Logika Stosowana

Wykład 2 - Logika modalna

Część 3

Marcin Szczuka

Instytut Informatyki UW

Wykład monograficzny, semestr letni 2017/2018

Plan wykładu

Ustalenie relacji konsekwencji

Niech $\mathbb{S}$ będzie formalnym systemem opartym na zbiorze aksjomatów $\mathcal{S}$.

Rodzina modeli prawdziwych

Przez $\mathcal{MOD}(\mathbb{S})$ oznaczamy rodzinę wszystkich modeli, w których $\mathcal{S}$ są przawdziwe (które modelują $\mathcal{S}$).

Poprzednio wykorzystywaliśmy już relację $\models^v_{\mathbb{S}}$.
Możemy ją teraz przedefiniować (równoważnie), by lepiej służyła naszym celom:

Konsekwencja semantyczna w $\mathbb{S}$

Przy poprzednich oznaczeniach:

$$\models^v_{\mathbb{S}} \phi \quad \Leftrightarrow_{def} \quad \forall_{\mathcal{M}\in\mathcal{MOD}(\mathbb{S})} \mathcal{M} \models^v \phi$$

Plan wykładu

Pełność systemu dowodzenia

W dalszych rozważaniach zakładamy, że $\mathbb{S}$ jest ustalonym systemem dowodzenia. Pełność systemu dowodzenia oznacza, że

$$\vdash_{\mathbb{S}} \phi \quad \Leftrightarrow \quad \models^{v}_{\mathbb{S}} \phi$$

Z twierdzenia o poprawności mamy już jedną implikację:

$$\vdash_{\mathbb{S}} \phi \quad \Rightarrow \quad \models^{v}_{\mathbb{S}} \phi$$

Aby pokazać drugą implikację, skonstrujemy specjalny model (v-strukturę) $(\mathcal{C}, \nu) \in \mathcal{MOD}(\mathbb{S})$ zwany *modelem kononicznym* dla $\mathbb{S}$.

Model $(\mathcal{C}_{\mathbb{S}}, \nu_{\mathbb{S}})$ jest w pewnym sensie najbardziej uniwersalnym modelem w $\mathcal{MOD}(\mathbb{S})$.

Własność tę wyrażamy w następnym twierdzeniu.

Twierdzenie o pełności (w modelu kanonicznym)

Dla każdego standardowego systemu wraz z modelem kanonicznym $(\mathcal{C}_{\mathbb{S}}, \nu_{\mathbb{S}})$ i dla każdej formuły ϕ, następujące warunki są równoważne:

(i) $(\mathcal{C}_{\mathbb{S}}, \nu_{\mathbb{S}}) \models^{v} \phi$

(ii) $\vdash_{\mathbb{S}} \phi$

(iii) $\models^{v}_{\mathbb{S}} \phi$

Zauważmy, że implikacja $(ii) \Rightarrow (iii)$ to jest po prostu poprawność systemu dowodzenia.
Implikacja $(iii) \Rightarrow (i)$ jest oczywista, gdyż $(\mathcal{C}, \nu) \in \mathcal{MOD}(\mathbb{S})$.
Zatem główną treścią tego twierdzenia jest implikacja $(i) \Rightarrow (ii)$.

Plan wykładu

Kroki w konstrukcji modelu kanonicznego

Intuicyjnie, zbiór formuł Φ jest sprzeczny względem systemu $\mathcal{S}$ jeśli można wyprowadzić formułę $\bot$ ze zbioru Φ.
Ponieważ WŁASNOŚĆ DEDUKCJI nie zachodzi dla relacji konsekwencji syntaktycznej, definiujemy pojęcie niesprzecznego zbioru formuł modalnych poprzez relację konsekwencji słabego dowodu $\vdash^w_{\mathbb{S}}$:

Definicja – $\mathbb{S}$-niesprzeczność

Zbiór formuł modalnych Φ nazywamy niesprzecznym z $\mathbb{S}$ (lub $\mathbb{S}$–niesprzecznym) jeżeli $\neg[\Phi \vdash^w_{\mathbb{S}} \bot]$ tzn. jeśli nie istnieją formuły $\phi_1, ..., \phi_n \in \Phi$ takie, że

$$\vdash_{\mathbb{S}} \phi_1 \wedge ... \wedge \phi_n \rightarrow \bot$$

Przez $\mathbf{CON}(\mathbb{S})$ oznaczamy zbiór wszystkich $\mathbb{S}$-niesprzecznych zbiorów formuł.

