8 Bisymulacja, logika i gry

8.1 Hierarchia aproksymantów

Definicja 64 *Definiujemy relacje* $\sim_\kappa$ *, dla* κ *przebiegającego liczby porządkowe, następująco:*

- $P \sim_0 Q$ *zawsze*
- $P \sim_{\kappa+1} Q$ *jeśli dla każdego* $t \in \mathrm{Act}^*$,

$$(i) \quad P \xrightarrow{t} P' \implies \exists Q' \ \ t.że \ \ Q \xrightarrow{t} Q' \ \ i \ \ P' \sim_\kappa Q'$$
$$(ii) \quad Q \xrightarrow{t} Q' \implies \exists P' \ \ t.że \ \ P \xrightarrow{t} P' \ \ i \ \ P' \sim_\kappa Q'.$$

- *jeśli* κ *jest graniczną liczbą porządkową, to*

$$\sim_\kappa \ = \bigcap_{\lambda<\kappa} \sim_\lambda .$$

Uwaga 65 *Każda relacją* $\sim_\kappa$ *jest równoważnością.* $\sim_1$ *to dokładnie równość śladów.*

Fakt 66 $\lambda < \kappa \implies \sim_\lambda \ \supseteq \ \sim_\kappa$.

Fakt 67 $\sim \ = \bigcap_\kappa \sim_\kappa$.

Pierwszy fakt wynika natychmiast z monotoniczności operatora definiującego bisymulację, natomiast drugi jest instancją twierdzenia Knastera-Tarskiego o punkcie stałym w kracie zupełnej[3].

Fakt 68 $\sim_0 \ \supsetneq \ \sim_1 \ \supsetneq \ldots$. *Dla* $i \in \omega$, $\sim_i \ \supsetneq \ \sim_\omega$.

Dowód: Definiujemy procesy P_i, Q_i, dla $i \in \omega$, jak następuje:

$$P_0 \equiv b.0 \qquad Q_0 \equiv c.0$$
$$P_{i+1} \equiv a.(P_i + Q_i) \qquad Q_{i+1} \equiv a.P_i + a.Q_i$$

Teraz łatwo jest pokazać indukcyjnie względem i, że

$$P_i \ \sim_i \ Q_i \ \sim_i \ P_i + Q_i$$
$$P_i \ \not\sim_{i+1} \ Q_i \ \not\sim_{i+1} \ P_i + Q_i \ \not\sim_{i+1} \ P_i$$

□

[3]Zakładamy tutaj, że mamy *zbiór* wszystkich procesów.

Ćwiczenie 94 *Dokończ dowód powyższego faktu.*

Fakt 69 $\sim_\omega \supsetneq \sim_{\omega+1}$.

Dowód: Zdefiniujemy procesy R, R' takie, że $R \sim_\omega R'$ ale $R \nsim_{\omega+1} R'$.

$$R_0 \equiv \sum\nolimits_{i\in\{0,1,2,\ldots\}} P_i$$
$$R_1 \equiv Q_0 + \sum\nolimits_{i\in\{1,2,\ldots\}} P_i$$
$$R_1 \equiv Q_0 + Q_1 + \sum\nolimits_{i\in\{2,3,\ldots\}} P_i$$
$$\ldots$$
$$R_\omega \equiv \sum\nolimits_{i\in\omega} Q_i$$

$$R \equiv \sum\nolimits_{i\in\omega} a.R_i$$
$$R' \equiv R + a.R_\omega$$

Teraz wystarczy pokazać kolejno:

- $R_\omega \sim_i R_i$ ale $R_\omega \nsim_{i+1} R_i$, dla $i \in \omega$
- $R \sim_\omega R'$
- $R_\omega \nsim_\omega R_i$, dla $i \in \omega$
- $R \nsim_{\omega+1} R'$.

