hyväksymispäivä arvosana

arvostelija

Ajoitetut automaatit

Taneli Rantala

Helsinki 8. lokakuuta 2002

Seminaariesitelmä

HELSINGIN YLIOPISTO
Tietojenkäsittelytieteen laitos

Ajoitetut automaatit

Taneli Rantala

Seminaariesitelmä

Tietojenkäsittelytieteen laitos

Helsingin yliopisto

8. lokakuuta 2002,

Tämä kirjoitus on esitelmä Rinnakkaisjärjestelmien mallinnus ja verifiointi-seminaaria varten. Se käsittelee lyhyesti ajoitettujen automaattien käsitteistöä ja ominaisuuksia.

Aiheluokat(Computing Reviews 1998):

Avainsanat:

Sisältö

1 Johdanto

Tässä esitelmässä käsitellään formalismia äärellistilaisten reaaliaikajärjestelmien mallintamiseen. Erona perinteisempiin formalismeihin jotka jättävät fyysisen ajan mallintamisen kokonaan pois. Formalismin olennaisen osan muodostavat ajoitetut Buchi-automaatit (eng. timed Buchi automata, TBA) ja vastaavat ajoitetut Muller-automaatit (eng. timed Muller automata, TMA). Tämä esitelmä keskittyy kuitenkin ajoitettuihin Buchi-automaatteihin esitellen muutamia niihin liittyviä laskettavuus/laskennallisuustuloksia. Lopuksi esitetään hieman ajoitettuihin automaatteihin liittyvää verifiointia.

2 Ajoitetun automaatin peruskäsitteitä

Tämä kappale esittelee ajoitettujen Buchi-automaattien peruskäsitteistöä ja oletus on että lukijalla on perustiedot Buchi-automaateista.Kappale pohjautuu suurelta osin

Alurinja Dillin artikkeliin [ADi94]

Aika kuvataan tässä esitelmässä nk. "tiheäksi"(eng. dense) eli ajan malliksi valitaan ei-negatiivisten reaalilukujen joukko R_+.

Määritelmä 1 *Merkkijonoon τ (Alur käyttää nimitystä sana, word) liitetään päättymätön aikajono $\tau = \tau_1\tau_2\ldots$ ajan arvoilla $\tau_i \in \mathbb{R}_+$ seuraavasti:*

1. Monotonisuus: τ kasvaa aidosti eli $\tau_i < \tau_{i+1}$ kaikille $i \geq 1$.

2. Eteneminen (eng. progress): Kaikille $t \in \mathbb{R}_+$ on olemassa $i \geq 1$ siten että $\tau_i > t$.

Ajoitettu merkkijono Buchi-automaatin aakkostossa Σ on pari (σ, τ) missä $\sigma = \sigma_1\sigma_2\ldots$ on ääretön merkkijono aakkostossa Σ ja τ on aikajono. Ajoitettu kieli *aakkostossa Σ on kyseisen aakkoston ajoitettujen merkkijonojen joukko.*

Edellä annettu määritelmä ajoitetulle merkkijonolle (σ, τ) voidaan ymmärtää myös syötteenä automaatille jolloin se esittää symbolia σ_i ajanhetkellä τ_i. Jos tällä samalla ajahetkellä σ_i sattuu useampia tapahtumia eli ajanhetkeen liittyy useampi symboli σ_i , $\sigma_{i'}$ niin ajoitetut merkkijonot määritellään hiukan eri tavalla. Tämä tarkoittaa monotonisuusehdon lieventämistä aidosta epäaitoon monotonisuuteen eli kaikilla $i \geq 1$ on $\tau_i \leq \tau_{i+1}$. Esiteltävät tulokset pitävät paikkansa myös tätä määritelmää käytettäessä.

Ajoitetun automaatin siirtymiä muodostettaessa on otettava huomioon syötesymbolin ohella myös aika jolloin symboli luettiin suhteessa aiemmin luettujen symbolien lukuaikoihin. Tätä varten määrittelemme äärellisen joukon *kelloja.* Kello voidaan asettaa/palauttaa nollaksi (eng. reset to zero) samanaikaisesti minkä tahansa siirtymän kanssa. Jokaiseen siirtymään määrittelemme *kelloehdon* (eng. clock constraint), joka määrä että siirtymä voidaan tehdä mikäli kellot, joita ehto koskee täyttävät ehdon.

Alur ja Dill huomauttavat että automaatin kellot ovat luonteeltaan "fiktiivisiä"eli vastaavuutta esimerkiksi hajautetun järjestelmän paikallisiin kelloihin ei ole.

Formaalimpi määritelmä kelloehdoille voidaan ilmaista seuraavasti:

Määritelmä 2 *Kellojen (tai kellomuuttujien) joukkoon X liittyy joukko kelloehtoja $\Phi(X)$, jossa kaikille $\delta \in \Phi(X)$ on määritelty seuraavaan tapaan induktiivisesti:*

$\delta := x \leq c \mid c \leq x \mid \neg\delta \mid \delta_1 \wedge \delta_2$

missä $x \in X$ *ja* $c \in \mathbb{Q}_+$.

