Tampereen yliopisto

Antti Simola

SYMBOLISET ÄÄRELLISET AUTOMAATIT JA BRZOZOWSKIN LAUSE

Informaatioteknologian ja viestinnän tiedekunta
Pro gradu -tutkielma
Matematiikka
Joulukuu 2024

TIIVISTELMÄ

Antti Simola: Symboliset äärelliset automaatit ja Brzozowskin lause
Pro gradu -tutkielma
Tampereen yliopisto
Matematiikan ja tilastotieteen tutkinto-ohjelma
Joulukuu 2024

Tässä tutkielmassa todistetaan Brzozowskin lause ja yleistetty Brzozowskin lause symbolisille äärellisille automaateille.

Luvussa 2 käydään läpi Boolen algebran perusteita, kuten Boolen renkaan ja Boolen algebran määritelmät. Esitellään Boolen algebran tärkeimmät identiteettilait ja todistetaan ne. Lisäksi havaitaan, että joukon A Boolen rengas on tulkittavissa joukon A Boolen algebraksi. Lopuksi esitellään ja todistetaan Stonen esityslause, joka on yksi Boolen algebran merkittävimmistä tuloksista.

Luvussa 3 tarkastellaan säännöllisen äärellisen lauseen ja kielen, sekä deterministen ja epädeterministen äärellisien automaattien käsitteitä. Todistetaan, että epädeterministisestä äärellisestä automaatista on mahdollista konstruoida deterministinen äärellinen automaatti ja että epädeterministisestä äärellisestä automaatista konstruoitu deterministinen äärellinen automaatti tunnistaa saman kielen kuin alkuperäinen epädeterministinen äärellinen automaatti. Luvussa 4 esitellään symbolisen säännöllisen lauseen ja kielen määritelmät sekä symbolisten deterministen ja epädeterministen automaattien käsitteet, niiden mintermit, sekä kieliin ja tiloihin liittyviä käsitteitä. Todennetaan ϵ-siirtymillä varustetun symbolisen epädeterministinen automaatin hyväksyvän jokaisen symbolisen säännöllisen kielen, Brzozowskin lauseen sekä symbolisten automaattien mintermeihin liittyviä väitteitä. Luvussa 5 tutkitaan peitteen ja atomipeitteen käsitteet, sekä atomipeitteen generoiman symbolisen epädeterministisen äärellisen automaatin, symbolisen atomaatin ja atomisen symbolisen epädeterministisen äärellisen automaatin käsitteet. Todistetaan apulauseita yleisen Brzozoskin lauseen todistusta varten.

Avainsanat: Boolen algebra, logiikka, automaattiteoria, symboliset automaatit
Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck -ohjelmalla.

Sisällys

1 Johdanto

Halmoksen ja Givantin kirjan [GH09] mukaan Boolen algebran kehitti englantilainen matemaatikko George Boole vuonna 1847. Boolen algebran teoria on yksi merkittävimmistä algebran alahaaroista. Se kehitettiin matematiikan logiikan tarpeisiin. Perinteisten laskutoimistusten sijaan käytetään komplementtia sekä kaksipaikkaisia konnektiiveja yhdistettä ja leikkausta. Boole kehitti Boolen algebran loogisen päättelyn matemaattiseen tutkimukseen. 1930-luvulla Stonen ja Tarskin työn ansiosta Boolen algebra irtautui logiikasta omaksi haarakseen, jota sovelletaan monilla muilla matematiikan haaroilla, muun muassa algebrassa, analyysissä, logiikassa, mittateoriassa, joukko-opissa, topologiassa, todennäköisyyslaskennassa sekä tilastotieteessä. Matematiikassa Boolen algebraa sovelletaan muun muassa ensimmäisen kertaluvun logiikan täydellisyyden todistuksessa ja jatkumohypoteesin riippumattomuustarkasteluissa. Boolen algebraa hyödynnetään myös runsaasti matematiikan ulkopuolellakin esimerkiksi antropologiassa, biologiassa, kemiassa, ekologiassa, taloustieteessä, sosiologiassa ja erityisesti tietotekniikassa ja filosofiassa. Tietotekniikassa sitä sovelletaan elektronisten piirien suunnittelussä, ohjelmoinnissa, tietokannoissa, vaativuusteoriassa sekä automaattiteoriassa.

Hopcroftin ja Ullmanin kirjan [HU79] perusteella automaattiteoria tutkii "abstrakteja laskentalaitteita". 1930-luvulla ennen varsinaisia tietokoneita Alan Turing tutki abstraktia laskentaa, jolla oli laskennan suhteen kaikki samat ominaisuudet kuin nykyajan moderneilla von Neumannin laskentaa hyödyntävillä tietokoneilla. Turingin tavoitteena oli määrittää täsmälleen, mitä abstraktilla laskennalla pystytään ja ei pystytä tekemään. Hänen löytämänsä rajat pätevät hänen tutkimiinsa Turingin koneisiin sekä moderneihin tietokoneisiin. 1940- ja 1950-luvuilla kehitettiin ja tutkittiin yksinkertaisempia koneita, joita nykyään kutsutaan äärellisiksi automaateiksi. Nämä kehitettiin mallintamaan aivojen toimintaa, mutta ne osoittautuivat erittäin hyödyllisiksi useisiin eri käyttötarkoituksiin. Niitä käytetään muun muassa virtapiirien suunnitteluun ja tarkistamiseen kehitetyissä ohjelmissa, sanastoanalysoijassa, joka hajottaa syötteeksi saamansa tekstin loogisiksi yksiköiksi avainsanoiksi ja välimerkeiksi. Yksinkertainen käytännön elämän esimerkki automaatista on lampun virtakatkaisin. Alkutilassa lamppu on pimeänä ja virtanappia ei olla painettu. Voimme painaa sen pohjaan. Jos lamppu muuten toimii normaalisti seuraavaksi lamppu valaisee huoneen ja voimme painaa sen pois päältä. Tilanteesta riippuen nämä molemmat voivat olla haluttuja niin lopputiloja.

Alan kehitykseen vaikutti vahvasti myös kielitieteilijä Noam Chomsky, joka 1950-luvun lopulla alkoi tutkimaan muodollisia kieliä. Vaikka nämä eivät olekaan koneita, ne ovat läheisessä suhteessa automaattien kanssa ja ovat esimerkiksi ohjelmointikielen kääntäjien pohjana. Symboliset deterministiset ja epädeterministiset äärelliset automaatit laajentavat deterministisiä ja epädeterministisiä äärellisiä automaatteja käyttämällä suuria tai jopa mahdollisesti äärettömän suuria Boolen algebran aakkostoja ja käyttämällä siirtymäkuvauksissa Boolen algebroille määriteltyjä predikaatteja. Tammin ja Veanaksen artikkelin [TV18] mukaan symbolisilla äärellisillä automaateilla on pyritty ratkaisemaan äärellisten automaattien rajoitteita, jotka liittyvät aakkoston kokoon. Perinteiset automaatit pystyvät käsittelemään vain äärellisiä ja pieniä aakkostoja. Käytännön sovelluksissa on kuitenkin tarvetta suuriin ja jopa äärettömiin aakkostoihin. Symboliset äärelliset automaatit esiteltiin Veanaksen, de Halleuxin ja Tillmannin artikkelissa [VdHT10]. Eri tutkijoiden toimesta niistä on kehitetty useita eri variaatioita, muun muassa symboliset alternoivat äärelliset automaatit, symboliset puuautomaatit, symboliset laajennetut äärelliset automaatit ja jo edellä mainitut symboliset deterministiset äärelliset automaatit ja symboliset epädeterministiset äärelliset automaatit. Symbolisia äärellisiä automaatteja on jo sovellettu artikkelin [DV17] mukaan puumanipulointiohjelmissa ja ohjelmasynteeseissä. Tässä

tutkielmassa kuitenkin keskitytään symbolisiin deterministisiin automaatteihin ja symbolisiin epädeterministisiin äärellisiin automaatteihin.
Lukijalta edellytetään algebran ja logiikan perusasioiden osaamista, kuten ideaaliteorian ymmärtämistä.

2 Boolen algebraa

Tutustutaan aluksi Boolen algebran perusteisiin. Tämä luku perustuu Givantiin ja Halmoksen teokseen [GH09] sekä Tammin ja Veanaksen artikkeliin [TV18]. Boolen algebra on algebran alahaara, joka eroaa muista haaroista siten, että se kehitettiin alunperin logiikan aritmetiikaksi. Perinteisten laskutoimitusten sijaan käytetään loogisia predikaatteja yhdiste $\vee$, leikkaus $\wedge$ ja negaatio $\neg$. Boolen algebra kehitettiin nimenomaan aritmetiikkana, joka soveltuisi logiikan matemaattiseen analysointiin.

Kerrataan aluksi renkaan määritelmä.

Määritelmä 2.1 (**Renkaan määritelmä**)**.** Olkoon A vähintään kahden alkion joukko. **Rengas** on kolmikko $(A, +, \cdot)$, jolle pätee seuraavat ehdot. Olkoot $a, b, c \in A$. $(A, +, \cdot)$ on liitännäinen yhteenlaskun ja kertolaskun suhteen eli

$$a + (b + c) = (a + b) + c$$
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

Lisäksi $(A, +, \cdot)$ on vaihdannainen yhteenlaskun suhteen, siis

$$a + b = b + a$$

Olkoot $0, 1 \in A$ $(A, +, \cdot)$:n yksiköt yhteenlaskun ja kertolaskun suhteen. Pitää siis olla

$$a + 0 = a$$
$$a \cdot 1 = 1 \cdot a = a.$$

Lisäksi kaikilla $a \in A$ on olemassa vasta-alkio $-a \in A$. Siis

$$a + (-a) = 0.$$

Osittelulakien pitää myös päteä eli

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(b + c) \cdot a = b \cdot a + c \cdot a.$$

Jos rengas on vaihdannainen kertolaskun suhteen eli kaikilla $a, b \in A$

$$a \cdot b = b \cdot a,$$

niin rengas $(A, +, \cdot)$ on **vaihdannainen rengas**. Kun kertolaskulla ei ole yksikköä eli ehto $a \cdot 1 = 1 \cdot a = a$ ei päde, rakennetta$(A, +, \cdot)$ kutsutaan **pseudorenkaaksi**.

Määritellään seuraavaksi Boolen renkaan käsite.

Määritelmä 2.2 (**Boolen rengas**)**.** Olkoon $(B, +, \cdot)$ rengas. Jos kaikki $a \in B$ ovat itsensä neliöitä, eli

$$a \cdot a = a,$$

niin rengas $(B, +, \cdot)$ on rengas on **idempotentti rengas** eli **Boolen rengas**.

Joissain lähteissä Boolen renkaaksi on määritetty vain idempotentti pseudorengas. Tässä tutkielmassa käytetään Halmoksen kirjan [GH09] mukaista määritelmää.

Esimerkki 2.3. Tarkastellaan kolmikkoa $(\mathbb{Z}_2, +, \cdot)$. Tiedämme, että $\mathbb{Z}_2$ sisältää vain alkiot $0, 1 \in \mathbb{Z}_2$. Tunnetusti $(\mathbb{Z}_p, +, \cdot)$ on kunta, jos ja vain jos p on alkuluku. Alkulukujen määritelmän mukaan 2 on pienin alkuluku, joten $(\mathbb{Z}_2, +, \cdot)$ on kunta. Kuntana $(\mathbb{Z}_2, +, \cdot)$ on myös rengas. Pitää siis tarkistaa vain idempotenttius.

$$1 \cdot 1 = 1$$
$$0 \cdot 0 = 0,$$

Määritelmä 2.4. Olkoon $\mathcal{X}$ mielivaltainen joukko ja $2^{\mathcal{X}}$ kaikkien kuvausten $\mathcal{X} \to 2$ joukko. Joukon $2^{\mathcal{X}}$ alkiot ovat **$\mathcal{X}$:n 2–arvoisia kuvauksia**. $\mathcal{X}$:lle on määritelty pisteittäin vakiokuvaukset 0 ja 1, siis

$$0(x) = 0 \quad \text{ja } 1(x) = 1.$$

Jos p ja q on $\mathcal{X}$:n 2–arvoisia kuvauksia, niin $p + q$ ja pq on määritelty pisteittäin siten, että

$$(p+q)(x) = p(x) + q(x) \qquad \text{ja} \qquad (pq)(x) = p(x)\, q(x).$$

Koska $2^{\mathcal{X}}$:lle pätevät rengasaksioomat ja se on idempotentti, niin sitä kutsutaan **joukon $\mathcal{X}$ Boolen renkaaksi.**

joten $(\mathbb{Z}_2, +\cdot)$ on idempotentti. Siis $(\mathbb{Z}_2, +\cdot)$ on Boolen rengas.

Määritellään renkaan karakteristika Murthyn kirjan [Mur12] mukaan.

Määritelmä 2.5. Olkoon $(R, +, \cdot)$ mielivaltainen rengas. Jos ei ole olemassa pienintä positiivistä $n \in \mathbb{N}$, jolla $n \cdot a = 0$ kaikilla $a \in R$, niin renkaan **karakteristika** $\operatorname{char}(R) = 0$. Muulloin renkaan $(R, +, \cdot)$ karakteristika on $\operatorname{char}(R) = n$, jossa $n \in \mathbb{N}$ on pienin positiivinen luonnollinen luku, jolla $n \cdot a = 0$ kaikilla $a \in R$.

Todistetaan Boolen renkaan karakteristikan olevan 2.

Lause 2.6. *Boolen renkaan $(A, +, \cdot)$ karakteristika on $\operatorname{char}(A) = 2$.*

Todistus. Olkoon $x \in A$. Tällöin

$$\begin{aligned} x + x &= (x+x)^2 \\ &= (x+x)(x+x) \\ &= x(x+x) + x(x+x) \\ &= x^2 + x^2 + x^2 + x^2 \\ &= x + x + x + x. \end{aligned}$$

Vähentämällä $x + x$ puolittain saadaan

$$0 = x + x.$$

Täten $\operatorname{char}(A) = 2$. □

Osoitetaan nyt Boolen renkaan vaihdannaisuuden seuraavan sen idempotenttiudesta.

Lause 2.7. *Olkoon $(A, +, \cdot)$ rengas. Jos $(A, +, \cdot)$ on idempotentti, niin se on myös vaihdannainen.*

Todistus. Olkoon $(A, +, \cdot)$ idempotentti rengas ja $x, y \in A$. Saadaan

$$\begin{aligned} x + y &= (x + y)^2 \\ &= x^2 + xy + yx + y^2 \\ &= x + xy + yx + y. \end{aligned}$$

Yksinkertaisella puolittaisella erotuksella saadaan

$$\begin{aligned} xy + yx &= 0 \\ &= xy + xy. \end{aligned}$$

Vähennetään vielä xy puolittain, jolloin päädytään haluttuun tulokseen

$$xy = yx.$$

Rengas $(A, +, \cdot)$ on täten vaihdannainen, jos se on idempotentti. □

Todistetaan, että $(\mathbb{Z}_2, +, \cdot)$ on suppein Boolen rengas.

Esimerkki 2.8. Osoitetaan, että $(\mathbb{Z}_2, +, \cdot)$ on suppein Boolen rengas. Aiemman perusteella tiedetään jo, että se on Boolen rengas. Siihen sisältyy vain alkiot $0, 1 \in \mathbb{Z}_2$. Olkoon nyt vielä $(B, +, \cdot)$ mielivaltainen Boolen rengas. Lisäksi $0_B, 1_B \in B$ ovat B:n nolla– ja ykkösalkiot. Määritellään kuvaus $f : \mathbb{Z}_2 \to B$, jolla $f(0) = 0_B$ ja $f(1) = 1_B$. Olkoot lisäksi $a, b \in \mathbb{Z}_2$. Tarkistetaan yhteen- ja kertolaskutaulut alkioille 0_B ja 1_B. Tiedetään, että 0_B on B:n nolla–alkio. Lauseen 2.6 perusteella tiedetään myös, että Boolen renkaan karakteristikan olevan 2. Siis yhteenlaskutaulu on seuraava.

$+$	0_B	1_B
0_B	0_B	1_B
1_B	1_B	0_B

Boolen algebroillakin nollalla kertominen tuottaa vastaukseksi nollan. Tiedetään myös 1_B olevan Boolen algebran ykkösalkio. Voidaan siis tehdä seuraava kertolaskutaulu

$\cdot$	0_B	1_B
0_B	0_B	0_B
1_B	0_B	1_B

Nyt alkiot 0_B ja 1_B käyttäytyvät renkaassa $(B, +, \cdot)$ täsmälleen samalla tavalla kuin 0 ja 1 käyttäytyvät renkaassa $(\mathbb{Z}_2, +, \cdot)$:ssa. Siis f on homomorfismi ja $(\mathbb{Z}_2, +, \cdot)$ uppoaa $(B, +, \cdot)$:n. Siis $(\mathbb{Z}_2, +, \cdot)$ on suppein Boolen rengas.

Boolen algebran teoria ei kuitenkaan rajoitu pelkästään Boolen renkaisiin. Tarkastellaan nyt toista oleellista Boolen algebran teorian käsitettä Boolen algebraa. Määritellään tämä tarkastelemalla mielivaltaista joukkoa, joka on varustettu yhdisteellä, leikkauksella ja komplementilla.

Määritelmä 2.9 (Boolen algebra). Olkoon B epätyhjä joukko. Kuusikkoa $(B, \wedge, \vee, \bar{\ }, 0, 1)$, jossa on kaksipaikkaiset laskutoimitukset $\wedge$, $\vee$, vakiot 0 ja 1 sekä yksipaikkainen laskutoimitus

$a \mapsto \overline{a}$, kutsutaan Boolen algebraksi, jos se täyttää seuraavat aksioomat kaikilla $a, b, c \in B$.

$$\begin{aligned}
\overline{0} = 1, \quad \overline{1} = 0,& \\
a \wedge 0 = 0, \quad a \vee 1 = 1,& \\
a \wedge 1 = a, \quad a \vee 0 = a,& \\
a \wedge \overline{a} = 0, \quad a \vee \overline{a} = 1,& \\
\overline{\overline{a}} = a,& \\
a \wedge a = a, \quad a \vee a = a,& \\
\overline{(a \wedge b)} = \overline{a} \vee \overline{b}, \quad \overline{(a \vee b)} = \overline{a} \wedge \overline{b},& \\
a \wedge b = b \wedge a, \quad a \vee b = b \vee a,& \\
a \wedge (b \wedge c) = (a \wedge b) \wedge c, \quad a \vee (b \vee c) = (a \vee b) \vee c,& \\
a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c), \quad a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c).&
\end{aligned}$$

Boolen algebran aksioomat ovat analogisia seuraavan lauseen 2.12 identiteettien kanssa.

Todistetaan vielä leikkauksen ja yhdisteen absorptiolait, jotka pätevät Boolen algebroille.

Lause 2.10. *Olkoon X mielivaltainen joukko, $(X, \wedge, \vee, \bar{\cdot}, 0, 1)$ sen Boolen algebra ja $a, b \in X$. Kaikilla a ja b pätee,*

$$a \wedge (a \vee b) = a \quad \textit{ja sen duaali} \quad a \vee (a \wedge b) = a.$$

Todistus. Olkoon $a, b \in X$. Nyt saadaan

$$\begin{aligned}
a \wedge (a \vee b) &= (a \vee 0) \wedge (a \vee b) \\
&= a \vee (0 \wedge b) \\
&= a \vee (b \wedge 0) \\
&= a \vee 0 \\
&= a.
\end{aligned}$$

Todistetaan väitteen duaali.

$$\begin{aligned}
a \vee (a \wedge b) &= (a \wedge 1) \vee (a \wedge b) \\
&= a \wedge (1 \vee b) \\
&= a \wedge (b \vee 1) \\
&= a \wedge 1 \\
&= a.
\end{aligned}$$

Absorptiolait siis pätevät. □

Jotta Boolen algebrojen määrittelystä olisi hyötyä, tarvitaan enemmän tietoa niiden rakenteesta. Esitellään tärkeimmät niille pätevät identiteettilait. Osajoukoille on myös määriteltävissä myös Boolen algebra.

