TEMPORAALILOGIIKKA

- 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.

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

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

  R usein transitiivinen.
  (lineaarinen/diskreetti/jatkuva/haarautuva...)

Muita operaattoreita:

- $\mathbf{G}Q = \neg\mathbf{F}\neg Q$; $\mathbf{H}Q = \neg\mathbf{P}\neg Q$
- $\mathbf{Always}\ Q = \mathbf{G}Q \wedge Q \wedge \mathbf{H}Q$ (aina)
- $\mathbf{U}$ (kunnes):

  $\mathcal{M}, s \mid\!\mid\!- A\mathbf{U}B$ joss jollekin t, sRt, $\mathcal{M}, t \mid\!\mid\!- B$
  ja kaikilla $u \in S$, jos sRu ja uRt, niin $\mathcal{M}, u \mid\!\mid\!- A$.

  $\boxed{\Rightarrow}$
  $\top\mathbf{U}B \leftrightarrow FB$
- $\mathbf{S}$ (siitä asti kun):

  $\mathcal{M}, s \mid\!\mid\!- A\mathbf{S}B$ joss jollekin t, tRs, $\mathcal{M}, t \mid\!\mid\!- B$
  ja kaikilla $u \in S$, jos uRs ja tRu, niin $\mathcal{M}, u \mid\!\mid\!- A$.

  $\boxed{\Rightarrow}$
  $\top\mathbf{S}B \leftrightarrow PB$
- $\mathbf{X}$ (seuraavassa tilassa):

  Kaikissa seuraavissa/jossakin seuraavassa?
  Saavutettavuusrelaatioiden suhde ($R_{\mathbf{X}}$ vs. $R_{\mathbf{F}}$)?

- Dynaaminen logiikka:

  modaalioperaattorit 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)

Temporaalilogiikka rinnakkaisessa ja hajautetussa laskennassa

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

Temporaalilogiikka

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

  Esimerkki.

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

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)

- Mallintarkastus
  —Tarkastetaan, onko järjestelmän mallilla halutut ominaisuudet
  —Tutkittavat ominaisuudet temp. logiikalla
  —Tehokkaita mallintarkastimia kehitetty

- Sovelletuimmat temporaalilogiikat: CTL ja LTL

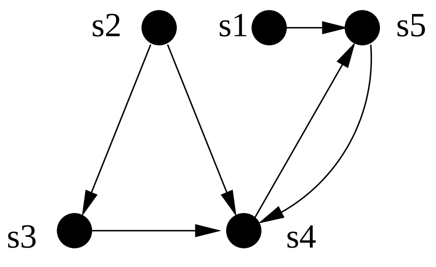
CTL
(Computation Tree Logic)

- Temporaalioperaattorit pareja:
  (i) Polkukvanttori $(\mathbf{A}/\mathbf{E})$
  (ii) temporaalioperaattori $(\mathbf{X}/\mathbf{U}/\mathbf{G}/\mathbf{F})$
- Syntaksi
  - Jokainen atomilause on CTL-lause.
  - Jos P, Q ovat CTL-lauseita, niin $P \land Q$, $\neg P$, $\mathbf{AX}P$, $\mathbf{A}(P\mathbf{U}Q)$, $\mathbf{E}(P\mathbf{U}Q)$ ovat myös.
- Esimerkkejä: $(P \land Q) \land \neg Q$
  $\mathbf{AX}(P \land \neg Q)$
  $\mathbf{E}(\mathbf{AX}P\mathbf{U}Q)$
- Muut operaattorit $(\mathbf{EX}, \mathbf{AG}, \ldots)$ määritellään lyhennysmerkintöinä näiden avulla.
- Huom. $\mathbf{X}/\mathbf{U}$-operaattorien sisäkkäisyys ja Boolen yhdistelmät rajoitettuja:
  $\mathbf{AXAX}P$ CTL-lause
  mutteivat $\mathbf{AXX}P$ ja $\mathbf{A}\neg\mathbf{X}P$

Semantiikka

- CTL:n mallit ovat mahdollisten maailmojen malleja $\langle S, R, v\rangle$, joissa saavutettavuusrelaatio R on sarjallinen.
- Huom. R on operaattoriin $\mathbf{X}$ liittyvä relaatio.
- **Täysi polku** on ääretön sarja $s_0, s_1, \ldots$ tiloja siten, että kaikilla i: s_iRs_{i+1}.