Maksymalnie niesprzeczny zbiór formuł

Definicja – maksymalna $\mathbb{S}$-niesprzeczność

Zbiór formuł modalnych Φ nazywamy maksymalnie niesprzecznym z $\mathbb{S}$ (lub maksymalnie $\mathbb{S}$–niesprzecznym) jeżeli Φ jest $\mathbb{S}$–niesprzeczny i żaden jego właściwy nadzbiór nie jest $\mathbb{S}$–niesprzeczny.
Przez $\mathbf{MAXCON}(\mathbb{S}) \subseteq \mathbf{CON}(\mathbb{S})$ oznaczamy zbiór wszystkich maksymalnie $\mathbb{S}$–niesprzecznych zbiorów.

Zbiór $\mathbf{MAXCON}(\mathbb{S})$ ma kilka ciekawych własności. Po pierwsze, z definicji wynika, że każdy zbiór $\Phi \in \mathbf{MAXCON}(\mathbb{S})$ jest również elementem zbioru $\mathbf{CON}(\mathbb{S})$, oraz dla każdej formuły ϕ mamy

$$\Phi \cup \{\phi\} \in \mathbf{MAXCON}(\mathbb{S}) \Rightarrow \phi \in \Phi$$

Po drugie, z niesprzeczności wynika, że nie istnieje taka formuła ϕ taka, że zarówno ϕ i $\neg\phi$ należą do Φ. Z maksymalności wynika, że dla każdej formuły ϕ, albo ϕ albo $\neg\phi$ musi należeć do Φ.

Własności $\mathbf{MAXCON}(\mathbb{S})$

Poniższe twierdzenie pozwala na swobodne operowanie spójnikami logicznymi (zdaniowymi) w ramach formuł należących do maksymalnie niesperzecznego zbioru formuł.

Twierdzenie – własności $\mathbf{MAXCON}(\mathbb{S})$

Niech $\Phi \in \mathbf{MAXCON}(\mathbb{S})$.
Wiemy wtedy, że $\top \in \Phi$, $\bot \notin \Phi$ oraz:

$$\begin{aligned}
\neg\phi \in \Phi &\Leftrightarrow \phi \notin \Phi \\
\psi \wedge \theta \in \Phi &\Leftrightarrow \psi \in \Phi \text{ i } \theta \in \Phi \\
\psi \vee \theta \in \Phi &\Leftrightarrow \psi \in \Phi \text{ lub } \theta \in \Phi \\
\neg\psi \rightarrow \theta \in \Phi &\Leftrightarrow \psi \notin \Phi \text{ lub } \theta \in \Phi
\end{aligned}$$

Plan wykładu

Nietrywialność $\mathbf{MAXCON}(\mathbb{S})$

Musimy pokazać, że $\mathbf{MAXCON}(\mathbb{S})$ jest niepusty i zawiera dostatecznie dużo zbiorów formuł żeby odróżnić formuły, które powinny być rozróżnialne.

Lemat 1 – istnienie $\mathbf{MAXCON}(\mathbb{S})$

Dla każdego zbioru formuł $\Phi \in \mathbf{CON}(\mathbb{S})$ istnieje $\Sigma \in \mathbf{MAXCON}(\mathbb{S})$ taki, że $\Phi \subseteq \Sigma$.

