Temporální logika

Temporální logika poskytuje rámec a prostředky pro analýzu dynamických (imperativních) stavových systémů a hraje zde stejnou úlohu jakou má klasická logika pro matematické systémy.

V intuitivním smyslu stavové systémy zahrnují „stavy“ a vykazují „chování“ při průchodu posloupnostmi takových stavů.

Máme na mysli například, programové moduly, komunikační protokoly, databázové systémy, logické obvody, čipy a obecně výpočetní procesy, které při provádění procházejí určitými stavy a vykazují specifické chování.

Doporučení pro další čtení: Při cvičení se probírají jen části se žlutým podkladem (jako tento odstavec). Ostatní text jen dokresluje sdělovanou informaci.

Podobně jako v klasické logice je vhodné začít s výrokovou verzí temporální logiky.

Stavy. K popisu stavů použijeme prvotní formule, které vyjadřují jednoduchá tvrzeni například „globální proměnná x má hodnotu 10“.

K popisu všech stavů použijeme množinu prvotních formulí, která může být konečná i nekonečná. Stav je určen pravdivostním ohodnocením všech prvotních formulí.

K popisu konkrétních systémů obvykle postačí konečná množina prvotních formulí.

Čas. Podobně jako výpočetní procesy postupují v jednotlivých krocích, uvažujeme čas diskretní sestávající z jednotlivých časových bodů od počátečního bodu (okamžiku) k dalším (budoucím) časovým bodům.

Budoucnost systému lze modelovat různým uspořádáním časových bodů. Nejjednodušším a vcelku realistickým předpokladem je uspořádání časových bodů do lineární množiny.

V takovém případě budou časové body tvořit konečnou nebo nekonečnou posloupnost, kterou očíslujeme přirozenými čísly

$$m_0 , m_1 , m_2 , m_3 , \ \ldots , m_n , m_{n+1} , \ \ldots$$

Takové uspořádání používá **Výroková lineární temporální logika** (**LTL**).

Při popisu složitějších systémů popisujících například distribuované výpočty se používají i jiná uspořádání časových bodů například ve tvaru stromu. Pak mluvíme o větvícím se čase.

Je-li V množina prvotních formulí, jazyk výrokové temporální logiky L_{LTL} sestává ze

- všech formulí z množiny V a
- symbolů **false** $\rightarrow$ $\Box$ $\bigcirc$ ( )

Temporální operátory $\bigcirc$, $\Box$, $\Diamond$ se (anglicky) nazývají

$\bigcirc$ *nexttime* nebo jen *next* ,

$\Box$ *always* nebo *henceforth* a

$\Diamond$ *sometime*.

Formule $\bigcirc A$, $\Box A$ **a** $\Diamond A$ se (anglicky) čtou

$\bigcirc A$: *nextA* , česky *příště A*,

$\Box A$: *alwaysA*, česky *vždy A*

$\Diamond A$: *sometimeA*, česky *někdy A*

Preference $\neg$, $\bigcirc$, $\Box$, $\Diamond$ váží silněji než $\vee$, $\wedge$, $\rightarrow$ a $\equiv$ má nejslabší prioritu.

Temporální operátory a přirozený jazyk

- α nechť znamená „*Měsíc obíhá Zemi*“,
- β nechť znamená „*Měsíc vychází*“,
- γ nechť znamená „*Měsíc zapadá*“.

- $\Diamond\beta$, která vyjadřuje tvrzení „*Měsíc někdy vyjde*“,
- $\Box\Diamond\beta$ s významem „*Měsíc bude vycházet znovu a znovu*“,
- $\Box(\beta \rightarrow \Diamond\gamma)$ s významem „*vždy po východu měsíce bude někdy následovat jeho západ*“.

Definice. (Formule LTL)

1. Každá prvotní formule z množiny V je formule.
2. Výroková konstanta **false** je formule.
3. Jsou-li A a B formule, potom $A \rightarrow B$ je formule.
4. Je-li A formule, potom $\bigcirc A$ a $\Box A$ jsou formule.