Määritelmä 2.11 (Osajoukkojen Boolen algebra). Olkoon $A \neq \varnothing$ joukko ja $\mathcal{P}(A)$ sen potenssijoukko, joka on varustettu leikkauksella $\cap$ ja yhdisteellä $\cup$ sekä komplentilla $\bar{\cdot}$. Potenssijoukolla $\mathcal{P}(A)$ on nolla– ja ykkösalkiona ovat tyhjä joukko $\varnothing$ ja koko joukko A. Rakennetta $\mathcal{P}(A)$, joka koostuun, konjunktiosta, disjunktiosta, negaatiosta, sekä osajoukoista $\varnothing$ ja A kutsutaan **A:n kaikkien osajoukkojen Boolen algebraksi** tai lyhyemmin A:n Boolen algebraksi.

Lause 2.12. *Olkoon X mielivaltainen joukko ja $A, B, C \subset X$ sen osajoukkoja. X:n Boolen algebralle pätee seuraavat identiteetit:*
Tyhjän joukon komplementin ja universaalijoukon komplementtienlait

$$\overline{\varnothing} = X, \quad \overline{X} = \varnothing, \tag{2.1}$$

konjuktion tyhjän joukon kanssa ja universaalijoukon kanssa disjunktionlait

$$A \cap \varnothing = \varnothing, \quad A \cup X = X, \tag{2.2}$$

negaation konjunktion ja disjunktionlait

$$A \cap \overline{A} = \varnothing, \quad A \cup \overline{A} = X, \tag{2.3}$$

identiteettilait

$$A \cap X = A, \quad A \cup \varnothing = A, \tag{2.4}$$

kaksoisnegaationlaki

$$\overline{\overline{A}} = A, \tag{2.5}$$

idempotenttilait

$$A \cup A = A, \quad A \cap A = A, \tag{2.6}$$

De Morganin-lait

$$\overline{(A \cap B)} = \overline{A} \cup \overline{B}, \quad \overline{(A \cup B)} = \overline{A} \cap \overline{B}, \tag{2.7}$$

vaihdannaisuuslait

$$A \cap B = B \cap A, \quad A \cup B = B \cup A, \tag{2.8}$$

liitäntälait

$$A \cap (B \cap C) = (A \cap B) \cap C, \quad A \cup (B \cup C) = (A \cup B) \cup C, \tag{2.9}$$

sekä osittelulait

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C). \tag{2.10}$$

Boolen algebran identiteetit ovat selvästi hyvin samankaltaisia Boolen renkaiden aksioomien kanssa, joka herättää toivoa, että löytyisi yhteys joukon A Boolen renkaan ja algebran välille. Siis herää kysymys, että pystytäänkö määrittelemään Boolen algebroille yhteen– ja kertolaskut yhdisteiden ja leikkausten kautta. Tarkastellaan Boolen rengasta $(B, +, \cdot)$ ja Boolen algebraa $(B, \wedge, \vee, \bar{\cdot}, 0, 1.)$.

Lause 2.13. *Olkoon B joukko. Olkoot $(B, +, \cdot)$ B:n Boolen rengas ja $(B, \wedge, \vee, \bar{\cdot}, 0, 1)$ B:n Boolen algebra. Tällöin Boolen algebrasta $(B, \wedge, \vee, \bar{\cdot}, 0, 1)$ voidaan tulkita Boolen rengas $(B, +, \cdot)$ laskutoimituksilla*

$$c + d = \left(c \wedge \overline{d}\right) \vee (d \wedge \overline{c}) \quad \text{ja} \quad c \cdot d = c \wedge d,$$

kun $c, d \in B$.

Todistus. Leikkaus on liitännäinen, vaihdannainen ja idempotentti, sekä sillä on ykkösalkio, koska leikkaus ja kertolasku ovat sama laskutoimitus. Näillä määritelmillä saadaan tulkittua Boolen algebran olevan Boolen rengas. Olkoon $e, f, g \in B$. Tarkistetaan ensin yhteenlaskun liitännäisyys.

$$\begin{aligned}
e + (f + g) &= e + \big((f \wedge \bar{g}) \vee (g \wedge \bar{f})\big) \\
&= \Big(e \wedge \overline{\big((f \wedge \bar{g}) \vee (g \wedge \bar{f})\big)}\Big) \vee \big(\big((f \wedge \bar{g}) \vee (g \wedge \bar{f})\big) \wedge \bar{e}\big) \\
&= \Big(e \wedge \Big(\overline{(f \wedge \bar{g})} \wedge \overline{(g \wedge \bar{f})}\Big)\Big) \vee \big(\big((f \wedge \bar{g}) \wedge \bar{e} \vee (g \wedge \bar{f}) \wedge \bar{e}\big)\big) \\
&= \big(e \wedge \big((\bar{f} \vee g) \wedge (\bar{g} \vee f)\big)\big) \vee \big(\big((f \wedge \bar{g}) \wedge \bar{e} \vee (g \wedge \bar{f}) \wedge \bar{e}\big)\big) \\
&= \big(e \wedge \big(\big((\bar{f} \vee g) \wedge \bar{g}\big) \vee \big((\bar{f} \vee g) \wedge f\big)\big)\big) \vee \big(\big((f \wedge \bar{e}) \wedge \bar{g} \vee (\bar{e} \wedge \bar{f}) \wedge\ g\big)\big) \\
&= \big(e \wedge \big(\big((\bar{f} \vee g) \wedge \bar{g}\big) \vee \big((\bar{f} \vee g) \wedge f\big)\big)\big) \vee \big(\big((f \wedge \bar{e}) \wedge \bar{g} \vee (\bar{e} \wedge \bar{f}) \wedge\ g\big)\big) \\
&= \big(e \wedge \big((\bar{f} \vee \bar{g}) \vee (g \wedge \bar{g}) \vee (\bar{f} \wedge f) \vee (g \wedge f)\big)\big) \vee \big(\big((f \wedge \bar{e}) \wedge \bar{g} \vee (\bar{e} \wedge \bar{f}) \wedge\ g\big)\big) \\
&= \big(e \wedge \big((\bar{f} \vee \bar{g}) \vee 0 \vee 0 \vee (g \wedge f)\big)\big) \vee \big(\big((f \wedge \bar{e}) \wedge \bar{g} \vee (\bar{e} \wedge \bar{f}) \wedge\ g\big)\big) \\
&= \big(e \wedge (\bar{f} \vee \bar{g}) \vee e \wedge (g \wedge f)\big) \vee \big(\big((f \wedge \bar{e}) \wedge \bar{g} \vee (\bar{e} \wedge \bar{f}) \wedge\ g\big)\big) \\
&= \big(\bar{g} \wedge (\bar{f} \vee e) \vee g \wedge (e \wedge f)\big) \vee \big(\big((f \wedge \bar{e}) \wedge \bar{g} \vee (\bar{e} \wedge \bar{f}) \wedge\ g\big)\big) \\
&= \big(e \wedge \bar{f}\big) \wedge \bar{g} \vee (e \wedge f) \wedge g \vee (f \wedge \bar{e}) \wedge \bar{g} \vee \big(\bar{f} \wedge \bar{e}\big) \wedge g \\
&= \big(\big((e \wedge \bar{f}) \vee (f \wedge \bar{e})\big) \wedge \bar{g}\big) \vee \big(g \wedge \big((e \wedge f) \vee (\bar{f} \wedge \bar{e})\big)\big) \\
&= \big(\big((e \wedge \bar{f}) \vee (f \wedge \bar{e})\big) \wedge \bar{g}\big) \vee \big(g \wedge \big((e \wedge f) \vee 0 \vee 0 \vee (\bar{f} \wedge \bar{e})\big)\big) \\
&= \big(\big((e \wedge \bar{f}) \vee (f \wedge \bar{e})\big) \wedge \bar{g}\big) \vee \big(g \wedge \big((e \wedge f) \vee (e \wedge \bar{e}) \vee (f \wedge \bar{f}) \vee (\bar{f} \wedge \bar{e})\big)\big) \\
&= \big(\big((e \wedge \bar{f}) \vee (f \wedge \bar{e})\big) \wedge \bar{g}\big) \vee \big(g \wedge \big(\big((\bar{e} \vee f) \wedge \bar{f}\big) \vee (\bar{e} \wedge f) \wedge e\big)\big) \\
&= \big(\big((e \wedge \bar{f}) \vee (f \wedge \bar{e})\big) \wedge \bar{g}\big) \vee \big(g \wedge \big((\bar{e} \vee f) \wedge (\bar{f} \vee e)\big)\big) \\
&= \big(\big((e \wedge \bar{f}) \vee (f \wedge \bar{e})\big) \wedge \bar{g}\big) \vee \Big(g \wedge \Big(\overline{(e \wedge \bar{f})} \wedge \overline{(f \wedge \bar{e})}\Big)\Big) \\
&= \big(\big((e \wedge \bar{f}) \vee (f \wedge \bar{e})\big) \wedge \bar{g}\big) \vee \Big(g \wedge \overline{\big((e \wedge \bar{f}) \vee (f \wedge \bar{e})\big)}\Big) \\
&= \big(e \wedge \bar{f}\big) \vee (f \vee \bar{e})\big) + g \\
&= (e + f) + g.
\end{aligned}$$

Varmistetaan yhteenlaskun vaihdannaisuus.

$$\begin{aligned}
e + f &= \big(e \wedge \bar{f}\big) \vee (f \wedge \bar{e}) \\
&= (f \wedge \bar{e}) \vee \big(e \wedge \bar{f}\big) \\
&= f + e.
\end{aligned}$$

Tarkistetaan yhteenlaskun nolla– sekä vasta–alkion olemassaolot. Ensin yhteenlaskun nolla–alkion olemassaolo.

$$\begin{aligned}
e + 0 &= \big(e \wedge \bar{0}\big) \vee (0 \wedge \bar{e}) \\
&= e \vee 0 \\
&= e.
\end{aligned}$$

Sitten vasta-alkion olemassaolo.

$$\begin{aligned} e + e &= (e \wedge \bar{e}) \vee (e \wedge \bar{e}) \\ &= 0 \vee 0 \\ &= 0 \end{aligned}$$

eli siis jokainen Boolen algebran alkio on oma vasta–alkionsa.

Todistetaan lopuksi osittelulait.

$$\begin{aligned} e \cdot (f + g) &= e \wedge (f + g) \\ &= e \wedge \left((f \wedge \bar{g}) \vee \left(g \wedge \bar{f}\right)\right) \\ &= (e \wedge (f \wedge \bar{g})) \vee \left(e \wedge \left(g \wedge \bar{f}\right)\right) \\ &= ((e \wedge f) \wedge \bar{g}) \vee \left((e \wedge g) \wedge \bar{f}\right) \\ &= ((e \wedge f) \wedge \bar{g}) \vee \left((e \wedge g) \wedge \bar{f}\right) \\ &= 0 \vee ((e \wedge f) \wedge \bar{g}) \vee 0 \vee \left((e \wedge g) \wedge \bar{f}\right) \\ &= (0 \wedge f) \vee ((e \wedge f) \wedge \bar{g}) \vee (0 \wedge g) \vee \left((e \wedge g) \wedge \bar{f}\right) \\ &= ((e \wedge \bar{e}) \wedge f) \vee ((e \wedge f) \wedge \bar{g}) \vee ((e \wedge \bar{e}) \wedge g) \vee \left((e \wedge g) \wedge \bar{f}\right) \\ &= ((e \wedge f) \wedge \bar{e}) \vee ((e \wedge f) \wedge \bar{g}) \vee ((e \wedge g) \wedge \bar{e}) \vee \left((e \wedge g) \wedge \bar{f}\right) \\ &= ((e \wedge f) \wedge (\bar{e} \vee \bar{g})) \wedge \left((e \wedge g) \wedge \left(\bar{e} \vee \bar{f}\right)\right) \\ &= \left((e \wedge f) \wedge \overline{(e \wedge g)}\right) \wedge \left((e \wedge g) \wedge \overline{(e \wedge f)}\right) \\ &= (e \wedge f) + (e \wedge g) \\ &= e \cdot f + e \cdot g \end{aligned}$$

sekä

$$\begin{aligned} (e + f) \cdot g & \\ &= (e + f) \wedge g \\ &= \left(\left(e \wedge \bar{f}\right) \vee (f \wedge \bar{e})\right) \wedge g \\ &= \left(\left(\left(e \wedge \bar{f}\right) \wedge g\right) \vee ((f \wedge \bar{e}) \wedge g)\right) \\ &= \left(\left(\left((e \wedge g) \wedge \bar{f}\right) \vee 0\right) \vee (((f \wedge g) \wedge \bar{e}) \vee 0)\right) \\ &= \left(\left(\left((e \wedge g) \wedge \bar{f}\right) \vee (e \wedge 0)\right) \vee (((f \wedge g) \wedge \bar{e}) \vee (f \wedge 0))\right) \\ &= \left(\left(\left((e \wedge g) \wedge \bar{f}\right) \vee (e \wedge (g \wedge \bar{g}))\right) \vee (((f \wedge g) \wedge \bar{e}) \vee (f \wedge (g \wedge \bar{g})))\right) \\ &= \left(\left(\left((e \wedge g) \wedge \bar{f}\right) \vee ((e \wedge g) \wedge \bar{g})\right) \vee (((f \wedge g) \wedge \bar{e}) \vee ((f \wedge g) \wedge \bar{g}))\right) \\ &= \left((e \wedge f) \wedge \left(\bar{f} \vee \bar{g}\right)\right) \vee ((f \wedge g) \wedge (\bar{e} \vee \bar{g})) \\ &= \left((e \wedge f) \wedge \overline{(f \wedge g)}\right) \vee \left((f \wedge g) \wedge \overline{(e \wedge g)}\right) \\ &= (e \wedge g) + (e \wedge g) \\ &= e \cdot g + f \cdot g \end{aligned}$$

Nyt $(B, \wedge, \vee, \bar{\cdot}, 0, 1)$ on tulkittavissa Boolen renkaaksi, koska yhteen- ja kertolaskuille pätee Boolen renkaan aksioomat.

□

Tästä eteenpäin voidaan käyttää Boolen rengaiden yhteen- ja kertolaskuille määritelmää $c + d = \left(c \wedge \bar{d}\right) \vee (d \wedge \bar{c})$ ja $c \cdot d = c \wedge d$. Nyt Boolen algebrasta voidaan tulkita Boolen rengas.

Määritelmä 2.14. Olkoon $(B, \wedge, \vee, \bar{\ }, 0, 1)$ mielivaltainen Boolen algebra ja $p, q \in B$. Relaatiota $\geq$ kutsutaan **Boolen algebran järjestysrelaatioksi**, Kun $p \wedge q = p$ tai yhtäpitävästi $p \vee q = p$, nin.

Tutkitaan sitten Boolen algebran maksimaalisia ideaaleja ja homomorfismeja, jotta luvun lopuksi voidaan todistaa Stonen esityslause. Esitetään aluksi ideaalille, sekä aidolle ja maksimaaliselle ideaalille määritelmät.

Määritelmä 2.15 (**Boolen algebran ideaali**)**. Ideaali** on Boolen algebran $(B, \wedge, \vee, \bar{\ }, 0, 1)$ osajoukko M, jolle pätee

1. $0 \in M$
2. jos $p \in M$ ja $q \in M$, niin $p \vee q \in M$,
3. jos $p \in M$ ja $q \in B$, niin $p \wedge q \in M$.

Jos $1 \notin M$, niin ideaali on **aito ideaali**.

Määritelmä 2.16 (**Maksimaalinen ideaali**)**.** Olkoon $\mathbb{B} = (B, \wedge, \vee, \bar{\ }, 0, 1)$ Boolen algebra. Boolen algebran $\mathbb{B}$ ideaali M on **maksimaalinen** , jos se on aito ideaali, joka ei aidosti sisälly mihinkään muuhun ideaalin. Toisin sanoen, jos N on ideaali, jolle $M \subseteq N$, niin joko $M = N$ tai $N = B$.

Määritelmä 2.17. Olkoon $\mathbb{B} = (B, \wedge, \vee, \bar{\ }, 0, 1)$ Boolen algebra ja E joukon B mielivaltainen osajoukko. Jokaisen E:n sisältävän ideaalin leikkaus on myös ideaali. Tämä ideaali on pienin ideaali, joka sisältää E:n ja sitä kutsutaan M E**:n generoimaksi ideaaliksi**. Jos yhden alkion joukko $\{p\}$ generoi ideaalin, kyseistä ideaalia kutsutaan **pääideaaliksi**.

Tutkitaan seuraavaksi Boolen algebran generoivien ideaalien ominaisuuksia. Esitetään seuraava lause ilman todistusta.

Lause 2.18. *Boolen algebran* $(B, \wedge, \vee, \bar{\ }, 0, 1)$ *alkio* p *on joukon* E *generoimassa ideaalissa, jos ja vain jos on olemassa sellainen* E*:n äärellinen osajoukko* F*, että* $p \leq \bigvee F$.

Lause 2.19. *Olkoon* M *ideaali ja* $p_0 \in B$ *Boolen algebran* $\mathbb{B} = (B, \wedge, \vee, \bar{\ }, 0, 1)$ *alkio. Joukon* $M \cup \{p_0\}$ *generoima ideaali on joukko*

$$N = \{p \vee q \mid p \leq p_0 \text{ ja } q \in M\}.$$

Todistus. Olkoon $E = M \cup \{p_0\}$. Käytetään seuraavaksi lausetta 2.18. Boolen algebran $\mathbb{B}$ alkio r on joukon E generoimassa ideaalissa, jos ja vain jos on olemassa äärellinen $F \subset E$, jolle pätee $r \leq \bigvee F$. Voidaan olettaa, että $p_0 \in F$ menettämättä yleispätevyyttä. Koska M on suljettu yhdisteen suhteen, niin F:n M:ssä olevat alkiot voidaan yhdistää yhdeksi alkioksi. Alkio r on siis E:n generoimassa ideaalissa, jos ja vain jos on olemassa alkio $s \in M$ siten, että $r \leq s \vee p_0$. Epäyhtälöstä seuraa

$$r = r \wedge (s \vee p_0) = (r \wedge s) \vee (r \wedge p_0)\,.$$

Merkitään $q = r \wedge s \in M$ ja $p = r \wedge p_0 \leq p_0$. Alkio r on siis E:n generoima ideaalissa, kun

$$r = q \vee p$$

jollain $q \in M$ ja jollain $p \leq p_0$. □

Lause 2.20. *Olkoon M ideaali ja $p_0 \in B$ Boolen algebran alkio. Jos $\bar{p}_0 \notin M$, niin $M \cup \{p_0\}$ generoima ideaali on aito ideaali.*

Todistus. Tehdään todistus vastaoletuksen kautta. Olkoon N $M \cup \{p_0\}$:n generoima ideaali. Oletetaan myös, että N ei ole aito ideaali. Koska N ei ole aito ideaali, niin $\bar{p}_0 \in N$. Täten lauseen 2.19 mukaan on olemassa $p, q \in M$, joille pätee $p \leq p_0$ ja $\bar{p}_0 = p \vee q$. Yksinkertaisella laskulla saadaan, että

$$\begin{aligned}
\bar{p}_0 &= \bar{p}_0 \wedge \bar{p}_0 \\
&= \bar{p}_0 \wedge (p \vee q) \\
&= (\bar{p}_0 \wedge p) \vee (\bar{p}_0 \wedge q) \\
&\leq (\bar{p}_0 \wedge p_0) \vee (\bar{p}_0 \wedge q) \\
&= 0 \vee (\bar{p}_0 \wedge q) \\
&= \bar{p}_0 \wedge q \leq q.
\end{aligned}$$

Täten $\bar{p}_0 \in M$, joten päädyttiin ristiriitaan. Vastaoletus ei siis päde. □

Lause 2.21. *Olkoon $\mathbb{B} = (B, \wedge, \vee, \bar{\ }, 0, 1)$ Boolen algebra. Boolen algebran $\mathbb{B}$:n järjestettyjen ideaalien epätyhjä ketju on ideaali I. Ideaali I on aito ideaali, jos ja vain jos jokainen ideaali $a \in I$ on aito ideaali.*

Todistus. Olkoon M_i epätyhjä perhe Boolen algebran $(B, \wedge, \vee, \bar{\ }, 0, 1)$ ideaaleja ja merkitään, että $M = \bigvee M_i$. Todistetaan määritelmän 2.15 ehdot. Oletuksen perusteella M sisältää vähintään yhden ideaalin $M_0 \subseteq M$, ja ideaalin määritelmän mukaan $0 \in M_0$, joten $0 \in M$.

