Temporaalilogiikat ja automaatit

Sari Leppänen

Helsinki 20.11.2001

Digitaalisten järjestelmien lisensiaattikurssi

Teknillinen korkeakoulu
Tietojenkäsittelyteorian laboratorio

Sisältö

1 Haarautuvan ajan temporaalilogiikat

Rinnakkaisjärjestelmien spesifiointikielenä käytettävä temporaalilogiikka on peräisin filosofiasta, missä se on eräs modaalilogiikan sivuhaara. Pnueli ehdotti artikkelissaan [8] ensimmäisen kerran temporaalilogiikan käyttämistä rinnakkaisilta ja reaktiivisilta järjestelmiltä vaadittavien ominaisuuksien kuvaamiseen. Temporaalilogiikassa laajennetaan klassista propositiologiikkaa ottamalla käyttöön joukko aikaoperaattoreita, joiden avulla on mahdollista kuvata ominaisuuksien ajallisia suhteita määrittelemättä kuitenkaan aikaa sinänsä.

Käytettäessä temporaalilogiikoita järjestelmiä ja ohjelmia koskevissa päättelyissä, aika oletetaan *diskreetiksi* jonoksi, missä peräkkäiset ajan hetket kuvautuvat luonnollisille luvuille. (Tarkastellessamme lineaarisia rakenteita rajoitumme edelleen *luonnollisiin malleihin* ,ks. määritelmä Clarke/Schlingloff s. 1650). Järjestelmää kuvattaessa nykyinen ajan hetki vastaa järjestelmän nykyistä tilaa ja seuraava ajan hetki vastaa järjestelmässä välittömästi seuraavaa tilaa. Jokaisella tilalla on olemassa välitön edeltäjä ja seuraaja.

Järjestelmän mahdolliset suoritukset voidaan mallintaa useiden erillisten laskentasekvenssien joukkona. Vaihtoehtoisesti järjestelmän suoritukset voidaan kuvata yhtenä laskentapuuna, missä haarautuminen kuvaa ohjelman suorituksenaikaista epädeterminististä valintaa. Ajan *luonne* käsitetään nyt haarautuvaksi, jolloin jokaista hetkeä voi seurata useita mahdollisia tulevaisuuden hetkiä. Ajan *rakenne* vastaa siis ääretöntä puuta, missä jokainen puun solmu rinnastetaan yhteen ajanhetkeen. Jokaisella solmulla on vähintään yksi, mutta mahdollisesti äärettömän monta seuraajasolmua. Ajalla on alkuhetki, jolla ei ole edeltäjää, ja tulevaisuus on ääretön. Tällainen näkemys ajasta on omaksuttu *haarautuvan ajan temporaalilogiikan* pohjaksi [7, 1, 5].

Ohjelman oikeellisuutta tarkastellessamme tutkimme laskentapuun *maksimaalisia polkuja*:

Määritelmä 1.1 *Polku $\sigma = (w_1, w_2, \ldots)$ on ääretön tai äärellinen tilajono, joka muodostetaan valitsemalla kullekin tilalle $w_i (0 \leq i < |\sigma|)$ seuraajatila w_{i+1} siten, että $(w_i, w_{i+1}) \in \mathcal{I}(R_j)(R_j \in \mathcal{R})$.*

Määritelmä 1.2 *Polku on maksimaalinen (täyspolku), jos se on ääretön tai jos äärellisen polun viimeisellä tilalla ei ole seuraajia ($\nexists w$ s.e. $w_n \prec w$)*

Maksimaalinen polku on täysin mallin mukainen. Jokaisella tilalla, jolla on alkuperäisessä mallissa seuraajatila, on seuraajatila myös polussa.

1.1 CTL (Computation Tree Logic)

Computation Tree Logic (CTL) on propositionaalinen haarautuvan ajan temporaalilogiikka, jonka Clarke ja Emerson määrittelivät artikkelissaan [3]. Klassisen propositiologiikan mukaisesti atomilauseista muodostetaan loogisilla lausekonnektiiveilla propo-

sitiolauseita, jotka ilmaisevat yksittäisiin ajan hetkiin liittyviä ominaisuuksia. Aikaoperaattoreiden avulla ominaisuudet laajennetaan koskemaan lineaarisia rakenteita, jotka koostuvat peräkkäisistä, aikajärjestykseen asetetuista, ajan hetkistä. CTL:n syntaksi määrittelee ainoastaan aikaoperaattorin *kunnes* ($\mathbf{U}$), jonka avulla voidaan määritellä edelleen muita aikaoperaattoreita.

Laskentapuu järjestelmän suoritusmallina kuvaa sekä tilojen ajallista järjestystä että ohjelman suorituksen haarautumista. CTL sisältää polkukvanttorit *kaikilla poluilla* ($\mathbf{A}$) ja *jollakin polulla* ($\mathbf{A}$), jotka mahdollistavat ominaisuuksien ilmaiseminen haarautuvassa rakenteessa.

Määritelmä 1.3 *CTL kielen syntaksi:*
$\mathbf{CTL} ::= \mathcal{P} \mid \bot \mid (\mathbf{CTL} \rightarrow \mathbf{CTL}) \mid \mathbf{E}\,(\mathbf{CTL}\ \mathbf{U}^+\ \mathbf{CTL}) \mid \mathbf{A}\,(\mathbf{CTL}\ \mathbf{U}^+\ \mathbf{CTL}) \mid.$

CTL:n syntaksi määrittelee tiukasti, että yhteen polkukvanttoriin voi liittyä täsmälleen yksi aikaoperaattori, eli polkukvanttorit ja aikaoperaattorit esiintyvät aina pareittain. CTL kaavat tulkitaan suhteessa järjestelmän suoritusta mallintavaan (äärettömään) laskentapuuhun. Merkitsemme laskentapuun yksikäsitteistä juurisolmua w_0:lla. Kukin laskentapuun solmu voidaan saavuttaa juurisolmusta w_0 ainoastaan yhtä äärellistä polkua pitkin. Seuraajarelaation transitiivisen sulkeuman suhteen siis pätee, että $(w_1, w_2) \in \mathcal{I}(<)$, joss solmu w_1 on juurisolmusta w_0 solmuun w_2 johtavan polun varrella.

