5 Słaba równoważność bisymulacyjna

Pojęcia słabej bisymulacji, słabej równoważności, słabej bisymulacji z dokładnością do słabej równoważności, itp. są analogiczne do swoich silnych odpowiedników, z tą różnicą, iż oparte one są o inną relację tranzycji. Zamiast tranzycji $\stackrel{\alpha}{\longrightarrow}$ będziemy teraz używać $\stackrel{\varepsilon}{\Longrightarrow}$ oraz $\stackrel{l}{\Longrightarrow}$, $l \in \mathcal{L}$, zdefiniowanych następująco:

$$\stackrel{\varepsilon}{\Longrightarrow} \;=\; (\stackrel{\tau}{\longrightarrow})^* \qquad\qquad \stackrel{l}{\Longrightarrow} \;=\; (\stackrel{\tau}{\longrightarrow})^* \circ \stackrel{l}{\longrightarrow} \circ (\stackrel{\tau}{\longrightarrow})^*.$$

Można jednolicie wyrazić obydwie relacje następująco:

Definicja 34 *Dla* $t = \alpha_1 \ldots \alpha_n \in \mathrm{Act}^*$, $P \stackrel{t}{\Longrightarrow} P'$ *jeśli*

$$P(\stackrel{\tau}{\longrightarrow})^* \stackrel{\alpha_1}{\Longrightarrow} (\stackrel{\tau}{\longrightarrow})^* \ldots (\stackrel{\tau}{\longrightarrow})^* \stackrel{\alpha_n}{\Longrightarrow} (\stackrel{\tau}{\longrightarrow})^* P'.$$

Dla $t \in \mathrm{Act}^*$, *niech* $\widehat{t}$ *oznacza ciąg* t, *z którego usunięto wszystkie wystąpienia* τ. *Powiemy, że* P' *jest słabym t-potomkiem procesu* P *jeśli* $P \stackrel{\widehat{t}}{\Longrightarrow} P'$.

Zauważmy, iż obydwie relacje wspomniane powyżej, $\stackrel{\varepsilon}{\Longrightarrow}$ oraz $\stackrel{l}{\Longrightarrow}$, są szczególnymi przypadkami relacji $P \stackrel{\widehat{\alpha}}{\Longrightarrow} P'$, dla $\alpha \in \mathrm{Act}$. Mamy zatem, dla $t \in \mathrm{Act}^*$, trzy relacje:

$$\stackrel{t}{\longrightarrow} \;\subsetneq\; \stackrel{t}{\Longrightarrow} \;\subsetneq\; \stackrel{\widehat{t}}{\Longrightarrow}.$$

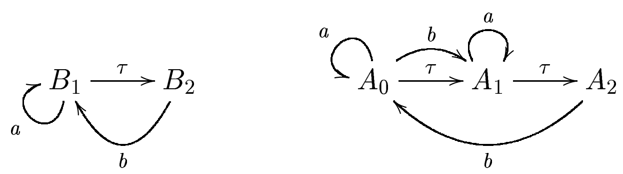
Dla pierwszej z nich, t określa *dokładnie* ile zdarzeń τ ma mieć miejsce. Dla drugiej, t specyfikuje ile *co najmniej* τ ma się odbyć. W przypadku trzeciej, nic nie wiadomo o liczbie τ.

Definicja 35 *Relację binarną* R *pomiędzy procesami nazywamy słabą bisymulacją, jeśli dla każdej pary* $(P, Q) \in R$, $\forall \alpha \in \mathrm{Act}$,

$$(i) \quad P \stackrel{\alpha}{\longrightarrow} P' \implies \exists Q' \;\; t.\dot{z}e \;\; Q \stackrel{\widehat{\alpha}}{\Longrightarrow} Q' \;\; i \;\; (P', Q') \in R$$

$$(ii) \quad Q \stackrel{\alpha}{\longrightarrow} Q' \implies \exists P' \;\; t.\dot{z}e \;\; P \stackrel{\widehat{\alpha}}{\Longrightarrow} P' \;\; i \;\; (P', Q') \in R.$$

Ćwiczenie 60 *Znajdź słabą bisymulację pomiędzy procesami:*



Będziemy czasem pisać krótko *bisymulacja* mając na myśli słabą bisymulację. Kilka poniższych faktów i definicji jest zupełnie analogicznych do faktów i definicji z poprzedniego rozdziału. Tym niemniej, dowody nie zawsze są zupełnie identyczne.