Edellä annettuun määrittelyyn oltaisiin voitu lisätä myös esimerkiksi kelloarvojen yhteenlasku, mutta myöhemmin nähdään että tämä johtasi ratkeamattomuuteen.

Kellotulkinta (eng. clock interpratation) ν on kuvaus kellojen joukolta X reaalilukujen joukolle $\mathbb{R}$. Sanomme, että kellotulkinta X:lle täyttää kelloehdon δ joss δ evaluoituu todeksi käyttäen ν :n antamia arvoja. Olkoon $Y \subseteq X$ ja $t \in \mathbb{R}$, tällöin merkintä $[Y \mapsto t]\nu$ tarkoittaa kellotulkintaa X:lle mikä asettaa t:n jokaiselle Y:n kellolle ja on muilta osin sama kuin ν muuten.

Nyt voimme määritellä ajoitetun Buchi-automaatin seuraavasti:

Määritelmä 3 *Ajoitettu Buchi automaatti (lyhenne TBA) A on kuusikko* $\langle \Sigma, S, S_0, C, E, F \rangle$, *missä*

- Σ *on äärellinen aakkosto*
- S *on äärellinen tilojen joukko*
- S_0 *on alkutilojen joukko*
- C *on äärellinen joukko kelloja*
- $E \subseteq S \times S \times \Sigma \times 2^C \times \Phi(C)$ *on siirtymien joukko.*

Kaari (eng. edge)$\langle s, s', a, \lambda, \delta \rangle$ *on siirtymä tilasta s tilaan s' symbolilla a, Joukko* $\lambda \subseteq C$ *tarkoittaa kelloja jotka asetetaan nollaan.* δ *on C:hen liittyvä kelloehto siten kuin edellä määrittelimme.* $F \subseteq S$ *on hyväksyvien tilojen joukko*

Määritelläksemme ajot yhdistämme aiemmin mainitut ajoitetut merkkijonot (σ, τ) ajoitettuun automaattiin seuraavasti:

Määritelmä 4 *Ajo r, merkitään* $(\bar{\sigma}, \bar{\tau})$, *ajoitetussa automaatissa ajoitetun merkkijonon mukaisesti on muotoa:*

$r : \langle s_0, \nu_0 \rangle \rightarrow^{\sigma_1,\tau_1} \langle s_1, \nu_1 \rangle \rightarrow^{\sigma_2,\tau_2} \langle s_2, \nu_2 \rangle \rightarrow^{\sigma_3,\tau_3} \ldots$

missä $s_i \in Sja\nu_i$ *kuten edellä, kaikille* $i \geq 0$ *täyttävät seuraavat ehdot:*

Aloitus:$s_0 \in S_0$ *ja* $\nu_0(x) = 0$ *kaikille* $x \in C$

"Konsekutiivisuus"(eng. consecution, seuraavuus, johdonmukaisuus) : kaikille $i \geq 1$*, on oleamassa kaari joukossa E muotoa* $\langle s_{i-1}, s_i, \sigma_i, \lambda_i, \delta_i \rangle$ *siten että* $(\nu_{i-1} + \tau_i + \tau_{i-1})$ *täyttää kelloehdon* δ_i *ja* ν_i *on yhtä kuin* $[\lambda_i \mapsto 0](\nu_{i-1} + \tau_i - \tau_{i-1})$.

Joukko inf(r) koostuu niistä tiloista $s \in S$ *joilla* $s = s_i$ *äärettömän monella* $i \geq 0$ *eli ne S:n tilat jotka esiintyvät ajossa äärettömän monta kertaa .*

Ajoitettuun merkkijonoon (σ, τ) littyvää ajoa r kutsutaan *hyväksyttäväksi* ajoksi mikäli $inf(r) \cap F \neq \varnothing$. Ajoitetun automaatin A hyväksymää kieltä eli niiden ajoitettujen merkkijonojen joukkoa, jotka A merkitään seuraavaasti: $L(A)$=\{ (σ, τ) | $\mathcal{A}$:lla on hyvaksyva ajo liittyen merkkijonoon (σ, τ)\}.Kieliä, joilla on hyväksyvä Buchi-automaatti kutsutaan säännöllisiksi, joten kutsumme kieliä, jotka ajoitettu Buchi-automaatti hyväksyy vastaavasti *ajoitetuiksi säännöllisiksi kieliksi* (eng. timed regular languages).

3 Ajoitettujen kielten ja automaattien ominaisuuksia

Tässä luvussa esitellään muutamia ajoitettujen automaattien/kielten perusominaisuuksia liittyen esimerkiksi kielten tyhjyystarkistuksiin ja kielillä suoritettaviin joukkoopillisiin operaatioihin.