$w_0 \models \mathbf{E}(\varphi\ \mathbf{U}^+\ \psi)$ joss on olemassa jokin juurisolmua seuraava solmu w_1, jossa kaava ψ pätee ja kaikissa niissä solmuissa, jotka ovat polulla juurisolmusta solmuun w_1 pätee kaava φ.

$w_0 \models \mathbf{A}(\varphi\ \mathbf{U}^+\ \psi)$ joss kaikilla maksimaalisilla poluilla juurisolmulla on jokin seuraajasolmu w_1, jossa kaava ψ pätee ja kaikilla poluilla, kaikissa juurisolmun ja solmun w_1 välisissä tiloissa pätee φ.

CTL:n syntaksi määrittelee ainoastaan aikaoperaattorin $\mathbf{U}^+$ (yhdessä kummankin polkukvanttorin). Sen avulla voimme kuitenkin määritellä lyhenteet *seuraavassa ajanhetkessä* ($\mathbf{X}$), *jonakin tulevana ajanhetkenä/aina lopulta* ($\mathbf{F}$) ja *aina* ($\mathbf{G}$).

Tarkastellaan aluksi aikaoperaattoria $\mathbf{X}$:

$$\mathbf{EX}\psi \triangleq \mathbf{E}(\bot\mathbf{U}^+\psi) \quad (1)$$
$$\mathbf{AX}\psi \triangleq \mathbf{A}(\bot\mathbf{U}^+\psi) \quad (2)$$
$$\mathbf{E}\overline{\mathbf{X}}\psi \triangleq \neg\mathbf{AX}\neg\psi \quad (3)$$
$$\mathbf{A}\overline{\mathbf{X}}\psi \triangleq \neg\mathbf{EX}\neg\psi \quad (4)$$

Aikaoperaattorilla *seuraavassa ajanhetkessä (tilassa)* on kaksi varianttia. Operaattoreiden $\mathbf{X}$ ja $\overline{\mathbf{X}}$ ero tulee esille ainoastaan, jos järjestelmän mallissa esiintyy *lopputiloja (terminal states)*. Kaava $\mathbf{EX}\psi$ ilmaisee, että välttämättä jossakin seuraajatilassa pätee ψ, joten epäsuorasti kaava vaatii myös, että kulloinkin tarkasteltavalla tilalla on ainakin

yksi seuraajatila. Kaava $\mathbf{A}\overline{\mathbf{X}}\psi$ pätee ainoastaan, jos kaikissa *olemassa olevissa* seuraatiloissa pätee ψ. Jos tarkasteltavalla tilalla ei ole seuraajatiloja, kaava pätee kyseisessä tilassa. Siis lopputilassa, jossa tilalla ei ole yhtään seuraajaa, kaava $\mathbf{A}\overline{\mathbf{X}}\psi$ pätee, mutta $\mathbf{AX}\psi$ ei (huomaa, että operaattori $\mathbf{X}$ määritellään käyttäen operaattoria $\mathbf{U}^+$). Malleissa, joissa ei ole lopputiloja, operaattoriparien $\mathbf{EX}$ ja $\mathbf{E}\overline{\mathbf{X}}$, sekä $\mathbf{AX}$ ja $\mathbf{A}\overline{\mathbf{X}}$ semantiikka on sama.

Kaikki CTL:n *next-time*-operaattorit ovat määriteltävissä $\mathbf{EX}$:n avulla, sillä

$$\mathbf{AX}\psi \quad \leftrightarrow \quad (\mathbf{A}\overline{\mathbf{X}}\psi \wedge \mathbf{EX}\top) \tag{5}$$
$$\mathbf{E}\overline{\mathbf{X}}\psi \quad \leftrightarrow \quad (\mathbf{EX}\psi \vee \mathbf{A}\overline{\mathbf{X}}\bot) \;\leftrightarrow\; (\mathbf{EX}\top \rightarrow \mathbf{EX}\psi). \tag{6}$$

Aikaoperaattorit *jonakin tulevana ajanhetkenä/aina lopulta* ($\mathbf{F}$) ja *aina* ($\mathbf{G}$) määritellään myös lyhenteinä:

$$\mathbf{EF}^+\psi \quad \triangleq \quad \mathbf{E}(\top\mathbf{U}^+\psi) \tag{7}$$
$$\mathbf{EF}^*\psi \quad \triangleq \quad (\psi \vee \mathbf{EF}^+\psi) \tag{8}$$
$$\mathbf{AF}^+\psi \quad \triangleq \quad \mathbf{A}(\top\mathbf{U}^+\psi) \tag{9}$$
$$\mathbf{AF}^*\psi \quad \triangleq \quad (\psi \vee \mathbf{AF}^*\psi) \tag{10}$$
$$\tag{11}$$

$$\mathbf{EG}^+\psi \quad \triangleq \quad \neg\mathbf{AF}^+\neg\psi \tag{12}$$
$$\mathbf{EG}^*\psi \quad \triangleq \quad (\psi \wedge \mathbf{EG}^+\psi) \tag{13}$$
$$\mathbf{AG}^+\psi \quad \triangleq \quad \neg\mathbf{EF}^+\neg\psi \tag{14}$$
$$\mathbf{AG}^*\psi \quad \triangleq \quad (\psi \wedge \mathbf{AG}^+\psi) \tag{15}$$
$$\tag{16}$$

Kaava $\mathbf{EF}^*\psi$ vaatii, että laskentapuussa on ainakin yksi tila, jossa kaava ψ on voimassa. Kaavan $\mathbf{AF}^*\psi$ mukaan ψ toteutuu mallin jokaisella maksimaalisella polulla. Kaava $\mathbf{AG}^*\psi$ ilmaisee *globaalin invarianttiominaisuuden* määrittäessään, että ψ:n tulee olla voimassa kaikkialla. Vastaavasti kaava $\mathbf{EG}^*\psi$ ilmaisee *lokaalin invarianttiominaisuuden* ja vaatii, että jonkin polun kaikissa tiloissa on ψ voimassa .

