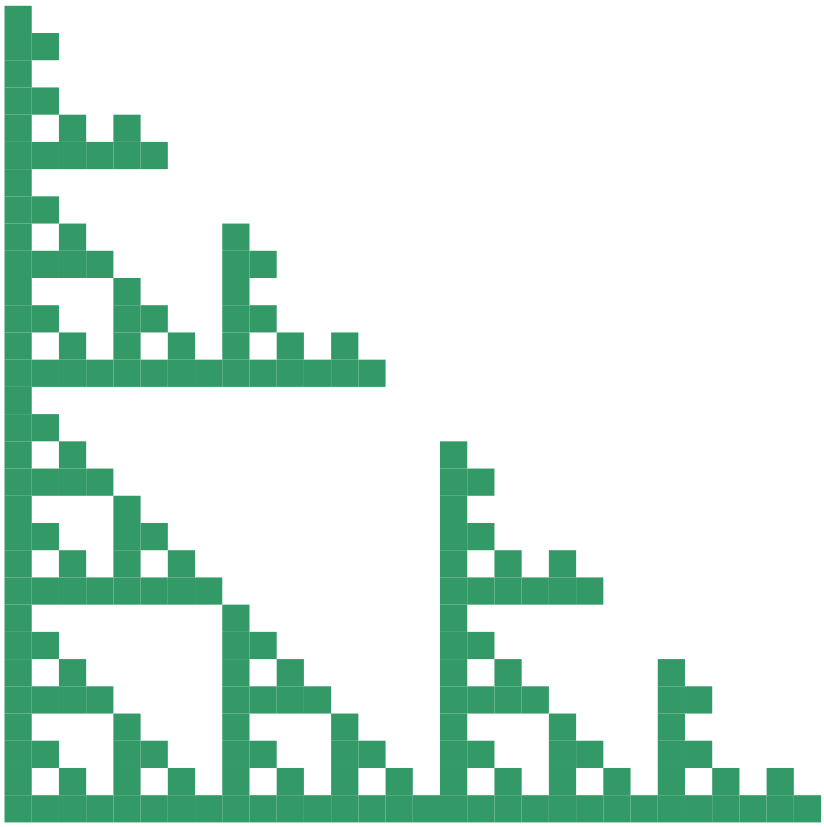
Äärellisten mallien teoria

Kerkko Luosto



Matematiikan ja tilastotieteen laitos
Helsingin yliopisto 1999–2010

Johdanto

Äärellisten mallien teoria on matemaattisen logiikan haara, jossa tutkitaan äärellisiä matemaattisia rakenteita matemaattisen logiikan menetelmin, usein erityisesti vaativuusteoreettisia sovelluksia silmällä pitäen. Alan nimessä esiintyvä 'malli ' ei siis viittaa reaalimaailman mallinnukseen, vaan on looginen käsite. Malleja ovat niin algebralliset rakenteet, kuten ryhmät, kunnat ja renkaat, kuin diskreetissä matematiikassa tutut verkot, puut ja lineaariset järjestykset. Matemaattisesta näkökulmasta katsoen äärellisten mallien teoriaa voi pitää *diskreetin matematiikan malliteoriana*; tietojenkäsittelynäkökulmassa taas painottuu *kuvailevan vaativuusteorian* rooli, ts. se, että äärellisten mallien teoria tarjoaa vaativuusluokkien loogisia karakterisointeja ja mahdollistaa vaativuusteoreettisten tulosten todistamisen tätä kautta.

Äärellisten mallien tutkimuksen Suomeen rantautumista lienee edistänyt kaikkein merkittävimmin Phokion Kolaitiksen Lahden Mukkulassa kesällä 1991 pitämä tiiviskurssi. Sittemmin myös suomalaiset ovat pitäneet tällaisia kursseja [Vää94, Hel97]. Lukukauden mittaisen erikoiskurssin pidin Helsingin yliopistossa ensimmäisen kerran syksyllä 1999. Sama luentopohja on ollut myös Taneli Huuskosen vuonna 2002 ja Juha Kontisen vuonna 2008 pitämissä kursseissa sekä tietenkin omissa luennoissani vuosina 2005 ja 2010.

Kurssina äärellisten mallien teoria on matemaattisen logiikan linjan valinnainen, ja muiden linjojen vapaasti valittava 10 opintopisteen laudatur-erikoiskurssi, joka soveltuu myös osaksi jatko-opinnoista. Valittu näkökulma on korostetusti matemaattinen ja tarvittavia kombinatorisia menetelmiä esittelevä, vaikkakaan teoreettisen tietojenkäsittelyn merkittävää vaikutusta alan ongelmien muotoutumiseen ei ole unohdettu.

Kurssilla tutustutaan ensin mallin käsitteeseen ja siihen, miten kahden mallin samanlaisuutta voi mitata eri tavoilla: homomorfisuudella, isomorfisuudella ja kombinatorisilla peleillä. Loogisiin käsitteisiin paneuduttaessa huomataan, että kombinatoriset pelit ovat suorassa yhteydessä logiikkaan. Malleja voi ajatella myös tietokoneohjelmien syötteinä eli relationaalisina tietokantoina; tämän idean kehittäminen johtaa deskriptiiviseen vaativuusteoriaan. Kurssin lopuksi käsitellään lyhyesti ensimmäisen kertaluvun logiikan 0–1-lakia ja yleistettyjä kvanttoreita.

Näiden luentojen lisäksi alalta on julkaistu useampi oppikirjoja. Näistä kurssia tukevat parhaiten Ebbinghausin ja Flumin [EF95] sekä Libkinin kirjat [Lib04]. Molemmat kirjat käsittelevät äärellisten mallien teoriaa selvästi laveammin kuin kurssi, ja ensimmäinen näistä kattaa kurssin lukujen aihepiirit täysin viimeistä lukua lukuun ottamatta. Hyvää kirjallisuutta on myös Immermanin kuvailevaa vaativuusteoriaa käsittelevä [Imm99].

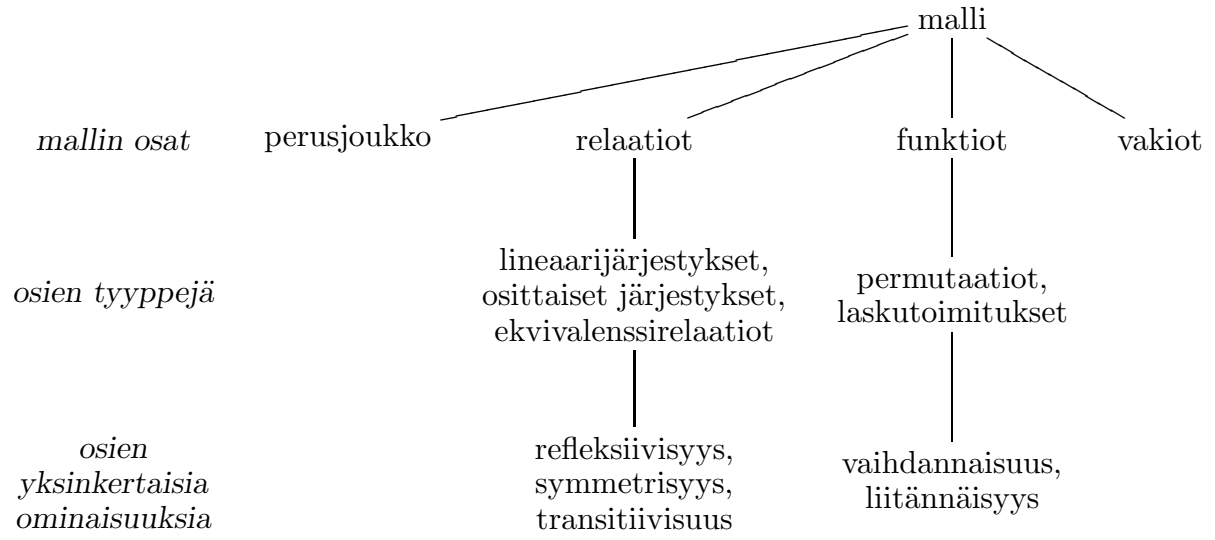
Mitäpä olisikaan matemaattinen logiikka ilman itseensä viittausta: tämä luentomateriaali on tosin säilynyt rakenteellisesti varsin alkuperäisen muotoisena, mutta vuosien varrella materiaali on hioutunut ja yksityiskohtia on kertynyt lisää. Niinpä ensimmäisenä luentovuonna asiaa oli täsmälleen kurssin verran, mutta nykyisessä luentomonisteessa on enemmän tekstiä, kuin mitä lukukauden kurssissa ehtii luennoida. Toisaalta se tarkoittanee myös, että materiaali pystyy luonnostaan joustamaan opiskelijoiden lähtötason ja toiveiden mukaan, ja tämä pohjana voi luennoida hieman toisistaan poikkeavia, mutta samanluontoisia kursseja.

Sisällys

I Mallit

Mallin käsite yleistää luonnollisella tavalla useita algebrassa ja diskreetissä matematiikassa esiintyviä matemaattisten rakenteiden käsitteitä. Malleja ovat niin algebran ryhmät, renkaat ja kunnat kuin diskreetin matematiikan verkot, puut ja lineaarijärjestetyt joukot. Toisaalta myös tietokoneohjelmien syötteitä voidaan pitää malleina, jos ne ovat relaatiotietokantojen kaltaisessa pelkistetyssä muodossa.

Mallit koostuvat relaatioista, funktioista ja vakioista. Tämän luvun rakenne on seuraavan kuvan kaltainen; luvun aikana kaavion asioita käydään läpi alhaalta ylöspäin.



1. Relaatiot

1.1. Määritelmä. Olkoon $n \in \mathbb{Z}_+ = \mathbb{N} \setminus \{0\}$ ($\mathbb{Z}_+$ on siis positiivisten kokonaislukujen joukko). Joukon X n-paikkaisella *relaatiolla* R tarkoitetaan karteesisen potenssin

$$X^n = \{\, (x_0, \ldots, x_{n-1}) \mid x_0, \ldots, x_{n-1} \in X \,\}$$

osajoukkoa, ts. $R \subset X^n$.

1.2. Esimerkki. Yksipaikkaiset relaatiot ovat yksinkertaisesti perusjoukon osajoukkoja. Näitä syntyy varsinkin väritysten yhteydessä: Olkoon $\chi\colon A \to F$ äärellinen väritys, ts. χ on kuvaus, jonka maalijoukko F on äärellinen. (Terminä sana 'väritys' vaikuttaa turhalta, koska se on määritelmän mukaan sanan 'kuvaus' synonyymi. Sanalla onkin

lähinnä herätemerkitys; se kertoo kysymyksenasettelun kombinatorisesta luonteesta.) Kun $c \in F$, väriä c olevien alkioiden joukko

$$\begin{aligned} C &= \chi^{-1}\,[\{c\}] \\ &= \{\, a \in A \mid \chi(a) = c \,\} \\ &= \{\, a \in A \mid \text{ alkion } a \text{ väri on } c \,\} \end{aligned}$$

on joukon A yksipaikkainen relaatio.

1.3. Esimerkki. Olkoon $T = \mathbb{R}^2$ euklidinen taso ja

$$V = \{\, (x, y, z) \in T^3 \mid \text{ On olemassa } r \in]0, 1[, \text{ jolle } y = (1 - r)x + rz \,\}$$

Tällöin V on kolmipaikkainen joukon T relaatio ja kaikilla $x, y, z \in T$ pätee

$(x, y, z) \in V$, jos ja vain jos x, y ja z ovat samalla suoralla ja y on x:n ja z:n välissä.

Tällä relaatiolla on tärkeä rooli tasogeometrian aksiomatisoinnissa.

Kaksipaikkaiset relaatiot

Kaksipaikkaiset relaatiot ovat yksipaikkaisia huomattavasti monimuotoisempia, ja useat relaatioita koskevat matemaattiset ilmiöt ilmenevät jo kaksipaikkaisten relaatioiden kohdalla. Kaksipaikkaisuuteen liittyy myös erityisominaisuuksia, kuten yhdisteltävyys, joiden takia matemaattinen käytäntö suosii niitä.

1.4. Määritelmä. Olkoon R joukon X kaksipaikkainen relaatio eli $R \subset X \times X$.

a) R on *refleksiivinen*, jos kaikilla $x \in X$ pätee $(x, x) \in R$. R on *irrefleksiivinen*, jos kaikilla $x \in X$ on voimassa $(x, x) \notin R$.

b) R on *symmetrinen*, jos kaikilla $x, y \in X$ pätee $(x, y) \in R$ täsmälleen silloin, kun $(y, x) \in R$. R on *antisymmetrinen*, jos kaikilla $x, y \in X$ ehdoista $(x, y) \in R$ ja $(y, x) \in R$ seuraa $x = y$.

c) R on *transitiivinen*, jos kaikilla $x, y, z \in X$ ehdoista $(x, y) \in R$ ja $(y, z) \in R$ seuraa $(x, z) \in R$.

d) R on *vertailullinen*, jos kaikilla eri alkioilla $x, y \in X$ ainakin toinen ehdoista $(x, y) \in R$ tai $(y, x) \in R$ on voimassa.

Huomautus. Irrefleksiivisyys ja epärefleksiivisyys ovat eri asioita: kahden alkion joukon $X = \{a, b\}$ relaatio $R = \{(a, a)\}$ ei ole refleksiivinen, siis on epärefleksiivinen, mutta ei ole irrefleksiivinenkään. Samoin antisymmetrisyys ja epäsymmetrisyys ovat eri käsitteitä. Tarkastellaan kolmen alkion joukon $\{a, b, c\}$ relaatiota $R = \{(a, b), (b, c), (c, b)\}$.

R ei ole symmetrinen, koska $(a, b) \in R$ mutta $(b, a) \notin R$. R ei ole antisymmetrinenkään, koska $(b, c) \in R$ ja $(c, b) \in R$, vaikka $b \neq c$.

1.5. Lause. *Olkoon R joukon X kaksipaikkainen relaatio. Tällöin R on yhtäaikaa symmetrinen ja antisymmetrinen täsmälleen silloin, kun $R \subset \Delta$, missä $\Delta = \{ (x, y) \in X \times X \mid x = y \}$ on joukon X diagonaali- eli yhtäsuuruusrelaatio.*

Todistus. Jos $R \subset \Delta$, niin kaikilla $(x, y) \in R$ pätee $x = y$, joten R on antisymmetrinen, mutta toisaalta myös $(y, x) = (x, x) = (x, y) \in R$, joten R on symmetrinen.

Oletetaan kääntäen, että R on symmetrinen ja antisymmetrinen. Olkoot x ja y joukon X eri alkioita. Symmetrisyyden vuoksi ehdot $(x, y) \in R$ ja $(y, x) \in R$ ovat joko kumpikin voimassa tai kumpikaan ei ole voimassa. Antisymmetrisyyden vuoksi edellinen vaihtoehto on mahdoton. Siis $(x, y) \notin R$ aina, kun $x, y \in X$, $x \neq y$. Tästä seuraa $R \subset \Delta$. □

Harjoitustehtävänä on osoittaa, että ominaisuuksien refleksiivisyys, symmetrisyys ja transitiivisuus välillä ei tietyssä mielessä ole lainkaan yksinkertaisia riippuvuussuhteita.

1.6. Määritelmä. Olkoot $R, S \subset X \times X$. Relaation R *käänteisrelaatio* on

$$R^{-1} = \{ (y, x) \mid (x, y) \in R \}$$

ja relaatioiden R ja S *yhdistetty relaatio* on

$$R \circ S = \{ (x, z) \in X \times X \mid \text{ On olemassa } y \in X, \text{ jolle } (x, y) \in S \text{ ja } (y, z) \in R \}$$

Huomautus. Kuvaus $f\colon X \to X$ on joukko-opillisen määritelmänsä mukaan kaksipaikkainen relaatio $f = \{ (x, f(x)) \mid x \in X \}$. Yo. määritelmät yleistävät käänteisfunktion ja yhdistetyn funktion käsitteitä. Kuvauksella f ei välttämättä ole käänteisfunktiota, mutta sillä on aina käänteisrelaatio (kun kuvausta f tarkastellaan relaationa). Lisäksi kuvauksen f käänteisfunktio on olemassa, jos ja vain jos kuvauksen f käänteisrelaatio f^{-1} on funktio, ja tällöin f^{-1} on tämä käänteisfunktio.

Vastaavasti yhdistetyn relaation merkinnässä relaatioiden R ja S järjestys on valittu niin, että kuvausten $f, g\colon X \to X$ yhdistetty kuvaus on sama kuin näiden yhdistetty relaatio:

$$\begin{aligned} f \circ g &= \{ (x, f(g(x)) \mid x \in X \} \\ &= \{ (x, z) \in X \times X \mid z = f(y), \text{ missä } y = g(x) \} \\ &= \{ (x, z) \in X \times X \mid \text{On olemassa } y \in X, \text{ jolle } (y, z) \in f \text{ ja } (x, y) \in g \} \\ &= \{ (x, z) \in X \times X \mid \text{On olemassa } y \in X, \text{ jolle } (x, y) \in g \text{ ja } (y, z) \in f \} \end{aligned}$$

$$x \underset{g}{\longmapsto} y \underset{f}{\longmapsto} z$$

Näillä relaatioalgebrallisilla merkinnöillä relaatioiden perusominaisuudet voidaan muotoilla seuraavasti. Olkoon $R \subset X \times X$. Tällöin

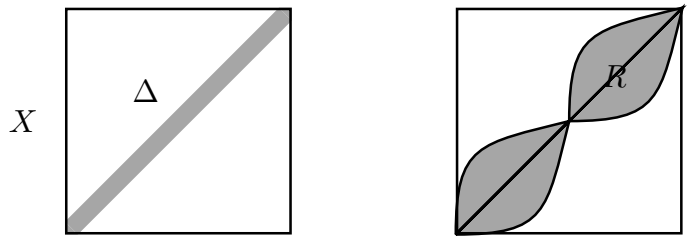
$$\begin{aligned} R \text{ on refleksiivinen} &\iff \Delta \subset R, \\ R \text{ on irrefleksiivinen} &\iff \Delta \cap R = \emptyset, \\ R \text{ on symmetrinen} &\iff R^{-1} \subset R \iff R^{-1} = R, \\ R \text{ on transitiivinen} &\iff R \circ R \subset R. \end{aligned}$$

Tässä Δ on joukon X diagonaalirelaatio.

Kaksipaikkaisia relaatioita voidaan havainnollistaa monin tavoin. Verkkomerkintöjä käyttäen:

$(x, x) \in R$ $(x, y) \in R$ $(x, y) \in R$ ja $(y, x) \in R$

Toinen tapa on piirtää relaatio tasoon:



X symmetrinen relaatio

1.7. Esimerkki.

a) Tarkastellaan joukon $\{0, \ldots, n-1\}$ $(n \in \mathbb{Z}_+)$ seuraajarelaatiota

$$S = \{\, (k, k+1) \mid k \in \{0, \ldots, n-2\} \,\}.$$

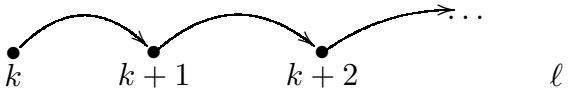
S on selvästi irrefleksiivinen ja antisymmetrinen, mutta ei transitiivinen, jos $n \geq 2$, koska tällöin $(0, 1) \in S$, $(1, 2) \in S$, mutta $(0, 2) \notin S$.

b) Olkoon X Pähkinäsaaren rauhan jälkeen syntyneiden suomalaisten joukko ja V vanhemmuusrelaatio:

$$V = \{\, (x, y) \in X \times X \mid y \text{ on } x\text{:n äiti tai isä} \,\}.$$

Tässäkin tapauksessa on ilmeisesti kyse irrefleksiivisestä ja antisymmetrisestä relaatiosta, joka ei ole transitiivinen.

Kummassakin edellisen esimerkin tapauksessa esimerkkirelaatioon liittyy luonnollisella tavalla transitiivinen relaatio. Kohdassa a lukujen $k, \ell \in \{0, \ldots, n-1\}$ tiukka järjestys $<$ on määriteltävissä seuraajarelaation S avulla, sillä $k < \ell$ täsmälleen silloin, kun voidaan muodostaa seuraavanlainen kaavio:



Kohdassa b vanhemmuusrelaation V avulla voidaan määrittää (suomalaista polveutumista vastaavat) esivanhemmat eli relaatio

$$E = \{\, (x, y) \in X \times X \mid x \text{ polveutuu } y\text{:stä (suomalaisten kautta)} \,\}$$

1.8. Määritelmä. Relaation $R \subset X \times X$ *transitiivinen sulkeuma* $\mathrm{TC}(R)$ on pienin relaatio $T \subset X \times X$, joka on transitiivinen ja sisältää relaation R.

Transitiivinen sulkeuma on hyvinmääritelty:

1.9. Lause. *Relaation $R \subset X \times X$ transitiivinen sulkeuma on*

$$\mathrm{TC}(R) = \bigcap \mathcal{T},$$

missä $\mathcal{T}$ on niiden transitiivisten relaatioiden $T \subset X \times X$, joille $R \subset T$, perhe. Toisaalta

$$\mathrm{TC}(R) = \bigcup_{n \in \mathbb{Z}_+} R^n,$$

missä $R^1 = R$ ja $R^{n+1} = R \circ R^n$.

Todistus. Perhe $\mathcal{T}$ on epätyhjä, sillä täysi relaatio $X \times X$ on transitiivinen ja sisältää relaation R. Merkitään $R^+ = \bigcap \mathcal{T}$. $R \subset R^+$, sillä R^+ on leikkaus relaatioista $T \in \mathcal{T}$, joille $R \subset T$. R^+ on myös transitiivinen: Olkoon $(x, y) \in R^+$ ja $(y, z) \in R^+$. Jokaisella $T \in \mathcal{T}$ pätee tällöin $\{(x, y), (y, z)\} \subset R^+ \subset T$, joten koska T on transitiivinen, $(x, z) \in T$. Siis $(x, z) \in \bigcap \mathcal{T} = R^+$. Koska $R \subset R^+$ ja R^+ on transitiivinen, $R^+ \in \mathcal{T}$ ja on siis perheen $\mathcal{T}$ relaatioista pienin, so. $R^+ = \mathrm{TC}(R)$.

Merkitään sitten $R' = \bigcup_{n \in \mathbb{Z}_+} R^n$, missä relaatiot R^n ovat kuten väitteessä. Induktiolla saadaan, että $R^n \subset \mathrm{TC}(R)$ kaikilla $n \in \mathbb{Z}_+$: nimittäin $R^1 = R \subset \mathrm{TC}(R)$ ja jos $R^n \subset \mathrm{TC}(R)$, niin

$$R^{n+1} = R \circ R^n \subset \mathrm{TC}(R) \circ \mathrm{TC}(R) \subset \mathrm{TC}(R).$$

Siis $R = R^1 \subset \bigcup_{n \in \mathbb{Z}_+} R^n = R' \subset \mathrm{TC}(R)$. Yhtäsuuruuden $R' = \mathrm{TC}(R)$ osoittamiseksi riittää siis näyttää, että R' on transitiivinen.

Osoitetaan aluksi induktiolla luvun $m \in \mathbb{Z}_+$ suhteen, että kaikilla $m, n \in \mathbb{Z}_+$ pätee $R^m \circ R^n = R^{m+n}$. Kun $m = 1$, saadaan nimittäin

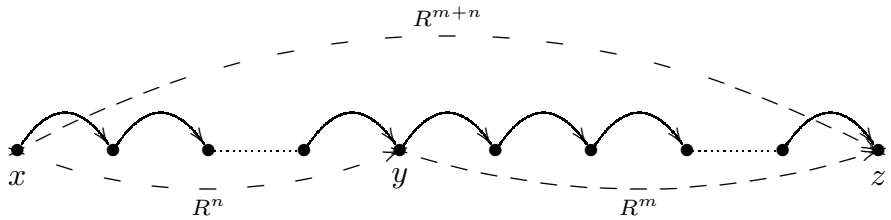
$$R^m \circ R^n = R^1 \circ R^n = R \circ R^n = R^{n+1} = R^{m+n}.$$

Oletetaan sitten, että kaikilla $n \in \mathbb{N}$ $R^m \circ R^n = R^{m+n}$. Tällöin jokaisella $n \in \mathbb{N}$

$$R^{m+1} \circ R^n = (R \circ R^m) \circ R^n = R \circ (R^m \circ R^n) = R \circ R^{m+n} = R^{(m+1)+n},$$

mikä päättää induktiotodistuksen.

(Oikeastaan tilanne on alla olevan kuvan mukainen: Jos $(x, y) \in R^n$, niin x:stä pääsee y:hyn n R-kaaren välityksellä. Jos y:stä pääsee z:aan m R-kaaren välityksellä, niin x:stä pääsee z:aan $m + n$ kaaren kautta.)



Olkoot $(x, y) \in R'$ ja $(y, z) \in R'$. Valitaan sellaiset $m, n \in \mathbb{N}$, että $(x, y) \in R^n$ ja $(y, z) \in R^m$. Tällöin $(x, z) \in R^m \circ R^n = R^{m+n} \subset R'$. Siis R' on transitiivinen. □

1.10. Esimerkki.

a) Joukon $X = \{0, \ldots, n-1\}$ $(n \in \mathbb{Z}_+)$ seuraajarelaation S transitiivinen sulkeuma $\mathrm{TC}(S) = \{\, (i,j) \in X \times X \mid i < j \,\}$ on joukon X luonnollinen tiukka järjestys. Jos nimittäin tarkastellaan relaation S potensseja kuten edellisessä lauseessa ($S^1 = S$, $S^{k+1} = S \circ S^k$), niin on helppoa osoittaa induktiolla, että $S^k = \{\, (i,j) \in X \times X \mid i + k = j \,\}$. Kun $i, j \in X$, niin $i < j$ on voimassa, jos ja vain jos jollakin $k \in \mathbb{Z}_+$ pätee $i + k = j$, mikä todistaa väitteen.

b) Olkoon X Pähkinäsaaren rauhan jälkeen syntyneiden suomalaisten joukko ja V vanhemmuusrelaatio. Huomataan, että

$$V^2 = \{\, (x,y) \in X \times X \mid y \text{ on } x\text{:n isoäiti tai isoisä (suomalaista kautta)} \,\},$$
$$V^3 = \{\, (x,y) \in X \times X \mid y \text{ on } x\text{:n isoisovanhempia (suomalaista kautta)} \,\}, \text{ jne.}$$

$\mathrm{TC}(V)$ on siis esivanhemmuusrelaatio.

Erilaisia relaatiotyypejä

Yhdistelemällä kaksipaikkaisten relaatioiden perusominaisuuksia (kuten refleksiivisyys, symmetrisyys ja transitiivisuus) saadaan tunnetuimpien relaatiotyyppien määritelmät.

1.11. Määritelmä. $E \subset X \times X$ on *ekvivalenssirelaatio*, jos se on refleksiivinen, symmetrinen ja transitiivinen.

Jokaisen joukon X yhtäsuuruusrelaatiolla $\Delta = \{\, (x,x) \mid x \in X \,\}$ on tietenkin nämä ominaisuudet. Kaikilla $x, y, z \in X$ pätee $x = x$, $x = y \iff y = x$ ja jos $x = y = z$, niin $x = z$. Ekvivalenssirelaation suuri merkitys matematiikassa perustuukin tähän yhtäsuuruuden jäljittelyyn: ekvivalenssirelaation avulla samaan ekvivalenssiluokkaan kuuluvat alkiot voidaan samastaa yhdeksi alkioksi.

1.12. Esimerkki. Olkoon T vuorokausien joukko ja

$$E = \{\, (x,y) \in T \times T \mid x\text{:stä } y\text{:hyn kuluu 7:llä jaollinen määrä päiviä} \,\}.$$

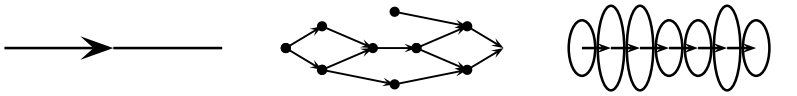
Tällöin E on ekvivalenssirelaatio, jonka ekvivalenssiluokkia ovat viikonpäivät. Esimerkiksi päivän 10.9.1999 ekvivalenssiluokka on perjantai.

Teemasta järjestys on kokoelman verran muunnelmia:

1.13. Määritelmä. Olkoon R joukon X kaksipaikkainen relaatio.

a) R on *esijärjestys*, jos R on refleksiivinen ja transitiivinen.
b) R on *osittainen järjestys*, jos R on refleksiivinen, antisymmetrinen ja transitiivinen.
c) R on *esilineaarijärjestys*, jos R on refleksiivinen, transitiivinen ja vertailullinen.
d) R on *lineaarijärjestys*, jos R on refleksiivinen, antisymmetrinen, transitiivinen ja vertailullinen.
e) R on *tiukka lineaarijärjestys*, jos R on irrefleksiivinen, transitiivinen ja vertailullinen. (Myös muista järjestystyypeistä on tiukat varianttinsa, jotka tässä sivuutetaan.)

Eri tyyppejä voi havainnollistaa seuraavanlaisilla kaavioilla:



lineaarijärjestys osittainen järjestys esilineaarijärjestys

1.14. Esimerkki. Seuraavassa esitetään perusteluitta muutamien tuttujen relaatioiden järjestysominaisuuksia:

a) Joukon $\mathbb{R}$ luonnollinen järjestys $\leq$ on lineaarijärjestys.

b) Joukossa $\mathbb{Z}$ määritellään jakojärjestys $\mid$ niin, että kaikilla $m, n \in \mathbb{Z}$ pätee $m \mid n \iff m$ on luvun n monikerta. Jakojärjestys $\mid$ on esijärjestys. Joukon $\mathbb{N}$ jakojärjestys $\mid \cap (\mathbb{N} \times \mathbb{N})$ on osittainen järjestys.

c) Olkoon X suljettujen reaalilukuvälien joukko. Tällöin relaatio $\preceq$, jolle $[a,b] \preceq [c,d] \iff d - c \geq b - a \iff [c,d]$ pidempi kuin $[a,b]$, kun $[a,b], [c,d] \in X$ on esilineaarijärjestys.

2. Funktiot

2.1. Määritelmä. Olkoon $n \in \mathbb{Z}_+$. Joukon X n-paikkaisella *funktiolla* tarkoitetaan kuvausta $f\colon X^n \to X$.

Joukko-opissa kuvaus samastetaan kuvaajansa kanssa, joten yllä oleva funktio on relaatio

$$\begin{aligned} f &= \{\, ((x_0, \ldots, x_{n-1}), f(x_0, \ldots, x_{n-1})) \mid x_0, \ldots, x_{n-1} \in X \,\} \\ &= \{\, (x_0, \ldots, x_{n-1}, f(x_0, \ldots, x_{n-1})) \mid x_0, \ldots, x_{n-1} \in X \,\} \end{aligned}$$

Siis n-paikkainen funktio on $n+1$-paikkainen relaatio. Jatkossa malliteoreettisten käsitteiden yhteydessä tullaan kuitenkin tekemään selvä ero sen mukaan, tarkastellaanko f:ää funktiona vai relaationa.

Palautettakoon mieleen kuvausten yleisiä perusominaisuuksia. Merkitään kuvauksen f määrittelyjoukkoa $\mathrm{dom}(f)$ ja arvojoukkoa $\mathrm{rg}(f)$. Merkintä $f\colon A \to B$ tarkoittaa sitä, että $A = \mathrm{dom}(f)$ ja $B \supset \mathrm{rg}(f)$. Kuvaus f on *injektio*, jos kaikilla eri alkioilla $x, y \in \mathrm{dom}(f)$ pätee $f(x) \neq f(y)$. Kuvaus $f\colon A \to B$ on *surjektio*, jos $B = f[A]$ eli $B = \mathrm{rg}(f)$. Huomattakoon, että väittämä "f on surjektio" on epätäsmällinen, koska $f\colon A \to B$ on myös $f\colon A \to C$ kaikilla $C \supset B$. Väittämä "joukon X n-paikkainen funktio f on surjektio" on kuitenkin selkeä, sillä tällöin tarkoitetaan kuvausta $f\colon X^n \to X$. $f\colon A \to B$ on *bijektio*, jos se on surjektio ja injektio.

Äärellisyyden erityispiirteet tulevat hyvin esiin funktioiden yhteydessä:

2.2. Lause. *Olkoon X joukko. Tällöin seuraavat ovat ovat yhtäpitäviä:*

a) X on äärellinen.

b) Jokainen joukon X yksipaikkainen funktio, joka on injektio, on myös surjektio.

c) Jokainen joukon X yksipaikkainen funktio, joka on surjektio, on myös injektio.

Todistus. Todistetaan kohtien negaatioiden yhtäpitävyys:

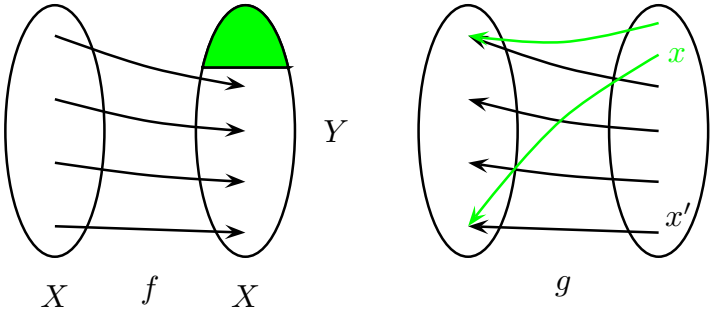
a′) X on ääretön.

b′) On olemassa joukon X yksipaikkainen funktio f, joka on injektio, mutta ei ole surjektio.

c′) On olemassa joukon X yksipaikkainen funktio f, joka on surjektio, mutta ei ole injektio.

Kohtien a′ ja b′ yhtäpitävyys on miltei äärettömyyden määritelmä: X on ääretön täsmälleen silloin, kun se on yhtämahtava aidon osajoukkonsa kanssa eli kun on olemassa $Y \subsetneq X$ ja bijektio $f\colon X \to Y$ eli on olemassa injektio $f\colon X \to X$, jolle $Y = \mathrm{rg}(f) \neq X$ eli joka ei ole surjektio.

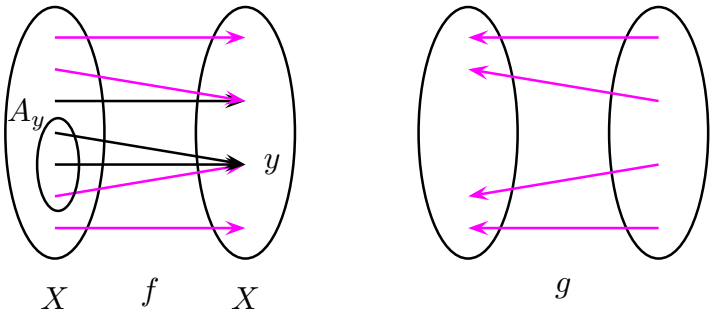
b′ $\Rightarrow$ c′: Olkoon $f\colon X \to X$ injektio, joka ei ole surjektio. Merkitään $Y = \mathrm{rg}(f) \neq X$. Tällöin f^{-1} on kuvaus $Y \to X$. Laajennetaan f^{-1} mielivaltaisella tavalla kuvaukseksi $g\colon X \to X$.



Tällöin g on surjektio, koska jokaisella $x \in X$ pätee $g(f(x)) = f^{-1}(f(x)) = x$. g ei ole injektio, koska on olemassa $x \in X \setminus Y$, ja alkiolle $x' = f(g(x))$ pätee $x \neq x'$, sillä $x \notin Y = \mathrm{rg}(f)$, mutta myös

$$g(x') = g(f(g(x))) = g(x).$$

c′ $\Rightarrow$ b′: Olkoon $f\colon X \to X$ surjektio, joka ei ole injektio. Tällöin käänteisrelaatio f^{-1} ei ole kuvaus, mutta jokaisella $y \in X$ on olemassa $x \in X$, jolle $(x, y) \in f$ eli $(y, x) \in f^{-1}$. Siis jokaisella $y \in X$ joukko $A_y = \{\, x \in X \mid (y, x) \in f^{-1} \,\}$ on epätyhjä.



Valinta-aksiooman nojalla on olemassa kuvaus $g\colon X \to X$, jolle $g \subset f^{-1}$. g on injektio, sillä joukot $A_y = f^{-1}[\{y\}]$ ovat erillisiä. g ei kuitenkaan ole surjektio, sillä joillakin $x, x' \in X$, $x \neq x'$, pätee $f(x) = f(x') = y$ ja $g(y) \neq x$ tai $g(y) \neq x'$, mistä seuraa, että $x \notin \mathrm{rg}(g)$ tai $x' \notin \mathrm{rg}(g)$. $\square$

Monipaikkaiset funktiot käyttäytyvät aivan eri tavalla:

2.3. Lause. *Olkoon X äärellinen joukko ja $n \in \mathbb{N}$, $n \geq 2$. Oletetaan, että on joukon X n-paikkainen funktio, joka on bijektio. Tällöin X on tyhjä tai yksiö.*

Todistus. Olkoon $k = |X|$, eli k on joukon X alkioiden lukumäärä. Koska on olemassa bijektio $f\colon X^n \to X$, niin $k^n = |X|^n = |X^n| = |X| = k \Rightarrow k = 0 \vee k^{n-1} = 1 \Rightarrow k = 0 \vee k = 1$. □

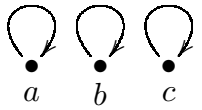
Yksipaikkaiset funktiot

2.4. Määritelmä. Alkio $x \in X$ on joukon X yksipaikkaisen funktion f *kiintopiste*, jos $f(x) = x$. Joukon X yksipaikkaista funktiota, joka on bijektio, kutsutaan *permutaatioksi*.

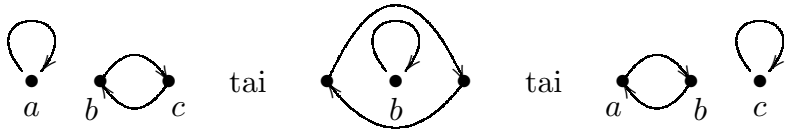
Kuten jo todettiin, yksipaikkainen funktio on itse asiassa kaksipaikkainen relaatio. Siksi on luonnollista, että yksipaikkaiset funktiot ovat huomattavasti monimuotoisempia kuin yksipaikkaiset relaatiot.

2.5. Esimerkki. Jo kolmen alkion joukolla $X = \{a, b, c\}$ on useita erilaisia yksipaikkaisia funktioita.

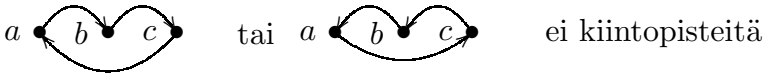
Permutaatiot



identtinen kuvaus,
kolme kiintopistettä

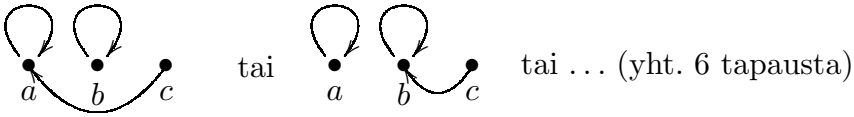


yksi kiintopiste (a tai b tai c)



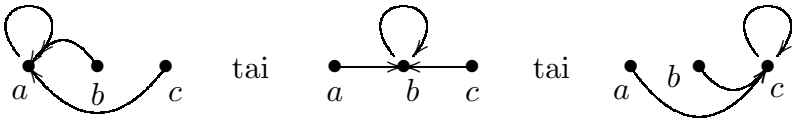
ei kiintopisteitä

Muut kuin permutaatiot

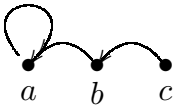


tai ... (yht. 6 tapausta)

2 kiintopistettä

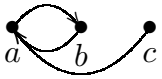


vakiofunktio (1 kiintopiste)



tai ... (6 tapausta)

1 kiintopiste, muttei vakiofunktio



tai ... (6 tapausta)

ei kiintopisteitä

Permutaatiot ovat erityisasemassa malliteoriassa: Toisaalta permutaatiot voivat olla mallin osasia. Toisaalta mallien symmetrioita kuvaavat automorfismit ovat permutaatioita, joten nämä ovat myös välineitä, joilla voi tulkita mallin ominaisuuksia.

Laskutoimitukset

2.6. Määritelmä. Joukon X kaksipaikkaista funktiota $*\colon X \times X \to X$ kutsutaan myös joukon X *laskutoimitukseksi*. Laskutoimitus $*$ on *vaihdannainen*, jos kaikilla $x, y \in X$ pätee

$$*(x, y) = *(y, x).$$

Laskutoimitus $*$ on *liitännäinen*, jos kaikilla $x, y, z \in X$ on voimassa

$$*(*(x, y), z) = *(x, *(y, z)).$$

Alkio $e \in X$ on *neutraali- eli ykkösalkio* laskutoimituksen $*$ suhteen, jos kaikilla $x \in X$ on voimassa

$$*(x, e) = *(e, x) = x.$$

Voidaan osoittaa, että neutraalialkio on yksikäsitteinen, jos sellainen on olemassa.

Alkiolla $x \in X$ on *käänteisalkio* $y \in X$, jos neutraalialkio e on olemassa ja

$$*(x, y) = *(y, x) = e.$$

Yllä funktioille on käytetty merkintää, jossa funktio edeltää muuttujaa. Algebrassa tavanomainen on kuitenkin sisämerkintä, jossa laskutoimitus $*$ merkitään muuttujien väliin. Tätä käyttäen yllä olevat yhtälöt muuntuvat tutumpaan muotoon:

$$\begin{aligned}
\text{(vaihdannaisuus)} \quad & x * y = y * x, \\
\text{(liitännäisyys)} \quad & (x * y) * z = x * (y * z), \\
\text{(neutraalialkio)} \quad & x * e = e * x = x \text{ ja} \\
\text{(käänteisalkio)} \quad & x * y = y * x = e.
\end{aligned}$$

2.7. Esimerkki. Joukossa $X = \{0, \ldots, n-1\}$, missä $n \in \mathbb{Z}_+$, määritellään laskutoimitus $+_n$ seuraavasti:

$$x +_n y = \begin{cases} x + y, & \text{jos } x + y < n \\ x + y - n, & \text{muuten.} \end{cases}$$

Algebra I:stä tiedetään, että $+_n$ on vaihdannainen ja liitännäinen laskutoimitus. 0 on tämän laskutoimituksen neutraalialkio, ja jokaisella $x \in X$ alkion x känteisalkio on $n - x \in X$, sillä $x +_n (n - x) = (x + n - x) - n = n - n = 0$.

3. Mallit

Tarkastellaan reaalilukujen ja rationaalilukujen systeemejä (järjestettyjä kuntia), jotka tavallisesti kirjoitetaan muodossa $\langle \mathbb{R}, +, \cdot, 0, 1, \leq \rangle$ ja $\langle \mathbb{Q}, +, \cdot, 0, 1, \leq \rangle$. Koska jälkimmäisen yhteen- ja kertolasku sekä lineaarijärjestys ovat edellisen systeemin rajoittumia joukkoon $\mathbb{Q}$, olisi tarkempaa kirjoittaa

$$\langle \mathbb{R}, +^{\mathbb{R}}, \cdot^{\mathbb{R}}, 0, 1, \leq^{\mathbb{R}} \rangle$$

ja

$$\langle \mathbb{Q}, +^{\mathbb{Q}}, \cdot^{\mathbb{Q}}, 0, 1, \leq^{\mathbb{Q}} \rangle,$$

missä $+^{\mathbb{Q}} = +^{\mathbb{R}} \restriction (\mathbb{Q} \times \mathbb{Q})$, $\cdot^{\mathbb{Q}} = \cdot^{\mathbb{R}} \restriction (\mathbb{Q} \times \mathbb{Q})$ ja $\leq^{\mathbb{Q}} = \leq^{\mathbb{R}} \restriction (\mathbb{Q} \times \mathbb{Q})$. Nämä aritmeettiset systeemit ovat silti siinä mielessä vertailukelpoisia, että $+^{\mathbb{R}}$ ja $+^{\mathbb{Q}}$, $\cdot^{\mathbb{R}}$ ja $\cdot^{\mathbb{Q}}$ sekä $\leq^{\mathbb{R}}$ ja $\leq^{\mathbb{Q}}$ ovat keskenään rinnastettavissa. Kummassakin systeemissä on siis yhteenlasku, kertolasku, nolla, ykkönen ja järjestys. Kun näitä vastaavat symbolit kerätään joukoksi, saadaan näiden yhteinen aakkosto $\{+, \cdot, 0, 1, \leq\}$. Aakkosto on siis mallin skemaattinen esitys, joka kertoo mallin rakenteen pääpiirteet. Seuraavassa työstetään käsitteet symbolit, aakkosto ja malli täsmällisesti.