Lause 5 *Ajoitettujen säännöllisten kielten joukko on suljettu (äärellisen) yhdisteen sekä leikkauksen suhteen.*

Todistus. Käsitellään n:n kokoista joukkoa ajoitettuja automaatteja: $A_i = (\Sigma, S_i, S_{i_0}, C_i, E_i, F_i)$, $i = 1, 2, \ldots, n$*. Olennaista tietoa ei menetetä jos oletetaan kellojoukkojen* C_i *olevan erillisiä. Yhdisteen tapaus on helppo:laaditaan erillinen yhdiste (eli ei redundantteja* *tiloja/siirtymiä/ ...) kaikista automaateista. Leikkaus voidaan toteuttaa muuntamalla normaalien Buchi-tulokonstruktiota. Kellojoukko tuloautomaatille on* $\cup_i C_i$. *Tuloautomaatin tilat ovat muotoa* $\langle s_1, \ldots, s_n, k\rangle$, *missä jokainen* $s_i \in S_i$ *ja* $1 \leq k \leq n$. *Monikon i:nnes komponentti pitää yllä tietoa automaatin* A_i *tilasta ja viimeinen komponentti k toimii syklisenä laskurina yksittäisten yksittäisten automaattien hyväksymistilojen suhteen. Laskuri alustetaan arvoon 1 ja sitä lisätään arvosta k arvoon (k+1) (modulo n) joss automaatin* A_k *nykyinen tila on hyväksymistila. Lisähuomautuksena mainittakoon että arvoksi n mod n valitaan n. Tuloautomaatin A alkutilat ovat muotoa* $\langle s_1, \ldots,_n, 1\rangle$ *missä jokainen* s_i *on automaatin* A_i *alkutila. Tuloautomaatin siirtymät määritellään ottamalla mukaan automaattien ne siirtymät, jotka tapahtuvat samalla merkillä. Siirtymä tilasta* $\langle s_1, \ldots, s_n, k\rangle$ *merkillä a tehdään tilaan* $\langle s'_1, \ldots, s'_n, j\rangle$ *missä j=(k+1) mod n mikäli* $s_k \in F_k$ *muutoin j=k. Nollaan asetettavat tällä siirtymällä yhdisteenä* $\cup_i \lambda_i$ *kelloehtojen ollessa muotoa* $\wedge_i \delta_i$. *Laskurin saa kaikki arvonsa väliltä* $1 \ldots n$ *äärettömän usein mikäli kaikkien automaattien hyväksymisehdot voidaan täyttää. Edelleen määrittelemme tuloautomaatin hyväksymistilojen joukoksi* $\langle s_1, \ldots, s_n, n\rangle$ *missä* $s_n \in F_n$ $\Box$

3.1 Tyhjyystarkistus

Tässä osassa kehitellään keinoa ajoitetun automaatin tyhjyystarkastukselle. Osoitamme että tavallisen Buchi-automaatin hyväksymä kieli on "konsistentti"verrattuna vastaavaan ajoitetun Buchi-automaatin hyväksymään ajoitettuun kieleen.

Ajoitetun automaatin määritelmässämme sallimme kelloehtoihin vertailut rationaalilukujen kanssa. Kuitenkin tyhjyystarkastusta varten riittää tarkastella automaattia, jonka kelloehdoissa käsitellään vain kokonaislukuja. Olkoot τ aikajono,$t \in \mathbb{Q}$ ja $t \cdot \tau = t\tau_1, t\tau_2, \ldots$.

Lemma 6 *Olkoon A ajoitettu automaatti,* (σ, τ) *ajoitettu merkkijono ja* $t \in \mathbb{Q}$. *Tällöin* $(\bar{s}, \bar{\nu})$ *on merkkijonon* (σ, τ) *mukainen automaatin A :n ajo joss* $(\bar{s}, t \cdot \bar{\nu})$ *on merkkijonon* $(\sigma, t \cdot \tau)$ *mukainen* A_t*:n ajo.* A_t *on ajoitettu automaatti, joka on saatu*

A:sta korvaamalla kelloehdoissa esiintyvät vakiot d uudella vakiolla $t \cdot d$

Todistus.Sivuutetaan$\square$

Lemmassa on siis oikeastaan kyse vain "lavennuksesta", sillä t voidaan valita kaikissa kelloehdoissa esiintyvien kaikkien rationaaliluku-vakioiden nimittäjien pienimmäksi monikerraksi. Voidaan osoittaa että $L(A)$ on tyhjä joss $L(A_t)$ on tyhjä, joten tarkastellaksemme A:n tyhjyyttä riittää rajoittua A_t:n.

Koska ajoitetun automaattin tuleva toiminta määräytyvät paitsi nykyisin tilan niin myös automaatin kellojen perusteella, on hyödyllistä määritellä automaatille A*laajennettu tila* (eng. extended state): $\langle s, \nu \rangle$ missä $s \in S$ ja ν on automaatin kellotulkinta.

Koska laajennettujen tilojen lukumäärä on ääretön (jopa ylinumeroituva, sillä ν oli kuvaus reaaliluvuille), ei voida rakentaa automaattia , jonka tilat koostuisivat A:n laajennetuista tiloista. Mutta jos kahdella laajennetulla tilalla on (a)samat A:n tilat (b) kellojen arvojen kokonaislukuosat ja (c) kellojen arvojen jäänösosat yhteisesti sovitussa järjestyksessä, niin kahta ajoa, jotka alkavat samasta A:n tilasta voidaan pitää "tarpeeksi samanlaisina". Kokonaisosien tarkastelua tarvitaan kelloehtojen täyttymisen tarkistukseen ja jäännösosien tarvitaan päätökseen mikä kello muuttaa kokonaislukosaansa ensin. Esimerkiksi jos kaksi kelloa x ja y ovat välillä [0,1] lajennetussa tilassa, niin kelloehdon (x=1) määrittelemän siirtymää voi seurata siirtymä ehdolla (y=1), riippuen ehdon (x<y) täyttymisestä.