Kaavat, joissa aikaoperaattori on muotoa $\{\mathbf{G},\mathbf{F}\}^*\psi$ vaativat, että ominaisuus pätee jollekin tai kaikille (riippuen käytetystä polkukvanttorista) tarkasteltasta tilasta lähteville poluille, kyseinen tila mukaanlukien. Kaavat, joissa esiintyy aikaoperaattorin toinen variantti ($\{\mathbf{G},\mathbf{F}\}^+\psi$) ovat kiinnostuneita ominaisuuden voimassaolosta vasta tarkasteltavan tilan välittömistä seuraajatiloista lähtien.

Määrittelemme $*$ -variantit aikaoperaattorille $\mathbf{U}^+$:

$$\mathbf{E}(\varphi\mathbf{U}^*\psi) \quad \triangleq \quad (\psi \vee \varphi \wedge \mathbf{E}(\varphi\mathbf{U}^+\psi)) \tag{17}$$
$$\mathbf{A}(\varphi\mathbf{U}^*\psi) \quad \triangleq \quad (\psi \vee \varphi \wedge \mathbf{A}(\varphi\mathbf{U}^+\psi)) \tag{18}$$

Algoritmien ja todistusten konstruoinnin kannalta on edullista määritellä mahdollisimman vähän perusoperaattoreita. CTL:n syntaksissa määrittelimme perusoperaattoreina $\mathbf{E}(\varphi \mathbf{U}^+ \psi)$ ja $\mathbf{A}(\varphi \mathbf{U}^+ \psi)$. Riittää kuitenkin määritellä $\mathbf{EU}^+$ ja $\mathbf{AF}^+$ perusoperaattoreina, sillä $\mathbf{AU}^+$ voidaan ilmaista näiden avulla:

$$\mathbf{A}(\varphi \mathbf{U}^+ \psi) \quad \leftrightarrow \quad (\mathbf{A}(\varphi \ \mathbf{W}^+ \ \psi)) \wedge \mathbf{AF}^+ \psi) \tag{19}$$

$$= \quad (\neg \mathbf{E}(\neg \psi \mathbf{U}^+ \neg(\varphi \vee \psi)) \wedge \mathbf{AF}^+ \psi). \tag{20}$$

Esimerkiksi CTL-kaava $\mathbf{EF}^+(started \wedge \neg ready)$ ilmaisee ominaisuuden ”jossakin alkutilaa seuraavassa tilassa jokin on aloitettu, mutta ei ole vielä valmis”. Jos kyseessä olisi mikroaaltouuni, kaavan toteutuminen edellyttäisi, että mikroaaltouunin ohjausohjelmassa on mahdollista päästä tilaan, jossa lämmitys on aloitettu, mutta lämmitysaikaa on vielä jäljellä. Koska kaavan toteutuminen selvästikin vaatii, että ”jotakin hyvää tapahtuu”, eli lämmitys aloitetaan (mutta ei samantien lopeteta), se kuvaa elävyysominaisuutta. Kaava $\mathbf{AG}^*(req \rightarrow \mathbf{AF}^+ ack)$ ilmaisee tyypillisesti tietoliikenneprotokollaa kuvaavan turvallisuusominaisuuden ”jos lähetetään pyyntö, siihen aina lopulta saadaan kuittaus”. Kyseessä on globaali invariantti eli kaavan tulee olla voimassa laskentapuun kaikkien polkujen kaikissa tiloissa. Kaavan toteutuminen ei kuitenkaan välttämättä takaa protokollan oikeanlaista toimintaa. Jos järjestelmä ei tee mitään (eikä näin ollen yhtään sanomaa lähetetä), kyseinen ominaisuus on silti voimassa.

Logiikoiden **CTL** ja **LTL** keskinäinen vertailu on hankalaa, sillä alla olevat mallit ovat erilaiset (laskentapuu vs. yksittäinen laskentasekvenssi). Tämän vuoksi tarkastelemmekin logiikoita suhteessa Kripke-malliin $(U, \mathcal{I}, w_0)$. Toisin kuin laskentasekvenssissä ja -puissa, Kripke-mallissa voi olla esimerkiksi silmukoita sekä erillisten tilojen välillä, että tilassa itsessään (self-loop). LTL:n suhteen rajoitumme ainoastaan tulevaisuutta käsitteleviin kaavoihin (future formulae), sillä edellä määrittelimme haarautuvalle ajalle, että alkutila on yksikäsitteinen, eikä sillä ole edeltäviä tiloja. LTL-kaava on *sekvenssipätevä (sequence-valid)* Kripke mallissa $\mathcal{M}$, joss se pätee kaikille kyseisestä mallista generoiduille luonnolllisille malleille $((w_0, w_1, \ldots), \mathcal{I}, w_0)$. Eli jos kaava on voimassa kyseisen maailman $\mathcal{U}$ kaikilla niillä maksimaalisilla poluilla $(w_0, w_1, \ldots)$, jotka alkavat alkutilasta w_0. Vastaavasti CTL-kaava on *puupätevä (tree-valid)*, jos sen ilmaisema ominaisuus on voimassa Kripke-mallista generoidun laskentapuun alkutilassa.

Nyt vertaillessamme LTL ja CTL logiikoiden ilmaisuvoimaa, voimme todeta, että kumpikaan logiikoista ei ole toistaan ilmaisuvoimaisempi. Esimerkiksi LTL-kaava $\mathbf{F}^+\mathbf{G}^+ p$ ei ole ilmaistavissa CTL logiikan kaavana. Vastaavasti CTL-kaava $\mathbf{AG}^+\mathbf{EF}^+ p$ ei ole ilmaistavissa LTL-logiikan kaavana. Kripke-malleilla logiikka CTL^* sisältää logiikat CTL ja LTL. Se erottaa polkukvantifioinnin ja aikakvantifioinnin käsitteet, joten voimme kirjoittaa kaavoja, jotka ovat muotoa $\mathbf{EG}^*\mathbf{F}^* p$. Binääripuilla logiikan $\mathbf{CTL}^*$ ilmaisuvoimaa voidaan verrata ensimmäisen kertaluvun logiikkaan, kun lisätään siihen toisen kertaluvun kvantifiointi laskentapoluille.