Symbolit: Symbolit ovat joko vakio-, relaatio- tai funktiosymboleita. Jokaisella relaatiosymbolilla R on *paikkaluku* $n \in \mathbb{Z}_+$, jota merkitään $n = \#(R)$. Samoin jokaisella funktiosymbolilla f on paikkaluku $n = \#(f) \in \mathbb{Z}_+$. Täydellisyyden vuoksi sovitaan, että vakiosymbolin c paikkaluku $\#(c) = 0$. Symboleilla ei ajatella olevan tämän kummempaa matemaattista rakennetta, joten niiden joukko-opillisen määritelmän voi jättää avoimeksi. Kuitenkin ajatellaan, että symboleita on seuraavassa mielessä riittävästi: jokaisen joukon A ulkopuolelta löytyy ainakin kutakin tyyppiä olevat symbolit eli vakiosymboli, n-paikkainen relaatiosymboli kullakin $n \in \mathbb{Z}_+$ ja n-paikkainen funktiosymboli kullakin $n \in \mathbb{Z}_+$. Symboleita on syytä ajatella yksinkertaisesti merkkeinä, joista voidaan tunnistaa laadun (vakio-, relaatio- tai funktiosymboli) ja paikkaluvun. Jatkossa tämä merkkivertaus käy yhä ilmeisemmäksi, kun symbolien avulla luentojen osassa II (logiikka) rakennetaan termejä ja lauseita.

Aakkostot: Aakkostot ovat symbolijoukkoja. Aakkoston τ vakiosymboleiden joukkoja merkitään $\mathrm{Con}(\tau)$:lla, relaatiosymbolien joukkoa $\mathrm{Rel}(\tau)$:lla ja funktiosymbolien joukkoa $\mathrm{Fun}(\tau)$:lla. Siis $\tau = \mathrm{Con}(\tau) \cup \mathrm{Rel}(\tau) \cup \mathrm{Fun}(\tau)$, missä $\mathrm{Con}(\tau)$, $\mathrm{Rel}(\tau)$ ja $\mathrm{Fun}(\tau)$ ovat erillisiä.

3.1. Määritelmä. Paria $\mathfrak{M} = (M, T)$ kutsutaan aakkoston τ *malliksi*, jos seuraavat ehdot ovat voimassa:

1) $M \neq \emptyset$; joukkoa M kutsutaan mallin $\mathfrak{M}$ *universumiksi* tai *perusjoukoksi* ja merkitään $M = \mathrm{Dom}(\mathfrak{M})$.
2) T on kuvaus, jonka määrittelyjoukko on $\mathrm{dom}(T) = \tau$. T kuvaa symbolin $X \in \tau$ *tulkinnalleen*, jota merkitään $T(X) = X^{\mathfrak{M}}$.
3) Jokaisella $c \in \mathrm{Con}(\tau)$ tulkinta $c^{\mathfrak{M}} \in \mathrm{Dom}(\mathfrak{M})$ eli $c^{\mathfrak{M}}$ on mallin $\mathfrak{M}$ alkio.
4) Jokaisella $R \in \mathrm{Rel}(\tau)$ tulkinta $R^{\mathfrak{M}}$ on joukon $\mathrm{Dom}(\mathfrak{M})$ n-paikkainen relaatio, missä $n = \#(R)$.
5) Jokaisella $f \in \mathrm{Fun}(\tau)$ tulkinta $f^{\mathfrak{M}}$ on joukon $\mathrm{Dom}(\mathfrak{M})$ n-paikkainen funktio, missä $n = \#(f)$.

3.2. Esimerkki. $\mathcal{R} = \langle \mathbb{R}, +^{\mathbb{R}}, \cdot^{\mathbb{R}}, 0, 1, \leq^{\mathbb{R}} \rangle$ ja $\mathcal{Q} = \langle \mathbb{Q}, +^{\mathbb{Q}}, \cdot^{\mathbb{Q}}, 0, 1, \leq^{\mathbb{Q}} \rangle$ ovat molemmat aakkoston $\tau = \{+, \cdot, 0, 1, \leq\}$ malleja, missä $+$ ja $\cdot$ ovat kaksipaikkaisia funktiosymboleita, 0, 1 vakiosymboleita ja $\leq$ on kaksipaikkainen relaatiosymboli. Edellisen mallin $\mathcal{R}$ universumi on reaalilukujen joukko $\mathbb{R}$, jälkimmäisen mallin $\mathcal{Q}$ rationaalilukujen joukko $\mathbb{Q}$. Esimerkiksi symbolin $+$ tulkinta mallissa $\mathcal{R}$ on reaalilukujen yhteenlasku $+^{\mathcal{R}} = +^{\mathbb{R}}$. Kuten edellä mainittiin, aakkosto τ on kyseessä olevan mallin skemaattinen esitys, joka kertoo tietyt asiat mallin rakenteesta. Erityisesti mallien $\mathcal{R}$ ja $\mathcal{Q}$ samanaakkostoisuus merkitsee näiden mallien tietynlaista samanrakenteisuutta. Aakkosto τ ei kuitenkaan paljasta esimerkiksi sitä, että $+^{\mathcal{R}}$ ja $+^{\mathcal{Q}}$ ovat molemmat vaihdannaisia laskutoimituksia. Vaikka kyseessä olevat laskutoimitukset ovat symbolin $+$ tulkintoja, symboli $+$ on vain kaksipaikkainen funktiosymboli, jolla on hyvin epäsäännöllisiä tulkintoja muissa τ-malleissa.

Luvuissa I.1 – I.3 esitettyjen relaatioiden ja funktioiden käsitteiden avulla on helppoa tutustua erilaisiin usein diskreetissä matematiikassa ja algebrassa esiintyviin malleihin.

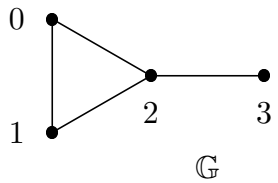
3.3. Määritelmä. Olkoon E kaksipaikkainen relaatiosymboli. *Verkolla* tarkoitetaan aakkoston $\{E\}$ mallia $\mathbb{G}$, jossa $E^{\mathbb{G}}$ on irrefleksiivinen ja symmetrinen relaatio. Universumin $\mathrm{Dom}(\mathbb{G})$ alkioita kutsutaan verkon *solmuiksi*, ja pareja $\{a, b\}$, missä $(a, b) \in E^{\mathbb{G}}$, *särmiksi*.

Huomautus. Äärellisessä verkossa $\mathbb{G}$ särmien lukumäärä on $\frac{1}{2}|E^{\mathbb{G}}|$ eli puolet särmärelaation koosta.

3.4. Esimerkki. Allaolevassa kuvassa on piirrettynä verkko $\mathbb{G} = \langle V, E \rangle$, missä $V = \mathrm{Dom}(\mathbb{G}) = \{0, 1, 2, 3\}$ on solmujen joukko ja

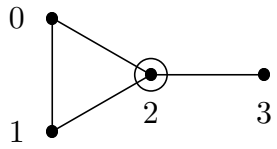
$$E^{\mathbb{G}} = \{(0,1), (1,0), (0,2), (2,0), (1,2), (2,1), (2,3), (3,2)\}.$$

Verkon $\mathbb{G}$ särmät ovat $\{0, 1\}$, $\{0, 2\}$, $\{1, 2\}$ ja $\{2, 3\}$.



$\mathbb{G}$

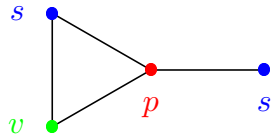
Verkkoteoriassa käsitellään usein mm. juurellisia verkkoja ja väritettyjä verkkoja. *Juurella* tarkoitetaan verkon yksilöityä solmua, kuten alla solmua 2.



$\mathbb{G}^*$

Luonnollinen tapa määritellä juurellinen verkko on siis seuraava: *Juurellisella verkolla* tarkoitetaan aakkoston $\{E, c\}$ mallia $\mathbb{G}^*$, missä c on vakiosymboli ja $\langle \mathrm{Dom}(\mathbb{G}^*), E^{\mathbb{G}^*} \rangle$ on verkko. Esimerkkitapauksessa $\mathrm{Dom}(\mathbb{G}^*) = \mathrm{Dom}(\mathbb{G}) = \{0, 1, 2, 3\}$, $E^{\mathbb{G}} = E^{\mathbb{G}^*}$ ja $c^{\mathbb{G}^*} = 2$.

Verkkoteoriassa tarkastellaan vuoroin solmujen, vuoroin särmien värityksiä. Kuvassa esimerkkiverkon solmut on väritetty kolmella värillä s (sininen), v (vihreä) ja p (punainen) niin, että kunkin särmän päätepisteet ovat erivärisiä.



$\mathcal{G}$

Solmujen väritys on kuvaus $\chi\colon \mathrm{Dom}(\mathbb{G}) \to \{s, v, p\}$, jolle $\chi(0) = s$, $\chi(1) = v$, $\chi(2) = p$ ja $\chi(3) = s$. Tieto värityksestä voidaan sisällyttää malliin muodostamalla aakkoston $\{E, S, V, P\}$ malli $\mathcal{G}$, missä S, V, P ovat yksipaikkaisia relaatiosymboleita, $\mathrm{Dom}(\mathcal{G}) = \mathrm{Dom}(\mathbb{G})$, $E^{\mathcal{G}} = E^{\mathbb{G}}$ sekä

$$\begin{aligned} S^{\mathcal{G}} &= \{\, a \in \mathrm{Dom}(\mathcal{G}) \mid \chi(a) = s \,\} = \{0, 3\} \quad \text{(siniset solmut)}\ , \\ V^{\mathcal{G}} &= \chi^{-1}[\{v\}] = \{1\} \quad \text{(vihreät solmut) ja} \\ P^{\mathcal{G}} &= \chi^{-1}[\{p\}] = \{2\} \quad \text{(punaiset solmut).} \end{aligned}$$

3.5. Määritelmä. Tyhjän aakkoston $\emptyset$ malleja kutsutaan *puhtaiksi* tai *pelkiksi joukoiksi*. Olkoon $\leq$ kaksipaikkainen relaatiosymboli. Aakkoston $\{\leq\}$ mallia $\mathfrak{M}$ kutsutaan *lineaarijärjestetyksi joukoksi*, jos $\leq^{\mathfrak{M}}$ on mallin universumin $\mathrm{Dom}(\mathfrak{M})$ lineaarijärjestys. Vastaavasti määritellään *osittaisesti järjestetty joukko*ja niin edelleen.

Äärellisten mallien teorian yhteys tietojenkäsittelyn teoriaan syntyy sitä kautta, että relaatiotietokannat ovat pelkistetyssä muodossaan äärellisiä malleja.

3.6. Esimerkki. Olkoon X kaikkien Pähkinänsaaren rauhan jälkeen syntyneiden suomalaisten joukko. Muodostetaan malli, jossa voidaan puhua suomalaisten välisistä sukulaisuussuhteista. (Tämä vastaa täysin ohjelman tietorakenteen suunnittelua.) Kiinnitetään aakkostoksi $\tau = \{\ddot{a}, i, \female, \male\}$, missä yksipaikkaisten funktioiden $\ddot{a}$ ja i on tarkoitus viitata vanhempiin ja yksipaikkaisten relaatioisymboleiden $\female$ ja $\male$ sukupuoleen. Määritellään τ-malli $\mathfrak{M}$ seuraavasti:

$$\mathrm{Dom}(\mathfrak{M}) = X, \text{ jonka tiedetään olevan epätyhjä,}$$

$$\ddot{a}^{\mathfrak{M}}\colon X \to X, \quad \ddot{a}^{\mathfrak{M}}(x) = \begin{cases} y, & \text{missä } y \text{ on } x\text{:n äiti, jos } y \in X \\ x, & \text{muuten.} \end{cases}$$

$$i^{\mathfrak{M}}\colon X \to X, \quad i^{\mathfrak{M}}(x) = \begin{cases} z, & \text{missä } z \text{ on } x\text{:n isä, jos } z \in X \\ x, & \text{muuten.} \end{cases}$$

$$\text{♀}^{\mathfrak{M}} \text{ on naispuolisten joukon } X \text{ alkioiden joukko}$$

ja

$$\text{♂}^{\mathfrak{M}} \text{ on miespuolisten joukon } X \text{ alkioiden joukko.}$$

Koska funktiosymbolin tulkinnan on aina oltava funktio, yllä on tehty se myönnytys luonnollisille tulkinnoille, että $\ddot{a}^{\mathfrak{M}}(x) = x$ tai $i^{\mathfrak{M}}(x) = x$, kun jompikumpi vanhemmista ei ole suomalainen tai on syntynyt ennen Pähkinänsaaren rauhaa.

3.7. Määritelmä. Mallin $\mathfrak{M}$ *mahtavuus* $\operatorname{card}(\mathfrak{M})$ on perusjoukon $\operatorname{Dom}(\mathfrak{M})$ koko eli $\operatorname{card}(\mathfrak{M}) = |\operatorname{Dom}(\mathfrak{M})|$. Malli $\mathfrak{M}$ on *äärellinen*, jos $\operatorname{card}(\mathfrak{M}) \in \mathbb{N}$ (eli oikeastaan $\operatorname{card}(\mathfrak{M}) \in \mathbb{Z}_+$, koska aina $\operatorname{Dom}(\mathfrak{M}) \neq \emptyset$).

Jatkossa huomio keskittyy äärellisiin malleihin, mutta äärettömiäkin käytetään esimerkkeinä, jos se on tarpeen.

Algebrasta löytyy runsaasti esimerkkejä malleista, joista tässä otetaan esille vain yksi tyyppi.

3.8. Määritelmä. Kiinnitetään kaksipaikkainen funktiosymboli $*$, ryhmälaskutoimituksen symboli. Aakkoston $\{*\}$ mallia $\mathbb{G}$ kutsutaan *ryhmäksi*, jos laskutoimitus $*^{\mathbb{G}}$ on liitännäinen, sillä on neutraalialkio ja jokaisella $x \in \operatorname{Dom}(\mathbb{G})$ on käänteisalkio.

3.9. Esimerkki. Olkoon $n \in \mathbb{Z}_+$. Algebran peruskursseilla tutustutaan ryhmiin $\mathfrak{Z}_n$, missä $\operatorname{Dom}(\mathfrak{Z}_n) = \{0, \ldots, n-1\}$ ja $*^{\mathfrak{Z}_n}$ on yhteenlasku modulo n: kun $a, b \in \{0, \ldots, n-1\}$,

$$a *^{\mathfrak{Z}_n} b = \begin{cases} a + b & \text{jos } a + b < n \\ a + b - n & \text{muuten.} \end{cases}$$

4. Homomorfismit

Yksi koko matematiikan läpi tunkeutuvista teemoista on matemaattisten objektien samanlaisuuden ja samankaltaisuuden tarkastelu. Yksinkertaisin esimerkki samanlaisuudesta on lukujen yhtäsuuruus, mutta koulugeometriassakin esiintyy monimuotoisempia samanlaisuuden ja samankaltaisuuden käsitteitä: yhtenevyys ja yhdenmuotoisuus. Matemaattisten objektien samanlaisuuden käsitettä kutsutaan monilla matematiikan aloilla isomorfismiksi, mutta poikkeuksiakin on, esimerkiksi topologisten avaruuksien homeomorfismi.

Koska usein on kyse erittäin monimutkaisista matemaattisista olioista, isomorfismin käsite itse asiassa selittää, mitkä olion piirteet ovat olennaisia piirteitä ja mitkä vain olion esittämisen takia mukaan tulevia ylimääräisiä seikkoja. Samanlaisuuden järjestelmällinen tutkimus johtaa erilaisiin isomorfismikriteereihin, luokittelutuloksiin

ja muihin senkaltaisiin tuloksiin. Koska isomorfismi on kahden matemaattisen olion vertaamiseen varsin mustavalkoinen menetelmä – oliothan joko ovat tai eivät ole isomorfisia – kuvaa täydennetään erilaisilla ekvivalensseilla, joihin saattaa liittyä mitta siitä, miten samankaltaisista olioista on kyse. Tällainen samankaltaisuuden käsite on esimerkiksi metristen avaruuksien L-bilipschitzekvivalenssi.

Tässä luvussa esitellään peruskäsitteet mallien homomorfismi ja isomorfismi, kun taas seuraavassa osassa vertailumenetelmiä kehitetään edelleen.

4.1. Määritelmä. Olkoot $\mathfrak{A}$ ja $\mathfrak{B}$ saman aakkoston τ malleja, sekä $h\colon \mathrm{Dom}(\mathfrak{A}) \to \mathrm{Dom}(\mathfrak{B})$ kuvaus. Kuvaus h on *homomorfismi* mallista $\mathfrak{A}$ malliin $\mathfrak{B}$, jos h toteuttaa seuraavat homomorfiaehdot:

1) Jokaisella $c \in \mathrm{Con}(\tau)$ pätee $h(c^{\mathfrak{A}}) = c^{\mathfrak{B}}$,

2) Kun $R \in \mathrm{Rel}(\tau)$, $\#(R) = n$ ja $(a_0, \ldots, a_{n-1}) \in R^{\mathfrak{A}}$, niin $(h(a_0), \ldots, h(a_{n-1})) \in R^{\mathfrak{B}}$.

3) Kun $f \in \mathrm{Fun}(\tau)$, $\#(f) = n$ ja $(a_0, \ldots, a_{n-1}) \in \mathrm{Dom}(\mathfrak{A})^n$, niin $h(f^{\mathfrak{A}}(a_0, \ldots, a_{n-1})) = f^{\mathfrak{B}}(h(a_0), \ldots, h(a_{n-1}))$.

Kuvaus h on *vahva homomorfismi* mallista $\mathfrak{A}$ malliin $\mathfrak{B}$, jos ehto 2 on voimassa seuraavassa vahvennetussa muodossa:

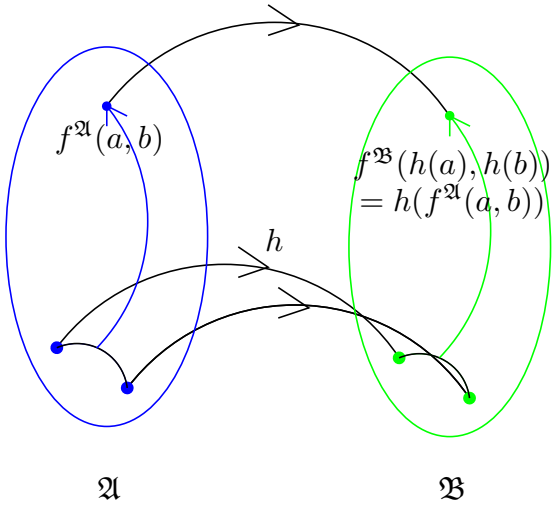
2′) Kun $R \in \mathrm{Rel}(\tau)$, $\#(R) = n$ ja $(a_0, \ldots, a_{n-1}) \in \mathrm{Dom}(\mathfrak{A})^n$, niin

$$(a_0, \ldots, a_{n-1}) \in R^{\mathfrak{A}} \iff (h(a_0), \ldots, h(a_{n-1})) \in R^{\mathfrak{B}}.$$

h on *upotus*, jos se on vahva homomorfismi ja injektio. h on mallien $\mathfrak{A}$ ja $\mathfrak{B}$ välinen *isomorfismi*, $h\colon \mathfrak{A} \cong \mathfrak{B}$, jos $h\colon \mathrm{Dom}(\mathfrak{A}) \to \mathrm{Dom}(\mathfrak{B})$ on vahva homomorfismi ja bijektio. Tällöin mallien $\mathfrak{A}$ ja $\mathfrak{B}$ sanotaan olevan *isomorfisia*, $\mathfrak{A} \cong \mathfrak{B}$. Isomorfismeja $h\colon \mathrm{Dom}(\mathfrak{A}) \to \mathrm{Dom}(\mathfrak{A})$ kutsutaan *automorfismeiksi*.

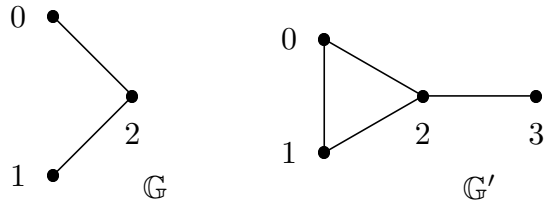
Intuitio isomorfismista on siis, että mallit $\mathfrak{A}$ ja $\mathfrak{B}$ ovat isomorfiset, jos mallin $\mathfrak{B}$ saa mallista $\mathfrak{A}$ vaihtamalla jokaisella $a \in \mathrm{Dom}(\mathfrak{A})$ alkion a alkioksi $h(a)$ (jollakin $h\colon \mathrm{Dom}(\mathfrak{A}) \to \mathrm{Dom}(\mathfrak{B})$). Tämä intuitio tekee homomorfiaehdot 1, 2′ ja 3 hyvin luonteviksi. Seuraava kuva havainnollistaa tapausta, missä f on kaksipaikkainen funktiosym-

boli.



Ajatus alkioiden vaihtamisesta johtaa relaatiosymboleiden kohdalla luonnostaan homomorfiaehtoon $2'$ eikä 2. Heikompi ehto 2 on kuitenkin monella tavalla käyttökelpoinen.

4.2. Esimerkki. Tarkastellaan verkkoja $\mathbb{G}$ ja $\mathbb{G}'$:



Kuvaus $i\colon \{0,1,2\} \to \{0,1,2,3\}$, $i(x) = x$ on homomorfismi, sillä relaatiosymboli E on mallien $\mathbb{G}$ ja $\mathbb{G}'$ aakkoston ainoa symboli ja homomorfiaehto 2 on voimassa: Kun $(a,b) \in E^{\mathbb{G}}$, niin $\{a,b\} = \{0,2\}$ tai $\{a,b\} = \{1,2\}$, ja koska $\{i(a), i(b)\} = \{a,b\}$ on myös verkon $\mathbb{G}'$ särmä, pätee $(i(a), i(b)) = (a,b) \in E^{\mathbb{G}'}$. Kuvaus i on myös injektio, mutta ei kuitenkaan upotus, koska i ei ole vahva homomorfismi: $(0,1) \notin E^{\mathbb{G}}$, mutta $(i(0), i(1)) = (0,1) \in E^{\mathbb{G}'}$.

Kuvaus $h\colon \{0,1,2\} \to \{0,1,2,3\}$, $h(0) = h(1) = 0$, $h(2) = 2$, on esimerkki homomorfismista, joka ei ole injektio ($h(0) = h(1)$, vaikka $0 \neq 1$). Kun $(a,b) \in E^{\mathbb{G}}$, niin nimittäin $\{a,b\} = \{0,2\}$ tai $\{a,b\} = \{1,2\}$, joten $\{h(a), h(b)\} = \{0,2\}$ ja siis $(h(a), h(b)) \in E^{\mathbb{G}'}$. Homomorfismi h on myös vahva, sillä jos $a, b \in \{0,1,2\}$ ja $(a,b) \notin E^{\mathbb{G}}$, niin $\{a,b\} = \{0,1\}$ tai $\{a,b\}$ on yksiö, ja kummassakin tapauksessa $\{h(a), h(b)\}$ on yksiö, joten verkossa $\mathbb{G}'$ pätee $(h(a), h(b)) \notin E^{\mathbb{G}'}$.

Verkon $\mathbb{G}$ voi upottaa verkkoon $\mathbb{G}'$ kuvauksella $j\colon \{0,1,2\} \to \{0,1,2,3\}$, $j(0) = 0$, $j(1) = 3$ ja $j(2) = 2$. Kuvaus j on nimittäin selvästi injektio, ja koska $\mathbb{G}$ ja $\mathbb{G}'$ ovat molemmat verkkoja, riittää tarkastaa seuraavat tapaukset:

$$(0,2) \in E^{\mathbb{G}} \text{ ja } (j(0), j(2)) = (0,2) \in E^{\mathbb{G}'},$$

$$(1,2) \in E^{\mathbb{G}} \text{ ja } (j(1), j(2)) = (3,2) \in E^{\mathbb{G}'}$$

sekä

$$(0,1) \notin E^{\mathbb{G}} \text{ ja } (j(0), j(1)) = (0,3) \notin E^{\mathbb{G}'}.$$

Verkot $\mathbb{G}$ ja $\mathbb{G}'$ eivät selvästikään ole isomorfisia. Helpoiten tämän voi perustella sillä, että $\mathbb{G}$ on kolmen ja $\mathbb{G}'$ neljän solmun verkko, joten ei ole olemassa edes bijektiota $f\colon \mathrm{Dom}(\mathbb{G}) \to \mathrm{Dom}(\mathbb{G}')$.

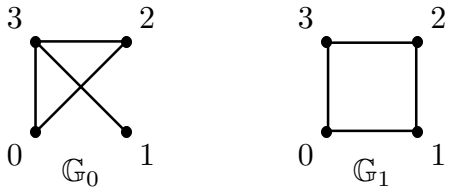
Käsitellään kevyesti isomorfiaan liittyvää kysymystä mallien luokittelusta. Välttämätön edellytys sille, että saman aakkoston τ äärelliset mallit $\mathfrak{A}$ ja $\mathfrak{B}$ ovat isomorfiset, on tietysti, että on ylipäätänsä olemassa bijektio $f\colon \mathrm{Dom}(\mathfrak{A}) \to \mathrm{Dom}(\mathfrak{B})$ eli $\mathrm{card}(\mathfrak{A}) = \mathrm{card}(\mathfrak{B})$. Jos $\tau = \emptyset$, eli $\mathfrak{A}$ ja $\mathfrak{B}$ ovat pelkkiä joukkoja, tämä riittääkin, sillä silloin jokainen bijektio $f\colon \mathrm{Dom}(\mathfrak{A}) \to \mathrm{Dom}(\mathfrak{B})$ on automaattisesti myös isomorfismi. Yleisessä tapauksessa ei kuitenkaan mikään tällainen yksinkertainen laskentaperiaate riitä.

4.3. Esimerkki.

a) Kahden solmun verkoille $\mathbb{G}$ ja $\mathbb{G}'$ (alla)

pätee $\mathrm{card}(\mathbb{G}) = \mathrm{card}(\mathbb{G}') = 2$, mutta $\mathbb{G} \ncong \mathbb{G}'$. On nimittäin helppoa havaita, että verkkojen isomorfismi säilyttää paitsi solmujen, myös särmien lukumäärän, ja että verkossa $\mathbb{G}'$ on yksi, mutta verkossa $\mathbb{G}$ ei lainkaan särmiä.

b) Osoitetaan, että on olemassa epäisomorfiset verkot, joissa on yhtä monta solmua ja yhtä monta särmää. Tarkastellaan alla olevia verkkoja $\mathbb{G}_0$ ja $\mathbb{G}_1$:



Kummassakin on neljä solmua ja neljä särmää. Olkoon $f\colon \{0,1,2,3\} \to \{0,1,2,3\}$, mielivaltainen bijektio ja $a = f(3)$. Solmun 3 aste verkossa $\mathbb{G}_0$ on 3 eli $\deg(3) = \big|\{\, x \mid (3,x) \in E^{\mathbb{G}_0} \,\}\big| = 3$. Solmun a aste verkossa $\mathbb{G}_1$ on joka tapauksessa 2. Siis on olemassa sellainen $x \in \{0,1,2\}$, että $(3,x) \in E^{\mathbb{G}_0}$, mutta $(f(3), f(x)) = (a, f(x)) \notin E^{\mathbb{G}_1}$, toisin sanoen f ei ole isomorfismi. Siis $\mathbb{G}_0 \ncong \mathbb{G}_1$.

Jos rajoitutaan sopiviin malliluokkiin, on kuitenkin olemassa kiinnostavia tapauksia, joissa mallin mahtavuus riittää karakterisoimaan mallin isomorfiatyypin. Tunnettu algebrallinen esimerkki on äärelliset kunnat: äärelliset kunnat $\mathbb{F}$ ja $\mathbb{F}'$ ovat isomorfiset täsmälleen silloin, kun ne ovat yhtä mahtavat. Tässä tyydymme vaatimattomampaan, mutta jatkon kannalta oleelliseen esimerkkiin.

4.4. Lause. *Kun $n \in \mathbb{Z}_+$, merkitään $\mathfrak{L}_n$:llä lineaarijärjestettyä joukkoa, jonka universumi on $\{0, \ldots, n-1\}$ ja jossa $\leq^{\mathfrak{L}_n}$ on universumin luonnollinen järjestys. Tällöin jokaista äärellistä lineaarijärjestettyä joukkoa $\mathfrak{B}$ vastaavat yksikäsitteiset $n \in \mathbb{Z}_+$ ja f, joille $f\colon \mathfrak{L}_n \cong \mathfrak{B}$.*

Todistus. Koska jokaisella $n \in \mathbb{Z}_+$ pätee $\mathrm{card}(\mathfrak{L}_n) = n$, riittää osoittaa, että on olemassa yksikäsitteinen $f\colon \mathfrak{L}_n \cong \mathfrak{B}$, missä $n = \mathrm{card}(\mathfrak{B})$. Osoitetaan ensin isomorfismin olemassaolo: Määritellään rekursiivisesti, että $f(k)$ on joukon $\mathrm{Dom}(\mathfrak{B}) \setminus \{f(0), \ldots, f(k-1)\}$ pienin alkio järjestyksen $\leq^{\mathfrak{B}}$ suhteen, kun $k = 0, \ldots, n-1$. Koska $n = \mathrm{card}(\mathfrak{B}) = \mathrm{card}(\mathfrak{L}_n)$, tällainen f on tietenkin bijektio. Vahva homomorfisuus seuraa myös helposti: Olkoon $k, \ell \in \{0, \ldots, n-1\}$. Jos $k \leq \ell$, niin $f(k)$ on joukon $\mathrm{Dom}(\mathfrak{B}) \setminus \{f(0), \ldots, f(k-1)\} = \{f(k), \ldots, f(n-1)\}$ pienin alkio, joten $f(k) \leq f(\ell)$. Jos taas $k > \ell$ (eli $k \leq \ell$ ei pidä paikkansa), niin $k \geq \ell$ ja $k \neq \ell$, joten $f(k) \geq f(\ell)$ ja $f(k) \neq f(\ell)$ (edellisen päättelyn ja kuvauksen f injektiivisyyden nojalla), joten $f(k) > f(\ell)$. Siis $f\colon \mathfrak{L}_n \cong \mathfrak{B}$.

Olkoon $g\colon \mathfrak{L}_n \cong \mathfrak{B}$. Koska $f^{-1}\colon \mathfrak{B} \cong \mathfrak{L}_n$, saadaan $f^{-1} \circ g\colon \mathfrak{L}_n \cong \mathfrak{L}_n$. Bijektioiden yhdistettynä kuvauksena $f^{-1} \circ g$ on bijektio eli joukon $\{0, \ldots, n-1\}$ permutaatio. Jos $f^{-1} \circ g \neq \mathrm{id}_{\{0,\ldots,n-1\}}$, niin joillakin $k, \ell \in \{0, \ldots, n-1\}$, $k < \ell$, pätee $(f^{-1} \circ g)(k) > \ell$, mikä on ristiriidassa sen kanssa, että $f^{-1} \circ g$ on isomorfismi. Siis $f^{-1} \circ g = \mathrm{id}_{\{0,\ldots,n-1\}}$ eli $f = g$, joten f on yksikäsitteinen. □

4.5. Määritelmä. Mallia $\mathfrak{M}$ kutsutaan *järjestetyksi malliksi*, jos mallin $\mathfrak{M}$ aakkostossa on kaksipaikkainen relaatiosymboli $\leq$, jonka tulkinta on perusjoukon $\mathrm{Dom}(\mathfrak{M})$ lineaarijärjestys.

4.6. Seuraus. Jokaista järjestettyä mallia $\mathfrak{M}$ vastaa yksikäsitteinen $\mathfrak{M}^* \cong \mathfrak{M}$, jolle $\mathrm{Dom}(\mathfrak{M}^*) = \{0, \ldots, n-1\}$ jollakin $n \in \mathbb{Z}_+$ ja $\leq^{\mathfrak{M}^*}$ on joukon $\{0, \ldots, n-1\}$ luonnollinen järjestys.

Todistus. Konstruoidaan ensin $\mathfrak{M}^*$, ja osoitetaan tämän jälkeen sen yksikäsitteisyys. Merkitään $M = \mathrm{Dom}(\mathfrak{M})$ ja jokaisella $m \in \mathbb{Z}_+$ $\leq_m$:llä joukon $\{0, \ldots, m-1\}$ luonnollista järjestystä. Koska $\mathfrak{M}$ on järjestetty malli, $\langle M, \leq^{\mathfrak{M}} \rangle$ on lineaarijärjestetty joukko, ja edellisen lauseen mukaan $f\colon \langle M, \leq^{\mathfrak{M}} \rangle \cong \langle \{0, \ldots, n-1\}, \leq_n \rangle$ jollain $n \in \mathbb{Z}_+$ ja f. Olkoon τ mallin $\mathfrak{M}$ aakkosto. Kopioidaan mallin $\mathfrak{M}$ vakiot, relaatiot ja funktiot bijektion f välityksellä joukon $\{0, \ldots, n-1\}$ vakioiksi, relaatioiksi ja funktioiksi, toisin sanoen asetetaan

1) $c^{\mathfrak{M}^*} = f(c^{\mathfrak{M}})$, kun $c \in \mathrm{Con}(\tau)$,

2) $R^{\mathfrak{M}^*} = \{\, (f(a_0), \ldots f(a_{k-1})) \mid (a_0, \ldots, a_{k-1}) \in R^{\mathfrak{M}} \,\}$, kun $R \in \mathrm{Rel}(\tau)$ ja $k = \#(R)$ sekä

3) $g^{\mathfrak{M}^*}\colon M^k \to M$, $g^{\mathfrak{M}^*}(a_0, \ldots, a_{k-1}) = f(g^{\mathfrak{M}}(f^{-1}(a_0), \ldots, f^{-1}(a_{k-1})))$, kun $g \in \mathrm{Fun}(\tau)$ ja $k = \#(g)$.

Tällöin on selvää, että $f\colon \mathfrak{M} \cong \mathfrak{M}^*$ (eli $f^{-1}\colon \mathfrak{M}^* \cong \mathfrak{M}$), ja havaitaan myös, että $\leq^{\mathfrak{M}^*} = \leq_n$, koska $f\colon \langle M, \leq^{\mathfrak{M}} \rangle \cong \langle \{0, \ldots, n-1\}, \leq_n \rangle$.

Oletetaan, että $g\colon \mathfrak{M} \cong \mathfrak{M}^{**}$ ja myös mallin $\mathfrak{M}^{**}$ universumi $\mathrm{Dom}(\mathfrak{M}^{**}) = \{0, \ldots, m-1\}$ jollakin $m \in \mathbb{Z}_+$ ja $\leq^{\mathfrak{M}^{**}} = \leq_m$. Tällöin $g\colon \langle M, \leq^{\mathfrak{M}} \rangle \cong \langle \{0, \ldots, m-1\}, \leq_m \rangle$ ja edellisen lauseen yksikäsitteisyydestä seuraa $m = n$ ja $f = g$. Siis $f\colon \mathfrak{M} \cong \mathfrak{M}^*$ ja $f\colon \mathfrak{M} \cong \mathfrak{M}^{**}$, mutta tästähän seuraa $\mathfrak{M}^* = \mathfrak{M}^{**}$. □

Edellistä tulosta voi pitää yksinkertaisena esityslauseena, toisin sanoen jokaisen järjestetyn mallin voi esittää luonnollisten lukujen alkupätkän päälle rakennettuna mallina. Järjestetyillä malleilla on paljon merkitystä tietojenkäsittelyteoreettisissa tarkasteluissa, sillä tietorakenteet joutuu perimmiltään käytännössä aina esittämään sarjallisessa muodossa. Käsitteen tulisi oikeastaan olla "lineaarijärjestetty malli", mutta alkuosa "lineaari-" on jätetty pois, koska käsitettä tarvitaan usein.

Luvun johdantoalun mukaisessa hengessä nyt ruvetaan rakentamaan samankaltaisuuden käsitettä eli menetelmiä approksimoida isomorfismia. Oleellinen työkalu tässä on osittaisen isomorfismin käsite.

4.7. Määritelmä. Olkoon $\mathfrak{A}$ aakkoston τ malli ja $\sigma \subset \tau$.

a) Malli $\mathfrak{B}$ on mallin $\mathfrak{A}$ *rajoittuma* aakkostoon σ, $\mathfrak{B} = \mathfrak{A}{\restriction}\sigma$, jos $\mathfrak{B}$ on aakkoston σ malli, $\mathrm{Dom}(\mathfrak{B}) = \mathrm{Dom}(\mathfrak{A})$ ja kaikilla $X \in \sigma$ pätee $X^{\mathfrak{B}} = X^{\mathfrak{A}}$.

b) Malli $\mathfrak{C}$ on mallin $\mathfrak{A}$ *alimalli*, jos mallin $\mathfrak{C}$ aakkosto on myös τ, $\mathrm{Dom}(\mathfrak{C}) \subset \mathrm{Dom}(\mathfrak{A})$, sekä

1) kaikilla $c \in \mathrm{Con}(\tau)$ on voimassa $c^{\mathfrak{C}} = c^{\mathfrak{A}}$,

2) kun $R \in \mathrm{Rel}(\tau)$, $\#(R) = k$, niin $R^{\mathfrak{C}} = R^{\mathfrak{A}} \cap \mathrm{Dom}(\mathfrak{C})^k$,

ja

3) kun $f \in \mathrm{Fun}(\tau)$, $\#(f) = k$, niin $f^{\mathfrak{C}} = f^{\mathfrak{A}} \restriction \mathrm{Dom}(\mathfrak{C})^k$.

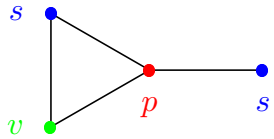
Kun $C = \mathrm{Dom}(\mathfrak{C})$, tätä merkitään myös $\mathfrak{C} = \mathfrak{A}|C$, ja mallin $\mathfrak{C}$ sanotaan olevan mallin $\mathfrak{A}$ *suhteellistuma* joukkoon C.

Rajoittuma ja suhteellistuma eli alimalli vastaavat siis kahta aivan erilaista tapaa supistaa mallia: mallista voi poistaa joko kokonaisia tulkintoja tai alkioita.

4.8. Esimerkki.

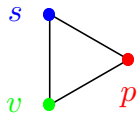
a) Reaalilukujen järjestelmällä $\mathfrak{R} = \langle \mathbb{R}, +^{\mathbb{R}}, \cdot^{\mathbb{R}}, 0, 1, \leq^{\mathbb{R}} \rangle$ on kaksi luonnollista rajoittumaa, yhteenlaskuryhmä $\mathfrak{R}{\restriction}\{+\} = \langle \mathbb{R}, +^{\mathbb{R}} \rangle$ ja monoidi $\mathfrak{R}{\restriction}\{\cdot\} = \langle \mathbb{R}, \cdot^{\mathbb{R}} \rangle$. Kertolaskuryhmän saa jälkimmäisestä mallista poistamalla nollan eli kertolaskuryhmä on $(\mathfrak{R}{\restriction}\{\cdot\})|(\mathbb{R} \setminus \{0\}) = \langle \mathbb{R}^*, \cdot^{\mathbb{R}^*} \rangle$.

b) Tarkastellaan esimerkin 3.4 väritettyä verkkoa $\mathcal{G} \in \mathrm{Str}(\{E, S, V, P\})$.



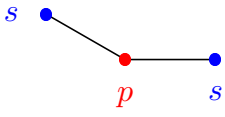
$\mathcal{G}$

Tällä on neljä kolmialkioista alimallia, nimittäin suhteellistumat joukkoihin $\{0, 1, 2\}$, $\{0, 1, 3\}$, $\{0, 2, 3\}$ ja $\{1, 2, 3\}$.

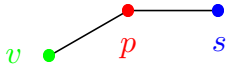


$\mathcal{G}|\{0, 1, 2\}$

$\mathcal{G}|\{0, 1, 3\}$

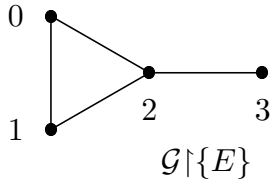


$\mathcal{G}|\{0, 2, 3\}$



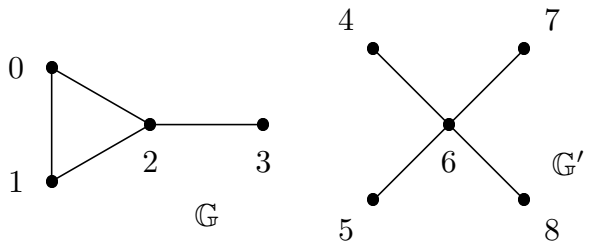
$\mathcal{G}|\{1, 2, 3\}$

Värittämätön verkko saadaan sen sijaan rajoittumana $\mathcal{G}|\{E\}$.



4.9. Määritelmä. Olkoot $\mathfrak{A}$ ja $\mathfrak{B}$ samanaakkostoisia malleja. *Osittaisella isomorfismilla* p mallista $\mathfrak{A}$ malliin $\mathfrak{B}$ tarkoitetaan isomorfismia $p\colon \mathfrak{A}' \cong \mathfrak{B}'$, missä $\mathfrak{A}'$ on mallin $\mathfrak{A}$ ja $\mathfrak{B}'$ mallin $\mathfrak{B}$ alimalli, tai erityistapauksena osittaiseksi isomorfismiksi hyväksytään tyhjä kuvaus $\emptyset$, jos mallien $\mathfrak{A}$ ja $\mathfrak{B}$ yhteisessä aakkostossa ei ole vakiosymboleita. $\mathrm{Part}(\mathfrak{A}, \mathfrak{B})$ on kaikkien niiden kuvausten joukko, jotka ovat osittaisia isomorfismeja mallista $\mathfrak{A}$ malliin $\mathfrak{B}$.

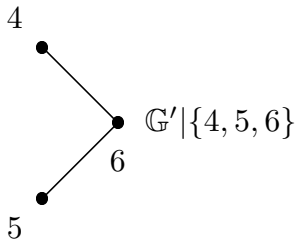
4.10. Esimerkki. Tarkastellaan kuvan verkkoja $\mathbb{G}$ ja $\mathbb{G}'$.



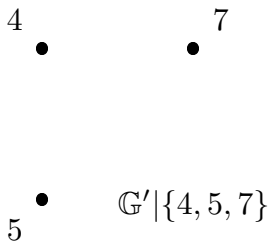
Määritetään jatkoa varten kaikki osittaiset isomorfismit $p \in \mathrm{Part}(\mathbb{G}, \mathbb{G}')$. Osittaisen isomorfismin määritelmän mukaan $\emptyset \in \mathrm{Part}(\mathbb{G}, \mathbb{G}')$. Koska yksisolmuiset verkot ovat kaikki isomorfisia, $\{(a, b)\} \in \mathrm{Part}(\mathbb{G}, \mathbb{G}')$ kaikilla $a \in \mathrm{Dom}(\mathbb{G}) = \{0, 1, 2, 3\}$ ja $b \in \mathrm{Dom}(\mathbb{G}') = \{4, 5, 6, 7, 8\}$, toisin sanoen jokainen vain yhdelle alkiolle määritetty kuvaus p, jolle $b = p(a) \in \{4, 5, 6, 7, 8\}$, on osittainen isomorfismi $\mathbb{G}$:stä $\mathbb{G}'$:uun. Näitä on $4 \cdot 5 = 20$ kappaletta.

