

7. WYKŁAD 7: NIEROZSTRZYGALNOŚĆ RACHUNKU PREDYKATÓW

Logiki predykatów jest nierozstrzygalna. Dokładniej, nierozstrzygalny jest następujący problem decyzyjny: *Czy dana formuła logiki pierwszego rzędu jest tautologią?* Aby wykazać, że tak jest, posłużymy się nierozstrzygalnością problemu stopu dla **maszyn Turinga**.

Przypomnijmy, że maszyna Turinga jest abstrakcyjnym modelem komputera, składającym się z nieskończonej długiej taśmy podzielonej na pola. Każde pole może znajdować się w jednym z N stanów. Maszyna zawsze jest ustawiona nad jednym z pól i znajduje się w jednym z M stanów. Zależnie od kombinacji stanu maszyny i pola maszyna zapisuje nową wartość w polu, zmienia stan, a następnie może przesunąć się o jedno pole w prawo lub w lewo. Każdą z takich operacji nazywamy **rozkazem**. Maszyna Turinga jest sterowana listą zawierającą dowolną liczbę takich rozkazów. N i M są dowolnymi liczbami skończonymi. Lista rozkazów dla maszyny Turinga może być traktowana jako jej program.

Formalnie, maszynę Turinga nad alfabetem $\mathcal{A}$ definiujemy jako uporządkowaną piątkę $\mathcal{M} = (\Delta, Q, \delta, q_0, q_f)$, gdzie:

- Δ jest skończonym alfabetem, zawierającym $\mathcal{A}$ oraz symbol $B \notin \mathcal{A}$,
- Q jest skończonym zbiorem stanów,
- $q_0 \in Q$ jest stanem początkowym,
- $q_f \in Q$ jest stanem końcowym,
- $\delta : (Q \setminus \{q_f\}) \times \Delta \rightarrow \Delta \times Q \times \{-1, 0, +1\}$ jest funkcją przejścia.

Zakładając, że zbiory Δ i Q są rozłączne, można zdefiniować **konfigurację** maszyny jako słowo postaci wqv , gdzie $q \in Q$ oraz $w, v \in \Delta$, przy czym utożsamiamy konfiguracje wqv i $wqvB$. Interpretacja tej definicji jest następująca: taśma maszyny jest nieskończona w prawo. Na początku taśmy zapisane jest słowo wv , dalej w prawo są same blanki, a głowica maszyny "patrzy" na pierwszy znak na prawo od w . Konfigurację postaci $C_w = q_0w$, gdzie $w \in \mathcal{A}^*$, nazywamy **początkową**, a konfigurację postaci wq_fv nazywamy **kończową** lub **akceptującą**.

Relację $\rightarrow_{\mathcal{M}}$ na konfiguracjach definiujemy następująco:

- Jeśli $\delta(q, a) = (b, p, +1)$ to $wqav \rightarrow_{\mathcal{M}} wbpv$;
- Jeśli $\delta(q, a) = (b, p, 0)$ to $wqav \rightarrow_{\mathcal{M}} wpbv$;
- Jeśli $\delta(q, a) = (b, p, -1)$ to $wcqav \rightarrow_{\mathcal{M}} wpcbv$ oraz $qav \rightarrow_{\mathcal{M}} pbv$ (gdy ruch w lewo jest niemożliwy.)

Symbolem $\twoheadrightarrow_{\mathcal{M}}$ oznaczamy przechodnio-zwrotne domknięcie relacji $\rightarrow_{\mathcal{M}}$. Jeżeli $C_w \twoheadrightarrow_{\mathcal{M}} C'$, gdzie C' jest konfiguracją akceptującą to mówimy, że maszyna akceptuje słowo w .

Problem stopu można równoważnie sformułować następująco: czy dana maszyna Turinga akceptuje słowo puste?

Lemat 20. *Niech ζ oznacza koniunkcję następujących formuł*

- $\forall y \neg P(y, c)$,
- $\forall x \exists y P(x, y)$,
- $\forall x \forall y (P(x, y) \rightarrow R(x, y))$,
- $\forall x \forall y \forall z (R(x, y) \rightarrow (R(y, z) \rightarrow R(x, z)))$,
- $\forall x \neg R(x, x)$.