Olkoon $a, b \in M$. Nyt on siis oltava ideaalit $M_j, M_k \subseteq M$, joilla $a \in M_j$ ja $b \in M_k$. Koska M on järjestetty ketju, niin on olemassa ideaali $M_l \subseteq M$, jolle $M_j, M_k \subseteq M_l$. Täten $a, b \in M_k$, ja nyt ideaalin määritelmän mukaan myös $a \vee b \in M_l$. Täten myös $a \vee b \in M$.

Olkoon $a \in M$. Nyt pitää olla jokin $M_i \subseteq M$, jolle pätee, että $a \in M_i$. Nyt Boolen algebran mielivaltaisella alkiolla b pätee, että $a \wedge b \in M_i$ ja siten myös $a \wedge b \in M$. Nyt siis M on ideaali.

Ideaali on epäaito, jos $1 \in M$. Nyt $1 \in M$, jos ja vain jos $1 \in M_j$ jollain $M_j \subseteq M$. Siis M on epäaito, jos ja vain jos jokin M_j on epäaito. □

Lause 2.22. *Boolen algebran $(B, \wedge, \vee, \bar{\ }, 0, 1)$ aito ideaali on maksimaalinen, jos ja vain jos kaikilla $p \in B$ joko $p \in M$ tai $\bar{p} \in M$.*

Todistus. Oletetaan aluksi, että on olemassa $p \in B$, jolla $p, \bar{p} \notin M$. Jos N on $M \cup \{p\}$:n generoima ideaali, niin N on aito ideaali. Täten $M \subsetneq N$, sillä $p \notin M$. Täten M ei ole maksimaalinen.

Kääntäen oletetaan, että aina joko $p \in M$ tai $\bar{p} \in M$ ja olkoon N on ideaali, jolla $M \subsetneq N$:n. On todistettava, että $N = B$. Koska $M \subseteq N$ on olemassa $p \in N$ siten, että $p \notin M$. Oletuksista seuraa, että $\bar{p} \in M$ ja siten myös $\bar{p} \in N$. Koska N on ideaali, niin $p \vee \bar{p} \in N$. Täten $N = B$. □

Määritelmä 2.23. Boolen ideaali M on **alkuideaali**, jos se on aito ideaali ja jos ehdosta $p \wedge q \in M$ seuraa $p \in M$, tai $q \in M$.

Lause 2.24 (**Maksimaali-ideaali teoreema**)**.** *Jokainen Boolen algebran aito ideaali sisältyy maksimaaliseen ideaaliin.*

Todistus. Olkoon M Boolen algebran $(B, \wedge, \vee, \bar{\ }, 0, 1)$ aito ideaali. Luetellaan alkiot B:n alkioiden jonossa $(p_i)_{i<\alpha}$. Määritellään vastaava jono $(M_i)_{i<\alpha}$ $(B, \wedge, \vee, \bar{\ }, 0, 1)$aitoja ideaaleja, joille pätee

1. $M_0 = M$,

2. $M_i \subseteq M_j$ aina, kun $i \leq j \leq \alpha$,

3. joko $p_i \in M_{i+1}$ tai $\bar{p}_i \in M_{i+1}$ kaikilla $i < \alpha$.

Olkoon sitten $M_0 = M$. M_0 on nyt aito ideaali oletusten nojalla. Ehto 1 toteutuu automaattisesti, sekä ehdot 2 ja 3 pätevät myös selvästi jonojen perheelle $(M_i)_{i<0}$. Olkoon $k \leq \alpha$ ordinaaliluku. Oletetaan, että aidot ideaalit M_i on määritelty kaikille ordinaaleille $i < k$ siten, että $(M_i)_{i<k}$ täyttää ehdot 1, 2 ja 3. Kun k on seuraaja ordinaali $k = i + 1$, niin joukon M_k määritelmä jakaantuu kahteen tapaukseen. Jos joko $p_i \in M_i$ tai $\bar{p}_i \in M_i$, valitaan $M_k = M_i$. Nyt induktio-oletuksen perusteella M_k on aito ideaali. Muulloin määritellään M_k olemaan joukon $M_i \cup \{p_i\}$ generoima ideaali. Lauseesta 2.20 seuraa,että myös tässä tapauksessa M_k on aito ideaali.

Kun k on rajaordinaali, merkitään

$$M_k = \bigcup_{i<k} M_i.$$

Lauseen 2.21 perusteella aitojen ideaalien yhdisteet ovat aitoja ideaaleja, joten nytkin M_k on aito ideaali. Joukko M_α on haettu maksimaalinen M:n laajennus. Se on aito ideaali konstruktion perusteella. Lisäksi ehtojen 1 ja 2 perusteella se laajentaa M:ää. Olkoon nyt $p \in B$ mielivaltainen alkio. Alkio p esiintyy jossain kohtaa B:n alkioiden luettelossa. Voidaan valita $p = p_i$. Nyt ehdon 3 perusteella, joko $p_i \in M_i$ tai $\bar{p}_i \in M_i$, joten ehdon 2 perusteella $p \in M_\alpha$ tai $\bar{p} \in M_\alpha$. Ei voi olla, että $p, \bar{p} \in M_\alpha$, sillä tällöin M_α ei olisi aito ideaali. M_α:n on siis maksimaalinen lauseen 2.22 perusteella. □

Maksimaali-ideaali teoreemalle voi esittää vahvemman muotoilun seuraavasti.

Lause 2.25 (Maksimaali-ideaali teoreema versio 2)**.** *Boolen algebran $\mathbb{B}$ jokaiselle aidolle ideaalille M ja jokaiselle alkiolle $p \in \mathcal{B}$, jolla $p \notin M$, on olemassa maksimaalinen ideaali N, jolla $M \subset N$, mutta $p \notin N$.*

Todistus. Lauseen 2.20 perusteella $M \cup \{\bar{p}\}$ generoima ideaali N on aito ideaali. Käytetään, sitten maksimaali-ideaali teoreemaa eli lausetta 2.24. Saadaan maksimaalinen ideaali H, jolla pätee, että $M \subset N \subset H$. Koska $\bar{p} \in H$, niin $p \notin H$. □

Määritelmä 2.26. Olkoon $(B, \wedge, \vee, \bar{\cdot}, 0, 1)$ ja $(C, \wedge, \vee, \bar{\cdot}, 0, 1)$ Boolen algebroja. **Boolen homomorfismi** on kuvaus $f : B \to C$, siten että kaikilla $p, q \in B$:

1. $f(p \wedge q) = f(p) \wedge f(q)$

2. $f(p \vee q) = f(p) \vee f(q)$

3. $f(\bar{p}) = \bar{f}(p)$.

Jos f on bijektio, niin sitä kutsutaan **isomorfismiksi**.

Määritelmä 2.27. Olkoon X mielivaltainen joukko ja 2^X on kaikkien kuvausten $\mathcal{X} \to \mathbb{Z}_2$ joukko. Joukon 2^X alkioita kutsutaan X:n **2-arvoisiksi kuvauksiksi**.

Lause 2.28. *Jokaisen Boolen algebran* $(B, \wedge, \vee, \bar{\ }, 0, 1)$ *jokaiselle nollasta eroavalle alkiolle* p *on olemassa 2-arvoinen homomorfismi* $x : B \to \mathbb{Z}_2$*, jolla*

$$x(p) = 1.$$

Todistus. Olkoon $\mathbb{B} = (B, \wedge, \vee, \bar{\ }, 0, 1)$ lauseen väitteen Boolen algebra ja $0 \neq p \in B$. Tarkastellaan p:n komplementin $\bar{p}$ generoimaa pääideaalia N. Koska $p \neq 0$, niin $\bar{p} \neq 1$ eli $1 \notin N$. Siis N on aito ideaali. Laajennetaan N maksimaaliseksi ideaaliksi M soveltamalla lausetta 2.24. Lauseen 2.22 perusteella huomataan, että $p \notin M$, sillä $\bar{p} \in M$. Ositus $(B/M, \wedge, \vee, \bar{\ }, 0, 1)$ on kahden alkion Boolen algebra. Olkoon z projektio $B \to B/M$, joka kuvaa jokaisen alkion $q \in \mathcal{B}$ sivuluokkaan $q/M = q + M$ ja y isomorfismi $B/M \to \mathbb{Z}_2$, joka kuvaa $0/M \to 0$ ja $1/M \to 1$. Nyt $x = y \circ z$ on etsitty 2-arvoinen homomorfismi $(B, \wedge, \vee, =, 0, 1)$:ssä, sillä

$$x(q) = y(z(q)) = y(q/M) = \begin{cases} 1, & \text{jos } q \notin M \\ 0, & \text{jos } q \in M \end{cases}.$$

Erityisesti $x(p) = 1$, koska $p \notin M$. □

Seuraava lause on Stonen esityslause. Se on yksi Boolen algebran merkittävimmistä tuloksista. Sen avulla pystytään vastaamaan niin sanottuun esitysongelmaan eli onko jokainen Boolen algebra isomorfinen joukkojen kunnan kanssa? Siis, jos $(B, \wedge, \vee, \bar{\ }, 0, 1)$ on Boolen algebra, onko olemassa joukko $\mathcal{X}$, että $(B, \wedge, \vee, \bar{\ }, 0, 1)$ on isomorfinen $\mathcal{P}(X)$ alialgebran kanssa?

Lause 2.29 (Stonen esityslause). *Merkitään* $\mathcal{X}$*:llä 2-arvoisten homomorfismien joukkoa Boolen algebrassa* $(B, \wedge, \vee, \bar{\ }, 0, 1)$*.* $(B, \wedge, \vee, \bar{\ }, 0, 1)$ *on upotettavissa* $\mathcal{P}(X)$*:n kuvauksella*

$$f(p) = \{x \in \mathcal{X} \mid x(p) = 1\}$$

kaikilla $p \in B$*.*

Todistus. Olkoon $(B, \wedge, \vee, \bar{\ }, 0, 1)$ Boolen algebra ja $p, q \in B$. Osoitetaan ensin, että f säilyttää yhdisteen:

$$\begin{aligned} f(p \vee q) &= \{x \in \mathcal{X} \mid x(p \vee q) = 1\} \\ &= \{x \in \mathcal{X} \mid x(p) \vee x(q) = 1\} \\ &= \{x \in \mathcal{X} \mid x(p) = 1 \text{ tai } x(q) = 1\} \\ &= \{x \in \mathcal{X} \mid x(p) = 1\} \cup \{x \in \mathcal{X} \mid x(q) = 1\} \\ &= f(p) \cup f(q). \end{aligned}$$

Osoitetaan samalla tavalla, että on f säilyttää leikkauksen:

$$\begin{aligned} f(p \wedge q) &= \{x \in \mathcal{X} \mid x(p \wedge q) = 1\} \\ &= \{x \in \mathcal{X} \mid x(p) \wedge x(q) = 1\} \\ &= \{x \in \mathcal{X} \mid x(p) = 1 \text{ ja } x(q) = 1\} \\ &= \{x \in \mathcal{X} \mid x(p) = 1\} \cap \{x \in \mathcal{X} \mid x(q) = 1\} \\ &= f(p) \cap f(q). \end{aligned}$$

Vastaavasti f säilyttää komplementin:

$$\begin{aligned} f(\bar{p}) &= \{x \in \mathcal{X} \mid x(\bar{p}) = 1\} \\ &= \{x \in \mathcal{X} \mid \bar{x}(p) = 1\} \\ &= \{x \in \mathcal{X} \mid x(p) = 0\} \\ &= \overline{\{x \in \mathcal{X} \mid x(p) = 1\}} \\ &= \overline{f(p)}. \end{aligned}$$

Kuvaus f on siis homomorfismi. Nyt f voidaan tulkita rengashomomorfismiksi, jolla on ydin. Lauseen 2.28 mukaan, jos $p \neq 0$, niin B:ssä on olemassa 2-arvoinen homomorfismi x, jolle $x(p) = 1$. Täten $f(p) \neq \varnothing$. Nyt siis jokainen $p \neq 0$ kuvautuu epätyhjälle joukolle, joten p ei voi olla f:n ytimessä. Siis f on bijektio, sillä sen ydin sisältää vain 0:n. □

3 Äärelliset automaatit

Tämä luku perustuu Hopcroftin ja Ullmanin kirjaan [HU79]. Automaattiteoria on matemaattisen logiikan ja teoreettisen tietotekniikan haara, jossa tutkitaan abstraksteja laskentalaitteita. Automaattiteoria sai alkunsa, kun Alan Turing kehitti 1930-luvulla Turingin koneiden käsitteen. Turingin koneilla on laskemiskyvyn suhteen täysin samat ominaisuudet kuin moderneilla von Neumannin laskentaa käyttävillä tietokoneilla, mutta Turingin koneet ovat äärettömiä toisin kuin tietokoneet. Turing yritti selvittää, mitä nämä Turingin koneet pystyvät ja eivät pysty laskemaan. Hänen tuloksensa pätevät abstraktien Turingin koneiden lisäksi myös oikeisiin moderneihin tietokoneisiin. 1940-luvulla tutkijat loivat yksinkertaisemman koneen äärellisen automaatin käsitteen. Tässä tutkielmassa keskitytään deterministisiin ja epädeterministisiin äärellisiin automaatteihin ja niiden ominaisuuksiin.

Merkitään ϵ:lla **tyhjää sanaa**, eli sanaa, jossa ei ole yhtään merkkiä. **Aakkostosta** Σ voidaan muodostaa joukot $\Sigma^+ = \Sigma^1 \cup \Sigma^2 \cup \dots$, jossa Σ^k on joukko k-pituisia merkkijonoja, joissa käytetään vain Σ:n merkkejä, ja $\Sigma^* = \Sigma^+ \cup \{\epsilon\}$. Niiden joukkoa $\mathcal{L}$ kutsutaan **Σ:n kieleksi**.

Määritelmä 3.1. Olkoot x ja y merkkijonoja. Olkoot x i:n merkin pituinen jono ja y j:n merkin pituinen jono. Merkitään $x = a_1 a_2 \dots a_i$ ja $y = b_1 b_2 \dots b_j$. Jonojen x ja y **konkatenaatio** on jono $xy = a_1 a_2 \dots a_i b_1 b_2 \dots b_j$. Merkkijonojen joukkojen L ja M konkatenaatio muodostetaan konkatenoimalla jokainen jono $a \in L$ kaikilla jonoilla $b \in M$. Joukkojen konkatenaatiota merkitään $L.M$:llä.

Esimerkki 3.2. Olkoon $L = \{001, 10, 111\}$ ja $M = \{\epsilon, 001\}$ merkkijonojen joukkoja. Näiden konkatenaatio $L.M = \{001, 10, 111, 001001, 10001, 111001\}$.

Määritellään säännölliset kielet.

Määritelmä 3.3 (**Säännöllinen lause ja kieli**)**.** Voidaan määrittää **säännölliset lauseet** rekursiivisesti. Merkitään $\mathcal{L}(X)$:llä säännöllistä lausetta vastaavaa kieltä.

- Vakiot ϵ ja $\varnothing$ ovat säännöllisiä lauseita, jotka ilmaisevat kielet $\{\epsilon\}$ ja $\varnothing$. Siis $\mathcal{L}(\epsilon) = \{\epsilon\}$ ja $\mathcal{L}(\varnothing) = \varnothing$.
- Olkoon a merkki, jolloin a on säännöllinen lause, joka ilmaisee kielen $\{a\}$. Siis $\mathcal{L}(a) = \{a\}$.
- Jos $\mathcal{X}$ ja $\mathcal{Y}$ on säännöllisiä lauseita, niin myös $X + Y$, XY ja $\neg\mathcal{L}(X)$ jotka ilmaisevat kielet $\mathcal{L}(\mathcal{X} + \mathcal{Y}) = \mathcal{L}(X) \cup \mathcal{L}(Y)$, $\mathcal{L}(XY) = \mathcal{L}(X)\,\mathcal{L}(Y)$ ja $\neg\mathcal{L}(X) = \Sigma^* \setminus X$.

Säännöllisten lauseiden määrittämä kieli on **säännöllinen kieli**.

Siirrytään nyt määrittelemään deterministinen äärellinen automaatti, ja sen hyväksymä kieli.

Määritelmä 3.4 (**Deterministinen äärellinen automaatti**)**.** Seuraavaa viisikkoa

$$\mathcal{A} = (Q, \Sigma, \delta, q_0, \mathcal{F})$$

kutsutaan **deterministiseksi äärelliseksi automaatiksi**, kun se toteuttaa seuraavat ehdot. Tässä merkitään Q:lla äärellistä **tilojen** joukkoa ja Σ:lla äärellistä **syötesymbolien** joukkoa eli aakkostoa. Merkitään $\delta : Q \times \Sigma \to Q$ **siirtymäkuvausta**, joka kuvaa tilan toiselle tilalle. Lopuksi olkoot $q_0 \in Q$ automaatin **alkutilaa** ja $\mathcal{F} \subseteq Q$ joukkoa **lopputiloja**. Tarvittaessa merkitään determinististä äärellistä automaattia lyhenteellä DFA.

Deterministisillä äärellisillä automaatilla on siis yksi alkutila, josta luetaan syöte. Kaikki syötteet, joilla ei loppujen lopulta päädytä johonkin lopputilaan hylätään. Tarkastellaan seuraavaksi minkälaisia kieliä DFA:t tunnistaa, mutta ennen sitä pitää määritellä laajennettu siirtymäfunktio.

Määritelmä 3.5. Määritellään DFA:ille **laajennettu siirtymäfunktio** $\hat{\delta}$. Kuvaus $\hat{\delta}$ ottaa syötteeksi sanan w ja antaa tulosteeksi tilan, johon päästiin sanaa käsitellessä. Määritellään se rekursiolla sanan w pituuden suhteen.

1. Olkoon $\hat{\delta}(q, \epsilon) = q$. Ollaan tilassa q eikä olla luettu syötteitä. Tässä automaatti ei siirry muihin tiloihin.
2. Olkoon w sana, jolle $w = xa$, siis a on w:n viimeinen merkki ja x on sanan alkuosa. Nyt

$$\hat{\delta}(q, w) = \delta\left(\hat{\delta}(q, x), a\right).$$

   Oletetaan, että x:n lukemisen jälkeen DFA päätyy tilaan p, eli $\hat{\delta}(q, x) = p$. Nyt saadaan

$$\hat{\delta}(q, w) = \delta\left(\hat{\delta}(q, x), a\right) = \delta(p, a).$$

Määritelmä 3.6 (Deterministisen äärellisen automaatin kieli). Olkoon $A = (Q, \Sigma, \delta, q_0, \mathcal{F})$ DFA. Nyt $\mathcal{L}(A)$ on A:n kieli, jossa

$$\mathcal{L}(A) = \{w \mid \hat{\delta}(q_0, w) \in \mathcal{F}\}.$$

DFA hyväksyy siis aakkoston Σ kaikki sanat, jotka päätyvät siirtymien kautta alkutilasta johonkin lopputilaan. Esitetään seuraava lause ilman todistusta.