2 Propositionaalisesti kvantifioitavat logiikat

Ensimmäisen kertaluvun ja temporaalilogiikan avulla emme kykene ilmaisemaan ominaisuuksia kuten: *"väittämä φ on voimassa joka toisessa pisteessä/laskentasekvenssin tilassa"*. Yritämme ilmaista kyseisen ominaisuuden LTL ja FOL -kaavoina:

$$\mathbf{G}^{2n}_{LTL}\varphi \triangleq \varphi \wedge \mathbf{G}^*(\varphi \rightarrow \overline{XX}\varphi) \quad (21)$$

$$(\mathbf{G}^{2n}_{FOL}\ \varphi)(t_0) \triangleq \varphi(t_0) \wedge \forall t \geq t_0(\varphi(t) \rightarrow \forall t_1, t_2(t \prec t_1 \prec t_2 \rightarrow \varphi(t_2))) \quad (22)$$

Yllä olevat kaavat kuvaavat vahvemman ominaisuuden, kuin mitä alunperin halusimme. Kaavat sisältävät implisiittisen vaatimuksen sille, että jos ominaisuus φ on voimassa alkutilassa ja sitä välittömästi seuraavassa tilassa, niin sen täytyy olla voimassa mallin kaikissa tiloissa.

Otamme käyttöön uuden proposition q, jonka avulla spesifioimme tarkasteltavan mallin (maailman U) ne tilat (pisteet), joissa kaavan φ totuus halutaan evaluoida. Toisin sanoen rajaamme proposition q ilmaiseman ominaisuuden perusteella kokonaistila-avaruudesta (maailmasta) sen osan, jossa kaavan φ ilmaisemaa ominaisuutta tarkastellaan. Kaavan totuus siis määrätään kussakin tilassa "kahdessa eri vaiheessa". Lisäproposition avulla voimme määrittää ominaisuuksia, jotka ovat tyyppiä "joka toisessa tilassa φ":

$$\mathbf{G}^{2n} \leftrightarrow \exists q(\mathbf{G}^{2n}_{LTL}\ q \wedge \mathbf{G}^*(q \rightarrow \varphi) \quad (23)$$

$$(\mathbf{G}^{2n}\varphi)(t_0) \leftrightarrow \exists q((\mathbf{G}^{2n}_{FOL}\ q)(t_0) \wedge \forall t \geq t_0(q(t) \rightarrow \varphi(t)))) \quad (24)$$

Temporaalipropositio, jolla tarkastelun kohteena oleva tila-avaruus määritetään, riippuu luonnollisesti siitä, mikä on tarkastelun kohteena oleva oleva malli (maailma) ja minkälaisen ominaisuuden verifioitava kaava ilmaisee. Ensimmäinen yo. kaavoista (23) on *qTL (quantified Temporal Logic)* logiikkaa ja jälkimmäinen (24) *monadisen toisen kertaluvun logiikkaa (MSOL)*.

2.1 qTL (quantified Temporal Logic)

Väitöskirjassaan *Theoretical Issues in the Design and Verification of Distributed Systems*[**?**, Sis83]uonna 1983 A. P. Sistla määritteli aikalogiikan laajennoksena *qTL* kielen.

Määritelmä 2.1 (qTL kielen syntaksi) *:*
$\mathbf{qTL} ::= \mathcal{P} \mid \mathcal{Q} \mid \perp \mid (\mathbf{qTL} \rightarrow \mathbf{qTL}) \mid (\mathbf{qTL}\ \mathbf{U}^+\ \mathbf{qTL}) \mid \mathbf{qTL}\ \mathbf{U}^-\ \mathbf{qTL}) \mid \exists \mathcal{Q}\, qTL.$

Temporaaliproposition käyttö on mahdollista, kun sisällytämme kieleen toisen syntaktisen luokan propositiomuuttujille. Muuttujavaluaatiot kiinnittävät kuhunkin toisen kertaluvun muuttujaan joukon tiloja kokonaistila-avaruudesta (s.e. $\mathbf{v}(q) \subseteq U$). Kaava $\exists q\ \varphi$ pätee mallille $\mathcal{M} = (\mathcal{U}, \mathcal{I}, v)$, jos φ pätee jollekin mallille $\mathcal{M}' = (\mathcal{U}, \mathcal{I}, v')$,

missä korkeintaan muuttujavaluaatio q:n osalta poikkeaa ”alkuperäisen” mallin $\mathcal{M}$ valuaatiosta. Mallissa $\mathcal{M}'$ tarkasteltavien tilojen joukko voi olla esimerkiksi osajoukko mallin $\mathcal{M}$ tiloista.

Luonnollisilla malleilla $\mathbf{U}^+$ ja $\mathbf{U}^-$ -operaattorit on mahdollista määritellä operaattoreiden $\mathbf{G}^*$ ja $\mathbf{X}$ avulla (Lemma 3.3. + seurauslause):

$$(\varphi \mathbf{U}^+ \psi) \quad \leftrightarrow \quad \forall q(\mathbf{G}^*(\mathbf{X}(\psi \vee (\varphi \wedge q)) \rightarrow \ q) \ \rightarrow \ q). \tag{25}$$

2.2 MSOL (Monadic Second Order Logic)

Vastaavasti, kuin edellä temporaalilogiikkaa, voimme laajentaa myös ensimmäisen kertaluvun logiikkaa (FOL) ja kvantifioida yli *valitun* pistejoukon. FOL logiikan laajennosta kutsutaan *monadiseksi*[1] *toisen kertaluvun logiikaksi (MSOL, Monadic Second Order Language)*.