Fakt 36 *Jeśli R, R' oraz R_i, dla $i \in I$, są słabymi bisymulacjami, to*

$$
\begin{array}{llll}
(i) & \textit{relacja identyczności} \ \equiv & \qquad (iii) & R' \circ R \\
(ii) & R^{-1} & \qquad (iv) & \bigcup_{i \in I} R_i
\end{array}
$$

są nimi też.

Ćwiczenie 61 *Udowodnij punkt (iii). (Wskazówka: ćwiczenie 66.)*

Definicja 37 *Procesy P i Q są <u>słabo równoważne</u>, ozn. $P \approx Q$, jeśli $(P, Q) \in R$, dla pewnej słabej bisymulacji R.*

Innymi słowy, słaba równoważność $\approx$ jest sumą wszystkich bisymulacji:

$$\approx \ = \bigcup_{R \text{ słaba bisymulacja}} R$$

Relację $\approx$ będziemy nazywać też *słabą równoważnością bisymulacyjną.*

Ćwiczenie 62 *Udowodnij, że*

(i) $\approx$ *jest największą słabą bisymulacją*

(ii) $\approx$ *jest równoważnością.*

Ćwiczenie 63 *Znajdź najmniejszą słabą bisymulację zawierającą wszystkie pary postaci $(P, \tau.P)$.*

Ćwiczenie 64 *Udowodnij fakt analogiczny do (20) z poprzedniego rozdziału:*

$$
P \approx Q \qquad \textit{wtw. gdy} \qquad
\begin{array}{l}
\forall \alpha \in \mathrm{Act}, \\
(i) \ \ P \xrightarrow{\alpha} P' \implies \exists Q' \ \ t.\dot{z}e \ \ Q \stackrel{\widehat{\alpha}}{\Longrightarrow} Q' \ \ i \ \ P' \sim Q' \\
(ii) \ \ Q \xrightarrow{\alpha} Q' \implies \exists P' \ \ t.\dot{z}e \ \ P \stackrel{\widehat{\alpha}}{\Longrightarrow} P' \ \ i \ \ P' \sim Q'
\end{array}
$$

Ćwiczenie 65 *Czy słaba równoważność jest również największym punktem stałym pewnego przekształcenia $\mathcal{F}$?*

Ćwiczenie 66 *Uzasadnij, że R jest bisymulacją wtw. gdy dla każdej pary $(P,Q) \in R$, $\forall\alpha \in \mathrm{Act}$,*

$$(i)\ \ P \stackrel{\widehat{\alpha}}{\Longrightarrow} P' \implies \exists Q' \ \ t.że\ \ Q \stackrel{\widehat{\alpha}}{\Longrightarrow} Q' \ \ i\ \ (P',Q') \in R$$
$$(ii)\ \ Q \stackrel{\widehat{\alpha}}{\Longrightarrow} Q' \implies \exists P' \ \ t.że\ \ P \stackrel{\widehat{\alpha}}{\Longrightarrow} P' \ \ i\ \ (P',Q') \in R.$$

Czyli powyższy „usymetryczniony" warunek można równoważnie przyjąć za definicję bisymulacji, zamiast definicji 35. Podstawowa różnica między nimi jest taka, że warunek użyty w definicji 35 jest znacznie łatwiejszy do sprawdzenia, podczas dowodzenia równoważności procesów za pomocą bisymulacji.