Dowód: Niech $\{\psi_i : i < \omega\}$ będzie numeracją wszystkich formuł. Definiujemy ciąg zbiorów formuł $\{\Delta_r : r < \omega\}$ następująco:

$$\Delta_0 = \Phi$$

$$\Delta_{r+1} = \begin{cases} \Delta_r \cup \{\phi_r\} & \text{jeśli ten zbiór należy do } \mathbf{CON}(\mathbb{S}), \\ \Delta_r & \text{w przeciwnym przypadku.} \end{cases}$$

Zauważmy, że $\Delta_r \in \mathbf{CON}(\mathbb{S})$ dla wszystkich $r < \omega$, wówczas definiujemy

$$\Sigma = \bigcup \{\Delta_r : r < \omega\} \in \mathbf{CON}(\mathbb{S})$$

Z przeprowadzonej konstrukcji również mamy $\Sigma \in \mathbf{MAXCON}(\mathbb{S})$.

Dostateczność $\mathbf{MAXCON}(\mathbb{S})$

Z Lematu 1 (o istnieniu $\mathbf{MAXCON}(\mathbb{S})$) możemy pokazać, następujący następujący fakt:

Lemat 2

Dla każdego zbioru formuł Ψ i formuły ϕ, mamy równoważność

$$\Psi \vdash^{w}_{\mathbb{S}} \phi \qquad \Leftrightarrow \qquad \forall_{\Sigma \in \mathbf{MAXCON}(\mathbb{S})} \left[\Psi \subseteq \Sigma \Rightarrow \phi \in \Sigma\right]$$

Z lematów 1 i 2 otrzymujemy wniosek:

Wniosek

dla każdej formuły ϕ mamy

$$\vdash_{\mathbb{S}} \phi \qquad \Leftrightarrow \qquad \forall_{\Sigma \in \mathbf{MAXCON}(\mathbb{S})} \left[\phi \in \Sigma\right]$$

Jesteśmy już gotowi do skonstruowania struktury modelu kanonicznego

$$\mathcal{C}_{\mathbb{S}} = (\mathbf{S}, \longrightarrow)$$

Zbiór stanów definiujemy przez $\mathbf{S} = \mathbf{MAXCON}(\mathbb{S})$. Relację przejścia $\longrightarrow$ między stanami $\Sigma, \Lambda \in \mathbf{S}$ określamy następująco:

$$\Sigma \longrightarrow \Lambda \qquad \Leftrightarrow \qquad \forall_{\phi}\ [\Box\phi \in \Sigma \Rightarrow \phi \in \Lambda]$$

Dalej będziemy używać oznaczenia $\Lambda \prec \Sigma$ (czyt.: Λ jest następnikiem Σ) zamiast $\Sigma \longrightarrow \Lambda$.

Wartościowanie kanoniczne $\nu_{\mathbb{S}} : VAR \times \mathbf{S} \to \{0, 1\}$ dla $\mathcal{C}_{\mathbb{S}} = (\mathbf{S}, \longrightarrow)$ definiujemy przez

$$\nu_{\mathbb{S}}(p, \Sigma) = \begin{cases} 1 & \text{jeśli } \ p \in \Sigma, \\ 0 & \text{w przeciwnym przypadku.} \end{cases}$$

dla dowolnej zmiennej $p \in VAR$ i stanu $\Sigma \in \mathbf{S}$.

Własności modelu kanonicznego

Z Lematu 1 (o istnieniu) mamy:

Lemat 3

Dla każdego stanu $\Sigma \in \mathbf{S}$ i każdej formuły ϕ mamy równoważność:

$$\Box\phi \in \Sigma \qquad \Leftrightarrow \qquad \forall_{\Upsilon \prec \Sigma} [\phi \in \Upsilon]$$

Możemy również przez indukcję względem konstrukcji formuły udowodnić następujący lemat.