Määritelmä 2.2 *MSOL kielen syntaksi:*
$\mathbf{MSOL} ::= \mathcal{P}(\mathcal{T}) \mid \mathcal{Q}(\mathcal{T}) \mid \bot \mid (\mathbf{MSOL} \rightarrow \mathbf{MSOL}) \mid \mathcal{R}^+(\mathcal{T}, \mathcal{T}) \mid \exists \mathcal{T}\ MSOL \mid \exists \mathcal{Q}\, MSOL \mid$

Kuten edellä, alla oleva malli on $\mathcal{M} = (\mathcal{U}, \mathcal{I}, v)$ ja eri muuttujavaluaatiot $(v, v', \ldots)$ kiinnittävät kuhunkin luokan Q toisen kertaluvun muuttujaan erilaisia pistejoukkoja maailmasta U.

Luonnollisilla malleilla logiikat qTL ja MSOL ovat yhtä ilmaisuvoimaisia.

2.3 Propositionaalinen μ-kalkyyli

Laskennan vaativuuden kannalta ei ole aina edullista sallia mielivaltaisia kvantifiointeja yli maailman U kaikkien erilaisten tila- tai pisteosajoukkojen. Sen vuoksi tila- tai pistejoukkojen kvantifiointiin liitetään *kiintopisteiden* käsite, joka määrittää tavan kvantifioida tila- tai pistejoukkoja. Kun toisen kertaluvun logiikkaan liitetään kiintopistekvantifiointi, saadaan tuloksena *propositionaalinen μ-kalkyyli (μTL)* [2, 9, 4, 6].

Määritelmä 2.3 *μTL kielen syntaksi:*
$\mu\mathbf{TL} ::= \mathcal{P} \mid \mathcal{Q} \mid \bot \mid (\mu\mathbf{TL} \ \rightarrow \ \mu\mathbf{TL}) \mid \langle \mathcal{R} \rangle \, \mu\mathbf{TL} \mid \nu \mathcal{Q} \, \mu\mathbf{TL}.$

Kielen semantiikka määritellään tässä logiikoiden MSOL ja FOL kautta:

- $\mathbf{MSOL}(\varphi)$, kun $\varphi = \{p \in \mathcal{P}, \bot, (\psi_1 \rightarrow \psi_2), \langle \mathcal{R} \rangle \psi\}$ kuten FOL(φ) (ch. 2.3)
- $\mathbf{MSOL}(q) \ \triangleq \ q(t_0)$, jos $q \in \mathcal{Q}$
- $\mathbf{MSOL}(\nu q \varphi) \ \triangleq \exists q(q(t_0) \wedge \forall t(q(t) \rightarrow \mathbf{MSOL}(\varphi)(t_0 := t)))$

[1] monadinen = yksipaikkainen

- $\mathbf{MSOL}(\mu q \varphi) \triangleq$
  $\forall q(\forall t(\mathbf{MSOL}(\varphi)(t_0 := t) \rightarrow q(t)) \rightarrow q(t_0))$.

Kaava $\varphi(t_0 := t)$ muodostetaan kaavasta φ korvaamalla jokainen muuttujan t_0 vapaa esiintymä muuttujalla t. Perusoperaattorina μ-kalkyylissa on ν, joka on merkitykseltään rajoitettu eksistentiaalikvanttori yli tila- tai pistejoukon. μ-operaattori on merkitykseltään rajoitettu universaalikvanttori ja on määriteltävissä ν-operaatorin avulla: $\mu = \neg\nu q \neg(\varphi\{q := \neg q\})$. Vastaavasti kuin edellä, kaava $\varphi(t := \psi)$ muodostetaan kaavasta φ korvaamalla jokainen muuttujan t vapaa esiintymä kaavalla ψ.

Vaikka kaava $(\varphi \mathbf{U}^+ \psi)$ määritellään eksistentiaalisena ensimmäisen kertaluvun lauseena, $\mu\mathbf{TL}$ kielessä se samaistetaan μ-kaavaan. Kaavassa korvaamme yksipaikkaisen "timanttioperaattorin" $< \mathcal{R} >$ operaattorilla $\mathbf{X}$. Nyt voimme ilmaista kaavan (25) seuraavasti:

$$\mathcal{M} \models (\varphi \mathbf{U}^+ \psi) \quad \leftrightarrow \quad \mathcal{M} \models \mu q \mathbf{X}(\psi \vee \varphi \wedge q). \tag{26}$$

Luonnollisille malleille voidaan vastaavasti muitakin aikaoperaattoreita kuvata $\mu\mathbf{TL}$ kaavoilla:

$$\mathbf{F}^+ \psi \quad \leftrightarrow \quad \mu q \mathbf{X}(\psi \vee q) \tag{27}$$
$$(\varphi \mathbf{W}^+ \psi) \quad \leftrightarrow \quad \nu q \overline{\mathbf{X}}(\psi \vee \varphi \wedge q) \tag{28}$$
$$\mathbf{G}^* \psi \quad \leftrightarrow \quad \nu q(\psi \wedge \overline{\mathbf{X}} q) \tag{29}$$
$$(\varphi \mathbf{U}^* \psi) \quad \leftrightarrow \quad \mu q(\psi \vee \varphi \wedge \mathbf{X} q) \tag{30}$$

$\mu\mathbf{TL}$ on ilmaisuvoimaltaan vähintään samaa luokkaa kuin CTL (ja CTL*) ja suurin osa ohjelmoitavista logiikoista.

2.3.1 Kiintopisteet

Seuraavassa tarkastelemme kvanttoreiden υ ja μ merkitystä käyttäen käsitteitä *suurin* ja *pienin kiintopiste*.