Lause 3.7 (DFA ja säännölliset kielet). *Kieli $\mathcal{M}$ on säännöllinen, jos ja vain jos on olemassa DFA $D = (Q, \Sigma, \delta, q_0, \mathcal{F})$, jolla $\mathcal{L}(D) = \mathcal{M}$.*

Esitetään seuraavaksi muutama yksinkertainen esimerkki DFA:ista. Käytetään tämän luvun esimerkeissä aakkostona joukkoa $\{0, 1\}$.

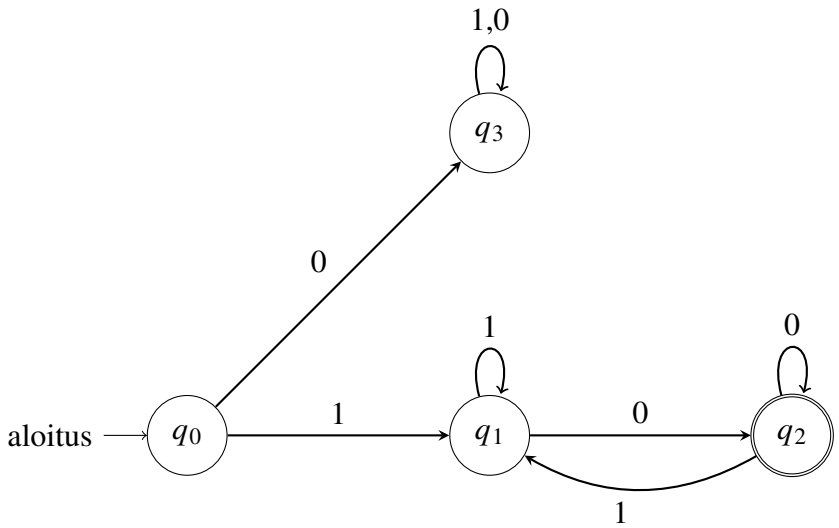
Esimerkki 3.8 (DFA, jonka sana alkaa ykköselllä ja loppuu nollaan). Voidaan kehittää esimerkiksi automaatin, joka hyväksyy kaikki sanat, jotka alkavat 1:llä ja loppuvat 0:aan. Tämän automaatin kieli olisi siis:

$$\mathcal{L} = \{10, 100, 110, \dots\}.$$

Tässä automaatissa on neljä tilaa, joita voidaan kuvailla seuraavasti.

- q_0: Tässä tilassa ei olla vielä luettu mitään syötteitä, mutta ainoa sallittu merkki on 1.
- q_1: Tässä tilassa ollaan luettu merkki 1 ja voidaan lukea molemmat merkit 1 ja 0. Jos luetaan merkki 0 siirrytään lopputilaan q_2. Jos taas luetaan merkki 1, pysytään tilassa q_1, niin kauan kunnes luetaan 0.
- q_2: Tässä tilassa ollaan luettu 1 ja viimeiseksi yksi 0. Voidaan vielä lukea merkit 0 ja 1. Jos luetaan 0 pysytään tilassa q_2 ja jos luemme 1 palaamme tilaan q_1.
- q_3: Tämä tila on virhetila, johon siirrytään, jos ensimmäinen merkki ei ole 1. Tilassa pysytään kunnes syöte hylätään.

Ohessa on siirtymäkaavio automaatista.



Selvästi q_0 on alkutila, sillä sen jälkeen otetaan ensimmäinen syöte. Tila q_2 on taas selvästi ainoa lopputila, koska se on ainoa tila johon pääsemiseltä edelletytään, että viimeisin luettu merkki oli 0. Kielen $\mathcal{L}$ DFA voidaan kirjoittaa auki:

$$\mathcal{A} = (\{q_0, q_1, q_2\}, \{0, 1\}, \delta, q_0, \{q_2\}) .$$

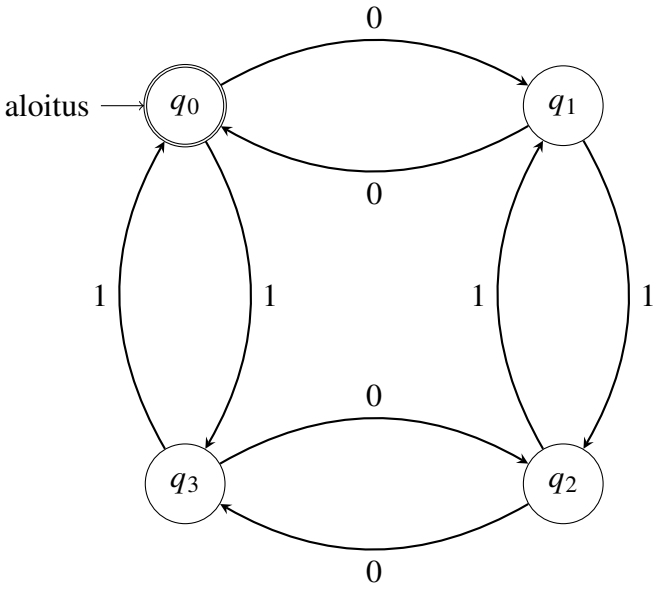
Esimerkki 3.9 (Parillinen määrä nollia ja ykkösiä). Tehdään esimerkiksi Hopcroftin kirjan [HU79] esimerkin 2.4. automaatti. Automaatti tunnistaa sanat, joissa on parillinen määrä nollia ja ykkösiä. Siis

$$\mathcal{L} = \{00, 11, 0101, 0011, 1001, 1100, \dots\}.$$

Tässä automaatissa on 4 tilaa, jotka voidaan tulkita seuraavasti:

- q_0: Automaatti on lukenut tällä hetkellä parillisen määrän nollia ja parillisen määrän ykkösiä.
- q_1: Automaatti on lukenut tällä hetkellä parittoman määrän nollia ja parillisen määrän ykkösiä.
- q_2: Automaatti on lukenut tällä hetkellä parittoman määrän nollia ja parittoman määrän ykkösiä.
- q_3: Automaatti on lukenut tällä hetkellä parillisen määrän nollia ja parittoman määrän ykkösiä.

Ohessa on esimerkin automaatin siirtymäkaavio.



Tässä q_0 on alkutila ja ainoa lopputila. Se on alkutila, sillä ennen kuin syötteitä aletaan lukemaan automaatti on saanut 0 ykköstä ja 0 nollaa. Nolla on tunnetusti parillinen luku. Tila q_0 on myös lopputila, koska se on ainoa tila, joka toteuttaa kielen $\mathcal{L}$. Voidaan kirjoittaa auki kielen $\mathcal{L}$ DFA:n. Se on

$$\mathcal{A} = (\{q_0, q_1, q_2, q_3\}, \{0, 1\}, \delta, q_0, \{q_0\}) .$$

Siirretään tarkastelemaan hivenen monimutkaisempaa automaattia.

Määritelmä 3.10 (**Epädeterministinen äärellinen automaatti**)**.** Seuraavaa viisikkoa

$$A = (Q, \Sigma, \delta, q_0, \mathcal{F})$$

kutsutaan **epädeterministiseksi äärelliseksi automaatiksi**. Merkitään Q:lla äärellistä joukkoa **tiloja** ja Σ:lla äärellistä joukkoa **syötesymboleja** eli aakkostoa. Kuvaus $\delta : Q \times \Sigma \to \mathcal{P}(Q)$ on **siirtymäkuvaus**, joka kuvaa tilan ja symbolin joukolle $\mathcal{F} \subseteq Q$ ja tila $q_0 \in Q$ on automaatin **alkutila** ja $\mathcal{F} \subseteq Q$ on joukko **lopputiloja**. Merkitään tarvittaessa epädeterminististä äärellistä automaattia lyhenteellä NFA.

On syytä huomata, että NFA:n ja DFA:n ero on minkälaisia tulosteita siirtymäfunktio δ antaa. DFA:n tapauksessa se palauttaa yksittäisen tilan ja NFA:n tapauksessa joukon tiloja.

Määritelmä 3.11. Seuraavaa viisikkoa

$$A = (Q, \Sigma, \delta, q_0, \mathcal{F})$$

kutsutaan **epsilon siirtymillä varustetuksi epädeterministiseksi äärelliseksi automaatiksi**. Merkitään Q:lla äärellistä joukkoa **tiloja** ja Σ:lla äärellistä joukkoa **syötesymboleja** eli aakkostoa. Kuvaus $\delta : Q \times (\Sigma \cup \{\epsilon\}) \to \mathcal{P}(Q)$ on **siirtymäkuvaus**, joka kuvaa tilan ja symbolin joukolle $\mathcal{F} \subseteq Q$ ja tila $q_0 \in Q$ on automaatin **alkutila** ja $\mathcal{F} \subseteq Q$ on joukko **lopputiloja**. Merkitään tarvittaessa epsilon siirtymillä varustettua epädeterminististä äärellistä automaattia lyhenteellä ϵNFA.

Epädeterminisellä äärellisellä automaatilla on myös yksi alkutila. Deterministisistä äärellisistä automaateista poiketen epädeterministisen äärellisen automaatin jokaisesta tilasta voidaan siirtyä 0, 1 tai usempaan tilaan. Samoin kuin deterministisellä äärellisellä automaatilla, jokainen syöte, joka ei lopulta päädy johonkin lopputilaan, hylätään. Epädeterministinen äärellinen

automaatti kykenee myös olemaan samaan aikaan useassa eri tilassa. Tämän ominaisuuden voi ajatella konkreettisemmin niin, että automaatti pystyy päättelemään siihen asti luetusta syötteestä, mitä seuraavaksi tapahtuu. Tämän ominaisuuden voi huomata esimerkistä 3.14. Nyt kysymykseksi herää minkälaisia kieliä NFA:t tunnistavat. Määritetään NFA:iden laajennettu siirtymäfunktio, kuten tehtiin DFA:den tapauksessa.

Määritelmä 3.12. Määritellään **laajennettu siirtymäfunktio** $\hat{\delta}$, joka ottaa syötteeksi sanan w ja antaa tulosteeksi tilojen joukon, joiden läpi NFA kulkee, kun se käsittelee sanan w rekursiolla sanan w pituuden suhteen.

1. Olkoon $\hat{\delta}(q, \epsilon) = \{q\}$ eli jos automaatti ei lue merkkejä syötteestä se on alkutilassa.
2. Oletetaan w:n olevan muotoa $w = xa$, jossa a on w:n viimeinen merkki ja x on w:n alkuosa. Olkoon $\delta(q, x) = \{p_1, p_2, \ldots, p_k\}$, jossa kaikki p_i ovat automaatin tiloja. Täten

$$\hat{\delta}(q, w) = \bigcup_{i=1}^{k} \delta(p_i, a).$$

Määritelmä 3.13 (Epädeterministisen äärellisen automaatin kieli). Olkoon $\mathcal{A} = (Q, \Sigma, \delta, q_0, \mathcal{F})$ NFA. Nyt $\mathcal{L}(\mathcal{A})$ on $\mathcal{A}$:n kieli, jossa

$$\mathcal{L}(\mathcal{A}) = \{w \in \Sigma^* \mid \delta(q_0, w) \cap \mathcal{F} \neq \varnothing\}.$$

NFA hyväksyy siis sanat $w \in \Sigma^*$, jossa laajennettu siirtymäfunktio sisältää vähintään yhden lopputilan.

Esitetään nyt myös NFA:ista kaksi yksinkertaista esimerkkiä.

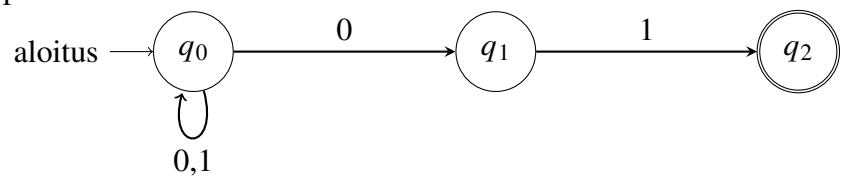
Esimerkki 3.14 (NFA, joka hyväksyy sanat, jos ja vain jos ne loppuvat merkkijonoon 01). Tehdään Hopcroftin kirjasta [HU79] esimerkki 2.6. Merkitään tätä NFA:ta $\mathcal{A}$:lla. $\mathcal{A}$ hyväksyy sanat, jos ja vain jos loppuvat pariin 01. Siis

$$\mathcal{L} = \{01, 001, 101, \ldots\}.$$

Siinä on 3 tilaa q_0, q_1 ja q_2. Tila q_0 on alkutila ja q_2 on ainoa lopputila. Tilassa q_0:ssa voidaan lukea molemmat syötteet 0 ja 1 ja pysyä vielä q_0:ssa. Tiloja voi ajatella seuraavasti:

- q_0: Alkutila, jossa $\mathcal{A}$ ei ole vielä lukenut yhteen syötettä tai ei ole vielä päätellyt, että viimeinen 01 on voinut alkaa.
- q_1: $\mathcal{A}$ on päätellyt viimeisen 01 jonon alkaneen ja lukee 1:sen ennen seuraavaan tilaan siirtymistä.
- q_2: $\mathcal{A}$ on huomannut, että w loppui 01 ja hyväksyy syötteen.

Ohessa on siirtymäkaavio esimerkin NFA:sta, joka hyväksyy syötteeksi kaikki sanat, jotka loppuvat 01:seen.



$\mathcal{L}$:n NFA $\mathcal{A}$ voidaan kirjoittaa auki:

$$\mathcal{A} = (\{q_0, q_1, q_2\}, \{0, 1\}, \delta, q_0, \{q_2\}).$$

Esimerkki 3.15 (**sanat joissa on lukujono 001**)**.** Tehdään nyt NFA $\mathcal{A}$, joka tunnistaa kaikki $\mathcal{L}$:n sanat, joissa esiintyy merkkijono 001. Siis $\mathcal{A}$:n kieli on

$$\mathcal{L} = \{001, 0001, 1001, \dots\}.$$

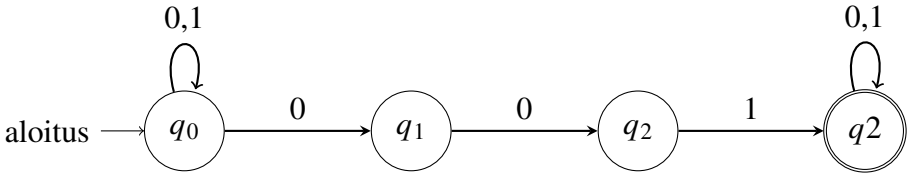
Automaatissa on 3 tilaa. Tila q_0 on alkutila, jossa voidaan lukea syötteet 0 ja 1. Tila q_2 on puolestaan lopputila, jossa pysytään, kunnes sana on loppunut. Tiloja voidaan ajatella seuraavasti:

- q_0: Alkutila, jossa pysytään niin kauan, että NFA päättelee 001 ketjun alkaneen.
- q_1: NFA on lukenut 0.
- q_2: NFA on lukenut 1. Sanasta löytyi 001 merkkijono, joten automaatti pysyy tässä tilassa, kunnes sana loppuu.

Kielen $\mathcal{L}$ NFA $\mathcal{A}$ automaatti voidaan kirjoittaa auki:

$$\mathcal{A} = \{\{q_0, q_1, q_2, q_3\}, \{0, 1\}, \delta, q_0, \{q_3\}\}.$$

Ohessa on esimerkin NFA:sta siirtymäkaavio.



DFA:t voi ajatella olevan NFA:ita, joilla jokaisella tilalla on vähintään yksi siirtymä, ja jokaisesta tilasta yhdellä syötteellä on vain yksi siirtymä. Mutta voidaanko aina rakentaa Σ:n mielivaltaisesta NFA:sta Σ:n DFA:n ?

Määritelmä 3.16. Olkoon NFA $\mathcal{N} = (Q_\mathcal{N}, \Sigma, \delta_\mathcal{N}, q_0, \mathcal{F}_\mathcal{N})$. $\mathcal{N}$:stä on mahdollista konstruoida DFA $\mathcal{D} = (Q_\mathcal{D}, \Sigma, \delta_\mathcal{D}, \{q_0\}, \mathcal{F}_\mathcal{D})$. Huomataan aluksi, että molempien automaattien aakkostot ovat samat. Lisäksi $\mathcal{D}$:n alkutila on joukko, joka sisältää vain $\mathcal{N}$:n alkutilan.

- $Q_\mathcal{D} = \mathcal{P}(Q_\mathcal{N})$.
- $\mathcal{F}_\mathcal{D}$ on osajoukkojen $\mathcal{A} \subseteq Q_\mathcal{N}$, joille pätee $\mathcal{S} \cap \mathcal{F}_\mathcal{N} \neq \emptyset$. Siis $\mathcal{F}_\mathcal{D}$ on $\mathcal{N}$:n tilojen joukko, joilla on vähintään yksi lopputila $\mathcal{N}$.ssä.
- Jokaisella $\mathcal{S} \subseteq Q_\mathcal{N}$ ja jokaisella $a \in \Sigma$

$$\delta_\mathcal{D}(\mathcal{S}, a) = \bigcup_{p \in S} \delta_\mathcal{N}(p, a).$$

Kutsutaan vastaisuudessa tätä konstruktiota N:n **determinististöimiseksi**. On hyvä muistaa, että, jos $Q_\mathcal{N}$:ssä on n alkiota, niin sen potenssijoukossa on 2^n alkiota. Joten NFA:sta konstruoitu DFA on huomattavasti suurempi kuin vastaava NFA. Kaikkiin tiloihin ei välttämättä DFA:lla pääsekään, jonka takia saavuttamattomat tilat voidaan ajatella hylättyinä tiloina.

On luonnollista ajatella, että jos NFA $\mathcal{N}$ tunnistaa kielen $\mathcal{A}$, niin siitä konstruoitu DFA $\mathcal{D}$ tunnistaa myös $\mathcal{A}$:n.

