TEMPORAALILOGIIKKA

E. M. Clarke et al.: *Model Checking*, luku 3 (s. 27–33).

E. A. Emerson: *Automated Temporal Reasoning about Reactive Systems*, luku 2 (s. 3–15).

1. Johdanto temporaalilogiikkaan

- Temporaalilogiikat ovat sovelletuimpia modaalilogiikkoja.
- Aikatulkinta: mahdolliset maailmat mahdollisia ajanhetkiä
- Laskennallinen tulkinta: mahdolliset maailmat mahdollisia laskennan tiloja
- Formaali malli $\langle S, R, v \rangle$, missä relaation sRt tulkintana on
  t on (eräs) s:n mahdollinen tulevaisuus ja
  s on (eräs) t:n mahdollinen menneisyys.

  $\mathcal{M}, s \Vdash \mathbf{F}Q$ joss $\mathcal{M}, t \Vdash Q$ jollekin $t \in S$ jolle sRt.

  $\mathcal{M}, s \Vdash \mathbf{P}Q$ joss $\mathcal{M}, t \Vdash Q$ jollekin $t \in S$ jolle tRs.

  R usein transitiivinen, lineaarinen/haarautuva, diskreetti/jatkuva, ...

Temporaalioperaattoreita

- $\mathbf{F}Q$ (joskus tulevaisuudessa, engl. future)
- $\mathbf{G}Q = \neg\mathbf{F}\neg Q$ (aina tulevaisuudessa, engl. globally)
- $\mathbf{P}Q$ (joskus menneisyydessä, engl. past)
- $\mathbf{H}Q = \neg\mathbf{P}\neg Q$ (aina menneisyydessä, engl. historically)
- $\mathbf{Always}\ Q = \mathbf{G}Q \wedge Q \wedge \mathbf{H}Q$ (aina)
- $\mathbf{X}$ (seuraavassa tilassa, engl. next):
  Kaikissa/jossakin?
  Saavutettavuusrelaatioiden suhde ($R_{\mathbf{X}}$ vs. $R_{\mathbf{F}}$)?

Binäärisiä temporaalioperaattoreita

- $\mathbf{U}$ (kunnes, engl. until):

  $\mathcal{M}, s \Vdash A\mathbf{U}B$ joss

  jollekin t, sRt, $\mathcal{M}, t \Vdash B$ ja kaikille $u \in S$,

  jos sRu ja uRt, niin $\mathcal{M}, u \Vdash A$.

  $\Longrightarrow\ \top\mathbf{U}B \leftrightarrow \mathbf{F}B$
- $\mathbf{S}$ (siitä asti kun, engl. since):

  $\mathcal{M}, s \Vdash A\mathbf{S}B$ joss

  jollekin t, tRs, $\mathcal{M}, t \Vdash B$ ja kaikille $u \in S$,

  jos uRs ja tRu, niin $\mathcal{M}, u \Vdash A$.

  $\Longrightarrow\ \top\mathbf{S}B \leftrightarrow \mathbf{P}B$

Dynaaminen logiikka

- Modaalioperaattori jokaista toimintoa a kohti:

$$[a]P$$

(P on tosi toiminnon a suorittamisen jälkeen).

- Toiminnoilla voi olla rakennetta:

$a;b$	sarjallistaminen
$a \cup b$	epädeterministinen valinta
a^*	toisto
$P?$	testaus (jos P tosi jatketaan, muuten ei)

Esimerkki. Tarkastellaan seuraavia dynaamisen logiikan lauseita:

$[(P?;a) \cup (\neg P?;b)]Q$ ([if P then a else b] Q)

$[(P?;a)^*;\neg P?]Q$ ([while P do a] Q)

2. Rinnakkainen ja hajautettu laskenta

- Useita rinnakkaisia ja hajautettuja prosesseja
- Jaetut resurssit, koordinointi, kommunikointi
- Keskeytyksetön toiminta
- Reaktiivisuus, epädeterministisyys
- Esimerkkejä: käyttöjärjestelmät, tietoliikenneprotokollat, laitteistokomponentit, ohjausjärjestelmät, . . .

Reaktiiviset järjestelmät

- Reaktiivisten järjestelmien suunnittelu haastavaa:
  - Virhetilanteet ovat usein vaikeasti toistettavissa.
  - Järjestelmien käyttäytymiset “äärettömiä” tilasekvenssejä.
- Tarvitaan uusia suunnittelumenetelmiä:

(i) Virheet paikallistettava mahdollisimman aikaisessa vaiheessa suunnittelua/toteutusta.