Koska ainoastaan monotonisille kaavoille voidaan taata kiintopisteen olemassaolo, aloitamme monotonisuuden määritelmällä:

Määritelmä 2.4 *Funktio $f : 2^U \rightarrow 2^U$ on monotoninen, jos*

$$P \subseteq Q \quad \rightarrow \quad f(P) \subseteq f(Q). \tag{31}$$

Määritelmä 2.5 *Funktion f kiintopiste on mikä tahansa joukko Q, jolle $f(Q) = Q$.*

Määritelmä 2.6 *Funktion f esikiintopiste on mikä tahansa joukko, $Q \subseteq U$, jolle $f(Q) \subseteq Q$.*

Määritelmä 2.7 *Funktion f jälkikiintopiste on mikä tahansa joukko, $Q \subseteq U$, jolle $Q \subseteq f(Q)$.*

Määritelmä 2.8 *Funktion f suurin kiintopiste on jälkikiintopistejoukkojen yhdiste $\bigcup\{Q|Q \subseteq f(Q)\}$.*

Määritelmä 2.9 *Funktion f pienin kiintopiste on esikiintopisteiden leikkaus $\bigcap\{Q\,|\,f(Q) \subseteq Q\}$.*

Teoreema 1 (Knaster-Tarski) *Olkoon $f : 2^U \to 2^U$ monotoninen funktio. Tällöin*

- *funktiolla f on $\subseteq$-järjestyksen suhteen yksikäsitteinen suurin kiintopiste, joka on $\bigcup\{Q|Q \subseteq f(Q)\}$ ja*
- *funktiolla f on $\subseteq$-järjestyksen suhteen yksikäsitteinen pienin kiintopiste, joka on $\bigcap\{Q\,|\,f(Q) \subseteq Q\}$.*

2.3.2 Predikaattimuuntimet

Kehyksessä $\mathcal{F} = (U, \mathcal{I})$ kaava φ määrittää maailmasta sellaisten pisteiden joukon $\varphi^{\mathcal{F}} \subseteq U$, joissa kaava pätee. Kaava φ, jossa on vapaa propositiomuuttja q määrittää kehyksessä $\mathcal{F} = (U, \mathcal{I})$ funktion, *predikaattimuuntimen* $\varphi^{\mathcal{F}}_q : U \to U$, joka on kuvaus pisteiden joukolta pisteiden joukolle. Jos $Q \subseteq U$, niin $\varphi^{\mathcal{F}}_q(Q) \triangleq \{w|(U, \mathcal{I}', w) \models \varphi\}$, missä $\mathcal{I}'$ eroaa $\mathcal{I}$:sta ainoastaan q:n osalta.

Logiikan $\mu\mathbf{TL}$ ja kiintopisteiden yhteys:

- $(\nu q\ \varphi)^{\mathcal{F}} = gfp(\varphi^{\mathcal{F}}_q)$
- $(\mu q\ \varphi)^{\mathcal{F}} = lfp(\varphi^{\mathcal{F}}_q)$

Kaava φ on positiivinen q:ssa, jos jokainen propositiomuuttujan q vapaa esiintymä kaavassa φ on positiivinen. Kuten yleensä, muuttuja q on kaavassa φ positiivinen, jos muuttujaan liittyvien negaatiomerkkien määrä on parillinen ja negatiivinen, jos siihen liittyvien negaatiomerkkien määrä on pariton.

Propositiomuuttuja q on positiivinen

- kaavassa q,
- kaavassa $(\varphi \to \psi)$, joss se esiintyy negatiivisena kaavassa φ tai positiivisena kaavassa ψ,
- kaavassa $< \mathcal{R} > \varphi$ ja $\nu q'\varphi$, jos se on positiivinen kaavassa φ.

Kaava φ on positiivinen q:ssa, jos sen jokainen alikaava $\nu q\psi$ on positiivinen q:ssa. Jos φ on positiivinen q:ssa, niin $\varphi^{\mathcal{F}}_q$ on monotoninen predikaattimuunnin.

Jos φ on positiivinen, niin

- $\models \nu q\ \varphi \leftrightarrow \varphi\{q := \nu q\ \varphi\}$
- $\models \mu q\ \varphi \leftrightarrow \varphi\{q := \mu q\ \varphi\}$
- Jos $(U,\mathcal{I}) \models (\mathcal{X} \leftrightarrow \varphi\{q := \mathcal{X}\})$, niin
  - $(U,\mathcal{I}) \models (\mathcal{X} \rightarrow \nu q\ \varphi)$ ja
  - $(U,\mathcal{I}) \models (\mu q\ \varphi \rightarrow \mathcal{X})$.
- $(U,\mathcal{I}) \models (\mathcal{X} \rightarrow \varphi\{q := \mathcal{X}\}) \ \rightarrow\ (U,\mathcal{I}) \models (\mathcal{X} \rightarrow \nu q\ \varphi)$
- $(U,\mathcal{I}) \models (\varphi\{q := \mathcal{X}\} \rightarrow \mathcal{X}) \ \rightarrow\ (U,\mathcal{I}) \models (\mu q\ \varphi \rightarrow \mathcal{X})$.

Kaavan (26) mukaan luonnollisilla malleilla $(\varphi \mathbf{U}^+ \psi)$ on kaavan $\mathbf{X}(\psi \vee \varphi \wedge q)$ pienin kiintopiste. Vastaavasti kaavan $\overline{\mathbf{X}}(\psi \vee \varphi \wedge q)$ suurin kiintopiste on $(\varphi \mathbf{W}^+ \psi)$. Näin ollen voimme esittää perustellusti seuraavat *rekursio- ja induktioaksioomat*:

Rekursioaksiooma:

$$\models (\varphi \mathbf{U}^+ \psi) \quad \leftrightarrow \quad \mathbf{X}(\psi \vee \varphi \wedge (\varphi \mathbf{U}^+ \psi)), \tag{32}$$
$$\models (\varphi \mathbf{W}^+ \psi) \quad \leftrightarrow \quad \overline{\mathbf{X}}(\psi \vee \varphi \wedge (\varphi \mathbf{W}^+ \psi)). \tag{33}$$

Induktioaksiooma:

$$(U,\mathcal{I}) \models (\mathbf{X}(\psi \vee \varphi \wedge \mathcal{X}) \quad \rightarrow \quad (U,\mathcal{I}) \models ((\varphi \mathbf{U}^+ \psi) \rightarrow \chi), \tag{34}$$
$$(U,\mathcal{I}) \models (\chi \rightarrow \overline{\mathbf{X}}(\psi \vee \varphi \wedge \chi)) \quad \rightarrow \quad (U,\mathcal{I}) \models (\chi \rightarrow (\varphi \mathbf{W}^+ \psi)). \tag{35}$$

Positiivinen $\mu\mathbf{TL}$-kaava ilmaisee predikaattimuuntimen suurimman tai pienimmän kiintopisteen. Monotonisille kaavoille kiintopisteet löytyvät aina, epämonotonisille kaavoille niiden olemassaoloa ei voida taata.