Ostatní spojky se zavádějí jako zkratky

- $\neg A$ je zkratka za formuli $\neg$ (**false** $\rightarrow A$)
- **true** je zkratka za formuli $\neg$ **false**
- $\vee$, $\wedge$, $\equiv$ jako v klasické logice ,
- $\Diamond A$ je zkratka za formuli $\neg \Box \neg A$

Zde jsou některé často používané temporální formule a jejich neformální čtení.

$A \rightarrow \circ B$	*„jestliže A potom B v dalším stavu“*
$A \rightarrow \Box B$	*„jestliže A potom B teď a v každém dalším stavu“*
$A \rightarrow \Diamond B$	*„jestliže A potom B teď nebo v nějakém dalším stavu“*
$\Box(A \rightarrow B)$	*„jestliže A teď nebo v nějakém dalším stavu potom B platí ve stejném stavu“*
$\Box\Diamond A$	*„teď a za každým dalším stavem někdy platí A“*
	„(od teď) A bude platit v nekonečně mnoha stavech“
	„formule A bude nastavát znovu a znovu“
$\Diamond\Box A$	*„od některého budoucího stavu bude stále platit A“*
	„A platí skoro vždycky (od jistého okamžiku dál) “

Popis komplexního systému – dobře fungující úřad

- Jeli požadavek podán, pak bude někdy doručen na správné místo $\Box(\textit{požadavek} \rightarrow \Diamond \textit{doručen})$,
- Je-li požadavek doručen, pak jeho zpracování bude zahájeno hned v následujícím okamžiku

$$\Box(\textit{doručen} \rightarrow \circ \textit{zpracováván}),$$

- Zpracovávaný požadavek bude jednou vyřízen (hotov) a pak už zůstane hotov (nebude se znovu otevírat)

$$\Box(\textit{zpracováván} \rightarrow \Diamond\Box \textit{hotov}).$$

Uvedené formule charakterizují chování komplexního systému, označíme je jako program **P** pro tento systém. Zdá se, že nemůže nastat situace, ve které by systém stále vysílal stejný požadavek, ale ten by nebyl nikdy hotov. Lze se o tom přesvědčit? Na přednášce ukážeme, že formule $\Box$ ***požadavek*** **&** $\Box\neg$***hotov*** nemůže platit, čili tato formule je s uvedným programem **P** nekonzistentní.

V klasické logice se pravdivostní hodnoty výrokových formulí určují z pravdivostního ohodnocení prvotních výroků (tedy v jediné interpretaci, v jednom ‘stavu’) .

V temporální logice, kde se výrokové formule tvoří také z prvotních formulí za použití modálních operátorů □, ◊ a ○ se pravdivostní hodnoty musí určovat z více pravdivostních ohodnocení těchto konstant (tedy ve více interpretacích , ve více ‘stavech’) .

Pro ‘stav’ používáme jako synonymum ‘svět’ a sémantika temporální logiky je definována pomocí Kripkeovy sémantiky ‘možných světů’ .

Sémantika pro Lineární Temporální Logiku LTL

Nechť V je množina prvotních formulí.

Temporální (nebo Kripkeova) *struktura* pro V je nekonečná posloupnost $\boldsymbol{M} = (\eta_0 , \eta_1 , \eta_2 , \ldots)$ pravdivostních ohodnocení

$$\eta_i : V \rightarrow \{ff , tt \}$$

které nazýváme *stavy.*

Říkáme, že η_0 je *počáteční stav* $\boldsymbol{M}$ v časovém bodu m_0 a že η_{n+1} je následující stav ke stavu η_n .

Stavy jsou tedy pravdivostní ohodnocení množiny prvotních formulí V a popisují ‘stav světa ‘ v časových okamžicích (časových bodech)

. $m_0, m_1, m_2, m_3, \ldots, m_n, m_{n+1}, \ldots$

Pro temporální strukturu $\boldsymbol{M}$, index i a formuli A *induktivně* definujeme pravdivostní hodnotu $\boldsymbol{M}_i(A)$, neformálně, pravdivostní hodnotu formule A v časovém bodě m_i.

