



TEMPORAALIOLOGIIKKA

- Sovelletuimpia modaalilogiikkoja
- Aikatulkinta: mahdolliset maailmat mahdollisia ajanhetkiä
- Laskennallinen tulkinta: mahdolliset maailmat mahdollisia laskennan tiloja
- Formaali malli $\langle S, R, v \rangle$:
 sRt : 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/diskreetti/jatkuva/haarautuva...)



Dynaaminen logiikka

- Modaaliooperaattorit tapahtumille:
 $[a]P$ (P tosi aina tapahtuman a jälkeen)
- Tapahtumilla voi olla rakennetta:
 $a; b$ (sarjallistaminen)
 $a \cup b$ (epädeterministinen valinta)
 a^* (toisto)
 $P?$ (Testi: jos P tosi jatketaan muuten ei).

Esimerkki.

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

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



Muita operaattoreita:

- $\mathbf{G}Q = \neg \mathbf{F}\neg Q$; $\mathbf{H}Q = \neg \mathbf{P}\neg Q$
- Always $Q = \mathbf{G}Q \wedge Q \wedge \mathbf{H}Q$ (aina)
- \mathbf{U} (kunnes):
 $\mathcal{M}, s \Vdash A \mathbf{U} B$ joss jollekin t, sRt , $\mathcal{M}, t \Vdash B$ ja kaikilla $u \in S$, jos sRu ja uRt , niin $\mathcal{M}, u \Vdash A$.
 $\Rightarrow \top \mathbf{U} B \leftrightarrow \mathbf{F}B$
- \mathbf{S} (siitä asti kun):
 $\mathcal{M}, s \Vdash A \mathbf{S} B$ joss jollekin t, tRs , $\mathcal{M}, t \Vdash B$ ja kaikilla $u \in S$, jos uRs ja tRu , niin $\mathcal{M}, u \Vdash A$.
 $\Rightarrow \top \mathbf{S} B \leftrightarrow \mathbf{P}B$
- \mathbf{X} (seuraavassa tilassa): kaikissa/jossakin?
 Saavutettavuusrelaatioiden suhde ($R_{\mathbf{X}}$ vs. $R_{\mathbf{F}}$)?



Temporaalilogiikka rinnakkaisessa ja hajautetussa laskennassa

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



Reaktiivisten järjestelmien suunnittelu

- Ko. järjestelmien suunnittelu haastavaa:
 - Virhetilanteet usein vaikeasti toistettavissa
 - Käyttäytyminen “ääretön”
- Tarvitaan uusia menetelmiä:
 - (i) Virheet paikallistettava mahdollisimman aikaisessa vaiheessa suunnittelua/toteutusta.
 - (ii) On pystyttävä käsittelemään päättymättömiä ajoja.



Temporaalilogiikan soveltaminen

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



Temporaalilogiikka

- Formaali malli järjestelmän käyttäytymiselle.
 - Kieli, jolla voidaan määrittellä järjestelmän ominaisuuksia.
- Esimerkki.**
- Keskinäinen poissulkeminen: $\mathbf{G}\neg(at_i(m) \wedge at_j(m'))$
 - Oikeellisuus:

(Osittainen: jos ehto P pätee ohjelman alkutilanteessa m_0 , ehto Q pätee lopputilanteessa m_e .)

$$at(m_0) \wedge P \rightarrow \mathbf{G}(at(m_e) \rightarrow Q)$$

(Kokonaisoikeellisuus: 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):

$$\mathbf{F}v_i \rightarrow (\neg v_i)\mathcal{U}p_i$$



Temporaalilogiikan soveltaminen (II)

- Mallintarkastus
 - Tarkastetaan, onko järjestelmän mallilla halutut ominaisuudet
 - Tutkittavat ominaisuudet temporaalilogiikalla
 - Tehokkaita mallintarkastimia kehitetty
- Sovelletuimmat temporaalilogiikat: CTL ja LTL

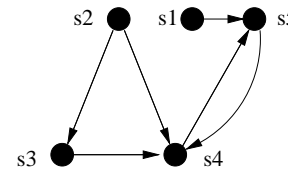
CTL (Computation Tree Logic)

- Temporaalioperaattorit pareja:
 - Polkukvanttori (**A/E**)
 - temporaalioperaattori (**X/U/G/F**)
- 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.
- Esimerkkejä: $(P \wedge Q) \wedge \neg Q$
 $\mathbf{AX}(P \wedge \neg Q)$
 $\mathbf{E}((\mathbf{AXP})\mathbf{U}Q)$

CTL semantiikka

- CTL:n mallit ovat mahdollisten maailmojen malleja $\langle S, R, v \rangle$, joissa saavutettavuusrelaatio R on **sarjallinen**.
- Huom. R on operaattoriin **X** liittyvä relaatio.
- Täysi polku** on ääretön sarja s_0, s_1, \dots tiloja siten, että kaikilla i : $s_i R s_{i+1}$. (Yksi tilasta s_0 lähtevän laskentapuun haara).

Esimerkki. Mallissa M :



Täysiä polkuja esim.