Jos malli on *kytketty (connected)*, niin jokainen mallin tila on saavutettavissa nykyisestä tilasta. Toisin sanoen $\forall w, w'(w < w' \vee w = w' \vee w > w')$. Tällöin operaattori $\mathbf{G}^+$ korvaa ensimmäisen kertaluvun universaalikvanttorin s.e. $\mathcal{M} \models \forall t p(t)$, joss $\mathcal{M} \models \mathbf{G}^+ p$. Tällöin:

$$\mathcal{M} \models \nu q \varphi \quad \leftrightarrow \quad \mathcal{M} \models \exists q(q \wedge \mathbf{G}^+(q \rightarrow \varphi)), \tag{36}$$
$$\mathcal{M} \models \mu q \varphi \quad \leftrightarrow \quad \mathcal{M} \models \forall q(\mathbf{G}^+(\varphi \rightarrow q) \rightarrow q). \tag{37}$$

Kytketyille, ja näin ollen myös luonnollisille malleille, $\mu\mathbf{TL}$ on korkeintaan yhtä ilmaisuvoimainen kuin $q\mathbf{TL}$ ja MSOL.

3 ω-automaatit ja ω-kielet

Luonnollisessa mallissa $\mathcal{M} \triangleq (U, \mathcal{I}, w_0)$ tulkintafunktio $\mathcal{I} : \mathcal{P} \to 2^U$ kertoo jokaista propositiota kohden, missä maailman U osajoukossa kyseinen propositio on voimassa. Määritelläään "päinvastaiseen suuntaan toimiva" merkintäfunktio $\mathcal{L} : U \to 2^{\mathcal{P}}$, joka ilmaisee kuhunkin pisteeseen liittyvän merkinnän eli siinä voimassa olevat propositiot. Jos $U = (w_0, w_1, w_2, \ldots)$, niin merkintöjen jonoa $\sigma = (\mathcal{L}(w_0), \mathcal{L}(w_1), \mathcal{L}(w_2), \ldots)$ kutsutaan ω-*sanaksi* aakkostossa $\Sigma \triangleq 2^{\mathcal{P}}$. Ja edelleen, ω-*kieli* on ω-sanojen joukko.

Toisaalta, määritelmän mukaan jokainen LTL kaava kuvaa niiden luonnollisten kehysten $(U, \{\mathcal{I}(R) | R \in \mathcal{R}\})$ joukon, joissa se on aina voimassa alkutilassa (*initially valid*). Näin ollen kaava kuvaa myös ne ω-kielet, joka kustakin kehyksestä on mahdollista generoida.

Kieliä määriteltäessä riittää, että tarkastelemme temporaalilogiikan osalta ainoastaan tulevaisuutta. LTL ja qTL logiikoilla on kyky erotella aikavaiheet (separation property) menneisyys (pure past), nykyhetki (pure present) ja tulevaisuus (pure future), kuten jo aikaisemmin on todettu (lemmat 2.6 ja 3.11). Edelleen, jokaiselle LTL tai qTL logiikan kaavalle löytyy vastaava, ainoastaan tulevaisuuteen viittaava kaava, joka määrittelee täsmälleen saman kielen (lemma 3.12).

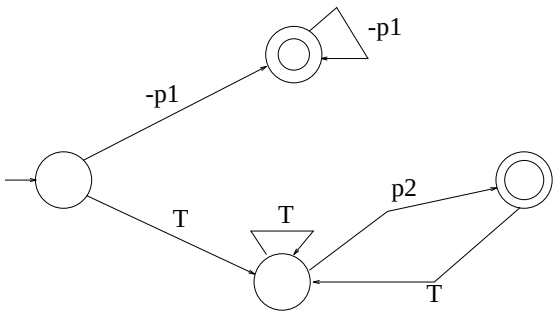
Kieliä voidaan määritellä myös (ω-)säännöllisillä lausekkeilla ja äärellisillä (ω-)automaateilla. Seuraavassa esitämme määritelmän (ω)-säännöllisen lausekkeen kuvaamalle kielelle:

Määritelmä 3.1 *(ω)-säännöllisen lausekkeen kuvaamalle kielelle pätee:*

- *Jokainen aakkoston merkki on ω-säännöllinen ilmaisu.*
- *Jos α ja β ovat ω-säännöllisiä ilmaisuja, niin niitä ovat myös ε (tyhjä kieli), $(\alpha + \beta)$ (yhdiste), $(\alpha; \beta)$ (peräkkäiskompositio) ja α^+ (kielen sanojen äärellinen toisto).*
- *Jos α on ω-säännöllinen ilmaisu, niin sellainen on myös α^ω (kielen sanojen ääretön toisto.)*

Esimerkiksi ω-säännöllinen lauseke $(\neg p1)^\omega + (\top^+; p2)^\omega$ määrittää kaikki ne äärettömät sanat $(\sigma_0, \sigma_1, \sigma_2, \ldots)$, joissa joko $\forall i$ pätee, että $p1 \notin \sigma_i$ tai äärettömän monelle i:lle pätee, että $p2 \in \sigma_i$. Lisäksi lauseke määrittää niiden luonnollisten mallien $(U, \{\mathcal{I}(R) | R \in \mathcal{R}, \{\mathcal{I}(p) | p \in \mathcal{P}\})$ joukon $\mathcal{M}$, joille $\mathcal{M} \models \mathbf{G}^*(\neg p1 \wedge \mathbf{X}\top) \vee \mathbf{G}^*\mathbf{F}^+ p2$. Koska kaavan mukaan kunkin luonnollisen mallin kaikilla pisteillä tulee olla seuraaja, mallien täytyy olla äärettömiä.