$\boldsymbol{M}_i(v) = \eta_i(v) \qquad v \in V$

$\boldsymbol{M}_i$ **(false)** = ff

$\boldsymbol{M}_i(A \rightarrow B)$ = tt *právě když*

. $\boldsymbol{M}_i(A)$ = ff *nebo* $\boldsymbol{M}_i(B)$ = tt

Pro operátory

$\boldsymbol{M}_i(\circ A) = \boldsymbol{M}_{i+1}(A)$

$\boldsymbol{M}_i(\Box A)$ = tt *právě když* $\boldsymbol{M}_j(A)$ = tt *pro každé* $j \geq i$

Pro definované symboly

$\boldsymbol{M}_i(\neg A)$ = tt *právě když* $\boldsymbol{M}_i(A)$ = ff

$\boldsymbol{M}_i(A \vee B)$ = tt *právě když*

$\boldsymbol{M}_i(A)$ = tt *nebo* $\boldsymbol{M}_i(B)$ = tt

$\boldsymbol{M}_i(A \wedge B)$ = tt *právě když*

$\boldsymbol{M}_i(A)$ = tt *a* $\boldsymbol{M}_i(B)$ = tt

$\boldsymbol{M}_i\,(A \equiv B)$ = tt *právě když* $\boldsymbol{M}_i\,(A) = \boldsymbol{M}_i\,(B)$

$\boldsymbol{M}_i\,(\mathbf{true})$ = tt

$\boldsymbol{M}_i\,(\Diamond A)$ = tt *právě když* $\boldsymbol{M}_j\,(A)$ = tt *pro nějaké* $\boldsymbol{j \geq i}$

Povšimněme si , že pravdivostní hodnoty $\mathbf{K}_i\,(\Box A)$ a $\mathbf{K}_i\,(\circ A)$ jsou definovány pomocí následujících stavů a aktuálního stavu.

Platí

$\boldsymbol{M}_i\,(\Diamond A)$ = tt *právě když* $\boldsymbol{M}_i\,(\neg\,\Box\,\neg A)$ = tt

právě když $\boldsymbol{M}_i\,(\Box\,\neg A)$ = ff

právě když $\boldsymbol{M}_j\,(\neg A)$ = ff *pro nějaké* $\boldsymbol{j \geq i}$

právě když $\boldsymbol{M}_j\,(A)$ = tt *pro nějaké* $\boldsymbol{j \geq i}$

Definice (validita, **sémantický důsledek**)

Nechť A je formule jazyka logiky $LTL(V)$ a $\mathbf{T}$ je množina for-mulí stejného jazyka.

Říkáme, že A je *validní* v temporální struktuře $\boldsymbol{M}$ pro V, (nebo že A je splněna v $\boldsymbol{M}$) a píšeme $\boldsymbol{M} \models A$ nebo $\models_{\boldsymbol{M}} A$, jestliže $\boldsymbol{M}_i\,(A)$ = tt *pro všechna* i

Říkáme, že struktura $\boldsymbol{M}$ je modelem množiny formulí $\mathbf{T}$, jestliže $\boldsymbol{M} \models B$ pro všechny formule B z $\mathbf{T}$.

Říkáme, že A je (sémantický) *důsledek* $\mathbf{T}$ a píšeme $\mathbf{T} \models A$, jestliže A je validní v každém modelu $\boldsymbol{M}$ množiny formulí $\mathbf{T}$.

Říkáme, že A je validní a píšeme $\models A$, jestliže A je validní v každé temporální struktuře $\boldsymbol{M}$.
Jinými slovy, A je validní, jestliže $\emptyset \models A$.

Příklad. $\neg\bigcirc A \equiv \bigcirc\neg A$ je validní formule.

Je třeba ukázat, že $\boldsymbol{M}_i(\neg\bigcirc A) = \boldsymbol{M}_i(\bigcirc\neg A)$ platí pro každou strukturu $\boldsymbol{M}$ a všechny časové body i.

$$\boldsymbol{M}_i(\neg\bigcirc A) = \text{tt} \Leftrightarrow \boldsymbol{M}_i(\bigcirc A) = \text{ff}$$
$$\Leftrightarrow \boldsymbol{M}_{i+1}(A) = \text{ff}$$
$$\Leftrightarrow \boldsymbol{M}_{i+1}(\neg A) = \text{tt}$$
$$\Leftrightarrow \boldsymbol{M}_i(\bigcirc\neg A) = \text{tt}$$

Lemma 1. (korektnost pravidla modus ponens)

Nechť $\boldsymbol{M}$ je temporální struktura a $i \in \mathrm{N}$ *(množina přirozených čísel)*, nechť $\boldsymbol{M}_i(A) = \text{tt}$ a $\boldsymbol{M}_i(A \to B) = \text{tt}$, potom $\boldsymbol{M}_i(B) = \text{tt}$.

