Úplnost a složitost

Co dělá uvažování o znalostech složitým

Formální systém k sémantice modální logiky agentů zavedeme bez speciálních požadavků na relace K.

Příklad, kdy nemusí platit reflexivita.

Není těžké si představit agenta, který odmítá připustit některé stavy jako možné, i když jeho informace je nevylučují.

Otec Jan si odmítá připustit, že jeho syn Omar bere drogy i když je Omar bere. Tím zmenší množinu možných stavů na ty, ve kterých Omar drogy nebere a může tvrdit, že „ví“ , že Omar není na drogách.

Jeho relace K není reflexivní: ve světě s , ve kterém Omar drogy bere, Jan nepovažuje s za možný.

Příklad, kdy nemusí platit symetrie.

Ve stavu s Janova manželka Hana je na návštěvě u své přítelkyně Anny a řekla o tom Janovi. Ten na to zapomněl a považuje za možný svět t, kdy mu Hana řekla, že jde navštívit svého bratra Roberta.

Kdyby Hana opravdu řekla, že jde navštívit Roberta, Jan by si to zapamatoval, protože nemá R. rád.

Tedy ve stavu t nepovažuje svět s za možný, protože si pamatuje, že H. řekla, že jde navštívit R. místo A.

{Při malé introspekci by si J. ve stavu t mohl uvědomit, že t není možný, kdyby si vzpomněl, co mu H. vlastně řekla. Ale málokdo takovou introspekci udělá.}

Jazyk.

Φ množina prvotních formulí

$L_n(\Phi)$ množina formulí, která vznikne uzavřením Φ na logické spojky konjunkce a negace a na modální operátory $K_1, \ldots, K_n$

$L_n^C(\Phi)$ $L_n^D(\Phi)$ množiny, které vzniknou z $L_n(\Phi)$ uzavřením na operátory E_G, C_G a D_G .

Struktury.

$M_n(\Phi)$ třída Kripkeho struktur pro n agentů nad Φ bez jakýchkoliv předpokladů o relacích K_i.

Podtřídy.

$M_n^r(\Phi)$ třída Kripkeho struktur s reflexivními relacemi K_i

$M_n^{rt}(\Phi)$ třída Kripkeho struktur s reflexivními a tranzitivními relacemi K_i

$M_n^{rst}(\Phi)$ třída Kripkeho struktur s reflexivními, symetrickými a tranzitivními relacemi K_i

Definice.

(i) Říkáme, že *binární relace* K na množině S *je Eukleidovská*, jestliže pro všechna s, t, u z S

$$(s,t) \in K \text{ a } (s,u) \in K \text{ implikuje } (t,u) \in K$$

(ii) K *je seriální*, jestliže pro každé s z S existuje t,

$$(s,t) \in K$$

Lemma.

(i) Je-li K *reflexivní a Eukleidovská relace,* potom K je symetrická a transitivní.

(ii) Je-li K symetrická a transitivní , potom je Eukleidovská.

(iii) Následující tvrzení jsou ekvivalentní

(a) K je reflexivní, symetrická a transitivní .

(b) K je symetrická, transitivní a seriální .

(c) K je reflexivní a Eukleidovská .

(iv) Je-li K relace seriální, symetrická a tranzitivní, potom je K i reflexivní, tedy je relací ekvivalence.

Důkaz.

Nechť K je binární relace na množině S.

(i) Předpokládejme, že K je reflexivní a Eukleidovská, ukážeme, že K je také symetrická a transitivní.

a) důkaz symetrie. Nechť pro libovolné s, t in S platí $(s, t)\ \varepsilon\ K$. Z reflexivity dostáváme $(s, s)\ \varepsilon\ K$, odkud také $(t, s)\ \varepsilon\ K$, protože K je Eukleidovská relace.

Celkem $(s, t)\ \varepsilon\ K$ -> $(t, s)\ \varepsilon\ K$ a K je symetrická relace.

b) transitivita. Nechť $(s, t)\ \varepsilon\ K$ a $(t, u)\ \varepsilon\ K$. Ze symetrie také $(t, s)\ \varepsilon\ K$. Protože K je Eukleidovská relace, dostáváme $(s, u)\ \varepsilon\ K$, tedy K je transitivní.