Ćwiczenie 67 *Rozważ ponownie dwie równoważne definicje bisymulacji, ale po zastąpieniu zdarzenia α przez skończony ciąg zdarzeń t. Czy dwie nowe definicje są również równoważne definicji 35?*

Jak wynika z ćwiczenia 63, $\approx$ nie jest z pewnością poszukiwaną przez nas równością semantyczną $=$, gdyż w ogólności $P \neq \tau.P$. Co więcej, $\approx$ nie jest kongruencją, gdyż $a.0 \approx \tau.a.0$ ale $a.0 + b.0 \not\approx \tau.a.0 + b.0$.

Ćwiczenie 68 *Pokaż ostatnią nierównoważność.*

Słaba równoważność utożsamia zbyt wiele par procesów, mamy zatem:

$$\sim \ \ \subsetneq \ = \ \subsetneq \ \ \approx . \tag{23}$$

Tym niemniej, relacja $\approx$ jest już bardzo blisko semantycznej równości. Oto kilka argumentów.

Definicja 38 *P jest <u>stabilny</u> jeśli nie ma τ-potomków (ozn. $P \stackrel{\tau}{\not\rightarrow}$).*

Fakt 39 $P \approx Q \implies P = Q$, *o ile P i Q są stabilne.*

Fakt ten ma kluczowe znaczenie dla dowodzenia równości procesów. Potwierdza on, iż słaba bisymulacja jest poprawną metodą dowodzenia równości procesów: zamiast dowodzić $P = Q$, w praktyce wystarczy rozważyć $start.P = start.Q$ (czyli zakładamy, iż działanie systemu rozpoczyna się od dodatkowego zdarzenia $start \notin \mathcal{L}(P) \cup \mathcal{L}(Q)$), a ta ostatnia para jest stabilna.

Fakt 40 *Jeśli $P \approx Q$, $P' \approx Q'$ oraz $P_i \approx Q_i$, dla $i \in I$, to:*

$(i)\ \ \alpha.P \approx \alpha.Q$ $\qquad$ $(iii)\ \ P\backslash L \approx Q\backslash L$

$(ii)\ \ \sum_{i\in I}\alpha_1.P_i \approx \sum_{i\in I}\alpha_1.Q_i$ $\qquad$ $(iv)\ \ P[f] \approx Q[f]$

$(v)\ \ P|P' \approx Q|Q'$

Jedyna różnica względem analogicznego faktu dla silnej równoważności to ograniczenie się w punkcie (ii) do sum *słabo strzeżonych*; w szczególności α_i może być równe τ. Z faktu 40 wynika, że $\approx$ jest kongruencją, gdy używamy jedynie sum słabo strzeżonych, co w praktyce jest zupełnie wystarczające.

Ćwiczenie 69 *Udowodnij fakt 40.*

Jako ostatni argument przemawiający za bliskością $=$ i $\approx$ wspomnijmy, że punkt (i) można wzmocnić następująco:

Fakt 41 *Jeśli* $P \approx Q$*, to* $\alpha.P \ = \ \alpha.Q$.

Dowody faktów 39 oraz 41 podamy później, gdy poznamy definicję równości semantycznej. Zanim ją jednak podamy, zajmiemy się analizą kilku przykładów praktycznych, ilustrujących przede wszystkim użycie bisymulacji do dowodzenia poprawności. Nasza dotychczasowa wiedza jest w zupełności wystarczająca, gdyż dzięki faktowi 39 będziemy mogli nie odróżniać $=$ od $\approx$.

5.1 Z dokładnością do $\approx$

Podobnie jak w przypadku silnej bisymulacji, chcemy usprawnić nieco naszą metodę dowodową tak, aby dla wykazania $P \approx Q$ wystarczyło znaleźć jak najmniejszą relację zawierającą parę (P, Q). Oto naturalna adaptacja definicji z poprzedniego rozdziału.