Důkaz. $\boldsymbol{M}_i(A \to B) = \text{tt}$, tedy $\boldsymbol{M}_i(A) = \text{ff}$ nebo $\boldsymbol{M}_i(B) = \text{tt}$.

Z předpokladu $\boldsymbol{M}_i(A) = \text{tt}$ dostáváme $\boldsymbol{M}_i(B) = \text{tt}$.

Věta 2. Je-li $\mathbf{T} \models A$ a $\mathbf{T} \models A \to B$, potom $\mathbf{T} \models B$.

Důkaz. Nechť struktura $\boldsymbol{M}$ je modelem $\mathbf{T}$. Potom pro každé i platí

$$\boldsymbol{M}_i(A) = \boldsymbol{M}_i(A \to B) = \text{tt}$$

a podle lemmatu 1 pak také $\boldsymbol{M}_i(B) = \text{tt}$. Tedy $\mathbf{T} \models B$.

Věta 3. Je-li $\mathbf{T} \models A$, potom $\mathbf{T} \models \circ A$ a $\mathbf{T} \models \Box A$. Speciálně $A \models \circ A$ a $A \models \Box A$.

Důkaz. Nechť $\boldsymbol{M}$ je libovolná temporální struktura, která je modelem $\mathbf{T}$ a nechť i je přirozené číslo.

Podle předpokladu platí $\boldsymbol{M}_j(A)$ pro všechna j, tedy také

$$\boldsymbol{M}_{i+1}(A) = \text{tt} \quad \text{a} \quad \boldsymbol{M}_j(A) = \text{tt} \text{ pro všechna } j,\ j \geq i .$$

To znamená, že

$$\mathbf{T} \models \circ A \quad \text{a} \quad \mathbf{T} \models \Box A .$$

Věta 4. Je-li $\mathbf{T} \models A \rightarrow B$ a $\mathbf{T} \models A \rightarrow \circ A$, potom $\mathbf{T} \models A \rightarrow \Box B$ (pravidlo indukce).

Důkaz. Nechť $\boldsymbol{M}$ je struktura pro $\mathbf{T}$. Rozlišíme 2 možnosti:

•Je-li $\boldsymbol{M} \models \neg A$, je tvrzení věty důsledkem vlastností spojky „$\rightarrow$“ .

•Neplatí-li $\boldsymbol{M} \models \neg A$, zvolme i nejmenší takové, že $\boldsymbol{M}_i \models A$. Tvrzení $\boldsymbol{M}_i \models \Box A$, $\boldsymbol{M}_i \models \Box B$ jsou jednoduchými důsledky předpokladů věty. Tedy pro všechna j platí $\boldsymbol{M}_j \models A \rightarrow \Box B$

Označení. Nechť $\boldsymbol{M} = (\eta_0 , \eta_1 , \eta_2 , \dots)$ je nějaká temporální struktura pro množinu výrokových konstant V. Nechť i je pevně zvolené přirozené číslo. Temporální strukturu $\boldsymbol{M}^i$, která vznikne z $\boldsymbol{M}$ posunutím času o i kroků do budoucnosti, definujeme takto:

$$\boldsymbol{M}^i = (\eta_0' , \eta_1' , \eta_2' , \dots)$$

kde $\eta_j' = \eta_{i+j}$ pro každé j. $\boldsymbol{M}^i$ je také temporální struktura podle původní definice, ale budeme ji úsporněji zapisovat jako

$$\boldsymbol{M}^i = (\eta_i , \eta_{i+1} , \eta_{i+2} , \dots , \eta_{i+j} , \eta_{i+j+1} , \dots) .$$

Následující tvrzení je temporální obdobou **Věty o dedukci** v klasické výrokové logice ($\mathbf{T} \models (A \to B)$ *iff* $\mathbf{T}, A \models B$).