Lemat 4

Dla każdego stanu $\Sigma \in \mathbf{S}$ i każdej formuły ϕ mamy równoważność:

$$((\mathcal{C}_{\mathbb{S}}, \nu_{\mathbb{S}}), \Sigma) \models \phi \qquad \Leftrightarrow \qquad \phi \in \Sigma$$

Stąd mamy wniosek.

Wniosek

Model kanoniczny $(\mathcal{C}_{\mathbb{S}}, \nu_{\mathbb{S}})$ jest modelem dla $\mathbb{S}$

Plan wykładu

Dowód pełności

Przypomnijmy, że dowód twierdzenia o pełności sprowadziliśmy do dowiedzenia implikacji $(i) \Rightarrow (ii)$, tj.

$$(\mathcal{C}_{\mathbb{S}}, \nu_{\mathbb{S}}) \models^{v} \phi \qquad \Rightarrow \qquad \vdash_{\mathbb{S}} \phi$$

Końcowy krok w dowodzie pełności

Niech ϕ będzie dowolną formułą. Z lematów 1-4 mamy:

$$\begin{aligned} (\mathcal{C}_{\mathbb{S}}, \nu_{\mathbb{S}}) \models^{v} \phi &\Leftrightarrow \forall_{\Sigma \in \mathbf{S}}((\mathcal{C}_{\mathbb{S}}, \nu_{\mathbb{S}}), \Sigma) \models \phi \\ &\Leftrightarrow \forall_{\Sigma \in \mathbf{S}} \phi \in \Sigma \\ &\Leftrightarrow \vdash_{\mathbb{S}} \phi \end{aligned}$$

Co kończy dowód twierdzenia o pełności dla logiki modalnej.

Plan wykładu

Rodziny modeli Kripkego

Niech $\mathcal{MOD}$ będzie rodziną wszystkich modeli Kripkego. Każdy model Kripkego (dla logiki jedno-modalnej) możemy interpretować jak relację na zbiorze stanów. Wyróżniamy pewne modele według własności odpowiadającej im relacji.

Oznaczmy przez:

- $\mathcal{MOD}^r$: rodzinę wszystkich modeli zwrotnych (reflexive)
- $\mathcal{MOD}^s$: rodzinę wszystkich modeli symetrycznych (symmetric)
- $\mathcal{MOD}^t$: rodzinę wszystkich modeli przechodnich (transitive)
- $\mathcal{MOD}^l$: rodzinę wszystkich modeli liniowych (serial)
- $\mathcal{MOD}^e$: rodzinę wszystkich modeli Euklidesowych (Euclidean)

Relacja R jest liniowa (szeregowa) wtw, gdy $\forall_s \exists_t (s,t) \in R$
Relacja R jest Euklidesowa wtw, gdy

$$\forall_{s,t,u}((s,t) \in R \wedge (s,u) \in R \Rightarrow (t,u) \in R)$$

Podrodziny modeli Kripkego

Możemy również używać jednocześnie kilka górnych indeksów, np. $\mathcal{MOD}^{rst}$ oznacza rodzinę wszystkich modeli zwrotnych, symetrycznych i przechodnich (czyli relacji równoważności).
Z własności formuł wyróżnionych (aksjomatów) możemy pokazać, że:

$$
\begin{aligned}
(\mathbb{T}) \quad & \mathcal{MOD}^{r} \subseteq \mathcal{MOD}(\mathbb{T}); \\
(\mathbb{S}4) \quad & \mathcal{MOD}^{rt} \subseteq \mathcal{MOD}(\mathbb{S}4) \\
(\mathbb{S}5) \quad & \mathcal{MOD}^{rts} \subseteq \mathcal{MOD}(\mathbb{S}5) \\
(\mathbb{KD}45) \quad & \mathcal{MOD}^{elt} \subseteq \mathcal{MOD}(\mathbb{KD}45)
\end{aligned}
$$

Niestety, nie wszystkie inkluzje są odwracalne. Np. nie każdy model w $\mathcal{MOD}(\mathbb{S}5)$ musi być relacją równoważności.