(ii) Nechť K je symetrická a transitivní relace, nechť pro libovolné s, t, u platí $(s, t) \varepsilon K$ a $(s, u) \varepsilon K$. Ze symetrie dostáváme $(t, s) \varepsilon K$ a z transitivity $(t, u) \varepsilon K$. Tedy K je Eukleidovská.

(iii) Nejprve dokážeme (a) -> (b). Nechť K je reflexivní, symetrická a transitivní a nechť s je libovolný prvek S. Z reflexivity dostáváme $(s, s) \varepsilon K$, tedy existuje prvek t takový, že $(s, t) \varepsilon K$. Relace K je seriální (a podle předpokladu také symetrická a transitivní.

(b) -> (c) Předpokládejme, že K je seriální, symetrická a transitivní. Dokážeme, že K je reflexivní a Eukleidovská.

c1) reflexivnost Nechť s je libovolný prvek S. Protože K je seriální, existuje t, takové, že $(s, t) \varepsilon K$.

Ze symetrie dostáváme $(t, s) \varepsilon K$ a z transitivity $(s, s) \varepsilon K$. Relace K je tedy reflexivní.

c2) Ukážeme, že K je Eukleidovská. Nechť s, t, u jsou libovolné prvky takové, že $(s, t) \varepsilon K$, $(s, u) \varepsilon K$. Ze symetrie potom také $(t, s) \varepsilon K$ a z transitivity $(t, u) \varepsilon K$. Tedy K je Eukleidovská.

(c) -> (a) Předpokládejme, že K je reflexivní a Eukleidovská relace. Je třeba dokázat, že je také symetrická a transitivní .

a1) symetrie Nechť $(s, t) \varepsilon K$. Z reflexivity také $(s, s) \varepsilon K$ a $(t, s) \varepsilon K$, protože K je Eukleidovská.

a2) transitivita Nechť s, t, u jsou libovolné prvky takové, že $(s, t) \varepsilon K$, $(t, u) \varepsilon K$. Ze symetrie potom $(t, s) \varepsilon K$ a $(s, u) \varepsilon K$, protože K je Eukleidovská.

(iv) Předpokládejme, že K je seriální, symetrická a transitivní. Ukážeme, že je také reflexivní, tedy že je to relace ekvivalence.

Nechť s je libovolný prvek S. Protože K je seriální, existuje t, takové že $(s, t) \varepsilon K$. Ze symetrie pak $(t, s) \varepsilon K$ a z transitivity $(s, s) \varepsilon K$. Relace K je reflexivní, tedy je to relace ekvialence.

Označení.

$$M_n, M_n^r, M_n^{rt}, M_n^{rst}, M_n^{rel}, M_n^{sst},$$

označují třídy Kripkeho struktur pro n agentů

- s reflexivními relacemi K_i
- s reflexivními a tranzitivními relacemi K_i
- s reflexivními, symetrickými a tranzitivními relacemi K_i
- s reflexivními a Eukleidovskými relacemi K_i
- se seriálními, symetrickými a transitivními relacemi K_i

Podle předchozího lemmatu pro vztahy mezi těmito třídami platí

$$M_n \supset M_n^{r} \supset M_n^{rt} \supset M_n^{rst} = M_n^{rel} = M_n^{sst}$$

Definice. (formule validní ve třídě Kripkeho struktur)

Nechť $\boldsymbol{M}_n$ je třída Kripkeho struktur pro n agentů. Říkáme, že formule A je validní ve třídě $\boldsymbol{M}_n$, je-li validní v každé struktuře M_n ze třídy $\boldsymbol{M}_n$.

Poznámka. Snadno se nahlédne, že ve větší třídě struktur je méně validních formulí.

Věta.

Pro všechny formule A, B jazyka L_n, struktury M_n ze třídy $\boldsymbol{M}_n$ a agenty $i = 1, 2, \ldots, n$ platí

(i) je-li A instancí nějaké výrokové tautologie, potom $M_n \models A$.

(ii) je-li $M \models A$ a $M \models A \rightarrow B$, potom $M \models B$.

(iii) $M_n \models (K_i A \wedge K_i(A \rightarrow B)) \rightarrow K_i B$.

(iv) je-li $M \models A$, potom $M \models K_i A$.