□

Ćwiczenie 95 *Dokończ dowód powyższego faktu.*

Uwaga 70 *Hierarchię relacji $\sim_\kappa$ oparliśmy na „długich krokach” $\xrightarrow{t}$, dla $t \in \mathrm{Act}^*$. Zauważmy, że rozsądną alternatywą jest oparcie jej na „krótkich krokach”, tj. na tranzycjach $\xrightarrow{\alpha}$, dla $\alpha \in \mathrm{Act}^*$.*

Ćwiczenie 96 *Pojęcie silnej bisymulacji pozostawało takie samo niezależnie od tego, czy formułowaliśmy je przy użyciu „długich” czy też „krótkich kroków”. Czy alternatywna definicja hierarchii $\sim_\kappa$ jest równoważna definicji 64 ?*

Ćwiczenie 97 *Wszystkie powyższe fakty pozostają prawdziwe dla alternatywnej definicji $\sim_\kappa$. Udowodnij fakty 68 i 69.*

W ogólności, $\sim_\kappa$ nie jest równe $\sim$ dla żadnej liczby porządkowej κ. Natomiast przy pewnym rozsądnym założeniu mamy $\sim_\omega \;=\; \sim_{\omega+1}$, a zatem $\sim_\omega \;=\; \sim$.

Definicja 71 *Proces P ma własność skończonego obrazu, jeśli dla każdego $\alpha \in$ Act, zbiór jego α-potomków $\{P' : P \xrightarrow{\alpha} P'\}$ jest skończony.*

Fakt 72 *Jeśli procesy P i Q oraz ich wszyscy potomkowie mają własność skończonego obrazu, to $P \sim_\omega Q \implies P \sim_{\omega+1} Q$.*

Dowód: Wiemy, że $P \sim_\omega Q$, czyli $P \sim_i Q$ dla wszystkich $i \in \omega$.

Załóżmy, że $P \xrightarrow{\alpha} P'$. Zatem, dla każdego i, mamy $Q \xrightarrow{\alpha} Q_i$ i $P' \sim_i Q_i$. Ponieważ na mocy założenia proces Q posiada tylko skończenie wiele α-potomków, co najmniej jeden z nich, powiedzmy Q', jest równy Q_i dla nieskończenie wielu i. Teraz łatwo pokazać, że $P' \sim_\omega Q'$.

Podobnie pokazujemy, że gdy $Q \xrightarrow{\alpha} Q'$, to dla pewnego P' mamy $P \xrightarrow{\alpha} P'$ i $P' \sim_\omega Q'$. Czyli dowiedliśmy $P' \sim_{\omega+1} Q'$. □

Innymi słowy: jeśli w języku pełnym $\mathcal{E}^+$ ograniczymy się do skończonych sum, to $\sim \;=\; \sim_\omega$.

Uwaga 73 *Łatwo wyobrazić sobie hierarchię „słabych" relacji $\approx_\kappa$, aproksymujących słabą równoważność $\approx$. Niestety, dla $\approx_\kappa$ fakt 72 nie zachodzi.*

Ćwiczenie 98 *Przypomnij sobie wszystkie (równoważne) definicje słabej bisymulacji. Na ile „rozsądnych" sposobów potrafisz zdefiniować $\approx_\kappa$? Czy definicje te są równoważne?*

8.2 Logika modalna (Hennessy-Milner logic) a równoważność bisymulacyjna

Definicja 74 (Logika HML$^\sim$ **)** *Składnia formuł logiki* HML$^\sim$ *:*

$$\begin{array}{lll} F \quad ::= \quad \langle\alpha\rangle F & & \alpha \in \text{Act} \\ \quad\quad\;\; \neg F & & \\ \quad\quad\;\; \bigwedge_{i\in I} F_i & & \textit{koniunkcja.} \end{array}$$

Formuła $\langle\alpha\rangle F$ dotyczy procesu (stanu) i mówi, że ma on α-potomka, w którym prawdziwa jest formuła F. Oto precyzyjna semantyka:

Definicja 75

$$
\begin{array}{ll}
P \vDash \langle\alpha\rangle F & \textit{jeśli dla pewnego } P',\ P \xrightarrow{\alpha} P' \ \textit{ i } \ P' \vDash F \\
P \vDash \neg F & \textit{jeśli nie zachodzi } \ P \vDash F \\
P \vDash \bigwedge_{i\in I} F_i & \textit{jeśli dla każdego } i, \ \ P \vDash F_i.
\end{array}
$$

Użyteczne są następujące skróty:

$$
\begin{array}{ll}
\texttt{true} \stackrel{\text{def}}{=} \bigwedge_{i\in\emptyset} F_i & \texttt{false} \stackrel{\text{def}}{=} \neg\texttt{true} \\
F_1 \wedge F_2 \stackrel{\text{def}}{=} \bigwedge_{i\in\{1,2\}} F_i & \bigvee_{i\in \mathrm{I}} F_i \stackrel{\text{def}}{=} \neg\bigwedge_{i\in \mathrm{I}} \neg F_i \\
\langle\alpha_1 \ldots \alpha_k\rangle F \stackrel{\text{def}}{=} \langle\alpha_1\rangle \ldots \langle\alpha_k\rangle F & [\alpha_1 \ldots \alpha_k] F \stackrel{\text{def}}{=} \neg\langle\alpha_1 \ldots \alpha_k\rangle\neg F
\end{array}
$$

Twierdzenie 76 *$P \sim Q$ wtw, gdy $(\forall F \in \mathrm{HML}^{\sim} \ . \ P \vDash F \iff Q \vDash F)$.*

Jest to najważniejsze twierdzenie w tym rozdziale. Mówi ono, że $\mathrm{HML}^{\sim}$ jest logiką charakterystyczną dla silnej równoważności. Istnieje wiele innych logik o tej własności, gdyż twierdzenie to jest prawdziwe dla każdej logiki bogatszej niż $\mathrm{HML}^{\sim}$, która nie potrafi odróżnić systemów silnie równoważnych. Zaletą $\mathrm{HML}^{\sim}$ jest jej prostota. Twierdzenie 76 jest bezpośrednim wnioskiem z twierdzenia 78, które sformułujemy poniżej.

Definicja 77 *Głębokość formuły modalnej definiujemy nastepująco:*

$$
\begin{array}{rcl}
\mathit{depth}(\langle t\rangle F) & = & \mathit{depth}(F) + 1, \quad t \in \mathrm{Act}^* \\
\mathit{depth}(\neg F) & = & \mathit{depth}(F) \\
\mathit{depth}(\bigwedge_{i\in I} F_i) & = & \textit{kres górny zbioru } \ \{\mathit{depth}(F_i) : i \in I\}
\end{array}
$$

W szczególności, $\mathit{depth}(\texttt{true}) = \mathit{depth}(\texttt{false}) = 0$. Niech $\mathrm{HML}^{\sim}_{\kappa}$ oznacza fragment logiki $\mathrm{HML}^{\sim}$ zawierający formuły o głębokości nie większej niż κ:

$$\mathrm{HML}^{\sim}_{\kappa} \stackrel{def}{=} \{F \in \mathrm{HML}^{\sim} \ : \mathit{depth}(F) \leq \kappa\}.$$

Twierdzenie 78 *Dla dowolnej liczby porządkowej κ, $P \sim_{\kappa} Q$ wtw, gdy $(\forall F \in \mathrm{HML}^{\sim}_{\kappa} \ . \ P \vDash F \iff Q \vDash F)$.*

Dowód: Dowód przez indukcję pozaskończoną po κ. Załóżmy tezę dla wszystkich $\lambda < \kappa$.