Formuła ζ jest zdaniem. Zdanie to jest spełnialne, a każdy jego model $\mathfrak{A}$ zawiera nieskończony ciąg różnych elementów $c^{\mathfrak{A}} = a_0, a_1, a_2, \dots$ takich że $(a_i, a_{i+1}) \in P^{\mathfrak{A}}$ dla każdego i .

Dowód pozostawiamy jako ćwiczenie.

Twierdzenie 22. *Nie istnieje algorytm rozstrzygający, czy dana formuła logiki predykatów jest tautologią.*

Dowód. Naszym celem jest efektywna konstrukcja, która dla dowolnej maszyny Turinga $\mathcal{M}$ utworzy formułę $\phi_{\mathcal{M}}$ o następującej własności:

$\mathcal{M}$ akceptuje słowo puste wtedy i tylko wtedy, gdy $\phi_{\mathcal{M}}$ jest tautologią.

Stąd natychmiast wynika teza twierdzenia. W przeciwnym razie taka konstrukcja pozwalałaby bowiem na rozstrzyganie problemu stopu. W istocie, wygodniej będzie skonstruować taką formułę $\phi_{\mathcal{M}}$, że

$\mathcal{M}$ zapętla się na słowie pustym wtedy i tylko wtedy, gdy $\phi_{\mathcal{M}}$ jest spełnialna,

i na koniec przyjąć $\phi_{\mathcal{M}} = \neg\phi_{\mathcal{M}}$. Język, w którym zapiszemy naszą formułę, będzie zależała od maszyny $\mathcal{M}$. Składa się on z:

- jednoargumentowych symboli relacyjnych S_q , dla wszystkich stanów $q \in Q$;
- dwuargumentowych symboli relacyjnych C_a , dla wszystkich symboli $a \in \Delta$;
- dwuargumentowego symbolu relacyjnego G ;
- stałej c i symboli P i Q występujących w formule ζ z Lematu.

Formuła $\phi_{\mathcal{M}}$ jest koniunkcją złożoną z wielu składowych, które teraz opiszemy. Pierwszą składową jest formuła ζ z Lematu. Każdy model tej formuły zawiera różnowartościowy ciąg $a_0, a_1, a_2, \dots$, który posłuży nam jako substytut ciągu liczb naturalnych (o elemencie a_i myślimy jak o liczbie i). Intuicyjny sens formuł atomowych naszej sygnatury jest taki:

- Formułę $S_q(x)$ czytamy: po x krokach obliczenia maszyna jest w stanie q .
- Formułę $G(x, y)$ czytamy: po x krokach głowica maszyny znajduje się w pozycji y .
- Formułę $C_a(x, y)$ czytamy: po x krokach na pozycji y znajduje się symbol a .

Dalsze składowe naszej formuły $\phi_{\mathcal{M}}$ są tak dobrane, aby każdy jej model reprezentował nieskończone obliczenie maszyny zaczynające się od słowa pustego. Oto te składowe:

- (1) $S_{q_0}(c) \wedge G(c, c) \wedge \forall x C_B(c, x)$;
- (2) $\forall x (\bigvee_{q \in Q} S_q(x))$;
- (3) $\forall x (S_q(x) \rightarrow \neg S_p(x))$, dla $q, p \in Q$, $q \neq p$;
- (4) $\forall x \forall y (\bigvee_{a \in \Delta} C_a(x, y))$;
- (5) $\forall x \forall y (C_a(x, y) \rightarrow \neg C_b(x, y))$, dla $a, b \in \Delta$, $a \neq b$;
- (6) $\forall x \exists y G(x, y)$;
- (7) $\forall x \forall y \forall z (G(x, y) \wedge G(x, z) \rightarrow y = z)$;
- (8) $\forall x \forall y \forall z (S_q(x) \wedge G(x, y) \wedge C_a(x, y) \wedge P(x, z) \rightarrow S_p(z) \wedge C_b(z, y))$, gdy $\delta(q, a) = (p, b, i)$;
- (9) $\forall x \forall y \forall z (\neg G(x, y) \wedge C_a(x, y) \wedge P(x, z) \rightarrow C_a(z, y))$;
- (10) $\forall x \forall y \forall z \forall v (S_q(x) \wedge G(x, y) \wedge P(x, z) \wedge P(y, v) \rightarrow G(z, v))$, gdy $\delta(q, a) = (p, b, +1)$;
- (11) $\forall x \forall y \forall z (S_q(x) \wedge G(x, y) \wedge P(x, z) \rightarrow G(z, y))$, gdy $\delta(q, a) = (p, b, 0)$;
- (12) $\forall x \forall y \forall z \forall v (S_q(x) \wedge G(x, y) \wedge P(x, z) \wedge P(v, y) \rightarrow G(z, v))$, gdy $\delta(q, a) = (p, b, -1)$;
- (13) $\forall x \forall y \forall z \forall v (S_q(x) \wedge G(x, c) \wedge P(x, z) \rightarrow G(z, c))$, gdy $\delta(q, a) = (p, b, -1)$;
- (14) $\forall x \neg S_{q_f}(x)$.