Lause 3.17. *Jos $\mathcal{D} = (Q_\mathcal{D}, \Sigma, \delta_\mathcal{D}, \{q_0\}, \mathcal{F}_\mathcal{D})$ on NFA $\mathcal{N} = (Q_\mathcal{N}, \Sigma, \delta_\mathcal{N}, q_0, \mathcal{F}_\mathcal{N})$:stä konstruoitu DFA, niin $\mathcal{L}(\mathcal{D}) = \mathcal{L}(\mathcal{N})$.*

Todistus. Todistetaan induktiolla sanan w pituuden $|w|$ suhteen, että

$$\hat{\delta}_{\mathcal{D}}(\{q_0\}, w) = \hat{\delta}_{\mathcal{N}}(q_0, w).$$

Tässä $\hat{\delta}_{\mathcal{N}}$ ja $\hat{\delta}_{\mathcal{D}}$ antaa molemmat tulosteeksi $Q_{\mathcal{N}}$:n osajoukkoja. Kuvaus $\hat{\delta}_{\mathcal{N}}$ tulkitsee sen $Q_{\mathcal{N}}$:n osajoukkona, kun taas $\hat{\delta}_{\mathcal{D}}$ tulkitsee sen $Q_{\mathcal{D}}$:n yhtenä tilana.
Perusaskel: Olkoon $w = \epsilon$ eli $|w| = |\epsilon| = 0$. Nyt $\hat{\delta}_{\mathcal{N}}$ ja $\hat{\delta}_{\mathcal{D}}$ määritelmien mukaan

$$\hat{\delta}_{\mathcal{D}}(\{q_0\}, \epsilon) = \{q_0\} = \hat{\delta}_{\mathcal{N}}(q_0, \epsilon).$$

Induktio-oletus: Olkoon w sana, jolla $|w| = n$. Tällöin

$$\hat{\delta}_{\mathcal{D}}(\{q_0\}, w) = \hat{\delta}_{\mathcal{N}}(q_0, w).$$

Induktioaskel: Olkoon w sana, jolla $|w| = n + 1$. Merkitään $w = xa$, jossa a on w:n viimeinen merkki. Induktio-oletuksesta seuraa, että $\hat{\delta}_{\mathcal{D}}(\{q_0\}, x) = \hat{\delta}_{\mathcal{N}}(q_0, x)$. Merkitään $\hat{\delta}_{\mathcal{D}}(\{q_0\}, x) = \hat{\delta}_{\mathcal{N}}(q_0, x) = \{p_1, p_2, \ldots, p_k\}$. Saadaan:

$$\hat{\delta}_{\mathcal{N}}(q_0, w) = \bigcup_{i=1}^{k} \delta_{\mathcal{N}}(p_i, a).$$

Osajoukon konstruktion perusteella saadaan, että

$$\delta_{\mathcal{D}}(\{p_1, p_2, \ldots, p_k\}, w) = \bigcup_{i=1}^{k} \delta_{\mathcal{N}}(p_i, a).$$

Edellisen ja $\hat{\delta}_{\mathcal{D}}(\{q_0\}, x) = \{p_1, p_2, \ldots, p_k\}$ mukaan

$$\hat{\delta}_{\mathcal{D}}(\{q_0\}, w) = \delta\left(\tilde{\delta}_{\mathcal{D}}(\{q_0\}, a), a\right) = \delta(\{p_1, p_2, \ldots, p_k\}, a) = \bigcup_{i=1}^{k} \delta_{\mathcal{N}}(p_i, a).$$

Nyt yhdistämällä saadaan, että $\hat{\delta}_{\mathcal{D}}(\{q_0, w\}) = \hat{\delta}_{\mathcal{N}}(\{q_0, w\})$. Lisäksi $\mathcal{D}$ ja $\mathcal{N}$ molemmat hyväksyvät sanan w, jos ja vain jos $\hat{\delta}_{\mathcal{D}}(\{q_0, w\})$ tai $\hat{\delta}_{\mathcal{N}}(\{q_0, w\})$ sisältävät $\mathcal{F}_{\mathcal{N}}$ tilan. Nyt siis $\mathcal{L}(\mathcal{N}) = \mathcal{L}(\mathcal{D})$. □

Nyt voidaan todentaa NFA:iden tunnistavan samat kielet DFA:iden kanssa.

Lause 3.18. *Jokin DFA tunnistaa kielen $\mathcal{L}$, jos ja vain jos jokin NFA tunnistaa kielen $\mathcal{L}$.*

Todistus. $\Leftarrow$ Tämä suunta todistettiin lauseessa 3.17.
$\Rightarrow$ Olkoon $\mathcal{D} = (Q, \Sigma, \delta_{\mathcal{D}}, q_0, F)$ DFA. Olkoon $\mathcal{N} = (Q, \Sigma, \delta_{\mathcal{N}}, q_0, F)$ tätä vastaava NFA, jossa δ_N määritellään säännöllä:

$$\text{Jos } \delta_{\mathcal{D}}(q, a) = p, \text{ niin } \delta_{\mathcal{N}}(q, a) = \{p\}.$$

Tässä $\hat{\delta}_{\mathcal{N}}$ ja $\hat{\delta}_{\mathcal{D}}$ antaa molemmat tulosteeksi $Q_{\mathcal{N}}$:n osajoukkoja. Laajennettu siirtymäfunktio $\hat{\delta}_{\mathcal{N}}$ tulkitsee sen $Q_{\mathcal{N}}$:n osajoukkona, kun taas $\hat{\delta}_{\mathcal{D}}$ tulkitsee sen $Q_{\mathcal{D}}$:n yhtenä tilana.
Todistetaan nyt induktiolla w:n pituuden suhteen, että jos $\hat{\delta}_{\mathcal{D}}(q_0, w) = p$, niin $\hat{\delta}_{\mathcal{N}}(q_0, w) = \{p\}$. jossa $p \in Q$ on $\mathcal{D}$:n tila.
Perusaskel: Olkoon $w = \epsilon$, jolloin $|w| = 0$. Nyt $\hat{\delta}_{\mathcal{D}}(q_0, w) = q_0$, joten $\hat{\delta}_{\mathcal{N}}(q_0, w) = \{q_0\}$.
Induktio-oletus: Olkoon $w = x$ sana, jolla $|w| = n$. Tällöin

$$\text{Jos } \hat{\delta}_{\mathcal{D}}(q_0, w) = p, \text{ niin } \hat{\delta}_{\mathcal{N}}(q_o, w) = \{p\}.$$

Induktiotodistus: Olkoon w sana, jolla $|w| = n + 1$. Merkitään $w = xa$, jossa a on sanan w viimeinen merkki. Induktio-oletuksen perusteella, jos $\hat{\delta}_{\mathcal{D}}(q_0, x) = p$, niin $\hat{\delta}_{\mathcal{N}}(q_0, x) = \{p\}$. Nyt $\hat{\delta}_{\mathcal{D}}$ määritelmän mukaan:

$$\hat{\delta}_{\mathcal{D}}(q_0, xa) = \delta_{\mathcal{D}}\left(\hat{\delta}_{\mathcal{D}}(\{q_0\}, x), a\right) = \delta_{\mathcal{D}}(p, a) = p'.$$

Nyt induktio-oletuksen mukaan $\hat{\delta}_{\mathcal{N}}(\{q_0\}, w) = \{p\}$.

$$\hat{\delta}_{\mathcal{N}}(q_0, xa) = \{q \in Q \mid \exists s \in p : q \in \delta_{\mathcal{N}}(s, a)\} = \{p'\}.$$

Nyt $\mathcal{D}$ hyväksyy w:n, jos ja vain jos, $\mathcal{N}$ hyväksyy w:n. Siis $\mathcal{L}(\mathcal{D}) = \mathcal{L}(\mathcal{N})$.

□

Nyt voidaan samalla tavalla kuin DFA:iden tapauksessa todistaa, että NFA:t hyväksyvät täsmälleen säännölliset kielet. Seuraava lause seuraa lauseista 3.7 ja 3.18.

Lause 3.19 (**NFA ja säännölliset kielet**). *Kieli $\mathcal{M}$ on säännöllinen, jos ja vain jos on olemassa NFA $\mathcal{N}$, jolla $\mathcal{L}(\mathcal{N}) = \mathcal{M}$.*

4 Symboliset äärelliset automaatit

Tämä luku perustuu Tammin ja Veanaksen artikkeliin [TV18]. Symboliset epädeterministiset äärelliset automaatit ovat yleistys epädeterministisistä äärellisistä automaateista, jotka kehitettiin käytännön sovelluksia varten tehtäviin, joissa vaadittiin isojen ja jopa äärettömän suurten aakkostojen käyttöä. Symbolisten automaattien aakkosten pohjana on Boolen algebra, jolla voi olla ääretön määrittelyjoukko. Viime aikoina symbolisia automaatteja on tutkittu symbolisten deterministen äärellisten automaattien minimoimisen ja symbolisten epädeterminisen äärellisten automaattien bisimulaatioiden näkökulmasta.

Tutustutaan aluksi Tammin ja Veanaksen artikkelissa [TV18] määriteltyyn efektiiviseen Boolen algebraan. Sitä käytetään symbolisten äärellististen automaattien pohjana. Määritellään se samalla tavalla, kuin se on määritelty heidän artikkelissaan.

Määritelmä 4.1 (**Efektiivinen boolen algebra**)**.** Olkoon $\mathcal{B} = (\Sigma, \Psi, [[\_]], \bot, \top, \vee, \wedge, \neg)$ kahdeksikko. Σ on perusjoukko, Ψ on joukko predikaatteja, jotka on suljettu Boolen algebran operaatioiden suhteen ja $\bot, \top \in \Psi$. $[[\_]] : \Psi \to 2^{\Sigma}$ on tulkintakuvaus, jolla $[[\bot]] = \varnothing$, $[[\top]] = \Sigma$, sekä kaikilla $\psi, \varphi \in \Psi$ pätee $[[\psi \wedge \varphi]] = [[\phi]] \cap [[\varphi]]$, $[[\psi \vee \varphi]] = [[\phi]] \cup [[\varphi]]$ ja $[[\neg\varphi]] = \Sigma \setminus [[\varphi]]$. Jos $[[\varphi]] \neq \varnothing$, φ on toteutuva. Oletetaan, että toteutuvuuden tarkistaminen on ratkeava. Tällöin rakennetta $\mathcal{B}$ kutsutaan **efektiiviseksi Boolen algebraksi**. Predikaatti φ on ψ **alipredikaatti**, jos $[[\varphi]] \subseteq [[\psi]]$. Σ:n alkiot ovat merkkejä ja **Σ:n sana** on jono $a_1 \ldots a_m$, jossa $a_j \in \Sigma, j = a, ..., m$. Jos $m = 0$, saadaan tyhjä sana, jota merkitään ϵ:lla. Merkitään kaikkien Σ:n sanojen joukkoa Σ^*. Oletetaan, että $\Sigma^n \cap \Sigma = \emptyset$, kun $n \geq 2$.

Kiinnitetään loppu tutkielman ajaksi jokin efektiivinen Boolen algebra $\mathcal{B}$. Ennen kuin voidaan määritellä symbolisten automaattien käsitteitä, on pohdittava millaisen kielen symboliset automaatit tunnistavat. Koska niiden aakkosto sisältää Boolen algebran predikaatteja, tavalliset säännölliset lauseet ja kielet eivät ole riittäviä. Tämän vuoksi määritellään symbolisia äärellisiä automaatteja varten symbolisten säännöllisen lauseen ja kielen käsitteet.

Määritelmä 4.2 (**Symbolinen säännöllinen lause ja kieli**)**.** Määritellään **symboliset säännölliset lauseet** rekursiivisesti. Olkoon $\mathcal{B} = (\Sigma, \Psi, [[\_]] \bot, \top, \vee\wedge, \neg)$ efektiivinen Boolen algebra. Tässä $[[\_]]$ on efektiivisen Boolen algebran määritelmässä 4.1 määritelty tulkintakuvaus.

- Vakiot ϵ ja $\varnothing$ on symbolisia säännöllisiä lauseita, jotka ilmaisevat kielet $\{\epsilon\}$ ja $\varnothing$. Siis $\mathcal{L}(\epsilon) = \{\epsilon\}$, $\mathcal{L}(\varnothing) = \varnothing$.
- Olkoon a merkki, jolloin a on symbolinen säännöllinen lause, joka ilmaisee kielen $\{a\}$. Siis $\mathcal{L}(a)$=$\{$a$\}$.
- Jokaiselle predikaatille $\varphi \in \Psi$, φ on symbolinen säännöllinen lause, joka ilmaisee kielen $\mathcal{L}(\varphi) = [[\varphi]]$.
- Jokaiselle symbolisille säännölliselle lauseelle X ja Y, lauseet $X + Y$, XY ja $\neg X$ ovat symbolisia säännöllisiä kieliä, jotka ilmaisevat kielet $\mathcal{L}(X + Y) = \mathcal{L}(X) \cup \mathcal{L}(Y)$, $\mathcal{L}(\mathcal{XY}) = \mathcal{L}(X)\,\mathcal{L}(Y)$ ja $\mathcal{L}(\neg X) = \Sigma^* \setminus \mathcal{L}(X)$.

Mikä tahansa kieli, jonka määrittää symbolinen säännöllinen lause, on **symbolinen säännöllinen kieli**.

Määritelmä 4.3 (**Symbolinen epädeterministinen äärellinen automaatti**)**.** Seuraavanlaista viisikkoa

$$\mathcal{N} = (\mathcal{B}, Q, \Delta, \mathcal{I}, \mathcal{F})$$

kutsutaan **symboliseksi epädeterministiseksi äärelliseksi automaatiksi** tai lyhennettynä s-NFA:ksi. Tässä $\mathcal{B} = (\Sigma, \Psi, [[\_]]\, \bot, \top, \vee\wedge, \neg)$ on määritelmän 4.1 mukainen efektiivinen Boolen algebra, jota käytämme aakkostona, Q on äärellinen joukko **tiloja**, $\Delta \subseteq Q \times \Psi \times Q$ on äärellinen joukko **siirtymiä**, $\mathcal{I} \subseteq Q$ äärellinen joukko **alkutiloja** ja $\mathcal{F} \subseteq Q$ on äärellinen joukko **lopputiloja**.

Samanlailla, kuin normaaleissa automaateissa sallimalla tyhjät siirtymät, saadaan määriteltyä s-ϵ-NFA.

Määritelmä 4.4. Seuraavanlaista viisikkoa

$$\mathcal{N} = (\mathcal{B}, Q, \Delta, \mathcal{I}, \mathcal{F})$$

kutsutaan **symboliseksi epädeterministiseksi äärelliseksi automaatiksi ϵ-siirtymillä** tai lyhennettynä s-ϵ-NFA:ksi. Tässä $\mathcal{B} = (\Sigma, \Psi, [[\_]]\, \bot, \top, \vee\wedge, \neg)$ on määritelmän 4.1 mukainen efektiivinen Boolen algebra, jota käytämme aakkostona, Q on äärellinen joukko **tiloja**, $\Delta \subseteq Q \times \Psi \times (Q \cup \{\epsilon\})$ on äärellinen joukko **siirtymiä**, $\mathcal{I} \subseteq Q$ äärellinen joukko **alkutiloja** ja $\mathcal{F} \subseteq Q$ on äärellinen joukko **lopputiloja**.

NFA:ista poiketen s-NFA:illa on huomattavasti suurempi aakkosto, joka saattaa olla jopa äärettömän suuri. Lisäksi niillä voi olla useita alkutiloja NFA:n yhdestä poiketen. Koska aakkosto sisältää efektiivisen Boolen algebran sen ilmaisuvoima on paljon suurempi.

Määritelmä 4.5 (**Vasen ja oikea kieli**)**.** s-NFA N:n tilan q **vasen kieli** $\mathcal{L}_{\mathcal{I},\mathrm{q}}(\mathcal{N})$ on joukko sanoja $w \in \Sigma^*$, joilla $w = \epsilon$ ja $q \in \mathcal{I}$ tai $w = a_1 \dots a_k$ ja on olemassa tilat $q_1, \dots, q_k \in Q$ siten, että $(q_{i-1}, \varphi_i, q_i) \in \Delta$ ja $a_i \in [[\varphi_i]]$, jolla $q_0 \in \mathcal{I}$ ja $q_k = q$.
s-NFA $\mathcal{N}$:n tilan q **oikea kieli**, jota merkitään $\mathcal{L}_q$ on joukko sanoja $w \in \Sigma^*$ siten, että joko $w = \epsilon$ ja $q \in \mathcal{F}$ tai $w = a_1, \dots, a_k$ ja on olemassa tilat $q_1, \dots, q_k \in Q$, joilla $(q_{i-1}, \varphi_i, q_i) \in \Delta$ ja $a_i \in [[\varphi_i]]$, jolla $q_0 = q$ ja $q_k \in F$.
Tila on **saavuttamaton**, jos sen vasen kieli on tyhjä ja **tyhjä**, jos sen oikea kieli on tyhjä. s-NFA on **tasapainoinen**, jos sillä ei ole tyhjiä tai saavuttamattomia tiloja. Automaatin $\mathcal{N}$:n **hyväksymä** eli **tunnistava kieli** on $\mathcal{L}(\mathcal{N}) = \bigcup_{q \in \mathcal{I}} \mathcal{L}_q(\mathcal{N})$. Jos kaksi s-NFA:tä hyväksyvät saman kielen ne ovat ekvivalentit.

Esitetään yksinkertainen esimerkki s-NFA:sta.

Esimerkki 4.6. Esitellään Saarikiven ja Veanaksen artikkelissa [SV17] esitelty esimerkki s-NFA:sta. Olkoon $\mathcal{N} = (\mathcal{B}, \{q_0, q_1\}, \Delta, \{q_0\}, \{q_0, q_1\})$. Tässä s-NFA

$$\mathcal{B} = \left(\mathbb{Z}_{10}, \{\varphi_{parillinen}, \varphi_{pariton}\}, [[\_]]\, \bot, \top, \vee\wedge, \neg\right),$$

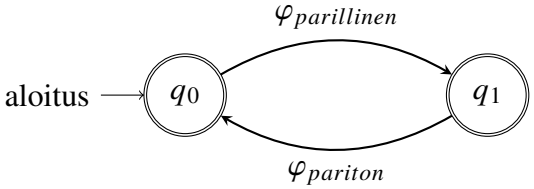
jossa $\left[\left[\varphi_{parillinen}\right]\right]$ on joukon $\{0, 2, 4, 6, 8\}$ karakteristinen kuvaus, toisin sanoen $\left[\left[\varphi_{parillinen}\right]\right](x) = 1$ kun $x \in \{0, 2, 4, 6, 8\}$, 0 muulloin. Vastaavasti kuten parillisessa tapauksessa $\left[\left[\varphi_{pariton}\right]\right]$ on joukon $\{1, 3, 5, 7, 9\}$ karakteristinen kuvaus siis, $\left[\left[\varphi_{pariton}\right]\right](x) = 1$, kun $x \in \{1, 3, 5, 7, 9\}$, 0 muulloin. Automaatti hyväksyy syötteeksi sanat, joissa on parillisessa merkin kohdassa on parillinen luku ja parittomassa on pariton luku. Tässä q_0 on sekä alkutila, että mahdollinen lopputila ja q_1 on mahdollinen lopputila. Siis, jos a_i on $\mathcal{N}$:n kielen $\mathcal{A}$ sanan w i merkki, jossa $i = 1, 2, 3, \dots$

- Tilassa q_0: Jos $i = 2n + 1$ ja $a_i \in \{1, 3, 5, 7, 9\}$, jossa $n, k \in \mathbb{N}$, syöte hyväksytään ja siirrytään tilaan q_1. Muulloin syöte hylätään.

- Tilassa q_1: Jos $i = 2k$ ja $a_i \in \{0, 2, 4, 6, 8\}$, jossa $n, k \in \mathbb{N}$, syöte hyväksytään ja siirrytään tilaan q_0, Muulloin syöte hylätään.

Tämä jatkuu kunnes sana w loppuu.

Ohessa on siirtymäkaavio esimerkin s-NFA:sta.



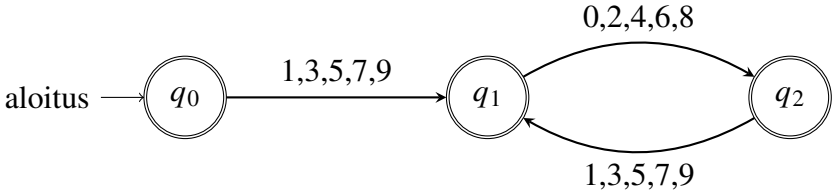
Tehdään esimerkin vuoksi sama toiminto NFA:lla. Tila q_0 on alkutila ja mahdollinen lopputila, jos saamme syötteeksi tyhjän sanan. Tilat q_1 ja q_2 ovat molemmat hyväksyviä tiloja, jotta voimme käsitellä sekä parillisen että parittoman pituisia sanoja. Tiloja voidaan ajatella seuraavasti:

- Alkutila q_0: Ei ole vielä luettu yhtään merkkiä. Jos luettava sana on tyhjä sana, syöte hyväksytään välittömästi. Jos $a_i \in \{1, 3, 5, 7, 9\}$, siirrytään tilaan q_2. Muulloin syöte hylätään.