Definicja 42 *Relację binarną* R *pomiędzy procesami nazwiemy* *słabą bisymulacją z dokładnością do* $\approx$, *jeśli dla każdej pary* $(P, Q) \in R$, $\forall \alpha \in \mathrm{Act}$,

$$(i)\ \ P \xrightarrow{\alpha} P' \implies \exists Q' \ \ t.że \ \ Q \overset{\widehat{\alpha}}{\Longrightarrow} Q' \ \ i \ \ (P', Q') \in \ \approx \circ R \circ \approx$$

$$(ii)\ \ Q \xrightarrow{\alpha} Q' \implies \exists P' \ \ t.że \ \ P \overset{\widehat{\alpha}}{\Longrightarrow} P' \ \ i \ \ (P', Q') \in \ \approx \circ R \circ \approx$$

Czytelnik znudzony kolejną z pozoru oczywistą wariacją na temat bisymulacji zapewne jest stuprocentowo pewien, że zachodzi:

Fakt 43 *Jeśli* R *jest słabą bisymulacją z dokładnością do* $\approx$*, to* $\approx \circ R \circ \approx$ *jest słabą bisymulacją. (A zatem* $R \subseteq \ \approx$*.)*

Ćwiczenie 70 *Spróbuj udowodnić powyższy fakt, zwracając baczną uwagę na szczegóły.*

Dlaczego wymagamy od czytelnika żmudnego dowodzenia *oczywistego* faktu? Dlatego, iż w rzeczywistości jednak fakt 43 *nie* zachodzi!

Ćwiczenie 71 *Spróbuj wykazać, że fakt 43 nie zachodzi. Rozważ $\alpha = \tau$ oraz parę procesów postaci $(\tau.P, 0)$, dla pewnego P. Znajdź relację R zawierającą tę parę taką, że R jest bisymulacją z dokładnością do $\approx$, a mimo to $R \not\subseteq\ \approx$.*

Cały problem znika, gdy oprzemy pojęcie bisymulacji z dokładnością do $\approx$ na symetrycznej wersji bisymulacji, rozważanej w ćwiczeniu 66. Ale wtedy sprawdzenie, że dana relacja jest bisymulacją z dokładnością do $\approx$ jest zbyt kosztowne!

Jednym ze sposobów rozwiązania problemu jest ograniczenie się do relacji R spełniających następujący warunek: dla każdej pary $(P, Q) \in R$, $\forall \alpha \in \mathrm{Act}$,

$$\begin{array}{ll} (i) & P \xrightarrow{\alpha} P' \implies \exists Q' \text{ t.że } Q \stackrel{\widehat{\alpha}}{\Longrightarrow} Q' \text{ i } (P', Q') \in\ \sim \circ R \circ \approx \\ (ii) & Q \xrightarrow{\alpha} Q' \implies \exists P' \text{ t.że } P \stackrel{\widehat{\alpha}}{\Longrightarrow} P' \text{ i } (P', Q') \in\ \approx \circ R \circ \sim \end{array} \qquad (24)$$

Np. rozważmy relację zawierającą tylko jedną parę $(\tau.a.0, 0)$, będącą jednym z rozwiązań ostatniego ćwiczenia, i zauważmy, iż została ona wyeliminowana przez powyższy warunek. Niestety, wyeliminowaliśmy za dużo, i w praktyce relacje spełniające (24) nie wystarczają (tak jest np. w przykładzie specyfikacji i implementacji systemu `Zarządca`).

