $P \sim_0 Q$ pre každé P, Q ($\sim_0 = CCS \times CCS$)
- $P \sim_{k+1} Q$ ak $\forall s, s \in Act^*$
1) ak $P \xrightarrow{s} P'$ tak existuje Q' také, že $Q \xrightarrow{s} Q'$ a platí $P' \sim_k Q'$
2) ak $Q \xrightarrow{s} Q'$ tak existuje P' také, že $P \xrightarrow{s} P'$ a platí $P' \sim_k Q'$
- pre každý limitný ordinál λ
$P \sim_\lambda Q$ ak $\forall k, k < \lambda$ platí $P \sim_k Q$ ($\sim_\lambda = \bigcap_{k<\lambda} \sim_k$).

Theorem

Ak $k < l$ *tak* $\sim_l \subseteq \sim_k$.

Theorem

$\sim = \bigcap_{k \in \mathcal{O}} \sim_k$

Theorem

$\sim_0, \sim_1, \ldots, \sim_\omega$ *sú ostro klesajúce.*

Dôkaz.
Ukážeme, že $P_i \sim_i Q_i$ ale $P_i \not\sim_{i+1} Q_i$ kde
$P_0 \equiv b.Nil$, $Q_0 \equiv c.Nil$
$P_{i+1} \equiv a.(P_i + Q_i)$, $Q_{i+1} \equiv a.P_i + a.Q_i$
Dôkaz indukciou.
Nech $P_i \sim_i Q_i$ ale $P_i \not\sim_{i+1} Q_i$.
$P_{i+1} \xrightarrow{a} P_i + Q_i$ a $Q_{i+1} \xrightarrow{a} P_i$ alebo $Q_{i+1} \xrightarrow{a} Q_i$
ale keďže $P_i \sim_i Q_i$ máme
$P_{i+1} \sim_{i+1} Q_{i+1}$
teraz ukážeme, že $P_{i+1} \not\sim_{i+2} Q_{i+1}$
t.j že $P_i + Q_i \not\sim_{i+1} P_i$ a $P_i + Q_i \not\sim_{i+1} Q_i$
Ak by ale $P_i + Q_i \sim_{i+1} P_i$ a $P_i + Q_i \sim_{i+1} Q_i$ tak by sme mali
$P_i \sim_{i+1} Q_i$ čo je spor s predpokladom.

Theorem

$\sim_{\omega} \neq \sim_{\omega+1}$ *ak povolíme neobmedzené* $\sum$.

Dôkaz.
Nech

$$
\begin{aligned}
R_0 &\overset{def}{=} \sum_{0 \leq i < \omega} P_i \\
R_1 &\overset{def}{=} Q_0 + \sum_{1 \leq i < \omega} P_i \\
R_2 &\overset{def}{=} Q_0 + Q_1 + \sum_{2 \leq i < \omega} P_i \\
&\vdots \\
R_\omega &\overset{def}{=} Q_0 + Q_1 + \dots
\end{aligned}
$$

Nech $R \equiv \sum_{i<\omega} a.R_i$ a $R' \equiv R + a.R_\omega$
Z predchádzajúceho vieme, že $R_\omega \sim_i R_i$ ale $R_\omega \not\sim_{i+1} R_i$.
Teraz ukážeme, že $R \sim_i R'$ pre , $i < \omega$ a teda $R \sim_\omega R'$.
Jediný zaujímavý prípad je, keď
$R' \xrightarrow{a} R_\omega$
ale vždy môžeme nájsť
R_i také, že $R \xrightarrow{a} R_i$ a $R_\omega \sim_i R_i$, teda $R \sim_\omega R'$.
Zároveň máme $R \not\sim_{\omega+1} R'$ keďže $R_i \not\sim_\omega R_\omega$.

Modálna logika

Nech $\phi \equiv < a > [a](< b > tt \wedge < c > tt)$

Potom máme
$P_2 \models \phi$

ale
$Q_2 \not\models \phi$

Podobne môžeme rozlíšiť každé P_i a Q_i.

Uvažujme modifikáciu $\mathcal{PL}$ takú, že za základný operátor budeme považovaž $< s >$ pre $s \in Act^*$.

Definition

$$\begin{aligned} depth(< s > \phi) &\stackrel{def}{=} depth(\phi) + 1 \\ depth(\neg\phi) &\stackrel{def}{=} depth(\phi) \\ depth(\wedge_{i\in I}\phi_i) &\stackrel{def}{=} sup_{i\in I}\{depth(\phi_i)\} \end{aligned}$$

Pre každý ordinál k definujeme:
$\mathcal{PL}_k = \{\phi, depth(\phi) \leq k\}$

Theorem

(i) Pre každý ordinál k platí

$P \sim_k Q$ *iff pre každé* $\phi, \phi \in \mathcal{PL}_k$, $P \models \phi \Leftrightarrow Q \models \phi$.

(ii) $P \sim Q$ *iff pre každé* $\phi, \phi \in \mathcal{PL}$, $P \models \phi \Leftrightarrow Q \models \phi$.

Dôkaz.
Stačí ukázať (i) keďže to implikuje (ii).
$\Rightarrow$
Nech $P \sim_k Q$ a $P \models \phi$ pre $\phi \in \mathcal{PL}_k$.
Chceme ukázať, že potom $Q \models \phi$.
Najzaujímavejší prípad je, keď
$\phi \equiv < s > \phi'$ a $depth(\phi) = l, l < k$.
Potom $P \xrightarrow{s} P'$ pre nejaké P', také, že $P' \models \phi'$.
Z $P \sim_k Q$ plynie $P \sim_{l+1} Q$ a teda
$Q \xrightarrow{s} Q'$ pre nejaké Q' a $P \sim_l Q$.
Z indukčného predpokladu máme $Q' \models \phi'$.
odkiaľ máme $Q \models \phi$.

$\Leftarrow$
Nech $P \not\sim_k Q$. potom nájdeme formulu $\phi, \phi \in \mathcal{PL}_k$, takú že $P \models \phi$ a $Q \not\models \phi$
Uvažujme prípad, že $k = l + 1$.
Bez ujmy na všeobecnosti, môžeme predpokladať, že pre nejaké s a P', $P \xrightarrow{s} P'$ a pre každé Q' ak $Q \xrightarrow{s} Q'$ tak $P' \not\sim_l Q'$.
Nech $\{Q_i, i \in I\}$ je množina všetkých s derivátov Q.
Potom pre každé $i, i \in I, P' \not\sim_l Q_i$.
Podľa indukčného predpokladu existujú formule $\phi_i, \phi_i \in \mathcal{PL}_l$ také, že $P' \models \phi_i$ a $Q_i \not\models \phi_i$.
Zoberme $\phi \equiv < s > \wedge_{i \in I} \phi_i$.
Ľahhko vidno, že $P \models \phi$ a $Q \not\models \phi$ a $\phi \in \mathcal{PL}_k$.
Nech k je limitný ordinál. Potom $P \not\sim_l Q$ pre nejaké $l, l < k$.
Potom podľa indukcie existuje $\phi, \phi \in \mathcal{PL}_l$ také, že $P \models \phi$ a $Q \not\models \phi$ ale $\phi \in \mathcal{PL}_k$.