V Kripkeho strukturách jsme ověřili, že validní jsou

- A1 Všechny instance výrokových tautologií
- A2 Distribuční axiom D
- Pravidlo Modus ponens
- Pravidlo generalizace znalostí

První a druhé schema axiomů jsme ověřili bez jakýchkoli předpokladů o relacích K_i, stejně jako odvozovací pravidla modus ponens a pravidlo generalizace.

První axiomatický systém $\mathbf{K}_n$

A1. Všechny instance tautologií výrokové logiky

A2. $(K_i A \wedge K_i(A \rightarrow B)) \rightarrow K_i B) \quad i = 1, \ldots, n$

(Distribuční axiom)

R1. Z A a $A \rightarrow B$ odvoď B (modus ponens)

R2. Z A odvoď $K_i A$ (Generalizace znalostí)

Systém $\mathbf{K}_n$ má dvě schemata axiomů a dvě odvozovací pravidla.

Jak vypadá důkaz formule $K_i(A \wedge B) \to K_i A$ v $\mathbf{K}_n$?

1. $(A \wedge B) \to A$ (A1)

2. $K_i((A \wedge B) \to A)$ (R2)

3. $(K_i(A \wedge B) \wedge K_i((A \wedge B) \to A)) \to K_i\mathrm{A}$ (A2)

4. $(3) \to (K_i((A \wedge B) \to A) \to (K_i(A \wedge B) \to K_i A))$

{instance tautologie} (A1)

$((p_1 \wedge p_2) \to p_3) \to (p_2 \to (p_1 \to p_3)))$

5. $(K_i((A \wedge B) \to A) \to (K_i(A \wedge B) \to K_i A))$ (3.4. MP)

6. $(K_i(A \wedge B) \to K_i A))$ (2.5. MP)

Ke zkrácení důkazů nemůžeme použít větu o dedukci, ta v našem formálním systému neplatí.

Příklad.

$$p \vdash K_i p \qquad \text{(Pravidlo generalizace)}$$

Ale $$\nvdash p \rightarrow K_i p \qquad (1)$$

ve struktuře

$$M = (\{s, t\}, \{p\}, \pi(p)(s) = true, \pi(p)(t) = false\ K_i = \{(s, t)\})$$

$$(M, s) \models p \quad (M, t) \not\models p$$

$$(M, s) \not\models K_1 p$$

není formule (1) pravdivá.

Z dosavadních výsledků plyne věta o korektnosti pro axiomatický systém $\mathbf{K}_n$.

Věta o korektnosti .

Nechť $M_n(\Phi)$ je třída Kripkeho struktur pro n agentů a nechť $M \in M_n(\Phi)$. Jsou-li A, B libovolné formule jazyka $L_n(\Phi)$, potom

$$\mathbf{K}_n \vdash A \quad \text{implikuje} \quad M \models A$$

tedy

$$\mathbf{K}_n \vdash A \quad \text{implikuje} \quad M_n(\Phi) \models A$$

Důkaz. Ukázali jsme, že v uvedené třídě struktur jsou validní všechny axiomy $\mathbf{K}_n$ včetně obou odvozovacích pravidel.

Zbývá dokázat Větu o úplnosti pro systém axiomů $\mathbf{K}_n$

Věta o úplnosti pro systém axiomů $\mathbf{K}_n$ ukazuje, že tento systém axiomů plně charakterizuje třídu struktur M_n, to znamená, že každá validní formule v M_n je dokazatelná v $\mathbf{K}_n$.

Věta o korektnosti dává prvni polovinu věty o úplnosti. Ukazuje, že každá formule, která je dokazatelná v $\mathbf{K}_n$ je validní, tedy platí ve všech strukturách třídy M_n. Opačnou implikaci nebudeme zatím dokazovat.

Věta (o úplnosti).

Axiomatický systém $\mathbf{K}_n$ je korektní a úplný (pro formule jazyka L_n) vzhledem ke třídě Kripkeho struktur M_n .

Idea důkazu. Korektnost jsme již dokázali. K důkazu věty o úplnosti stačí tedy dokázat , že

každá validní formule jazyka L_n je dokazatelná v $\mathbf{K}_n$. (1)

Tvrzení (1) je důsledkem následujícího tvrzeni:

každá $\mathbf{K}_n$-konzistentní formule A z L_n je splnitelná v M_n (2)

Poznámka.

Tvrzení (2) znamená, že ke každé $\mathbf{K}_n$-konzistentní formuli A jazyka L_n existuje ve třídě M_n Kripkeho struktura, která je modelem A.