Kaksialkioisten verkkojen isomorfiatyyppejä on kaksi, särmätön ja särmällinen. Edellisiä vastaavat ne $2 \cdot 2 \cdot 6 = 24$ kuvausta $\{(a, b), (c, d)\}$, missä $a \in \{0, 1\}$, $c = 3$ ja $\{b, d\} \subset \{4, 5, 7, 8\}$, $b \neq d$, jälkimmäisiä ne $2 \cdot 4 \cdot 4 = 32$ kuvausta $p = \{(a, b), (c, d)\}$, missä $\{a, c\}$ on $\mathbb{G}$:n ja $\{b, d\}$ on $\mathbb{G}'$:n särmä.

Olkoon $B \subset \mathrm{Dom}(\mathbb{G}')$ kolmialkioinen joukko. Havaitaan, että jos $6 \in B$, niin $\mathbb{G}'|B \cong \mathbb{G}'|\{4, 5, 6\}$,



ja jos $6 \notin B$, niin $\mathbb{G}'|B \cong \mathbb{G}'|\{4,5,7\}$.



$\mathbb{G}'|\{4,5,7\}$

Verkolla $\mathbb{G}$ ei ole alimalleja, jotka olisivat verkon $\mathbb{G}'|\{4,5,7\}$ kanssa isomorfisia (vrt. edelliseen esimerkkiin), ja verkon $\mathbb{G}'|\{4,5,6\}$ kanssa isomorfiset $\mathbb{G}$:n alimallit ovat $\mathbb{G}|\{0,2,3\}$ ja $\mathbb{G}|\{1,2,3\}$. Kun siis $A = \{a,2,3\}$ ja $B = \{b,6,b'\}$, missä $a \in \{0,1\}$, $\{b,b'\} \subset \{4,5,7,8\}$ ja $b \neq b'$, niin $p\colon A \to B$, $p(2) = 6$, $\{p(a),p(3)\} = \{b,b'\}$ ovat osittaisia isomorfismeja. Muita osittaisia isomorfismeja ei ole, sillä verkolla $\mathbb{G}'$ ei ole alimalleja, jotka olisivat isomorfisia neljän solmun verkon $\mathbb{G}$ kanssa.

Harjoituksia osaan I

1. Näytä, että refleksiivisyyden, symmetrisyyden ja transitiivisyyden välillä ei ole seuraavassa mielessä mitään yksinkertaisia riippuvuussuhteita: Olkoon $X = \{a, b, c\}$ kolmen alkion joukko. Tällöin on olemassa sellaiset joukon X kaksipaikkaiset relaatiot

$$R_{+++}, R_{++-}, R_{+-+}, R_{+--}, R_{-++}, R_{-+-}, R_{--+}, R_{---},$$

että R_{+++} on refleksiivinen, symmetrinen ja transitiivinen, R_{++-} on refleksiivinen, symmetrinen, mutta epätransitiivinen, ..., R_{---} ei ole refleksiivinen, ei symmetrinen eikä transitiivinen.

2. Olkoon $X \subset \mathbb{R}^2$ neljän tason pisteen joukko, ja

$$V = \{\, (x, y, z) \in X^3 \mid y \text{ on } x\text{:n ja } z\text{:n välissä samalla suoralla} \,\}.$$

Kuinka suuri $|V|$ voi olla, ts. kuinka monta kolmikkoa relaatiossa V voi olla?

3. Esitä esimerkki äärellisen joukon esijärjestyksestä, joka ei ole osittainen järjestys eikä esilineaarijärjestys.

4. Tutki kustakin väitteestä, pitääkö se paikkansa kaikilla relaatioilla R, S ja T.

a) $R \circ R \subset R$.
b) $(R^{-1} \circ S^{-1})^{-1} \circ R^{-1} = S$.
c) $(R \circ S) \cup (S \circ T) \subset (R \cup S) \circ (S \cup T)$.

5. Olkoon X äärellinen n alkion joukko, $r(n)$ kaikkien, $s(n)$ symmetristen ja $a(n)$ antisymmetristen joukon X kaksipaikkaisten relaatioiden lukumäärä. Määritä $r(n)$, $s(n)$ ja $a(n)$ sekä laske $\lim_{n\to\infty} a(n)/s(n)$.

6. Olkoon R kuusialkioisen joukon X symmetrinen relaatio. Todista, että on olemassa eri alkiot $x, y, z \in X$, joille joko

$$(x, y) \in R,\ (y, z) \in R \text{ ja } (z, x) \in R$$

tai

$$(x, y) \notin R,\ (y, z) \notin R \text{ ja } (z, x) \notin R.$$

Osoita esimerkin avulla, että tulos ei pidä paikkaansa ilman symmetrisyyttä.

7. Osoita, että jokaista $n \in \mathbb{Z}_+$ kohti on olemassa sellainen $k \in \mathbb{Z}_+$, että seuraava ehto on voimassa. Olkoon R n-alkioisen joukon X kaksipaikkainen relaatio. Tällöin $\mathrm{TC}(R) = \bigcup_{j=1}^{k} R^j$.

8. Olkoon f äärellisen joukon X permutaatio ja $R = \mathrm{TC}(f)$ (yksipaikkainen funktio on joukko-opillisesti kaksipaikkainen relaatio, joten merkintä on mielekäs). Millainen relaatio R on?: Onko se jotain kurssilla esitettyä tyyppiä? Miten R suhtautuu funktioon f?

9. Olkoon $X = \{a, b, c\}$ kolmen alkion joukko.
a) Mikä on joukon X eri laskutoimitusten lukumäärä?
b) Kuinka moni näistä laskutoimituksista on vaihdannainen?
c) Kuinka moni näistä laskutoimituksista on vaihdannainen ja liitännäinen?
(Vihje: erilaiset symmetriat helpottavat laskemista. Esim. $(a * b) * c$ on jokin alkioista a, b tai c.)

10. Olkoon X joukko ja S joukon X äärellisten epätyhjien osajoukkojen joukko. Osoita, että joukon X vaihdannaiseen ja liitännäiseen laskutoimitukseen $*$ voidaan liittää kuvaus $\Pi\colon S \to X$ (*äärellisten joukkojen tulo*), jolle
1° Kaikilla $a \in X$ pätee $\Pi(\{a\}) = a$.
2° Kaikilla erillisillä $A, B \in S$ pätee $\Pi(A \cup B) = \Pi(A) * \Pi(B)$.
Voisiko tällainen Π olla olemassa, vaikka laskutoimitus $*$ ei olisi vaihdannainen tai ei olisi liitännäinen?

11. Kun $k \in \mathbb{Z}_+$, olkoon $r_k(n)$ joukon $\{0, \ldots, n-1\}$ k-paikkaisten relaatioiden ja $f_k(n)$ k-paikkaisten funktioiden lukumäärä. Osoita, että

$$\lim_{n\to\infty} f_k(n)/r_k(n) = \infty \text{ ja } \lim_{n\to\infty} r_{k+1}(n)/f_k(n) = \infty.$$

12. Olkoot X ja F äärellisiä joukkoja, joissa on vähintään kaksi alkiota. Liitetään jokaiseen joukon X väritykseen $\chi\colon X \to F$ kaksi mallia: Mallin $\mathfrak{A}(\chi)$ aakkosto on $\tau = \{\, U_c \mid c \in F \,\}$, missä relaatiot U_c, $c \in F$, ovat yksipaikkaisia. Mallin $\mathfrak{B}(\chi)$ aakkosto on $\sigma = \{E\}$, missä E on kaksipaikkainen. Kummankin mallin universumi on X. Mallissa $\mathfrak{A}(\chi)$ pätee

$$U_c^{\mathfrak{A}(\chi)} = \chi^{-1}(\{c\}),$$

kun $c \in F$, ja mallissa $\mathfrak{B}(\chi)$ on voimassa

$$E^{\mathfrak{B}(\chi)} = \{\, (x, y) \in X \times X \mid \chi(x) = \chi(y) \,\}.$$

a) Osoita, että $E^{\mathfrak{B}(\chi)}$ on ekvivalenssirelaatio kaikilla värityksillä $\chi\colon X \to F$.
b) Osoita, että kaikilla eri $\chi, \chi'\colon X \to F$ pätee $\mathfrak{A}(\chi) \neq \mathfrak{A}(\chi')$, mutta on olemassa sellaiset eri väritykset $\chi, \chi' : X \to F$, että $\mathfrak{B}(\chi) = \mathfrak{B}(\chi')$.
c) Osoita, että on olemassa sellaiset eri väritykset $\chi, \chi'\colon X \to F$, että $\mathfrak{A}(\chi) \cong \mathfrak{A}(\chi')$.

13. Osoita, että jokainen äärellinen malli $\mathfrak{A}$ on isomorfinen jonkin sellaisen mallin $\mathfrak{B}$, jonka universumi on $\{0, \ldots, n-1\}$ jollakin $n \in \mathbb{Z}_+$, kanssa.

14. Olkoon τ äärellinen aakkosto. Osoita, että on olemassa sellainen polynomifunktio p, että mahtavuutta n olevia keskenään epäisomorfisia aakkoston τ-malleja on korkeintaan $2^{p(n)}$ kappaletta. Osoita, että jos τ on relationaalinen, niin polynomifunktio p voidaan valita niin, että näitä malleja on myös vähintään $2^{p(n)}/n!$ kappaletta.

15. Kutsutaan kuvausta I äärellisiltä verkoilta luonnollisille luvuille *verkkojen invariantiksi*, jos isomorfisille verkoille $\mathbb{G}$ ja $\mathbb{G}'$ pätee $I(\mathbb{G}) = I(\mathbb{G}')$. Olkoot $I_0, \ldots, I_k$ ($k \in \mathbb{N}$) verkkojen invariantteja. Oletetaan lisäksi, että on olemassa sellainen $s \in \mathbb{N}$, että kaikilla verkoilla $\mathbb{G}$ ja $i \in \{0, \ldots, k\}$ pätee $I_i(\mathbb{G}) \leq \mathrm{card}(\mathbb{G})^s$. Osoita, että tällöin invariantit eivät voi kuvata verkkoja isomorfiaa vaille, ts. on olemassa *epäisomorfiset* $\mathbb{G}$ ja $\mathbb{G}'$, joille $I_i(\mathbb{G}) = I_i(\mathbb{G}')$, kun $i \in \{0, \ldots, k\}$.

16. Määritä neljän solmun verkkojen isomorfismityyppien eli keskenään epäisomorfisten verkkojen lukumäärä. Luettele lisäksi nelisolmuisten kolmisärmäisten verkkojen väliset homomorfismit. Mitkä näistä ovat vahvoja?

17. Malli $\mathfrak{A}$ uppoaa malliin $\mathfrak{B}$, joka uppoaa edelleen malliin $\mathfrak{C}$. Osoita, että $\mathfrak{A}$ uppoaa malliin $\mathfrak{C}$.

18. Kun $n \in \mathbb{Z}_+$, mallien $\mathfrak{S}_n$ ja $\mathfrak{C}_n$ universumi on $\{0, \ldots, n-1\}$. Kaksipaikkaisen relaatiosymbolin S tulkinta $\{S\}$-mallissa $\mathfrak{S}_n$ olkoon seuraajarelaatio

$$S^{\mathfrak{S}_n} = \{\, (k, k+1) \mid k \in \{0, \ldots, n-2\} \,\}.$$

Yksipaikkaisen funktiosymbolin tulkinta $\{f\}$-mallissa $\mathfrak{C}_n$ on vastaavasti

$$f^{\mathfrak{C}_n} \colon \{0, \ldots, n\} \to \{0, \ldots, n\},\ f^{\mathfrak{C}_n}(k) = \begin{cases} k+1, & \text{kun } k \in \{0, \ldots, n-2\} \\ 0, & \text{kun } k = n-1. \end{cases}$$

Määritä, a) millä positiivisten kokonaislukujen pareilla (m, n) malli $\mathfrak{S}_m$ uppoaa malliin $\mathfrak{S}_n$ ja b) millä positiivisten kokonaislukujen pareilla (m, n) malli $\mathfrak{C}_m$ uppoaa malliin $\mathfrak{C}_n$.

19. Osoita, että jokainen äärellinen osittaisesti järjestetty joukko uppoaa luonnollisten lukujen jakojärjestykseen $\langle\, \mathbb{N}, \mid \,\rangle$.

20. Olkoon E kaksipaikkainen relaatiosymboli ja $A = \{0, 1, 2, 3, 4\}$. Tarkastellaan niitä aakkoston $\{E\}$ malleja $\mathfrak{A}$, joille $\mathrm{Dom}(\mathfrak{A}) = A$ ja $E^{\mathfrak{A}}$ on ekvivalenssirelaatio. Kuinka monta tällaista mallia $\mathfrak{A}$ on olemassa? Kuinka monta näitä on isomorfismia vaille? Millä näistä on eniten isomorfisia kopioita tarkasteltavassa luokassa?

II Pelit

Tässä osassa kehitetään vertailumenetelmiä melleille. Kahden mallin vertailu on yleensä mielekästä vain, jos mallit ovat samanaakkostoisia. Keskeisiä käsitteitä ovat samanlaisuuden käsitteenä toimiva ja edellisessä osassa esitelty

1) isomorfismi

sekä samankaltaisuutta mittaavat

2) osittainen isomorfismi asteeseen k saakka

ja

3) osittainen isomorfismi k muuttujan suhteen

ja näihin liittyvät Ehrenfeuchtin ja Fraïssén peli sekä helmipeli.

1. Ehrenfeuchtin ja Fraïssén peli

Vertaillaan kahta saman aakkoston τ mallia $\mathfrak{A}$ ja $\mathfrak{B}$ siinä mielessä, että haluttaisiin jollain tavalla mitata, kuinka samanlaisia ne ovat. Oletetaan yksinkertaisuuden vuoksi, että τ on *relationaalinen* eli $\mathrm{Rel}(\tau) = \tau$. Isomorfismi on tarkoitusta varten liian karkea, mutta tehdään silti seuraava ajatuskoe: Oletetaan, että kaksi tutkijaa, Akseli ja Elina, yrittävät selvittää, ovatko malli isomorfisia, mutta he ovat eri mieltä asiasta. Akselin mielestä $\mathfrak{A} \ncong \mathfrak{B}$, kun taas Elina uskoo, että $\mathfrak{A} \cong \mathfrak{B}$. Akseli toteaa, että Elinan pitäisi pystyä esittämään isomorfismi $f\colon \mathfrak{A} \cong \mathfrak{B}$ perustellakseen uskomustaan. Elina valittaa, että se olisi aivan liian työlästä, koska mallit ovat suuria, mutta esittää puolestaan, että häneltä voi kysyä funktion f arvoa missä tahansa pisteessä. Akseli tarkentaa, että koska f on bijektio, hän voi yhtä hyvin kysyä, mikä on alkion $a \in \mathrm{Dom}(\mathfrak{A})$ kuva $b = f(a) \in \mathrm{Dom}(\mathfrak{B})$ kuin toisin päin, mikä on alkion $b \in \mathrm{Dom}(\mathfrak{B})$ alkukuva $a = f^{-1}(b) \in \mathrm{Dom}(\mathfrak{A})$. Lisäksi hän vaatii, että hänen pitäisi voida esittää useampia kysymyksiä.

Seuraavaksi Akseli ja Elina sopivat, kuinka monta kysymystä k riittää vakuuttamaan Akselin. Akseli aloittaa kysymällä, miten $a_0 \in \mathrm{Dom}(\mathfrak{A})$ kuvautuu malliin $\mathfrak{B}$, ja Elina vastaa alkiolla $b_0 \in \mathrm{Dom}(\mathfrak{B})$, tai Akseli kysyy alkion $b_0 \in \mathrm{Dom}(\mathfrak{B})$ alkukuvaa $a_0 \in \mathrm{Dom}(\mathfrak{A})$. Molemmissa tapauksissa he tulevat valinneeksi parin $(a_0, b_0) \in \mathrm{Dom}(\mathfrak{A}) \times \mathrm{Dom}(\mathfrak{B})$. Seuraavalla Akselin kysymyksellä ja Elinan vastauksella he valitsevat parin (a_1, b_1), sitten parin (a_2, b_2) jne. aina pariin (a_{k-1}, b_{k-1}) saakka. (Kysymyskierrokset on siis indeksoitu nollasta alkaen.) Tilanteen edistymistä voi kuvata relaatiolla p_ℓ, joka kertoo, mitkä parit ovat selvillä ennen kierrosta ℓ:

$$p_\ell = \{\, (a_j, b_j) \mid j \in \{0, \ldots, \ell - 1\} \,\}.$$

Siis aluksi $p_0 = \emptyset$, sitten $p_1 = \{(a_0, b_0)\}$, $p_2 = \{(a_0, b_0), (a_1, b_1)\}$ jne.

Jos Elina todella käyttää vastauksissaan johdonmukaisesti yhtä isomorfismia $f\colon \mathfrak{A} \cong \mathfrak{B}$, niin jokaisella $\ell \in \{0, \ldots, k\}$ pätee $p_\ell \subset f$, joten p_ℓ on osittainen isomorfismi mallista $\mathfrak{A}$ malliin $\mathfrak{B}$. Ajatuskokeen henkeen kuitenkin kuuluu, ettemme tiedä, onko Elinalla

käytettävissään isomorfismi $f\colon \mathfrak{A} \cong \mathfrak{B}$. Saattaa olla, että Elina vastaa vain tuntumalta, tai voi jopa olla, että Elina todellisuudessa tietää, että $\mathfrak{A} \ncong \mathfrak{B}$, mutta hän yrittää estää tätä paljastumasta. Jos p_ℓ ei olekaan osittainen isomorfismi, niin huijaus on paljastunut. Kääntäen jatkossa tullaan valitsemaan osittainen isomorfisuus siksi kriteeriksi, jolla tarkkaillaan Elinan vastauksien järkevyyttä.

Ajatuskokeessa esitetyn idean voi jalostaa samanlaisuutta mittaaviksi käsitteiksi kahdella eri tavalla, algebrallisella ja peliteoreettisella. Edellinen muotoilu on Fraïssén esittämä, jälkimmäinen on peräisin Ehrenfeuchtilta. Osoittautuu, että nämä johtavat yhtäpitäviin lopputuloksiin, joten on lähinnä makukysymys, kumpaa menetelmää käyttää. Peliteoreettinen tapa tuntuu olevan lähempänä tässä esitettyä ideaa, mutta senkin käsittelyssä on tekniset puolensa.

Fraïssén systeemi

Algebrallisen muotoilun ymmärtämistä helpottaa seuraava havainto: Oletetaan, että Elina noudattaa jotain sääntöä vastauksissaan. Merkitään I_i:llä kaikkien niiden tilanteiden p_{k-i} joukkoa, jotka voisivat syntyä eri Akselin kysymyksillä, kun Elina noudattaa tätä sääntöä (joukkojen I_i indeksi i on jäljellä olevien kysymyksien lukumäärä). Tällöin jokaisella $p \in I_{i+1}$ on tietynlaisia laajennuksia joukossa I_i, ja seuraavassa määritelmässä muotoillaan tarkasti, minkälaisia.

1.1. Määritelmä. Olkoot $\mathfrak{A}$ ja $\mathfrak{B}$ samanaakkostoisia malleja. Tällöin osittainen isomorfismi $p \in \mathrm{Part}(\mathfrak{A}, \mathfrak{B})$ *laajenee eteenpäin joukkoon* $I \subset \mathrm{Part}(\mathfrak{A}, \mathfrak{B})$, jos jokaisella $a \in \mathrm{Dom}(\mathfrak{A})$ on olemassa sellainen $q \in I$, että $p \subset q$ ja $a \in \mathrm{dom}(q)$. Kuvaus p *laajenee taaksepäin joukkoon* $I \subset \mathrm{Part}(\mathfrak{A}, \mathfrak{B})$, jos p^{-1} laajenee eteenpäin joukkoon $I^{-1} = \{\, p^{-1} \mid p \in I \,\}$. Kuvaus p *laajenee edestakaisesti joukkoon* $I \subset \mathrm{Part}(\mathfrak{A}, \mathfrak{B})$, jos p laajenee eteen- ja taaksepäin joukkoon I.

Huomattakoon, että p laajenee taaksepäin joukkoon I täsmälleen silloin, kun jokaisella $b \in \mathrm{Dom}(\mathfrak{B})$ on olemassa sellainen $q \in I$, että $p \subset q$ ja $b \in \mathrm{rg}(q)$.

Jos joukon I oletetaan olevan suljettu rajoittumien suhteen, niin edestakaisen laajenemisen ehto saadaan muokattua muotoon, joka on lähempänä ajatuskoetta.

1.2. Lemma. *Olkoot* $\mathfrak{A}$ *ja* $\mathfrak{B}$ *samanaakkostoisia malleja,* $p \in \mathrm{Part}(\mathfrak{A}, \mathfrak{B})$ *ja* $I \subset \mathrm{Part}(\mathfrak{A}, \mathfrak{B})$. *Oletetaan, että* I *on rajoittumien suhteen suljettu eli jos* $r \subset q \in I$, *niin* $r \in I$. *Tällöin seuraavat ovat yhtäpitäviä:*

a) p *laajenee edestakaisesti joukkoon* I.

b) Jokaista $a \in \mathrm{Dom}(\mathfrak{A})$ *vastaa* $b \in \mathrm{Dom}(\mathfrak{B})$, *jolle* $p \cup \{(a, b)\} \in I$, *ja jokaista* $b \in \mathrm{Dom}(\mathfrak{B})$ *vastaa* $a \in \mathrm{Dom}(\mathfrak{A})$, *jolle* $p \cup \{(a, b)\} \in I$.

Todistus. Osoitetaan ensin seuraavien väitteiden yhtäpitävyys:

c) p laajenee eteenpäin joukkoon I.

d) Jokaista $a \in \mathrm{Dom}(\mathfrak{A})$ vastaa $b \in \mathrm{Dom}(\mathfrak{B})$, jolle $p \cup \{(a, b)\} \in I$.

Ehdosta d seuraa tietenkin ehto c, sillä kun $a \in \mathrm{Dom}(\mathfrak{A})$, ehdon d mukaan on olemassa $b \in \mathrm{Dom}(\mathfrak{B})$, jolle $q = p \cup \{(a, b)\} \in I$, ja selvästi $p \subset q$ ja $a \in \mathrm{dom}(q)$. Oletaan kääntäen ehto c. Olkoon $a \in \mathrm{Dom}(\mathfrak{A})$. Ehdon c mukaan on olemassa $q \in I$,

jolle $p \subset q$ ja $a \in \mathrm{dom}(q)$. Merkitään $r = p \cup \{(a, q(a))\} = p \cup \{(a, b)\}$, missä $b = q(a)$. Tällöin $p \subset r \subset q$ ja koska I on rajoittumien suhteen suljettu, niin $p \cup \{(a, b)\} = r \in I$.

Määritelmän ja edellisessä kappaleessa todistetun perusteella seuraavat ovat yhtäpitäviä:

a) p laajenee edestakaisesti joukkoon I.

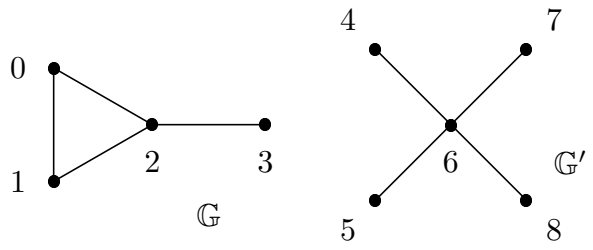
a') p laajenee eteenpäin joukkoon I ja p^{-1} laajenee eteenpäin joukkoon I^{-1}.

b') Jokaista $a \in \mathrm{Dom}(\mathfrak{A})$ vastaa $b \in \mathrm{Dom}(\mathfrak{B})$, jolle $p \cup \{(a, b)\} \in I$, ja jokaista $b \in \mathrm{Dom}(\mathfrak{B})$ vastaa $a \in \mathrm{Dom}(\mathfrak{A})$, jolle $(p \cup \{(a, b)\})^{-1} = p^{-1} \cup \{(b, a)\} \in I^{-1}$.

b) Jokaista $a \in \mathrm{Dom}(\mathfrak{A})$ vastaa $b \in \mathrm{Dom}(\mathfrak{B})$, jolle $p \cup \{(a, b)\} \in I$, ja jokaista $b \in \mathrm{Dom}(\mathfrak{B})$ vastaa $a \in \mathrm{Dom}(\mathfrak{A})$, jolle $p \cup \{(a, b)\} \in I$. □

1.3. Määritelmä. Samanaakkostoiset mallit $\mathfrak{A}$ ja $\mathfrak{B}$ ovat *osittaisesti isomorfisia asteeseen* $k \in \mathbb{N}$ *saakka*, $\mathfrak{A} \cong_k \mathfrak{B}$, jos on olemassa sellainen jono $(I_0, \ldots, I_k)$ epätyhjiä osittaisten isomorfismien joukkoja $I_i \subset \mathrm{Part}(\mathfrak{A}, \mathfrak{B})$, $i \in \{0, \ldots, k\}$, että jokainen $p \in I_{i+1}$, missä $i \in \{0, \ldots, k-1\}$, laajenee edestakaisesti joukkoon I_i. Jos jonoa halutaan korostaa, merkitään $(I_0, \ldots, I_k)\colon \mathfrak{A} \cong_k \mathfrak{B}$.

1.4. Esimerkki. Tarkastellaan jälleen verkkoja $\mathbb{G}$ ja $\mathbb{G}'$:



Merkitään $p_{a,b} = \{(a, b)\}$, kun $a \in \mathrm{Dom}(\mathbb{G})$ ja $b \in \mathrm{Dom}(\mathbb{G}')$. Osoitetaan, että

$$(I_0, I_1, I_2)\colon \mathbb{G} \cong_2 \mathbb{G}',$$

missä

$$I_0 = \{\, p \in \mathrm{Part}(\mathbb{G}, \mathbb{G}') \mid |p| \leq 2 \,\},$$
$$I_1 = \{p_{2,6}\} \cup \{\, p_{a,b} \mid a \in \mathrm{Dom}(\mathbb{G}), b \in \mathrm{Dom}(\mathbb{G}'), a \neq 2, b \neq 6 \,\}$$

ja

$$I_2 = \{\emptyset\}.$$

Triviaalisti $I_i \subset \mathrm{Part}(\mathbb{G}, \mathbb{G}')$ jokaisella $i \in \{0, 1, 2\}$. Kuvaus $\emptyset$ laajenee edestakaisesti joukkoon I_1, koska $\bigcup_{p \in I_1} \mathrm{dom}(p) = \mathrm{Dom}(\mathbb{G})$ ja $\bigcup_{p \in I_1} \mathrm{rg}(p) = \mathrm{Dom}(\mathbb{G}')$. Näytetään vielä, että jokainen $p \in I_1$ laajenee edestakaisesti joukkoon I_0. Tässä on kaksi tapausta:

1) $p = p_{2,6}$. Jokaisella $a \in \{0, 1, 3\}$ kuvaus $\{(2, 6), (a, 4)\}$ on osittainen isomorfismi ja siis joukossa I_0. Samoin jokaisella $b \in \{4, 5, 7, 8\}$ kuvaus $\{(2, 6), (0, b)\} \in I_0$. Tapauksessa $a = 2$ tai $b = 6$ voidaan valita p:n laajennukseksi $p \in I_0$ itse.

2) $p = p_{a,b}$, missä $a \neq 2$ ja $b \neq 6$. Tutkitaan, voidaanko p laajentaa eteenpäin joukkoon I_0. Olkoon $c \in \mathrm{Dom}(\mathbb{G})$. Jos $c = a$, niin p:n laajentamisessa kuvaukseksi $q \in$

I_0, jolle $a \in \mathrm{dom}(q)$, ei ole mitään ongelmaa: voidaan valita $q = p$. Oletetaan siis $c \neq a$. Jos alkioiden a ja c välillä on särmä, niin $q = \{(a,b),(c,6)\} \in I_0$. Jos särmää taas ei ole, niin valitaan $u \in \{4,5,7,8\} \setminus \{b\}$ mielivaltaisesti; huomataan, että $q = \{(a,b),(c,u)\}$ on osittainen isomorfismi, koska alkioiden b ja u välillä ei ole särmää. Siis $q \in I_0$.

Taaksepäinen laajentaminen analysoidaan hyvin samankaltaisella tavalla. Olkoon $d \in \mathrm{Dom}(\mathbb{G}')$. Jälleen voidaan olettaa $d \neq b$. Jos alkioiden b ja d välillä on särmä, niin $q = \{(a,b),(2,d)\} \in I_0$. Jos särmää ei ole ja $a \neq 3$, niin $q = \{(a,b),(3,d)\} \in I_0$, muuten $q = \{(a,b),(0,d)\} \in I_0$.

Toisaalta $\mathbb{G} \not\cong_3 \mathbb{G}'$. Jos nimittäin olisi $(J_0,J_1,J_2,J_3)\colon \mathbb{G} \cong_3 \mathbb{G}'$, niin voitaisiin valita osittaiset isomorfismit $p_i \in J_i$, $i \in \{0,1,2,3\}$, että $p_3 \subset p_2 \subset p_1 \subset p_0$ ja $2 \in \mathrm{dom}(p_2)$, $1 \in \mathrm{dom}(p_1)$ ja $0 \in \mathrm{dom}(p_0)$. Siis $\{0,1,2\} \subset \mathrm{dom}(p_0)$, mutta tällöinhän p_0 upottaisi kolmion verkkoon $\mathbb{G}'$, mikä on todettu mahdottomaksi esimerkissä 4.10.

Relaatiot $\cong_k$ ovat haluamallamme tavalla samanlaisuuden mittoja.

1.5. Lause. *Olkoot $\mathfrak{A}$ ja $\mathfrak{B}$ samanaakkostoisia malleja sekä $k \in \mathbb{N}$.*

a) Jos $\mathfrak{A} \cong \mathfrak{B}$, niin $\mathfrak{A} \cong_k \mathfrak{B}$.

b) Jos $\mathfrak{A} \cong_{k+1} \mathfrak{B}$, niin $\mathfrak{A} \cong_k \mathfrak{B}$.

c) Oletetaan, että $\mathfrak{A}$ ja $\mathfrak{B}$ ovat äärellisiä ja $\mathfrak{A} \not\cong \mathfrak{B}$. Tällöin $\mathfrak{A} \not\cong_{r+1} \mathfrak{B}$, missä $r = \min\{\mathrm{card}(\mathfrak{A}), \mathrm{card}(\mathfrak{B})\}$.

Todistus. a) Oletetaan, että $f\colon \mathfrak{A} \cong \mathfrak{B}$. Koska f on isomorfismi, se on erityisesti osittainen isomorfismi eli $f \in \mathrm{Part}(\mathfrak{A},\mathfrak{B})$. Huomataan, että f laajenee triviaalisti eteenpäin joukkoon $I = \{f\}$, koska jokaisella $a \in \mathrm{Dom}(\mathfrak{A})$ pätee valmiiksi $a \in \mathrm{dom}(f)$ ja $f \in I$. Vastaavasti f^{-1} laajenee eteenpäin joukkoon $I^{-1} = \{f^{-1}\}$, joten f laajenee edestakaisesti joukkoon I. Siis $(I)_{i\in\{0,\ldots,k\}} = \underbrace{(I,\ldots,I)}_{k+1 \text{ kpl}}\colon \mathfrak{A} \cong_k \mathfrak{B}$.

b) Jos $(I_0,\ldots,I_{k+1})\colon \mathfrak{A} \cong_{k+1} \mathfrak{B}$, niin selvästi $(I_0,\ldots,I_k)\colon \mathfrak{A} \cong_k \mathfrak{B}$.

c) Oletetaan vastoin väitettä, että $\mathfrak{A}$ ja $\mathfrak{B}$ ovat äärellisiä, epäisomorfisia malleja, mutta $(I_0,\ldots,I_{r+1})\colon \mathfrak{A} \cong_{r+1} \mathfrak{B}$, missä $r = \min\{\mathrm{card}(\mathfrak{A}), \mathrm{card}(\mathfrak{B})\}$. Koska $I_{r+1} \neq \emptyset$, voidaan valita $p_{r+1} \in I_{r+1}$. Symmetrian vuoksi voidaan olettaa, että $r = \mathrm{card}(\mathfrak{A})$; luetellaan $\mathfrak{A}$:n alkiot: $\mathrm{Dom}(\mathfrak{A}) = \{a_1,\ldots,a_r\}$. Laajentumisominaisuuden vuoksi on olemassa sellaiset osittaiset isomorfismit $p_i \in I_i$, $i \in \{1,\ldots,r\}$, että $p_i \supset p_{i+1}$ ja $a_i \in \mathrm{dom}(p_i)$. Erityisesti $\mathrm{Dom}(\mathfrak{A}) \subset \mathrm{dom}(p_1)$, joten itse asiassa $\mathrm{dom}(p_1) = \mathrm{Dom}(\mathfrak{A})$ ja p_1 on upotus mallista $\mathfrak{A}$ malliin $\mathfrak{B}$. Koska $p_1\colon \mathfrak{A} \not\cong \mathfrak{B}$, kuvaus p_1 ei voi olla surjektio. Valitaan $b \in \mathrm{Dom}(\mathfrak{B}) \setminus \mathrm{rg}(p_1)$. Koska p_1 laajenee taaksepäin joukkoon I_0, on olemassa $p_0 \in I_0$, jolle $p_1 \subset p_0$ ja $b \in \mathrm{rg}(p_0)$. Siis toisaalta p_0 laajentaa aidosti kuvausta p_1, sillä $b \in \mathrm{rg}(p_0) \setminus \mathrm{rg}(p_1)$, toisaalta $\mathrm{dom}(p_1) = \mathrm{Dom}(\mathfrak{A}) = \mathrm{dom}(p_0)$, mikä on ristiriitaista. □

Ehrenfeuchtin peli

Algebrallisen muotoilun jälkeen esitellään peliteoreettinen muotoilu. Peli on varsinaisesti peräisin Ehrenfeuchtilta, mutta eri muotoilujen yhtäpitävyyden vuoksi on tapana puhua Ehrenfeuchtin ja Fraïssén pelistä.

Käsitteiden selventämiseksi joudutaan rajoittamaan yleiskielistä sanojen käyttöä: "Peli" (englanniksi "game") tarkoittaa jatkossa pelin pelaamiseen liittyvää säännöstöä, "ottelu" (engl. "play") taas tarkoittaa näiden sääntöjen mukaista tapahtumaa, ts. pelinkulkua tai pelierää.

Määriteltävä peli, k-kierroksinen mallien $\mathfrak{A}$ ja $\mathfrak{B}$ välinen *Ehrenfeuchtin ja Fraïssén peli (eli EF-peli)*, $\mathrm{EF}_k(\mathfrak{A}, \mathfrak{B})$, riippuu kolmesta parametristä: samanaakkostoisista relationaalisista malleista $\mathfrak{A}$ ja $\mathfrak{B}$ sekä luvusta $k \in \mathbb{N}$. Peliä pelaa kaksi pelaajaa, jota kutsutaan Akseliksi ($\forall$) ja Elinaksi ($\exists$).

Pelikierros: Jokaisella kierroksella $i \in \{0, \ldots, k-1\}$ Akseli valitsee ensin luvun 0 tai luvun 1 ja tämän valinnan mukaan jatkaa valitsemalla alkion $\mathfrak{A}$:sta tai $\mathfrak{B}$:stä, ts. *Akselin siirto* on joko pari $(0, a)$, missä $a \in \mathrm{Dom}(\mathfrak{A})$, tai $(1, b)$, missä $b \in \mathrm{Dom}(\mathfrak{B})$. Elina valitsee sitten alkion toisesta mallista eli vastaa siirtoon $(0, a)$ siirrolla $b \in \mathrm{Dom}(\mathfrak{B})$ tai siirtoon $(1, b)$ siirrolla $a \in \mathrm{Dom}(\mathfrak{A})$. Molemmissa tapauksessa pelaajat tulevat valinneeksi parin $(a, b) \in \mathrm{Dom}(\mathfrak{A}) \times \mathrm{Dom}(\mathfrak{B})$. Akselin ja Elinan siirtoparista $((0, a), b)$ voidaan pitää kirjaa kaaviolla

	$\forall$	$\exists$
$\mathfrak{A}$	a	
$\mathfrak{B}$		b

,

kun taas siirtoparia $((1, b), a)$ vastaa kaavio

	$\forall$	$\exists$
$\mathfrak{A}$		a
$\mathfrak{B}$	b	

.

Ottelun lopputulos: Olkoon (ε_i, c_i) Akselin siirto ja d_i Elinan siirto kierroksella $i \in \{0, \ldots, k-1\}$. Näistä siirroista muodostuu pari $(a_i, b_i) \in \mathrm{Dom}(\mathfrak{A}) \times \mathrm{Dom}(\mathfrak{B})$, missä

$$(a_i, b_i) = \begin{cases} (c_i, d_i), & \text{jos } \varepsilon_i = 0 \\ (d_i, c_i), & \text{jos } \varepsilon_i = 1. \end{cases}$$

Ottelulla tarkoitetaan siirroista muodostuvaa jonoa

$$\boldsymbol{u} = ((\varepsilon_0, c_0), d_0, (\varepsilon_1, c_1), d_1, \ldots, (\varepsilon_{k-1}, c_{k-1}), d_{k-1}).$$

Luku ε_i on ottelun seuraamisen kannalta epäoleellista tietoa heti, kun kierros on päättynyt. Siksi *ottelutilanteella* ennen kierrosta i tarkoitetaan jonoa

$$p_i = \{\, (a_j, b_j) \mid j \in \{0, \ldots, i-1\} \,\} \subset \mathrm{Dom}(\mathfrak{A}) \times \mathrm{Dom}(\mathfrak{B}).$$

Tässä $i \in \{0, \ldots, k\}$ eli myös erikoistapaus $i = k$ on järkevä hyväksyä, vaikka kierrosta k ei enää pelatakaan. *Ottelun lopputilanteena* on jono $r_{\boldsymbol{u}} = p_k$. *Elina voittaa*, jos $r_{\boldsymbol{u}} \in \mathrm{Part}(\mathfrak{A}, \mathfrak{B})$, muuten *Akseli voittaa*.

1.6. Esimerkki. Akseli ja Elina pelaavat kolmi- ja kaksikierroksiset EF-ottelut tuttujen verkkojen (ks. esim. 1.4) $\mathbb{G}$ ja $\mathbb{G}'$ välillä. Kolmikierroksista ottelua

$$((1,6),2,(0,0),4,(0,1),7)$$

voi kuvata kaaviolla

	$\forall$	$\exists$	$\forall$	$\exists$	$\forall$	$\exists$
$\mathbb{G}$		2	0		1	
$\mathbb{G}'$	6			4		7

ja kaksikierroksista samoin alkanutta ottelua kaaviolla

	$\forall$	$\exists$	$\forall$	$\exists$
$\mathbb{G}$		2	0	
$\mathbb{G}'$	6			4

.

Peliä $\mathrm{EF}_3(\mathbb{G},\mathbb{G}')$ vastaavan ottelun lopputilanne on $p=\{(2,6),(0,4),(1,7)\}$. Akseli voitti tämän ottelun, koska mallissa $\mathbb{G}$ on solmujen 0 ja 1 välillä särmä, mutta $\mathbb{G}'$:ssa ei ole särmää solmujen $p(0)=4$ ja $p(1)=7$ välillä, joten p ei ole osittainen isomorfismi. Sen sijaan toiseen peliin $\mathrm{EF}_2(\mathbb{G},\mathbb{G}')$ liittyvän ottelun voittaja on Elina, sillä $q=\{(2,6),(0,4)\}\in\mathrm{Part}(\mathbb{G},\mathbb{G}')$.

Edellinen esimerkki ei tietenkään mittaa verkkojen $\mathbb{G}$ ja $\mathbb{G}'$ samanlaisuutta yhtä hyvin kuin esimerkki 1.4. Vaikka Akseli voittikin kolmikierroksisen ottelun ja Elina kaksikierroksisen, niin ongelmaksi jää, pelasivatko pelaajat parhaalla mahdollisella tavalla. Mitenkään ei voida tyytyä tarkastelemaan sitä, että Elina tai Akseli voittaa yksittäisen ottelun, vaan yleisesti ottaen kiinnostavinta on, voiko jompikumpi voittaa ottelun siitä riippumatta, miten toinen pelaa. Tämän täsmällinen muotoilu vaatii seuraavan määritelmän.

1.7. Määritelmä. Tarkastellaan peliä $\mathrm{EF}_k(\mathfrak{A},\mathfrak{B})$. Merkitään

$$T_\exists=\mathcal{P}(\mathrm{Dom}(\mathfrak{A})\times\mathrm{Dom}(\mathfrak{B})).$$

Vastaavasti

$$T_\forall=T_\exists\times\big((\{0\}\times\mathrm{Dom}(\mathfrak{A}))\cup(\{1\}\times\mathrm{Dom}(\mathfrak{B}))\big).$$

Elinan strategialla tarkoitetaan kuvausta $\alpha\colon T_\forall\to\mathrm{Dom}(\mathfrak{A})\cup\mathrm{Dom}(\mathfrak{B})$, jolle $\alpha(q,(\varepsilon,c))\in\mathrm{Dom}(\mathfrak{B})$, jos $\varepsilon=0$, ja $\alpha(q,(\varepsilon,c))\in\mathrm{Dom}(\mathfrak{A})$, jos $\varepsilon=1$, kun $(q,(\varepsilon,c))\in T_\exists$). Vastaavasti *Akselin strategialla* on kuvaus $\beta\colon T_\exists\to(\{0\}\times\mathrm{Dom}(\mathfrak{A}))\cup(\{1\}\times\mathrm{Dom}(\mathfrak{B}))$.

Elina on noudattanut strategiaansa α ottelussa

$$\boldsymbol{u}=((\varepsilon_0,c_0),d_0,(\varepsilon_1,c_1),d_1,\ldots,(\varepsilon_{k-1},c_{k-1}),d_{k-1}),$$

jos jokaisella $i\in\{0,\ldots,k-1\}$ pätee $d_i=\alpha(p_i,(\varepsilon_i,c_i))$, missä p_i on ottelutilanne ottelussa $\boldsymbol{u}$ ennen kierrosta i. Vastaavasti *Akseli on noudattanut strategiaansa β ottelussa* $\boldsymbol{u}$, jos jokaisella $i\in\{0,\ldots,k-1\}$ pätee $(\varepsilon_i,c_i)=\beta(p_i)$.

Elinan strategia α on *voittostrategia*, jos Elina voittaa jokaisen ottelun $\boldsymbol{u}$, jossa hän on noudattanut strategiaa α. Vastaavalla tavalla määritellään Akselin voittostrategia.

Algebrallisen ja peliteoreettisen muotoilun yhtäpitävyyden todistamiseksi on hyödyllistä todistaa ensin seuraava tekninen aputulos.

1.8. Lemma. *Oletetaan, että* $\mathfrak{A} \cong_k \mathfrak{B}$, *missä mallit* $\mathfrak{A}$ *ja* $\mathfrak{B}$ *ovat relationaalisia. Tällöin on olemassa rajoittumien suhteen suljetut* J_i, $i \in \{0, \ldots, k\}$, *joille* $(J_0, \ldots, J_k)\colon \mathfrak{A} \cong_k \mathfrak{B}$.