(ii) On pystyttävä käsittelemään päättymättömiä ajoja.

Temporaalilogiikka

- Formaali malli järjestelmän käyttäytymiselle.
- Kieli, jolla voidaan määritellä järjestelmän ominaisuuksia.

Esimerkki.

- Keskinäinen poissulkeminen: $\mathbf{G}\neg(at_i(m) \wedge at_j(m'))$.
- Osittainen oikeellisuus: jos ehto P pätee ohjelman alkutilanteessa m_0, ehto Q pätee lopputilanteessa m_e:
  $at(m_0) \wedge P \rightarrow \mathbf{G}(at(m_e) \rightarrow Q)$.
- Täysi oikeellisuus: vaaditaan lisäksi ehto, että ohjelma pysähtyy:
  $at(m_0) \wedge P \rightarrow \mathbf{F}(at(m_e) \wedge Q)$.
- Ei turhia toimintoja: vastaus v_i vain saatuun pyyntöön p_i:
  $\mathbf{F}v_i \rightarrow (\neg v_i)\mathbf{U}p_i$.

Temporaalilogiikan soveltaminen

- Oikeellisuuden todistaminen
  - Järjestelmän toiminta ja oikeellisuusehdot mallitetaan temporaalilogiikan lauseina
  - Todistetaan temporaalilogiikan avulla, että oikeellisuusehdot seuraavat järjestelmän ominaisuuksista (kompositionaalisesti)
  - Virhealtista ja vaikeasti automatisoitavissa
- Ohjelmasynteesi
  - Ohjelman määrittely temporaalilogiikalla
  - Määrittelyn malli antaa ohjelman
  - Helpommin automatisoitavissa (jopa suoritettavat temporaalispesifikaatiot mahdollisia)

Temporaalilogiikan soveltaminen (jatkoa)

- Mallintarkastus
  - Tarkastetaan, onko järjestelmän mallilla halutut ominaisuudet
  - Tutkittavat ominaisuudet temporaalilogiikalla
  - Tehokkaita mallintarkastimia kehitetty
- Sovelletuimpia temporaalilogiikkoja ovat CTL ja LTL.

3. CTL (Computation Tree Logic)

- Temporaalioperaattorit muodostuvat pareista, joissa on
  (i) polkukvanttori ($\mathbf{A}/\mathbf{E}$) ja
  (ii) temporaalioperaattori ($\mathbf{X}/\mathbf{U}/\mathbf{G}/\mathbf{F}$).
- CTL-syntaksi:
  - Jokainen atomilause on CTL-lause.
  - Jos P, Q ovat CTL-lauseita, niin $P \wedge Q$, $\neg P$, $\mathbf{AX}P$, $\mathbf{A}(P\mathbf{U}Q)$, $\mathbf{E}(P\mathbf{U}Q)$ ovat myös CTL-lauseita.

Esimerkki.

$$(P \wedge Q) \wedge \neg Q \qquad \mathbf{AX}(P \wedge \neg Q) \qquad \mathbf{E}((\mathbf{AX}P)\mathbf{U}Q)$$

CTL:n syntaksi

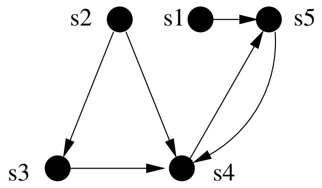
- Huom! Temporaalioperaattoreiden $\mathbf{X}/\mathbf{U}$ sisäkkäisyys ja Boolen yhdistelmät ovat CTL:ssä rajoitettuja:
  Esim. $\mathbf{AXAX}P$ on CTL-lause, mutteivät $\mathbf{AXX}P$ ja $\mathbf{A}\neg\mathbf{X}P$.
- Muut operaattorit ($\mathbf{EX}, \mathbf{AG}, \mathbf{EG}, \mathbf{AF}, \mathbf{EF}$) määritellään lyhennysmerkintöinä annettujen operaattoreiden ($\mathbf{AX}$, $\mathbf{A}(.\mathbf{U}.)$, $\mathbf{E}(.\mathbf{U}.)$) avulla.
- CTL kuvaa laskentapuun ominaisuuksia ja polkukvanttoreilla voidaan kertoa, päteekö tietty ominaisuus jollekin vai kaikille tilasta lähteville laskentapoluille.

Esimerkki. $\mathbf{AX}P$ (kaikilla laskentapoluilla seuraavassa tilassa P) ja $\mathbf{E}(P\mathbf{U}Q)$ (on olemassa polku, jossa P kunnes Q).

