OMINAISUUKSIEN ILMAISEMINEN TEMPORAALILOGIIKALLA

1. CTL vs. LTL
2. Esimerkkejä temporaalilauseista
3. Vaatimusmäärittelyt
4. Reiluusominaisuudet ja CTL

E. M. Clarke et al.: *Model Checking*, luku 3 (s. 27–33).

1. CTL vs. LTL

- LTL-lauseen totuus määräytyy mallin antamista **täysistä poluista**.
- Sen sijaan 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 seuraavaa 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 $\hat{v}(\langle s, n \rangle, P) = v(s, P)$ kaikilla $\langle s, n \rangle$.

- 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 ovat samantyyppisiä, mutta niiden tulkinnat eroavat!
- Mahdollisuuslauseita ei voida ilmaista LTL:llä.

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

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

Sen sijaan LTL-lause $\mathbf{GF}P$ ei ole pätevä, koska se on epätosi täydellä polulla $(s_0, s_0, s_0, \ldots)$.

Eroja ilmaisuvoimassa

- Siis "on olemassa polku" -tyyppiset CTL-lauseet eivät ole ilmaistavissa LTL-lauseilla.

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

  LTL-lause $\mathbf{F}P$ ei ole pätevä em. mallissa $\mathcal{M}$, koska se on 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 annettua mallia $\mathcal{M}$ ja asetetaan $v(s_0, Q) = \text{true}$ ja $v(s_1, Q) = \text{false}$.

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

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

2. Esimerkkejä temporaalilauseista

- $\mathbf{EF}(started \wedge \neg ready)$:
  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 tilaan *restart*.

3. Vaatimusmäärittelyt

- Temporaalilogiikkoja voidaan käyttää reaktiivisten järjestelmien vaatimusmäärittelyyn.
- Tyypilliset reaktiivisille järjestelmille asetettavat vaatimukset jakutuvat seuraaviin luokkiin:
  1. Saavutettavuusominaisuudet
  2. Turvallisuusominaisuudet
  3. Elävyysominaisuudet
  4. Reiluusominaisuudet

Saavutettavuusominaisuudet

- Yksinkertaisin ominaisuusluokka, joka ilmaisee, että jokin järjestelmän tila (jossa annettu ehto P on voimassa) on saavutettavissa (järjestelmän alkutilasta).
- Vastaavat temporaalilauseet ovat muotoa $\mathbf{EF}P$.
- Ehdollinen saavutettavuus on ilmaistavissa lauseella $\mathbf{E}(Q\mathbf{U}P)$.

Esimerkki. Tarkastellaan seuraavia lauseita:

1. $\mathbf{EF}(started \wedge \neg ready)$.
2. $\mathbf{EF}(restart)$.
3. $\mathbf{E}(\neg restart\mathbf{U}ready)$.

Turvallisuusominaisuudet

- Turvallisuusominaisuudet ilmaisevat, että mitään pahaa ei voi tapahtua järjestelmän suorituksen aikana.
- Turvallisuusominaisuudella tarkoitetaan vaatimusta, jolle löytyy ominaisuuden rikkoutuessa aina äärellinen vastasuoritus:
  Jos järjestelmä ei toteuta annettua turvallisuusominaisuutta P, on sillä äärellinen suoritus, jolla P tulee epätodeksi.

Esimerkki. Tarkastellaan seuraavia ominaisuuksia:

1. Keskinäinen poissulkeminen: $\mathbf{AG}\neg(atCS_1 \wedge atCS_2)$.
2. Osittainen oikeellisuus: $atl_0 \wedge P \rightarrow \mathbf{AG}(atl_h \rightarrow Q)$.

Elävyysominaisuudet

- Elävyysominaisuudet ilmaisevat, että jotain hyvää tapahtuu.
- Elävyysominaisuuksille ei ole äärellisiä vastasuorituksia:
  jos järjestelmä ei toteuta annettua elävyysominaisuutta P, tämä on havaittavissa vain äärettömistä suorituksista.

Esimerkki. Tarkastellaan seuraavia ominaisuuksia:

1. (Toistettava) saavutettavuus: $\mathbf{AGEF}restart$.
2. Temporaali-implikaatio: $\mathbf{AG}(P \rightarrow \mathbf{AF}Q)$.
3. Nälkiintymättömyys: $\mathbf{AG}(atTry_i \rightarrow \mathbf{AF}atCS_i)$.
4. 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.

Esimerkki. Määritellään prosessille atomilauseet
en (prosessi on toimintavalmis) ja *ex* (prosessi suoritetaan).

1. Ehdoton reiluus: $\mathbf{GF}ex$.
2. Vahva reiluus: $\mathbf{GF}en \rightarrow \mathbf{GF}ex$.
3. Heikko reiluus: $\mathbf{FG}en \rightarrow \mathbf{GF}ex$.

4. Reiluusominaisuudet ja CTL

- Käytettäessä CTL-logiikkaa reiluusvaatimukset käsitellään muuttamalla polkukvanttorien ($\mathbf{A}/\mathbf{E}$) semantiikkaa.
- Kvantifiointi määritellään yli reilujen polkujen (eikä kaikkien polkujen kuten perustapauksessa).
- Reiluusehdot annetaan joukkona lauseita F ja totuusmääritelmässä otetaan huomioon ainoastaan F-reilut polut:

Määritelmä. Täysi polku x on F-reilu joss jokaiselle $P \in F$ jokin tila, jossa P on tosi, esiintyy äärettömän usein polulla x.

Muunneltu totuusmääritelmä

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 $i \geq 0$, jolle $\mathcal{M}, s_i \models_F Q$ ja $\mathcal{M}, s_j \models_F P$ kaikille $0 \leq j < i$.
- $\mathcal{M}, s \models_F \mathbf{E}(P\mathbf{U}Q)$ joss mallissa $\mathcal{M}$ on olemassa F-reilu täysi polku $(s_0, s_1, \ldots)$ siten, että $s = s_0$ ja on olemassa $i \geq 0$, jolle $\mathcal{M}, s_i \models_F Q$ ja $\mathcal{M}, s_j \models_F P$ kaikille $0 \leq j < i$.

Esimerkki. *Ehdoton reiluus* ilmaistavissa joukolla $F = \{ex\}$ ja *reilu kanava* joukolla $F = \{send \rightarrow rec\}$.