Věta 6. $\mathbf{T} \cup \{A\} \models B$ *právě když* $\mathbf{T} \models \Box A \to B$.

Sémantický důkaz nebudeme provádět, ale povšimneme si, že z přesné obdoby klasické Věty o dedukci platí jen tvrzení

Věta 7. Je-li $\mathbf{T} \models A \to B$ *potom* $\mathbf{T} \cup \{A\} \models B$.

Obrácená implikace v LTL neplatí! Stačí uvažovat případ, kdy **T** je prázdná množina. Podle Věty 3 platí $A \models \Box A$ pro libovolnou formuli, ale implikace $A \to \Box A$ nemusí být validní formule. Není pravdivá v žádné temporální struktuře $\boldsymbol{M}$, kde pro nějaké i a $j > i$ platí $\boldsymbol{M}_i(A) =$ tt a $\boldsymbol{M}_j(A) =$ ff . Stačí uvažovat případ, kdy A je některá výroková konstanta.

Binární temporální operátory

Oblíbeným binárním operátorem je temporální obdoba programového konstruktu **until** . Nejčastěji se značí $A \cup B$.

Definice. $A \cup B$

Pro temporální strukturu $\boldsymbol{M}$, index i a formule A , B definujeme pravdivostní hodnotu $\boldsymbol{M}_i (A \cup B)$ následovně

$\boldsymbol{M}_i (A \cup B) =$ tt $\Leftrightarrow$ $\boldsymbol{M}_j (B) =$ tt *pro nějaké* j , $j > i$ *a*
$\boldsymbol{M}_k (A) =$ tt *pro každé* k , $i < k < j$

Důležité validní formule

(1)

$\models \Box\neg A \equiv \neg \Diamond A$ $\qquad$ $\models \Diamond\neg A \equiv \neg \Box A$

$\models \circ\neg A \equiv \neg \circ A$

$\models \Box \Diamond \neg A \equiv \neg \Diamond \Box A$ $\qquad$ $\models \Diamond \Box \neg A \equiv \neg \Box \Diamond A$

Následující validní implikace nelze zesílit na ekvivalence

$\models A \rightarrow \Diamond A$ $\qquad$ $\models \Box A \rightarrow A$

$\models \circ A \rightarrow \Diamond A$ $\qquad$ $\models \Box A \rightarrow \circ A$

$\models \Box A \rightarrow \Diamond A$ $\qquad$ $\models \Box A \rightarrow \circ \Box A$

$\models A \cup B \rightarrow \Diamond A$ $\qquad$ $\models \Diamond \Box A \rightarrow \Box \Diamond A$

Idempotence $\Diamond$, $\Box$, $\Box\Diamond$ a $\Diamond\Box$

$\models \Diamond\Diamond A \equiv \Diamond A$ $\qquad$ $\models \Box\Box A \equiv \Box A$

$\models \Diamond\Box \Diamond\Box A \equiv \Diamond\Box A$ $\qquad$ $\models \Box\Diamond \Box\Diamond A \equiv \Box\Diamond A$

Ale operátor příštího stavu není idempotentní. Formule $\circ\circ A \equiv \circ A$ není validní.

Vlastnosti nekonečných modalit **$\Box\Diamond$ a $\Diamond\Box$: „konzumují“** všechny ostatní modality s jedním argumentem, které jsou na ně aplikované. S menším násilím na syntax formulí to můžeme kompaktně vyjádřit takto

$\models (\Box\Diamond) A \equiv \circ (\Box\Diamond) A \equiv \Diamond (\Box\Diamond) A \equiv \Box (\Box\Diamond) A$

$\models \Box\Diamond (\Box\Diamond) A \equiv \Diamond\Box (\Box\Diamond) A$

$\models (\Diamond\Box) A \equiv \circ (\Diamond\Box) A \equiv \Diamond (\Diamond\Box) A \equiv \Box (\Diamond\Box) A$

