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** perusteella.

  Teknisesti malli $\mathcal{M}$ voidaan "avata" laskentapuuksi $\hat{\mathcal{M}} = \langle \hat{S}, \hat{R}, \hat{v} \rangle$

  (i) ottamalla solmuiksi $\hat{S}$ parit $\langle s, n \rangle$, missä $s \in S$ ja n on luonnollinen luku, joka antaa kullekin puun tilalle yksikäsitteisen tunnisteen,
  (ii) aloittamalla tilasta $\langle s_0, 0 \rangle$ ja
  (iii) 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.

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

- Mallintarkastuksen kannalta vastavuus:

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

- 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 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: $atl_0 \wedge P \rightarrow \mathbf{AF}(atL_h \wedge Q)$

Mallintarkastus

Onko annettu lause P tosi annetussa mallissa M?

- Malli M: järjestelmän malli

  Saadaan järjestelmän kuvauksesta, joka on usein jotain spesifiointikieltä: SDL, VHDL, prosessialgebra, automaatit, Petri-verkot ...

- Lause P: järjestelmän kiinnostava ominaisuus.

  Usein annettu temporaalilogiikalla: CTL, LTL, CTL*, ...

—Täysin automatisoitavissa.

—Realististen järjestelmien mallit usein suuria.

—Jo nykyiset tekniikat teollisesti sovellettavissa.

Mallin generointi

Mallintarkastusta varten järjestelmän kuvauksesta muodostetaan mahdollisten maailmojen malli M.

- Eksplisiittinen esitystapa

  Malli M muodostetaan kuvauksesta saavutettavuusanalyysitekniikalla ennen mallintarkastusta (tilaräjähdys).

- On-the-fly -tekniikka

  Malli M muodostetaan kuvauksesta saavutettavuusanalyysitekniikalla mallintarkastuksen aikana tarpeen mukaan.

- Symbolinen esitystapa

  Tilasiirtymäfunktio esitetään Boolen funktiona symbolisesti.

Globaali ja lokaali mallintarkastus

- Globaali mallintarkastus:

  Missä mallin tiloissa annettu lause P on tosi?

- Lokaali mallintarkastus:

  Onko lause P tosi mallin annetussa tilassa s_0?

Lokaali mallintarkastus (yhdistettynä on-the-fly -tekniikkaan) mahdollistaa mallintarkastuksen, jossa mallin kaikkia tiloja ei tarvitse välttämättä tutkia (eikä edes muodostaa).

Globaalin mallintarkastuksen toteuttaminen on suoraviivaisempaa ja se voidaan saada tehokkaaksi ja vähemmän muistia käyttäväksi.

Laskennallinen vaativuus

- CTL

  Mallitarkastus: $\mathbf{P}$-täydellinen
  $O(|M| \cdot |P|)$

- LTL

  Mallitarkastus: $\mathbf{PSPACE}$-täydellinen
  $O(|M| \cdot exp(|P|))$

- CTL*

  Mallitarkastus: $\mathbf{PSPACE}$-täydellinen
  $O(|M| \cdot exp(|P|))$

Globaali CTL-mallintarkastusalgoritmi

(i) Järjestetään lauseen P alilauseet järjestykseen:

$P_0, P_1, \ldots, P_n$ missä P_i esiintyy vasta kaikkien aitojen alilauseidensa jälkeen.

Esimerkki. Lauseen $\mathbf{A}(P\mathbf{U}\mathbf{E}(Q\mathbf{U}\neg P))$ eräs mahdollinen alilausejärjestys:

$P, Q, \neg P, \mathbf{E}(Q\mathbf{U}\neg P), \mathbf{A}(P\mathbf{U}\mathbf{E}(Q\mathbf{U}\neg P))$

(ii) Kaikille $i = 0, 1, \ldots, n$ määrätään lauseen P_i totuusarvo jokaisessa tilassa $s \in S$ seuraavasti:

- Jos P_i atomilause, saadaan totuusarvo suoraan mallista.
- Jos P_i muotoa $\neg P_j$ tai $P_j \wedge P_l$, saadaan totuusarvo alilauseiden P_j, P_l totuusarvoista.
- Jos P_i muotoa $\mathbf{AX}P_j$, saadaan totuusarvo alilauseen P_j totuusarvoista kaikissa s:n seuraajissa.