Toto tvrzení můžeme považovat za druhé tvrzení Věty o úplnosti.

Analogie s predikátovou logikou je zřejmá.

Dříve než se budeme věnovat větě o úplnosti zavedeme některé užitečné definice.

Definice. (Konzistence formule s množinou axiomů)

(i) Je-li AX množina axiomů a A je formule, říkáme, že formule A je konzistentní s množinou AX, jestliže ¬A není dokazatelné z AX.

(ii) Konečná množina formulí $\{A_1, \ldots, A_n\}$ je konzistentní s množinou formulí AX, je-li s ní konzistentní formule $A_1 \wedge \ldots \wedge A_n$.

(iii) Nekonečná množina formulí F je konzistentní s AX, je-li každá konečná podmnožina $\{A_1, \ldots, A_n\}$ množiny F konzistentní s AX.

Poznámka.

Z tvrzení (2) plyne tvrzení (1). K důkazu věty o úplnosti tedy stačí dokázat tvrzení (2).

Předpokládejme, že platí (2) a že A je $\mathbf{K}_n$-konzistentní formule z L_n. Kdyby A nebyla dokazatelná v $\mathbf{K}_n$, potom ani formule $\neg\neg A$ není dokazatelná v $\mathbf{K}_n$, takže formule $\neg A$ je $\mathbf{K}_n$-konzistentní. Z (2) potom plyne, že $\neg A$ je splnitelná ve třídě M_n, a to je ve sporu s předpokladem validity formule A.

Důkaz Věty o úplnosti.

Podle předchozí poznámky stačí dokázat tvrzení (2).

Idea důkazu. Je-li A $\mathbf{K}_n$-konzistentní formule z L_n, tvrzení (2) se dokazuje sestrojením kanonické struktury M ve třídě M_n, ve které je formule A pravdivá. (tento důkaz celý neprovádíme).

Podobně jako v predikátové logice důležitým krokem k důkazu věty o úplnosti je obdoba Lindenbaumovy věty, která zaručuje rozšíření bezesporné množiny formulí do maximální bezesporné množiny formulí, která je úplná teorie.

Lemma. (o maximální množině formulí)

Nechť L je jazyk, který je spočetný a obsahuje výrokové spojky a AX je bezesporná množina formulí jazyka L, která obsahuje každou instanci schematu A1 a každou instanci odvozovacího pravidla R1.

Potom lze každou množinu formulí $\boldsymbol{F}$, která je bezesporná s AX rozšířit do maximální množiny $\boldsymbol{F}'$ bezesporné s AX.

Idea důkazu. Postupujeme jako ve výrokové logice, seřadíme formule jazyka L do posloupnosti $A_1, \ldots, A_n \ldots$ a konstruujeme množiny

$$F \equiv F_0 \subseteq F_1 \subseteq \ldots \subseteq F_n \subseteq F_{n+1} \subseteq \ldots$$

tak, že formuli A_n přidáme k F_n jen v případě, že je s množinou F_n bezesporná. Tak vznikne množina F_{n+1} .

Položíme

$$F' = \bigcup F_n \qquad (1)$$

a ukážeme, že F' je maximální AX - bezesporná množina.

• AX-bezespornost: Kdyby množina F' byla AX-sporná z definice AX-bezespornosti plyne, že existuje konečná množina $F'' = \{A_1, \ldots, A_k\}$ formulí z F', která je AX-sporná. Potom z definice F' je F'' podmnožinou některé z množin F_n, která je podle konstrukce AX-bezesporná.

• maximálnost: Kdyby F' nebyla maximální AX-bezesporná množina, potom existuje AX-bezesporná formule A, která není prvkem F'. Přitom z definice AX-bezespornosti plyne, že ani formule $\neg A$ není prvkem množiny F. To je ve sporu s následujícím tvrzením a) o vlastnostech maximálních AX-bezesporných množin.

Pro maximální bezesporné množiny platí: Je-li F maximální AX-bezesporná množina potom

(a) pro každou formuli A jazyka L právě jedna z formulí A a $\neg A$ je prvkem F

(b) $A \wedge B \in F$ právě když $A \in F$ a $B \in F$

(c) jsou - li formule A a $A \rightarrow B$ v F, potom také formule B je prvkem F.