- Tila q_1: On luettu parittoman merkin kohdalla pariton luku. Jos seuraavaksi luetaan jokin $a_{i+1} \in 0, 2, 4, 6, 8$, niin siirrytään tilaan q_2. Jos sana ei jatku, automaatti hyväksyy tässä kohtaa syötteen. Muulloin syöte hylätään.

- Tila q_2: On luettu parillisen merkin kohdalla pariton luku. Jos seuraavaksi luetaan jokin $a_{i+2} \in 1, 3, 5, 7, 9$, niin siirrytään tilaan q_1. Jos sana ei jatku, automaatti hyväksyy tässä kohtaa syötteen. Muulloin syöte hylätään.

Tämä jatkuu kunnes koko sana on luettu. Ohessa on siirtymäkaavio NFA:sta.



Määritellään seuraavaksi s-NFA:ita kieliä ja tiloja koskevia tärkeitä käsitteitä.

Määritelmä 4.7. symbolisen automaatin epädeterministisen automaatin $\mathcal{N} = (\mathcal{B}, Q, \Delta, \mathcal{F}, \mathcal{I})$ **käänteisautomaatti** on viisikko

$$\mathcal{N}^{\mathcal{R}} = \left(\mathcal{B}, Q, \Delta^{\mathcal{R}}, \mathcal{I}, \mathcal{F}\right),$$

jossa $(p, \varphi, q) \in \Delta^{\mathcal{R}}$, jos ja vain jos $(q, \varphi, p) \in \Delta$, kun $p, q \in Q$ ja $\varphi \in \Psi$. Jos $\mathcal{N}$ tunnistaa kielen $\mathcal{L}$, niin $\mathcal{N}^{\mathcal{R}}$ tunnistaa sen **käänteiskielen** $\mathcal{L}^{\mathcal{R}}$. Automaatti $\mathcal{N}$ on **normalisoitu predikaateille**, jos kaikilla $p, q \in Q$ on olemassa korkeintaan yksi predikaatti $\varphi \in \Psi$, jolla $(p, \varphi, q) \in \Delta$.

Minkä tahansa $\mathcal{N}$ saa normalisoitua s-NFA $\mathcal{N}^{\mathcal{N}}$:ksi, jossa kaikki erilliset siirtymät (p, φ_1, q) ja (p, φ_2, q) on korvattu yhdellä siirtymällä $(p, \varphi_1 \vee \varphi_2, q)$. $\mathcal{N}$ on **täydellinen**, jos kaikilla $p \in Q$ ja $a \in \Sigma$, on olemassa siirtymä $(p, \varphi, q) \in \Delta$, jolla $a \in [[\varphi]]$ ja $q \in Q$.

Määritelmä 4.8 (s-NFA:n morfismit). Olkoon $\mathcal{N}_1 = (\mathcal{B}, Q_1, \Delta_1, \mathcal{I}_1, \mathcal{F}_1)$ ja $\mathcal{N}_2 = (\mathcal{B}, Q_2, \Delta_2, \mathcal{I}_2, \mathcal{F}_2)$ s-NFA:ita. Kuvaus $\pi : Q_1 \to Q_2$ on **morfismi** $\mathcal{N}_1$:sestä $\mathcal{N}_2$:seen, jos ja vain jos $\pi(\mathcal{I}_1) \subseteq \mathcal{I}_2$, $\pi(\mathcal{F}_1) \subseteq \mathcal{F}_2$, ja kaikilla tiloilla $p, q \in Q_1$ ja $a \in \Sigma$ pätee, että jos $(p, \varphi_1, q) \in \Delta_1$, jollain φ_1, niin $a \in [[\varphi_1]]$. Tällöin on olemassa φ_2, jolla $(\pi(p), \varphi_2, \pi(q)) \in \Delta_2$ ja $a \in [[\varphi_2]]$.

Määritelmä 4.9 (Symbolinen deterministinen äärellinen automaatti). Seuraavaa viisikkoa

$$\mathcal{N} = (\mathcal{B}, Q, \Delta, q_0, \mathcal{F})$$

kutsutaan **symboliseksi deterministiseksi äärelliseksi automaatiksi** tai lyhennettynä s-NFA:ksi. Tässä $\mathcal{B} = (\Sigma, \Psi, [[\_]]\, \bot, \top, \vee\wedge, \neg)$ on efektiivinen Boolen algebra, jota käytetään aakkostona, Q on äärellinen joukko tiloja, $\Delta \subseteq Q \times \Psi \times Q$ on äärellinen joukko siirtymiä, $q_0 \in Q$ alkutila ja $\mathcal{F} \subseteq Q$ on äärellinen joukko lopputiloja. Lisäksi pitää päteä, että kaikille siirtymille (p, φ, q), $(p', \varphi', q') \in \Delta$, jos $p = p'$ ja $[[\varphi \wedge \varphi']] \neq \emptyset$, niin $q = q'$.

Määritelmä 4.10. s-DFA on minimaalinen, jos se sisältää pienimmän määrän tiloja kaikkien ekvivalenttien s-DFA:iden joukossa.

Oletetaan loppututkielman ajaksi, että s-DFA:ta ovat täydellisiä. Vastaavasti kuten tavallisten epädeterministisen äärellisen automaatin tapauksessa, voidaan todistaa, että symboliset epädeterministiset äärelliset automaatit hyväksyvät jokaisen symbolisen säännöllisen kielen. Todistetaan tämä ϵ-siirtymillä varustetuille symbolisille äärellisille automaateille.

Lause 4.11. *Automaatti s-ϵNFA hyväksyy jokaisen symbolisen säännöllisen kielen.*

Todistus. Jokainen s-ϵNFA on konstruoitavissa symbolisista säännöllisistä kielistä rakenteellisella induktiolla. s-ϵNFA:t vakioille ϵ ja $\varnothing$ ovat $\mathcal{N}_\epsilon = (\mathcal{B}, \{q\}\, \varnothing, q, \{q\})$ ja $\mathcal{N}_\varnothing = (\mathcal{B}, \varnothing, \varnothing, q, \varnothing)$ ja mille tahansa $\varphi \in \Psi$ saadaan s-ϵNFA $\mathcal{N}_\varphi = (\mathcal{B}, \{q_1.q_2\}, \{q_1, \varphi, q_2\}, \{q_1\}, \{q_2\})$. Olkoot nyt X ja Y symbolisiä säännöllisiä lauseita. Olkoon $\mathcal{N}_X = (\mathcal{B}, Q_X, \Delta_X, \mathcal{I}_X, \mathcal{F}_X)$ X:n s-ϵNFA ja $\mathcal{N}_Y = (\mathcal{B}, Q_Y, \Delta_Y, \mathcal{I}_Y, \mathcal{F}_Y)$ vastaavasti Y:n s-ϵNFA, joissa Q_X ja Q_Y ovat toisistaan erillisiä. Nyt lauseiden $X + Y$, XY ja $\neg X$ s-ϵNFA:t ovat:

$$\begin{aligned}\mathcal{N}_{X+Y} = (&\mathcal{B}, Q_X \cup Q_Y \cup \{q_1, q_2\},\\ &\Delta_X \cup \Delta_Y \cup (\{q_1\} \times \{\epsilon\} \times (\mathcal{I}_X \cup \mathcal{I}_Y)) \cup ((\mathcal{F}_X \cup \mathcal{F}_Y) \times \{\epsilon\} \times \{q_2\}), \{q_1\}, \{q_2\}),\end{aligned}$$

$$\mathcal{N}_{XY} = (\mathcal{B}, Q_X \cup Q_Y, \Delta_X \cup \Delta_Y \cup (\mathcal{F}_X \times \{\epsilon\} \times \mathcal{I}_Y)\, \mathcal{I}_X, \mathcal{F}_Y)$$

ja

$$\begin{aligned}\mathcal{N}_{\neg X} = (&\mathcal{B}, Q_X \cup \{q_1, q_2\}, \Delta_X \cup (\{q_1\} \times \{\epsilon\} \times (\mathcal{I}_X \cup \{q_2\}))\\ &\cup (\mathcal{F}_X \times \{\epsilon\} \times (\mathcal{I}_X \cup \{q_2\})), \{q_1\}, \{q_2\}), \text{ jossa } q_1, q_2 \notin Q_X \cup Q_Y\end{aligned}$$

□

Todistetaan, että samoin kuin normaaleilla automaateilla symboliset epädeterministiset äärelliset automaatit ovat tulkittavissa symbolisiksi epädeterministisiksi automaateiksi. Samoin kuin edellisessä luvussa tätä konstruktiota kutsutaan **determinisöinniksi**.

Lause 4.12. *Olkoon $\mathcal{N} = (\mathcal{B}, Q_\mathcal{N}, \Delta_\mathcal{N}, \mathcal{I}, \mathcal{F}_\mathcal{N})$ s-NFA. $\mathcal{N}$ on deterministisöitävissä s-DFA:ksi $\mathcal{D} = (\mathcal{B}, Q_\mathcal{D}, \Delta_\mathcal{D}, q_0, \mathcal{F}_\mathcal{D})$.*

Todistus. Todistetaan väite konstruoimalla $\mathcal{N}$:stä $\mathcal{D}$.

- Muodostetaan tilojen $q \in \mathcal{N}$ joukko $\mathcal{S}_s$, joiden välillä on siirtymä $(p, \varphi, q) \in \Delta_\mathcal{N}$ $\varphi \in \Psi$. Kaikilla $q \in \mathcal{S}_s$ on $\varphi_{s,\varphi} = \bigvee_{(p,\varphi,q)\in\Delta, p\in s} \varphi$ ja jokaiselle $s' \subseteq S_S$, olkoon $\varphi_{s,s'} = \left(\bigwedge_{q\in s'} \varphi_{s,q}\right) \wedge \left(\bigwedge_{q\in\mathcal{S}_{s,s'}} \neg\varphi_{s,q}\right)$. Jos $\varphi_{s,s'}$ on toteutuva, lisäämme s':n $Q_\mathcal{D}$:n ja siirtymän $\left(s, \varphi_{s,s'}, s'\right)$ $\Delta_\mathcal{D}$:n.
- $s_0 = \mathcal{I}$.
- $\mathcal{F}^\mathcal{D} = \{s \in Q^\mathcal{D} \mid s \cap \mathcal{F} \neq \varnothing\}$.

□

Merkitään s-NFA $\mathcal{N}$:stä deterministisöityä automaatti vastaisuudessa $\mathcal{N}^\mathcal{D}$:nä. Oletetaan nyt, että loppu tutkielmassa s-DFA:t on täydellisiä.

Määritelmä 4.13 (**Minimaalinen s-DFA**)**.** s-DFA on minimaalinen, jos sillä on pienin määrä tiloja kaikkien ekvivalenttien s-DFA:ien joukossa ja s-DFA on normalisoitu predikaattien joukossa.

Minimaalinen s-DFA on yksikäsitteinen tilojen uudelleen nimeämiseen ja predikaattien ekvivalenssiin saakka. Minimaalisen s-DFA:n erillisten tilojen kielet eroavat toisistaan. Todistetaan nyt tutkielman seuraava merkittävä lause.

Lause 4.14 (**Brzozowskin lause symbolisille automaateille**)**.** *Jos s-NFA $\mathcal{N}$:llä ei ole tyhjiä tiloja ja $\mathcal{N}^\mathcal{R}$ on s-DFA, niin $\mathcal{N}^\mathcal{D}$ on minimaalinen.*

Todistus. Olkoon $\mathcal{N} = (\mathcal{B}, Q, \Delta, \mathcal{I}, \mathcal{F})$ s-NFA, joilla ei ole tyhjiä tiloja. Sen käänteisautomaatti $\mathcal{N}^\mathcal{R} = \left(\mathcal{B}, Q, \Delta^\mathcal{R}, \mathcal{F}, \mathcal{I}\right)$ on s-DFA. Koska $\mathcal{N}^\mathcal{R}$ on s-DFA, niin $\mathcal{F}$ on yksikkö. Jos $|Q| = 1$, niin $\mathcal{N}$ ja $\mathcal{N}^\mathcal{R}$ ovat samat automaatit. Deterministisöity $\mathcal{N}^\mathcal{D}$ on täydellinen, normalisoitu ja sillä on 1 tai 2 tilaa. $\mathcal{N}^\mathcal{D}$ on selvästi minimaalinen, jos sillä on yksi tila. Jos $\mathcal{N}^\mathcal{D}$:llä on kaksi tilaa, niin toinen tiloista on epätyhjä alkutila, ja toinen on tyhjä tila, joten nämä kielet ovat tyhjät, joka implikoi, että $\mathcal{N}^\mathcal{D}$ on minimaalinen.
Jos $|Q| \geq 2$. Olkoon $q, q' \in Q$, jossa $q \neq q'$. Näytetään, että $\mathcal{L}_q(\mathcal{N}) \cap \mathcal{L}_{q'}(N) = \varnothing$. Olkoon $w \in \Sigma^*$ sana siten että $w \in \mathcal{L}_q(\mathcal{N})$ ja $w \in \mathcal{L}_{q'}(\mathcal{N})$. Nyt siis q ja q' pitää olla lopputiloja, mutta $\mathcal{N}$:llä on vain yksi lopputila. Joka on on siis ristiriita. Jos $w = a_1 \dots a_k$, jossa $k \geq 1$, on olemassa tiloja $q_{i-1}, q'_{i-1}, q_i \in Q$, joilla $q_{i-1} \neq q'_{i-1}$ ja siirtymät $(q_{i-1}, \varphi, q), \left(q'_{i-1}, \varphi', q\right) \in \Delta$, joilla $a_i \in [[\varphi]]$ ja $a_i \in [[\varphi']]$. Siten $\varphi \wedge \varphi'$ on toteutuva, joka implikoi, että $\mathcal{N}^\mathcal{R}$ ei ole deterministinen, joka on ristiriita.
Olkoon nyt $s_1, s_2 \in \mathcal{N}^\mathcal{D}$ erillisiä. Koska molemmat $s_1, s_2 \subseteq Q$, niin on olemassa sellainen $q \in Q$, että joko $q \in s_1$ ja $q \notin s_2$ tai $q \notin s_1$ ja $q \in s_2$. Koska $\mathcal{L}_{s_1}\left(\mathcal{N}^\mathcal{D}\right) = \bigcup_{q\in s_1} \mathcal{L}_q(\mathcal{N})$ ja $\mathcal{L}_{s_2}\left(\mathcal{N}^\mathcal{D}\right) = \bigcup_{q\in s_2} \mathcal{L}_q(\mathcal{N})$, todistettiin että $\mathcal{L}_q(\mathcal{N}) \cap \mathcal{L}'_q(\mathcal{N}) = \varnothing$ kaikilla erillisillä $q, q' \in Q$ ja oletuksen, että kaikilla $q \in Q$ pätee $\mathcal{L}_q(\mathcal{N}) \neq \varnothing$. Täten nyt määritelmän 4.13 mukaan $\mathcal{N}^\mathcal{D}$ on minimaalinen. □

Määritellään nyt s-NFA:ille mintermien käsite.

Määritelmä 4.15 (**s-NFA:n mintermit**)**.** Olkoon $\mathcal{N}$ s-NFA, s-NFA $\mathcal{N}^\mathcal{N}$ predikaatti normalisoitu versio $\mathcal{N}$:stä ja $\varphi_1 \dots \varphi_k$ $\mathcal{N}^\mathcal{N}$ predikaatit. Mikä tahansa toteutuva $\left(\bigwedge_{i\in S} \varphi_i\right) \wedge \left(\bigwedge_{i\in\bar{S}} \neg\varphi_i\right)$, jolle $S \subseteq \{1, \dots, k\}$ ja $\bar{S} = \{1, \dots, k\} \setminus S$ on $\mathcal{N}$ **mintermi**. N ja N^N mintermit ovat selvästi samat. $\mathcal{N}$ mintermien avulla saamme osituksen Σ:n.

Mintermejä voi ajatella siis predikaattien leikkauksina. Osoitetaan seuraavaksi, että s-NFA:n mintermit on s-DFA:n mintermien alipredikaatti.

Lause 4.16. *Kielen $\mathcal{L}$ s-NFA:n mintermi on $\mathcal{L}$ minimaalisen s-DFA mintermin alipredikaatti.*

Todistus. Olkoon ensin $\mathcal{N}$ s-NFA, jonka kaikki tilat on saavutettavia ja $\mathcal{N}^{\mathcal{N}}$ sen normalisoitu versio. Näiden automaattien determinoidut versiot $\mathcal{N}^{\mathcal{D}}$ ja $\mathcal{N}^{\mathcal{ND}}$ ovat determinointi prosessin takia sama automaatti. Olkoon nyt $s \subseteq Q$ $\mathcal{N}^{\mathcal{D}}$:n tila ja $\varphi_1 \dots \varphi_k$ $\mathcal{N}^{\mathcal{N}}$:n predikaatteja ja $\psi_1 \dots \psi_2$ ovat $\mathcal{N}^{\mathcal{ND}}$:n predikaatteja. Automaatin $\mathcal{N}^{\mathcal{ND}}$:n konstruktion perusteella huomataan, että kaikki ψ_j:t ovat muotoa $(\bigwedge_{i\in S} \varphi_i) \wedge \left(\bigwedge_{i\in \bar{S}} \neg\varphi_i\right)$, jossa $S \subseteq \{1, \dots, k\}$ ja $\bar{S} = \{1, \dots, k\} \setminus S$, joten mikä tahansa predikaatti $(\bigwedge_{i\in S} \varphi_i) \wedge \left(\bigwedge_{i\in \bar{S}} \neg\varphi_i\right)$ on jonkin ψ_k:n alipredikaatti. $\mathcal{N}^{\mathcal{ND}}$ on deterministinen, joten $\psi_h \wedge \psi_j$ ei ole toteutuva, kun $h \neq j$. Täten $(\bigwedge_{i\in S} \varphi_i) \wedge \left(\bigwedge_{i\in \bar{S}} \neg\varphi_i\right)$ on $\psi_j \wedge \left(\bigwedge_{h\in\{1,\dots,l\}, h\neq j} \neg\psi_h\right)$ alipredikaatti. Koska jokainen $\mathcal{N}^{\mathcal{N}}$:n mintermi on konjunktio muotoa $(\bigwedge_{i\in S} \varphi_i) \wedge \left(\bigwedge_{i\in \bar{S}} \neg\varphi_i\right)$ olevista predikaateista ja jokainen $\mathcal{N}^{\mathcal{ND}}$:n mintermi on muotoa $\psi_j \wedge \left(\bigwedge_{h\in\{1,\dots,l\}, h\neq j} \neg\psi_h\right)$, voidaan todeta, että $\mathcal{N}^{\mathcal{N}}$:n jokainen mintermi on jonkin $\mathcal{N}^{\mathcal{ND}}$ alipredikaatti. Koska $\mathcal{N}$:n ja $\mathcal{N}^{\mathcal{N}}$:n mintermit ovat samat, sama pätee myös $\mathcal{N}^{\mathcal{D}}$ ja $\mathcal{N}^{\mathcal{ND}}$:n mintermeille. Joten samme, että jokainen $\mathcal{N}$:n mintermi on jonkin $\mathcal{N}^{\mathcal{D}}$:n mintermin alipredikaatti.
Koska jos s-DFA:lla on vain saavutettavia tiloja, niin sen jokainen predikaatti on minimaalisen s-DFA:n predikaatin alipredikaatti. Tästä seuraa, että $\mathcal{N}^{\mathcal{D}}$:n mintermi on on $\mathcal{L}$:n minimallisen s-DFA:n alipredikaatti. Jolloin mikä tahansa $\mathcal{N}$: n mintermi on L:n minimaalisen s-DFA:n mintermin alipredikaatti.
Lopuksi tarkastellaan tilannetta, jossa s-NFA:lla on saavuttamattomia tiloja. Edellä näytettiin, että $\mathcal{N}$ saavutettavan osan jokainen mintermi on on minimaalisen s-DFA:n mintermin alipredikaatti. Selvästi jokainen $\mathcal{N}$:n mintermi on $\mathcal{N}$:n saavutettavan osan jonkin mintermin alipredikaatti. Siis $\mathcal{N}$:n mikä tahansa mintermi on $\mathcal{L}$:n minimaalisen s-DFA:n mintermin alipredikaatti. □

Lause 4.17. *Olkoon $\mathcal{N}$ s-NFA ja $\mathcal{D}$ $\mathcal{L}$:n minimaalinen s-DFA. Mikä tahansa $\mathcal{D}$:n mintermi on $\mathcal{N}$:n mintermien disjunktio.*

Todistus. $\mathcal{N}$ mintermit osittavat Σ:n. Luonnollisesti samoin tekee $\mathcal{D}$:n mintermit. Nyt määritelmän 4.15 mukaan $\mathcal{N}$: mintermit ovat $\mathcal{D}$ mintermien alipredikaatti, josta seuraa, että mikä tahansa $\mathcal{D}$:n mintermi on $\mathcal{N}$:n mintermien disjunktio. □

Lause 4.18. *$\mathcal{L}$ ja $\mathcal{L}^{\mathcal{R}}$ mintermit ovat samat.*

Todistus. Olkoon $\mathcal{D}$ symbolisen säännöllisen kielen$\mathcal{L}$ s-DFA. Lauseen 4.14 mukaan kääntämällä $\mathcal{D}$ ja deterministisöimalla tulokseksi saadaan s-NFA $\mathcal{D}^{\mathcal{R}}$, $\mathcal{D}^{\mathcal{RD}}$:ksi saadaan $\mathcal{L}^{\mathcal{R}}$:n minimaalisen s-DFA:n. Siirtymäpredikaatit eivät muutu kun automaatti muokataan käänteisautomatiksi, joten $\mathcal{D}^{\mathcal{R}}$ siirtymä predikaattit ovat samat kuin $\mathcal{D}$:n siirtymäpredikaatit. Vastaavasti $\mathcal{D}^{\mathcal{R}}$:n mintermit ovat samat $\mathcal{D}$:n mintermit. Käyttämällä Boolen operaatioita $\mathcal{D}^{\mathcal{R}}$:ään, saamme tulokseksi $\mathcal{D}^{\mathcal{R}}$:n mintermien disjunktiot, jotka ovat $\mathcal{D}^{\mathcal{RD}}$:n predikaatit. Täten, $\mathcal{D}^{\mathcal{RD}}$:n mintermit ovat $\mathcal{D}$:n mintermejä.