- Jos P_i muotoa $\mathbf{A}(P_j\mathbf{U}P_l)$, saadaan totuusarvo seuraavasti käyttämällä ekvivalenssia:

  $$\mathbf{A}(P_j\mathbf{U}P_l) \equiv P_l \vee (P_j \wedge \mathbf{AXA}(P_j\mathbf{U}P_l))$$

  1. Merkitään lause P_i todeksi kaikissa tiloissa, joissa P_l on tosi.
  2. Merkitään lause P_i todeksi tilassa s, jos P_j on tosi siinä ja P_i tosi **kaikissa** sen seuraajissa, kunnes uusia tällaisia tiloja ei löydy. Merkitään P_i epätodeksi muissa tiloissa.

- Jos P_i muotoa $\mathbf{E}(P_j\mathbf{U}P_l)$, saadaan totuusarvo seuraavasti käyttämällä ekvivalenssia:

  $$\mathbf{E}(P_j\mathbf{U}P_l) \equiv P_l \vee (P_j \wedge \mathbf{EXE}(P_j\mathbf{U}P_l))$$

  1. Merkitään lause P_i todeksi kaikissa tiloissa, joissa P_l on tosi.
  2. Merkitään lause P_i todeksi tilassa s, jos P_j on tosi siinä ja P_i tosi **jossakin** sen seuraajassa, kunnes uusia tällaisia tiloja ei löydy. Merkitään P_i epätodeksi muissa tiloissa.

Huom! Aikavaativuus $\mathcal{O}(|P| * |S| * (|S| + |R|))$

Toteutustekniikkaa

Lauseiden $\mathbf{A}(P_j\mathbf{U}P_l)$ / $\mathbf{E}(P_j\mathbf{U}P_l)$ evaluointia voidaan parantaa ja päästä aikavaativuuteen $\mathcal{O}(|P| * (|S| + |R|))$.

Esimerkiksi [Clarke/Emerson/Sistla, 1986]:

- Lause P_i muotoa $\mathbf{A}(P_j\mathbf{U}P_l)$:

  Käydään läpi kaikki tilat s:

  Jos lausetta P_i ei ole vielä evaluoitu tilassa s, toimitaan seuraavasti:

  Jos P_l tosi, merkitään lause P_i todeksi ja muutoin jos P_j epätosi, P_i epätodeksi.

  Muutoin (P_l epätosi ja P_j tosi tilassa s), merkitään s ja tarkastetaan rekursiivisesti tilan s seuraajat, kunnes kaikki seuraajat on käyty läpi tai seuraaja, jossa P_i on epätosi, löytyy. P_i tosi tilassa s, jos se on tosi kaikissa seuraajissa.

  Jos tässä tarkastuksessa päädytään merkittyyn tilaan (jossa on jo vierailtu), P_i merkitään tilassa epätodeksi.

- Lause P_i muotoa $\mathbf{E}(P_j\mathbf{U}P_l)$ käyttäen **edeltäjärelaatiota**:

  Käydään läpi kaikki tilat s:

  Jos lausetta P_i ei ole vielä evaluoitu tilassa s ja P_l tosi siinä, merkitään lause P_i tilassa s todeksi ja

  tutkitaan tilan s edeltäjät syvyysuuntaisesti rekursiivisesti (käyden joka tilassa korkeintaan kerran) seuraavasti: jos edeltäjässä t P_j on tosi, merkitään P_i todeksi tilassa t ja tutkitaan t:n edeltäjät.

Nyt kukin tila käsitellään kerran ja lauseiden $\mathbf{A}(P_j\mathbf{U}P_l)/\mathbf{E}(P_j\mathbf{U}P_l)$ evaluoinnin työmäärä korkeintaan $\mathcal{O}(|S| + |R|)$.

- Globaalilla menetelmällä ei saada suoraan vastaesimerkkiä ja joudutaan evaluoimaan lause mallin jokaisessa tilassa, vaikka oltaisiin kiinnostuneita vain yhdestä tilasta.
- On olemassa myös paikallisia mallintarkastusmenetelmiä, joissa sama worst-case aikavaativuus $\mathcal{O}(|P| * (|S| + |R|))$.

Lisää CTL-mallintarkastuksesta esim.

Keijo Heljanko, Model Checking the Branching Time Temporal Logic CTL, Research Report A45, Digital Systems Laboratory, Helsinki University of Technology, May 1997.
`http://www.tcs.hut.fi/pub/reports/A45abstract.html`