Myös kelloarvojen kokonaislukuosat voivat olla mielivaltaisen pitkiä, mutta mikäli kelloa ei ikinä verrata c:tä suuremman vakion kanssa, niin kellon arvolla, sen ylittäessä c:n, ei ole merkitystä polkua valittaessa. Otamme käyttöön seuraavat merkinnät: Kun $t \in \mathbb{R}_+$, niin fract(t) on t:n jäännösosa ja $\lfloor t \rfloor$ on t:n kokonaisosa eli $t = \lfloor t \rfloor + fract(t)$.

Määritelmä 7 *Olkoon* $A = \langle \Sigma, S, S_0, C, E, F \rangle$ *ajoitettu automaatti. Jokaisella* $x \in C$*, olkoon* c_x *suurin kokonaisluku c missä* $(x \leq c)$ *tai* $(c \leq x)$ *alikaava jollekin E:n olevalle kelloehdolle(*c_x *on siis kaikissa E:n kelloehdoissa esiintyvien vakioiden maksimi tai supremum). Ekvivalenssirelaatio* $\sim$ *on määritelty kellotulkintojen joukolle C seuraavasti:*

$\nu \sim \nu'$ joss

1. Kaikille $x \in C$, joko $\lfloor \nu(x) \rfloor = \lfloor \nu'(x) \rfloor$ tai $\lfloor \nu(x) \rfloor > c_x \wedge \lfloor \nu'(x) \rfloor > c_x$

2. Kaikille $x, y \in C$ joilla on $\nu(x) \leq c_x$ ja $\nu(y) \leq c_x$ on seuraavasti: $fract(\nu(x)) \leq fract(\nu(y))$ joss $fract(\nu'(x)) \leq fract(\nu'(y))$.

3. Kaikille $x \in C$ joilla $\nu(x) \leq c_x$ on $fract(\nu(x)) = 0$ joss $fract(\nu'(x)) = 0$.

Kelloalue automaatille A on nyt kelloehtojen ekvivalenssiluokka relaatiolla $\sim$.

Käytämme merkintää $[\nu]$ kuvaamaan kelloaluetta johon ν kuuluu. Esimerkkinä kellotulkinta ν, joka on kelloille x ja y $\nu(x)$= 0.3 ja $\nu(y)$= 0.7. Jokainen ekvivalenssiluokkaan $[\nu]$ kuuluva kellotulkinta täyttää ehdon (0<x<y<1) ja merkitsemmekin aluetta nyt [0 < x < y< 1].

Jokainen kelloalue voidaan ilmaista seuraavasti:

1) Jokaiselle kellolle x, yksi kelloehto joukosta

$\{x = c | c = 0, 1, \ldots, c_x\} \cup \{c - 1 < x < c | c = 1, \ldots, c\_x\} \cup \{x > c_x\}$

2) Jokaiselle kelloparille x ja y joilla c-1<x<c ja d-1<y<d jotka ovat kaavoissa muotoa 1) joillekin c ja d on joko fract(x) on pienempi, yhtä suuri tai suurempi kuin fract(y).

Laskemalla yhtälöiden kombinaatioiden lukumäärä saadaan yläraja kelloalueiden lukumäärälle, joka on $|C|! \cdot 2^{|C|} \cdot \Pi_x(2c_x + 2)$.

Ajoitetun automaatin A tyhjyystarkistuksessa täytyy ensiksi laatia automaatti, jonka polut "imitoivat"A:n ajoja. Tätä automaattia kutsutaan *alueautomaatiksi* (eng. region automaton) merkitään R(A). Alueautomaatin tila koostuu A:n tilasta ja kellojen senhetkisten tilojen ekvivalenssiluokasta, ollen siis muotoa $\langle s, \alpha \rangle$ missä $s \in S$ ja α on kelloalue. Tulkinta on että A:n laajennettua tilaa $\langle s, \nu \rangle$ vastaa R(A):n tila $\langle s, [\nu] \rangle$. Siirtymä R(A):ssa määritellään seuraavasti: R(A):ssa on siirtymä tilasta $\langle s, \alpha \rangle$ tilaan $\langle s', \alpha' \rangle$ merkillä a joss A:ssa on siirtymä tilasta $\langle s, \nu \rangle$ tilaan $\langle s', \nu' \rangle$ merkillä a, kun $\nu \in \alpha$ ja $\nu' \in \alpha'$. Siirtymän määrittelyssä voidaan käyttää myös *aikaseuraaja*-relaatiota (eng. time-successor) kelloalueiden joukkoon. Kelloalueen aikaseuraajat ovat kaikki ne kelloalueet jotka $\nu \in \alpha$ saavuttaa ajan kuluessa eli kaikki ne $\alpha^{'}$, joille $\nu + t \in \alpha^{'}$ jollain $t \in \mathbb{R}_{+}$.