Pełność w sensie Kripkego i kanoniczność

Definicja – pełność w sensie Kripkego

Mówimy, że system formalny $\mathbb{S}$ jest pełny w sensie Kripkego jeśli

$$\vdash_{\mathbb{S}} \phi \qquad \Leftrightarrow \qquad \models^{u}_{\mathbb{S}} \phi$$

dla dowolnej formuły ϕ

Definicja – system kanoniczny

Mówimy, że system formalny $\mathbb{S}$ jest kanoniczny jeśli jego model kanoniczny $\mathcal{C}_{\mathbb{S}}$ jest strukturalnym modelem dla $\mathbb{S}$.

Zachodzi następujące twierdzenie (bez dowodu):

Twierdzenie

Każdy kanoniczny system jest pełny w sensie Kripkego

Przykładami systemów kanonicznych są $\mathbb{K}$, $\mathbb{KD}$ i $\mathbb{KR}$.

Plan wykładu

Rozstrzygalność systemu formalnego

Będziemy rozpatrywać problemy dowodliwości, spełnialności i prawdziwości formuł modalnych w danym systemie formalnym.

Pokażemy, że problem badania prawdziwości formuł modalnych w zadanym systemie formalnym jest roztrzygalny tzn., że dla każdego systemu dowodzenia $\mathbb{S}$ istnieje algorytm $\mathcal{A}_{\mathbb{S}}$, który dla każdej formuły ϕ sprawdza w czasie skończonym czy ϕ jest poprawna/prawidłowa (valid) w $\mathbb{S}$.

Formuła ϕ jest poprawna/prawidłowa (valid) w klasie modeli (struktur) Kripkego jeśli jest prawdziwa we wszystkich stanach wszystkich modeli (struktur) z tej klasy.

Długość formuły

Dana jest formuła modalna ψ. Intuicyjnie, długość formuły ψ (oznaczona przez $|\psi|$) jest liczbą symboli logicznych wystepujących w ψ.
Formalnie, długość formuły możemy definiowac rekurencyjnie względem budowy formuły:

Definicja – długość formuły

$$\begin{aligned} |p| &= 1 \qquad \text{dla } p \in VAR \\ |\neg\psi| &= |\psi| + 1 \\ |\psi \wedge \phi| &= |\psi \vee \phi| = |\psi \to \phi| = |\psi| + |\phi| + 1 \\ |\Box\psi| &= |\Diamond\psi| = |\psi| + 1 \end{aligned}$$

Na przykład dla formuły

$$\psi = \Box(p \to \Box(q \vee \neg r)) \wedge \neg r$$

mamy $|\psi| = 11$.

Podformuły

Pojęcie podformuły też można definiować rekurencyjnie:

Definicja – podformuły

Formułę ϕ nazywamy podformułą formuły ψ wtedy i tylko wtedy, gdy spełnia jeden z następujących warunków:

- $\phi = \psi$;
- $\psi = \neg\theta$ i ϕ jest podformułą θ;
- $\psi = \psi_1 \odot \psi_2$ (gdzie $\odot \in \{\vee, \wedge, \rightarrow\}$) i ϕ jest albo podformułą ψ_1 lub podformułą ϕ_2;
- $\psi = \Box\theta$ i ϕ jest podformułą θ;

Zbiór wszystkich podformuł ψ oznaczamy przez $Sub(\psi)$

Na przykład dla formuły ψ z poprzedniego slajdu mamy

$$Sub(\psi) = \{p, q, r, \neg r, q \vee \neg r, \Box(q \vee \neg r), p \rightarrow \Box(q \vee \neg r), \Box(p \rightarrow \Box(q \vee \neg r)), \psi\}$$

Podformuły – własności

Następny lemat jest ważny dla dalszych rozważań.

