Pätevyys ja toteutuvuus

- CTL/CTL*

  Lause (tilalause) P on pätevä, jos jokaiselle mallille $\mathcal{M}$ ja tilalle s, $\mathcal{M}, s \models P$.

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

- LTL

  Lause (polkulause) P on pätevä, jos jokaiselle mallille $\mathcal{M}$ ja jokaiselle sen täydelle polulle x, $\mathcal{M}, x \models P$.

  Lause P on toteutuva, jos on olemassa malli $\mathcal{M}$ ja sen täysi polku x siten, että $\mathcal{M}, x \models P$.

Huom! Lause on pätevä joss sen negaatio ei ole toteutuva.

CTL vs. LTL

- LTL-lauseen totuus määräytyy mallin antamien **täysien polkujen** perusteella.
- CTL-lauseen totuus määräytyy mallin $\mathcal{M} = \langle S, R, v \rangle$ antaman **laskentapuun** $\hat{\mathcal{M}} = \langle \hat{S}, \hat{R}, \hat{v} \rangle$ perusteella, missä

  $\hat{S}$, $\hat{R}$ ovat pienimmät joukot, joille

  - $\langle s_0, 0 \rangle \in \hat{S}$
  - jos $\langle s, n \rangle \in \hat{S}$, niin $\{\langle t, n+1 \rangle \mid sRt\} \subseteq \hat{S}$ ja $\{\langle \langle s, n \rangle, \langle t, n+1 \rangle \rangle \mid sRt\} \subseteq \hat{R}$

  ja $\hat{v}(\langle s, n \rangle, P) = v(s, P)$.

- Mallintarkastuksen kannalta vastavuus:

CTL:	LTL:
$\mathcal{M}, s_0 \models P$	$\mathcal{M}, x \models P$ kaikilla täysillä poluilla $x = (s_0, \ldots)$.

- CTL- ja LTL-operaattorit samantyyppisiä mutta tulkinnat eroavat!

- Mahdollisuuslauseita ei voida ilmaista LTL:llä.

  Esimerkki. CTL-lauseelle $\mathbf{AGEF}P$ ei löydy vastaavaa LTL-lausetta.

  Tarkastellaan CTL-lausetta $\mathbf{GF}P$.

  Lause $\mathbf{AGEF}P$ pätevä mallissa $\mathcal{M} = \langle S, R, v\rangle$:
  $S = \{s_0, s_1\}$, $R = \{\langle s_0, s_0\rangle, \langle s_0, s_1\rangle, \langle s_1, s_0\rangle\}$,
  $v(s_0, P) = \text{false}$, $v(s_1, P) = \text{true}$

  mutta LTL-lause $\mathbf{GF}P$ ei ole pätevä:
  epätosi täydellä polulla $(s_0, s_0, s_0, \dots)$

- On olemassa polku -tyyppiset CTL-lauseet eivät ole ilmaistavissa LTL-lauseilla.

  Esimerkki. CTL-lauseelle $\mathbf{EF}P$ ei löydy vastaavaa LTL-lausetta.

  Tarkastellaan LTL-lausetta $\mathbf{F}P$.
  Lause ei ole pätevä y.o. mallissa $\mathcal{M}$:
  epätosi täydellä polulla $(s_0, s_0, s_0, \dots)$

  mutta lause $\mathbf{EF}P$ on pätevä.

- Reiluusominaisuudet eivät ole ilmaistavissa CTL-lauseina

  Esimerkki. LTL-lauseelle $\mathbf{FG}Q$ ei löydy vastaavaa CTL-lausetta.

  Tarkastellaan CTL-lausetta $\mathbf{AFAG}Q$ ja edellä olevaa mallia $\mathcal{M}$, jossa
  $v(s_0, Q) = \text{true}$, $v(s_1, Q) = \text{false}$

  Lause $\mathbf{FG}Q$ on toteutuva
  (täysi polku $(s_0, s_0, \dots)$)

  mutta CTL-lause $\mathbf{AFAG}Q$ ei ole eikä myöskään lause $\mathbf{EFAG}Q$.

Esimerkkejä temporaalilogiikan käytöstä

- $\mathbf{EF}(started \wedge \neg ready)$

  On mahdollista päästä tilaan, jossa $started$ tosi muttei $ready$.

- $\mathbf{AG}(req \rightarrow \mathbf{AF}ack)$

  Jos pyyntö tulee, saadaan siihen kuittaus.

- $\mathbf{AGAF}enabled$

  $enabled$ on tosi äärettömän usein jokaisella laskentapolulla

- $\mathbf{AGEF}restart$

  Jokaisesta tilasta on mahdollista päästä $restart$ tilaan

CTL/LTL: monen prosessin malli

- CTL/LTL-malli voidaan laajentaa erottamaan eri prosessit yleistämällä saavutettavuusrelaatio $\mathbf{R}$ perheeksi relaatioita $\{R_1, \ldots, R_k\}$, missä kukin R_i on yhden yksittäisen prosessin saavutettavuusrelaatio.

- Huom! Nyt relaation $\bigcup \mathbf{R}$ täytyy olla sarjallinen.

- Operaattori $\mathbf{X}$ voidaan määritellä jokaiselle prosessille:

  $\mathcal{M}, s \models \mathbf{AX}_i P$ joss $\mathcal{M}, t \models P$ kaikilla t, joilla sR_it.

- Täysi polku voidaan määritellä äärettömäksi jonoksi $(s_0, d_1, s_1, d_2, s_2, d_3, \ldots)$, missä kukin d_i antaa indeksin saavutettavuusrelaatioon: kaikilla $i = 1, 2, \ldots,\ s_{i-1}R_{d_i}s_i$.

- Määritellään kullekin prosessille i atomilauseet
  - en_i (prosessi i on toimintavalmis):
    $\mathcal{M}, s \models en_i$ joss on olemassa $t \in S$,
    jolle sR_it
  - ex_i (prosessi i suoritetaan):
    $\mathcal{M}, x \models ex_i$ joss $d_1 = i$
- Esimerkkejä:
  - Lukkiutumattomuus
    $\mathbf{AG}(en_1 \vee \cdots \vee en_k)$
  - Ehdoton reiluus:
    $\bigwedge_{i=1}^{k} \mathbf{GF} ex_i$
  - Heikko reiluus:
    $\bigwedge_{i=1}^{k} (\mathbf{FG} en_i \rightarrow \mathbf{GF} ex_i)$
  - Vahva reiluus:
    $\bigwedge_{i=1}^{k} (\mathbf{GF} en_i \rightarrow \mathbf{GF} ex_i)$

Turvallisuus- ja elävyysominaisuudet

- Turvallisuusominaisuuksia
  (mitään pahaa ei tapahdu):
  - Lukkiutumattomuus:
    $\mathbf{AG}(en_1 \vee \cdots \vee en_k)$
  - Keskinäinen poissulkeminen:
    $\mathbf{AG}\neg(atCS_1 \wedge atCS_2)$
  - Osittainen oikeellisuus:
    $atl_0 \wedge P \rightarrow \mathbf{AG}(atl_h \rightarrow Q)$
- Elävyysominaisuuksia
  (jotain hyvää tapahtuu)
  - Temporaali-implikaatio:
    $\mathbf{AG}(P \rightarrow \mathbf{AF} Q)$
  - Nälkiintymättömyys:
    $\mathbf{AG}(atTry_i \rightarrow \mathbf{AF} atCS_i)$
  - Totaalinen oikeellisuus:
    $atl_0 \wedge P \rightarrow \mathbf{AF}(atL_h \wedge Q)$