Kelloalueen aikaseuraajat voidaan nyt konstruoida seuraavasti:

Olkoon α kelloalue joka täyttää ehdon $x > c_x$ kaikille kelloille x. Ainoa seuraaja α:lle on α itse.

Olkoon joukko $C_0 \neq \emptyset$ niiden kellojen x joukko, joille α täyttää ehdon (x=c) jollekin c_x. Tällöin ajan kuluessa C_0:n kellojen jäännösosat tulevat nollasta eroaviksi ja kelloalue vaihtuu. Kelloalueen α aikaseuraajat ovat samat kuin kelloalue β:n aikaseuraajat, jotka määritellään seuraavasti:

1)Olkoon x_0, jos α täyttää ehdon $(x = c_x)$ niin β täyttää ehdon $(x > c_x)$. Muutoin jos α täyttää ehdon x=c niin β täyttää ehdon $(c < x < c + 1)$. Mikäli $x \notin C_0$ niin ehdot β:ssa ovat samat kuin α:ssa.

2)Kelloille x ja y, joille on $x < c_x$ ja $y < c_y$ on tosi α:ssa, on jäännösosien järjestysrelaatio β:ssa sama kuin α:ssa.

Jos kumpaakaan edellä mainituista tapauksista ei voida käyttää, niin olkoon C_0 niiden kellojen x joukko joille α ei täytä ehtoa $x > c_x$ ja joilla on maksimaaliset jäännösosat. Toisin sanoen kaikille kelloille y joille α ei täytä ehtoa $(y > c_y)$, $fract(y) \leq fract(x)$ on ehto α:ssa. Nyt ajan kuluessa kellot C_0:ssa saavat kokonaislukuarvoja.Olkoon β seuraavasti määritelty kelloalue:

1)Olkoon x_0, jos α täyttää ehdon (c-1<x<c) niin β täyttää ehdon (x=c). Jos $x \notin C_0$, niin ehdot β:ssa ovat samat kuin α:ssa. 2)Olkoot kellot x ja y siten että (c-1<x<c) ja (d-1<y<d) kuten edellisessä kohdassa, niin jäännösosien järjestysrelaatio on β:ssa sama kuin α:ssa. Kelloalueen α aikaseuraajia ovat α itse, β ja kaikki β:n aikaseuraajat.

Voimme nyt laatia formaalin määritelmän alueautomaatille.

Määritelmä 8 *Ajoitetulle automaatille* $A = \langle \Sigma, S, S_0, C, E, F \rangle$ *vastaava alueautomaatti* $R(A)$ *aakkostossa* Σ *on seuraava:*

R(A):n tilat ovat muotoa $\langle s, \alpha \rangle$*, missä* $s \in S$ *ja* α *on kelloalue*

Alkutilat ovat muotoa $\langle s, [\nu_0]\rangle$ *missä* $s_0 \in S_0$ *ja* $\nu_0(x) = 0$ *kaikille* x

R(A):ssa on siirtymä $\langle\langle s, \alpha\rangle, \langle s', \alpha'\rangle, a\rangle$ *joss on siirtymä* $\langle s, s', a, \lambda, \delta\rangle$ *ja alue* α'' *siten että 1)* α'' *on* α*:n aikaseuraaja, 2)*α'' *täyttää ehdot* δ *ja 3)* $\alpha' = [\lambda \mapsto 0]\alpha''$

Alur ja Dill ovat laskeneet alueautomaatin tilojen määrän kertaluokaksi $O(|S| \cdot 2^{|\lambda(\mathbb{A}|})$ ja siirtymien kertaluokaksi $O(|E| \cdot 2^{|\delta(\mathbb{A})|})$. Automaatti voidaan laskea siis ajassa $O[(|S| + |E|) \cdot 2^{|\delta(\mathbb{A})|}]$, sillä aikaseuraajien laskeminen voidaan suorittaa lineaarisessa ajassa suhteessa kelloalueen esityksen pituuteen (mikäli käytetään binäärikoodausta). [ADi94]

Seuraavaksi määrittelemme vastavuudet A:n ja R(A):n ajojen välille.

Määritelmä 9 *Olkoon* r=$(\bar{s}, \bar{\nu})$ *A:n ajo kuten aiemmin määriteltiin. Tällöin sen projektio* $[r] = (\bar{s}, [\bar{\nu}])$ *on jono*

$[r] : \langle s_0, [\nu_0]\rangle \rightarrow^{\sigma_1} \langle s_1, [\nu_1]\rangle \rightarrow^{\sigma_2} \langle s_2, [\nu_2]\rangle \rightarrow^{\sigma_3} \ldots$

Nyt [r] on automaatin R(A) ajo merkkijonolla σ. Koska aika etenee rajatta ajossa r, jokainen kello x joko asetetaan nollaan äärettömän usein tai jostain ajanhetkestä kasvaa rajatta. Joten kaikilla x on äärettömän monella $i \geq 0$ $[\nu_i]$ täyttää ehdon $[(x = 0) \vee (x > c_x)]$. Tämän pohjalta voidaan laatia seuraava määritelmä:

Määritelmä 10 *Muotoa*

$r : \langle s_0, \alpha_0\rangle \rightarrow^{\sigma_1} \langle s_1, \alpha_1\rangle \rightarrow^{\sigma_2} \langle s_2, \alpha_2\rangle \rightarrow^{\sigma_3} \ldots$

oleva R(A):n ajo $r = (\bar{s}, \bar{\alpha})$ *on* etenevä *(eng. progressive) joss jokaiselle kellolle* x*, on äärettömän monta* $i \geq 0$ *siten että* α_i *täyttää ehdon* $[(x = 0) \vee (x > c_x)]$

Lemma 11 *Jos* r *on R(A):n etenevä ajo merkkijonolla* σ *niin on olemassa aikajono* τ *ja A:n ajo* r' *merkkijonolla* (σ, τ) *siten että* $r = [r']$.
Todistus. Sivuutetaan (katso esim.[ADi94])□

Lemman mukaan R(A):n etenevät ajot vastaavat siis A:n projektioajoja.

Tarkastelaksemme ajoitetun Buchi-automaatin tyhjyyden tarkistuksen kertaluokkaa, tarvitsemme muutamia apukäsitteitä ja tuloksia.

Olkoon L ajoitettu kieli. Tällöin *Untime*(L) on ω-kieli koostuen merkkijonoista $\sigma \in \Sigma^\omega$ siten että $(\sigma, \tau) \in$ L jollakin aikajonolla τ.

Lause 12 *Olkoon* $A = \langle \Sigma, S, S_0, C, E, F \rangle$ *ajoitettu Buchi-automaatti. Tällöin löytyy Buchi-automaatti, joka hyväksyy aakkoston* Σ *kielen* Untime*[L(A)].*

Todistus. Olkoon A' A:sta muodostettu alueautomaatti. Alueautomaatin määritelmästämme seuraa että mikäli r on A:n hyväksyvä ajo merkkijonolla (σ, τ)*, on [r] etenevä ja hyväksyvä ajo A':ssa merkkijonolla* σ*. Käänteinen seuraa edellisestä lemmasta. Jos [r'] on hyväksyvä ajo A':ssa on r' hyväksyvä ajo A:ssa. Edelleen seuraa, että* $\sigma \in$*Untime[L(A)] joss A':lla on etenevä ja hyväksyvä ajo merkkijonolla* σ*. Voidaan laatia myös kolmas automaatti A" siten että A':lla on etenevä ja hyväksyvä ajo merkkijonolla* σ *joss A" on hyväksyvä ajo merkkijonolla* σ*. A" on etsitty automaatti: L(A")* = Untime*[L(A)].*$\square$

Lause 13 *Ajoitetun* $B\ddot{u}chi - automaatin A = \langle \Sigma, S, S_0, C, E, F \rangle$ *kielen L(A) tyhjyys voidaan tarkistaa ajassa* $O[(|S| + |E|) \cdot 2^{|\lambda(\mathbb{A})|}]$.

Todistus. Olkoon A' samalainen automaatti kuin edellisen lauseen todistuksessa. Aiemmin mainittiin A':n tilojen määrän olevan $O(|S| \cdot 2^{|\delta(\mathbb{A}|})$ *ja siirtymien määrän* $O(|E| \cdot 2^{|\delta(\mathbb{A})|})$*. Kieli L(A) on epätyhjä joss A':ssa on sykli C siten että C on saavutettavissa jostakin A':n alkutilasta ja C sisältää ainakin yhden tilan joukosta F' ja ainakin yhden jokaisesta joukosta* F_x*.* F_x *määritellään seuraavasti: olkoon x ja* $F_x = \{\langle s, \alpha \rangle | \alpha \models [(x = 0) \vee (x > c_x)]\}$*. Tarkistus voidaan tehdä lineaarisessa ajassa A':n kokoon nähden* $\square$

Lause 14 *Annetun ajoitetun automaatin A tyhjyystarkastuksen ongelma on PSPACE-täydellinen.*

Todistus.[Kuuluminen PSPACE:een] Vaikka alueautomaatin tilojen määrä on eksponentiaalinen verrattuna kellojen määrään, voidaan silti laatia epädeterministinen tarkistus alueautomaatille "arvaamalla"haluttu polku polynomisella tilankäytöllä. Yksi-

tyiskohdat sivuutetaan. [PSPACE-kovuus]Tyhjyystarkastusongelma palautetaan ongelmaan lineaarisen rajoitetun automaatin pysähtymisestä tietyllä syötteellä, minkä tiedetään olevan PSPACE-täydellinen. Yksityiskohdat sivuutetaan(katso esim [ADi94]).□

3.2 Ratkeamattomat ongelmat

Tässä osassa esittelemme muutamia ajoitettuihin kieliin liittyviä ratkeamattomuustuloksia.Sitä varten tarvitsemme kuitenkin käsitteistöä. Π_1^1 -ongelmien luokka koostuu "hyvin ratkeamattomista ongelmista, joidenkin ollessa epäaritmeettisia joukkoja" [ADi94]

Epädeterministinen 2-laskurinen Turingin kone M koostuu kahdesta laskurista C ja D sekä n:n pituisesta käskyjonosta. M:n tila (Alur käyttää termiä konfiguraatio, eng. configuration)koostuu kolmikosta $\langle i, c, d\rangle$, missä i on "käskylaskuri" ja c sekä d edellä mainitut kaksi laskuria. M etenee epädeterministisesti jompaan kumpaan kahden laskurin osoittamasta paikasta. M:n laskenta on päättymätön jono tiloja, alkaen alkutilasta $\langle 1, 0, 0\rangle$. Laskenta on *toistuva* (eng. recurring) mikäli äärettömän monessa käydyssä tilassa i=1.