Todistus. Valitaan joukot I_i, $i \in \{0, \ldots, k\}$, joille $(I_0, \ldots, I_k)\colon \mathfrak{A} \cong_k \mathfrak{B}$. Kun $i \in \{0, \ldots, k\}$, asetetaan

$$J_i = \{\, p \mid \exists p^* \in I_i (p \subset p^*) \,\}.$$

Selvästi $I_i \subset J_i$, joten $J_i \neq \emptyset$. Koska tarkasteltava aakkosto on relationaalinen, osittaisten isomorfismien rajoittumat ovat osittaisia isomorfismeja, joten J_i on rajoittumien suhteen suljettu ja $J_i \subset \mathrm{Part}(\mathfrak{A}, \mathfrak{B})$ (oletuksen mukaanhan $I_i \subset \mathrm{Part}(\mathfrak{A}, \mathfrak{B})$).

Riittää enää osoittaa, että jokainen $p \in J_{i+1}$, $i \in \{0, \ldots, k-1\}$, laajenee edestakaisesti joukkoon J_i. Olkoon $a \in \mathrm{Dom}(\mathfrak{A})$. Koska $p \in J_{i+1}$, on olemassa $p^* \in I_{i+1}$, jolle $p \subset p^*$. Koska p^* laajenee eteenpäin joukkoon I_i on olemassa $q \in I_i \subset J_i$, jolle $q \supset p$ ja $a \in \mathrm{dom}(q)$. Siis p laajenee eteenpäin joukkoon J_i ja taaksepäinen laajeneminen osoitetaan symmetrisellä tavalla. □

1.9. Lause. *Olkoot* $\mathfrak{A}$ *ja* $\mathfrak{B}$ *saman relationaalisen aakkoston malleja ja* $k \in \mathbb{N}$. *Tällöin seuraavat ovat yhtäpitäviä:*

a) $\mathfrak{A} \cong_k \mathfrak{B}$.

b) Elinalla on voittostrategia pelissä $\mathrm{EF}_k(\mathfrak{A}, \mathfrak{B})$.

Todistus. Oletetaan, että kohta a on voimassa, ja todistetaan kohta b. Olkoon $(I_0, \ldots, I_k)\colon \mathfrak{A} \cong_k \mathfrak{B}$, missä edellisen lemman nojalla joukkojen I_i, $i \in \{0, \ldots, k\}$, voidaan olettaa olevan rajoittumien suhteen suljettuja. Muodostetaan Elinalle strategia $\alpha\colon T_\forall \to \mathrm{Dom}(\mathfrak{A}) \cup \mathrm{Dom}(\mathfrak{B})$. Kiinnitetään ensin $a^* \in \mathrm{Dom}(\mathfrak{A})$ ja $b^* \in \mathrm{Dom}(\mathfrak{B})$. Olkoon $(q, (\varepsilon, c)) \in T_\forall$. Merkitään $\ell = |q|$. Tarkastellaan kolmea eri tapausta.

1) Kun $\ell \geq k$ tai $q \notin I_{k-\ell}$, asetetaan

$$\alpha(q, (\varepsilon, c)) = \begin{cases} b^*, & \text{jos } \varepsilon = 0 \\ a^*, & \text{jos } \varepsilon = 1 \end{cases}.$$

(Tässä tapauksessa ottelutilanteella q ei ole Elinan kannalta mitään mieltä, varsinkaan hänen käyttämänsä strategian suhteen.)

2) Oletetaan, että $\ell < k$, $q \in I_{k-\ell}$ ja $\varepsilon = 0$. Koska $k - \ell > 0$ ja $q \in I_{k-\ell}$, niin q laajenee eteenpäin joukkoon $I_{k-\ell-1}$. Voidaan siis valita $r \in I_{k-\ell-1}$, jolle $q \subset r$ ja $c \in \mathrm{dom}(r)$. Asetetaan

$$\alpha(q, (\varepsilon, c)) = r(c).$$

3) Oletetaan, että $\ell < k$, $q \in I_{k-\ell}$ ja $\varepsilon = 1$. Tässä tapauksessa q laajenee taaksepäin joukkoon $q \in I_{k-\ell-1}$ kuvaukseksi $r \in I_{k-\ell-1}$, jolle $q \subset r$ ja $c \in \mathrm{rg}(r)$. Asetetaan

$$\alpha(q, (\varepsilon, c)) = r^{-1}(c).$$

Selvästi α on hyvinmääritelty Elinan strategia. Olkoon

$$\boldsymbol{u} = ((\varepsilon_0, c_0), d_0, (\varepsilon_1, c_1), d_1, \ldots, (\varepsilon_{k-1}, c_{k-1}), d_{k-1})$$

ottelu, jossa Elina noudattaa strategiaa α, ts. jokaisella $i \in \{0, \ldots, k-1\}$ pätee

$$d_i = \alpha(p_i, (\varepsilon_i, c_i)),$$

missä $p_i = \{\, (a_j, b_j) \mid j \in \{0, \ldots, i-1\} \,\}$ on ottelutilanne ottelussa $\boldsymbol{u}$ ennen kierrosta i. Todistetaan induktiolla, että $p_i \in I_{k-i}$ jokaisella $i \in \{0, \ldots, k\}$. Aluksi saadaan $\emptyset = p_0 \in I_{k-0} = I_k$, sillä I_k on epätyhjä ja rajoittumien suhteen suljettu. Oletetaan, että $p_i \in I_{k-i}$, missä $i \in \{0, \ldots, k-1\}$. Huomattakoon, että $i = |p_i|$. Jos $\varepsilon_i = 0$, niin strategian määritelmän kohta 2 kertoo, että on olemassa sellainen $r \in I_{k-i-1}$, että

$$p_{i+1} = p_i \cup \{(c_i, d_i)\} = p_i \cup \{(c_i, \alpha(q_i, (\varepsilon_i, c_i)))\} = p_i \cup \{(c_i, r(c_i))\} \subset r.$$

Jos taas $\varepsilon_i = 1$, niin jollakin $r \in I_{k-i-1}$ pätee

$$p_{i+1} = p_i \cup \{(c_i, d_i)\} = p_i \cup \{(\alpha(q_i, (\varepsilon_i, c_i)), c_i)\} \subset r.$$

Koska I_{k-i-1} on rajoittumien suhteen suljettu, niin molemmissa tapauksissa seuraa $p_{i+1} \in I_{k-i-1}$. Erityisesti ottelun $\boldsymbol{u}$ lopputulos $p_k \in I_{k-k} = I_0 \subset \mathrm{Part}(\mathfrak{A}, \mathfrak{B})$, joten Elina voittaa pelin $\boldsymbol{u}$, jossa hän on noudattanut strategiaa $\boldsymbol{u}$. Siis α on voittostrategia.

Oletetaan kääntäen kohta b eli että Elinalla on voittostrategia pelissä $\mathrm{EF}_k(\mathfrak{A}, \mathfrak{B})$. Kun $i \in \{0, \ldots, k\}$, sisältäköön I_i ne $p \subset \mathrm{Dom}(\mathfrak{A}) \times \mathrm{Dom}(\mathfrak{B})$, jotka ovat kierrosta $k-i$ edeltäviä ottelutilanteita jossakin ottelussa, jossa Elina on noudattanut strategiaa α. Koska α on voittostrategia, niin jokainen tällainen p on voittoon päättyneen ottelun lopputuloksen rajoittumana osittainen isomorfismi (tässä käytetään taas aakkoston relationaalisuutta). Siis $I_i \subset \mathrm{Part}(\mathfrak{A}, \mathfrak{B})$; samoin on selvää, että $I_i \neq \emptyset$.

Olkoon nyt $p \in I_{i+1}$, $i \in \{0, \ldots, k-1\}$, ja $a \in \mathrm{Dom}(\mathfrak{A})$. Tällöin $(p, (0, a))$ on ottelutilanne Akselin siirron jälkeen ottelussa, jossa Elina on noudattanut α:aa. Merkitään $b = \alpha(p, (0, a))$. Tällöin $p \cup \{(a, b)\}$ on myös ottelutilanne ottelussa, jossa Elina noudattaa α:aa, joten $p \cup \{(a, b)\} \in I_i$. Taaksepäinen laajeneminen osoitetaan vastaavasti. Siis $(I_0, \ldots, I_k) \colon \mathfrak{A} \cong_k \mathfrak{B}$. □

2. Helmipeli

Keskeinen ero EF-pelissä isomorfismiin verrattuna on se, että malleja tutkittaessa riittää tarkastella (kerrallaan) rajoitettua määrää pisteitä. Itse asiassa tilanne on vielä helpompi: Jos ottelukierroksen ajatellaan kuluttavan yhden aikayksikön, niin mallien tarkasteluun vaadittava aika on rajattu.

Kun EF-peliä muunnellaan hieman, saadaan helmipeli, jossa aikaresurssin sijasta rajoitetaankin vain muistiresurssia, abstraktissa mielessä. Jotta muistin käytön rajaus

ei rajottaisi tarkasteluun käytettyä aikaa, täytyy siirtoja voida jossain mielessä unohtaa. Voidaan esimerkiksi ajatella, että Akseli ja Elina kirjaavat siirtonsa liitutaululle, jossa on tilaa vain k siirtoparille. Kun taulu täyttyy, siirtoja voi pyyhkiä pois. Pyyhkimisoikeutta ei ole järkevää antaa Elinalle, sillä silloin peli olisi oleellisesti EF-peli, jossa viimeisen siirron voi peruuttaa. Pelin luonne muuttuu täysin, kun Akseli on ainoa, joka saa peruuttaa siirron.

Barwisen systeemi

Siinä missä EF-peliä vastaavaa algebrallista muotoilua kutsutaan osittaiseksi isomorfiaksi johonkin asteeseen saakka, helmipeliä vastaavassa muotoilussa puhutaan muuttujien määrästä. Määritelmässä ovat valmiiksi mukana muutamat säännöllisyysominaisuudet, jotka edellisen luvun variantissa osoitettiin olevan oletettavissa. Siirtojen unohtamista vastaa osittaisen isomorfismin rajoittuma.

2.1. Määritelmä. Olkoot $\mathfrak{A}$ ja $\mathfrak{B}$ samanaakkostoisia relationaalisia malleja sekä $k \in \mathbb{N}$. Mallit $\mathfrak{A}$ ja $\mathfrak{B}$ ovat *osittaisesti isomorfisia k muuttujan suhteen*, $\mathfrak{A} \cong^k \mathfrak{B}$, jos on olemassa seuraavanlainen epätyhjä $I \subset \mathrm{Part}(\mathfrak{A}, \mathfrak{B})$:

1) Kaikilla $p \in I$ pätee $|p| \leq k$.
2) I on rajoittumien suhteen suljettu.
3) Kun $p \in I$ ja $|p| < k$, niin p laajenee edestakaisesti joukkoon I.

Kun joukkoa I halutaan korostaa, niin merkitään $I\colon \mathfrak{A} \cong^k \mathfrak{B}$.

Ekvivalenssilla $\cong^k$ on samanlaisia perusominaisuuksia kuin $\cong_k$:lla.

2.2. Lause. *Olkoot $\mathfrak{A}$ ja $\mathfrak{B}$ samanaakkostoisia relationaalisia malleja ja $k \in \mathbb{N}$. Tällöin:*

a) Jos $\mathfrak{A} \cong \mathfrak{B}$, niin $\mathfrak{A} \cong^k \mathfrak{B}$.
b) Jos $\mathfrak{A} \cong^k \mathfrak{B}$, niin $\mathfrak{A} \cong_k \mathfrak{B}$.
c) Jos $\mathfrak{A} \cong^{k+1} \mathfrak{B}$, niin $\mathfrak{A} \cong^k \mathfrak{B}$.

Todistus. a) Oletetaan, että $f\colon \mathfrak{A} \cong \mathfrak{B}$. Asetetaan

$$I = \{\, f\restriction C \mid C \subset \mathrm{Dom}(\mathfrak{A}),\ |C| \leq k \,\}.$$

Koska $\mathfrak{A}$:n ja $\mathfrak{B}$:n yhteinen aakkosto on relationaalinen, niin $I \subset \mathrm{Part}(\mathfrak{A}, \mathfrak{B})$. Selvästi $I \neq \emptyset$, I on rajoittumien suhteen suljettu ja $|p| \leq k$ kaikilla $p \in I$. Jos $p \in I$, missä $|p| < k$, ja $a \in \mathrm{Dom}(\mathfrak{A})$, $b \in \mathrm{Dom}(\mathfrak{B})$, niin $p \cup \{(a, f(a))\}, p \cup \{(f^{-1}(b), b)\} \in I$. Siis $I\colon \mathfrak{A} \cong^k \mathfrak{B}$.

b) Oletetaan, että $I\colon \mathfrak{A} \cong^k \mathfrak{B}$. Merkitään jokaisella $i \in \{0, \ldots, k\}$

$$I_i = \{\, p \in I \mid |p| \leq k - i \,\}.$$

Olkoon $p \in I_{i+1}$ ja $a \in \mathrm{Dom}(\mathfrak{A})$, missä $i \in \{0, \ldots, k-1\}$. Koska $p \in I$ ja $|p| \leq k - (i+1) < k$, niin p laajenee edestakaisesti joukkoon I. Siis on olemassa $q \in I$,

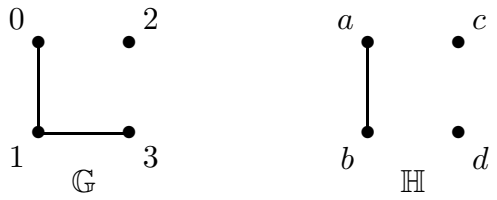
jolle $a \in \mathrm{dom}(q)$ ja $p \subset q$. Koska I on rajoittumien suhteen suljettu, niin $r \in I$, missä $r = p \cup \{(a, q(a))\}$. Toisaalta

$$|r| \leq |p| + 1 \leq k - (i+1) + 1 = k - i,$$

sillä $p \in I_{i+1}$. Siis $r \in I_i$ ja p laajenee eteenpäin joukkoon I. Taaksepäinen laajeneminen osoitetaan symmetrisesti. Siis $(I_0, \ldots, I_k) \colon \mathfrak{A} \cong_k \mathfrak{B}$.

c) Oletetaan $I \colon \mathfrak{A} \cong^{k+1} \mathfrak{B}$. Asetetaan $J = \{\, p \in I \mid |p| \leq k \,\}$. Selvästi J täyttää kokoehdon ja on suljettu rajoittumien suhteen. Kun $p \in J$, $|p| < k$, niin myös $|p| < k+1$, joten p laajenee edestakaisesti joukkoon I. Koska I on rajoittumien suhteen suljettu, vastaaville laajennuksille q voidaan olettaa pätevän $|q| \leq |p| + 1 \leq k$. Siis $q \in J$, joten p laajenee edestakaisesti joukkoon J. Siten $J \colon \mathfrak{A} \cong^k \mathfrak{B}$. □

2.3. Esimerkki. Tarkastellaan seuraavia verkkoja $\mathbb{G}$ ja $\mathbb{H}$.



Laskuharjoituksissa ratkaistusta tehtävästä seuraa, että $\mathbb{G} \cong_2 \mathbb{H}$. Kuitenkin $\mathbb{G} \ncong^2 \mathbb{H}$. Jos nimittäin olisi $I \colon \mathbb{G} \cong^2 \mathbb{H}$, niin $\emptyset \in I$ ja kaksi kertaa eteenpäin laajentamalla saataisiin $p = \{(0, x), (3, y)\} \in I$ jollakin $x, y \in \mathrm{Dom}(\mathbb{H})$. Koska $p \in \mathrm{Part}(\mathbb{G}, \mathbb{H})$, niin $\deg_{\mathbb{H}}(x) = 0$ tai $\deg_{\mathbb{H}}(y) = 0$, sillä astetta yksi olevat alkiot ovat toisiinsa yhdeydessä $\mathbb{H}$:ssa. Symmetrian vuoksi voidaan olettaa, että $\deg_{\mathbb{H}}(x) = 0$. Koska I on rajoittumien suhteen suljettu, niin $q = \{(0, x)\} \in I$. Nyt huomataan, ettei q:lla voi olla laajennusta $r \in I$, jolle $1 \in \mathrm{dom}(r)$, sillä alkioiden 0 ja 1 välillä on $\mathbb{G}$:ssä särmä, mutta $\deg_{\mathbb{H}}(x) = 0$. Siis $\mathbb{G} \ncong^2 \mathbb{H}$.

Varsinainen helmipeli

Osittaiselle isomorfialle k muuttujan suhteenkin voidaan esittää peliteoreettinen vastine. Tässä tyydytään sääntöjen esittelemiseen; algebrallisen ja peliteoreettisen muotoilun yhtäpitävyys osoitettaisiin samalla tavalla kuin EF-peli tapauksessa.

Olkoot $\mathfrak{A}$ ja $\mathfrak{B}$ samanaakkostoisia relationaalisia malleja sekä $k \in \mathbb{N}$. Kuten EF-pelin kohdalla, peli $\mathrm{PG}^k(\mathfrak{A}, \mathfrak{B})$ eli *k helmen helmipeli mallien* $\mathfrak{A}$ *ja* $\mathfrak{B}$ *välillä* riippuu näistä kolmesta parametrista sekä peliä pelaavat Akseli ($\forall$) ja Elina ($\exists$). Toisin kuin EF-peli, helmipeliä pelataan äärettömän monta kierrosta.

Kierros: Jokaisella kierroksella $i \in \mathbb{N}$ Akseli valitsee parin (h, c), missä joko $h \in \{1, \ldots, k\}$ ja $c \in \mathrm{Dom}(\mathfrak{A})$ tai $h \in \{-k, \ldots, -1\}$ ja $c \in \mathrm{Dom}(\mathfrak{B})$. Elina vastaa siirrolla $(-h, d)$, missä edellisessä tapauksessa ($h > 0$) täytyy olla $d \in \mathrm{Dom}(\mathfrak{B})$, jälkimmäissä $d \in \mathrm{Dom}(\mathfrak{A})$. Kaavioina siirtoja voidaan merkitä

	$\forall$	$\exists$
$\mathfrak{A}$	$\textcircled{h}\, c$	
$\mathfrak{B}$		$\textcircled{-h}\, d$

tai

	$\forall$	$\exists$
$\mathfrak{A}$		$\textcircled{h}\, d$
$\mathfrak{B}$	$\textcircled{-h}\, c$	

.

Akselin sanotaan *asettavan helmen h alkiolle c*, kun taas Elina *asettaa helmen $-h$ alkiolle d*. Helmiä on siis käytettävissä k paria $(1,-1),\ldots,(k,-k)$.

Ottelun lopputulos: Olkoon Akselin siirto kierroksella $i \in \mathbb{N}$ pari (h_i, c_i) ja Elinan $(-h_i, d_i)$. Määritellään ensin, mitä tarkoitetaan *ottelutilanteella p_i* ennen kierrosta $i \in \mathbb{N}$. Sanotaan helmen h olevan pelilaudalla, jos jollakin $j \in \mathbb{N}$, $j < i$, pätee $h_j = h$ tai $-h_j = h$ eli *kierroksella j on pelattu helmellä h. Helmen h sanotaan olevan alkiolla c*, jos helmi on pelilaudalla ja viimeisellä kierroksella $j < i$, kun helmellä on pelattu, helmi on asetettu alkiolle c. Ottelutilanne p_i on kaikkien sellaisten parien (a, b) joukko, että jollakin $h \in \{1,\ldots,k\}$ helmi h on alkiolla a ja helmi $-h$ alkiolla b.

Elina voittaa ottelun, jos jokaisella $i \in \mathbb{N}$ pätee $p_i \in \mathrm{Part}(\mathfrak{A}, \mathfrak{B})$, muuten *Akseli voittaa*.

Kuten EF-pelillekin, helmipelille voitaisiin määritellä strategia ja voittostrategia. Samaan tapaan olisi mahdollista osoittaa, että $\mathfrak{A} \cong^k \mathfrak{B}$, jos ja vain jos Elinalla on voittostrategia pelissä $\mathrm{PG}^k(\mathfrak{A}, \mathfrak{B})$.

Pelisääntöjä olisi mahdollista muokata parillakin tavalla, ilman että se vaikuttaisi voittostrategioiden olemassaloon. Ensiksikin huomataan, että Akselin voitto ratkeaa äärellisen monen kierroksen jälkeen, kun taas Elinan voitto ei varmistu, ennen kuin ottelun äärettömän monta kierrosta on pelattu. Periaatteessa ottelu voitaisiin siis katkaista, jos $p_i \notin \mathrm{Part}(\mathfrak{A}, \mathfrak{B})$. Toisaalta jos Akselilla on voittostrategia, niin sama ottelutilanne ei voi toistua voittostrategiaa noudattavassa ottelussa. Siis ottelutilanteen toistuttua ottelun voisi katkaista ja Elina voitaisiin julistaa voittajaksi.

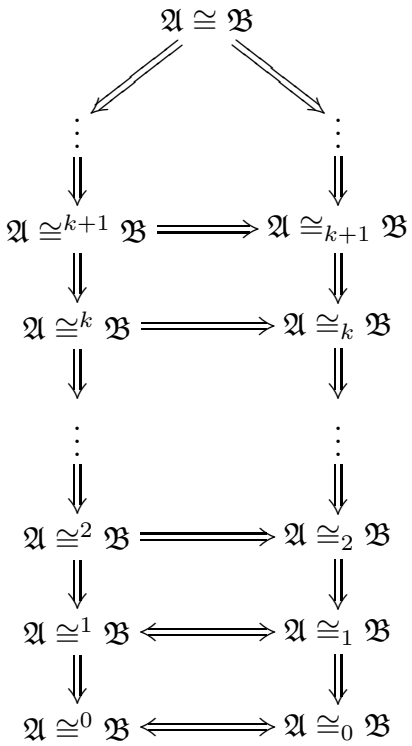
2.4. Esimerkki. Edellistä esimerkkiä 2.3 voisi vastata vaikkapa seuraavanlainen kierroksella 2 ratkeava peli.

	$\forall$	$\exists$	$\forall$	$\exists$	$\forall$	$\exists$
$\mathbb{G}$	$\textcircled{1}\, 0$		$\textcircled{2}\, 3$		$\textcircled{1}\, 1$	
$\mathbb{H}$		$\textcircled{-1}\, a$		$\textcircled{-2}\, c$		$\textcircled{-1}\, d$

3. Vertailua

Lauseista 1.5 ja 2.2 seuraa, että osittaiseen isomorfismiin liittyvät ekvivalenssit

muodostavat relationaalisilla malleilla seuraavanlaisen hierarkian.



Lauseiden faktoihin on lisätty kaksi helppoa huomiota. Samanaakkostoisilla relationaalisilla $\mathfrak{A}$ ja $\mathfrak{B}$ pätee nimittäin $\emptyset \in \mathrm{Part}(\mathfrak{A}, \mathfrak{B})$, joten $(\{\emptyset\})\colon \mathfrak{A} \cong_0 \mathfrak{B}$ ja $\{\emptyset\}\colon \mathfrak{A} \cong^0 \mathfrak{B}$. Erityisesti $\mathfrak{A} \cong^0 \mathfrak{B} \iff \mathfrak{A} \cong_0 \mathfrak{B}$. Edelleen jos $(I_0, I_1)\colon \mathfrak{A} \cong_1 \mathfrak{B}$, missä I_0 ja I_1 ovat rajoittumien suhteen suljettuja, niin $\emptyset \in I_1$ laajenee edestakaisesti joukkoon I_0, joten $I\colon \mathfrak{A} \cong^1 \mathfrak{B}$, missä $I = \{\, p \in I_0 \mid |p| \leq 1 \,\}$. Siis myös $\mathfrak{A} \cong^1 \mathfrak{B} \iff \mathfrak{A} \cong_1 \mathfrak{B}$.

Kaavio herättää kysymyksiä: Ovatko hierarkiat aitoja, ts. voidaanko jokaisella $k \in \mathbb{N}$ esittää esimerkki sellaisista malleista $\mathfrak{A}$ ja $\mathfrak{B}$, että $\mathfrak{A} \cong_k \mathfrak{B}$, mutta $\mathfrak{A} \ncong_{k+1} \mathfrak{B}$ (tai vastaavasti $\mathfrak{A} \cong^k \mathfrak{B}$, mutta $\mathfrak{A} \ncong^{k+1} \mathfrak{B}$)? Entä onko olemassa esimerkkiä malleista, joille $\mathfrak{A} \cong_k \mathfrak{B} \not\Rightarrow \mathfrak{A} \cong^k \mathfrak{B}$? Esimerkeissä olisi lisäksi hyvä rajoittua relationaalisiin malleihin.

Vertaillaan samankaltaisuuden mittoja systemaattisesti parissa yksinkertaisessa tapauksessa.

Puhtaat joukot

Olkoot A ja B äärellisiä epätyhjiä joukkoja. Merkitään $k = |A|$ ja $\ell = |B|$. Selvästi $\langle A \rangle \cong \langle B \rangle$, jos ja vain jos $k = \ell$. Oletetaan $k \neq \ell$, merkitään $r = \min\{k, \ell\}$ ja jokaisella $i \in \{0, \ldots, r\}$

$$I_i = \{\, p \mid p \text{ injektio, } \mathrm{dom}(p) \subset A, \mathrm{rg}(p) \subset B, |p| \leq r - i \,\}.$$

Koska puhtaissa joukoissa ei ole perusjoukkojen lisäksi rakennetta, niin pätee $I_i \subset \mathrm{Part}(\langle A \rangle, \langle B \rangle)$. Olkoon $p \in I_{i+1}$, missä $i \in \{0, \ldots, r-1\}$, ja olkoon $a \in A$. Koska

$I_{i+1} \subset I_i$, voidaan olettaa, että $a \notin \mathrm{dom}(p)$. Koska $|p| \leq r-(i+1) < r \leq \ell$, niin on olemassa $b \in B \setminus \mathrm{rg}(p)$. Siten $q = p \cup \{(a,b)\}$ on injektio, jolle $|q| = |p|+1 \leq r-(i+1)+1 = r-i$, ts. $q \in I_i$. Siis p laajenee eteenpäin joukkoon I_i. Taaksepäinen laajeneminen seuraa siitä, että $|p| < k$. Siis $(I_0, \ldots, I_r)\colon \langle A\rangle \cong_r \langle B\rangle$.

Toisaalta epätyhjä joukko $I_0 \subset \mathrm{Part}(\langle A\rangle, \langle B\rangle)$ on rajoittumien suhteen suljettu ja $|p| \leq r$, kun $p \in I_0$. Koska $I_1 = \{\, p \in I_0 \mid |p| < r \,\}$, niin jokainen $p \in I_0$, jolle $|p| < r$, laajenee edestakaisesti joukkoon I_0. Siis $I_0\colon \langle A\rangle \cong^r \langle B\rangle$.

Lukua r ei voi kasvattaa $r+1$:ksi, sillä lauseen 1.5 kohdan c mukaan $\langle A\rangle \ncong_{r+1} \langle B\rangle$. (Tämä on helppoa näyttää tietenkin suoraankin.)

Yhteenveto: Puhtaille joukoille ekvivalenssirelaatiot $\cong_k$ ja $\cong^k$ yhtyvät. Toisaalta jokaisella $k \in \mathbb{Z}_+$ esimerkiksi joukoille $A = \{0, \ldots, k-1\}$ ja $B = \{0, \ldots, k\}$ pätee $\langle A\rangle \cong^k \langle B\rangle$, mutta $\langle A\rangle \ncong^{k+1} \langle B\rangle$ ja $\langle A\rangle \ncong_{k+1} \langle B\rangle$, joten pystysuuntaiset hierarkiat ovat aitoja. Vain esimerkit malleista, joille $\mathfrak{A} \cong^0 \mathfrak{B} \not\Rightarrow \mathfrak{A} \cong^1 \mathfrak{B}$ ja $\mathfrak{C} \cong^0 \mathfrak{D} \not\Rightarrow \mathfrak{C} \cong^1 \mathfrak{D}$, puuttuvat.

Väritetyt joukot

Olkoon $\chi\colon A \to C$ äärellisen epätyhjän joukon väritys. Tätä vastaava malli, *väritetty joukko*, muodostetaan seuraavasti: Otetaan jokaista väriä $c \in C$ kohti käyttöön uusi yksipaikkainen relaatiosymboli U_c. Väritetty joukko $\mathfrak{M}_\chi$ on aakkoston $\{\, U_c \mid c \in C \,\}$ malli, jolle

$$\mathrm{Dom}(\mathfrak{M}_\chi) = A \text{ ja}$$
$$U_c^{\mathfrak{M}_\chi} = \chi^{-1}\{c\} = \{\, a \in A \mid \chi(a) = c \,\} = \{\, a \in A \mid \text{alkion } a \text{ väri on } c \,\},$$

kun $c \in C$. Olkoon $\xi\colon B \to C$ äärellisen epätyhjän B väritys. Helposti huomataan, että $f\colon \mathfrak{M}_\chi \to \mathfrak{M}_\xi$ on isomorfismi täsmälleen silloin, kun f on bijektio, joka säilyttää värit eli $\chi = \xi \circ f$. Vastaavasti $p \in \mathrm{Part}(\mathfrak{M}_\chi, \mathfrak{M}_\xi)$, jos ja vain jos p on injektio, jolle $\mathrm{dom}(p) \subset A$, $\mathrm{rg}(p) \subset B$ ja $\chi\restriction \mathrm{dom}(p) = \xi \circ p$. Merkitään

$$C_0 = \{\, c \in C \mid \left|U_c^{\mathfrak{M}_\chi}\right| \neq \left|U_c^{\mathfrak{M}_\xi}\right| \,\} = \{\, c \in C \mid |\chi^{-1}\{c\}| = |\xi^{-1}\{c\}| \,\}.$$

Tällöin $\mathfrak{M}_\chi \cong \mathfrak{M}_\xi$, jos ja vain jos $C_0 = \emptyset$.

Oletetaan nyt $\mathfrak{M}_\chi \ncong \mathfrak{M}_\xi$. Merkitään

$$r = \min\big(\{\, \left|\chi^{-1}\{c\}\right| \mid c \in C_0 \,\} \cup \{\, \left|\xi^{-1}\{c\}\right| \mid c \in C_0 \,\}\big)$$

ja muodostetaan osittaisten isomorfismien systeemi asettamalla

$$I_i = \{\, p \in \mathrm{Part}(\mathfrak{M}_\chi, \mathfrak{M}_\xi) \mid |p| \leq r - i \,\},$$

kun $i \in \{0, \ldots, r\}$. Olkoon $p \in I_{i+1}$ ja $b \in B$, missä $i \in \{0, \ldots, r-1\}$. Koska $I_{i+1} \subset I_i$, voidaan olettaa, että $b \notin \mathrm{rg}(p)$. Merkitään $c = \xi(b)$ ja tarkastellaan kahta eri tapausta.

1) Jos $c \notin C_0$, niin $\left|\chi^{-1}\{c\}\right| = \left|\xi^{-1}\{c\}\right|$. Koska p säilyttää värit, myös $\left|\chi^{-1}\{c\} \smallsetminus \mathrm{dom}(p)\right| = \left|\xi^{-1}\{c\} \smallsetminus \mathrm{rg}(p)\right|$. Koska $b \in \xi^{-1}\{c\} \smallsetminus \mathrm{rg}(p)$, erityisesti on olemassa $a \in \chi^{-1}\{c\} \smallsetminus \mathrm{dom}(p)$. Kuvaus $q = p \cup \{(a,b)\}$ on siis injektio, joka säilyttää värit. Koska $|q| = |p|+1 \leq r-(i+1)+1 = r-i$, niin $q \in I_i$, joten p laajenee taaksepäin joukkoon I_i.

2) Jos $c \in C_0$, niin $\chi^{-1}\{c\} \smallsetminus \mathrm{dom}(p) \neq \emptyset$ seuraa siitä, että $|\mathrm{dom}(p)| = |p| \leq r-(i+1) < r$ ja $|\chi^{-1}\{c\}| \geq r$ luvun r määritelmän nojalla. Siis tässäkin tapauksessa voidaan valita $a \in \chi^{-1}\{c\} \smallsetminus \mathrm{dom}(p)$ ja pätee $q = p \cup \{(a,b)\} \in I_i$.

Siis p laajenee taaksepäin joukkoon I_i. Laajeneminen eteenpäin osoitetaan symmetrisellä tavalla. Siis $(I_0,\ldots,I_r)\colon \mathfrak{M}_\chi \cong_r \mathfrak{M}_\xi$. Samalla tavalla kuin puhtaiden joukkojen tapauksessa osoitetaan, että myös $I_0\colon \mathfrak{M}_\chi \cong^r \mathfrak{M}_\xi$.

Toisaalta $\mathfrak{M}_\chi \ncong_{r+1} \mathfrak{M}_\xi$ ja siis myös $\mathfrak{M}_\chi \ncong^{r+1} \mathfrak{M}_\xi$. Oletetaan nimittäin, että olisi $(I_0,\ldots,I_r)\colon \mathfrak{M}_\chi \cong_{r+1} \mathfrak{M}_\xi$, missä joukot I_i, $i \in \{0,\ldots,r+1\}$, olisivat rajoittumien suhteen suljettuja. Valitaan $c_0 \in C_0$ niin, että $r = \min\{\left|\chi^{-1}\{c_0\}\right|, \left|\xi^{-1}\{c_0\}\right|\}$. Voidaan olettaa, että $r = \left|\chi^{-1}\{c_0\}\right|$. Koska $c_0 \in C_0$, niin tällöin $r = \left|\chi^{-1}\{c_0\}\right| < \left|\xi^{-1}\{c_0\}\right|$, joten voidaan valita eri alkiot $b_0,\ldots,b_r \in \xi^{-1}\{c_0\}$. Laajennusominaisuudesta seuraisi nyt, että on olemassa $p_0 \in I_0$, jolle $\mathrm{rg}(p) \in \{b_0,\ldots,b_r\}$. Koska p säilyttäisi värit, niin $\mathrm{dom}(p) \subset \chi^{-1}\{c_0\}$, joten $r = \left|\chi^{-1}\{c_0\}\right| \geq |\mathrm{dom}(p)| = r+1 > r$, mikä on ristiriita.

Väritettyjenkään joukkojen tapauksessa ei huomata mitään eroa relaatioiden $\cong_k$ ja $\cong^k$ välillä ($k \in \mathbb{N}$). Yksi uusi esimerkki kuitenkin saatiin: jos $\mathfrak{M}_\chi$ ja $\mathfrak{M}_\xi$ ovat molemmat yksivärisiä, mutta erivärisiä, niin $\mathfrak{M}_\chi \cong_0 \mathfrak{M}_\xi$, mutta $\mathfrak{M}_\chi \ncong_1 \mathfrak{M}_\xi$, sillä tässä tapauksessa $r = 0$.

Lineaarijärjestetyt joukot

Väritetyt joukot ovat malleja, joilla on hyvin vähän rakennetta. Lineaarijärjestetyt joukot edustavat tietyssä mielessä toista ääripäätä, joten ei oikeastaan ole yllätys, että ekvivalenssien suhde muuttuu täysin erilaiseksi. Aloitetaan analysoimalla isomorfismia asteeseen k saakka.

3.1. Lause. *Olkoot $\mathfrak{A}$ ja $\mathfrak{B}$ äärellisiä lineaarijärjestettyjä joukkoja sekä $k \in \mathbb{N}$. Oletetaan, että* $\mathrm{card}(\mathfrak{A}) \geq 2^k - 1$ *ja* $\mathrm{card}(\mathfrak{B}) \geq 2^k - 1$. *Tällöin $\mathfrak{A} \cong_k \mathfrak{B}$.*

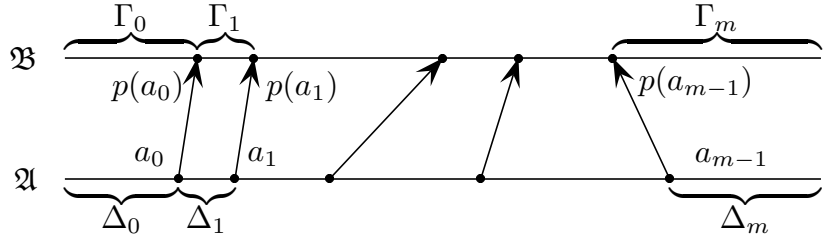
Todistus. Olkoon $i \in \{0,\ldots,k\}$. Määritellään joukko $I_i \subset \mathrm{Part}(\mathfrak{A},\mathfrak{B})$. Olkoon $p \in \mathrm{Part}(\mathfrak{A},\mathfrak{B})$. Luetellaan $\mathrm{dom}(p) = \{a_0,\ldots,a_{m-1}\}$ suuruusjärjestyksessä pienimmästä suurimpaan. Joukko $\mathrm{dom}(p)$ jakaa $\mathrm{Dom}(\mathfrak{A}) \smallsetminus \mathrm{dom}(p)$:n väleiksi $\Delta_0,\ldots,\Delta_m$ (suuruusjärjestyksessä), joista osa voi olla tyhjiä. Vastaavasti $\mathrm{rg}(p) = \{p(a_0),\ldots,p(a_{m-1})\}$ jakaa $\mathrm{Dom}(\mathfrak{B}) \smallsetminus \mathrm{rg}(p)$:n väleiksi $\Gamma_0,\ldots,\Gamma_m$. Asetetaan $p \in I_i$, jos ja vain jos kaikilla $j \in \{0,\ldots,m\}$

1) $|\Delta_j| = |\Gamma_j|$
   tai
2) $|\Delta_j| \geq 2^i - 1$ ja $|\Gamma_j| \geq 2^i - 1$.

Vastinvälien pitää siis olla yhtäpitkiä tai riittävän suuria.

Osoitetaan, että $(I_0,\ldots,I_k)\colon \mathfrak{A} \cong_k \mathfrak{B}$. Selvästi $\emptyset \in I_i$ jokaisella $i \in \{0,\ldots,k\}$, sillä $\mathrm{card}(\mathfrak{A}) \geq 2^k - 1 \geq 2^i - 1$ ja $\mathrm{card}(\mathfrak{B}) \geq 2^k - 1 \geq 2^i - 1$. Olkoon $i \in \{0,\ldots,k-1\}$ ja

$p \in I_{i+1}$. Näytetään, että p laajenee edestakaisesti joukkoon I_i.



Symmetrian vuoksi riittää tarkastella eteenpäin laajentumista. Olkoot välit Δ_j ja Γ_j ($j \in \{0, \ldots, m\}$) kuten edellisessä kappaleessa. Olkoon $a \in \mathrm{Dom}(\mathfrak{A})$. Koska $2^{i+1} - 1 \geq 2^i - 1$, niin $p \in I_i$, joten voidaan olettaa, että $a \notin \mathrm{dom}(p)$. Olkoon $j \in \{0, \ldots, m\}$ se yksikäsitteinen indeksi, jolla $a \in \Delta_j$. Alkio a jakaa joukon $\Delta_j \setminus \{a\}$ kahteen väliin, joista pienempiä alkioita edustaa Δ'_j, suurempia Δ''_j. Tarkastellaan kahta eri tapausta

a) Oletetaan, että $|\Delta_j| = |\Gamma_j|$. Tällöin on olemassa $b \in \Gamma_j$, joka jakaa $\Gamma_j \setminus \{b\}$:n väleihin Γ'_j ja Γ''_j, joille $\left|\Delta'_j\right| = \left|\Gamma'_j\right|$ ja $\left|\Delta''_j\right| = \left|\Gamma''_j\right|$. Asetetaan $q = p \cup \{(a, b)\}$. Kuvaukseen q liittyvät vastinvälit ovat yhtä suuria tai jollakin $t \in \{0, \ldots, m\} \setminus \{j\}$ välit Δ_t ja Γ_t, missä $|\Delta_t| \geq 2^{i+1} \geq 2^i - 1$ ja $|\Gamma_t| \geq 2^{i+1} \geq 2^i - 1$. Siis $q \in I_i$.

b) Oletetaan, että $|\Delta_j| \geq 2^{i+1} - 1$ ja $|\Gamma_j| \geq 2^{i+1} - 1$. Jos $\left|\Delta'_j\right| < 2^i - 1$, niin $\left|\Delta''_j\right| = |\Delta_j| - \left|\Delta'_j\right| - 1 > (2^{i+1} - 1) - (2^i - 1) - 1 = 2^i - 1$. Valitaan tällöin $b \in \Gamma_j$ niin, että $\Gamma_j \setminus \{b\}$ jakautuu väleihin Γ'_j ja Γ''_j, missä $\left|\Gamma'_j\right| = \left|\Delta'_j\right|$. Tällöin $\left|\Gamma''_j\right| > 2^i - 1$. Jos $\left|\Delta''_j\right| < 2^i - 1$, voidaan b valita vastaavasti niin, että $\left|\Gamma''_j\right| = \left|\Delta''_j\right|$. Lopuksi jos $\left|\Delta'_j\right| \geq 2^i - 1$ ja $\left|\Delta''_j\right| \geq 2^i - 1$, niin $b \in \Gamma_j$ voidaan valita niin, että $\left|\Gamma'_j\right| \geq 2^i - 1$ ja $\left|\Gamma''_j\right| \geq 2^i - 1$, sillä $|\Gamma_j| \geq 2^{i+1} - 1$ ja $\frac{(2^{i+1}-1)-1}{2} = 2^i - 1$. Kussakin tapauksessa seuraa $p \cup \{(a, b)\} \in I_i$.

Siis $(I_0, \ldots, I_k) \colon \mathfrak{A} \cong_k \mathfrak{B}$. □

Aivan vastakkainen tulos saadaan osittaisille isomorfismeille k muuttujan suhteen.

3.2. Lause. *Olkoot $\mathfrak{A}$ ja $\mathfrak{B}$ äärellisiä lineaarijärjestettyjä joukkoja. Tällöin jos $\mathfrak{A} \cong^2 \mathfrak{B}$, niin $\mathfrak{A} \cong \mathfrak{B}$.*

Todistus. Osoitetaan vastoin väitettä, että $I \colon \mathfrak{A} \cong^2 \mathfrak{B}$, vaikka $\mathfrak{A} \ncong \mathfrak{B}$. Voidaan olettaa, että $\mathfrak{A} = \mathfrak{L}_m$ ja $\mathfrak{B} = \mathfrak{L}_n$, missä $m < n$. Määritellään induktiolla luvut $j_t \in \{0, \ldots, n-1\}$, kun $t \in \mathbb{N}$. Asetetaan $j_0 = n - 1$. Koska $\emptyset \in I$ laajenee taaksepäin joukkoon I, niin on olemassa $j_1 \in \{0, \ldots, m - 1\}$, jolle $\{(j_1, j_0)\} \in I$. Oletetaan, että j_t, $t \in \mathbb{Z}_+$, on määritelty niin, että $p = \{(j_t, j_{t-1})\} \in I$. Laajennetaan kuvausta p taaksepäin joukkoon I kuvaukseksi $q \in I$, jolle $j_t \in \mathrm{rg}(q)$. Tällöin $q = \{(j_{t+1}, j_t), (j_t, j_{t-1})\}$ jollakin $j_{t+1} \in \{0, \ldots, m - 1\}$. Koska I on rajoittumien suhteen suljettu, niin $\{(j_{t+1}, j_t)\} \in I$.