Esimerkki. Mallissa M:



Täysiä polkuja esim.
$s1, s5, s4, s5, s4, \ldots$
$s2, s4, s5, s4, \ldots$
$s2, s3, s4, s5, s4, \ldots$

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 $(s_0, s_1, \dots)$ missä $s = s_0$, on olemassa i, jolle $\mathcal{M}, s_i \models Q$ ja kaikille $j < i$, $\mathcal{M}, s_j \models P$.
- $\mathcal{M}, s \models \mathbf{E}(P\mathbf{U}Q)$ 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 $j < i$, $\mathcal{M}, s_j \models P$.

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 $\mathcal{M}, s2 \not\models \mathbf{AX}P$ mutta $\mathcal{M}, s3 \models \mathbf{AX}P$
$\mathcal{M}, s2 \not\models \mathbf{A}(Q\mathbf{U}P)$ mutta $\mathcal{M}, s2 \models \mathbf{E}(Q\mathbf{U}P)$
$\mathcal{M}, s3 \not\models \mathbf{E}(Q\mathbf{U}P)$ mutta $\mathcal{M}, s4 \models \mathbf{A}(Q\mathbf{U}P)$

- Lyhennysmerkintöjä:
  $\mathbf{EX}P$: $\neg\mathbf{AX}\neg P$
  $\mathbf{AF}P$: $\mathbf{A}(\top\mathbf{U}P)$
  $\mathbf{EF}P$: $\mathbf{E}(\top\mathbf{U}P)$
  $\mathbf{AG}P$: $\neg\mathbf{EF}\neg P$
  $\mathbf{EG}P$: $\neg\mathbf{AF}\neg P$
- Huomaa refleksiivisyys ja transitiivisuus operaattorissa $\mathbf{U}$:
  Jos $\mathcal{M}, s_0 \models P$, niin $\mathcal{M}, s_0 \models \mathbf{A}(Q\mathbf{U}P)$ (ja siis esim. $\mathcal{M}, s_0 \models \mathbf{AF}P$).
  Jos s_0Rs_1, s_1Rs_2 ja $\mathcal{M}, s_2 \models P$, niin $\mathcal{M}, s_0 \models \mathbf{EF}P$.

LTL
(Linear Temporal Logic)

- Lineaarisen ajan temporaalilogiikka, jossa operaattori $\mathbf{X}, \mathbf{U}, \mathbf{G}, \mathbf{F}$
- 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 Boolen yhdistelmät mahdollisia: $(\mathbf{X}\neg\mathbf{X}P)\mathbf{U}(\mathbf{XX}P)$

Semantiikka

LTL-malli kuten CTL-malli
(joukko täydellisiä polkuja).

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

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

- $\mathcal{M}, x \models P$ joss $v(s_0, P) = \text{true}$, missä $x = (s_0, s_1, \dots)$ ja P 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, jolle $\mathcal{M}, x^i \models Q$ ja kaikille $j < i$ $\mathcal{M}, x^j \models P$.

Esimerkki. Edellisessä mallissa M täydet polut
$x_1 = (s2, s3, s4, s5, s4, \dots)$ ja
$x_2 = (s2, s4, s5, s4, \dots)$
Nyt $M, x_1 \not\models \mathbf{X}P$ mutta $M, x_2 \not\models \mathbf{X}P$
$M, x_1 \not\models Q\mathbf{U}P$ mutta $M, x_2 \models Q\mathbf{U}P$

- Lyhennysmerkintöjä:

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

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

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

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

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

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

  $\mathcal{M}, x \models \mathbf{G}P \to P$

  $\mathcal{M}, x \models \mathbf{G}P \to \mathbf{GG}P$

CTL*

Syntaksi

CTL* = CTL + 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 $P\mathbf{U}Q$ ovat polkulauseita.

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

Semantiikka

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