Lause 15 *Aakkostolla Σ annetun ajoitetun automaatin ongelma siitä hyväksyykö se kaikki merkkijonot on Π_1^1-kova.*
Todistus.Palautamme ongelman M:n toistuvien laskentojen olemassaolosta tähän ongelmaan. Yksityiskohdat sivuutetaan (kts. esim [ADi94])

Tämän lauseen avulla samme seuraavanlaisen tuloksen.

Korollaari 16 *Olkoon A_1 ja A_2 kaksi ajoitettua automaattia aakkostolla Σ. Ominaisuuden $L(A_1) \subseteq L(A_2)$ tarkistaminen kuuluu luokkaan Π_1^1*
Todistus Palautamme ajoitetun automaatin A:n universaalisuusongelman (aakkostolla Σ) tähän ongelmaan. Olkoon A_{univ} automaatti, joka hyväksyy jokaisen Σ:n ajoitetun merkkijonon. Automaatti A on universaali joss $L(A_{univ}) \subseteq L(A)$.□

Määritelmä 17 *Olkoot* A_1 *ja* A_2 *kaksi ajoitettua automaattia aakkostolla* Σ. $A_1 \sim_1 A_2$ *joss* $L(A_1) = L(A_2)$. $A_1 \sim_2 A_2$ *joss kaikille ajoitetuille automaateille* A *aakkostolla* Σ. $L(A_1) \cap L(A)$ *on tyhjä täsmälleen silloin kun* $L(A_2) \cap L(A)$.

Lause 18 *Kahdelle ajoitetulle automaatille* A_1 *ja* A_2 *aakkostolla* Σ*,*

1. Kysymyksen $A_1 \sim_1 A_2$ *ratkaisu on* Π_1^1*-kova*

2. Kysymyksen $A_1 \sim_2 A_2$ *ratkaisu on co-RE-täydellinen*

Todistus.Sivuutetaan.$\square$

Aiemmin totesimme, että ajoitettujen säännöllisten kielten luokka on suljettu yhdisteen ja leikkauksen suhteen. Vastaava ei kuitenkaan päde komplementoinnille:

Korollaari 19 *Ajoitettujen kielten luokka ei ole suljettu komplementoinnin suhteen.* *Todistus. Olkoot* A_1 *ja* A_2 *ajoitettuja automaatteja aakkostolla* Σ. $L(A_1) \subseteq L(A_2)$ *joss* $L(A_1)$*:n ja* $L(A_2)$*:n komplementin leikkaus on tyhjä. Oletetaan nyt että ajoitetut Buchi-automaatit ovat suljettuja komplementin suhteen. Edelleen* $L(A_1) \not\subseteq L(A_2)$ *joss on olemassa ajoitettu automaatti siten että* $L(A_1) \cap L(A)$ *on epätyhjä , mutta* $L(A_2)(A)$ *on tyhjä. Eli* $L(A_1) \not\subseteq L(A_2)$ *joss* A_1 *ja* A_2 *eivät ole relaatiossa* $\sim_2$*. Edellisestä lauseesta seuraa nyt, ettäsisältymisongelman komplementti on rekursiivisesti lueteltava. Tämä on ristiristiriidassa sisältymisongelman* Π_1^1*-kovuuden kanssa.*$\square$

Aiemmin määrittelimme kelloehdot siten, että sallimme vakiovertailujen lisäksi Boolen operatiot (konjunktio,disjunktio, komplementti). Jos lisäämme yhteenlaskuoperaatiot kellojen välille tyyliin: $(x + y \geq x' + y')$ missä x, y, x', y' ovat kaikki kelloja, lisäämme formalismin ilmaisuvoimaa: automaatissa voidaan nyt esimerkiksi vertailla viipeitä. Ongelmana on kuitenkin tyhjyystarkastuksen muodostuminen Π_1^1-kovaksi. Todistus tälle saadaan käyttämällä aiemmin käsiteltyä kaksilaskurista epädeterminististä Turingin konetta.

4 Ajoitettujen automaattien verifionti

Tässä osassa käsitellään kuinka ajoitettuja automaatteja voidaan käyttää todistamaan äärellistilaisia reaaliaikajärjestelmiä oikeiksi.

