

TEMPORAALIOLOGIIKKA

1. Johdanto temporaalilogiikkaan
2. Rinnakkainen ja hajautettu laskenta
3. CTL (Computation Tree Logic)
4. LTL (Linear Temporal Logic)
5. CTL*
6. Pätevyys ja toteutuvuus

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).

Temporaalioperaattoreita

- **FQ** (joskus tulevaisuudessa, engl. *future*)
- **GQ** = $\neg F\neg Q$ (aina tulevaisuudessa, engl. *globally*)
- **PQ** (joskus menneisydessä, engl. *past*)
- **HQ** = $\neg P\neg Q$ (aina menneisydessä, engl. *historically*)
- **Always Q** = $GQ \wedge Q \wedge HQ$ (aina)
- **X** (seuraavassa tilassa, engl. *next*):
Kaikissa/jossakin?
Saavutettavuusrelaatioiden suhde (R_X vs. R_F)?

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, ...

Binäärisiä temporaalioperaattoreita

- **U** (kunnes, engl. *until*):
 $\mathcal{M}, s \Vdash \mathbf{U}A\mathbf{B}$ joss
jollekin $t, sRt, \mathcal{M}, t \Vdash B$ ja kaikille $u \in S$,
jos sRu ja uRt , niin $\mathcal{M}, u \Vdash A$.
 $\implies \top \mathbf{U}B \leftrightarrow \mathbf{F}B$
- **S** (siitä asti kun, engl. *since*):
 $\mathcal{M}, s \Vdash \mathbf{S}A\mathbf{B}$ joss
jollekin $t, tRs, \mathcal{M}, t \Vdash B$ ja kaikille $u \in S$,
jos uRs ja tRu , niin $\mathcal{M}, u \Vdash A$.
 $\implies \top \mathbf{S}B \leftrightarrow \mathbf{P}B$

Dynaaminen logiikka

- Modaaliooperaattori 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:

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

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

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.

2. Rinnakkainen ja hajautettu laskenta

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

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)

3. CTL (Computation Tree Logic)

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

Esimerkki.

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

Temporaalilogiikan soveltaminen (jatkoa)

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

CTL:n syntaksi

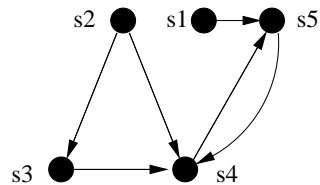
- Huom! Temporaalioperaattoreiden **X/U** sisäkkäisyys ja Boolean yhdistelmät ovat CTL:ssä rajoitettuja:
 - Esim. **AXAXP** on CTL-lause, mutteivät **AXXP** ja **A¬XP**.
- Muut operaattorit (**EX, AG, EG, AF, EF**) määritellään lyhennysmerkintöinä annettujen operaattoreiden (**AX, A(.U.), E(.U.)**) avulla.
- CTL kuvaa laskentapuun ominaisuuksia ja polkukvanttoreilla voidaan kertoa, päteekö tietty ominaisuus jollekin vai kaikille tilasta lähteville laskentapoluille.

Esimerkki. **AXP** (kaikilla laskentapoluilla seuraavassa tilassa P) ja **E(PUQ)** (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 **X**.
- **Täysi polku** on ääretön sekvenssi s_0, s_1, \dots 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.

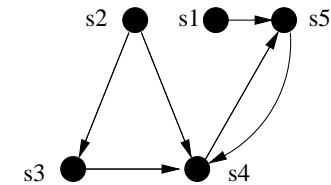
$s_1, s_5, s_4, s_5, s_4, \dots$

$s_2, s_4, s_5, s_4, \dots$

$s_2, s_3, s_4, s_5, s_4, \dots$

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. $\mathcal{M}, s_2 \not\models \mathbf{A}(QUP)$, mutta $\mathcal{M}, s_2 \models \mathbf{E}(QUP)$.
3. $\mathcal{M}, s_3 \not\models \mathbf{E}(QUP)$, mutta $\mathcal{M}, s_4 \models \mathbf{A}(QUP)$.