(d) je - li A dokazatelná z AX, potom $A \in F$

Přitom z tvrzení a) plyne, že F je úplná teorie.

Tvrzení (a) - (d) ponecháváme jako cvičení.

Definice. (formule validní ve třídě Kripkeho struktur)

Nechť M_n je třída Kripkeho struktur pro n agentů. Říkáme, že formule A je validní ve třídě M_n, je-li validní v každé struktuře M_n ze třídy M_n.

Budeme se zabývat vlastnostmi znalostí ve třídě M_n Kripkeho struktur, to znamená formulemi, které jsou v této třídě validní. Připomeňme, že v těchto strukturách nedáváme žádné předpoklady o vlastnostech relací K_i.

Protože třída struktur M_n^{rst}, ve které jsou relace K_i reflexivní, symetrické a transitivní - tedy relace ekvivalence, je vlastní podtřídou třídy M_n, můžeme očekávat, že v této třídě bude více validních formulí.

V Kripkeho strukturách třídy M_n jsme ověřili, že validní jsou

- A1 Všechny instance výrokových tautologií
- A2 Distribuční axiom **D**
- Pravidlo Modus ponens
- Pravidlo generalizace znalostí

První a druhé schema axiomů jsme ověřili bez jakýchkoli předpokladů o relacích K_i, stejně jako odvozovací pravidla modus ponens a pravidlo generalizace.

Jaké výsledky platí, když relace K_i nějak omezíme?

Nabízí se tyto axiomy

- A3 Axiom znalostí (Axiom pravdy) **T**
- A4 Axiom pozitivní introspekce **4**
- A5 Axiom negativní introspekce **5**

Dá se ukázat, že

• validnost Axiomu znalostí plyne z reflexivity relací K_i, tedy axiom **T** je pravdivý ve všech strukturách třídy M_n^r

• validnost Axiomu pozitivní introspekce **4** plyne z tranzitivity relací K_i, tím spíše je **4** validní ve třídě M_n^{rt}

• validnost Axiomu negativní introspekce **5** plyne ze symetrie a tranzitivity relací K_i tedy **5** jetím spíše validní ve třídě M_n^{rst}.

Názvosloví

KD45 je teorie sestávající z axiomů $\mathbf{K}_n$ s axiomy **D**, **4**, **5.**

KT4 vznikne rozšířením $\mathbf{K}_n$ o axiomy **T** a **4**.

K se většinou vynechává, takže píšeme **D45** a **T4**.

Historické názvy:	**T4**	S4	$S4_n$
	T45	S5	$S5_n$

Věta

Pro modální teorie v jazyce L_n platí

- $\mathbf{K}_n$ je úplná axiomatizace vzhledem k třídě M_n
- $\mathbf{T}_n$ je úplná axiomatizace vzhledem ke třídě M_n^r
- $\mathbf{S4}_n$ je úplná axiomatizace vzhledem ke třídě M_n^{rt}
- $\mathbf{S5}_n$ je úplná axiomatizace vzhledem ke třídě M_n^{rst}
- $\mathbf{KD45}_n$ je úplná axiomatizace vzhledem ke třídě M_n^{elt}.

K analýze složitosti důkazů v jednotlivých systémech modální logiky potřebujeme některé definice a značení.

Definice. (i) Je-li A množina, $|A|$ *označuje mohutnost této množiny* (pokud A je konečná, jde o počet jejích prvků).

(ii) *Délku formule* B (tedy počet jejích symbolů) označujeme $|B|$. Například $|p \wedge E_{[1,2]}p| = 9$. (Počítáme písmena, čísla, logické symboly, závorky a čárky).

Délku formulí $E_G B$, $C_G B$ a $D_G B$ definujeme jako $2 + 2|G| + |B|$, protože prvky G počítáme jako různé symboly a počítáme i čárky a množinové závorky v G.

Je-li A formule, množinu všech jejích podformulí označujeme $Sub(A)$, dá se ukázat, že $|Sub(A)| < |A| + 1$.

Složitost problému validity.

$S5_1,\ KD45_1$	$K_n, T_n, S4_n, n \geq 1$ $S5_n, KD45_n, n \geq 2$	$K_n^C, T_n^C, n \geq 1$ $S4_n^C, S5_n^C, KD45_n^C, n \geq 2$
$NP - úplný$	$PSPACE - úplný$	$EXPTIME - úplný$