Induktiolla saadaan, että $j_t > j_{t+1}$ jokaisella $t \in \mathbb{N}$. Tämä pätee arvolla $t = 0$, koska $j_1 < m \leq n - 1 = j_0$. Koska edellä $q \in \mathrm{Part}(\mathfrak{L}_m, \mathfrak{L}_n)$, niin $j_{t+1} < j_t \iff j_t < j_{t-1}$. Induktio-oletukseen yhdistämällä tästä seuraa induktioaskel. Siis $(j_t)_{t \in \mathbb{N}}$ on aidosti laskeva jono luonnollisia lukuja, mikä on mieletöntä. □

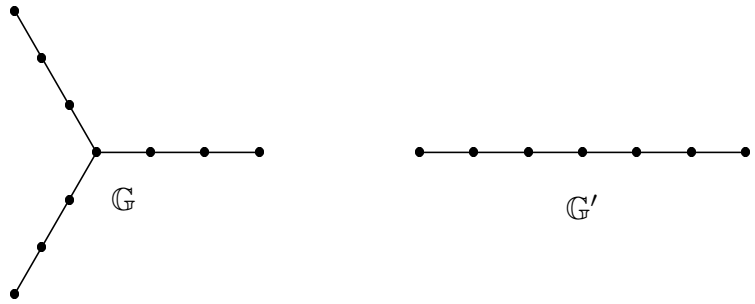
Olkoon $k \in \mathbb{N}$. Kun valitaan $\mathfrak{A} = \mathfrak{L}_{2^k-1}$ ja $\mathfrak{B} = \mathfrak{L}_{2^k}$, niin kahden edellisen lauseen perusteella $\mathfrak{A} \cong_k \mathfrak{B}$ ja $\mathfrak{A} \ncong^2 \mathfrak{B}$. Siis luvun alussa olevasta kaaviosta seuraavat kaikki syy-seuraus-suhteet, joita isomorfismin ja osittaisten isomorfismien eri muotojen välillä on.

Harjoituksia osaan II

1. Olkoot $\mathfrak{M}$ ja $\mathfrak{N}$ aakkoston $\{E\}$ epäisomorfisia äärellisiä malleja, joissa $E^{\mathfrak{M}}$ ja $E^{\mathfrak{N}}$ ovat ekvivalenssirelaatioita. Relaatiossa $E^{\mathfrak{M}}$ on k ekvivalenssiluokkaa, joissa on $m_0, \ldots, m_{k-1}$ alkiota pienimmästä suurimpaan. Relaatiossa $E^{\mathfrak{N}}$ on vastaavasti ℓ luokkaa, joissa n_i ($i = 0, \ldots, \ell - 1$; $n_i \leq n_{i+1}$, kun $i = 0, \ldots, \ell - 2$) alkiota. Mikä on suurin aste r, johon saakka $\mathfrak{M}$ ja $\mathfrak{N}$ ovat osittaisesti isomorfisia?

2. Kun $n \in \mathbb{N}$, merkitään $A_n = \{\, m \in \mathbb{N} \mid m|n \,\}$, ts. A_n on luvun n positiivisten tekijöiden joukko. Tarkastellaan malleja $\mathfrak{A} = \langle\, A_{24}, \mid \rangle$ ja $\mathfrak{B} = \langle\, A_{36}, \mid \rangle$. Etsi suurin $k \in \mathbb{N}$, jolle $\mathfrak{A} \cong_k \mathfrak{B}$.

3. Määritä suurin aste k, johon saakka kuvan verkot $\mathbb{G}$ ja $\mathbb{G}'$ ovat osittaisesti isomorfisia.



4. Olkoon $n \in \mathbb{Z}_+$ ja $\tau = \{U, \leq\}$ relationaalinen aakkosto, missä $\#(U) = 1$ ja $\#(\leq) = 2$. Tarkastellaan aakkoston τ malleja $\mathfrak{M}$, joissa $\leq^{\mathfrak{M}}$ on universumin lineaarijärjestys. Kun $k = 0, 1, 2, \lfloor \log_2 n - 1 \rfloor$, esitä esimerkki tällaisista malleista $\mathfrak{A}_k$ ja $\mathfrak{B}_k$, joiden koot ovat n ja $n + 1$, $\mathfrak{A}_k \cong_k \mathfrak{B}_k$ sekä $\mathfrak{A}_k \ncong_{k+1} \mathfrak{B}_k$.

5. Olkoon

$$S = \{\, (k, k+1) \mid k \in \{0, \ldots, 3n-2\} \,\}$$

joukon $X = \{0, \ldots, 3n-2\}$ seuraajarelaatio, $n \in \mathbb{Z}_+$. Tarkastellaan malleja $\mathfrak{M} = \langle X, S, n-1, 2n-1 \rangle$ ja $\mathfrak{N} = \langle X, S, 2n-1, n-1 \rangle$. Osoita, että $\mathfrak{M} \cong_r \mathfrak{N}$, missä $r = \lfloor \log_2 n - 1 \rfloor$.

6. Olkoon τ relationaalinen aakkosto, $k \in \mathbb{N}$ sekä $\mathfrak{M}$ ja $\mathfrak{N}$ aakkoston τ malleja, joilla on erilliset perusjoukot. *Mallipari* (tai *erillinen yhdiste*) $\mathfrak{M} \sqcup \mathfrak{N}$ on määritelmän mukaan aakkoston τ malli $\mathfrak{A}$, jolle $\mathrm{Dom}(\mathfrak{A}) = \mathrm{Dom}(\mathfrak{M}) \cup \mathrm{Dom}(\mathfrak{N})$ ja $R^{\mathfrak{A}} = R^{\mathfrak{M}} \cup R^{\mathfrak{N}}$, kun $R \in \tau = \mathrm{Rel}(\tau)$.Olkoot $\mathfrak{M}'$ ja $\mathfrak{N}'$ myös aakkoston τ malleja, joille $\mathrm{Dom}(\mathfrak{M}') \cap \mathrm{Dom}(\mathfrak{N}') = \emptyset$. Osoita, että jos $\mathfrak{M} \cong_k \mathfrak{M}'$ ja $\mathfrak{N} \cong_k \mathfrak{N}'$, niin $\mathfrak{M} \sqcup \mathfrak{N} \cong_k \mathfrak{N}' \sqcup \mathfrak{N}'$.

7. Olkoot $\mathfrak{A}$, $\mathfrak{A}'$, $\mathfrak{B}$ ja $\mathfrak{B}'$ relationaalisia saman aakkoston malleja, joilla on erilliset universumit. Osoita, että jos p on osittainen isomorfismi mallista $\mathfrak{A}$ malliin $\mathfrak{A}'$ ja q on osittainen isomorfismi mallista $\mathfrak{B}$ malliin $\mathfrak{B}'$, niin $p \cup q$ on osittainen isomorfismi malliparista $[\mathfrak{A}, \mathfrak{A}']$ malliparii $[\mathfrak{B}, \mathfrak{B}']$.

8. Olkoon $k \in \mathbb{Z}_+$ ja mallit $\mathfrak{A}$, $\mathfrak{A}'$, $\mathfrak{B}$ ja $\mathfrak{B}'$ kuten yllä. Todista suoraan käyttämättä luentojen lausetta, että jos Elinalla on voittostrategiat peleissä $\mathrm{EF}_k(\mathfrak{A}, \mathfrak{A}')$ ja $\mathrm{EF}_k(\mathfrak{B}, \mathfrak{B}')$, niin hänellä on voittostrategia myös malliparien välisessä pelissä
$\mathrm{EF}_k([\mathfrak{A}, \mathfrak{B}], [\mathfrak{A}', \mathfrak{B}'])$.

9. Verkkojen $\mathbb{G}$ ja $\mathbb{G}'$ mallipari $[\mathbb{G}, \mathbb{G}']$ on luentojen määritelmän mukaan aakkoston $\tau = \{E, U, V\}$ malli $\mathbb{G}''$, jolle $E^{\mathbb{G}''} = E^{\mathbb{G}} \cup E^{\mathbb{G}'}$, $U^{\mathbb{G}} = \mathrm{Dom}(\mathbb{G})$ ja $V^{\mathbb{G}} = \mathrm{Dom}(\mathbb{G}')$, mikäli verkoilla $\mathbb{G}$ ja $\mathbb{G}'$ on valmiiksi erilliset solmujoukot. Osoita, että on olemassa sellainen ensimmäisen kertaluvun logiikan τ-lause φ, että kaikille verkoille $\mathbb{G}$ ja $\mathbb{G}'$ pätee $[\mathbb{G}, \mathbb{G}'] \models \varphi$, jos ja vain jos Elina voittaa pelin $\mathrm{EF}_2(\mathbb{G}, \mathbb{G}')$.

10. Olkoot $\mathfrak{A}$ ja $\mathfrak{B}$ erikokoisia äärellisiä lineaarijärjestettyjä joukkoja, joista toisessa on vähemmän kuin 2^{k-1} alkiota. Osoita, että Akselilla on voittostrategia pelissä $\mathrm{EF}_k(\mathfrak{A}, \mathfrak{B})$.

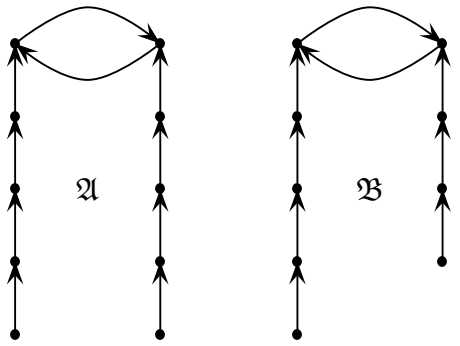
11. Aakkoston $\{E\}$, $\#(E) = 2$, mallia $\mathbb{G}$ kutsutaan *verkoksi*, jos $E^{\mathbb{G}}$ on symmetrinen ja irrefeksiivinen. Luettele 4 solmun verkkojen isomorfiatyypit.

12. Tarkastellaan 4 solmun verkkojen $\mathbb{G}$ ja $\mathbb{G}'$ välistä kahden kierroksen Ehrenfeuchtin ja Fraïssén peliä $\mathrm{EF}_2(\mathbb{G}, \mathbb{G}')$.
a) Osoita, että Akselilla on voittostrategia pelissä, jos $\mathbb{G} \ncong \mathbb{G}'$ ja verkossa $\mathbb{G}$ on 0 tai 6 särmää.
b) Osoita, että Akseli voittaa pelin, jos verkossa $\mathbb{G}$ on solmu, josta ei lähde särmiä, ja verkossa $\mathbb{G}'$ ei ole tällaista solmua.
c) Määritä sellaiset neljän solmun verkkojen parit $(\mathbb{G}, \mathbb{G}')$, että $\mathbb{G} \ncong \mathbb{G}'$, mutta Elinalla on voittostrategia pelissä $\mathrm{EF}_2(\mathbb{G}, \mathbb{G}')$.

13. Olkoot $\mathbb{G}$ ja $\mathbb{G}'$ edelleen neljän solmun verkkoja. Määritä, milloin $\mathbb{G} \cong^2 \mathbb{G}'$ eli verkot ovat osittaisesti isomorfisia kahden muuttujan suhteen.

14. Kun $n \in \mathbb{N}$ ja $n \geq 3$, niin $\mathbb{C}_n$ on n solmun sykli eli verkko, jolle $\mathrm{Dom}(\mathbb{C}_n) = \{0, \ldots, n-1\}$ ja $E^{\mathbb{C}_n} = \{\, (a, b) \in \{0, \ldots, n-1\}^2 \mid a \equiv b \pm 1 \pmod{n} \,\}$. Todista, että kun $m, n \in \mathbb{N}$ ja $m > n \geq 3$, niin $\mathbb{C}_m \ncong^3 \mathbb{C}_n$.

15. Aakkoston $\{R\}$, $\#(R) = 2$, malleissa $\mathfrak{A}$ ja $\mathfrak{B}$ on kuvan mukaiset relaatiot. Määritä suurin $k \in \mathbb{N}$, jolle pätee $\mathfrak{A} \cong^k \mathfrak{B}$ eli Elinalla on voittostrategia ko. mallien välisessä k helmen helmipelissä.



16. Olkoot $\mathfrak{A}$, $\mathfrak{B}$ ja $\mathfrak{C}$ saman aakkoston malleja sekä $k \in \mathbb{N}$. Todista, että
a) Jos $\mathfrak{A} \cong_k \mathfrak{B}$ ja $\mathfrak{B} \cong_k \mathfrak{C}$, niin $\mathfrak{A} \cong_k \mathfrak{C}$.
b) Jos $\mathfrak{A} \cong^k \mathfrak{B}$ ja $\mathfrak{B} \cong^k \mathfrak{C}$, niin $\mathfrak{A} \cong^k \mathfrak{C}$.

17. Olkoon R kolmipaikkainen relaatiosymboli. Kutsutaan aakkoston $\{R\}$ mallia $\mathfrak{A}$ *Steinerin kolmikkomalliksi*, jos seuraavat kolme ehtoa ovat voimassa.
1) Relaatio $R^{\mathfrak{A}}$ on toistoton eli kaikilla $(a, b, c) \in R^{\mathfrak{A}}$ alkiot a, b ja c ovat eri alkioita.
2) Relaatio $R^{\mathfrak{A}}$ on täysin symmetrinen eli kaikilla $(a, b, c) \in R^{\mathfrak{A}}$ pätee $(b, c, a) \in R^{\mathfrak{A}}$ ja $(a, c, b) \in R^{\mathfrak{A}}$.
3) Jokaista alkioparia $a, b \in \mathrm{Dom}(\mathfrak{A})$ vastaa yksikäsitteinen $c \in \mathrm{Dom}(\mathfrak{A})$, jolle $(a, b, c) \in R^{\mathfrak{A}}$.

Osoita, että äärelliset, vähintään seitsenalkioiset Steinerin kolmikkomallit ovat osittaisesti isomorfisia neljän muuttujan suhteen.

18. Esitä esimerkki kahdesta vähintään seitsenalkioisesta epäisomorfisesta Steinerin kolmikkomallista.

19. Olkoot $\mathbb{G}$ ja $\mathbb{H}$ äärellisiä verkkoja, joilla kummallakin on ℓ yhtenäistä komponenttia. Olkoot $\mathbb{G}_i$, $i \in \{0, \ldots, \ell-1\}$, verkon $\mathbb{G}$ ja $\mathbb{H}_i$, $i \in \{0, \ldots, \ell-1\}$, verkon $\mathbb{H}$ yhtenäiset komponentit.
a) Osoita, että jos jokaisella $i \in \{0, \ldots, \ell-1\}$ pätee $p_i \in \mathrm{Part}(\mathbb{G}_i, \mathbb{H}_i)$, niin $\bigcup_{i \in \{0,\ldots,\ell-1\}} p_i \in \mathrm{Part}(\mathbb{G}, \mathbb{H})$.
b) Olkoon $k \in \mathbb{N}$. Osoita, että jos jokaisella $i \in \{0, \ldots, \ell-1\}$ pätee $\mathbb{G}_i \cong_k \mathbb{H}_i$, niin $\mathbb{G} \cong_k \mathbb{H}$.
c) Osoita, että vastaavasti jos jokaisella $i \in \{0, \ldots, \ell-1\}$ pätee $\mathbb{G}_i \cong^k \mathbb{H}_i$, niin $\mathbb{G} \cong^k \mathbb{H}$.

III Logiikat

Tähän mennessä aakkoston rooli on jäänyt mallin käsitteessä hivenen irralliseksi seikaksi, sillä symboleita on käytetty lähinnä mallin rakenneosien (funktioiden, relaatioiden ja vakioiden) indeksoimiseen. Aakkostojen käytölle tulee enemmän mieltä, kun aakkoston symbolien avulla aletaan rakentaa formaaleja ilmaisuja, lauseita, joita voidaan käyttää mallin rakennetta tutkittaessa. Toisin kuin logiikan alkeiskursseilla, tällä kurssilla ensimmäisen kertaluvun logiikka ei ole mitenkään hallitsevassa asemassa, vaan sen rinnalla tarkastellaan muitakin logiikoita, kuten äärellisen monen muuttujan logiikkaa, toisen kertaluvun logiikkaa ja kiintopistelogiikkaa. Päättelyjärjestelmätkin ovat korkeintaan sivuroolissa äärellisten mallien teoriassa, eikä tarkasteltaviin logiikoihin välttämättä edes voida liittää sellaisia.

Logiikalla tarkoitetaan tässä järjestelmää, joka 1) rajaa, mitkä ilmaisut ovat sallittuja eli mitkä ovat logiikan lauseet, 2) määrittelee, mitkä symbolit esiintyvät sen lauseissa ja 3) kiinnittää tulkinnan lauseille. Muodollisesti logiikka on siis kolmikko $\mathcal{L} = (\Omega, T, \models_{\mathcal{L}})$, missä Ω on logiikan $\mathcal{L}$ lauseiden kokoelma, T on (luokka)kuvaus, joka liittää lauseeseen $\varphi \in \Omega$ sen aakkoston $T(\varphi)$, ja $\models_{\mathcal{L}}$ on mallien ja lauseiden välinen *totuusrelaatio*, ts. $\mathfrak{M} \models_{\mathcal{L}} \varphi$ luetaan "mallissa $\mathfrak{M}$ on totta φ". Relaatio $\mathfrak{M} \models_{\mathcal{L}} \varphi$ edellyttää, että $\mathfrak{M}$ on σ-malli, missä $\sigma \supset T(\varphi)$ eli kaikki lauseessa φ esiintyvät symbolit on tulkittu mallissa $\mathfrak{M}$.

Koska tavoitteena on tiettyjen konkreettisten logiikoiden esittely, tällä kurssilla ei paneuduta sen enempää edellä esitettyyn abstraktin logiikan käsitteeseen. Tarvittavat logiikat muodostetaan kaikki samalla tavalla: Vakio- ja funktiosymboleista kootaan termit, joita käytetään atomilauseissa. Atomilauseesta kasataan logiikan lauseet erilaisilla lauseenmuodostussäännöillä. Koska tarkasteltavien logiikoiden yhteisten lauseiden totuus tulkitaan näissä samalla tavalla, on järkevää käyttää totuusrelaatiolle yhteistä symbolia $\models$ ja puhua lauseiden tavanomaisista tulkinnoista.

1. Vakiot, muuttujat ja termit

1.1. Määritelmä. a) *Termit* ovat merkkijonoja, jotka muodostuvat induktiivisesti seuraavien sääntöjen mukaan:

1) Vakiosymbolit ovat termejä.
2) Jos f on k-paikkainen funktiosymboli ja $t_0, \ldots, t_{k-1}$ ovat termejä, niin $f(t_0, \ldots, t_{k-1})$ on termi.

b) *Termin aakkosto (eli termissä esiintyvien symbolien joukko)* $\tau(t)$ määritellään induktiolla:

1) Vakion c aakkosto on $\tau(c) = \{c\}$.
2) Jos t on muotoa $f(t_0, \ldots, t_{k-1})$, niin

$$\tau(t) = \bigcup_{i=0}^{k-1} \tau(t_i) \cup \{f\}.$$

c) Termi t voidaan *tulkita* mallissa, jonka aakkosto σ sisältää termin aakkoston $\tau(t)$. Tulkinta määritellään induktiolla:

1) Vakion tulkinta $c^{\mathfrak{M}}$ on osa mallin määritelmää.

2) $f(t_0, \ldots, t_{k-1})^{\mathfrak{M}} = f^{\mathfrak{M}}(t_0^{\mathfrak{M}}, \ldots, t_{k-1}^{\mathfrak{M}})$.

Teknisesti muuttujat ja vakiosymbolit samastetaan tällä kurssilla. Se, puhutaanko vakiosymbolista vai muuttujasta, riippuu käytöstä, tai tarkemmin sanoen tarkasteluaakkostosta. Tarkasteluaakkoston ulkopuoliset vakiosymbolit mielletään vapaiksi muuttujiksi. Olkoot $\mathfrak{M}$ aakkoston σ malli ja t termi, jolle $\tau(t) \setminus \sigma$ on joukko vakiosymboleita, lueteltuna $\tau(t) \setminus \sigma = \{x_0, \ldots, x_{k-1}\}$. Jos $\tau(t) \setminus \sigma \neq \emptyset$, termiä t ei voi tulkita suoraan mallissa $\mathfrak{M}$, vaan vakiosymbolit x_i, $i \in \{0, \ldots, k-1\}$, ovat mallin $\mathfrak{M}$ kannalta vapaita muuttujia. Malli $\mathfrak{M}$ täytyy siis laajentaa $\sigma \cup \{x_0, \ldots, x_{k-1}\}$-malliksi, ennen kuin tulkinta on mahdollinen. Olkoot $a_0, \ldots, a_{k-1} \in \mathrm{Dom}(\mathfrak{M})$ ja $\mathfrak{M}^* = \langle \mathfrak{M}, a_0, \ldots, a_{k-1} \rangle$ tällainen laajennus. Muuttujien tulkinnat ovat siis $x_i^{\mathfrak{M}^*} = a_i$, kun $i \in \{0, \ldots, k-1\}$. Tällöin merkitään

$$t^{\mathfrak{M}^*} = t^{\mathfrak{M}}[a_0/x_0, \ldots, a_{k-1}/x_{k-1}].$$

Merkintä tekee siis mallin $\mathfrak{M}^*$ eksplisiittisen määrittelemisen tarpeettomaksi.

Jatkoa varten tarvitaan seuraavaa tulosta:

1.2. Lause. *Olkoon h homomorfismi mallista $\mathfrak{A}$ malliin $\mathfrak{B}$. Jos t on mallien yhteisen aakkoston τ termi, niin $h(t^{\mathfrak{A}}) = t^{\mathfrak{B}}$.*

Todistus. Todistetaan väite induktiolla aakkoston τ termien t suhteen.

1) Jos t on vakiosymboli, niin $h(t^{\mathfrak{A}}) = t^{\mathfrak{B}}$ on suoraan yksi niistä ehdoista, joita homomorfismeille asetetaan.

2) Oletaan, että t on muotoa $f(t_0, \ldots, t_{k-1})$, missä termeille t_i pätee induktio-oletus $h(t_i^{\mathfrak{A}}) = t_i^{\mathfrak{B}}$, kun $i \in \{0, \ldots, k-1\}$. Koska h on homomorfismi, niin

$$\begin{aligned} h(t^{\mathfrak{A}}) &= h(f^{\mathfrak{A}}(t_0^{\mathfrak{A}}, \ldots, t_{k-1}^{\mathfrak{A}})) \\ &= f^{\mathfrak{B}}(h(t_0^{\mathfrak{A}}), \ldots, h(t_{k-1}^{\mathfrak{A}})) \\ &= f^{\mathfrak{B}}(t_0^{\mathfrak{B}}, \ldots, t_{k-1}^{\mathfrak{B}}) = t^{\mathfrak{B}}. \quad \square \end{aligned}$$

1.3. Seuraus. Jos termi t on muotoa $t(x_0, \ldots, x_{k-1})$ (eli aakkoston $\tau \cup \{x_0, \ldots, x_{k-1}\}$ termi), niin

$$h(t^{\mathfrak{A}}[a_0/x_0, \ldots, a_{k-1}/x_{k-1}]) = t^{\mathfrak{B}}[h(a_0)/x_0, \ldots, h(a_{k-1})/x_{k-1}]).$$

Todistus. Laajennetaan $\mathfrak{A}$ aakkoston $\tau \cup \{x_0, \ldots, x_{m-1}\}$ malliksi $\mathfrak{A}^* = \langle \mathfrak{A}, a_0, \ldots, a_{m-1} \rangle$ ja $\mathfrak{B}$ malliksi $\mathfrak{B}^* = \langle \mathfrak{B}, h(a_0), \ldots, h(a_{m-1}) \rangle$, ts. $\mathfrak{A}^* \restriction \tau = \mathfrak{A}$, $\mathfrak{B}^* \restriction \tau = \mathfrak{B}$ ja $x_i^{\mathfrak{A}^*} = a_i$, $x_i^{\mathfrak{B}^*} = h(a_i)$, kun $i \in \{0, \ldots, k-1\}$. Tällöin h on paitsi homomorfismi mallista $\mathfrak{A}$ malliin $\mathfrak{B}$, myös homomorfismi mallista $\mathfrak{A}^*$ malliin $\mathfrak{B}^*$, joten edellisen lauseen nojalla

$$h(t^{\mathfrak{A}}[a_0/x_0, \ldots, a_{m-1}/x_{m-1}]) = h(t^{\mathfrak{A}^*}) = t^{\mathfrak{B}^*} = t^{\mathfrak{B}}[h(a_0)/x_0, \ldots, h(a_{m-1})/x_{m-1}]. \quad \square$$

Algebrassa ja lineaarialgebrassa on totuttu siihen, että joukon virittämän joukon alkiot voidaan lausua virittäjien avulla. Tämä yleistyy malliteoriassa.

1.4. Määritelmä. Olkoon $\mathfrak{A}$ aakkoston τ malli ja $X \subset \mathrm{Dom}(\mathfrak{A})$. Jos $X = \emptyset$ ja $\mathrm{Con}(\tau) = \emptyset$, niin *osajoukon X mallissa $\mathfrak{A}$ virittämä joukko* on $\langle X \rangle^{\mathfrak{A}} = \emptyset$, muuten $\langle X \rangle^{\mathfrak{A}} = \mathrm{Dom}(\mathfrak{B})$, missä $\mathfrak{B}$ on pienin mallin $\mathfrak{A}$ alimalli, jolle $X \subset \mathrm{Dom}(\mathfrak{B})$.

1.5. Lause. *Olkoon $\mathfrak{A}$ τ-malli ja $X \subset \mathrm{Dom}(\mathfrak{A})$. Tällöin joukon X virittämä joukko $\langle X \rangle^{\mathfrak{A}}$ sisältää täsmälleen ne alkiot, jotka voidaan esittää muodossa $t^{\mathfrak{A}}[a_0/x_0, \ldots, a_{m-1}/x_{m-1}]$, missä $a_0, \ldots, a_{m-1} \in X$ ja $t(x_0, \ldots, x_{m-1})$ on termi.*

Todistus. Merkitään B':lla niiden alkioiden $b \in \mathrm{Dom}(\mathfrak{A})$ joukkoa, jotka voidaan kirjoittaa muodossa $b = t^{\mathfrak{A}}[a_0/x_0, \ldots, a_{m-1}/x_{m-1}]$, missä $a_0, \ldots, a_{m-1} \in X$ ja $t(x_0, \ldots, x_{m-1})$ on termi. Jos $X = \emptyset$, niin $B' = \{\, t^{\mathfrak{A}} \mid t \text{ on aakkoston } \tau \text{ termi} \,\}$, joten jos lisäksi τ ei sisällä vakiosymboleita, niin $B' = \emptyset$. Oletetaan siis, että $X \neq \emptyset$ tai τ sisältää vakiosymboleita.

Ensiksikin $X \subset B'$, sillä jokainen $a \in X$ voidaan kirjoittaa muotoon $a = x^{\mathfrak{A}}[a/x]$. Osoitetaan sitten, että B' on suljettu mallissa $\mathfrak{A}$. Kun $c \in \mathrm{Con}(\tau)$, triviaalisti $c^{\mathfrak{A}} \in B'$. Olkoon $f \in \mathrm{Fun}(\tau)$, $k = \#(f)$, ja $b_0, \ldots, b_{k-1} \in B'$. Valitaan termit $t_i(x_0, \ldots, x_{m-1})$ niin, että $b_i = t_i^{\mathfrak{A}}[a_0/x_0, \ldots, a_{m-1}/x_{m-1}]$, kun $i \in \{0, \ldots, m-1\}$. (Tämä saattaa vaatia muuttujien nimien vaihtelua niin, että muuttujat voidaan tulkita samoin eri termeissä.) Tällöin termille $u = f(t_0, \ldots, t_{k-1})$ on voimassa

$$\begin{aligned} f^{\mathfrak{A}}(b_0, \ldots, b_{k-1}) &= f^{\mathfrak{A}}(t_0^{\mathfrak{A}}[a_0/x_0, \ldots, a_{m-1}/x_{m-1}], \ldots, t_{k-1}^{\mathfrak{A}}[a_0/x_0, \ldots, a_{m-1}/x_{m-1}]) \\ &= u^{\mathfrak{A}}[a_0/x_0, \ldots, a_{m-1}/x_{m-1}] \in B'. \end{aligned}$$

Koska $X \subset B'$ ja B' on suljettu mallissa $\mathfrak{A}$, niin $\mathfrak{A}|B'$ on $\mathfrak{A}$:n alimalli, jolle $X \subset \mathrm{Dom}(\mathfrak{A}|B')$. Siis $\langle X \rangle^{\mathfrak{A}} \subset B'$.

Olkoon toisaalta $\mathfrak{B}$ mallin $\mathfrak{A}$ alimalli, jolle $X \subset \mathrm{Dom}(\mathfrak{B})$. Tällöin jokaisella termillä $t(x_0, \ldots, x_{m-1})$ ja jokaisella $a_0, \ldots, a_{m-1} \in X$ pätee $t^{\mathfrak{A}}[a_0/x_0, \ldots, a_{m-1}/x_{m-1}] = t^{\mathfrak{B}}[a_0/x_0, \ldots, a_{m-1}/x_{m-1}] \in \mathrm{Dom}(\mathfrak{B})$. Siis $B' \subset \mathrm{Dom}(\mathfrak{B})$, ja koska tämä pätee kaikille tällaisille $\mathfrak{B}$, niin $B' \subset \langle X \rangle$. □

2. Lauseet ja kaavat

Yleensä logiikan lauseilla on, kuten termeilläkin, sisäistä rakennetta eli ne muodostuvat tiettyjen sääntöjen mukaan induktiivisesti yksinkertaisemmista osista. Logiikat onkin usein mahdollista määritellä kertomalla, mitä lauseenmuodostusääntöjä lauseita muodostettaessa käytetään. Tässä aliluvussa kuvataan ensimmäisen kertaluvun logiikan lauseiden muodostuksessa käytettyjä sääntöjä. Valtaosa tarkasteltavista logiikoista ei ainoastaan sisällä FO:ta alilogiikkanaan, vaan myös on suljettu tämän lauseenmuodostussääntöjen suhteen.

Atomilauseet

Atomilauseilla tarkoitetaan merkkijonoja, jotka ovat joko muotoa

1) $t = u$, missä t ja u ovat termejä, tai
2) $R(t_0, \ldots, t_{k-1})$, missä R on k-paikkainen relaatiosymboli ja $t_0, \ldots, t_{k-1}$ termejä.

Tavanomaisessa tulkinnassa atomilauseen aakkosto on ensimmäisessä tapauksessa $\tau(t = u) = \tau(t) \cup \tau(u)$ ja toisessa $\tau(R(t_0, \ldots, t_{k-1})) = \bigcup_{i=0}^{k-1} \tau(t_i) \cup \{R\}$. Edelleen jos $\mathfrak{M}$ on σ-malli, jolle $\sigma \supset \tau(\varphi)$, missä φ on tarkasteltava atomilause, niin ensimmäisessä tapauksessa

$$\mathfrak{M} \models t = u, \text{ jos ja vain jos } t^{\mathfrak{M}} = u^{\mathfrak{M}},$$

jälkimmäisessä

$$\mathfrak{M} \models R(t_0, \ldots, t_{k-1}), \text{ jos ja vain jos } (t_0^{\mathfrak{M}}, \ldots, t_{k-1}^{\mathfrak{M}}) \in R^{\mathfrak{M}}.$$

Aakkoston τ atomilauseilla tarkoitetaan niitä atomilauseita φ, joille $\tau(\varphi) \subset \tau$.

Huomautus. Atomilause φ on todellakin merkkijono eli äärellinen jono merkkejä, joista osa on lauseen φ aakkoston $\tau(\varphi)$ symboleita, osa jonossa $=(,)$ esiintyviä loogisia symboleita. Kun t ja u ovat eri termejä, atomilauseet $t = u$ ja $u = t$ ovat eri lauseita, vaikka niiden merkitys on sama, koska niissä esiintyvät symbolit ovat eri järjestyksessä.

2.1. Lause. *Olkoon h homomorfismi mallista $\mathfrak{A}$ malliin $\mathfrak{B}$. Olkoon φ mallien yhteisen aakkoston τ atomilause.*

a) Jos $\mathfrak{A} \models \varphi$, niin $\mathfrak{B} \models \varphi$.

b) Oletetaan, että h on upotus. Tällöin $\mathfrak{A} \models \varphi$, jos ja vain jos $\mathfrak{B} \models \varphi$.

Todistus. Tarkastellaan atomilauseen muodon mukaan kahta eri tapausta.

1) Atomilause φ on muotoa $t = u$, missä t ja u ovat aakkoston τ termejä. Oletetaan, että $\mathfrak{A} \models \varphi$ eli $t^{\mathfrak{A}} = u^{\mathfrak{A}}$. Koska homomorfismit säilyttävät termit (lause 1.2), niin tästä seuraa $t^{\mathfrak{B}} = h(t^{\mathfrak{A}}) = h(u^{\mathfrak{A}}) = u^{\mathfrak{B}}$ eli $\mathfrak{B} \models \varphi$. Kohdan b todistamiseksi oletetaan, että h on vahva ja $\mathfrak{B} \models \varphi$ eli $h(t^{\mathfrak{A}}) = t^{\mathfrak{B}} = u^{\mathfrak{B}} = h(u^{\mathfrak{A}})$. Koska h on upotus, se on injektio, joten $t^{\mathfrak{A}} = u^{\mathfrak{A}}$ eli $\mathfrak{A} \models \varphi$.

2) Oletetaan, että φ on muotoa $R(t_0, \ldots, t_{k-1})$, missä $R \in \tau$ ja $t_0, \ldots, t_{k-1}$ ovat aakkoston τ termejä. Jos nyt $\mathfrak{A} \models \varphi$ eli $(t_0^{\mathfrak{A}}, \ldots, t_{k-1}^{\mathfrak{A}}) \in R^{\mathfrak{A}}$, niin kuvauksen h homomorfisuudesta ja termien säilymisestä seuraa $(t_0^{\mathfrak{B}}, \ldots, t_{k-1}^{\mathfrak{B}}) = (h(t_0^{\mathfrak{A}}), \ldots, h(t_{k-1}^{\mathfrak{A}})) \in R^{\mathfrak{B}}$. Siis $\mathfrak{B} \models \varphi$.

Jos kääntäen $\mathfrak{B} \models \varphi$ ja h on vahva homomorfismi, niin ehdosta $(h(t_0^{\mathfrak{A}}), \ldots, h(t_{k-1}^{\mathfrak{A}})) = (t_0^{\mathfrak{B}}, \ldots, t_{k-1}^{\mathfrak{B}}) \in R^{\mathfrak{B}}$ seuraa $(t_0^{\mathfrak{A}}, \ldots, t_{k-1}^{\mathfrak{A}}) \in R^{\mathfrak{A}}$ eli $\mathfrak{A} \models \varphi$. □

Tällä kurssilla ei tehdä muodollista eroa vakiosymboleiden ja muuttujien eikä lauseiden ja kaavojen välillä. Kun työskentelyaakkosto τ on kiinnitetty, niin vakiosymboleita, jotka eivät ole aakkostossa τ, voi pitää muuttujina. Vastaavasti lausetta φ, jonka aakkostolle pätee $\tau(\varphi) \subset \tau \cup C$ jollakin vakiosymboleiden joukolla C, pidetään aakkoston τ *kaavana*. Jos $C = \{x_0, \ldots, x_{k-1}\}$, tätä voidaan korostaa merkitsemällä kaavaa $\varphi(x_0, \ldots, x_{k-1})$:llä.

Jos $\mathfrak{A}$ on τ-malli ja $\varphi(x_0, \ldots, x_{k-1})$ aakkoston τ kaava, niin φ:n totuutta mallissa $\mathfrak{A}$ ei voi määrittää, ellei φ satu olemaan myös aakkoston τ lause. Olkoot $a_0, \ldots, a_{k-1} \in \mathrm{Dom}(\mathfrak{A})$ ja $\mathfrak{A}^*$ mallin $\mathfrak{A}$ laajennus $\tau \cup \{x_0, \ldots, x_{k-1}\}$-malliksi, jolle $x_i^{\mathfrak{A}^*}$ kaikilla $i \in \{0, \ldots, k-1\}$, ts. $\mathfrak{A}^* = \langle \mathfrak{A}, a_0, \ldots, a_{k-1} \rangle$. Tällöin merkitään

$$\mathfrak{A} \models \varphi[a_0/x_0, \ldots, a_{k-1}/x_{k-1}],$$

jos ja vain jos $\mathfrak{A}^* \models \varphi$.

Näillä merkinnöillä voidaan muotoilla edelliselle lauseelle seuraava suora seuraus:

2.2. Seuraus. Olkoon h homomorfismi τ-mallista $\mathfrak{A}$ τ-malliin $\mathfrak{B}$, $\psi(x_0, \ldots, x_{k-1})$ aakkoston τ atomikaava ja $a_0, \ldots, a_{k-1} \in \mathrm{Dom}(\mathfrak{A})$. Tällöin

a) Jos $\mathfrak{A} \models \psi[a_0/x_0, \ldots, a_{k-1}/x_{k-1}]$, niin $\mathfrak{B} \models \psi[h(a_0)/x_0, \ldots, h(a_{k-1})/x_{k-1}]$.

b) Jos h on upotus, niin $\mathfrak{A} \models \psi[a_0/x_0, \ldots, a_{k-1}/x_{k-1}]$, jos ja vain jos $\mathfrak{B} \models \psi[h(a_0)/x_0, \ldots, h(a_{k-1})/x_{k-1}]$.

Todistus. Merkitään $\mathfrak{A}^* = \langle \mathfrak{A}, a_0, \ldots, a_{k-1} \rangle$ ja $\mathfrak{B}^* = \langle \mathfrak{B}, h(a_0), \ldots, h(a_{k-1}) \rangle$. Tällöin h on paitsi homomorfismi mallista $\mathfrak{A}$ malliin $\mathfrak{B}$, myös homomorfismi mallista $\mathfrak{A}^*$ malliin $\mathfrak{B}^*$. Jos h on vahva homomorfismina mallista $\mathfrak{A}$ malliin $\mathfrak{B}$, se on vahva myös mallista $\mathfrak{A}^*$ malliin $\mathfrak{B}^*$. Siis edellisen lauseen mukaan:

a) jos $\mathfrak{A} \models \psi[a_0/x_0, \ldots, a_{k-1}/x_{k-1}]$ eli $\mathfrak{A}^* \models \psi$, niin $\mathfrak{B}^* \models \psi$ eli $\mathfrak{B} \models \psi[h(a_0)/x_0, \ldots, h(a_{k-1})/x_{k-1}]$,

ja

b) jos h on upotus, niin $\mathfrak{A} \models \psi[a_0/x_0, \ldots, a_{k-1}/x_{k-1}]$, $\mathfrak{A}^* \models \psi$, $\mathfrak{B}^* \models \psi$ ja $\mathfrak{B} \models \psi[h(a_0)/x_0, \ldots, h(a_{k-1})/x_{k-1}]$ ovat kaikki yhtäpitäviä. □

Kun lausetta sovelletaan osittaisiin isomorfismeihin, saadaan:

2.3. Seuraus. Olkoon $p \in \mathrm{Part}(\mathfrak{A}, \mathfrak{B})$, missä $\mathfrak{A}$ ja $\mathfrak{B}$ ovat τ-malleja. Tällöin jokaiselle aakkoston τ atomilauseelle φ pätee

$$\mathfrak{A} \models \varphi, \text{ jos ja vain jos } \mathfrak{B} \models \varphi.$$

Edelleen jos $\vartheta(x_0, \ldots, x_{k-1})$ on aakkoston τ atomikaava ja $a_0, \ldots, a_{k-1} \in \mathrm{dom}(p)$, niin

$$\mathfrak{A} \models \vartheta[a_0/x_0, \ldots, a_{k-1}/x_{k-1}] \text{ ja}$$
$$\mathfrak{B} \models \vartheta[p(a_0)/x_0, \ldots, p(a_{k-1})/x_{k-1}]$$

ovat yhtäpitäviä.

Todistus. Jos $p = \emptyset$, niin aakkosto τ ei sisällä vakiosymboleita eikä näin ollen atomilauseitakaan, joten ensimmäinen väite on triviaalisti totta. Oletetaan siis $p \neq \emptyset$. Tällöin $p\colon \mathfrak{A}^* \cong \mathfrak{B}^*$ jollakin $\mathfrak{A}$:n alimallilla $\mathfrak{A}^*$ ja $\mathfrak{B}$:n alimallilla $\mathfrak{B}^*$. Koska isomorfismi p on myös upotus mallista $\mathfrak{A}^*$ malliin $\mathfrak{B}$ ja kanonista alimallisuhdetta vastaa upotus, saadaan $\mathfrak{A} \models \varphi$, jos ja vain jos $\mathfrak{A}^* \models \varphi$, jos ja vain jos $\mathfrak{B} \models \varphi$.

Jatkoväite seuraa samalla tavalla edellisestä seurauksesta. □

Lauseenmuodostussääntöjä

a) Lauseen φ *negaatiolla* tarkoitetaan lausetta $\neg\varphi$ (merkkijonoa, jossa merkkijonon φ eteen on kirjoitettu looginen symboli $\neg$). Tavanomaisessa tulkinnassa lauseen $\neg\varphi$ aakkosto on $\tau(\neg\varphi) = \tau(\varphi)$. Edelleen

$$\mathfrak{M} \models \neg\varphi, \text{ jos ja vain jos } \mathfrak{M} \not\models \varphi,$$

kun $\mathfrak{M}$ on σ-malli, jolle $\sigma \supset \tau(\varphi)$.

b) Lauseiden φ ja ψ *konjunktio* on $(\varphi \wedge \psi)$. Tavanomaisessa tulkinnassa $\tau(\varphi \wedge \psi) = \tau(\varphi) \cup \tau(\psi)$ (käytännössä konjunktiota vastaavat sulut jätetään kirjoittamatta, jos lauseen pystyy jäsentämään oikein muutenkin) ja

$$\mathfrak{M} \models \varphi \wedge \psi, \text{ jos ja vain jos } \mathfrak{M} \models \varphi \text{ ja } \mathfrak{M} \models \psi,$$

kun $\mathfrak{M}$ on σ-malli, jolle $\tau(\varphi \wedge \psi) \subset \sigma$.

c) Lauseesta φ syntyy *eksistenssikvantifioinnilla* lause $\exists x\varphi$, jolle tavanomaisessa tulkinnassa pätee $\tau(\exists x\varphi) = \tau(\varphi) \setminus \{x\}$. Edelleen

$$\mathfrak{M} \models \exists x\varphi(x),$$

jos ja vain jos mallilla $\mathfrak{M}\restriction\tau(\varphi) \setminus \{x\}$ on laajennus $\mathfrak{M}^*$ aakkoston $\tau(\varphi)$ malliksi, jolle $\mathfrak{M}^* \models \varphi$.

3. Logiikat FO ja FVL

Edellä esitettyjen lauseenmuodostussääntöjen avulla on helppo määritellä ensimmäisen kertaluvun logiikka.

3.1. Määritelmä. *Ensimmäisen kertaluvun logiikka* $\mathrm{FO} = \mathcal{L}_{\omega\omega}$ on pienin logiikka, joka sisältää atomilauseet ja on suljettu negaation, konjunktion ja eksistenssikvantifionnin suhteen.

Lauseiden monimutkaisuutta voi mitata monin tavoin, joista yksinkertaisin lienee lauseen pituus merkkeinä ja käyttökelposimpia kvanttoriaste ja sidottujen muuttujien lukumäärä. Monet ensimmäisen kertaluvun logiikkaa koskevat tulokset etenevät induktiolla kvanttoriasteen suhteen. Lisäksi kvanttoriaste ja muuttujien lukumäärä liittyvät luonnollisella tavalla vaativuusteoreettisiin tarkasteluihin. Näissä kvanttoriastetta vastaa aikavaativuus ja muuttujien lukumäärää tilavaativuus.

3.2. Määritelmä. FO:n lauseen ϑ *kvanttoriaste* $\mathrm{qr}(\vartheta)$ määritellään induktiolla lauseen rakenteen suhteen:

1) $\mathrm{qr}(\vartheta) = 0$, kun ϑ on atomilause.
2) Kun $\vartheta = \neg\psi$, niin $\mathrm{qr}(\vartheta) = \mathrm{qr}(\psi)$.
3) Kun ϑ on muotoa $\varphi \wedge \psi$, niin $\mathrm{qr}(\vartheta) = \max\{\mathrm{qr}(\psi), \mathrm{qr}(\varphi)\}$.
4) Kun ϑ on muotoa $\exists x\psi$, niin $\mathrm{qr}(\exists x\psi) = \mathrm{qr}(\psi) + 1$.