Mahdollisten maailmojen semantiikka

- CTL:n mallit ovat mahdollisten maailmojen malleja $\langle S, R, v\rangle$, joissa saavutettavuusrelaatio R on sarjallinen.
- Huom! Relaatio R liittyy operaattoriin $\mathbf{X}$.
- Täysi polku on ääretön sekvenssi $s_0, s_1, \ldots$ tiloja siten, että kaikille i pätee $s_i R s_{i+1}$. (Yksi tilasta s_0 lähtevän laskentapuun haara).

Esimerkki. Tarkastellaan kuvassa esitettyä mallia M:



Täysiä polkuja esim.

$s1, s5, s4, s5, s4, \ldots$

$s2, s4, s5, s4, \ldots$

$s2, s3, s4, s5, s4, \ldots$

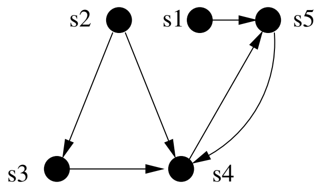
Totuusmääritelmä

Määritellään milloin CTL-lause on tosi tilassa s ($\mathcal{M}, s \models P$):

- $\mathcal{M}, s \models P$ joss $v(s, P) = \text{true}$, kun P on atomilause.
- $\mathcal{M}, s \models \neg P$ joss $\mathcal{M}, s \not\models P$.
- $\mathcal{M}, s \models P \wedge Q$ joss $\mathcal{M}, s \models P$ ja $\mathcal{M}, s \models Q$.
- $\mathcal{M}, s \models \mathbf{AX}P$ joss $\mathcal{M}, t \models P$ kaikille t, joille sRt.
- $\mathcal{M}, s \models \mathbf{A}(P\mathbf{U}Q)$ joss mallissa $\mathcal{M}$ kaikille täysille poluille $(s_0, s_1, \ldots)$, missä $s = s_0$, on olemassa $i \geq 0$, jolle $\mathcal{M}, s_i \models Q$ ja $\mathcal{M}, s_j \models P$ kaikille $0 \leq j < i$.
- $\mathcal{M}, s \models \mathbf{E}(P\mathbf{U}Q)$ joss mallissa $\mathcal{M}$ on olemassa täysi polku $(s_0, s_1, \ldots)$ siten, että $s = s_0$ ja on olemassa $i \geq 0$, jolle $\mathcal{M}, s_i \models Q$ ja $\mathcal{M}, s_j \models P$ kaikille $0 \leq j < i$.

Esimerkki

Palataan edellä esiteltyyn malliin M:



Määritellään $v(P, s_4) = \text{true}$ ja muutoin $v(P, s) = \text{false}$ sekä $v(Q, s_2) = \text{true}$ ja muutoin $v(Q, s) = \text{false}$.

1. $\mathcal{M}, s_2 \not\models \mathbf{AX}P$, mutta $\mathcal{M}, s_3 \models \mathbf{AX}P$.
2. $\mathcal{M}, s_2 \not\models \mathbf{A}(Q\mathbf{U}P)$, mutta $\mathcal{M}, s_2 \models \mathbf{E}(Q\mathbf{U}P)$.
3. $\mathcal{M}, s_3 \not\models \mathbf{E}(Q\mathbf{U}P)$, mutta $\mathcal{M}, s_4 \models \mathbf{A}(Q\mathbf{U}P)$.

Lisää temporaalioperaattoreita

- Määritellään seuraavat operaattorit lyhennysmerkintöinä:

$$\begin{array}{ll} \mathbf{EX}P\text{: } \neg\mathbf{AX}\neg P & \mathbf{AG}P\text{: } \neg\mathbf{EF}\neg P \\ \mathbf{AF}P\text{: } \mathbf{A}(\top\mathbf{U}P) & \mathbf{EG}P\text{: } \neg\mathbf{AF}\neg P \\ \mathbf{EF}P\text{: } \mathbf{E}(\top\mathbf{U}P) & \end{array}$$

- Huomaa refleksiivisyys ja transitiivisuus operaattorissa $\mathbf{U}$:

  Esimerkki. Jos $\mathcal{M}, s_0 \models P$, niin $\mathcal{M}, s_0 \models \mathbf{A}(Q\mathbf{U}P)$ ja $\mathcal{M}, s_0 \models \mathbf{E}(Q\mathbf{U}P)$
  (ja siis esim. $\mathcal{M}, s_0 \models \mathbf{AF}P$).
  Jos $s_0 R s_1$, $s_1 R s_2$ ja $\mathcal{M}, s_2 \models P$, niin $\mathcal{M}, s_0 \models \mathbf{E}(\top\mathbf{U}P)$ $(= \mathbf{EF}P)$.