Vastaavalla päättelyllä saadaan, että $\mathcal{D}$:n mintermit ovat $\mathcal{D}^{\mathcal{RD}}$mintermejä. Olkoon $\mathcal{D}^{\mathcal{RD}}$ säännöllisen kielen $\mathcal{L}^{\mathcal{R}}$ s-DFA. Kääntämällä $\mathcal{D}^{\mathcal{RD}} : n$, saadaan $\mathcal{D}^{\mathcal{D}}$, sillä, jos $(p, \varphi, q) \in \Delta^{\mathcal{RRD}} \iff (q, \varphi, p) \in \Delta^{\mathcal{RD}} \iff (p, \varphi, q) \in \Delta^{\mathcal{D}}$. Nyt siis lauseen 4.14 mukaan $\mathcal{D}^{\mathcal{RRD}} = \mathcal{D}^{\mathcal{D}}$ on $\mathcal{L}$:n minimaalinen s-DFA. Siirtymäpredikaatit eivät muutu automaatin kääntämisestä, joten $\mathcal{D}^{\mathcal{D}}$:n siirtymäpredikaatit ovat samat kuin $\mathcal{D}^{\mathcal{RD}}$:n siirtymäpredikaatit. Vastaavasti $\mathcal{D}^{\mathcal{D}}$:n mintermit ovat samat kuin $\mathcal{D}^{\mathcal{RD}}$:n mintermit. $\mathcal{D}^{\mathcal{D}}$:n predikaatit voidaan muodostaa käyttämällä Boolen operaatioita $\mathcal{D}$:n predikaatteihin. Tuloksena saamamme predikaatit ovat $\mathcal{D}$:n mintermien disjunktioita. Joten $\mathcal{D}$:n mintermit ovat $\mathcal{D}^{\mathcal{RD}}$:n mintermejä. Joten, saamme, että $\mathcal{D}$:n ja $\mathcal{D}^{\mathcal{RD}}$:n mintermit ovat samat eli $\mathcal{L}$ ja $\mathcal{L}^{\mathcal{R}}$ ovat samoja. □

Vaikka symbolisen säännöllisen kielen voi määritellä äärettömän suurelle aakkostolle, kuitenkin minkä tahansa s-NFA:n mintermien joukko on äärellinen, koska s-NFA:lla on äärellinen joukko siirtymäkuvauksia. Esitellään seuraavaksi symbolisen säännnöllisen kielen ositukset, vasen kongruenssi ja atomit.

Määritelmä 4.19 (**osamäärä, alkuosamäärä, loppuosamäärä**)**.** Symbolisen säännöllisen kielen **osamäärä** sanalle $w \in \Sigma^*$ on kieli $w^{-1}\mathcal{L} = \{x \in \Sigma^* \mid wx \in \mathcal{L}\}$. On olemassa yksi **alkuosamäärä** $\epsilon^{-1}\mathcal{L} = \mathcal{L}$. Osamäärä on **loppuosamäärä**, jos $\epsilon \subseteq a^{-1}\mathcal{L}$, jossa $a \in \Sigma^*$.

Kielen $\mathcal{L}$:n ositukset ovat $\mathcal{L}$:n minimaalisen s-DFA:n tilojen kielet.

Määritelmä 4.20 (**vasen kongruenssi**)**.** Olkoon $x, y \in \Sigma^*$. Symbolisen säännöllisen kielen $\mathcal{L}$ **vasen kongruenssi** täyttää seuraavat ehdot: $x \equiv_{\mathcal{L}} y$, jos kaikilla $a \in \Sigma^*$, $ax \in \mathcal{L}$ jos ja vain jos $ay \in \mathcal{L}$.

Määritelmä 4.21 (**Symbolisen säännöllisen kielen atomit**)**.** Symbolisen säännöllisen kielen $\mathcal{L}$ atomi on $\mathcal{L}$ vasen kongruenssiluokka. Siis atomi on sanojen joukko, jotka kuuluvat täsmälleen samoihin osamääriin. Kielen $\mathcal{L}$ atomi on mikä tahansa epätyhjä kieli, joka on muotoa $\tilde{\mathcal{K}}_1 \cap \cdots \cap \tilde{\mathcal{K}}_n$, jossa $\tilde{\mathcal{K}}_i$ on joko $\mathcal{K}_i$ tai $\bar{\mathcal{K}}_i$, jossa $\bar{\mathcal{K}}_i$ on $\Sigma^* \setminus K_i$ ja $\mathcal{K}_1, \ldots, \mathcal{K}_n$ ovat kielen $\mathcal{L}$ ositukset. Atomi $\mathcal{A}$ on **alkuatomi**, jos $\mathcal{L} \in \mathcal{A}$ ja **loppuatomi**, jos $\epsilon \subset \mathcal{A}$. On olemassa täsmälleen yksi alkuatomi $\hat{\mathcal{K}}_1 \wedge \cdots \wedge \hat{\mathcal{K}}_n$, jossa $\hat{\mathcal{K}}_i = \mathcal{K}_i$, jos $\epsilon \in \mathcal{K}_i$, ja $\hat{\mathcal{K}}_i = \bar{\mathcal{K}}_i$ muulloin.

Selvästi jokainen ositus on atomeiden disjunktio. Määritellään sitten s-NFA:n tilan kielen yhtälö.

Määritelmä 4.22 (**Tilan kielen yhtälö**)**.** Olkoon $\mathcal{N} = (\mathcal{B}, Q, \Delta, \mathcal{I}, \mathcal{F})$ s-NFA, jonka tilojen joukko on $Q = \{q_1, \ldots, q_n\}$. Tilan q_i kielen yhtälö on

$$\mathcal{L}_i = \bigvee_{(q_i, \varphi, q_j) \in \Delta} [[\varphi]]\, \mathcal{L}_j \cup \mathcal{L}_i^{\epsilon} \quad i = 1, \ldots, n, \tag{4.1}$$

jossa $\mathcal{L}_i^{\epsilon} = \{\epsilon\}$, jos $q_i \in \mathcal{F}$ ja muulloin $\mathcal{L}_i^{\epsilon} = \varnothing$

Muokkaamalla tilan kielen yhtälöä saadaan kielen $\mathcal{L}$ minimaalinen s-DFA. Oleellisesti, koska ositukset ovat minimaalisten s-DFA:iden kieliä ja atomit ovat osamäärien leikkauksia tai osamäärien komplementtien leikkauksia, voidaan ilmaista atomit yhtälön oikean puolen leikkauksina tai niiden komplementteina. Olkoon siis kielen $\mathcal{L}$ minimaalinen s-DFA $\mathcal{D} = (\mathcal{B}, Q, \Delta, \mathcal{I}, \mathcal{F})$, jonka tilojen joukko on $Q = \{q_1, \ldots, q_n\}$. Koska $\mathcal{D}$:n minkä tahansa tilan q_i kieli on $\mathcal{K}_i$ ositus, niin yhtälöt

$$\mathcal{K} = \bigvee_{(q_i, \varphi_i, q_j) \in \Delta} \left[\left[\varphi_{i_j}\right]\right] \mathcal{K}_j \cup \mathcal{K}_i^{\epsilon}, \quad i = 1, \ldots, n$$

pätevät, jossa $\mathcal{K}_i^{\epsilon} = \{\epsilon\}$, jos $\epsilon \in \mathcal{K}_i$, ja $\mathcal{K}_i^{\epsilon} = \varnothing$ muulloin. Näitä muokkaamalla saadaan atomeille seuraava määritrlmä.

Määritelmä 4.23 (**Atomin kielen yhtälö**)**.** Olkoon $\mathcal{D} = (\mathcal{B}, Q, \Delta, \mathcal{I}, \mathcal{F})$ kielen $\mathcal{L}$ minimaalinen s-DFA. Atomin $\mathcal{A}_h$ kielen yhtälö on

$$\mathcal{A}_h = \left[\left[\varphi_{h_1}\right]\right] \mathcal{A}_{h_1} \cup \cdots \cup \left[\left[\varphi_{h_k}\right]\right] \mathcal{A}_{h_k} \cup \mathcal{A}_h^{\epsilon}, \tag{4.2}$$

jossa $\varphi_{h_1}, \ldots, \varphi_{h_k}$ ovat $\mathcal{L}$:n predikaatteja, $\mathcal{A}_{h_1}, \ldots, \mathcal{A}_{h_k}$on kielen $\mathcal{L}$ atomeja ja $\mathcal{A}_h^{\epsilon} = \{\epsilon\}$, jos $\epsilon \in \mathcal{A}_h$ ja muulloin $\mathcal{A}_h^{\epsilon} = \varnothing$.

Todetaan vielä, että selvästi $\varphi_{h_1}, \ldots, h_{h_k}$ ovat kielen $\mathcal{L}$ mintermien disjunktioita. Nyt voidaan esittää seuraavat väitteet.

Lause 4.24. *Olkoon φ kielen $\mathcal{L}$ mintermi. Jos $a\mathcal{A}_j \subseteq \mathcal{A}_i$ pätee, jollain $a \in [[\varphi]]$ ja $\mathcal{L}$:n atomeille $\mathcal{A}_i, \mathcal{A}_j$, niin $[[\varphi]]\,\mathcal{A}_j \subseteq \mathcal{A}_i$.*

Todistetaan tästä yleisempi versio.

Lause 4.25. *Olkoon φ kielen $\mathcal{L}$ mintermi. Jos $a\mathcal{L}_j \subseteq \mathcal{L}_i$ pätee jollakin $a \in [[\varphi]]$ ja $\mathcal{L}$:n atomien konjunktioilla $\mathcal{L}_i, \mathcal{L}_j$, niin $[[\varphi]]\,\mathcal{L}_j \subseteq \mathcal{L}_i$.*

Todistus. Oletetaan $a\mathcal{L}_j \subseteq \mathcal{L}_i$ pätee jollain $a \in [[\varphi]]$ sekä $\mathcal{L}$:n atomien disjunktiona luoduilla kielillä $\mathcal{L}_i, \mathcal{L}_j$. Nyt kaikilla $\mathcal{A}_h \subseteq \mathcal{L}_j$ on olemassa atomi $\mathcal{A}_g \subseteq \mathcal{L}_i$, jolle $a\mathcal{A}_h \subseteq \mathcal{A}_g$. Lauseen 4.24 mukaan kaikilla $\mathcal{A}_h \subseteq \mathcal{L}_j$, on olemassa atomi $\mathcal{A}_g \subseteq L_i$, jolla pätee$[[\varphi]]\,\mathcal{A}_h \subseteq \mathcal{A}_g$. Täten $[[\varphi]]\,\mathcal{L}_j \subseteq \mathcal{L}_i$. □

5 Yleistetty Brzozowskin lause

Tämä luku perustuu Tammin ja Veanaksen artikkeliin [TV18]. Jatketaan symbolisen kielen $\mathcal{L}$ atomien tarkastelua ja määritellään vielä muutama erityyppinen symbolisen äärellinen automaatti. Esitellään ja todistetaan yleistetty Brzozowskin lause symbolisille automaateille, joka on symbolisille äärellisille automaateille muokattu versio Brzozowskin ja Tammin artikkelissa [BT14] esitellystä ja todistetusta väitteestä normaaleille determinisöidyille NFA:ille. Brzozowski ja Tamm osoittivat, että kaikille NFA $\mathcal{N}$:lle pätee, että $\mathcal{N}^{\mathcal{D}}$ on minimaalinen, jos ja vain jos $\mathcal{N}^{\mathcal{R}}$ on atominen. Tätä varten tarvitaan kuitenkin muun muassa atomisen automaatin määritelmä. Määritellään aivan aluksi peitteen ja atomipeitteen käsitteet.

Määritelmä 5.1 (**Peite ja atominen peite**)**.** Olkoon $\mathcal{L}$ symbolinen säännöllinen kieli. Joukko kieliä $\{\mathcal{L}_1, \ldots, \mathcal{L}_k\}$ on **peite**, jos $\mathcal{L}$:n jokainen ositus $\mathcal{K}_j$ on $\mathcal{L}_i$:den leikkaus. Jos jokainen $\mathcal{L}_i$ on atomien yhdiste, niin peite on **atominen peite**.

Voidaan määritellä nyt atomipeitteen generoiman automaatin, jonka alkutilojen joukko on atomipeite.

Määritelmä 5.2 (**Atomipeitteen generoima s-NFA**)**.** Kielen $\mathcal{L}$ **atomipeitteen** $\{\mathcal{L}_1, \ldots, \mathcal{L}_k\}$ **generoima s-NFA** on

$$\mathcal{G} = (\mathcal{B}, Q, \Delta, \mathcal{I}, \mathcal{F}),$$

jossa $\mathcal{B}$ on efektiivinen Boolen algebra, Q äärellinen joukko tiloja, Δ äärellinen joukko siirtymiä, $\mathcal{I}$ äärellinen joukkko alkutiloja ja $\mathcal{F}$on äärellinen joukko lopputiloja. Lisäksi seuraavat ehdot pätevät: $Q = \{q_1, \ldots, q_2\}$, $I = \{q_i \mid \mathcal{L}_i \subseteq \mathcal{L}\}$, $\mathcal{F} = \{q_i \mid \epsilon \in \mathcal{L}_i\}$ ja $(q_i, \varphi, q_j) \in \Delta$, jos ja vain jos, $[[\varphi]]\, \mathcal{L}_j \subseteq \mathcal{L}_i$ kaikilla $q_i, q_j \in Q$ ja $\mathcal{L}$:n mintermillä φ.

Seuraavat lauseet pätee atomipeitteen generoimalle s-NFA:lle.

Lause 5.3. *Seuraavat ominaisuudet pätevöt s-NFA $\mathcal{G}$:lle:*

1. $\mathcal{L}_{q_i}(\mathcal{G}) \subseteq \mathcal{L}_i$ *kaikilla* $q_i \in Q$.
2. $\mathcal{L}(\mathcal{G}) \subseteq \mathcal{L}$.

Todistus. **1.** Olkoon $\mathcal{G}$ atomipeitteen generoima s-NFA. Tarkastellaan $\mathcal{G}$:n tilaa q_i. Olkoon sana $w \in \mathcal{L}_{q_i}$. Jos $w = \epsilon$, niin $q_i \in \mathcal{F}$. Siten määritelmän 5.2 perusteella $\epsilon \in \mathcal{L}_i$. Jos $w \in \Sigma$, niin on olemassa q_j, jolla $q_j \in \mathcal{F}$. Huomataan, että lause 4.25 pätee määritelmän 5.2 mukaan jokaisella kieliparille $\mathcal{L}_i, \mathcal{L}_j$ pätee, että aina kun on voimassa inkluusio $\mathcal{L}_j \subseteq w^{-1}\mathcal{L}_i$, jossa $w \in \Sigma$, niin on olemassa myös $\mathcal{G}$:n siirtymä (q_i, φ, q_j) siten, että $w \in [[\varphi]]$. Siis $\mathcal{L}_j \subseteq w^{-1}\mathcal{L}_i$ ja $\epsilon \in \mathcal{L}_i$.

2. Koska $\mathcal{L}(\mathcal{G})$ on $\mathcal{G}$:n alkutilojen oikeiden kielien disjunktio, niin väite seuraa määritelmästä 5.2. □

Lause 5.4. *Yhtäsuuruus $\mathcal{L}_{q_i}(G) = \mathcal{L}_i$ pätee kaikilla $q_i \in Q$, jos ja vain jos $a^{-1}\mathcal{L}_i$ on yhdiste $\mathcal{L}_j$:stä kaikille $\mathcal{L}_i$ ja $a \in \Sigma$. Tässä $\mathcal{L}_i$ ja $\mathcal{L}_j$ on atomien yhdisteitä.*

Todistus. Olkoon $\mathcal{G}$ atomipeitteen generoima s-NFA. Oletetaan ensin, että $\mathcal{L}_{q_i} = \mathcal{L}_i$ kaikilla $q_i \in Q$. Tarkastellaan mielivaltaisia $\mathcal{L}_i$ ja $a \in \Sigma$. Nyt pätee

$$a^{-1}\mathcal{L}_i = a\mathcal{L}_{q_i}(\mathcal{G}) = \bigcup_{q_j \in \delta(q_i, a)} \mathcal{L}_{q_j}(\mathcal{G}) = \bigcup_{\mathcal{L}_j \subseteq a^{-1}\mathcal{L}_i} \mathcal{L}_j.$$

Kääntäen oletetaan, että $a^{-1}\mathcal{L}_i$ on $\mathcal{L}_j$:den yhdiste kaikilla $\mathcal{L}_i$ ja $a \in \Sigma$. Tarkastellaan mielivaltaista $\mathcal{G}$:n tilaa q_i. Lauseen 5.3 nojalla, $\mathcal{L}_{q_i}(\mathcal{G}) \subseteq \mathcal{L}_i$ pätee, joten pitää todistaa vain $\mathcal{L}_i \subseteq \mathcal{L}_{q_i}(\mathcal{G})$. Olkoon nyt w mielivaltainen $\mathcal{L}_i$:n sana. Jos $w = \epsilon$, niin $q_i \in \mathcal{F}$, ja siten $w \in \mathcal{L}_{q_i}(\mathcal{G})$. Jos $w \in \Sigma^*$, niin $w^{-1}\mathcal{L}_i$ on $\mathcal{L}_j$ yhdiste. Koska $w \in \mathcal{L}_i$, on olemassa $\mathcal{L}_j$ siten, että $\mathcal{L}_j \subseteq w^{-1}\mathcal{L}_j$ ja $\epsilon \in \mathcal{L}_j$. Lisäksi on olemassa $q_j \in \mathcal{F}$, jolla $q_j \in \delta(q_i, w)$. Joten $w \in \mathcal{L}_{q_i(\mathcal{G})}$, joten $\mathcal{L}_{q_i}(\mathcal{G}) = \mathcal{L}_i$. □

Seuraava lause seuraa suoraan lauseesta 5.4.