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

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

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

CTL

- Huom. **X/U**-operaattorien sisäkkäisyys ja Boolean yhdistelmät rajoitettuja:
 \mathbf{AXAXP} CTL-lause
 mutteivat \mathbf{AXXP} ja $\mathbf{A}\neg\mathbf{XP}$
- Muut operaattorit (**EX, AG, EG, AF, EF**) määritellään lyhennysmerkintöinä annettujen operaattoreiden (**AX, A(.U.), E(.U.)**) avulla.
- CTL kuvaa laskentapuun ominaisuuksia ja kvanttoreilla voidaan kertoa, päteekö tietty ominaisuus jollekin vai kaikille tilasta lähteville haaroille.
 Esim. \mathbf{AXP} (kaikilla laskentapoluilla seuraavassa tilassa P)
 $\mathbf{E}(PUQ)$ (on olemassa polku, jossa P kunnes Q)

CTL Semantiikka (II)

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 $\mathcal{M}, s \models Q$.
- $\mathcal{M}, s \models \mathbf{AXP}$ 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 , jolle $\mathcal{M}, s_i \models Q$ ja kaikille $j < i$, $\mathcal{M}, s_j \models P$.
- $\mathcal{M}, s \models \mathbf{E}(PUQ)$ joss mallissa \mathcal{M} on olemassa täysi polku (s_0, s_1, \dots) siten, että $s = s_0$ ja on olemassa i , jolle $\mathcal{M}, s_i \models Q$ ja kaikille $j < i$, $\mathcal{M}, s_j \models P$.



CTL Semantiikka (III)

Esimerkki. Olkoon edellisessä mallissa M :

$v(P, s4) = \text{true}$ ja muutoin $v(P, s) = \text{false}$ sekä
 $v(Q, s2) = \text{true}$ ja muutoin $v(Q, s) = \text{false}$.

Nyt $M, s2 \not\models \mathbf{AX}P$ mutta $M, s3 \models \mathbf{AX}P$
 $M, s2 \not\models \mathbf{A}(QUP)$ mutta $M, s2 \models \mathbf{E}(QUP)$
 $M, s3 \not\models \mathbf{E}(QUP)$ mutta $M, s4 \models \mathbf{A}(QUP)$



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.
- Esimerkkejä:
 - $\neg \mathbf{X}(P \wedge \neg Q)$
 - $\mathbf{X}(\mathbf{X}(\mathbf{X}P\mathbf{U}(Q \wedge P))) \wedge P$
- Operaattorit (\mathbf{G}, \mathbf{F}) näiden avulla lyhennysmerkintöinä.
- Huom. \mathbf{X}/\mathbf{U} -operaattorien sisäkkäisyys ja Boolean yhdistelmät mahdollisia: $((\mathbf{X}(\neg \mathbf{X}P))\mathbf{U}(\mathbf{X}(\mathbf{X}P)))$



CTL

- Lyhennysmerkintöjä:

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

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

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

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

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

$M, s_0 \models \mathbf{E}(QUP)$

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

Jos $s_0 R s_1, s_1 R s_2$ ja $M, s_2 \models P$, niin

$M, s_0 \models \mathbf{E}(\top \mathbf{U} P)$ (= \mathbf{EFP}).



LTL semantiikka

LTL-malli on kuten CTL-malli mutta lauseet tulkitaan täysillä poluilla (eikä tiloissa kuten CTL:ssä).

Jos $x = (s_0, s_1, \dots)$ täysi polku, $x^i = (s_i, s_{i+1}, \dots)$

Määritellään milloin mallissa M lause P on tosi täydellä polulla x ($M, x \models P$)

- $M, x \models P$ joss $v(s_0, P) = \text{true}$, missä $x = (s_0, s_1, \dots)$ ja P atomilause.
- $M, x \models \neg P$ joss $M, x \not\models P$.
- $M, x \models P \wedge Q$ joss $M, x \models P$ ja $M, x \models Q$.
- $M, x \models \mathbf{X}P$ joss $M, x^1 \models P$
- $M, x \models P\mathbf{U}Q$ joss on olemassa i , jolle $M, x^i \models Q$ ja kaikille $j < i$ $M, x^j \models P$.

LTL semantiikka (II)

Esimerkki. Edellisessä mallissa M täydet polut

$x_1 = (s_2, s_3, s_4, s_5, s_4, \dots)$ ja

$x_2 = (s_2, s_4, s_5, s_4, \dots)$

Nyt $M, x_1 \not\models \mathbf{X}P$ mutta $M, x_2 \models \mathbf{X}P$

$M, x_1 \not\models QUP$ mutta $M, x_2 \models QUP$

CTL*

$\text{CTL}^* = \text{CTL} + \text{LTL}$

(CTL: tilalauseet/LTL: polkulauseet)

CTL*-lauseita ovat seuraavilla säännöillä saatavat **tilalauseet**.

- 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 $\mathbf{P}UQ$ ovat polkulauseita.

Esim. $\mathbf{E}\neg(\mathbf{P}UQ)$ on CTL*-lause mutta $\neg(\mathbf{P}UQ)$ ei.

LTL

- Lyhennysmerkintöjä:

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

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

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

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

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

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

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

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

Itse asiassa kaikilla M, x pätee esimerkiksi:

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

Semantiikka:

- $M, s_0 \models P$ joss $v(s_0, P) = \text{true}$, kun P on atomilause.
- $M, s_0 \models \neg P$ joss $M, s_0 \not\models P$.
- $M, s_0 \models P \wedge Q$ joss $M, s_0 \models P$ ja $M, s_0 \models Q$.
- $M, s_0 \models \mathbf{E}P$ joss mallissa M on olemassa täysi polku $x = (s_0, s_1, \dots)$, jolle $M, x \models P$
- $M, s_0 \models \mathbf{A}P$ joss mallissa M kaikille täysille poluille $x = (s_0, s_1, \dots)$, $M, x \models P$
- $M, x \models P$ joss $M, s_0 \models P$, missä $x = (s_0, s_1, \dots)$ ja P tilalause.
- $M, x \models \neg P$ joss $M, x \not\models P$
- $M, x \models P \wedge Q$ joss $M, x \models P$ ja $M, x \models Q$.
- $M, x \models \mathbf{X}P$ joss $M, x^1 \models P$
- $M, x \models \mathbf{P}UQ$ joss on olemassa i , jolle $M, x^i \models Q$ ja kaikille $j < i$ $M, x^j \models P$.