$\models \Box\Diamond (\Diamond\Box) A \equiv \Diamond\Box (\Diamond\Box) A$

Podle své definice jsou operátory $\Diamond$ a $\Box\Diamond$ povahy *existenční* a operátory $\Box$ a $\Diamond\Box$ povahy *univerzální*, zatímco operátor $\cup$ (*until*) je v prvním argumentu univerzální a ve druhém argumentu existenční.
Vykazují podobné chování jako existenční kvantifikátor a univerzální kvantifikátor v predikátové logice.

$$\models \Diamond(A \vee B) \equiv (\Diamond A \vee \Diamond B) \qquad \models \Box\Diamond(A \vee B) \equiv (\Box\Diamond A \vee \Box\Diamond B)$$

$$\models \Box(A \wedge B) \equiv (\Box A \wedge \Box B) \qquad \models \Diamond\Box(A \wedge B) \equiv (\Diamond\Box A \wedge \Diamond\Box B)$$

Pro operátor $\cup$ (*until*) a boolovské spojky konjunkce a disjunkce platí tyto distributivní vztahy.

$$\models ((A \wedge B) \cup C) \equiv ((A \cup C) \wedge (B \cup C))$$
$$\models (A \cup (B \vee C)) \equiv ((A \cup C) \vee (B \cup C))$$

.

Operátor $\circ$ (next) se vztahuje k jedinému časovému bodu, proto se distribuuje se všemi boolovskými spojkami.

$$\models \circ(A \vee B) \equiv (\circ A \vee \circ B) \qquad \models \circ(A \wedge B) \equiv (\circ A \wedge \circ B)$$
$$\models \circ(A \rightarrow B) \equiv (\circ A \rightarrow \circ B) \qquad \models \circ(A \equiv B) \equiv (\circ A \equiv \circ B)$$

přitom ekvivalence $\models \circ\neg A \equiv \neg\circ A$ již byla uvedena výše.

Pro kombinace operátorů universální a existenční povahy platí jen implikace, které nelze zesílit na ekvivalence.

$$\models (\Box A \vee \Box B) \rightarrow \Box(A \vee B) \qquad \models \Diamond\Box(A \vee B) \rightarrow (\Diamond\Box A \vee \Diamond\Box B)$$
$$\models \Diamond(A \wedge B) \rightarrow (\Diamond A \wedge \Diamond B) \qquad \models \Box\Diamond(A \wedge B) \rightarrow (\Box\Diamond A \wedge \Box\Diamond B)$$

$$\models ((A \cup C) \vee (B \cup C)) \rightarrow ((A \vee B) \cup C).$$
$$\models (A \cup (B \wedge C)) \rightarrow ((A \cup B) \wedge (A \cup C))$$

Povšimneme si, že uvedené operátory jsou monotonní v každém argumentu.

$\models \Box(A \to B) \to (\Box A \to \Box B)$ $\quad\quad$ $\models \Box(A \to B) \to (\Diamond A \to \Diamond B)$

$\models \bigcirc(A \to B) \to (\bigcirc A \to \bigcirc B)$

$\models \Box(A \to B) \to (\Diamond\Box A \to \Diamond\Box B)$ $\quad\quad$ $\models \Box(A \to B) \to (\Diamond\Box A \to \Diamond\Box B)$

$\models \Box(A \to B) \to ((A \cup C) \to (B \cup C))$

$\models \Box(A \to B) \to ((C \cup A) \to (C \cup B))$

$\models (A \cup B) \equiv B \vee (A \wedge \bigcirc(A \cup B))$

Nakonec uvedeme důležité charakteristiky temporálních operátorů pomocí pevných bodů.

$\models \Diamond A \equiv (A \vee \bigcirc\Diamond A)$ $\quad\quad$ (3) $\quad\quad$ $\models \Box A \equiv (A \wedge \bigcirc\Box A)$

Pozor : sice platí $\models \Box A \to (A \to \bigcirc\Box A)$, ale formule popisující opačnou implikaci $(A \to \bigcirc\Box A) \to \Box A$ určitě neplatí !

Příklady zdrojů dalších informací:

- Huth M., Ryan M.: *Logic in Computer Science*, Cambridge University Press, 2004
- Programový systém SPIN