Lemat – własności podformuł

Dla każdej formuły ψ zachodzi nierówność

$$|Sub(\psi)| \leq |\psi|$$

Twierdzenie o roztrzygalności, sprowadzimy do udowodnienia dwóch ważnych kroków (twierdzeń pomocniczych):

1. Pokażemy, że koszt sprawdzenia prawdziwości (model-checking) formuły w strukturze Kripkego zależy od długości formuły i wielkości struktury.
2. Pokażemy, że istnieje skończony model Kripkego, który na mocy pkt. 1 pozwoli na sprawdzanie poprawności w sposób algorytmiczny w czasie skończonym.

Twierdzenie – koszt weryfikacji

Dla każdej struktury $(\mathcal{K}, val, s)$ i formuły ψ, relację

$$(\mathcal{K}, val, s) \models \psi$$

można sprawdzić w czasie $O(|\psi| \cdot |\mathcal{K}|^2)$

Dowód: Uporządkujemy podformuły ψ według ich długości:

$$Sub(\psi) = \{\phi_1, \phi_2, ..., \phi_k\}$$

w ten sposób, by zachodziło $i < j$ gdy ϕ_i jest podformułą ϕ_j.
Po kolei, dla $i = 1, 2, ...$, sprawdzamy relację $(\mathcal{K}, val, s) \models \phi_i$ dla wszystkich stanów s w $\mathcal{K}$. Dla każdej ustalonej formuły ϕ_i, czas sprawdzeń dla wszystkich stanów wynosi $O(|\mathcal{K}|^2)$.

Q.E.D.

Plan wykładu

Własność skończonego modelu

Dla uzyskania rozstrzygalności musimy jeszcze pokazać, że w oszacowaniu występującym w poprzednim twierdzeniu czynnik $|\mathcal{K}|$ jest skończony.

Twierdzenie, które o tym mówi nosi nazwę *własności skończonego modelu*.

Ogólnie, dowolny system formalny (logika) $\mathbb{L}$ ma własność skończonego modelu (**fmp** - finite model property), jeśli istnieje taka rodzina modeli $\mathcal{M}$ dla $\mathbb{L}$, że jeśli formuła ψ nie może być wyprowadzona z $\mathbb{L}$ to istnieje skończony model w rodzinie $\mathcal{M}$ w którym ψ jest fałszywe.

Własnośc ta zachodzi dla logik monomodalnych i wielomodalnych.

Twierdzenie – własność skończonego modelu

Jeśli formuła ψ jest niesprzeczna w systemie dowodzenia $\mathbb{S}$ to istnieje model $\mathcal{K}$ dla $\mathbb{S}$ o niewięcej niż $2^{|\psi|}$ stanach taki, że:

$$\mathcal{K} \models_{\mathbb{S}} \psi$$

Własność skończonego modelu – dowód

Przez $Sub^*(\psi)$ oznaczamy zbiór wszystkich podformuł ψ i ich negacji tzn.:

$$Sub^*(\psi) = Sub(\psi) \cup \{\neg\phi : \phi \in Sub(\psi)\}$$

Podobnie jak w przypadku twierdzenia o pełności, rozpatrywamy pewne podzbiory formuł $\Sigma \in Sub^*(\psi)$, które są niesprzeczne (tzn. $\Sigma \nvdash_{\mathbb{S}} \bot$). Niech $\mathbf{MAXCON}(\psi)$ będzie rodziną *maksymalnie niesprzecznych zbiorów formuł* z $Sub^*(\psi)$. Konstrujemy model Kripkego $\mathcal{K} = (\mathbf{S}, \longrightarrow)$. Zbiór stanów definiujemy przez $\mathbf{S} = \{s_\Sigma : \Sigma \in \mathbf{MAXCON}(\psi)\}$. Relację przejścia $\longrightarrow$ między stanami $s_\Sigma, s_\Lambda \in \mathbf{S}$ określamy następująco:

$$s_\Sigma \longrightarrow s_\Lambda \qquad \Leftrightarrow \qquad \forall_\theta \ [\Box\theta \in \Sigma \Rightarrow \theta \in \Lambda]$$

dla dowolnej zmiennej $p \in Sub(\phi)$ i stanu $\Sigma \in \mathbf{S}$, wartościowanie val definiujemy przez

$$val(p, \Sigma) = \begin{cases} 1 & \text{jeśli } \ p \in \Sigma, \\ 0 & \text{w przeciwnym przypadku.} \end{cases}$$