Wybierzemy inne rozwiązanie problemu bisymulacji z dokładnością do $\approx$, oparte na pojęciu *pre-bisymulacji.* Różni się ona od słabej bisymulacji tylko tym, że bierze w pewien sposób pod uwagę liczbę zdarzeń τ wykonanych przez procesy: jeśli para (P, Q) jest w relacji pre-bisymulacji, to zawsze proces Q ma prawo wykonać *co najmniej* tyle zdarzeń τ co proces P, i vice versa, proces P ma prawo wykonać *co najwyżej* tyle τ co Q. pre-bisymulacja jest w praktyce zupełnie wystarczająca dla wykazania poprawności implementacji względem specyfikacji, gdyż w przeważającej liczbie przypadków implementacja wykonuje znacznie więcej τ niż specyfikacja. Przypomnijmy, iż dowodzenie poprawności odbywa się zwykle następująco: i specyfikację i implementację wyrażamy jako procesy, `Imp` i `Spec`, odpowiednio. Następnie implementację `Imp` uważa się za poprawną, gdy

$$\texttt{Spec} \approx \texttt{Imp}.$$

Oto precyzyjna definicja nowego pojęcia:

Definicja 44 *Relację binarną R pomiędzy procesami nazywamy <u>pre-bisymulacją</u>, jeśli dla każdej pary $(P, Q) \in R$, $\forall \alpha \in \mathrm{Act}$,*

$$(i) \quad P \xrightarrow{\alpha} P' \implies \exists Q' \ \textit{t.że}\ Q \stackrel{\alpha}{\Longrightarrow} Q' \ \textit{i}\ (P', Q') \in R$$

$$(ii) \quad Q \xrightarrow{\alpha} Q' \implies \exists P' \ \textit{t.że}\ (P \xrightarrow{\alpha} P' \ \textit{lub}\ P \xrightarrow{\widehat{\alpha}} P') \ \textit{i}\ (P', Q') \in R.$$

Mówimy, że procesy P, Q są w relacji pre-porządku pre-bisymulacyjnego, ozn. $P \lessapprox Q$, jeśli (P, Q) należy do pewnej pre-bisymulacji.

Ćwiczenie 72 *Pokaż, że relacja $\lessapprox$ jest pre-porządkiem (zwrotna i przechodnia) oraz, że jest zachowana przez wszystkie operatory z wyjątkiem wyboru.*

Oczywiście:

$$\sim \;\subsetneq\; \lessapprox \;\subsetneq\; \approx .$$

A nawet więcej: każda silna bisymulacja jest pre-bisymulacją, a ta jest słabą bisymulacją.
Zaletą pre-bisymulacji w porównaniu do słabej bisymulacji jest to, że pozwala ona zdefiniować *pre-bisymulację z dokładnością do* $\lessapprox$ w taki sposób, by metoda dowodowa oparta na niej była poprawna (względem $\lessapprox$), patrz wniosek 47 poniżej.

Definicja 45 *Relację binarną R pomiędzy procesami nazywamy <u>pre-bisymulacją z dokładnością do $\lessapprox$</u>, jeśli dla każdej pary $(P,Q) \in R$, $\forall \alpha \in \mathrm{Act}$,*

$$(i)\;\; P \xrightarrow{\alpha} P' \implies \exists Q' \text{ t.że } Q \stackrel{\alpha}{\Longrightarrow} Q' \text{ i } (P',Q') \in \;\sim \circ R \circ \lessapprox$$

$$(ii)\;\; Q \xrightarrow{\alpha} Q' \implies \exists P' \text{ t.że } (P \xrightarrow{\alpha} P' \text{ lub } P \xrightarrow{\widehat{\alpha}} P') \text{ i } (P',Q') \in \lessapprox \circ R \circ \lessapprox$$

Lemat 46 *Jeśli R jest pre-bisymulacją z dokładnością do $\lessapprox$, to $\lessapprox \circ R \circ \lessapprox$ jest pre-bisymulacją.*

Ćwiczenie 73 *Udowodnij lemat.*

Wniosek 47 *Jeśli R jest pre-bisymulacją z dokładnością do $\lessapprox$, to $R \subseteq \lessapprox$.*

Ćwiczenie 74 *Czy jeśli $P \approx Q$, to $\mathcal{L}(P) = \mathcal{L}(Q)$? Czy jeśli $P \sim Q$, to $\mathcal{L}(P) = \mathcal{L}(Q)$?*