Kvanttoriasteen käyttökelpoisuus perustuu pitkälti seuraavaan tulokseen:

3.3. Lemma. *Olkoon τ äärellinen aakkosto, jossa ei ole funktiosymboleita, ja $r \in \mathbb{N}$. Tällöin loogista ekvivalenssia vaille on olemassa vain äärellisen monta lausetta $\varphi \in \mathrm{FO}[\tau]$, joille $\mathrm{qr}(\varphi) \leq r$.*

Todistus. Väite todistetaan induktiolla luvun $r \in \mathbb{N}$ suhteen yhtaikaa kaikille ehdon toteuttaville aakkostoille τ. Ennen induktion aloittamista osoitetaan kaksi aputulosta, joihin induktiotodistus perustuu.

1) Aakkoston τ atomilauseita φ on vain äärellinen määrä. Aakkoston τ äärellisyyden vuoksi nimittäin $k = |\mathrm{Con}(\tau)|$, $s = |\mathrm{Rel}(\tau)|$ ja $m = \max\{\, \#(R) \mid R \in \mathrm{Rel}(\tau) \,\}$ ovat äärellisiä. Koska τ ei sisällä funktiosymboleita, niin termejä ovat vain vakiosymbolit, joita on k kappaletta. Muotoa $c = d$, $c, d \in \mathrm{Con}(t)$, olevia atomilauseita on siis k^2 kappaletta. Kullakin $R \in \mathrm{Rel}(\tau)$ muotoa $R(c_0, \ldots, c_{n_R-1})$ olevia atomilauseita on taas k^{n_R} kappaletta, missä $n_R = \#(R)$. Siis atomilauseita on korkeintaan $k^2 + s \cdot k^m$ kappaletta.

2) Äärellisen joukon Φ lauseesta voidaan muodostaa loogista ekvivalenssia vaille vain äärellinen määrä Boolen kombinaatioita. Merkitään nimittäin jokaisella $\Phi_0 \subset \Phi$

$$\psi_{\Phi_0} = \bigwedge_{\varphi \in \Phi_0} \varphi \wedge \bigwedge_{\varphi \in \Phi \setminus \Phi_0} \neg\varphi$$

ja $\Psi = \{\, \psi_{\Phi_0} \mid \Phi_0 \subset \Phi \,\}$. Selvästi $\psi \wedge \psi'$ on ristiriitainen lause, kun $\psi, \psi' \in \Psi$ ovat eri lauseita, ja $\bigvee_{\psi \in \Psi} \psi$ on tautologia. Merkitään jokaisella $\Psi_0 \subset \Psi$

$$\vartheta_{\Psi_0} = \bigvee_{\psi \in \Psi_0} \psi$$

ja $\Theta = \{\, \vartheta_{\Psi_0} \mid \Psi_0 \subset \Psi \,\}$. Tällöin $|\Theta| = 2^{|\Psi|} = 2^{2^{|\Phi|}}$ eli Θ on äärellinen. Kun $\varphi \in \Phi$, φ on loogisesti ekvivalentti lauseen

$$\bigvee_{\substack{\Phi_0 \subset \Phi, \\ \varphi \in \Phi_0}} \psi_{\Phi_0} \in \Theta$$

kanssa. On helppoa osoittaa, että kun $\Psi_0, \Psi_1 \subset \Psi$, niin $\neg\vartheta_{\Psi_0}$ on loogisesti ekvivalentti $\vartheta_{\Psi \setminus \Psi_0}$:n ja $\vartheta_{\Psi_0} \wedge \vartheta_{\Psi_1}$ lauseen $\vartheta_{\Psi_0 \cap \Psi_1}$ kanssa, joten Θ on loogista ekvivalenssia vaille suljettu negaation ja konjuktion ja siis Boolen kombinaatioiden suhteen.

Todistetaan nyt induktiolla itse väite.

3) Kvanttoriastetta 0 olevia eli *kvanttorittomia* $\mathrm{FO}[\tau]$:n lauseita on loogista ekvivalenssia vaille vain äärellisen monta, koska kvanttorittomat lauseet ovat Boolen kombinaatioita atomilauseista. Kohdan 1 nojalla aakkoston τ atomilauseita on vain äärellisen monta, ja kohdan 2 nojalla näistä voi muodostaa loogista ekvivalenssia vaille vain äärellisen monta Boolen kombinaatiota.

4) Tarkastellaan lauseita $\vartheta \in \mathrm{FO}[\tau]$, joille $\mathrm{qr}(\vartheta) \leq r + 1$. Induktio-oletuksen mukaan korkeintaan kvanttoriastetta r olevia $\mathrm{FO}[\tau]$:n lauseita on äärellinen määrä, kuten myös τ-kaavoja $\psi(x)$ eli lauseita $\psi \in \mathrm{FO}[\tau \cup \{x\}]$, joille $\mathrm{qr}(\psi) = r$, missä $x \notin \tau$ on kiinnitetty muuttuja. Siis on olemassa äärellinen joukko $\Phi \subset \mathrm{FO}[\tau]$, joka sisältää loogista ekvivalenssia vaille kaikki lauseet $\varphi \in \mathrm{FO}[\tau]$, joille joko $\mathrm{qr}(\varphi) \leq r$ tai φ on muotoa $\exists x\psi$, missä $\mathrm{qr}(\psi) = r$. Jokainen $\vartheta \in \mathrm{FO}[\tau]$, jolle $\mathrm{qr}(\vartheta) \leq r + 1$, on loogisesti ekvivalentti joukon Φ lauseesta muodostetun Boolen kombinaation kanssa, joita kohdan 2 mukaan on äärellinen määrä (loogista ekvivalenssia vaille). □

3.4. Määritelmä. Olkoot $\mathfrak{A}$ ja $\mathfrak{B}$ saman aakkoston τ malleja ja $k \in \mathbb{N}$. $\mathfrak{A}$ *ja* $\mathfrak{B}$ *ovat kvanttoriasteeseen* k *saakka ekvivalentteja*, $\mathfrak{A} \equiv_k \mathfrak{B}$, jos kaikille logiikan FO aakkoston τ lauseille, joille $\mathrm{qr}(\varphi) \leq k$, pätee $\mathfrak{A} \models \varphi$, jos ja vain jos $\mathfrak{B} \models \varphi$.

Mielivaltainen konjuktio

Toisen tärkeän logiikan muodostamiseen tarvitaan vielä yksi uusi lauseenmuodostussääntö. Lausejoukon Φ *mielivaltaisella konjuktiolla* tarkoitetaan lausetta $\bigwedge \Phi$. Tavanomaisessa tulkinnassa konjuktion $\bigwedge \Phi$ aakkosto on $\tau(\bigwedge \Phi) = \bigcup_{\varphi \in \Phi} \tau(\varphi)$ ja jos $\mathfrak{M}$ on σ-malli, jolle $\sigma \supset \tau(\bigwedge \Phi)$, niin $\mathfrak{M} \models \bigwedge \Phi$ täsmälleen silloin, kun kaikilla $\varphi \in \Phi$ pätee $\mathfrak{M} \models \varphi$.

Merkintä $\bigwedge \Phi$ on siinä mielessä hämäävä, että jos Φ on ääretön, $\bigwedge \Phi$ ei millään voi olla merkkijono. Merkintä pitääkin mieltää lyhennysmerkinnäksi parille $(\bigwedge, \Phi)$. Aiemmatkin lauseenmuodostussäännöt voi ymmärtää joukko-opillisesti niin, että jos negaatioita, konjuktioita tai eksistenssikvantifioituja lauseita muodostetaan merkkijonoista, niin tuloskin on merkkijono, mutta muuten vain sopivanlainen joukko, esim. $\neg\varphi$ olisi tällöin $(\neg, \varphi)$.

Vaihtoehtoinen merkintä lauseelle $\bigwedge \Phi$ on $\bigwedge_{\varphi \in \Phi} \varphi$. Jos $\Phi = \{ \varphi_i \mid i \in I \}$, niin myös indeksoitu merkintä $\bigwedge_{i \in I} \varphi_i$ on luonnollinen. Näitä merkintöjä voi käyttää myös siinä tapauksessa, että Φ on äärellinen joukko ensimmäisen kertaluvun lauseita, jolloin konjunktiota voidaan tarkastella logiikan FO lauseena.

3.5. Määritelmä. $\mathcal{L}_{\infty\omega}$ on pienin logiikka, joka sisältää atomilauseet ja on suljettu negaation, mielivaltaisten konjunktioiden ja eksistenssikvantifionnin suhteen.

Logiikka $\mathcal{L}_{\infty\omega}$ on äärellisten mallien kannalta käyttökelvottoman voimakas: jokainen malliluokka jonkin kiinteän aakkoston äärellisiä malleja on $\mathcal{L}_{\infty\omega}$:ssa määriteltävissä. Muuttujien määrää rajoittamalla saadaan kuitenkin muodostettua hyödyllinen $\mathcal{L}_{\infty\omega}$:n alilogiikka.

3.6. Määritelmä. Logiikan $\mathcal{L}_{\infty\omega}$ lauseen φ *sidottujen muuttujien* joukko $\mathrm{bv}(\varphi)$ määritellään induktiolla:

1) $\mathrm{bv}(\varphi) = \emptyset$, kun φ on atomilause.
2) $\mathrm{bv}(\neg\vartheta) = \mathrm{bv}(\vartheta)$.
3) $\mathrm{bv}(\bigwedge \Phi) = \bigcup_{\varphi \in \Phi} \mathrm{bv}(\varphi)$.
4) $\mathrm{bv}(\exists x \psi) = \mathrm{bv}(\psi) \cup \{x\}$.

3.7. Määritelmä. *Äärellisen monen muuttujan logiikka* $\mathrm{FVL} = \mathcal{L}^{\omega}_{\infty\omega}$ on $\mathcal{L}_{\infty\omega}$:n alilogiikka, joka sisältää täsmälleen ne $\mathcal{L}_{\infty\omega}$:n lauseet ϑ, joissa on vain äärellisen monta sidottua muuttujaa eli joille $\mathrm{bv}(\vartheta)$ on äärellinen.

4. FO:n pelikarakterisaatio

Osassa I esiteltiin osittainen isomorfismi asteeseen k saakka ja k muuttujan suhteen puhtaasti kombinatorisesti. Seuraavien kahden luvun tarkoituksena on osoittaa, että

nämä relaatiot ja niitä vastaavat pelit voi karakterisoida puhtaasti loogisten käsitteiden avulla.

Merkitään $h\colon A \rightharpoonup B$, jos h on osittainen kuvaus joukosta A joukkoon B eli kuvaus, jolle $h \subset A \times B$. Seuraava apukäsite helpottaa todistusten seuraamista.

4.1. Määritelmä. Olkoot $\mathfrak{A}, \mathfrak{B}$ aakkoston t malleja ja $h\colon \mathrm{Dom}(\mathfrak{A}) \rightharpoonup \mathrm{Dom}(\mathfrak{B})$. Kuvaus h *säilyttää* aakkoston τ kaavan $\vartheta(x_0, \ldots, x_{m-1})$, jos kaikilla $a_0, \ldots, a_{m-1} \in \mathrm{dom}(h)$ pätee:

$$\text{jos } \mathfrak{A} \models \vartheta[a_0/x_0, \ldots, a_{m-1}/x_{m-1}], \text{ niin } \mathfrak{B} \models \vartheta[h(a_0)/x_0, \ldots, h(a_{m-1})/x_{m-1}].$$

Kuvaus h *säilyttää kaavan ϑ vahvasti*, jos kaikilla $a_0, \ldots, a_{m-1} \in \mathrm{dom}(h)$ on voimassa

$$\mathfrak{A} \models \vartheta[a_0/x_0, \ldots, a_{m-1}/x_{m-1}], \text{ jos ja vain jos } \mathfrak{B} \models \vartheta[h(a_0)/x_0, \ldots, h(a_{m-1})/x_{m-1}].$$

Seurauksen 2.2 voi nyt muotoilla: osittaiset isomorfismit säilyttävät atomikaavat vahvasti. Huomattakoon myös, että $p \in \mathrm{Part}(\mathfrak{A}, \mathfrak{B})$ säilyttää kaavan ϑ vahvasti täsmälleen silloin, kun p säilyttää kaavan ϑ ja $p^{-1} \in \mathrm{Part}(\mathfrak{B}, \mathfrak{A})$ säilyttää kaavan ϑ.

4.2. Lemma. *Olkoon $p \in \mathrm{Part}(\mathfrak{A}, \mathfrak{B})$ ja $I \subset \mathrm{Part}(\mathfrak{A}, \mathfrak{B})$, missä $\mathfrak{A}$ ja $\mathfrak{B}$ ovat τ-malleja. Oletetaan, että jokainen $q \in I$ säilyttää aakkoston τ kaavan $\vartheta(\boldsymbol{x}, y)$. Oletetaan lisäksi, että p laajenee eteenpäin joukkoon I. Tällöin p säilyttää kaavan $\exists y\vartheta(\boldsymbol{x}, y)$. Jos lisäksi jokainen $q \in I$ säilyttää kaavan ϑ jopa vahvasti ja p laajenee edestakaisesti joukkoon I, niin p säilyttää kaavan $\exists y\vartheta(\boldsymbol{x}, y)$ vahvasti.*

Todistus. Merkitään muuttujajonon muuttujia $\boldsymbol{x} = (x_0, \ldots, x_{m-1})$. Oletetaan, että $\mathfrak{A} \models \exists y\vartheta[a_0/x_0, \ldots, a_{m-1}/x_{m-1}]$, missä $a_0, \ldots, a_{m-1} \in \mathrm{dom}(p)$. Valitaan $c \in \mathrm{Dom}(\mathfrak{A})$, jolle $\mathfrak{A} \models \vartheta[a_0/x_0, \ldots, a_{m-1}/x_{m-1}, c/y]$. Koska p laajenee eteenpäin joukkoon I, on olemassa $q \in I$, jolle $p \subset q$ ja $c \in \mathrm{dom}(q)$. Koska q säilyttää kaavan ϑ, niin

$$\mathfrak{B} \models \vartheta[q(a_0)/x_0, \ldots, q(a_{m-1})/x_{m-1}, q(c)/y]$$

eli

$$\mathfrak{B} \models \vartheta[p(a_0)/x_0, \ldots, p(a_{m-1})/x_{m-1}, q(c)/y],$$

sillä $q{\restriction}\{a_0, \ldots, a_{m-1}\} = p{\restriction}\{a_0, \ldots, a_{m-1}\}$. Siis $\mathfrak{B} \models \exists y\vartheta[p(a_0)/x_0, \ldots, p(a_{m-1})/x_{m-1}]$, joten p säilyttää kaavan $\exists y\vartheta(\boldsymbol{x}, y)$.

Oletetaan, että p laajenee joukkoon I jopa edestakaisesti ja jokainen $q \in I$ säilyttää kaavan ϑ vahvasti. Tällöin p^{-1} laajenee eteenpäin joukkoon I^{-1} ja jokainen $r \in I^{-1}$ säilyttää kaavan ϑ. Siis myös p^{-1} säilyttää kaavan $\exists y\vartheta$. Koska sekä p että p^{-1} säilyttävät kaavan $\exists y\vartheta$, p säilyttää sen vahvasti. □

Nyt tavoitellusta karakterisaatiosta voidaan todistaa toinen puoli.

4.3. Lause. *Olkoot $\mathfrak{A}$ ja $\mathfrak{B}$ saman aakkoston τ malleja, joille $(I_0, \ldots, I_k)\colon \mathfrak{A} \cong_k \mathfrak{B}$. Olkoon $p \in I_s$, missä $s \in \{0, \ldots, k\}$. Tällöin p säilyttää vahvasti jokaisen* FO*:n aakkoston τ kaavan ϑ, jolle $\mathrm{qr}(\vartheta) \leq s$.*

Todistus. Todistetaan väite induktiolla kaavan ϑ rakenteen suhteen kaikille $p \in I_s$, $s \in \{0, \ldots, k\}$.

1) Jos ϑ on atomikaava, niin jokainen $p \in \mathrm{Part}(\mathfrak{A}, \mathfrak{B})$ ja erityisesti jokainen $p \in I_s$, $s \in \{0, \ldots, k\}$, säilyttää vahvasti kaavan ϑ.

2) Oletetaan, että p säilyttää kaavan ϑ vahvasti. Koska p säilyttää kaavan ϑ, niin p^{-1} säilyttää kaavan $\neg\vartheta$. Koska p^{-1} säilyttää kaavan ϑ, niin p säilyttää kaavan $\neg\neg\vartheta$. Siis p säilyttää kaavan $\neg\neg\vartheta$ vahvasti.

3) Oletetaan, että $\vartheta(x_0, \ldots, x_{m-1})$ on muotoa $\varphi \wedge \psi$ ja $\mathrm{qr}(\vartheta) \leq s$, $p \in I_s$, $s \in \{0, \ldots, k\}$. Tällöin $\mathrm{qr}(\varphi) \leq s$ ja $\mathrm{qr}(\psi) \leq s$, joten induktio-oletuksen mukaan p säilyttää kaavat φ ja ψ vahvasti. Siis kun $a_0, \ldots, a_{m-1} \in \mathrm{dom}(p)$, niin seuraavat ovat yhtäpitäviä:

a) $\mathfrak{A} \models \vartheta[a_0/x_0, \ldots, a_{m-1}/x_{m-1}]$,

a') $\mathfrak{A} \models \varphi[a_0/x_0, \ldots, a_{m-1}/x_{m-1}]$ ja $\mathfrak{A} \models \psi[a_0/x_0, \ldots, a_{m-1}/x_{m-1}]$,

b') $\mathfrak{B} \models \varphi[p(a_0)/x_0, \ldots, p(a_{m-1})/x_{m-1}]$ ja $\mathfrak{B} \models \psi[p(a_0)/x_0, \ldots, p(a_{m-1})/x_{m-1}]$ sekä

b) $\mathfrak{B} \models \vartheta[p(a_0)/x_0, \ldots, p(a_{m-1})/x_{m-1}]$.

4) Oletetaan, että $\vartheta(\boldsymbol{x})$ on muotoa $\exists y \psi(\boldsymbol{x}, y)$. Oletetaan lisäksi, että $p \in I_{s+1}$, $s \in \{0, \ldots, k-1\}$ ja $\mathrm{qr}(\vartheta) \leq s+1$. Siis $\mathrm{qr}(\psi) \leq s$. Oletuksesta $(I_0, \ldots, I_k)\colon \mathfrak{A} \cong_k \mathfrak{B}$ seuraa, että $p \in I_{s+1}$ laajenee edestakaisesti joukkoon I_s. Induktio-oletuksen nojalla jokainen $q \in I_s$ säilyttää vahvasti kaavan ψ. Edellisestä lemmasta seuraa sen vuoksi, että p säilyttää kaavan $\exists y \psi(\boldsymbol{x}, y)$ eli ϑ:n. □

4.4. Seuraus. Jos $\mathfrak{A} \cong_k \mathfrak{B}$, niin $\mathfrak{A} \equiv_k \mathfrak{B}$.

Todistus. Jos $\mathfrak{A} \cong_k \mathfrak{B}$, niin $(I_0, \ldots, I_k)\colon \mathfrak{A} \cong_k \mathfrak{B}$ joillakin $I_i \subset \mathrm{Part}(\mathfrak{A}, \mathfrak{B})$, $i \in \{0, \ldots, k\}$. Tässä $I_k \neq \emptyset$; valitaan $p \in I_k$ mielivaltaisesti. Edellisen lauseen mukaan p säilyttää vahvasti kaikki lauseet $\varphi \in \mathrm{FO}[\tau]$, $\mathrm{qr}(\varphi) \leq k$, missä τ on mallien $\mathfrak{A}$ ja $\mathfrak{B}$ yhteinen aakkosto. Mutta tämähän tarkoittaa, että näille lauseille pätee $\mathfrak{A} \models \varphi$ täsmälleen silloin, kun $\mathfrak{B} \models \varphi$. □

Edellistä tulosta ei voi kääntää aivan kaikissa tilanteissa, mutta kylläkin riittävän usein.

4.5. Lause. *Olkoon τ äärellinen relationaalinen aakkosto, $k \in \mathbb{N}$ ja $\mathfrak{A}, \mathfrak{B}$ τ-malleja, joille $\mathfrak{A} \equiv_k \mathfrak{B}$. Tällöin $\mathfrak{A} \cong_k \mathfrak{B}$.*

Todistus. Kun $r \in \{0, \ldots, k\}$, joukko I_r sisältäköön ne äärelliset $p \in \mathrm{Part}(\mathfrak{A}, \mathfrak{B})$, jotka säilyttävät (vahvasti) kaikki FO:n aakkoston τ kaavat ϑ, joille $\mathrm{qr}(\vartheta) \leq r$. Jos $m = |p|$, niin rajoituksetta voidaan olettaa, että tässä kaava on muotoa $\vartheta(x_0, \ldots, x_{m-1})$, ts. kaavassa ϑ esiintyy korkeintaan m muuttujaa ja ne on valittu kiinteästä joukosta $\{x_0, \ldots, x_{m-1}\}$. Lemman 3.3 mukaan tällaisia kaavoja (eli logiikan FO aakkoston $\tau \cup \{x_0, \ldots, x_{m-1}\}$ lauseita) on vain äärellisen monta loogista ekvivalenssia vaille.

Oletuksesta $\mathfrak{A} \equiv_k \mathfrak{B}$ seuraa, että $\emptyset$ säilyttää kaikki lauseet $\varphi \in \mathrm{FO}[\tau]$, joille $\mathrm{qr}(\varphi) \leq k$. Siis $\emptyset \in I_i$ kaikilla $i \in \{0, \ldots, k\}$, joten joukot I_i ovat epätyhjiä.

Riittää enää osoittaa, että kaikilla $i \in \{0, \ldots, k\}$ jokainen $p \in I_{i+1}$ laajenee edestakaisesti joukkoon I_i. Olkoon $\mathrm{dom}(p) = \{a_0, \ldots, a_{m-1}\}$. Symmetrian vuoksi riittää jälleen tarkastella vain laajentamista eteenpäin. Olkoon $c \in \mathrm{Dom}(\mathfrak{A})$. Väitetään, että jollakin $b \in \mathrm{Dom}(\mathfrak{B})$ pätee $q_b = p \cup \{(c, b)\} \in I_i$. Muutenhan jokaisella $b \in \mathrm{Dom}(\mathfrak{B})$ pätisi $q_b \notin I_i$, mistä seuraa, että on olemassa korkeintaan kvanttoriastetta i oleva FO:n τ-kaava $\vartheta_b(x_0, \ldots, x_{m-1}, x_m)$, jolle

$$\mathfrak{A} \not\models \vartheta_b[a_0/x_0, \ldots, a_{m-1}/x_{m-1}, c/x_m],$$

vaikka

$$\mathfrak{B} \models \vartheta_b[q_b(a_0)/x_0, \ldots, q_b(a_{m-1})/x_{m-1}, q_b(c)/x_m]$$

eli

$$\mathfrak{B} \models \vartheta_b[p(a_0)/x_0, \ldots, p(a_{m-1})/x_{m-1}, b/x_m].$$

Erilaisia kaavoja ϑ_b on vain äärellinen määrä (kun loogisesti ekvivalentit kaavat valitaan aina samoiksi), joten $\mathfrak{B} \models \varphi[p(a_0)/x_0, \ldots, p(a_{m-1})/x_{m-1}]$, missä φ on FO:n kaava

$$\forall x_m \bigvee_{b \in \mathrm{Dom}(\mathfrak{B})} \vartheta_b(x_0, \ldots, x_{m-1}, x_m).$$

Kuitenkin $\mathfrak{A} \models \bigwedge_{b \in \mathrm{Dom}(\mathfrak{B})} \neg\vartheta_b[a_0/x_0, \ldots, a_{m-1}/x_{m-1}, c/x_m]$, joten

$$\mathfrak{A} \not\models \varphi[a_0/x_0, \ldots, a_{m-1}/x_{m-1}].$$

Tämä on ristiriidassa sen kanssa, että kuvauksen p piti säilyttää φ vahvasti.

Siis jollakin $b \in \mathrm{Dom}(\mathfrak{B})$ pätee $p \cup \{(c, b)\} \in I_i$, joten p laajenee eteenpäin joukkoon I_i. □

Yhdistämällä edellinen lause seuraukseen 4.4 saadaan:

4.6. Seuraus. Olkoon τ äärellinen relationaalinen aakkosto, $k \in \mathbb{N}$ ja $\mathfrak{A}, \mathfrak{B}$ τ-malleja. Tällöin $\mathfrak{A} \equiv_k \mathfrak{B}$, jos ja vain jos $\mathfrak{A} \cong_k \mathfrak{B}$.

5. FVL:n pelikarakterisaatio

Logiikan FVL^k ekvivalenssin karakterisointi etenee samoja latuja kuin ekvivalenssin $\equiv_k$, ja todistuksissa päästään hyödyntämään jo saatuja aputuloksia. Tiettyjä erityispiirteitä seuraa siitä, että kvanttoriasteen sijasta nyt tarkastellaan muuttujien lukumääriä. Yleensä logiikan $\mathcal{L}$ aakkoston τ kaavoiksi kelpuutetaan kaikki ne lauseet φ, joille $\tau(\varphi) \setminus \tau$ sisältää vain muuttujia (eli vakiosymboleita). Logiikoille $\mathcal{L}_{\infty\omega}$ ja FVL tämä toimiikin, mutta logiikalle FVL^k tavanomainen kaavan määritelmä ei ole tarkoituksenmukainen, sillä jos kaavassa $\varphi(x_0, \ldots, x_{m-1})$ esiintyy ℓ sidottua muuttujaa, niin lauseessa $\exists x_0 \ldots \exists x_{m-1}\varphi$ voi olla $\ell + m$ sidottua muuttujaa, nimittäin silloin, kun muuttujat $x_0, \ldots, x_{m-1}$ eivät esiinny kaavassa φ sidottuina. On siis mahdollista, että $\varphi \in \mathrm{FVL}^k[\tau \cup \{x_0, \ldots, x_{m-1}\}]$, mutta $\exists x_0 \ldots \exists x_{m-1}\varphi \notin \mathrm{FVL}^k[\tau]$.

5.1. Määritelmä. Olkoon $k \in \mathbb{N}$. Merkitään $\mathrm{fv}_\tau(\varphi) = \tau(\varphi) \setminus \tau$, kun φ on logiikan $\mathcal{L}_{\infty\omega}$ aakkoston τ kaava. Kaavaa φ sanotaan *aakkoston τ alilogiikan* FVL^k *kaavaksi*, jos φ:ssä esiintyy kaikkiaan korkeintaan k muuttujaa, ts.

$$|\mathrm{bv}(\varphi) \cup \mathrm{fv}_\tau(\varphi)| \leq k.$$

Huomattakoon, että tämäkin kaavan määritelmä sallii induktiotodistukset kiinteän aakkoston τ logiikan FVL^k kaavojen suhteen. Yksinkertaisimmin tämän voi ilmaista

niin, että kaavan alikaavoissa esiintyy korkeintaan niin monta muuttujaa kuin kaavassa itsessään.

5.2. Lause. *Olkoot $\mathfrak{A}$ ja $\mathfrak{B}$ relationaalisen aakkoston τ malleja, joille $I\colon \mathfrak{A} \cong^k \mathfrak{B}$. Tällöin jokainen aakkoston τ logiikan* FVL^k *kaava ϑ säilyy vahvasti jokaisessa kuvauksessa $p \in I$.*

Todistus. Todistetaan väite induktiolla kaavan ϑ rakenteen suhteen.

1) Seurauksessa 2.2 on osoitettu, että kaikki $p \in I \subset \mathrm{Part}(\mathfrak{A}, \mathfrak{B})$ säilyttävät vahvasti atomikaavat.

2) Oletetaan, että $\vartheta = \neg\psi$. Induktio-oletuksen mukaan jokainen $p \in I$ säilyttää vahvasti kaavan ψ, mikä on selvästi yhtäpitävää sen kanssa, että nämä kuvaukset säilyttävät vahvasti myös kaavan ϑ.

3) Oletetaan, että $\vartheta(x_0, \ldots, x_{k-1})$ on muotoa $\bigwedge \Phi$, missä jokainen $p \in I$ säilyttää vahvasti jokaisen $\varphi \in \Phi$. Olkoon $p \in I$ ja $a_0, \ldots, a_{k-1} \in \mathrm{dom}(p)$. Jos

$$\mathfrak{A} \models \vartheta[a_0/x_0, \ldots, a_{k-1}/x_{k-1}],$$

niin $\mathfrak{A} \models \varphi[a_0/x_0, \ldots, a_{k-1}/x_{k-1}]$ kaikilla $\varphi \in \Phi$. Induktio-oletuksen mukaan $\mathfrak{B} \models \varphi[p(a_0)/x_0, \ldots, p(a_{k-1})/x_{k-1}]$ kaikilla $\varphi \in \Phi$, joten $\mathfrak{B} \models \vartheta[p(a_0)/x_0, \ldots, p(a_{k-1})/x_{k-1}]$. Samalla tavalla osoitetaan, että jos $\mathfrak{B} \models \vartheta[p(a_0)/x_0, \ldots, p(a_{k-1})/x_{k-1}]$, niin $\mathfrak{A} \models \vartheta[a_0/x_0, \ldots, a_{k-1}/x_{k-1}]$. Siis p säilyttää vahvasti kaavan ϑ.

4) Oletetaan, että ϑ on muotoa $\exists x\psi$ ja jokainen $q \in I$ säilyttää vahvasti kaavan ψ. Olkoon $p \in I$. Koska kaavassa ϑ esiintyy korkeintaan k muuttujaa, joista x vain sidottuna, niin ϑ on muotoa $\vartheta(y_0, \ldots, y_{k-2})$. Olkoot $a_0, \ldots, a_{k-2} \in \mathrm{dom}(p)$. Merkitään $r = p{\restriction}\{a_0, \ldots, a_{k-2}\}$; tällöin $|r| \leq k-1 < k$, joten r laajenee edestakaisesti joukkoon I. Koska jokainen $q \in I$ säilyttää vahvasti kaavan ψ, lemmasta 4.2 seuraa, että r säilyttää kaavan $\exists x\psi$. Siis

$$\mathfrak{A} \models \vartheta[a_0/x_0, \ldots, a_{k-2}/x_{k-2}],$$

jos ja vain jos

$$\mathfrak{B} \models \vartheta[r(a_0)/x_0, \ldots, r(a_{k-2})/x_{k-2}],$$

eli

$$\mathfrak{B} \models \vartheta[p(a_0)/x_0, \ldots, p(a_{k-2})/x_{k-2}]. \quad \square$$

5.3. Lause. *Olkoot $\mathfrak{A}$ ja $\mathfrak{B}$ relationaalisen aakkoston τ malleja. Jos $\mathfrak{A} \equiv \mathfrak{B}$* ($\mathrm{FVL}^k$)*, niin $\mathfrak{A} \cong^k \mathfrak{B}$.*

Todistus. Joukko I sisältäköön kaikki $p \in \mathrm{Part}(\mathfrak{A}, \mathfrak{B})$, joille $|p| \leq k$ ja jotka säilyttävät jokaisen logiikan FVL^k aakkoston τ kaavan, missä τ on mallien $\mathfrak{A}$ ja $\mathfrak{B}$ yhteinen aakkosto. Koska $\mathfrak{A} \equiv \mathfrak{B}$ (FVL^k), pätee $\emptyset \in I$ (tyhjä kuvaus säilyttää triviaalisti kaavat, jotka eivät ole aakkoston τ lauseita). Rajoitusehto $|p| \leq k$ pätee, kun $p \in I$, ja I on selvästi rajoittumien suhteen suljettu.

Jäljelle jää osoittaa, että jokainen $p \in I$, $|p| < k$, laajenee edestakaisesti joukkoon I. Olkoon $b \in \mathrm{Dom}(\mathfrak{B})$; etsitään sellainen $c \in \mathrm{Dom}(\mathfrak{A})$, että $p \cup \{(c, b)\} \in I$. Oletetaan vastoin tätä tavoitetta, että jokaisella $c \in \mathrm{Dom}(\mathfrak{A})$ pätee $q_c = p \cup \{(c, b)\} \notin I$. Merkitään $\mathrm{dom}(p) = \{a_0, \ldots, a_{m-1}\}$, missä $m < k$. Tällöin jokaista

$c \in \mathrm{Dom}(\mathfrak{A})$ vastaa sellainen logiikan FVL^k aakkoston τ kaava $\vartheta_a(x_0, \ldots, x_{m-1}, y)$, että $\mathfrak{B} \not\models \vartheta_a[p(a_0)/x_0, \ldots, p(a_{m-1})/x_{m-1}, b/y]$, vaikka $\mathfrak{A} \models \vartheta_a[a_0/x_0, \ldots, a_{m-1}/x_{m-1}, c/y]$. Siis $\mathfrak{A} \models \varphi[a_0/x_0, \ldots, a_{m-1}/x_{m-1}]$, missä $\varphi(x_0, \ldots, x_{m-1})$ on

$$\forall y \bigvee_{a \in \mathrm{Dom}(\mathfrak{A})} \vartheta_a(x_0, \ldots, x_{m-1}, y),$$

mutta $\mathfrak{B} \not\models \varphi[p(a_0)/x_0, \ldots, p(a_{m-1})/x_{m-1}]$. Kuitenkin jokainen ϑ_a on FVL^k:n kaava, jossa sidotut muuttujat on voitu valita niin, että $\mathrm{fv}_\tau(\vartheta_a) \cup \mathrm{bv}(\vartheta_a) \subset \{x_0, \ldots, x_{k-2}, y\}$. Tällöin φ on FVL^k:n aakkoston τ kaava, mikä on ristiriidassa sen kanssa, että p säilyttää kaikki tällaiset kaavat vahvasti.

Siis p laajenee taaksepäin joukkoon I. Symmetrisellä tavalla osoitetaan eteenpäin laajeneminen. □

Yhdistämällä edelliset lauseet saadaan:

5.4. Seuraus. Olkoot $\mathfrak{A}$ ja $\mathfrak{B}$ saman relationaalisen aakkoston τ malleja. Tällöin $\mathfrak{A} \equiv \mathfrak{B}$ (FVL^k), jos ja vain jos $\mathfrak{A} \cong^k \mathfrak{B}$. □

6. Määrittelemättömyystuloksia

Osan I kombinatorista tuloksista voidaan johtaa nopeasti muutamia määrittelemättömyystuloksia. Johdettavat tulokset ovat helppoja, mutta kuvaavat hyvin, miten pelikarakterisaatioita voi käytää tämäntyyppisten tulosten johtamiseen. Lisäksi nämäkin yksinkertaiset lauseet kertovat perustavanlaatuisia seikkoja FO:n ja FVL:n ilmaisukykyjen rajoista.

6.1. Lause. *Olkoon $S \subset \mathbb{N}$ ääretön joukko, jolle myös $\mathbb{N} \setminus S$ on ääretön. Tällöin ei ole olemassa sellaista lausetta $\varphi \in \mathrm{FVL}[\emptyset]$, että jokaiselle äärelliselle puhtaalle joukolle $\langle A \rangle$ pätisi*

$$\langle A \rangle \models \varphi, \text{ jos ja vain jos } |A| \in S.$$

Todistus. Oletetaan vastoin väitettä, että tällainen φ olisi olemassa. Merkitään $k = |\mathrm{bv}(\varphi)|$. Koska S ja $\mathbb{N} \setminus S$ ovat äärettömiä, on olemassa $m \in S$ ja $m \in \mathbb{N} \setminus S$, joille $m > k$ ja $n > k$. Valitaan joukot A ja B niin, että $|A| = m$ ja $|B| = n$. Tällöin $\langle A \rangle \models \varphi$ ja $\langle B \rangle \not\models \varphi$. Toisaalta luvun I.7 puhtaita joukkoja koskevista tuloksista tiedetään, että $\langle A \rangle \cong^k \langle B \rangle$, joten FVL:n pelikarakterisaatiosta seuraa $\langle A \rangle \equiv \langle B \rangle$ (FVL^k). Erityisesti $\langle A \rangle \models \varphi$, jos ja vain jos $\langle B \rangle \models \varphi$, mikä on ristiriidassa edellisen virkkeen kanssa. □

6.2. Seuraus. Mallin koon parillisuus ei ole ilmaistavissa ensimmäisen kertaluvun logiikassa.

Todistus. Valitaan lauseessa joukoksi $S = \{\, 2n \mid n \in \mathbb{N} \,\}$, ja käytetään hyväksi sitä, että FO:n lauseet ovat myös FVL:n lauseita. □

Ensimmäisen kertaluvun logiikassa saadaan, toisin kuin äärellisen monen muuttujan logiikassa, sama tulos myös lineaarijärjestetyissä joukoissa.

6.3. Lause. *Olkoon $S \subset \mathbb{N}$ ääretön joukko, jolle myös $\mathbb{N} \setminus S$ on ääretön. Tällöin ei ole olemassa sellaista lausetta $\varphi \in \mathrm{FO}[\{\leq\}]$, että jokaiselle lineaarijärjestetylle joukolle $\mathfrak{A}$ pätisi*

$$\mathfrak{A} \models \varphi, \text{ jos ja vain jos } \mathrm{card}(\mathfrak{A}) \in S.$$

Todistus. Oletetaan vastoin väitettä, että tällainen φ olisi olemassa. Merkitään $r = \mathrm{qr}(\varphi)$ ja valitaan $m \in S$ ja $n \in \mathbb{N} \setminus S$ niin, että $m > 2^r$ ja $n > 2^r$. Osan I luvun 7 ja FO:n pelikarakterisaation nojalla $\mathfrak{L}_m \cong_k \mathfrak{L}_n$ eli $\mathfrak{L}_m \equiv_k \mathfrak{L}_n$, joten $\mathfrak{L}_m \models \varphi$, jos ja vain jos $\mathfrak{L}_n \models \varphi$. Toisaalta pitäisi olla voimassa $\mathfrak{L}_m \models \varphi$ ja $\mathfrak{L}_n \not\models \varphi$, sillä $m \in S$ ja $n \in \mathbb{N} \setminus S$, mikä on ristiriita. □

Harjoituksia osaan III

1. Olkoon τ aakkosto, joka sisältää kaksipaikkaisen funktiosymbolin f mutta ei muita funktiosymboleita. Osoita, että jokaista tämän aakkoston $\{f\}$ termiä t vastaa seuraavanlainen termi t':
1) Kaikki funktiosymbolin f esiintymät ovat termissä ennen vakiosymboleiden esiintymiä.
2) Jos $\mathfrak{M}$ on τ-malli, jossa $f^{\mathfrak{M}}$ on liitännäinen, niin $t^{\mathfrak{M}} = (t')^{\mathfrak{M}}$.

2. Olkoon f yksipaikkainen funktiosymboli. Tarkastellaan aakkoston $\{f\}$ viiden alkion malleja $\mathfrak{M}$.
a) Esitä esimerkki tällaisesta $\mathfrak{M}$ ja yksiöstä $\{a\}$, joka virittää koko mallin eli $\langle\{a\}\rangle_{\mathfrak{M}} = \mathfrak{M}$, vaikka kahden alkion joukko $\{b, c\} \subset \mathrm{Dom}(\mathfrak{M})$ ei viritä koko mallia.
b) Voivatko kaikki kahden alkion osajoukot $A \subset \mathrm{Dom}(\mathfrak{M})$ olla suljettuja viiden alkion $\{f\}$-mallissa $\mathfrak{M}$, vaikka $f^{\mathfrak{M}}$ ei olisi identtinen kuvaus?
c) Esitä jokaisella $k \in \{1, 2, 3, 4, 5\}$ esimerkki mallista $\mathfrak{M}$, jossa yksiöt virittävät kaikkiaan k eri mallin $\mathfrak{M}$ alimallia.

3. Olkoon A äärellinen joukko. *Joukon A symmetrinen ryhmä* on ryhmä $\mathbf{Sym}(A) = \langle \mathrm{Sym}(A), \circ \rangle$, missä $\mathrm{Sym}(A) = \{\, f \mid f \text{ on joukon } A \text{ permutaatio} \,\}$. Määritä pienin määrä alkioita, jolla ryhmän $\mathbf{Sym}(A)$ voi virittää.

4. Ryhmän $\mathbb{G}$ *kommutaattoreilla* tarkoitetaan muotoa $[a, b] = a^{-1}b^{-1}ab$, $a, b \in \mathrm{Dom}(\mathbb{G})$, olevia alkioita. Ryhmän $\mathbb{G}$ *kommutaattorialiryhmä* $\mathbb{G}'$ on $\mathbb{G}$:n kommutattoreiden virittämä aliryhmä. Olkoon h surjektiivinen homomorfismi ryhmästä $\mathbb{G}$ ryhmään $\mathbb{H}$. Todista, että $h \restriction \mathrm{Dom}(G')$ on homomorfismi ryhmästä $\mathbb{G}'$ ryhmään $\mathbb{H}'$.

5. Olkoon s yksipaikkainen funktiosymboli. Määrittele luvut m, joille on olemassa aakkoston $\{s\}$ malli $\mathfrak{A}$, jossa on neljä alkiota ja jolla on täsmälleen m alimallia. (Vihje: luokittele mallit ensin sen mukaan, mikä on pienin $\mathrm{Dom}(\mathfrak{A})$:n ekvivalenssirelaatio E, jolle $s^{\mathfrak{A}} \subset E$.)

6. Olkoon f yksipaikkainen funktiosymboli.
a) Osoita, että ovat olemassa aakkoston $\{f\}$ ensimmäisen kertaluvun lauseet φ ja ψ, joille

$$\mathfrak{M} \models \varphi, \text{ jos ja vain jos } f^{\mathfrak{M}} \text{ on injektio}$$

ja

$$\mathfrak{M} \models \psi, \text{ jos ja vain jos } f^{\mathfrak{M}} \text{ on surjektio.}$$

b) Esitä esimerkki ensimmäisen kertaluvun $\{f\}$-lauseesta, jolla on äärettömiä mutta ei lainkaan äärellisiä malleja.

7. Osoita, että ensimmäisen kertaluvun logiikassa voidaan ilmaista (samassa mielessä kuin edellisen tehtävän kohdassa a):
a) Aakkoston $\{\leq\}$ malli $\mathfrak{M}$ on esilineaarijärjestetty joukko.

b) Aakkoston $\{\cdot\}$ malli $\mathbb{G}$ on ryhmä.

8. Olkoon $\mathfrak{Z}_n$ aakkoston $\{+\}$ malli, missä $\mathrm{Dom}(\mathfrak{Z}_n) = \{0, \ldots, n-1\}$ ja $+^{\mathfrak{Z}_n}$ on yhteenlasku modulo n. Esitä esimerkki ensimmäisen kertaluvun lauseesta, joka on totta mallissa $\mathfrak{Z}_{13}$ mutta ei mallissa $\mathfrak{Z}_{17}$.