ω-*automaatti* määritellään kuten tavallinen epädeterministinen automaatti, laajennettuna erillisellä *toistotilojen (recurring states)* joukolla. Toistotilat sisällyttävät *reiluusehdon* automaattiin.



Kuva 1: Büchi-automaatti

Määritelmä 3.2 *Kun $\Sigma = 2^{\mathcal{P}}$, niin ω-automaatti on monikko $(S, \Delta, S_0, S_{acc}, S_{rec})$, missä*

- *S on tilojen joukko,*
- *$\Delta \subseteq S \times \Sigma \times S$ on siirtymärelaatio*
- *$S_0 \subseteq S$ on alkutilojen joukko*
- *$S_{acc} \subseteq S$ on hyväksyvien tilojen joukko (äärellisille sanoille)*
- *$S_{rec} \subseteq S$ on toistotilojen joukko (äärettömille sanoille).*

Büchi-automaatti on äärellistilainen ω-automaatti, *reilu* siirtymäsysteemi, jossa tilojen joukko S on äärellinen. *LTS (Labelled Transition System)* on siirtymäsysteemi, jossa kaikki tilat ovat toistotiloja ja hyväksyviä tiloja. *Heikosti reilu* siirtymäsysteemi on sellainen ω-automaatti, jossa kaikki tilat ovat toistotiloja ja ainoastaan lopputilat (*terminal states*), joista ei ole siirtymää seuraajatilaan, ovat hyväksyviä tiloja. Yleensä LTS:ien ja heikosti reilujen siirtymäsysteemien yhteydessä ei käytetä hyväksyvien tilojen ja toistotilojen käsitteitä.

Määritelmä 3.3 (ω-automaatin hyväksymisehto) *ω-automaatti hyväksyy epätyhjän sanan $\sigma \triangleq (\sigma_0, \sigma_1, \sigma_2, \ldots)$, jos löytyy jokin funktio ρ, joka liittää jokaiseen muuttujan i ($< |\sigma|$) arvoon jonkin automaatin tilan ($\rho(\sigma_i) \in S$ s.e.*

- *$\rho(0)$ kuuluu alkutilojen joukkoon,*
- *$\forall i : 0 \leq i < n : (\rho(i), \sigma_i, \rho(i+1)) \in \Delta$ ja*
- *$(\rho(n), \sigma_n, s) \in \Delta$, missä s on hyväksymistila ja σ on äärellinen ja*
- *jos sana on ääretön ja $inf(\rho)$ on äärettömän usein ρ:ssa esiintyvien tilojen joukko, niin $inf(\rho) \cap S_{rec} \neq \{\}$ (ainakin yhdessä toistotilassa vieraillaan äärettömän usein).*

Automaatti hyväksyy luonnollisen mallin $\mathcal{M}$, joss se hyväksyy mallin $\mathcal{M}$ generoiman ω-sanan. Siirtymäsysteemin kieli muodostuu niiden polkujen joukosta, jotka saadaan ”aukikerimällä” (*unwinding*) siirtymäsysteemi.

Kuvan 1 Büchi-automaatti määrittelee täsmälleen saman kielen kuin ω-säännöllinen lauseke $(\neg p1)^\omega + (\top^+; p2)^\omega$. ω-säännölliset lausekkeet ja Büchi-automaatit ovat ilmaisuvoimaltaan samanarvoisia.

4 Toisen kertaluvun kielten ilmaisuvoima

Teoreema 2 (Büchi, Wolper, Sistla) *ω -kielten määrittelyssä seuraavilla formalismeilla on sama ilmaisuvoima:*

- μ**TL**
- **qTL**
- **MSOL**
- *Büchi-automaatit*
- *ω-säännölliset lausekkeet.*

Jokaiselle μTL kaavalle voidaan muodostaa vastaava qTL kaava määritelmään perustuen. Lemman 3.2 mukaisesti MSOL ja qTL kielten ilmaisuvoima on sama. Lemman 3.14 mukaan jokaista qTL ja MSOL kaavaa vastaa jokin Büchi-automaatti, joka määrittää samanlaisen mallien joukon, kuin ko. kaavat. Lemman 3.13 sanoo, että ω-säännölliset lausekkeet ja Büchi-automaatit ovat samanarvoisia, ja edelleen lemmassa 3.15 todettiin, että ω-säännölliset lausekkeet voidaan muttaa μTL-kaavoiksi.

Viitteet

[1] Pnueli A. Ben-Ari M., Manna Z. The temporal logic of branching time. *Acta Informatica*, 20:207–226, 1983.

[2] E.M. Clarke and E.A. Emerson. Characterizing Properties of Parallel Programs as Fixpoints. In *7th International Colloqium on Automata, Languages and Programming*, number 85 in Lecture Notes in Computer Science, 1980.

[3] E.M. Clarke and E.A. Emerson. Design and Synthetis of Synchronization Skeletons Using Branching Time Temporal Logics. In *Workshop on Logic on Programs*, number 131 in Lecture Notes in Computer Science. Springer-Verlag, 1981.

[4] Kozen D. Results on the propositional μ-calculus. *Theoretical Computer Science*, 27:333–354, 1983.

[5] Halpern J.Y. Emerson E.A. ”sometimes” and ”not never” revisited: on branching time vs. linear time. *Journal of the ACM*, 33:151–178, 1986.

[6] Parikh R. Kozen D. A decision procedure for the propositional μ-calculus. In *Proceedings of Int. Symp. Logic of Programs*, 1983.

[7] L. Lamport. ”sometimes” is sometimes ”not never”. In *Proceedings of 7th Annual ACM Symposium on Principles of Programming Languages*, pages 174–185. ACM, 1980.

[8] A. Pnueli. The temporal logic of programs. In *Proceedings of 18th Annual IEEE Symposium on Foundations of Computer Science*, pages 46–57, 1977.

[9] Pratt V. A decidable μ-calculus. In *Proceedings of Annual ACM Symposium on Foundations of Computer Science*, 1981.