Jälkisemantiikassa (eng. trace semantics) liitämme jokaiseen prosessiin joukon havaittuja tapahtumia ja mallinnamme prosessia sen kaikkien *jälkien* joukolla. Jälki on lineaarinen tapahtumajono, jossa tapahtumia voidaan pitää välittömästi tapahtuvina. Mallissame jälki on jono tapahtumajoukko. Jos siis kaksi tapahtumaa a ja b tapahtuvat samanaikaisesti, niin jäljessä on merkintä a,b. Rajoitumme tässä ainoastaan äärettömien jonojen tarkasteluun. Muodollisemmin ilmaistuna käytämme seuraavaa määritelmää: Olkoon A tapahtumajoukko tällöin jälki $\sigma = \sigma_1\sigma 2 \ldots$ on ääretön jono $.P^+(A)$:ssa, joka on kaikkien A:n epätyhjien osajoukkojen joukko. *Ajaton prosessi* on pari (A,X) koostuen tapahtumien joukosta A ja mahdollisesta jälkien joukosta X.

Prosesseille voidaan rinnakkaiskompositio-operaatio, joka voidaan määritellä projektion avulla. σ:n projektio joukolle B muodostetaan ottamalla leikkaus kunkin σ:n tapahtumajoukon ja B:n kanssa ja poistamalla kaikki tyhjät joukot jonosta. Projektiolle käytetään merkintää $\sigma\lceil B$. Prosessien joukon $P_i = \{(A_i, X_i)| \wedge_i \sigma\lceil A_{ii}\}$ rinnakkaiskompositio on prosessi $|_i P_i$, jonka tilajoukko on $\cup_i A_i$ ja jälkijoukkona $\{\sigma \in P_+(\cup_i A_i)^\omega| \wedge_i \sigma\lfloor A_i \in X_i\}$Eli σ on $|_i P_i$:n jälki joss $\sigma\lceil A_i$ on P_i:n jälki jokaisella $i = 1, \ldots, n$.

Verifiointikysymys voidaan nyt esittää sisältymisongelmana. Sekä toteutus että spesifikaatio annetaan ajattomina prosesseina, olkoon (A, X_I) implmentaatio ja (A, X_S) spesifikaatio, implementaatio on *oikea* suhteessa spesifikaatioon joss $X_I \subseteq X_S$.

Seuraavaksi meidän on liitettävä prosessimalliimme aika. Ajan arvoiksi valitsemme reaaliluvut kuten aiemmin. Ajoitettu jälki tapahtumajoukolla A on pari (σ, τ) missä σ on jälki ja τ on aikajono kuten aiemmin. Ajoitetussa jäljessä siis τ_i ilmaisee ajan jolloin σ_i tapahtui. Edelleen määrittelemme *ajoitetun prosessin* (eng. timed process) (A,L) missä A on äärellinen tapahtumajoukko ja L on ajoitettujen jälkien joukko A:lla.

Operaatiot ajoitetuille prosesseille määritellään tavalliseen tapaan. Rinnakkaiskompositiossa täytyy muista että kaikkien prosessien yhteisten tapahtumien aikojen täytyy olla samat.

Lause 20 *Olkoot $P_i = (A_i, L(\mathcal{A}_i))$, $i = 1, \ldots, n$ ajoitettuja säännöllisiä prosesseja (Ajoitettu prosessi on säännöllinen joss prosessin jäljet voidaan tunnistaa ajoitetulla Buchi-automaatilla),$\mathcal{A}_i$:t niitä mallintavat ajoitetut automaatit ja $\mathcal{A}_s$ spesifikaation ajoitettu automaatti. Tällöin sisältymis-ongelma $[||_i P_i] \subseteq L(\mathcal{A}_s)$ kuuluu luokkaan PSPACE.*

Todistus. Laaditaan toteutusautomaattien ja spesifikaatio-automaatin tuloautomaatti, josta laaditaan alueautomaatti, jonka tilankulutus on polynomiaalista verrattuna syöteautomaatteihin. Yksityiskohdat sivuutetaan. $\Box$

5 Muita formalismeja

Muita formalismeja reaaliaikajärjestelmien mallintamiseen ja verifiointiin ovat esimerkikisi MITL (Metric Interval Temporal Logic)[AFH96], joka on "reaaliaikasovellus" Pnuelin esittämästä lineaarisen ajan temporaaalilogiikasta (LTL)[Pnu77] . Toisenlaista paradigmaa noudattavat esimerkiksi probabilistiset mallit: niissä halutaan saadun ajoitetun automaatin todennäköisyydeksi hyväksyä jokin tietty merkkijono (jokin ei-toivottu ominaisuus) nolla[ACD91].

Lähteet

ACD91 Alur R. , Courcoubetis C.,Dill D.L. *Model checking for probabilistic real-time systems.* Automata, Languages and Programming: Proceedings of th 18th ICALP, LNCS 510,pages 115-136. Springer-Verlag

ADi94 Alur R., Dill D.L. *A theory of timed automata* Theoretical Computer Science 126:183-235. 1994

AFH96 Alur R., Feder T., Henzinger T.A. *The benefits of relaxing punctuality* Journal of the ACM 43(1):116-146,1996

Pnu77 Pnueli A. *The temporal logic of programs* Proc. of tthe 18th IEEE Symposium on Foundations of Computer Science sivut 46-77,1977