4. LTL (Linear Temporal Logic)

- Lineaarisen ajan temporaalilogiikka, jossa operaattorit $\mathbf{X}, \mathbf{U}, \mathbf{G}, \mathbf{F}$.
- Syntaksi:
  - Jokainen atomilause on LTL-lause.
  - Jos P, Q ovat LTL-lauseita, niin $P \wedge Q$, $\neg P$, $\mathbf{X}P$, $P\mathbf{U}Q$ ovat myös LTL-lauseita.
- Esimerkkejä: $\neg\mathbf{X}(P \wedge \neg Q)$ ja $\mathbf{X}(\mathbf{X}(\mathbf{X}P\mathbf{U}(Q \wedge P)) \wedge P)$.
- Mm. operaattorit $\mathbf{G}$ ja $\mathbf{F}$ määritellään em. operaattorien avulla lyhennysmerkintöinä: $\mathbf{F}P = \top\mathbf{U}P$ ja $\mathbf{G}P = \neg\mathbf{F}\neg P$.
- Huom! Operaattorien $\mathbf{X}$ ja $\mathbf{U}$ sisäkkäisyys ja Boolen yhdistelmät ovat mahdollisia kuten LTL-lauseessa $(\mathbf{X}(\neg\mathbf{X}P))\mathbf{U}(\mathbf{X}(\mathbf{X}P))$.

LTL-mallit ja totuusmääritelmä

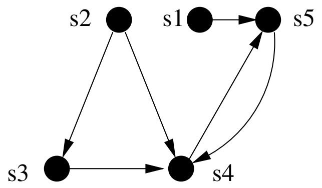
- LTL-malli on kuten CTL-malli mutta lauseet tulkitaan täysillä poluilla (eikä tiloissa kuten CTL:ssä).
- Jos $x = (s_0, s_1, \ldots)$ on täysi polku, niin $x^i = (s_i, s_{i+1}, \ldots)$.

Määritelmä. Olkoon $\mathcal{M}$ LTL-malli ja $x = (s_0, s_1, \ldots)$ sen täysi polku.

- $\mathcal{M}, x \models P$ joss $v(s_0, P) = \text{true}$, missä P on atomilause.
- $\mathcal{M}, x \models \neg P$ joss $\mathcal{M}, x \not\models P$.
- $\mathcal{M}, x \models P \wedge Q$ joss $\mathcal{M}, x \models P$ ja $\mathcal{M}, x \models Q$.
- $\mathcal{M}, x \models \mathbf{X}P$ joss $\mathcal{M}, x^1 \models P$.
- $\mathcal{M}, x \models P\mathbf{U}Q$ joss on olemassa $i \geq 0$, jolle $\mathcal{M}, x^i \models Q$ ja $\mathcal{M}, x^j \models P$ kaikille $0 \leq j < i$.

Esimerkki

Palataan vielä kertaalleen malliin M:



Atomilauseiden totuusarvot määriteltiin $v(P, s_4) = \text{true}$ ja muutoin $v(P, s) = \text{false}$ sekä $v(Q, s_2) = \text{true}$ ja muutoin $v(Q, s) = \text{false}$.

Täysien polkujen $x_1 = (s2, s3, s4, s5, s4, \ldots)$ ja $x_2 = (s2, s4, s5, s4, \ldots)$ osalta voidaan todeta seuraavaa:

1. $M, x_1 \not\models \mathbf{X}P$, mutta $M, x_2 \models \mathbf{X}P$.
2. $M, x_1 \not\models Q\mathbf{U}P$, mutta $M, x_2 \models Q\mathbf{U}P$.

Lisää temporaalioperaattoreita

- Määritellään seuraavat operaattorit lyhennysmerkintöinä:

  $\mathbf{F}P$: $\top\mathbf{U}P$ $\mathbf{G}P$: $\neg\mathbf{F}\neg P$

  $\overset{\infty}{\mathbf{F}}P$: $\mathbf{GF}P$ $\overset{\infty}{\mathbf{G}}P$: $\mathbf{FG}P$

  $P\mathbf{B}Q$: $\neg((\neg P)\mathbf{U}Q)$

  (engl. before)
- Huomaa refleksiivisyys ja transitiivisuus operaattorissa $\mathbf{U}$:

  Esimerkki. Jos $\mathcal{M}, x \models P$, niin $\mathcal{M}, x \models (Q\mathbf{U}P)$.