„$\Rightarrow$": załóżmy, że $P \sim_\kappa Q$ i $P \vDash F$, $\mathrm{depth}(F) \leq \kappa$. Rozpatrzymy tylko przypadek $F \equiv \langle t \rangle F'$; pozostałe przypadki oczywiste. Niech $\lambda := \mathrm{depth}(F')$; oczywiście $\lambda < \kappa$. Ponieważ $P \vDash F$, wiemy, że $P \xrightarrow{t} P'$ dla pewnego P', takiego, że $P' \vDash F'$. Ponieważ $\lambda < \kappa$, na pewno $P \sim_{\lambda+1} Q$. Zatem $Q \xrightarrow{t} Q'$ dla pewnego Q', takiego, że $P' \sim_\lambda Q'$. Z założenia indukcyjnego, $Q' \vDash F'$, a więc $Q \vDash \langle t \rangle F' \equiv F$.

„$\Leftarrow$": załóżmy, że $P \nsim_\kappa Q$. Skonstruujemy formułę $F \in \mathrm{HML}^\sim_\kappa$ odróżniającą P i Q, tzn. taką, że $P \vDash F$ a zarazem $Q \nvDash F$.

a) Załóżmy najpierw, że κ jest następnikiem jakiejś liczby porządkowej, $\kappa = \lambda+1$. Zatem bez utraty ogólności wiemy, że istnieją P' oraz $t \in \mathrm{Act}^*$ takie, że $P \xrightarrow{t} P'$ oraz dla każdego Q', jeśli $Q \xrightarrow{t} Q'$, to $P' \nsim_\lambda Q'$.[4] Niech $\{Q_i : i \in \mathrm{I}\}$ oznacza zbiór wszystkich t-potomków procesu Q. Z założenia indukcyjnego dla każdego i istnieje formuła $F_i \in \mathrm{HML}^\sim_\lambda$ taka, że $P' \vDash F_i$ a zarazem $Q_i \nvDash F_i$. Niech $F := \langle t \rangle \bigwedge_{i \in II} F_i$; $\mathrm{depth}(F) \leq \lambda + 1 = \kappa$. Oczywiście $P \vDash F$, natomiast $Q \nvDash F$.

b) Teraz załóżmy, że κ jest liczbą graniczną. Zatem $P \nsim_\kappa Q$ dla pewnej $\lambda < \kappa$. Z założenia indukcyjnego $P \vDash F$ a zarazem $Q \nvDash F$, dla pewnej formuły $F \in \mathrm{HML}^\sim_\lambda \subseteq \mathrm{HML}^\sim_\kappa$. (zauważmy, że dla odróżnienia P i Q wystarczają już formuły należące do $\bigcup_{\lambda<\kappa} \mathrm{HML}^\sim_\lambda \subsetneq \mathrm{HML}^\sim_\kappa$). □

Ćwiczenie 99 *Czy twierdzenie 78 pozostaje prawdziwe dla alternatywnej definicji $\sim_\kappa$ zaproponowanej w uwadze 70? Jeśli nie, to jak trzeba zmodyfikować definicję 77?*

Ćwiczenie 100 *Uważny Czytelnik zauważył zapewne, że w punkcie b) w dowodzie twierdzenia 78, budując formułę rozróżniającą dwa procesy nie korzystamy wogóle z negacji! Czy negacja jest więc zbędna czy też może w rzeczywistości korzystamy z niej w sposób ukryty?*

Dowód twierdzenia 76: Bezpośredni wniosek z twierdzenia 78 i faktu 67. □

Ćwiczenie 101 *Znajdź najpłytszą formułę F_i odróżniającą procesy P_i i Q_i, dla $i \in \omega$, tzn. taką, że $P_i \vDash F_i$ i zarazem $Q_i \nvDash F_i$.*

Ćwiczenie 102 *Wyobraźmy sobie, że faktycznie rezygnujemy z negacji (por. ćwiczenie 100). Czym należy zastąpić relację $\sim$ w twierdzeniu 76 oraz relację $\sim_\kappa$ w twierdzeniu 78 aby twierdzenia te były znów prawdziwe?*

[4] Albo istnieje Q' oraz t takie, że $Q \xrightarrow{t} Q'$ oraz dla każdego P', jeśli $P \xrightarrow{t} P'$, to $P' \nsim_\lambda Q'$. Przypadek ten pomijamy a jego dowód jest idealnie symetryczny.