Lause 5.5. *Jos $a^{-1}\mathcal{L}_i$ on $\mathcal{L}_j$:den yhdiste, kaikilla $\mathcal{L}_i$ ja $a \in \Sigma$, niin G hyväksyy $\mathcal{L}$:n.*

Todistus. Olkoon $\mathcal{G}$ atomien generoima s-NFA. Jos $a^{-1}\mathcal{L}_i$ on $\mathcal{L}_j$:den yhdiste kaikilla $\mathcal{L}_i$ ja $a \in \Sigma$, niin lauseesta 5.4 seuraa, että $\mathcal{L}_{q_i}(\mathcal{G}) = \mathcal{L}_i$ pätee kaikilla $i \in Q$.

Nyt

$$\mathcal{L}(\mathcal{G}) = \bigcup_{q_i \in \mathcal{I}} \mathcal{L}_{q_i}(\mathcal{G}) = \bigcup_{\mathcal{L}_i \subseteq \mathcal{L}} \mathcal{L}_i = \mathcal{L}.$$

Täten $\mathcal{L}(\mathcal{G}) = \mathcal{L}$. □

Yksinkertainen esimerkki atomipeitteestä on $\mathcal{L}$:n atomien joukko $A = \{A_1, \ldots, A_m\}$, jossa A_m on loppuatomi. Brzozowskin ja Tammin esittelivät atomaatin käsitteen artikkelissa [BT14]. Atomaatti on epädeterminististinen automaatti, jonka tiloina käytetään kielen atomeja eli osamäärien ja niiden komplementtejin epätyhjiä leikkausia. Määritellään tästä symbolinen versio.

Määritelmä 5.6 (**Symbolinen atomaatti**)**.** Kielen $\mathcal{L}$ **symbolinen atomaatti** on s-NFA

$$\mathcal{A} = (\mathcal{B}, Q, \Delta, \mathcal{I}, \{q_m\}),$$

jossa $\mathcal{B}$ on efektiivinen Boolen algebra, Q on äärellinen joukko tiloja, δ on äärellinen joukko siirtymiä, $\mathcal{I}$ äärellinen alkutilojen joukko ja $\{q_m\}$ ainoa lopputila. Lisäksi $Q = \{q_1, \ldots, q_m\}$, $I = \{q_i \mid \mathcal{A}_i \subseteq \mathcal{L}\}$ ja $(q_i, \varphi, q_j) \in \Delta$, jos ja vain jos $[[\varphi]] \subseteq \mathcal{A}i$ jos $\mathcal{A}_i, \mathcal{A}_j \in A$ ja φ on $\mathcal{L}$:n mintermi.

Symbolisissa atomaateista on hyvä huomata, että niillä on täsmälleen yksi lopputila, joka on atomipeitteen loppuatomi. Tiedetään Tammin ja Brzozowskin aikaisemmasta artikkelista [BT14], että jokaisella atomilla A_i ja $a \in \Sigma$ $a^{-1}A_i$ on atomien yhdiste. Täten lauseen 5.4 perusteella kaikilla $q_i \in Q$ pätee $\mathcal{L}_{q_i}(A) = A_i$. Lauseen 5.5 perusteella $\mathcal{L}(\mathcal{A}) = \mathcal{L}$. Lisäksi vastaavasti kuin Tammin ja Brzozowski artikkelissa [BT14] esitetyssä klassisessa tapauksessa saamme, että $A^{\mathcal{R}}$ predikaatti normalisoitu versio on käänteiskielen $\mathcal{L}^{\mathcal{R}}$ minimaalinen s-DFA.

Toinen esimerkki atoimipeitteestä on kielen $\mathcal{L}$ **alkuosamäärät** $\mathcal{K}' = \{\mathcal{K}'_1, \ldots, \mathcal{K}'_k\}$, joka koostuu $\mathcal{L}$:n epätyhjistä osamääristä, jotka eivät ole muiden osamäärien yhdisteitä. Alkuosamääriä on sovellettu Deniksen, Lemayn ja Terlutten artikkelissa [DLT01] kanononisen äärellisen jäännösautomaatin määrittelyssä, joka on NFA, jonka kielinä toimii jäännökset eli sen kielen osamäärät. Määritellään kanoninen äärellinen jäännösautomaatti eli kanoninen RFSA:n symbolinen versio yleissivistyksen vuoksi.

Määritelmä 5.7 (Kanoninen symbolinen äärellinen jäännösautomaatti)**.** Olkoon viisikko

$$\mathcal{R} = (\mathcal{B}, Q, \Delta, \mathcal{I}, \mathcal{F}),$$

jossa $\mathcal{B}$ on efektiivinen Boolen algebra, Q on äärellinen joukko tiloja, Δ äärellinen joukko siirtymiä, $\mathcal{I}$ äärellinen alkutilojen joukko ja $\mathcal{F}$ äärellinen lopputilojen joukko. $\mathcal{R}$ on kielen $\mathcal{L}$ **kanoninen symbolinen äärellinen jäännösautomaatti** eli kanoninen s-RFSA, jos $Q = \{q_1, \ldots, q_k\}$, $\mathcal{I} = \{q_i \mid \mathcal{K}'_i \subseteq \mathcal{L}\}$ ja $(q_i, \varphi, q_j) \in \Delta$, jos ja vain jos $[[\varphi]]\,\mathcal{K}'_j \subseteq \mathcal{K}'_i$, kun $\mathcal{K}'_i, \mathcal{K}'_j \in \mathcal{K}'$ ja $\mathcal{L}$:n mintermillä φ.

Jokainen kielen $\mathcal{L}$ osamäärä on on $\mathcal{L}$:n alkuosamäärien yhdiste, joten jokaisella alkuosamäärällä $\mathcal{K}_i'$ ja $a \in \Sigma$, $a^{-1}\mathcal{K}'_i$ on alkuideaalien yhdiste. Vastaavasti, kuin edellä olevassa esimerkissä $q_i \in Q$ on jokin alkuositus $\mathcal{K}_i'$ ja $\mathcal{L}(R) = \mathcal{L}$.

Siirrytään tarkastelemaan deterministisöityjen s-NFA:iden vasempia kieliä.

Lause 5.8. *Olkoon s-NFA $\mathcal{N} = (\mathcal{B}, Q, \delta, \mathcal{I}, \mathcal{F})$. $\mathcal{N}^{\mathcal{D}}$ tilan s vasen kieli on $\mathcal{L}_{\{\mathcal{I}\},s}\left(\mathcal{N}^{\mathcal{D}}\right) = \bigcap_{q\in s}\mathcal{L}_{\mathcal{I},q}(\mathcal{N}) \cap \bigcap_{q\notin s}\overline{\mathcal{L}_{\mathcal{I},q}(\mathcal{N})}$.*

Todistus. Olkoon $\mathcal{N} = (\mathcal{B}, Q, \delta, \mathcal{I}, \mathcal{F})$ s-NFA. Olkoon s $\mathcal{N}^{\mathcal{D}}$:n tila ja sana $w \in \mathcal{L}_{\{\mathcal{I}\},s}\left(\mathcal{N}^{\mathcal{D}}\right)$ on tilan s vasemman kielen sana. Todistataan väite induktiolla w:n pituuden suhteen.

Perusaskel: Olkoon $w = \epsilon$, jolloin siis $|w| = 0$. Nyt $s = \mathcal{I}$ on $\mathcal{N}^{\mathcal{D}}$:n alkutila. $\epsilon \in \mathcal{L}_{\{\mathcal{I}\},s}(\mathcal{N})$ kaikilla $q \in \mathcal{I}$ ja $\epsilon \notin \mathcal{L}_{\{\mathcal{I}\},s}(\mathcal{N})$ kaikilla $q \in \mathcal{I}$, joten selvästi $\epsilon \in \mathcal{L}_{\{\mathcal{I}\},s}\left(\mathcal{N}^{\mathcal{D}}\right)$, jos ja vain jos $\epsilon \in \bigcap_{q\in s}\mathcal{L}_{\mathcal{I},q}(\mathcal{N}) \cap \bigcap_{q\notin s}\overline{\mathcal{L}_{\mathcal{I},q}(\mathcal{N})}$.

Induktio-oletus: Olkoon $w = u$ ja $|w| = |u| = n$ siten, että $u \in \Sigma^*$. Oletetaan, että $u \in \mathcal{L}_{\{\mathcal{I}\},s'}\left(\mathcal{N}^{\mathcal{D}}\right)$ pätee $\mathcal{N}^{\mathcal{D}}$:n tilalle s', jos ja vain jos, $u \in \bigcap_{q\in s'}\mathcal{L}_{\mathcal{I},q}(\mathcal{N}) \cap \bigcap_{q\notin s'}\overline{\mathcal{L}_{\mathcal{I},q}(\mathcal{N})}$.

Induktioaskel: Olkoon nyt $w = ua$, jossa $w \in \Sigma^*$ ja $a \in \Sigma$. Nyt $|w| = |ua| = n + 1$. Jos $w \in \mathcal{L}_{\{\mathcal{I}\},s}\left(\mathcal{N}^{\mathcal{D}}\right)$, niin on olemassa $\mathcal{N}^{\mathcal{D}}$ tila s^*, jolle pätee, että $u \in \mathcal{L}_{\{\mathcal{I}\}}, s * \left(\mathcal{N}^{\mathcal{D}}\right)$ ja on olemassa siirtymä $\left(s^*, \varphi_{s^*,s}s\right)$, jossa $a \in \left[\left[\varphi_{s^*,s}\right]\right]$. Nyt lauseen 4.12 perusteella $\varphi_{s^*,s} = \left(\bigcap_{q\in s}\varphi_{s^*,q}\right) \cap \left(\bigcap_{q\in S_{s^*}\setminus s}\overline{\varphi_{s^*,q}}\right)$, jossa $\varphi_{s^*,q} = \bigvee_{(p,\varphi,q)\in\delta, p\in s^*}\varphi$ ja S_{s^*} on $\mathcal{N}$ tilojen q joukko, joihin on siirtymä, siten, että on olemassa $p \in s^*$, jolla (p, φ, q). Induktio-oletuksen perusteella $u \in \mathcal{L}_{\{\mathcal{I}\},q}\left(\mathcal{N}^{\mathcal{D}}\right)$ pätee kaikilla $q \in s^*$ ja $u \notin \mathcal{L}_{\{\mathcal{I}\},q}\left(\mathcal{N}^{\mathcal{D}}\right)$ pätee kaikilla $q \notin s^*$, joten induktio-oletuksen ja edellisen perusteella $ua \in \mathcal{L}_{\mathcal{I},q}(\mathcal{N})$ kaikilla $q \in s$ ja $ua \notin \mathcal{L}_{\mathcal{I},q}(\mathcal{N})$ kaikilla $q \notin s$. Joka on yhtäpitävää, sen kanssa, että $ua \in \bigcap_{q\in s}\mathcal{L}_{\mathcal{I},q}(\mathcal{N}) \cap \bigcap_{q\notin s}\overline{\mathcal{L}_{\mathcal{I},q}(\mathcal{N})}$. □

Tarkastellaan seuraavaksi symbolisen säännöllisen kielen s-DFA:ta $\mathcal{D} = (\mathcal{B}, \mathcal{S}, \Delta, \{s_1\}, \mathcal{S}_{\mathcal{F}})$, jonka tilojen joukko on $\mathcal{S} = \{s_1, \ldots, s_n\}$. Olkoon lisäksi $\mathcal{L}_i = \mathcal{L}_{\{s_1\},s_i}$ tilan s_i vasen kieli, kun $i = 1, \ldots, n$. Edellisen lauseen perusteella $\mathcal{L}_i \cap \mathcal{L}_j = \varnothing$, kun $s_i \neq s_j$. Todetaan lisäksi, että kielen $\mathcal{L}$ minkä tahansa s-DFA $\mathcal{D}'$:n tilojen ja kielien $\mathcal{L}_i$ välillä on yksi moneen suhde. Nimittäin jokainen $\mathcal{L}_i$ on sitä vastaavien tilojen vasempien kielien disjunktio. Pelkästään tilanteessa, jossa $\mathcal{D}'$ on minimaalinen, suhde on yksi yhteen suhde.

Lause 5.9. *Olkoon $\mathcal{N}$ s-NFA. $\mathcal{N}^{\mathcal{D}}$ on minimaalinen, jos ja vain jos $\mathcal{N}$:n jokainen vasen kieli on $\mathcal{L}_i$:den yhdiste.*

Todistus. Olkoon $\mathcal{N} = (\mathcal{B}, Q, \delta, \mathcal{I}, \mathcal{F})$ s-NFA ja siitä determinitisöity s-DFA $\mathcal{N}^{\mathcal{D}}$:n minimaalinen s-DFA. Jokaisella $\mathcal{N}^{\mathcal{D}}$:n tilalla q_i vasen kieli on $\mathcal{L}_i$.

Tehdään vastaoletus, että on olemassa $\mathcal{N}$:n tila q_k, jonka kieli ei ole vasempien kielten yhdiste. Siis on olemassa sana $u \in \mathcal{L}_h, u \in \mathcal{L}_{\mathcal{I},q_k}(\mathcal{N})$, mutta $\mathcal{L}_h \nsubseteq \mathcal{L}_{\mathcal{I},q_k}(\mathcal{N})$.

Olkoon $s_u \in \mathcal{N}^{\mathcal{D}}$:n tila siten, että $w \in \mathcal{L}_{\{\mathcal{I}\},s_u}\left(\mathcal{N}^{\mathcal{D}}\right)$. $\mathcal{N}^{\mathcal{D}}$ on minimaalinen, niin $\mathcal{L}_{\{\mathcal{I}\},s_u}\left(\mathcal{N}^{\mathcal{D}}\right) = \mathcal{L}_h$. Lauseen 5.8 perusteella $q_k \in s_u$ ja $\mathcal{L}_{\{\mathcal{I}\},s_u}\left(\mathcal{N}^{\mathcal{D}}\right) \subseteq \mathcal{L}_{\mathcal{I},q_k}(\mathcal{N})$. Siis $\mathcal{L}_h = \mathcal{L}_{\{\mathcal{I}\},s_u}\left(\mathcal{N}^{\mathcal{D}}\right) \subseteq \mathcal{L}_{\mathcal{I},q_k}(\mathcal{N})$, siis $\mathcal{L}_h \subseteq \mathcal{L}_{\mathcal{I},q_k}(\mathcal{N})$, joka on ristiriidassa vastaoletuksen kanssa.

Todistetaan toinen suunta. Olkoon $\mathcal{N}$:n kaikki vasemmat kielet $\mathcal{L}_i$:den yhdisteitä. Nyt lauseen 5.8 perusteella $\mathcal{N}^{\mathcal{D}}$:n jokainen vasen kieli on konjuktioita $\mathcal{N}$:n vasemmista kielistä ja koska selvästi $\mathcal{N}^{\mathcal{D}}$:n mikä tahansa vasen kieli on $\mathcal{L}_i$:n osajoukko. Siis $\mathcal{N}^{\mathcal{D}}$:n vasemmat kielet ovat täsmälleen $\mathcal{L}_i$:t. $\mathcal{N}^{\mathcal{D}}$ on minimaalinen. □

Määritellään atomisen symbolisen epädeterministisen automaatin käsite.

Määritelmä 5.10 (Atominen s-NFA). Olkoon s-NFA

$$\mathcal{N} = (\mathcal{B}, Q, \Delta, \mathcal{I}, \mathcal{F}),$$

jossa $\mathcal{B}$ on efektiivinen Boolen algebra, Q on äärellinen joukko tiloja, Δ on äärellinen joukko siirtymiä, $\mathcal{I}$ on äärellinen joukko alkutiloja ja $\mathcal{F}$ on äärellinen joukko lopputiloja. $\mathcal{N}$ on **atominen**, jos kaikki $q \in Q$ $\mathcal{L}_q(\mathcal{N})$ ovat $\mathcal{L}(\mathcal{N})$ atomien yhdisteitä.

Esitellään ja todistetaan lopuksi yleistetty Brzozowskin lause symbolisille automaateille.

Lause 5.11 (**Yleistetty Brzozowskin lause symbolisille automaateille**)**.** *Kaikilla s-NFA* $\mathcal{N}$ $\mathcal{N}^{\mathcal{D}}$ *on minimaalinen, jos ja vain jos* $\mathcal{N}^{\mathcal{R}}$ *on atominen.*

Todistus. Määritelmän 5.6 ja symbolisen atomaatin ominaisuuksien perusteella kielen atomit ovat samoja kuin käänteiskielen s-DFA:n tilojen vasemmat käänteiskielet. Siis $\mathcal{N}^{\mathcal{R}}$ on atominen, jos ja vain jos $\mathcal{N}$:n jokainen vasen kieli on $\mathcal{L}_i$:n yhdiste. Nyt siis lauseen 5.9, mukaan $\mathcal{N}^{\mathcal{R}}$ on minimaalinen, jos ja vain jos $\mathcal{N}^{\mathcal{R}}$ on atominen. □

Lähteet

[BT14] Janusz Brzozowski and Hellis Tamm. Theory of átomata. *Theoret. Comput. Sci.*, 539:13–27, 2014.

[DLT01] François Denis, Aurélien Lemay, and Alain Terlutte. Residual finite state automata. In *STACS 2001 (Dresden)*, volume 2010 of *Lecture Notes in Comput. Sci.*, pages 144–157. Springer, Berlin, 2001.

[DV17] Loris D'Antoni and Margus Veanes. The power of symbolic automata and transducers. In *Computer aided verification. Part I.*, volume 10426 of *Lecture Notes in Comput. Sci.*, pages 47–67. Springer, Cham, 2017.

[GH09] Steven Givant and Paul Halmos. *Introduction to Boolean algebras*. Undergraduate Texts in Mathematics. Springer, New York, 2009.

[HU79] John E. Hopcroft and Jeffrey D. Ullman. *Introduction to automata theory, languages, and computation*. Addison-Wesley Series in Computer Science. Addison-Wesley Publishing Co., Reading, MA, 1979.

[Mur12] S. Murthy. *Algebra: Abstract and Modern*. Pearson Education India, 2012.

[SV17] Olli Saarikivi and Margus Veanes. Minimization of symbolic transducers. In *Computer aided verification. Part II.*, volume 10427 of *Lecture Notes in Comput. Sci.*, pages 176–196. Springer, Cham, 2017.

[TV18] Hellis Tamm and Margus Veanes. Theoretical aspects of symbolic automata. In *SOFSEM 2018: theory and practice of computer science*, volume 10706 of *Lecture Notes in Comput. Sci.*, pages 428–441. Springer, Cham, 2018.

[VdHT10] Margus Veanes, Peli de Halleux, and Nikolai Tillmann. Rex: Symbolic regular expression explorer. In *2010 Third International Conference on Software Testing, Verification and Validation*, pages 498–507, 2010.