Pätevyys ja toteutuvuus

- CTL/CTL*

  Lause (tilalause) P on pätevä mallissa $\mathcal{M}$ ($\mathcal{M} \models P$), jos jokaiselle mallin 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 mallissa $\mathcal{M}$ ($\mathcal{M} \models P$), jos jokaiselle mallin 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 $\mathcal{M}, x \models P$.

- Lause on pätevä, jos se on pätevä jokaisessa mallissa.
  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.

  Teknisesti malli $\mathcal{M}$ voidaan "avata" laskentapuuksi $\hat{\mathcal{M}} = \langle \hat{S}, \hat{R}, \hat{v}\rangle$ missä solmut $\hat{S}$ ovat pareja $\langle s, n\rangle$ s.e. $s \in S$ ja n on luonnollinen luku (antaa kullekin puun tilalle yksikäsitteisen tunnisteen):
  (i) aloittamalla tilasta $\langle s_0, 0\rangle$,
  (ii) avaamalla mallia käyttämällä sääntöä:
  jos $\langle s, n\rangle \in \hat{S}$ ja sRt, niin $\langle t, m\rangle \in \hat{S}$ ja $\langle\langle s, n\rangle, \langle t, m\rangle\rangle \in \hat{R}$, missä m on uusi luonnollinen luku, joka ei ole muualla käytössä.
  (iii) ottamalla valuaatioksi: $\hat{v}(\langle s, n\rangle, P) = v(s, P)$.

- Mallintarkastuksen kannalta vastavuus:

  CTL: $\mathcal{M}, s_0 \models P$

  LTL: $\mathcal{M}, x \models P$ 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 LTL-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: se on epätosi täydellä polulla $(s_0, s_0, s_0, \ldots)$

- Siis "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 $(s_0, s_0, s_0, \ldots)$

  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 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 $(s_0, s_0, \ldots)$)

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

Esimerkkejä

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

Vaatimusmäärittelyt

- Temporaalilogiikkaa käytetään reaktiivisten järjestelmien vaatimusmäärittelyyn
- Tyypilliset järjestelmän vaatimukset voidaan jakaa seuraaviin luokkiin
  - Saavutettavuusominaisuudet
  - Turvallisuusominaisuudet
  - Elävyysominaisuudet
  - Reiluusominaisuudet

Saavutettavuusominaisuudet

- Yksinkertaisin ominaisuusluokka, joka ilmaisee, että jokin järjestelmän tila (jossa annetut ehdot P ovat voimassa) on saavutettavissa (järjestelmän alkutilasta).
- Vastaava temporaalilause: $\mathbf{EF}P$.
- Esimerkkejä:
  $\mathbf{EF}(started \wedge \neg ready)$
  $\mathbf{EF}(restart)$
- Monimutkaisempi luokka: ehdollinen saavutettavuus $\mathbf{E}(Q\mathbf{U}P)$
- Esimerkki: $\mathbf{E}(\neg restart\mathbf{U}ready)$

Turvallisuusominaisuudet

- Turvallisuusominaisuudet ilmaisevat, ettei mitään pahaa ei tapahdu.
- Turvallisuusominaisuudella tarkoitetaan vaatimusta, jolle löytyy aina "äärellinen vastasuoritus":
  jos järjestelmä ei toteuta annettua turvallisuusominaisuutta, on sillä äärellinen suoritus, joka rikkoo omaisuuden.
- Esimerkkejä
  - Keskinäinen poissulkeminen: $\mathbf{AG}\neg(atCS_1 \wedge atCS_2)$
  - Osittainen oikeellisuus: $atl_0 \wedge P \rightarrow \mathbf{AG}(atl_h \rightarrow Q)$

Elävyysominaisuudet

- Elävyysominaisuudet ilmaisevat, että jotain hyvää tapahtuu.
- Elävyysominaisuudella ei ole "äärellistä vastasuoritusta":
  jos järjestelmä ei toteuta annettua elävyysominaisuutta, tämä näkyy vain äärettömissä suorituksissa.
- Esimerkkejä
  - (Toistettava) saavutettavuus: $\mathbf{AGEF}restart$
  - Temporaali-implikaatio: $\mathbf{AG}(P \rightarrow \mathbf{AF}Q)$
  - Nälkiintymättömyys: $\mathbf{AG}(atTry_i \rightarrow \mathbf{AF}atCS_i)$
  - Totaalinen oikeellisuus: $atl_0 \wedge P \rightarrow \mathbf{AF}(atL_h \wedge Q)$

Reiluusominaisuudet

- Reiluusominaisuudet ovat elävyysominaisuuksia, jotka vaativat, että annetun ehdon toteuttava tila toistuu äärettömän usein.
- Reiluusehdot eivät ole suoraan ilmaistavissa CTL-logiikalla mutta ovat LTL-logiikalla.
- Esimerkkejä
  - Määritellään prosessille atomilauseet
    en (prosessi on toimintavalmis) ja ex (prosessi suoritetaan).
  - Ehdoton reiluus: $\mathbf{GF}ex$
  - Heikko reiluus: $\mathbf{FG}en \rightarrow \mathbf{GF}ex$
  - Vahva reiluus: $\mathbf{GF}en \rightarrow \mathbf{GF}ex$

Reiluusominaisuudet ja CTL

- Käytettäessä CTL-logiikkaa reiluusvaatimukset käsitellään muuttamalla polkukvanttorien ($\mathbf{A}/\mathbf{E}$) semantiikkaa:
  kvantifiointi on yli reilujen polkujen
  (eikä kaikkein polkujen kuten perustapauksessa).
- Reiluusehdot annetaan joukkona lauseita F.
- Täysi polku x on F-reilu joss jokaiselle $P \in F$ jokin tila, jossa P on tosi, esiintyy äärettömän usein polulla x.

Reiluusominaisuudet ja CTL

- F-reilu semantiikka ($\models_F$) siis huomioi ainoastaan F-reilut polut.
- Relaatio $\models_F$ määritellään kuten $\models$ paitsi, että polkukvantifiointi koskee vain F-reiluja polkuja:
  - $\mathcal{M}, s \models_F P$ joss on olemassa tilasta s alkava F-reilu täysi polku ja $v(s, P) = \text{true}$, kun P on atomilause
  - $\mathcal{M}, s \models_F \mathbf{A}(P\mathbf{U}Q)$ joss mallissa $\mathcal{M}$ kaikille F-reiluille täysille poluille $(s_0, s_1, \ldots)$ missä $s = s_0$, on olemassa i, jolle $\mathcal{M}, s_i \models_F Q$ ja kaikille $j < i$, $\mathcal{M}, s_j \models_F P$.
  - $\mathcal{M}, s \models_F \mathbf{E}(P\mathbf{U}Q)$ joss mallissa $\mathcal{M}$ on olemassa F-reilu täysi polku $(s_0, s_1, \ldots)$ siten, että $s = s_0$ ja on olemassa i, jolle $\mathcal{M}, s_i \models_F Q$ ja kaikille $j < i$, $\mathcal{M}, s_j \models_F P$.
- Esim. ehdoton reiluus: $F = \{ex\}$ ja reilu kanava: $F = \{send \rightarrow rec\}$