Uwaga 79 *Twierdzenia 76 i 78 stosują się do dowolnego systemu tranzycyjnego, gdyż* $\sim_\kappa$ *i relacja spełniania formuł są zdefiniowane tylko przy pomocy relacji tranzycji* $\stackrel{t}{\longrightarrow}$.

Ćwiczenie 103 *Zaproponuj modyfikację* $\mathrm{HML}^{\approx}$ *logiki* $\mathrm{HML}^{\sim}$ *opartą na słabych tranzycjach* $\stackrel{t}{\Longrightarrow}$.

Wniosek 80 *Natychmiastowy wniosek płynący z uwagi 79: obydwa twierdzenia 76 i 78 zachodzą również dla słabej równoważności i (odpowiednio zdefiniowanej) słabej logiki* $\mathrm{HML}^{\approx}$ *oraz dla odpowiednio dobranych słabych aproksymantów* $\approx_\kappa$ *(por. ćwiczenie 98).*

Logika modalna $\mathrm{HML}^{\sim}$ jest infinitarna, zatem niezbyt użyteczna w praktyce. W niektórych przypadkach wystarczy ograniczyć się do fragmentu finitarnego $\mathrm{HML}^{\sim}_{\mathrm{fin}} \subsetneq \mathrm{HML}^{\sim}$, w którym zamiast ogólnej koniunkcji mamy formułę `true` oraz koniunkcję binarną $F_1 \wedge F_2$.

Twierdzenie 81 *Jeśli procesy* P *i* Q *oraz ich wszyscy potomkowie mają własność skończonego obrazu, to* $P \sim Q$ *wtw, gdy* $(\forall F \in \mathrm{HML}^{\sim}_{fin} \,.\, P \vDash F \iff Q \vDash F)$.

Dowód: Wystarczy pokazać tylko jedną implikację „$\Leftarrow$". Załóżmy, że $P \nsim Q$, a więc na mocy faktu 72, $P \nsim_k Q$ dla pewnego $k \in \omega$. Z własności skończonego obrazu wynika, że formuła F rozróżniająca P i Q, którą skonstruowaliśmy w punkcie b) w dowodzie twierdzenia 78, należy do $\mathrm{HML}^{\sim}_{\mathrm{fin}}$. □

8.3 Gry a równoważność bisymulacyjna

Uściślimy teraz nieprecyzyjne dotychczas pojęcie gry bisymulacyjnej pomiędzy Kowalskim a Nowakiem. Przypomnijmy: celem Kowalskiego jest wykazanie, iż dwa procesy są równoważne a celem jego oponenta jest dowiedzenie, iż się różnią.

Załóżmy, ze dany jest system tranzycyjny, składający się ze zbioru procesów (stanów) $\mathcal{P}$ oraz z relacji tranzycji $\stackrel{\alpha}{\longrightarrow}$, dla każdego $\alpha \in \mathrm{Act}$. *Konfiguracjami* gry będą elementy zbioru $V = V_N \cup V_K$, gdzie

$$V_N = \mathcal{P} \times \mathcal{P}$$
$$V_K = \mathcal{P} \times \mathcal{P} \times \mathrm{Act} \times \{\mathrm{l}, \mathrm{r}\}.$$

W konfiguracji należącej do zbioru V_N kolej na ruch Nowaka; w konfiguracji ze zbioru V_K rusza się Kowalski. W konfiguracji $(P, Q) \in V_N$, Nowak może wykonać ruch prowadzący do konfiguracji $(P', Q, \alpha, \mathrm{l}) \in V_K$ pod warunkiem, że $P \stackrel{\alpha}{\longrightarrow} Q$. Symetrycznie, Nowak może wykonać ruch z konfiguracji (P, Q) do $(P, Q', \alpha, \mathrm{r}) \in V_K$ o ile