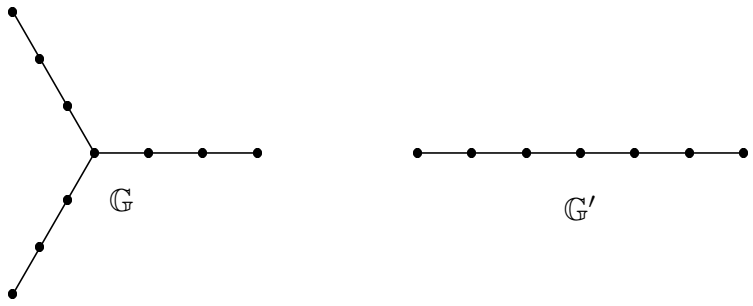
9. Perinteisessä vuosilukutehtävässä muodostetaan kulloisenkin vuoden vuosiluvusta peräkkäisiä luonnollisia lukuja peruslaskutoimitusten avulla:

$$0 = 1 \cdot (9 - 6 - 3),\ 1 = 1 + 9 - 6 - 3,\ \ldots.$$

Logiikan avulla tehtävän voi määritellä näin:

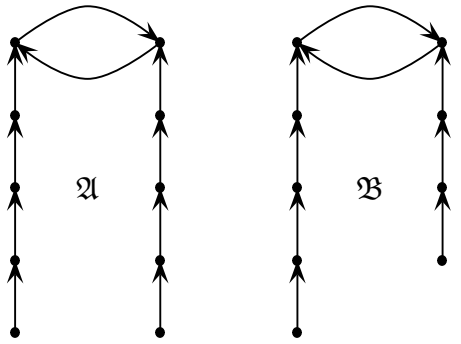
Olkoon $\mathfrak{Q}$ aakkoston $\tau = \{+, -, \cdot, /, a, b, c, d\}$ malli, jolle $\mathrm{Dom}(\mathfrak{Q}) = \mathbb{Q}$ ja laskutoimitukset on tulkittu tavanomaisesti, paitsi että $q/^{\mathfrak{Q}}0 = 0$ kaikilla $q \in \mathbb{Q}$. Vakioiden a, b, c, d tulkinnat ovat vuosiluvun numerot $a^{\mathfrak{Q}} = 1$, $b^{\mathfrak{Q}} = 9$, $c^{\mathfrak{Q}} = 6$ ja $d^{\mathfrak{Q}} = 3$. Luonnollisen luvun n sanotaan olevan *esitettävissä*, jos on olemassa aakkoston τ termi t, jonka tulkinta on $t^{\mathfrak{Q}} = n$ ja jossa jokainen vakiosymboli esiintyy täsmälleen kerran, ja vieläpä järjestyksessä a, b, c, d. Tehtävänä on löytää sellainen luku $M \in \mathbb{N}$, että luvut $0, \ldots, M$ ovat esitettävissä mutta $M + 1$ ei. Ratkaise vuoden 1963 vuosilukutehtävä.

10. Esitä esimerkki mahdollisimman alhaista kvanttoriastetta r olevasta ensimmäisen kertaluvun logiikan lauseesta φ, joka on totta kuvan verkossa $\mathbb{G}$, mutta ei verkossa $\mathbb{G}'$. Huomaa perustella, miksi r ei voi olla pienempi (vrt.tehtävään II.3).



11. Aakkoston $\{R\}$, $\#(R) = 2$, malleissa $\mathfrak{A}$ ja $\mathfrak{B}$ on kuvan mukaiset relaatiot. Kuinka korkeata kvanttoriastetta $r \in \mathbb{N}$ oleva FO:n lause tarvitaan erottamaan mallit $\mathfrak{A}$ ja $\mathfrak{B}$ toisistaan? Vrt. tehtävään II.15, jossa analysoitiin

mallien välistä helmipeliä. Tässä tarvitaan Ehrenfeuchtin ja Fraïssén peliä.)



12. Olkoon $n \in \mathbb{N}$, $n > 1$. Osoita, ettei ole olemassa tyhjän aakkoston ensimmäisen kertaluvun lauseita φ ja ψ_n (eli lauseita $\varphi \in \mathrm{FO}[\emptyset]$ ja $\psi_n \in \mathrm{FO}[\emptyset]$), joille pätee jokaisessa äärellisessä mallissa $\mathfrak{M}$

a) $\mathfrak{M} \models \varphi$, jos ja vain jos $\mathrm{card}(\mathfrak{M})$ on alkuluku.

b) $\mathfrak{M} \models \psi_n$, jos ja vain jos $\mathrm{card}(\mathfrak{M})$ on luvulla n jaollinen.

(Käytä hyväksesi tietoja puhtaiden joukkojen osittaisista isomorfiaominaisuuksista.)

13. Todista, ettei ensimmäisen kertaluvun lauseella voi ilmaista aakkostossa $\{U, V\}$ ($\#(U) = \#(V) = 1$), että U:n ja V:n tulkinnat ovat yhtämahtavia. Toisin sanoen: Ei ole olemassa sellaista $\varphi \in \mathrm{FO}[\{U, V\}]$, että jokaisessa $\{U, V\}$-mallissa $\mathfrak{M}$ pätee $\mathfrak{M} \models \varphi$, jos ja vain jos $\left|U^{\mathfrak{M}}\right| = \left|V^{\mathfrak{M}}\right|$.

14. Olkoon $\tau = \{E\}$, missä E on kaksipaikkainen.

a) Kirjoita FO:n lause, joka ilmaisee E:n tulkinnan olevan mallin universumin ekvivalenssirelaatio. Onko kirjoittamasi lauseen kvanttoriaste 3?

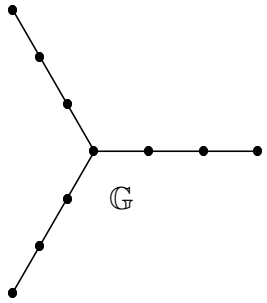
b) Etsi sellaiset τ-mallit $\mathfrak{A}$ ja $\mathfrak{B}$, että $E^{\mathfrak{A}}$ on $\mathrm{Dom}(\mathfrak{A})$:n ekvivalenssirelaatio, $\mathfrak{A} \cong_2 \mathfrak{B}$, mutta $E^{\mathfrak{B}}$ ei ole transitiivinen.

c) Osoita, että kohdan a lausetta ei voi korvata lauseella, jonka kvanttoriaste olisi 2.

15. Lause $\varphi \in \mathrm{FO}[\tau]$ on τ-mallin $\mathfrak{M}$ *Scottin lause*, jos $\mathfrak{M} \models \varphi$ ja kaikille $\mathfrak{N} \in \mathrm{Str}(\tau)$, jotka ovat lauseen φ malleja, pätee $\mathfrak{M} \cong \mathfrak{N}$. Mallin $\mathfrak{M}$ *Scottin korkeus* on

$$\mathrm{Sh}(\mathfrak{M}) = \min(\{\, \mathrm{qr}(\varphi) \mid \varphi \text{ mallin } \mathfrak{M} \text{ Scottin lause} \,\} \cup \{\infty\}).$$

Määritä alla olevan verkon $\mathbb{G}$ Scottin korkeus.



16. Olkoon E kaksipaikkainen relaatiosymboli ja $n \in \mathbb{N}$, $n \geq 3$. Osoita, että kvanttoriastetta n olevilla FO[$\{E\}$]:n lauseilla ei voi ilmaista seuraavia:

a) Ekvivalenssirelaatiolla on vähintään $n+1$ ekvivalenssiluokkaa.
b) Kussakin ekvivalenssiluokassa on vähintään $n+1$ alkiota.

Kirjoita FO:n lauseet, jotka ilmaisevat em. asiat kvanttoriastetta $n+1$ olevalla lauseella.

17. Osoita, että jokaista $r \in \mathbb{N}$ vastaa sellainen $n \in \mathbb{N}$, että yhdestä n-syklistä koostuva verkko $\mathbb{G}$ on kahdesta n-syklistä koostuvan verkon $\mathbb{G}'$ kanssa asteeseen r saakka osittaisesti isomorfinen. Tässä siis $\mathrm{Dom}(\mathbb{G}) = \{0, \ldots, n-1\}$, $\mathrm{Dom}(\mathbb{G}') = \{0, \ldots, 2n-1\}$ sekä

$$E^{\mathbb{G}} = \{\, (k, k+1) \mid k = 0, \ldots, n-2 \,\} \cup \{(n-1, 0)\}$$

ja

$$\begin{aligned} E^{\mathbb{G}'} =& \{\, (k, k+1) \mid k = 0, \ldots, n-2 \,\} \cup \{(n-1, 0)\} \\ & \cup \{\, (k, k+1) \mid k = n, \ldots, 2n-2 \,\} \cup \{(2n-1, n)\} \end{aligned}$$

18. Osoita edellisen tehtävän avulla, että yhtenäisyys ei ole ilmaistavissa ensimmäisen kertaluvun logiikassa FO.

19. Osoita, että äärellisten verkkojen yhtenäisyys on määriteltävissä äärellisen monen muuttujan logiikalla FVL, ja määritä pienin määrä muuttujia, joka tarvitaan tämän ilmaisemiseen.

20. Osoita edelleen, että kaikilla $k, \ell, r \in \mathbb{Z}_+$ on olemassa sellaiset $\mathbb{G}$ ja $\mathbb{G}'$, että $\mathbb{G}$:ssä on k yhtenäistä komponenttia, $\mathbb{G}'$:ssa ℓ yhtenäistä komponenttia ja $\mathbb{G} \cong_r \mathbb{G}'$.

21. Olkoon $\mathcal{K}$ mielivaltainen isomorfian suhteen suljettu luokka järjestettyjä τ-malleja, missä τ on äärellinen yksi- ja kaksipaikkaisista relaatiosymboleista koostuva aakkosto. (Huomaa, että luentomuistiinpanoissa selitetyn käytännön mukaan järjestetty malli on aina äärellinen.) Osoita, että $\mathcal{K}$ on määriteltävissä kahden muuttujan logiikassa FVL^2.

Olkoot $\mathfrak{A}$ ja $\mathfrak{B}$ relationaalisen aakkoston τ malleja. Oletetaan, että $\mathrm{Dom}(\mathfrak{A}) \cap \mathrm{Dom}(\mathfrak{B}) = \emptyset$. *Mallien $\mathfrak{A}$ ja $\mathfrak{B}$ mallipari $\mathfrak{A} \oplus \mathfrak{B}$ määritellään seuraavasti: Otetaan käyttöön kaksi uutta yksipaikkaista relaatiosymbolia U ja V. Merkitään $\sigma = \tau \cup \{U, V\}$. Tällöin $\mathfrak{A} \oplus \mathfrak{B}$ on aakkoston σ malli, jolle*

$$\begin{aligned} &\mathrm{Dom}(\mathfrak{A} \oplus \mathfrak{B}) = \mathrm{Dom}(\mathfrak{A}) \cup \mathrm{Dom}(\mathfrak{B}), \\ &U^{\mathfrak{A}} = \mathrm{Dom}(\mathfrak{A}),\ V^{\mathfrak{A}} = \mathrm{Dom}(\mathfrak{B}) \text{ ja} \\ &R^{\mathfrak{A} \oplus \mathfrak{B}} = R^{\mathfrak{A}} \cup R^{\mathfrak{B}}, \end{aligned}$$

kun $R \in \tau$. Mallipari voidaan määritellä myös, kun $\mathrm{Dom}(\mathfrak{A}) \cap \mathrm{Dom}(\mathfrak{B}) \neq \emptyset$: *Valitaan $\mathfrak{B}' \cong \mathfrak{B}$, jolle* $\mathrm{Dom}(\mathfrak{A}) \cup \mathrm{Dom}(\mathfrak{B}') = \emptyset$, *ja asetetaan $\mathfrak{A} \oplus \mathfrak{B} = \mathfrak{A} \oplus \mathfrak{B}'$. Mallipari on tällöin isomorfiaa vaille yksikäsitteisesti määritelty riippumatta siitä, mikä on mallin $\mathfrak{B}'$ valintamekanismi.*

22. Osoita, ettei ole olemassa sellaista lausetta $\vartheta \in \mathrm{FVL}[\{E, U, V\}]$, että kaikilla verkoilla $\mathbb{G}, \mathbb{H}$, joiden perusjoukot ovat erillisiä, pätisi seuraava:

$$\mathbb{G} \text{ uppoaa verkkoon } \mathbb{H}, \text{ jos ja vain jos } \mathbb{G} \oplus \mathbb{H} \models \vartheta,$$

missä $\mathbb{G} \oplus \mathbb{H}$ on $\{E, U, V\}$-malli, jolle $(\mathbb{G} \oplus \mathbb{H}) \restriction \{E\} = \mathbb{G} \sqcup \mathbb{H}$, $U^{\mathbb{G} \oplus \mathbb{H}} = \mathrm{Dom}(\mathbb{G})$ ja $V^{\mathbb{G} \oplus \mathbb{H}} = \mathrm{Dom}(\mathbb{H})$.

23. Olkoot $\mathfrak{A}$, $\mathfrak{A}'$, $\mathfrak{B}$ ja $\mathfrak{B}'$ relationaalisia saman aakkoston malleja, joilla on erilliset perusjoukot.

a) Osoita, että jos p on osittainen isomorfismi mallista $\mathfrak{A}$ malliin $\mathfrak{A}'$ ja q on osittainen isomorfismi mallista $\mathfrak{B}$ malliin $\mathfrak{B}'$, niin $p \cup q$ on osittainen isomorfismi malliparista $\mathfrak{A} \oplus \mathfrak{B}$ malliparin $\mathfrak{A}' \oplus \mathfrak{B}'$.

b) Näytä, että jos $\mathfrak{A} \cong_k \mathfrak{A}'$ ja $\mathfrak{B} \cong_k \mathfrak{B}'$, niin $\mathfrak{A} \oplus \mathfrak{B} \cong_k \mathfrak{A}' \oplus \mathfrak{B}'$.

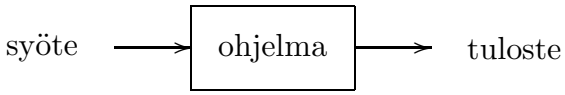
24. Olkoon τ relationaalinen äärellinen aakkosto ja $\vartheta \in \mathrm{FO}[\sigma]$, missä $\sigma = \tau \cup \{U, V\}$. Osoita, että on olemassa sellaiset äärelliset joukot $\Phi, \Psi \subset \mathrm{FO}[\tau]$, että lauseen ϑ totuusarvo mallissa $\mathfrak{A} \oplus \mathfrak{B}$ riippuu vain lauseiden Φ totuusarvoista mallissa $\mathfrak{A}$ ja lauseiden Ψ totuusarvoista mallissa $\mathfrak{B}$, kun $\mathfrak{A}$ ja $\mathfrak{B}$ ovat erillisiä τ-malleja.

25. Osoita, että äärellisten verkkojen yhtenäisyys on määriteltävissä äärellisen monen muuttujan logiikalla FVL, ja määritä pienin määrä muuttujia, joka tarvitaan tämän ilmaisemiseen.

IV Kuvailevaa vaativuusteoriaa

Edellisissä luvuissa on ollut esimerkkejä malleista: toisaalta puhtaasti matemaattisia objekteja, kuten ryhmiä, lineaarijärjestettyjä joukkoja ja verkkoja, toisaalta sellaisia malleja, kuten suomalaisten sukulaisuussuhteita kuvaava malli, jotka ovat luonteeltaan pikemminkin tietokantoja. Itse asiassa relationaalisen aakkoston malli ja relaatiotietokanta ovat likipitäen samoja asioita. Oleellista on, että äärellistä mallia voi hyvällä syyllä pitää tietokoneohjelman syötteen rakenteisena, siis korkean abstraktiotason, kuvauksena. Tämä avaa mahdollisuuden analysoida tietokoneiden laskentaa loogisten käsitteiden avulla, mitä kutsutaan *deskriptiiviseksi eli kuvailevaksi vaativuusteoriaksi*.

Tarkastellaan alla olevaa vahvasti idealisoitua kuvaa laskennasta:

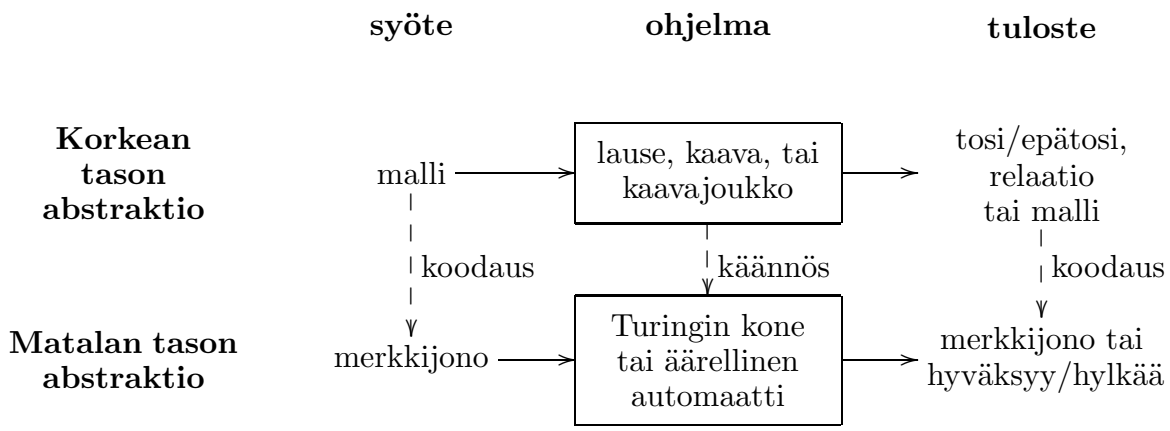


(Tietokoneohjelmat ovat nykyään tietenkin yleensä interaktiivisia, joten syötteet ja tulosteet vuorottelevat. Tällöinkin yllä olevaa kaaviota voidaan pitää laskennan yksittäisen askeleen kuvauksena, eikä mikään estä soveltamasta logiikkaa tässäkin tapauksessa. Osa deskriptiivisestä vaativuusteoriasta painottuukin niin sanottujen dynaamisten logiikoiden tutkimukseen, mitä ei ole valitettavasti mahdollista tarkastella tällä kurssilla.)

Tietojenkäsittelyn laskentaa on tutkittu teoreettisesti jo 1930-luvulta alkaen, siis ennen tietokoneiden aikakautta. Lyhyen ajanjakson aikana Church, Kleene, Turing ja Post esittelivät useita eri laskennan malleja ja perustavanlaatuisia laskettavuuden teorian tuloksia. Laskennan malleista Alan Turingin esittelemä on saavuttanut vakiintuneen aseman teoreettisessa tietojenkäsittelyssä. Turingin malli edustaa matalan tason abstraktiota: syöte ja tuloste ovat merkkijonoja, joista syöte on laskennan alkaessa kirjoitettuna syötenauhalle ja tuloste laskennan loputtua tulostenauhalla. Lisäksi ohjelmalla on käytössään yksi tai useampia tulostenauhoja. Itse ohjelma, Turingin kone, esitetään tila-automaattina.

Äärellisten mallien teoria tuo mukanaan korkean tason abstraktion. Syötteinä tarkastellaan nyt malleja; tulosteet ovat tilanteen mukaan joko malleja, relaatioita (toisin sanoen mallin osia) tai vastauksia tosi/epätosi. Logiikan lauseet, kaavat tai kaavajoukot mielletään nyt ohjelmiksi. Ajatus siis on, että kun malli syötetään lauseelle, vastaukseksi

saadaan tieto, onko lause tosi vai epätosi. Tilanne näyttää siis tältä:



Kaavion äärellinen automaatti, johon tutustutaan seuraavassa luvussa, on eräänlainen riisuttu versio Turingin koneesta. "Matalan tason abstraktiota" ei pidä lainkaan ymmärtää halventavana ilmaisuna; matalan ja korkean tason abstraktioita tarvitaan eri asioiden kuvaamiseen. Turingin kone on oiva väline ohjelmien tila- ja aikavaatimusten teoreettiseen tutkimukseen. Turingin koneen suorittamat askeleet ovat niin yksinkertaisia ja samantyyppisiä, että niiden on syytä ajatella kuluttavan saman verran aikaa kunkin. Samoin merkkijonojen pituuksien avulla voi laskea ohjelman vaatiman muistitilan suuruutta.

Korkean tason abstraktioista malli on syötteen ja logiikan lause ohjelman rakenteen kuvaus. Erityisesti erilaiset kvantifioinnit vastaavat ohjelmassa esiintyviä kontrollirakenteita. Tarkastellaan esimerkiksi kysymystä, onko $\{\leq\}$-mallin $\mathfrak{M}$ relaatio $\leq^{\mathfrak{M}}$ antisymmetrinen. Antisymmetrisyyttä vastaa ensimmäisen kertaluvun lause

$$\forall x \forall y((x \leq y \wedge y \leq x) \rightarrow x = y)$$

jonka totuutta mallissa tutkittaisiin seuraavalla algoritmilla:

vast $\leftarrow$ true; % *oletusarvo*
for $a \in \mathrm{Dom}(\mathfrak{M})$
  for $b \in \mathrm{Dom}(\mathfrak{M})$
    if $(a \leq^{\mathfrak{M}} b)$ **and** $(b \leq^{\mathfrak{M}} a)$ **and** $(a \neq b)$
    then vast $\leftarrow$ false;
return vast.

Universaalikvantifiointi $\forall x$ kääntyy siis varsin suoraviivaisella tavalla ohjelman kontrollirakenteeksi **for** $a \in \mathrm{Dom}(\mathfrak{M}) \ldots$. Tämä ei kuitenkaan riitä ainoaksi kontrollirakenteeksi, joten jatkossa tullaan tutustumaan useisiin FO:ta voimakkaampiin logiikoihin, joissa on uusia kvantifiointitapoja, jotka vastaavat voimakkampia kontrollirakenteita.

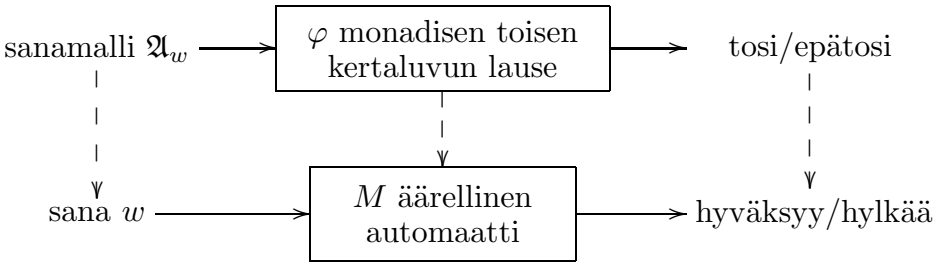
Yksi kaavion oleellisista piirteistä on siinä esiintyvät koodaukset ja käännökset, joiden avulla luodaan vastaavuuksia korkean ja matalan abstraktiotason välille. Esimerkiksi polynomiaalisessa ajassa ratkeavien ongelmien luokka PTIME määritellään

Turingin koneen avulla matalalla tasolla, ja sitä vastaa kiintopistelogiikka IFP (järjestettyjen mallien luokassa) korkealla tasolla. Yleensä mallien koodaaminen merkkijonoiksi on rutiininomaista työtä, ja varsinaiset ongelmat piilevät käännöksiin liittyvissä todistuksissa.

Tässä luvussa tarkastellaan kahta koodaus-käännös-tilannetta: ensin tarkastellaan äärellisten automaattien ja monadisen toisen kertaluvun logiikan suhdetta, sitten vaativuusluokkaa PTIME ja kiintopistelogiikkaa IFP. Ensimmäisen tapauksen tilanne on varsin rajoittunut ja yksinkertainen, joten se toimii hyvin johdatuksena deskriptiiviseen vaativuusteoriaan.

1. Sanamallit ja äärelliset automaatit

Seuraavassa kahdessa luvussa esitellään seuraavaan kaavioon liittyvät käsitteet ja tulokset:



Merkit, sanat ja kielet

Olkoon Σ epätyhjä *merkistö* eli joukko merkkejä. (Merkit eivät välttämättä ole aakkoston symboleita, mutta ovat samalla tavalla rakenteettomia. Tällä kurssilla merkkeihin ei liitetä mitään tulkintaa.) Merkistön Σ *sanoilla* tarkoitetaan yksinkertaisesti joukon Σ alkioista muodostettuja äärellispituisia jonoja. Merkistön Σ sanojen joukkoa merkitään Σ^*:llä, ts $\Sigma^* = \bigcup_{n\in\mathbb{N}} \Sigma^n$. On tavanomaista merkitä jonoa $w = (\alpha_0, \ldots, \alpha_{n-1}) \in \Sigma^*$ lyhyesti $w = \alpha_0 \ldots \alpha_{n-1}$. Vastaavasti sanojen $w_1, w_2 \in \Sigma^*$ katenaatiota eli yhteenliittämistä $w = w_1 \hat{} w_2$ merkitään $w = w_1 w_2$. Sanan $w = \alpha_0 \ldots \alpha_{n-1}$, missä $\alpha_0, \ldots, \alpha_{n-1} \in \Sigma$ ja $n \in \mathbb{N}$, pituus on $n = |w| \in \mathbb{N}$. Erityisesti on olemassa yksikäsitteinen sana, jonka pituus on nolla; tätä tyhjää jonoa merkitään $\lambda = ()$.

Merkistön Σ *kielellä* L tarkoitetaan osajoukkoa $L \subset \Sigma^*$. Kielistä voi muodostaa uusia kieliä paitsi joukko-opillisilla operaatioilla, myös yhteenliittämisellä:

$$L_1 L_2 = \{\, w_1 w_2 \mid w_1 \in L_1,\ w_2 \in L_2 \,\} \quad (L_1, L_2 \subset \Sigma^*)$$

ja toistolla ($L \subset \Sigma^*$):

$$L^* = \{\, w_0 \ldots w_{n-1} \mid n \in \mathbb{N}, \text{ jokaisella } i = 0, \ldots, n-1 \text{ pätee } w_i \in L \,\}$$

Jälkimmäinen merkintä yleistää luonnollisella tavalla merkintää Σ^*, L^* koostuu siis niistä sanoista, jotka saadaan liittämällä äärellisen monta L:n sanaa peräkkäin. Edelleen merkitään $L^+ = LL^*$, erityisesti $\Sigma^+ = \Sigma^* \setminus \{\lambda\}$.

Sanamallit

Sanaa $w \in \Sigma^+$ vastaamaan ajatellaan sanamalli $\mathfrak{A}_w$ seuraavien periaatteiden mukaisesti: On luonnollista vaatia, että mallissa $\mathfrak{A}_w$ on yhtä monta alkiota kuin mikä on sanan w pituus. Koska sanassa w yleensä on samojen merkkien toistoa, mallin $\mathfrak{A}_w$ universumin on syytä olla pikemminkin sanan indeksien eli merkkien paikkojen joukko kuin merkkien joukko. Sanassa w merkit ovat tietyssä järjestyksessä, jonka on syytä heijastua myös sanamalliin $\mathfrak{A}_w$. Jotta tiedettäisiin, mikä merkki on missäkin paikassa, tarvitaan yksipaikkaisia relaatiosymboleita.

Jatkossa oletetaan, että on olemassa jokin mekanismi liittää merkkiin α yksipaikkainen relaatiosymboli U_α. Merkistöä Σ vastaavalla aakkostolla tarkoitetaan tällöin aakkostoa

$$\tau = \{\leq\} \cup \{\, U_\alpha \mid \alpha \in \Sigma \,\}.$$

Näin päädytään seuraavaan määritelmään:

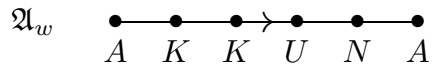
1.1. Määritelmä. Olkoon Σ merkistö ja τ sitä vastaava aakkosto. Sanaa $w = \alpha_0 \dots \alpha_{n-1} \in \Sigma^+$ vastaavalla *sanamallilla* tarkoitetaan aakkoston τ mallia $\mathfrak{A}_w$, jolle

$$\mathrm{Dom}(\mathfrak{A}_w) = \{0, \dots, n-1\},$$

$$\leq^{\mathfrak{A}_w} \text{ on } \mathrm{Dom}(\mathfrak{A}_w)\text{:n luonnollinen järjestys,}$$

$$U_\alpha = \{\, i \in \{0, \dots, n-1\} \mid \alpha_i = \alpha \,\}, \text{ kun } \alpha \in \Sigma.$$

1.2. Esimerkki. Olkoon $\Sigma = \{\mathsf{a}, \mathsf{b}, \mathsf{c}, \dots, \mathsf{å}, \mathsf{ä}, \mathsf{ö}\}$ ja $w = \mathsf{akkuna} \in \Sigma$. Tällaisessa konkreettisessa tapauksessa on luonnollista olettaa, että $A = U_{\mathsf{a}}$, $B = U_{\mathsf{b}}$ ja niin edelleen eli pienaakkosta vastaava yksipaikkainen relaatiosymboli on vastaava suuraakkonen. Tällöin $\mathfrak{A}_w$ on malli, jolle $\mathrm{Dom}(\mathfrak{A}_w) = \{0, 1, \dots, 5\}$, $\leq^{\mathfrak{A}_w} = \{\, (i,j) \in \mathbb{N} \times \mathbb{N} \mid 0 \leq i \leq j \leq 5 \,\}$, $A^{\mathfrak{A}_w} = \{0, 5\}$, $K^{\mathfrak{A}_w} = \{1, 2\}$, $N^{\mathfrak{A}_w} = \{4\}$, $U^{\mathfrak{A}_w} = \{3\}$ ja muiden symboleiden tulkinnat ovat tyhjiä. Kuvana:



Huomautus. Sanaa λ ei vastaa sanamalli, koska mallin universumi on määritelmän mukaan epätyhjä. Siksi määritelmässä on oletus $w \in \Sigma^+ = \Sigma^* \setminus \{\lambda\}$.

Olkoon Σ merkistö ja τ sitä vastaava aakkosto. Varsin helposti huomataan, että äärellinen τ-malli $\mathfrak{B}$ on isomorfinen jonkin sanamallin kanssa, jos ja vain jos
1) $\leq^{\mathfrak{B}}$ on $\mathrm{Dom}(\mathfrak{B})$:n lineaarijärjestys ja

2) $\mathrm{Dom}(\mathfrak{B})$ on erillinen yhdiste joukoista $U_\alpha^{\mathfrak{B}}$, $\alpha \in \Sigma$, eli $\bigcup_{\alpha\in\Sigma} U_\alpha^{\mathfrak{B}} = \mathrm{Dom}(\mathfrak{B})$ ja $U_\alpha \cap U_\beta = \emptyset$, kun $\alpha, \beta \in \Sigma$, $\alpha \neq \beta$.

Tämä on FO:ssa ilmaistavissa. Olkoon $\psi_\Sigma \in \mathrm{FO}[\tau]$ seuraava lause

$$\vartheta \wedge \forall x \bigvee_{\alpha\in\Sigma} U_\alpha(x) \wedge \bigwedge_{\substack{\alpha,\beta\in\Sigma \\ \alpha\neq\beta}} \neg\exists x \left(U_\alpha(x) \wedge U_\beta(x)\right),$$

missä ϑ ilmaisee kohdan 1. Tällöin äärelliselle τ-mallille $\mathfrak{B}$ pätee $\mathfrak{B} \models \psi_\Sigma$, jos ja vain jos jollakin $w \in \Sigma^+$ $\quad \mathfrak{B} \cong \mathfrak{A}_w$.

Sanojen katenoimista eli liittämistä yhteen vastaa mallien puolella operaatio, joka on luonnollista määritellä laajemmassa kuin sanamallien luokassa, nimittäin järjestetyille malleille.

1.3. Määritelmä. Olkoot $\mathfrak{A}$ ja $\mathfrak{B}$ saman relationaalisen aakkoston τ järjestettyjä malleja. Mallien $\mathfrak{A}$ ja $\mathfrak{B}$ *järjestetty summa* $\mathfrak{A} \lhd\!\!\cdot \mathfrak{B}$ on tällöin seuraavalla tavalla muodostettu τ-malli $\mathfrak{C}$:

Olkoon $\mathfrak{B}' \cong \mathfrak{B}$ sellainen mallin $\mathfrak{B}$ isomorfinen kopio, että $\mathrm{Dom}(\mathfrak{A})$ ja $\mathrm{Dom}(\mathfrak{B}')$ ovat erillisiä. Tällöin

1) $\mathrm{Dom}(\mathfrak{C}) = \mathrm{Dom}(\mathfrak{A}) \cup \mathrm{Dom}(\mathfrak{B}')$,
2) $\leq^{\mathfrak{C}} = \leq^{\mathfrak{A}} \cup \leq^{\mathfrak{B}} \cup \{\, (a,b) \mid a \in \mathrm{Dom}(\mathfrak{A}), b \in \mathrm{Dom}(\mathfrak{B}') \,\}$ (ts. järjestyksessä $\leq^{\mathfrak{C}}$ ensin tulevat $\mathfrak{A}$:n, sitten $\mathfrak{B}'$:n alkiot alkuperäisessä järjestyksessä)

ja

3) kaikilla $R \in \tau \setminus \{\leq\}$ pätee $R^{\mathfrak{C}} = R^{\mathfrak{A}} \cup R^{\mathfrak{B}}$.

Huomautus. Määritelmässä $\mathfrak{A} \lhd\!\!\cdot \mathfrak{B}$ on määrätty vain isomorfiaa vaille, sillä kopion $\mathfrak{B}'$ muodostamismekanismia ei ole rajattu. Niinpä on luonnollista sopia, että $\mathfrak{B}' = \mathfrak{B}$, jos mallien $\mathfrak{A}$ ja $\mathfrak{B}$ universumit ovat valmiiksi erilliset. Lisäksi jos Σ on merkistö ja τ vastaava sanamallien aakkosto, niin kaikilla $w, w' \in \Sigma^+$ pätee

$$\mathfrak{A}_{ww'} \cong \mathfrak{A}_w \lhd\!\!\cdot \mathfrak{A}_{w'}.$$

On luonnollista sopia, että $\mathfrak{A}_w \lhd\!\!\cdot \mathfrak{A}_{w'} = \mathfrak{A}_{ww'}$.

Äärellinen automaatti

Äärellinen automaatti on yksinkertaisin abstrakteista koneista, jotka lukevat merkkijonoja syötteinä.

1.4. Määritelmä. *Äärellinen automaatti* on viisikko $M = (Q, \Sigma, \delta, a, F)$, missä

1) Q on äärellinen joukko *tiloja*,
2) Σ on äärellinen epätyhjä merkistö,
3) $\delta\colon Q \times \Sigma \to Q$ on *tilasiirtymäfunktio*,
4) $a \in Q$ on *alkutila*,

ja

5) $F \subset Q$ on *lopputilojen eli hyväksyvien tilojen* joukko.

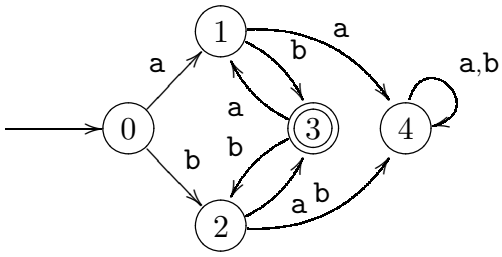
Äärellisen automaatin M laskentaa kuvaa rekursiivisesti määritelty kuvaus $\delta^*\colon \Sigma^* \to Q$:

$$\delta^*(\lambda) = a,\ \delta^*(w\alpha) = \delta(\delta^*(w), \alpha),\ \text{kun } w \in \Sigma^*, \alpha \in \Sigma.$$

Laskennan alkaessa M on siis tilassa a. M lukee syötteestä, olkoon se $w \in \Sigma^*$, kirjaimen kerrallaan alusta loppuun. Jos automaatti on syötteen alkupätkän w_0 luettuaan tilassa $q = \delta^*(w_0)$ ja lukee seuraavaksi merkin α, se siirtyy tilaan $q' = \delta(q, \alpha)$. Syötteen luettuaan M on siten tilassa $\delta^*(w)$. Jos $\delta^*(w) \in F$, niin automaatin sanotaan *hyväksyneen* syötteen w, muuten M *hylkää* w:n. Automaatin M *tunnistama kieli* on

$$L(M) = \{\, w \in \Sigma^* \mid \delta^*(w) \in F \,\}.$$

1.5. Esimerkki. Merkistön $\{\mathtt{a}, \mathtt{b}\}$ kieli L koostukoon parillispituisista sanoista $w = \alpha_0\alpha_1 \ldots \alpha_{2n-1} \in \{a, b\}^*$ ($n \in \mathbb{N}$), joille $w \neq \lambda$ (eli $n \neq 0$) ja $\{\alpha_{2i}, \alpha_{2i+1}\} = \{\mathtt{a}, \mathtt{b}\}$, kun $i \in \{0, \ldots, n-1\}$. Esimerkiksi siis $\mathtt{baabba}, \mathtt{abba} \in L$. Seuraavan kuvan automaatti tunnistaa kielen L:



Kuvassa käytetty symboliikka on varsin arvattava. Ympyrät kuvaavat tiloja, joista alkutilaa 0 osoittaa sisään tuleva nuoli ja hyväksyviä tiloja (tässä vain tila 3) kaksinkertaisella reunalla. Nuolet kuvaavat tilasiirtymäfunktion arvoja, toisin sanoen jos tilasta q on merkillä $\mathtt{a}$ nimetty nuoli tilaan q', niin $q' = \delta(q, \mathtt{a})$. Kuvan automaatti on siis $M = (Q, \Sigma, \delta, a, F)$, missä

$$Q = \{0, 1, 2, 3, 4\}, \qquad \Sigma = \{\mathtt{a}, \mathtt{b}\},$$

$$\delta\colon Q \times \Sigma \to Q,\ \begin{cases} \delta(0, \mathtt{a}) = 1, & \delta(0, \mathtt{b}) = 2, \\ \delta(1, \mathtt{a}) = 4, & \delta(1, \mathtt{b}) = 3, \\ \delta(2, \mathtt{a}) = 3, & \delta(2, \mathtt{b}) = 4, \\ \delta(3, \mathtt{a}) = 1, & \delta(3, \mathtt{b}) = 2, \\ \delta(4, \mathtt{a}) = \delta(4, \mathtt{b}) = 4, \end{cases}$$

$$a = 0 \qquad \text{ja} \qquad F = \{3\}.$$

Automaatti aloittaa siis tilasta 0. Muutoin parillisen monta merkkiä luettuaan automaatti on aina joko tilassa 4 tai tilassa 3. Tila 4 on niin sanottu virhetila, sillä se ei ole hyväksyvä tila eikä automaatti kerran siihen jouduttuaan pysty siitä poistumaan. Huomataan, että M joutuu tähän tilaan, jos jollakin $i \in \{0, \ldots, \lfloor \frac{m-1}{2} \rfloor\}$ sanassa $w = \alpha_0 \ldots \alpha_{m-1}$ on toisto $\alpha_{2i} = \alpha_{2i+1}$. Jos siis δ^* on kuten äärellisen automaatin määritelmässä,

$$\delta^*(\lambda) = 0;$$

$$\delta^*(w) = 3,\ \delta^*(\mathtt{a}) = \delta^*(w\mathtt{a}) = 1,\ \delta^*(\mathtt{b}) = \delta^*(w\mathtt{b}) = 2,\ \text{kun } w \in L,$$

ja

$$\delta^*(w) = 4, \text{ jos } w = w_0\mathtt{aa}w_1 \text{ tai } w = w_0\mathtt{bb}w_1 \text{ jollakin parillispituisella}$$
$$w_0 \in \{\mathtt{a},\mathtt{b}\}^* \text{ ja mielivaltaisella } w_1 \in \{\mathtt{a},\mathtt{b}\}^*.$$

Siis $L(M) = \{\, w \in \{\mathtt{a},\mathtt{b}\}^* \mid \delta^*(w) \in F \,\} = \{\, w \in \{\mathtt{a},\mathtt{b}\}^* \mid \delta^*(w) = 3 \,\} = L$, eli M tunnistaa kielen L.

Seuraava määritelmä parantaa kuvaa siitä, minkälaisia kieliä äärelliset automaatit voivat tunnistaa.

1.6. Määritelmä. Olkoon Σ merkistö. Joukon Σ^* ekvivalenssirelaatio $\sim$ on *invariantti*, jos kaikilla $w, w' \in \Sigma^*$ ja $\alpha \in \Sigma$ pätee: jos $w \sim w'$, niin $w\alpha \sim w'\alpha$.

1.7. Esimerkki.

a) Olkoon Σ merkistö ja $\sim = \{\, (w, w') \in \Sigma^* \times \Sigma^* \mid |w| = |w'| \,\}$, toisin sanoen $w, w' \in \Sigma^*$ ovat $\sim$-ekvivalentteja, jos ne ovat samanpituisia. Tällainen $\sim$ on selvästi invariantti, koska uuden merkin lisääminen säilyttää ekvivalenssin.

b) Epäinvariantteja ekvivalenssirelaatioita on helppo keksiä. Ehkä yksinkertaisin on merkistöä $\{\mathtt{a}\}$ vastaava joukon $\{\mathtt{a}\}^*$ ekvivalenssirelaatio $\sim$: $w \sim w'$, jos ja vain jos $w = w'$ tai $\{w, w'\} = \{\lambda, \mathtt{a}\}$, kun $w, w' \in \{\mathtt{a}\}^*$. Tällöin $\lambda \sim \mathtt{a}$, mutta $\mathtt{a} \not\sim \mathtt{aa}$.

1.8. Lemma. *Olkoon Σ äärellinen epätyhjä merkistö ja $\sim$ joukon Σ^* ekvivalenssirelaatio. Oletetaan, että $\sim$ on invariantti ja $\sim$:llä on vain äärellisen monta ekvivalenssiluokkaa. Olkoon $L \subset \Sigma^*$ yhdiste ekvivalenssin $\sim$ (joistakin) ekvivalenssiluokista. Tällöin on olemassa äärellinen automaatti M, joka hyväksyy kielen L.*

Todistus. Muodostetaan M ekvivalenssin $\sim$ ekvivalenssiluokista. Tarkastellaan siis äärellistä automaattia $M = (Q, \Sigma, \delta, a, F)$, missä

$$\begin{aligned}
Q &= \{\, [w]_\sim \mid w \in \Sigma^* \,\} \text{ eli } \sim\text{:n ekvivalenssiluokkien joukko,}\\
a &= [\lambda]_\sim \text{ eli tyhjän jonon ekvivalenssiluokka,}\\
F &= \{\, [w]_\sim \mid w \in L \,\} \text{ ja}\\
\delta &: Q \times \Sigma \to Q, \quad \delta([w]_\sim, \alpha) = [w\alpha]_\sim.
\end{aligned}$$

Q on äärellinen, sillä ekvivalenssilla $\sim$ oletettiin olevan vain äärellisen monta ekvivalenssiluokkaa. Lisäksi on syytä tarkistaa, että tilasiirtymäfunktio δ on hyvinmääritelty. Olkoot $w, w' \in \Sigma^*$ ja $a \in \Sigma$. Jos $[w]_\sim = [w']_\sim$ eli $w \sim w'$, niin invarianttiuden tähden $wa \sim w'a$ eli $[wa]_\sim = [w'a]_\sim$. Siis δ on hyvinmääritelty.

Triviaalilla induktiolla saadaan, että $\delta^*(w) = [w]_\sim$, kun $w \in \Sigma^*$, missä δ^* on kuten äärellisen automaatin määritelmässä. Automaatin M tunnistama kieli on

$$\begin{aligned}
L(M) &= \{\, w \in \Sigma^* \mid \delta^*(w) \in F \,\} = \{\, w \in \Sigma^* \mid [w]_\sim \in F \,\}\\
&= \{\, w \in \Sigma^* \mid [w]_\sim = [w_0]_\sim \text{ jollakin } w_0 \in L \,\}\\
&= \{\, w \in \Sigma^* \mid w \sim w_0 \text{ jollakin } w_0 \in L \,\}\\
&= L,
\end{aligned}$$

sillä L on yhdiste ekvivalenssin $\sim$ ekvivalenssiluokista. □

Huomautus. Oletus, että ekvivalenssirelaatiolla $\sim$ on vain äärellisen monta ekvivalenssiluokkaa, on erittäin oleellinen. Itse asiassa joukon Σ^* identtisyysrelaatio $\Delta = \{ (w, w') \in \Sigma^* \times \Sigma^* \mid w = w' \}$ on invariantti ekvivalenssirelaatio; ja jokainen kieli $L \subset \Sigma^*$ on yhdiste Δ:n ekvivalenssiluokista! Δ:lla on kuitenkin äärettömän monta ekvivalenssiluokkaa, nimittäin kukin $\{w\}$, $w \in \Sigma^*$.

Jatkossa tullaan yllättäen huomaamaan, että edellisen lemman tuloksen voi kääntää.