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 .
- $\mathcal{M}, s \models \mathbf{A}(PUQ)$ joss mallissa \mathcal{M} kaikille täysille poluille (s_0, s_1, \dots) , missä $s = s_0$, on olemassa $i \geq 0$, jolle $\mathcal{M}, s_i \models Q$ ja $\mathcal{M}, s_j \models P$ kaikille $0 \leq j < i$.
- $\mathcal{M}, s \models \mathbf{E}(PUQ)$ joss mallissa \mathcal{M} on olemassa täysi polku (s_0, s_1, \dots) 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 $0 \leq j < i$.

Lisää temporaalioperaattoreita

- Määritellään seuraavat operaattorit lyhennysmerkintöinä:

EXP: $\neg \mathbf{AX} \neg P$ **AGP**: $\neg \mathbf{EF} \neg P$

AFP: $\mathbf{A}(\top U P)$ **EGP**: $\neg \mathbf{AF} \neg P$

EFP: $\mathbf{E}(\top U P)$

- Huomaa **refleksiivisyys** ja **transitiivisuus** operaattorissa **U**:

Esimerkki. Jos $\mathcal{M}, s_0 \models P$, niin $\mathcal{M}, s_0 \models \mathbf{A}(QUP)$ ja $\mathcal{M}, s_0 \models \mathbf{E}(QUP)$

(ja siis esim. $\mathcal{M}, s_0 \models \mathbf{AFP}$).

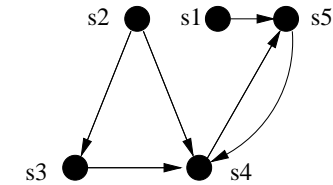
Jos $s_0 R s_1$, $s_1 R s_2$ ja $\mathcal{M}, s_2 \models P$, niin $\mathcal{M}, s_0 \models \mathbf{E}(\top U P)$ (= **EFP**).

4. LTL (Linear Temporal Logic)

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

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 $x_1 = (s_2, s_3, s_4, s_5, s_4, \dots)$ ja $x_2 = (s_2, s_4, s_5, s_4, \dots)$ osalta voidaan todeta seuraavaa:

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

LTL-mallit ja totuusmääritelmä

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

Määritelmä. Olkoon \mathcal{M} LTL-malli ja $x = (s_0, s_1, \dots)$ 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 $\mathcal{M}, x^1 \models P$.
- $\mathcal{M}, x \models \mathbf{P}UQ$ joss on olemassa $i \geq 0$, jolle $\mathcal{M}, x^i \models Q$ ja $\mathcal{M}, x^j \models P$ kaikille $0 \leq j < i$.

Lisää temporaalioperaattoreita

- Määritellään seuraavat operaattorit lyhennysmerkintöinä:

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

$$\overset{\infty}{\mathbf{F}}P: \mathbf{G}F P \qquad \overset{\infty}{\mathbf{G}}P: \mathbf{F}G P$$

$$\mathbf{P}BQ: \neg((\neg P)UQ)$$

(engl. *before*)

- Huomaa **refleksiivisyys** ja **transitiivisuus** operaattorissa **U**:

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

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

Itse asiassa kaikilla \mathcal{M}, x pätee esim. seuraavat:

$$\mathcal{M}, x \models \mathbf{G}P \rightarrow P \text{ ja } \mathcal{M}, x \models \mathbf{G}P \rightarrow \mathbf{G}G P.$$

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 **EP** ja **AP** 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 **XP** ja **PUQ** ovat polkulauseita.

Esimerkki. Mm. $E\neg(PUQ)$ on CTL^* -lause mutta $\neg(PUQ)$ ei.

Totuusmääritelmä (jatkuu)

Määritelmä.

Olkoon $x = (s_0, s_1, \dots)$ 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 $\mathcal{M}, x^1 \models P$
- $\mathcal{M}, x \models \mathbf{P}UQ$ joss on olemassa $i \geq 0$ siten, että $\mathcal{M}, x^i \models Q$ ja $\mathcal{M}, x^j \models P$ kaikille $0 \leq j < i$.

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 $x = (s_0, s_1, \dots)$, 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 $x = (s_0, s_1, \dots)$, missä $s_0 = s$, pätee $\mathcal{M}, x \models P$.

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

6. Pätevyys ja toteutuus

- 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.