Własność skończonego modelu – dowód

Pokażemy, że dla każdej formuły $\phi \in Sub(\psi)$ mamy

$$\mathcal{K}, s_\Sigma \models_{\mathbb{S}} \phi \qquad \Leftrightarrow \qquad \phi \in \Sigma \tag{1}$$

Pokażemy to przez indukcję. Jeśli $\phi = p$ jest zmienną to (1) jest prawdziwe z definicji wartościowania. Jeśli $\phi = \neg\phi_1$ lub $\phi = \phi_1 \odot \phi_2$ dla $\odot \in \{\wedge, \vee, \rightarrow, ..\}$, to (1) też jest prawdziwe.

Rozpatrujemy przypadek, gdy $\phi = \Box\theta$ i $\phi \in \Sigma$.
Pokażemy, że $(\mathcal{K}, s_\Sigma) \models_{\mathbb{S}} \phi$.
Istotnie, niech $s_{\Lambda_1}, ..., s_{\Lambda_k}$ będą następnikami wierzchołka s_Σ w modelu $\mathcal{K}$, wówczas formuła θ musi należeć do zbiorów $\Lambda_1, ..., \Lambda_k$.
Z założenia indukcyjnego mamy
$(\mathcal{K}, s_{\Lambda_1}) \models_{\mathbb{S}} \theta$ i $(\mathcal{K}, s_{\Lambda_2}) \models_{\mathbb{S}} \theta$, ..., $(\mathcal{K}, s_{\Lambda_1}) \models_{\mathbb{S}} \theta$.

Czyli $\mathcal{K}, s_\Sigma \models \phi$.

Własność skończonego modelu – dowód

Z drugiej strony, niech $\phi = \Box\theta$ i $(\mathcal{K}, s_\Sigma) \models_{\mathbb{S}} \phi$. Niech $\Sigma/\Box = \{\theta : \Box\theta \in \Sigma\}$. Wówczas możemy pokazać, że $(\Sigma/\Box) \cup \{\neg\theta\}$ musi być sprzecznym zbiorem formuł, bo w przeciwnym przypadku, istniałoby rozszerzenie $(\Sigma/\Box) \cup \{\neg\theta\} \subseteq \Lambda \in \mathbf{MAXCON}$. Stan s_Λ jest następnikiem stanu s_Σ według definicji i z założenia indukcyjnego mamy $(\mathcal{K}, s_\Lambda) \models_{\mathbb{S}} \neg\theta$ co jest sprzeczne z tym, że $(\mathcal{K}, s_\Sigma) \models_{\mathbb{S}} \phi$. Skoro $(\Sigma/\Box) \cup \{\neg\theta\}$ jest sprzecznym zbiorem, to istnieją formuły $\phi_1, ...\phi_k \in \Sigma/\Box$ takie, że $\mathbb{S}, \phi_1, ..., \phi_k, \neg\theta \vdash \bot$, czyli

$$\mathbb{S} \vdash \phi_1 \wedge ... \wedge \phi_k \to \theta$$

Stosując regułę wymuszania mamy:

$$\mathbb{S} \vdash \Box(\phi_1 \wedge ... \wedge \phi_k \to \theta)$$

czyli

$$\mathbb{S} \vdash \Box\phi_1 \wedge ... \wedge \Box\phi_k \to \Box\theta$$

Skoro $\Box\phi_1, ..., \Box\phi_k \in \Sigma$ to $\Box\theta$ też musi należeć do Σ.

Q.E.D.