Przypuśćmy teraz, że maszyna $\mathcal{M}$ ma nieskończone obliczenie dla pustego słowa wejściowego. Zbudujemy model $\mathfrak{A}$ dla formuły $\phi_{\mathcal{M}}$. Dziedziną tego modelu jest zbiór $\mathbb{N}$ liczb naturalnych. Stałą c interpretujemy jako zero, relacja $P^{\mathfrak{A}}$ to relacja następnika, a $R^{\mathfrak{A}}$ to (ostra) relacja mniejszości. Relacje $S_q^{\mathfrak{A}}$, $C_a^{\mathfrak{A}}$ i $G^{\mathfrak{A}}$ określamy zgodnie z ich intuicyjną interpretacją na podstawie przebiegu nieskończonego obliczenia maszyny. Nietrudno się przekonać, że wszystkie człony koniunkcji są prawdziwe w $\mathfrak{A}$, czyli zdanie $\phi_{\mathcal{M}}$ jest spełnialne.

Przystąpmy więc do trudniejszej części dowodu. Załóżmy mianowicie, że $\mathfrak{A} \models \phi_{\mathcal{M}}$ dla pewnego modelu $\mathfrak{A}$. Wtedy także $\mathfrak{A} \models \zeta$, niech więc a_i będą elementami $\mathfrak{A}$, o których mowa w Lemacie. Model $\mathfrak{A}$ spełnia

też wszystkie pozostałe składowe formuły $\phi_{\mathcal{M}}$. Składowe (2) i (3) gwarantują, że każdy z elementów a_i należy do dokładnie jednej z relacji S_q . Podobnie, każda para (a_i, a_j) należy do dokładnie jednej z relacji C_a , oraz każde a_i jest w relacji G z dokładnie jednym elementem modelu $\mathfrak{A}$ – tu używamy składowych (4)–(7).

Rozpatrzmy obliczenie maszyny $\mathcal{M}$ dla słowa pustego. Pokażemy, że jest to obliczenie nieskończone. Jeśli obliczenie maszyny $\mathcal{M}$ składa się z co najmniej n kroków, to przez q_n oznaczmy stan, w którym znajduje się maszyna $\mathcal{M}$ po wykonaniu tych n kroków, a przez k_n pozycję głowicy w tym momencie. Zawartością m -tej komórki taśmy po n -tym kroku obliczenia niech zaś będzie symbol b_{nm} .

Przez indukcję ze względu na n dowodzimy, że dla dowolnego $n \in \mathbb{N}$ obliczenie składa się z co najmniej n kroków, oraz:

$$a_n \in S_{q_n}^{\mathfrak{A}}, (a_n, a_m) \in C_{b_{nm}}^{\mathfrak{A}}, (a_n, a_{k_n}) \in G^{\mathfrak{A}}.$$

Inaczej mówiąc, model $\mathfrak{A}$ prawidłowo reprezentuje kolejne konfiguracje maszyny. Dla $n = 0$ powyższe związki wynikają wprost z prawdziwości członu (1) naszej koniunkcji. W kroku indukcyjnym skorzystamy przede wszystkim z członu (14), który gwarantuje, że stan q_n nie jest końcowy. Określona jest więc wartość funkcji przejścia $\delta(q_n, b_{mk_n})$. Możemy więc odwołać się do składowych (9–12), które zapewniają poprawną zmianę stanu i symbolu pod głowicą (8), zachowanie bez zmian reszty taśmy (9) i przesunięcie głowicy (10–12). $\square$