$Q \xrightarrow{\alpha} Q'$. Jak widać, konfiguracje z V_K zawierają informację o ostatnim ruchu Nowaka, potrzebną Kowalskiemu do wykonania poprawnej odpowiedzi. Kowalski może wykonać ruch z $(P', Q, \alpha, \mathrm{l}) \in V_K$ do $(P', Q') \in V_N$, o ile $Q \xrightarrow{\alpha} Q'$. Symetrycznie, może on wykonać ruch z $(P, Q', \alpha, \mathrm{r})$ do $(P', Q') \in V_N$, o ile $P \xrightarrow{\alpha} P'$. Otrzymujemy w ten sposób relację przejścia $R \subseteq V \times V$, a dokładniej $R \subseteq V_N \times V_K \cup V_K \times V_N$, opisującą wszystkie dozwolone ruchy graczy.

Gra rozpoczyna się w wybranej *konfiguracji początkowej* $v_0 = (P_0, Q_0) \in V_N$. *Rozgrywką* w grze nazywamy dowolny skończony lub nieskończony ciąg konfiguracji $r = v_0 v_1 v_2 \ldots$ taki, że

(i) $(v_i, v_{i+1}) \in R$,

(ii) jeśli ciąg r jest skończony, $r = v_0 v_1 v_2 \ldots v_m$, to nie istnieje $v' \in V$ takie, że $(v_m, v') \in R$ (rozgrywka kończy się tylko wtedy, gdy jeden z graczy nie ma żadnego ruchu).

Jeśli rozgrywka r jest skończona, $r = v_0 v_1 v_2 \ldots v_m$, to przegrywa ten gracz, który powinien wykonać ruch z v_m. W przeciwnym przypadku, tzn. gdy rozgrywka jest nieskończona, wygrywa Kowalski.

Niech $V^* V_K \subseteq V^+$ oznacza zbiór niepustych skończonych ciągów konfiguracji takich, że ostatnia konfiguracja należy do V_K. *Strategia* Kowalskiego to dowolna funkcja częściowa $s : V^* V_K \to V_N$ taka, że jeśli $s(rv) = v'$, to $(v, v') \in R$ (ruch wybrany przez strategię jest zawsze dozwolony). Mówimy, że Kowalski stosuje strategię s w rozgrywce $r = v_0 v_1 \ldots$ jeśli dla każdego v_i, jeśli $v_i \in V_K$ to albo v_i jest ostatnią konfiguracją w r, albo strategia jest określona dla $v_0 \ldots v_i$ i $s(v_0 \ldots v_i) = v_{i+1}$. Podobnie definiujemy strategię Nowaka.

Mówimy, ze strategia s Kowalskiego (Nowaka) jest *wygrywająca* jeśli Kowalski (Nowak) wygrywa każdą rozgrywkę, w której stosuje strategię s.

Twierdzenie 82

(i) $P_0 \sim Q_0$ *wtw, gdy Kowalski ma strategię wygrywającą.*

(ii) $P_0 \nsim Q_0$ *wtw, gdy Nowak ma strategię wygrywającą.*

Ćwiczenie 104 *Dowód twierdzenia pozostawiamy jako ćwiczenie Czytelnikowi.*

Bezpośredni wniosek z twierdzenia 82: gra bisymulacyjna jest zawsze *zdeterminowana*, tzn. dokładnie jeden z graczy ma strategię wygrywającą.

Ćwiczenie 105 *Czy twierdzenie 82 pozostanie prawdziwe, gdy zmienimy definicję rozgrywki usuwając punkt (ii). Umówmy się, że „niedokończona" rozgrywka oznacza poddanie się gracza, którego konfiguracja jest na końcu rozgrywki, a zatem wygraną przeciwnika.*