  Jos $\mathcal{M}, x \models \mathbf{X}^i P$ jollekin $i \geq 0$, niin $\mathcal{M}, x \models (\top\mathbf{U}P)$.

  Itse asiassa kaikilla $\mathcal{M}, x$ pätee esim. seuraavat: $\mathcal{M}, x \models \mathbf{G}P \rightarrow P$ ja $\mathcal{M}, x \models \mathbf{G}P \rightarrow \mathbf{GG}P$.

5. CTL*

- Idea: CTL* = CTL (tilalauseet) + LTL (polkulauseet).
- Seuraavilla säännöillä saatavat **tilalauseet** ovat CTL*-lauseita:
  - Jokainen atomilause on tilalause.
  - Jos P, Q ovat tilalauseita, niin $P \wedge Q$ ja $\neg P$ ovat myös.
  - Jos P on polkulause, niin $\mathbf{E}P$ ja $\mathbf{A}P$ ovat tilalauseita.
  - Jokainen tilalause on polkulause.
  - Jos P, Q ovat polkulauseita, niin $P \wedge Q$ ja $\neg P$ ovat myös.
  - Jos P, Q ovat polkulauseita, niin $\mathbf{X}P$ ja $P\mathbf{U}Q$ ovat polkulauseita.

Esimerkki. Mm. $\mathbf{E}\neg(P\mathbf{U}Q)$ on CTL*-lause mutta $\neg(P\mathbf{U}Q)$ ei.

CTL*-mallit ja totuusmääritelmä

Määritelmä. Olkoon $\mathcal{M}$ CTL*-malli ja s sen mikä tahansa tila.

- $\mathcal{M}, s \models P$ joss $v(s, P) = \text{true}$, kun P on atomilause.
- $\mathcal{M}, s \models \neg P$ joss $\mathcal{M}, s \not\models P$.
- $\mathcal{M}, s \models P \wedge Q$ joss $\mathcal{M}, s \models P$ ja $\mathcal{M}, s \models Q$.
- $\mathcal{M}, s \models \mathbf{E}P$ joss mallissa $\mathcal{M}$ on olemassa täysi polku $x = (s_0, s_1, \ldots)$, missä $s_0 = s$ ja jolle $\mathcal{M}, x \models P$.
- $\mathcal{M}, s \models \mathbf{A}P$ joss mallissa $\mathcal{M}$ kaikille täysille poluille $x = (s_0, s_1, \ldots)$, missä $s_0 = s$, pätee $\mathcal{M}, x \models P$.

Relaatio $\mathcal{M}, x \models P$ määritellään seuraavaksi.

Totuusmääritelmä (jatkuu)

Määritelmä.
Olkoon $x = (s_0, s_1, \ldots)$ mikä tahansa CTL*-mallin $\mathcal{M}$ täysi polku.

- $\mathcal{M}, x \models P$ joss $\mathcal{M}, s_0 \models P$, missä P on mikä tahansa tilalause.
- $\mathcal{M}, x \models \neg P$ joss $\mathcal{M}, x \not\models P$.
- $\mathcal{M}, x \models P \wedge Q$ joss $\mathcal{M}, x \models P$ ja $\mathcal{M}, x \models Q$.
- $\mathcal{M}, x \models \mathbf{X}P$ joss $\mathcal{M}, x^1 \models P$
- $\mathcal{M}, x \models P\mathbf{U}Q$ joss on olemassa $i \geq 0$ siten, että $\mathcal{M}, x^i \models Q$ ja $\mathcal{M}, x^j \models P$ kaikille $0 \leq j < i$.

6. Pätevyys ja toteutuvuus

- CTL/CTL*

  Lause (tilalause) P on pätevä mallissa $\mathcal{M}$ ($\mathcal{M} \models P$), joss $\mathcal{M}, s \models P$ jokaiselle mallin $\mathcal{M}$ tilalle s.

  Lause P on toteutuva, joss on olemassa malli $\mathcal{M}$ ja tila s siten, että $\mathcal{M}, s \models P$.
- LTL

  Lause (polkulause) P on pätevä mallissa $\mathcal{M}$ ($\mathcal{M} \models P$), joss $\mathcal{M}, x \models P$ jokaiselle mallin $\mathcal{M}$ täydelle polulle x.

  Lause P on toteutuva, joss on olemassa malli $\mathcal{M}$ ja sen täysi polku x siten, että $\mathcal{M}, x \models P$.
- Lause on pätevä, joss se on pätevä jokaisessa mallissa, joss sen negaatio ei ole toteutuva.