Plan wykładu

Złożoność spełnialności modalnej

W tej części zajmiemy się ustaleniem, jaki jest (pesymistyczny) koszt algorytmicznego sprawdzania spełnialności (satisfiability) w jednomodalnej logice zdaniowej.
Skoncentrujemy się na pokazaniu, że spełnialność w logice jednomodalnej $\mathbb{S}5$ jest problemem $\mathbb{NP}$-zupełnym.
Ogólnie, o złożoności logik modalnych wiemy, że:

$\mathbb{NP}$-zupełny	$\mathbb{S}5_1, \mathbb{KD}45_1$
$PSPACE$-zupełny	$\mathbb{K}_n, \mathbb{T}_n, \mathbb{S}4_n$ dla $n \geq 1$ $\mathbb{S}5_n, \mathbb{KD}45_n$ dla $n \geq 2$

Wiemy też, że weryfikacja w każdym nietrywialnym, zdaniowym systemie modalnym jest co najmniej tak trudna jak $\mathbb{NP}$ ($\mathbb{NP}$-trudna). To wynika z faktu, że jest nie łatwiejsza od spełnialności w rachunku zdań (SAT), które to zadanie jest $\mathbb{NP}$-zupełne.

$\mathbb{NP}$-zupełność spełnialności modalnej

Będziemy pokazywać $\mathbb{NP}$-zupełność zadania SAT($\mathbb{S}5$). W tym celu musimy wykonać dwa kroki:

1. Pokazać, że SAT($\mathbb{S}5$) jest $\mathbb{NP}$-trudne. To już ustaliliśmy na poprzednim slajdzie.
2. Pokazać, że SAT($\mathbb{S}5$)$\in \mathbb{NP}$.

Aby pokazać, że SAT($\mathbb{S}5$)$\in \mathbb{NP}$ skorzystamy z modyfikacji wcześniej pokazanego twierdzenia o modelu skończonym. Pokażemy, że dla $\mathbb{S}5$ można zawsze znaleźć skończony model o dostatecznie małym rozmiarze. Następnie pokażemy, że taki mały model pozwala na weryfikację spełnialności wewnątrz klasy $\mathbb{NP}$.

Twierdzenie o małym modelu $\mathbb{S}5$

Formuła ϕ w sytemie $\mathbb{S}5$ jest spełnialna wtedy i tylko wtedy gdy jest spełnialna w strukturze $\mathcal{K} \in \mathcal{MOD}^{rts}$ o co najwyżej $|\phi|$ stanach.

NP-zupełność dla $\mathbb{S}5$

Twierdzenie o NP-zupełności $\mathbb{S}5$

Problem spełnialności w sytemie $\mathbb{S}5$ jest $\mathbb{NP}$-zupełny.

Dowód (nieformalny szkic): Jak już wcześniej zauważyliśmy, spełnialność w $\mathbb{S}5$ jest $\mathbb{NP}$-trudna.
Musimy pokazać algorytm który sprawdza spełnialność w $\mathbb{S}5$ i jest w $\mathbb{NP}$.
Ponieważ nasz algorytm ma z założenia działać na maszynie niedeterministycznej, dla badanej fromuły ϕ postępujemy następująco:

1. **Zgadujemy** strukturę $M \in \mathcal{MOD}^{rts}$ o co najwyżej $|\phi| = m$ stanach (istnieje z poprzedniego twierdzenia).
2. **Sprawdzamy** że ϕ jest spełniona w pewnym stanie w M.

Krok 1 powyżej wymaga co najwyżej $O(m^2)$ kroków (bez dowodu).
Krok 2, zgodnie z twierdzeniem o koszcie weryfikacji wymaga co najwyżej $O(|\phi| \cdot |M|^2)$ kroków, czyli $O(m \cdot m^2)$.
Zatem mamy algorytm o pesymistycznym, niedeterministycznym koszcie wielomianowym ($O(m^3)$). Zatem weryfikacja jest w $\mathbb{NP}$.