2. Monadinen toisen kertaluvun logiikka ja Büchin lause

Olkoon Σ merkistö ja $\tau = \{\leq\} \cup \{ U_\alpha \mid \alpha \in \Sigma \}$ sitä vastaava sanamallien aakkosto. Kun K on sanamallien kanssa isomorfisista τ-malleista koostuva luokka äärellisiä malleja, luokkaa K vastaa kieli

$$L = \{ w \in \Sigma^+ \mid \mathfrak{A}_w \in K \}.$$

Kääntäen jokaista kieltä $L \subset \Sigma^+$ vastaa malliluokka

$$K = \{ \mathfrak{B} \in \mathrm{Str}(\tau) \mid \mathfrak{B} \cong \mathfrak{A}_w \text{ jollakin } w \in L \}.$$

Kun tarkastellaan jotakin kieltä $L \subset \Sigma^+$, on siis luonnollista kysyä, paitsi onko L äärellisellä automaatilla tunnistettavissa, myös onko vastaava luokka K jossakin logiikassa määriteltävissä.

2.1. Määritelmä. Olkoon $L \subset \Sigma^+$ merkistön Σ kieli ja τ merkistöä Σ vastaava sanamallien aakkosto. Kieli L on *määriteltävissä* logiikan $\mathcal{L}$ *lauseella* φ, jonka aakkosto on τ, jos luokalle

$$K = \{ \mathfrak{B} \in \mathrm{Str}(\tau) \mid \mathfrak{B} \cong \mathfrak{A}_w \text{ jollakin } w \in L \}$$

pätee

$$K = \{ \mathfrak{B} \in \mathrm{Str}(\tau) \mid \mathfrak{B} \models \varphi,\ \mathfrak{B} \text{ äärellinen.} \}$$

Tällöin kielen L sanotaan myös olevan *määriteltävissä logiikassa* $\mathcal{L}$.

Edellä olevassa määritelmässä $\mathcal{L}$ voi olla mikä tahansa logiikka, mutta koska kurssilla ei opeteta abstraktia logiikan käsitettä, käytännössä $\mathcal{L}$ on jokin kurssilla esiintyvistä logiikoista, kuten $\mathcal{L} = \mathrm{FO}$ tai $\mathcal{L} = \mathrm{FVL}$. Itse asiassa ensimmäisen kertaluvun logiikka FO osoittautuu tarkoituksiimme riittämättömäksi, joten tässä luvussa tutustutaan toisen kertaluvun logiikan muunnelmiin.

Olkoon Σ äärellinen merkistö ja τ sitä vastaava sanamallien aakkosto. Aiemmin on jo todettu, että on olemassa lause $\psi_\Sigma \in \mathrm{FO}[\tau]$, joka ilmaisee äärellisen mallin olevan aakkoston τ sanamallin kanssa isomorfinen. Jos FO on logiikan $\mathcal{L}$ alilogiikka, niin $\psi_\Sigma \in \mathcal{L}[\tau]$. Tällöin seuraavat ovat yhtäpitäviä kielelle $L \subset \Sigma^+$:

a) Kieli L on logiikassa $\mathcal{L}$ määriteltävissä.
b) On olemassa $\vartheta \in \mathcal{L}[\tau]$, jolle $L = \{\, w \in \Sigma^+ \mid \mathfrak{A}_w \models \vartheta \,\}$.

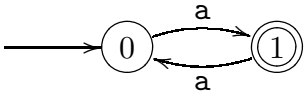
Jos nimittäin L on lauseella φ määriteltävissä, niin kohdassa b voidaan valita $\vartheta = \varphi$, sillä kaikilla $w \in \Sigma^+$ $\quad \mathfrak{A}_w \models \vartheta \iff \mathfrak{A}_w \in K \iff w \in L$. Jos taas kohdan b lause ϑ on olemassa, niin L on määriteltävissä lauseella $\varphi = \vartheta \wedge \psi_\Sigma$: Kaikilla äärellisillä τ-malleilla $\mathfrak{B}$ pätee

$$\begin{aligned}\mathfrak{B} \models \varphi &\iff \mathfrak{B} \models \vartheta \text{ ja } \mathfrak{B} \cong \mathfrak{A}_w \text{ jollakin } w \in \Sigma^+ \\ &\iff \mathfrak{B} \cong \mathfrak{A}_w \models \vartheta \text{ jollakin } w \in \Sigma^+ \\ &\iff \mathfrak{B} \cong \mathfrak{A}_w \text{ jollakin } w \in L \\ &\iff \mathfrak{B} \in K.\end{aligned}$$

2.2. Esimerkki. Tarkastellaan merkistöä $\{\mathtt{a}\}$ vastaavaa sanamallien aakkostoa $\{\leq, A\}$ ja kieltä $L = \{\, w \in \{\mathtt{a}\}^* \mid |w| \text{ pariton} \,\}$. Kieltä L vastaava malliluokka on nyt yksinkertaisesti

$$K = \{\, \mathfrak{B} \in \mathrm{Str}(\{\leq, A\}) \mid \mathrm{card}(\mathfrak{B}) \text{ pariton}, A^{\mathfrak{B}} = \mathrm{Dom}(\mathfrak{B}), \leq^{\mathfrak{B}} \mathrm{Dom}(\mathfrak{B})\text{:n lin.järj.} \,\}.$$

Kielen L tunnistaa alla oleva äärellinen automaatti M.



Kieli L ei ole kuitenkaan määriteltävissä FO:ssa samasta syystä, kuin lineaarijärjestettyjen joukkojen parillisuuskaan ei ole määriteltävissä. Jokaisella $m \in \mathbb{N}$ sanoille $w, w' \in \{\mathtt{a}\}^*$, joille $|w| = 2^m$ ja $|w'| = 2^m + 1$, pätee nimittäin $\mathfrak{A}_w \equiv_m \mathfrak{A}_{w'}$. L on siis esimerkki kielestä, joka voidaan tunnistaa äärellisellä automaatilla, mutta joka ei ole FO:ssa määriteltävissä.

Toisen kertaluvun logiikka

Toisen kertaluvun logiikkaan liittyy uusi kaavanmuodostussääntö, eksistentiaalinen toisen kertaluvun kvantifiointi. Olkoon φ lause, jonka aakkosto on $\tau(\varphi)$. Olkoon R relaatiosymboli. Lauseesta φ relaatiosymboli R *eksistentiaalisesti kvantifioimalla* muodostettua lausetta merkitään $\exists R\,\varphi$. Kvantifiointia kutsutaan toisen kertaluvun kvantifioinniksi, koska R ei ole vakiosymboli, vaan relaatiosymboli. Lauseen $\exists R\,\varphi$ aakkosto on $\tau(\exists R\,\varphi) = \tau(\varphi) \setminus \{R\}$.

Lauseen $\exists R\,\varphi$ luonnollinen tulkinta määritellään seuraavasti: Olkoon $\mathfrak{M}$ aakkoston $\sigma \supset \tau(\varphi) \setminus \{R\}$ malli. Tällöin $\mathfrak{M} \models \exists R\,\varphi$, jos ja vain jos rajoittumalla $\mathfrak{M}{\restriction}(\tau(\varphi) \setminus \{R\})$ on laajennus $\tau(\varphi)$-malliksi $\mathfrak{M}^*$, jolle $\mathfrak{M}^* \models \varphi$. Siinä erityistapauksessa, että $R \notin \sigma$, edellinen määritelmä on yhtäpitävä seuraavan luonnollisen muotoilun kanssa: $\mathfrak{M} \models \exists R\,\varphi$, jos ja vain jos on olemassa sellainen $\#(R)$-paikkainen $\mathrm{Dom}(\mathfrak{M})$:n relaatio S, että $\langle \mathfrak{M}, S \rangle \models \varphi$.

Kuten ensimmäisen kertaluvun universaalikvanttorin tapauksessa, lausetta $\forall R\varphi$ pidetään lyhennysmerkintänä lauseesta $\neg\exists R\neg\varphi$.

2.3. Määritelmä. *Toisen kertaluvun logiikka* SO määritellään seuraavasti: Logiikan SO lauseita ovat ne, jotka saadaan atomilauseista negaatiota, konjunktiota, (ensimmäisen kertaluvun) eksistentiaalista kvantifiointia ja toisen kertaluvun eksistentiaalista kvantifiointia käyttäen. Lauseiden semantiikka määritellään niin, että kaikilla lauseilla on luonnolliset tulkinnat.

2.4. Esimerkki. Äärellisen mallin mahtavuuden parillisuus on ilmaistavissa toisen kertaluvun lauseella

$$\begin{aligned}\varphi = \exists R\,(&\forall x\forall y(R(x,y)\leftrightarrow R(y,x))\\ &\wedge\forall x\exists y\,(R(x,y)\wedge\neg x=y\wedge\forall z(R(x,z)\leftrightarrow y=z))\,,\end{aligned}$$

missä R on kaksipaikkainen. Lause φ on totta äärellisessä mallissa $\mathfrak{M}$, jos on olemassa $\mathrm{Dom}(\mathfrak{M})$:n relaatio S (joka ei siis yleensä ole valmiiksi tulkittuna mallissa $\mathfrak{M}$), joka on 1) symmetrinen, 2) irrefleksiivinen ja 3) jokaisella $a\in\mathrm{Dom}(\mathfrak{M})$ on olemassa yksikäsitteinen $b\in\mathrm{Dom}(\mathfrak{M})$, jolle $(a,b)\in S$. Toisaalta ehto 3 sanoo itse asiassa, että S on joukon $\mathrm{Dom}(\mathfrak{M})$ yksipaikkainen funktio, ja ehto 2 vastaa tällöin kiintopisteettömyyttä ja ehto 1 voidaan kirjoittaa muotoon $S^{-1}=S$. Siis $\mathfrak{M}\models\varphi$, jos ja vain jos on olemassa joukon $\mathrm{Dom}(\mathfrak{M})$ yksipaikkainen funktio S, joka on bijektio, itsensä käänteisfunktio ja kiintopisteetön. Tällainen S niputtaa $\mathrm{Dom}(\mathfrak{M})$:n alkiot pareiksi eli $\{\,\{a,S(a)\}\mid a\in\mathrm{Dom}(\mathfrak{M})\,\}$ on $\mathrm{Dom}(\mathfrak{M})$:n ositus. Tällainen selvästi on olemassa täsmälleen silloin, kun $\mathrm{card}(\mathfrak{M})$ on parillinen.

Parillisuus on tyyppiesimerkki asiasta, joka ei ole ilmaistavissa FO:ssa. Siis SO on aidosti vahvempi kuin FO. Osoittautuu, että äärellisten automaattien tunnistamien kielten määrittelemiseen riittävät SO:n alilogiikat.

Toisen kertaluvun logiikan alilogiikkoja

Lauseesta φ relaatiosymboli X eksistentiaalisesti kvatifioimalla muodostettua lausetta $\exists X\varphi$ sanotaan *monadiseksi eksistentiaaliseksi kvantifioinniksi*, jos X on yksipaikkainen.

2.5. Määritelmä. *Monadisen toisen kertaluvun logiikan* MSO lauseita ovat täsmälleen ne, jotka saadaan atomilausesta negaatiota, konjunktiota, ensimmäisen kertaluvun eksistentiaalista kvantifiointia ja toisen kertaluvun monadista eksistentiaalista kvantifiointia käyttäen. *Logiikan* $\mathrm{Mon}-\Sigma^1_1$ lauseita ovat ne MSO:n lauseet, jotka ovat muotoa

$$\exists X_0\ldots\exists X_{\ell-1}\,\varphi,$$

missä $\ell\in\mathbb{N}$, $X_0,\ldots,X_{\ell-1}$ ovat yksipaikkaisia relaatiosymboleita ja φ on ensimmäisen kertaluvun logiikan FO lause.

2.6. Lemma. *Jokainen äärellisen automaatin tunnistama kieli $L \subset \Sigma^+$ on logiikassa* $\mathrm{Mon}-\Sigma^1_1$ *määriteltävissä.*

Todistus. Olkoon $M = (Q, \Sigma, \delta, a, F)$ äärellinen automaatti, joka tunnistaa kielen L, ja $\tau = \{\leq\} \cup \{\, U_\alpha \mid \alpha \in \Sigma \,\}$ merkistöä Σ vastaava sanamallien aakkosto. Otetaan jokaista tilaa $q \in Q$ kohti käyttöön uusi yksipaikkainen relaatiosymboli X_q. Merkitään $\varrho = \tau \cup \{\, X_q \mid q \in Q \,\}$.

Tarkastellaan mielivaltaista sanaa $w = \beta_0 \dots \beta_{\ell-1} \in \Sigma^+$ ($\beta_i \in \Sigma$, $i = 0, \dots, \ell-1$) ja vastaavan sanamallin $\mathfrak{A}_w$ laajennusta ϱ-malliksi $\mathfrak{A}^*$, jossa uusien relaatiosymbolien tulkinnat ovat

$$X_q^{\mathfrak{A}^*} = \{\, i \in \{0, \dots, \ell-1\} \mid \delta^*(\beta_0 \dots \beta_{i-1}) = q \,\},$$

kun $q \in Q$ (δ^* kuten äärellisen mallin määritelmässä). Siis $i \in X_q^{\mathfrak{A}^*}$, jos ja vain jos sanaa w lukeva äärellinen automaatti on luettuaan i merkkiä tilassa q. Mallissa $\mathfrak{A}^*$ on selvästi totta lause φ, joka ilmaisee perheen $\{\, X_q^{\mathfrak{A}^*} \mid q \in Q \,\} \setminus \{\emptyset\}$ olevan $\mathrm{Dom}(\mathfrak{A}^*)$:n ositus, siis lause

$$\varphi = \forall x \bigvee_{q \in Q} X_q(x) \wedge \bigwedge_{\substack{q, q' \in Q \\ q \neq q'}} \neg \exists x \left(X_q(x) \wedge X_{q'}(x) \right).$$

Koska tilajoukko Q on äärellinen, yllä olevat disjunktiot ja konjunktiot ovat äärellisiä, joten $\varphi \in \mathrm{FO}[\varrho]$.

Olkoot $\alpha(x)$ ja $\omega(x)$ FO:n kaavoja, jotka ilmaisevat x:n olevan pienin alkio ja vastaavasti suurin alkio, toisin sanoen

$$\alpha(x) = \forall y \, (x \leq y) \quad \text{ja} \quad \omega(x) = \forall y \, (y \leq x).$$

Kaava $\sigma(x, y) = x \leq y \wedge \neg x = y \wedge \forall z (z \leq y \to z = y \vee z \leq x)$ ilmaisee muuttujan y olevan muuttujan x välitön seuraaja. Mallissa $\mathfrak{A}^*$ on myös totta seuraava lause $\vartheta \in \mathrm{FO}[\varrho]$, joka kertoo, miten kuhunkin tilaan on päädytty:

$$\begin{aligned} \vartheta = {} & \forall x \, (\alpha(x) \to X_a(x)) \\ & \wedge \bigwedge_{\substack{q, q' \in Q, \, \beta \in \Sigma \\ \delta(q, \beta) = q'}} \forall t \forall x \, (\sigma(t, x) \wedge X_q(t) \wedge U_\beta(t) \to X_{q'}(x)) \end{aligned}$$

Ylempi rivi ilmaisee äärellisen automaatin olevan alussa tilassa a. Alemman rivin konjunktiossa käydään läpi kaikki tapaukset, miten tilasta q voidaan siirtyä tilaan q' lukemalla merkki β.

Olkoon nyt $\mathfrak{B}$ mallin $\mathfrak{A}$ sellainen laajennus ϱ-malliksi, että $\mathfrak{B} \models \varphi \wedge \vartheta$. Merkitään jokaisella $i \in \{0, \dots, \ell-1\}$ $\quad q_i = \delta^*(\beta_0 \dots \beta_i)$, ja osoitetaan induktiolla, että $i \in X_{q_i}^{\mathfrak{B}}$.

1) $q_0 = a$ ja $\mathfrak{B} \models \forall x (\alpha(x) \to X_\alpha(x))$. Koska $\mathfrak{B} \models \alpha[0/x]$, pätee siis $\mathfrak{B} \models X_a(x)[0/x]$ eli $0 \in X_a^{\mathfrak{B}} = X_{q_0}^{\mathfrak{B}}$.
2) Oletetaan, että $i \in X_{q_i}^{\mathfrak{B}}$. Koska $\delta(q_i, \beta_i) = q_{i+1}$ ja $\mathfrak{B} \models \vartheta$, niin $\mathfrak{B} \models \forall t \forall x (\sigma(t, x) \wedge X_{q_i}(t) \wedge U_{\beta_i}(t) \to X_{q_{i+1}}(x)$ eli erityisesti $\mathfrak{B} \models \sigma(t, x) \wedge X_{q_i}(t) \wedge U_{\beta_i}(t) \to X_{q_{i+1}}(x)[i/t, i+1/x]$. Luku $i+1$ on luvun i seuraaja, joten $\mathfrak{B} \models \sigma[i/t, i+1/x]$. Oletuksesta $i \in X_{q_i}^{\mathfrak{B}}$

seuraa $\mathfrak{B} \models X_{q_i}(t)[i/t]$. Koska $\mathfrak{B}$ on sanamallin $\mathfrak{A}_w$ laajennus, $\mathfrak{B} \models U_{\beta_i}(t)[i/t]$. Siis $\mathfrak{B} \models X_{q_{i+1}}(x)[i+1/x]$ eli $i+1 \in X^{\mathfrak{B}}_{q_{i+1}}$.

Induktiotodistus osoitti, että $X^{\mathfrak{A}^*}_q \subset X^{\mathfrak{B}}_q$ jokaisella $q \in Q$. Toisaalta $\mathfrak{B} \models \varphi$, joten $\{ X^{\mathfrak{B}}_q \mid q \in Q \} \setminus \{\emptyset\}$ on joukon $\mathrm{Dom}(\mathfrak{B}) = \{0, \ldots, \ell - 1\}$ ositus, joten sisältyvyydet eivät voi olla aitoja. Siis $\mathfrak{B} = \mathfrak{A}^*$ eli $\mathfrak{A}^*$ on ainoa sanamallin $\mathfrak{A}_w$ laajennus ϱ-malliksi $\mathfrak{A}^* \models \varphi \wedge \vartheta$.

Äärellinen automaatti M hyväksyy sanan w, jos ja vain jos $\mathfrak{A}^* \models \chi$, missä

$$\chi = \bigvee_{\substack{q \in Q,\, \beta \in \Sigma \\ \delta(q,\beta) \in F}} \exists x(\omega(x) \wedge U_\beta(x) \wedge X_q(x)) \in \mathrm{FO}[\varrho]$$

Lause χ kertoo automaatin siirtyvän viimeistä merkkiä β lukiessaan tilasta q hyväksyvään tilaan q'.

Lopuksi väitetään, että lause

$$\xi = \exists X_{q_0} \ldots \exists X_{q_{s-1}} (\psi_\Sigma \wedge \varphi \wedge \vartheta \wedge \chi)$$

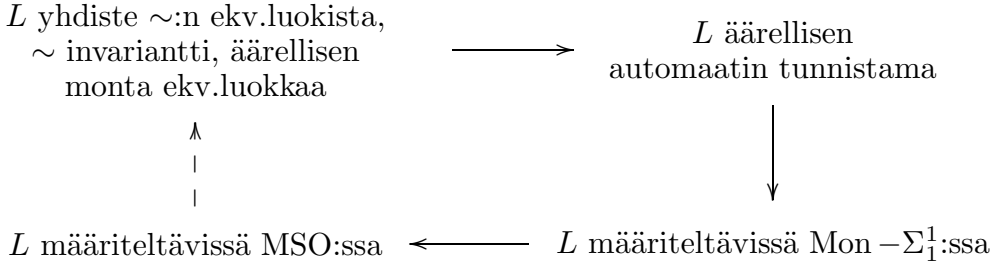
on kielen L määrittelevä lause. Tässä $s = |Q|$, $\{q_0, \ldots, q_{s-1}\} = Q$ ja $\psi_\Sigma \in \mathrm{FO}[\tau]$ ilmaisee äärellisen mallin olevan sanamallin kanssa isomorfinen. Siis $\psi_\Sigma \wedge \varphi \wedge \vartheta \wedge \chi \in \mathrm{FO}[\varrho]$ ja $\xi \in \mathrm{Mon} - \Sigma^1_1[\tau]$ (lauseen ξ aakkosto on $\varrho \setminus \{X_{q_0}, \ldots X_{q_{s-1}}\} = \tau$). Merkitään

$$K = \{ \mathfrak{M} \in \mathrm{Str}(\tau) \mid \mathfrak{M} \models \xi,\ \mathfrak{M} \text{ äärellinen } \}$$

Olkoon äärellinen $\mathfrak{A} \in \mathrm{Str}(\tau)$ mielivaltainen. Jos $\mathfrak{A} \ncong \mathfrak{A}_w$ kaikilla $w \in \Sigma^+$, niin $\mathfrak{A} \not\models \psi_\Sigma$, mistä seuraa $\mathfrak{A} \not\models \xi$ eli $\mathfrak{A} \notin K$. Oletetaan nyt, että $\mathfrak{A} \cong \mathfrak{A}_w$ jollakin $w \in \Sigma^+$. Tällöin $\mathfrak{A} \models \xi$, jos ja vain jos mallilla $\mathfrak{A}$ on laajennus ϱ-malliksi $\mathfrak{A}' \models \psi_\Sigma \wedge \varphi \wedge \vartheta \wedge \chi$. Mutta koska $\mathfrak{A} \cong \mathfrak{A}_w$, tämän kanssa yhtäpitävää on, että mallilla $\mathfrak{A}_w$ on tällainen laajennus. Edellä todettiin jo, että mallilla $\mathfrak{A}_w$ on täsmälleen yksi ϱ-laajennus $\mathfrak{A}^*$, jolle $\mathfrak{A}^* \models \varphi \wedge \vartheta$, joten $\mathfrak{A} \models \xi$, jos ja vain jos $\mathfrak{A}^* \models \chi$, jos ja vain jos M hyväksyy sanan w, jos ja vain jos $w \in L$. Siis

$$K = \{ \mathfrak{M} \in \mathrm{Str}(\tau) \mid \mathfrak{M} \cong \mathfrak{A}_w \text{ jollakin } w \in L \}. \quad \square$$

Büchin lause



Koska Mon $-\Sigma^1_1$ on logiikan MSO alilogiikka, jokainen Mon $-\Sigma^1_1$:ssä määriteltävä kieli on myös MSO:ssa määriteltävä. Käsitteisiin tutustumisen yhteydessä on siis todistettu yllä olevan kaavion tulokset. Kierroksen sulkemiseen tarvitaan vielä katkoviivalla merkitty tulos, että jokainen MSO:ssa määriteltävä kieli L on yhdiste invariantin ekvivalenssirelaation $\sim$ ekvivalenssiluokista, missä $\sim$:llä on äärellisen monta ekvivalenssiluokkaa. Sanojen ekvivalenssia vastaa logiikan tasolla sanamallien ekvivalenssi, joten olisi luonnollista ryhtyä analysoimaan logiikkaan MSO liittyviä mallien ekvivalensseja. Ongelmana on vain, ettei MSO:n analysoimiseen ole vielä tarjolla mitään menetelmiä.

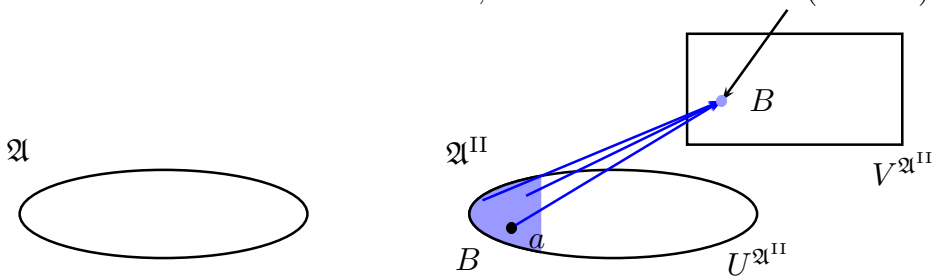
Paljastuu, että Ehrenfeuchtin ja Fraïssén pelistä on jälleen apua. Osoittautuu nimittäin, että ensimmäisen kertaluvun logiikassa FO voi jäljitellä logiikan MSO ilmaisuvoimaa sillä tavoin, että itse malliin lisätään uusia rakenteita.

Olkoon τ relationaalinen aakkosto ja $\mathfrak{A}$ aakkoston τ malli. Otetaan käyttöön uudet relaatiosymbolit U, V ja E, missä $\#(U) = \#(V) = 1$ ja $\#(E) = 2$. Määritellään aakkoston $\tau \cup \{U, V, E\}$ malli $\mathfrak{A}^{\mathrm{II}}$. Merkitään $A = \mathrm{Dom}(\mathfrak{A})$ ja oletetaan yksinkertaisuuden vuoksi, että $A \cap \mathcal{P}(A) = \emptyset$. (Jos näin ei ole, muodostetaan isomorfinen kopio $\mathfrak{A}' \cong \mathfrak{A}$, jolle $\mathrm{Dom}(\mathfrak{A}') \cup \mathcal{P}(\mathrm{Dom}(\mathfrak{A})) = \emptyset$, konstruoidaan $(\mathfrak{A}')^{\mathrm{II}}$ kuten jatkossa ja asetetaan lopuksi $\mathfrak{A}^{\mathrm{II}} = (\mathfrak{A}')^{\mathrm{II}}$.) Tällöin

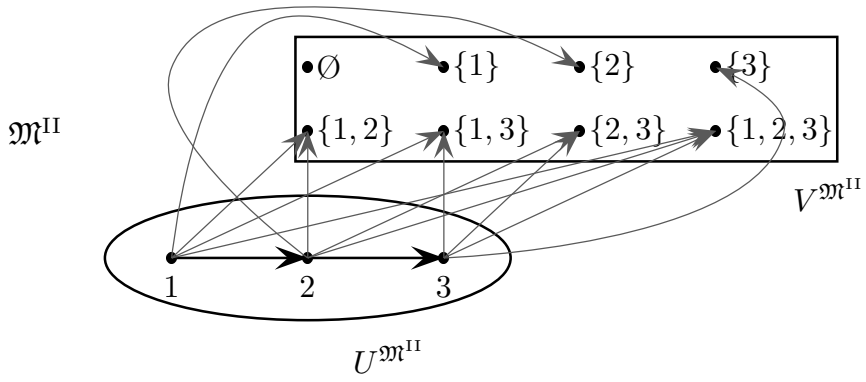
$$\begin{aligned} \mathrm{Dom}(\mathfrak{A}^{\mathrm{II}}) &= A \cup \mathcal{P}(A), \\ U^{\mathfrak{A}^{\mathrm{II}}} &= A, \qquad V^{\mathfrak{A}^{\mathrm{II}}} = \mathcal{P}(A), \\ E^{\mathfrak{A}^{\mathrm{II}}} &= \{\, (a, B) \in A \times \mathcal{P}(A) \mid a \in B \,\}, \end{aligned}$$

ja

$$R^{\mathfrak{A}^{\mathrm{II}}} = R^{\mathfrak{A}}, \text{ kun } R \in \tau.$$



2.7. Esimerkki. Olkoon $\mathfrak{M}$ $\{S\}$-malli, missä $\mathrm{Dom}(\mathfrak{M}) = \{1, 2, 3\}$ ja $S^{\mathfrak{M}} = \{(1, 2), (2, 3)\}$. $\mathfrak{M}^{\mathrm{II}}$ on ikään kuin $\mathfrak{M}$ potenssijoukolla vahvistettuna:



$\mathrm{card}(\mathfrak{M}) = 3$, mutta $\mathrm{card}(\mathfrak{M}^{\mathrm{II}}) = 3 + 2^3 = 11$.

2.8. Lemma. *Olkoon τ kiinteä relationaalinen aakkosto. Tällöin jokaista $\varphi \in \mathrm{MSO}[\tau]$ vastaa sellainen $\varphi^* \in \mathrm{FO}[\tau \cup \{U, V, E\}]$, missä relaatiosymbolit U, V ja E ovat kuten $\mathfrak{A}^{\mathrm{II}}$:n määritelmässä, että kaikilla $\mathfrak{M} \in \mathrm{Str}(\tau)$ pätee $\mathfrak{M} \models \varphi$, jos ja vain jos $\mathfrak{M}^{\mathrm{II}} \models \varphi^*$.*

Todistus. Määritellään *-käännös laajemmassa luokassa, nimittäin kaikille MSO:n lauseille φ, joiden aakkostolle σ pätee, että $\sigma \setminus \tau = \{x_0, \ldots, x_{k-1}, Y_0, \ldots, Y_{\ell-1}\}$ koostuu äärellisen monesta uudesta vakiosymbolista (eli muuttujasta) $x_0, \ldots, x_{k-1}$ ja äärellisen monesta uudesta yksipaikkaisesta relaatiosta (eli toisen kertaluvun muuttujasta) $Y_0, \ldots, Y_{\ell-1}$. Relaatiosymbolien $Y_0, \ldots, Y_{\ell-1}$ uutuus sisältää myös teknisen ehdon $Y_i \neq U, V$, kun $i = 0, \ldots, \ell - 1$. Käännöksessä φ^* relaatiosymbolin Y_i tilalla esiintyy vakiosymboli y_i, kun $i = 0, \ldots, \ell - 1$. *-käännöksen induktiivinen määritelmä on seuraava:

1) $\varphi = \varphi^*$, jos φ on atomilause, jossa ei esiinny uusia relaatiosymboleita.
2) $Y(x)^* = E(x, y)$, kun Y on uusi relaatiosymboli, x muuttuja ja y Y:tä vastaava muuttuja.
3) $(\neg\vartheta)^* = \neg\vartheta^*$,
4) $(\vartheta \wedge \psi)^* = \vartheta^* \wedge \psi^*$,
5) $(\exists x\, \vartheta)^* = \exists x\, (U(x) \wedge \vartheta^*)$, kun x on muuttuja, ja
6) $(\exists Y\, \vartheta)^* = \exists y\, (V(y) \wedge \vartheta^*)$, kun Y on uusi relaatiosymboli ja y sitä vastaava muuttuja.

Lauseiden φ käännökset φ^* ovat selvästi FO:ssa, ja jos $\varphi \in \mathrm{MSO}[\tau]$, niin $\varphi^* \in \mathrm{FO}[\tau]$. Käännöksen idea on selvä: MSO:ssa on kahdenlaisia kvantifiointeja, ensimmäisen ja toisen kertaluvun. FO:ssa on vain yhdenlaisia kvantifiointeja, mutta mallissa $\mathfrak{M}^{\mathrm{II}}$ on kahdenlaisia alkioita. Käännökseen on siis liitettävä tieto, millaisia alkioita kvantifioidaan.

Osoitetaan nyt induktiolla, että jos φ on kuten yllä, niin kaikilla $\mathfrak{M} \in \mathrm{Str}(\tau)$, $a_0, \ldots, a_{k-1} \in \mathrm{Dom}(\mathfrak{M})$ ja $B_0, \ldots, B_{\ell-1} \subset \mathrm{Dom}(\mathfrak{M})$ pätee

$$\mathfrak{N} = \langle \mathfrak{M}, a_0, \ldots, a_{k-1}, B_0, \ldots, B_{\ell-1} \rangle \models \varphi,$$

jos ja vain jos

$$\mathfrak{N}^* = \langle \mathfrak{M}^{\mathrm{II}}, a_0, \ldots, a_{k-1}, B_0, \ldots, B_{\ell-1} \rangle \models \varphi^*.$$

Tässä siis $\mathfrak{N}$ on $\tau \cup \{x_0, \ldots, x_{k-1}, Y_0, \ldots, Y_{\ell-1}\}$-malli, jossa $x_i^{\mathfrak{N}} = a_i$ $(i = 0, \ldots, k-1)$ ja $Y_j^{\mathfrak{N}} = B_j$ $(j = 0, \ldots, \ell - 1)$, kun taas $\mathfrak{N}^*$ on $\tau \cup \{U, V, E\} \cup \{x_0, \ldots, x_{k-1}, y_0, \ldots, y_{\ell-1}\}$-malli, jossa $x_i^{\mathfrak{N}^*} = a_i$ $(i = 0, \ldots, k-1)$ ja $y_j^{\mathfrak{N}^*} = B_j$ $(j = 0, \ldots, \ell - 1)$ on vakiosymbolin tulkinta!

1) Jos φ on atomilause, jossa ei esiinny uusia relaatiosymboleita, niin $\varphi = \varphi^*$ ja $\mathfrak{N}^*$:n ja $\mathfrak{N}$:n tulkinnat yhtyvät lauseessa esiintyvien symboleiden kohdalla, joten väite on totta.
2) Olkoon $\varphi = Y(x)$, missä Y on uusi relaatiosymboli. Olkoon $\mathfrak{M} \in \mathrm{Str}(\tau)$, $\mathfrak{N} = \langle \mathfrak{M}, a, B \rangle$ ja $\mathfrak{N}^* = \langle \mathfrak{M}^{\mathrm{II}}, a, B \rangle$, missä $a \in \mathrm{Dom}(\mathfrak{M})$ ja $B \subset \mathrm{Dom}(\mathfrak{M})$. Tällöin

$$\begin{aligned} \mathfrak{N} \models \varphi &\iff \mathfrak{N} \models Y(x) \iff x^{\mathfrak{N}} \in Y^{\mathfrak{N}} \iff a \in B \\ &\iff (a, B) \in E^{\mathfrak{M}^{\mathrm{II}}} \iff (x^{\mathfrak{N}^*}, y^{\mathfrak{N}^*}) \in E^{\mathfrak{N}^*} \iff \mathfrak{N}^* \models E(x, y) \\ &\iff \mathfrak{N}^* \models \varphi^*. \end{aligned}$$

3) ja 4) ovat ilmeisiä.

5) Olkoon φ muotoa $\exists x\vartheta$, missä x on muuttuja, ja φ:n akkosto on σ, missä $\sigma \setminus \tau = \{x_0, \ldots, x_{k-1}, Y_0, \ldots, Y_{\ell-1}\}$, x_i:t muuttujia, Y_j:t yksipaikkaisia relaatiosymboleita. Olkoot vielä $\mathfrak{M} \in \mathrm{Str}(\tau)$, $a_0, \ldots, a_{k-1} \in \mathrm{Dom}(\mathfrak{M})$ ja $B_0, \ldots, B_{\ell-1} \subset \mathrm{Dom}(\mathfrak{M})$ sekä $\mathfrak{N} = \langle \mathfrak{M}, a_0, \ldots, a_{k-1}, B_0, \ldots, B_{\ell-1}\rangle$ ja $\mathfrak{N}^* = \langle \mathfrak{M}^{\mathrm{II}}, a_0, \ldots, a_{k-1}, B_0, \ldots, B_{\ell-1}\rangle$. Induktio-oletuksen mukaan kaikilla $a \in \mathrm{Dom}(\mathfrak{M})$ pätee $\langle \mathfrak{N}, a\rangle \models \vartheta \iff \langle \mathfrak{N}^*, a\rangle \models \vartheta^*$. Jos siis $\mathfrak{N} \models \varphi$ eli $\mathfrak{N} \models \exists x\vartheta$, niin jollakin $a \in \mathrm{Dom}(\mathfrak{M})$ pätee $\langle \mathfrak{N}, a\rangle \models \vartheta$ ja $\langle \mathfrak{N}^*, a\rangle \models \vartheta^*$. Koska $a \in \mathrm{Dom}(\mathfrak{M}) = U^{\mathfrak{M}^{\mathrm{II}}} = U^{\mathfrak{N}^*}$, tästä seuraa $\langle \mathfrak{N}^*, a\rangle \models U(x) \wedge \vartheta^*$ ja edelleen $\mathfrak{N}^* \models \exists x(U(x) \wedge \vartheta^*)$, eli $\mathfrak{N}^* \models \varphi^*$. Jos kääntäen $\mathfrak{N}^* \models \varphi^*$ eli $\mathfrak{N}^* \models \exists x(U(x) \wedge \vartheta^*)$, niin jollakin $a \in U^{\mathfrak{N}^*} = \mathrm{Dom}(\mathfrak{M})$ pätee $\langle \mathfrak{N}^*, a\rangle \models \vartheta^*$, mistä seuraa $\langle \mathfrak{N}, a\rangle \models \vartheta$ ja $\mathfrak{N} \models \varphi$.

6) Olkoon φ muotoa $\exists Y\vartheta$, missä Y on uusi relaatiosymboli. Olkoon φ:n aakkosto ja sihen liittyvät symbolit, mallit, vakiot ja joukot kuten edellisessä kohdassa. Olkoon vielä y Y:tä vastaava muuttuja. Induktio-oletuksen mukaan jokaisella $B \subset \mathrm{Dom}(\mathfrak{M})$ pätee $\langle \mathfrak{N}, B\rangle \models \vartheta \iff \langle \mathfrak{N}^*, B\rangle \models \vartheta^*$. Siis seuraavat ovat yhtäpitäviä:

$$\begin{aligned}
&\mathfrak{N} \models \varphi,\\
&\text{jollakin } B \subset \mathrm{Dom}(\mathfrak{M}) \quad \langle \mathfrak{N}, B\rangle \models \vartheta,\\
&\text{jollakin } B \subset \mathrm{Dom}(\mathfrak{M}) = V^{\mathfrak{N}^*} \quad \langle \mathfrak{N}^*, B\rangle \models \vartheta^*,\\
&\mathfrak{N}^* \models \exists y\,(V(y) \wedge \vartheta^*)
\end{aligned}$$

ja

$$\mathfrak{N}^* \models \varphi^*. \quad \square$$

2.9. Seuraus. Olkoon Σ äärellinen epätyhjä merkistö, τ sitä vastaava sanamallien aakkosto ja $L \subset \Sigma^+$ MSO:ssa määriteltävä kieli. Kun $m \in \mathbb{N}$, merkitään

$$\sim_m = \{\, (w, w') \in \Sigma^* \times \Sigma^* \mid \mathfrak{A}^{\mathrm{II}}_w \equiv_m \mathfrak{A}^{\mathrm{II}}_{w'} \text{ tai } w = w' = \lambda \,\}.$$

Tällöin $\sim_m$ on joukon Σ^* ekvivalenssirelaatio, jolla on äärellisen monta ekvivalenssiluokkaa, ja jollakin $m \in \mathbb{N}$ kieli L on $\sim_m$:n joidenkin ekvivalenssiluokkien yhdiste.

Todistus. Olkoon $m \in \mathbb{N}$. Koska $\equiv_m$ on ekvivalenssirelaatio aakkoston $\tau \cup \{U, V, E\}$ mallien luokassa, myös $\sim_m$ on ekvivalenssirelaatio. Näillä ekvivalenssirelaatioilla on äärellisen monta ekvivalenssiluokkaa, koska aakkosto τ on äärellinen.

Kiinnitetään lause $\varphi \in \mathrm{MSO}[\tau]$, joka määrittelee kielen L, ja olkoon lause $\varphi^* \in \mathrm{MSO}[\tau\{U, V, E\}]$ kuten lemmassa. Merkitään $m = \mathrm{qr}(\varphi^*)$ ja osoitetaan, että L on ekvivalenssirelaation $\sim_m$ ekvivalenssiluokkien yhdiste. Olkoon $w \in L$; täytyy osoittaa, että $[w]_{\sim_m} \subset L$. Olkoot $w, w' \in \Sigma^+$ ja $w \sim_m w'$, missä siis $w \in L$. Koska φ määrittelee kielen L, niin $\mathfrak{A}_w \models \varphi$, joten $\mathfrak{A}^{\mathrm{II}}_w \models \varphi^*$. Ekvivalenssista $w \sim_m w'$ seuraa nyt $\mathfrak{A}^{\mathrm{II}}_w \equiv_m \mathfrak{A}^{\mathrm{II}}_{w'}$, joten myös $\mathfrak{A}^{\mathrm{II}}_{w'} \models \varphi^*$. Siis $w' \in L$, joten $[w]_{\sim_m} \subset L$. $\square$

Tarkastetaan vielä, että seurauksessa esiintyvä ekvivalenssirelaatio on invariantti.

2.10. Lemma. *Olkoon Σ äärellinen epätyhjä merkistö ja $m \in \mathbb{N}$. Tällöin jos $\mathfrak{A}^{\mathrm{II}}_w \equiv_m \mathfrak{A}^{\mathrm{II}}_{w'}$, niin $\mathfrak{A}^{\mathrm{II}}_{w\alpha} \equiv_m \mathfrak{A}^{\mathrm{II}}_{w'\alpha}$, kun $w, w' \in \Sigma^+$ ja $\alpha \in \Sigma$.*

Todistus. Merkitään $n = |w|$ ja $n' = |w'|$, $\mathcal{A} = V^{\mathfrak{A}^{\mathrm{II}}_w} = \mathcal{P}(\{0,\ldots,n-1\})$ ja $\mathcal{A}' = V^{\mathfrak{A}^{\mathrm{II}}_{w'}} = \mathcal{P}(\{0,\ldots,n'-1\})$. Asetetaan jokaista osittaista isomorfismia $p \in \mathrm{Part}(\mathfrak{A}^{\mathrm{II}}_w, \mathfrak{A}^{\mathrm{II}}_{w'})$ vastaamaan kuvaus p^*, jolle

1) $p \subset p^*$,
2) $\mathrm{dom}(p^*) = \mathrm{dom}(p) \cup \{n\} \cup \mathcal{B}'$

ja

3) $p^*(n) = n'$ ja kaikilla $B \in \mathcal{B}$ on voimassa $p^*(B \cup \{n\}) = p(B) \cup \{n'\}$,

missä $\mathcal{B} = \mathrm{dom}(p) \cap \mathcal{A}$ ja $\mathcal{B}' = \{\, B \cup \{n\} \mid B \in \mathcal{B} \,\}$.

Osoitetaan, että $p^* \in \mathrm{Part}(\mathfrak{A}^{\mathrm{II}}_{w\alpha}, \mathfrak{A}^{\mathrm{II}}_{w'\alpha})$. Ensiksi huomataan, että $p^*[\mathrm{dom}(p)] = \mathrm{rg}(p)$, $p^*[\{n\}] = \{n'\}$ ja $p^*[\mathcal{B}']$ ovat kaikki erillisiä joukkoja ja että $p^* \restriction \mathrm{dom}(p)$ ja $p^* \restriction \mathcal{B}'$ ovat injektioita, joten p^* on injektio. On myös vaivatonta tarkistaa, että homomorfiaehto on voimassa kaikille yksipaikkaisille relaatioille $X \in \tau \cup \{U, V, E\}$; oikeastaan riittää todeta, että $n \in U^{\mathfrak{A}^{\mathrm{II}}_{w\alpha}}_\alpha$ ja $p^*(n) = n' \in U^{\mathfrak{A}^{\mathrm{II}}_{w'\alpha}}_\alpha$ sekä $n \notin U^{\mathfrak{A}^{\mathrm{II}}_{w\alpha}}_\gamma$ ja $n' \notin U^{\mathfrak{A}^{\mathrm{II}}_{w'\alpha}}_\gamma$, kun $\gamma \in \Sigma \setminus \{\alpha\}$. Koska n on joukon $\{0,\ldots,n\}$ $\leq^{\mathfrak{A}^{\mathrm{II}}_{w\alpha}}$-suurin ja $n' = p(n)$ joukon $\{0,\ldots,n'\}$ $\leq^{\mathfrak{A}^{\mathrm{II}}_{w'\alpha}}$-suurin alkio, homomorfiaehto on voimassa myös $\leq$:lle. Lopuksi todetaan, että kaikilla $k \in \mathrm{dom}(p) \cap \{0,\ldots,n-1\}$ ja $B \in \mathcal{B}$ on voimassa

$$\begin{aligned}
(k, B \cup \{n\}) \in E^{\mathfrak{A}^{\mathrm{II}}_{w\alpha}} &\iff k \in B \cup \{n\} \iff k \in B \\
&\iff (k,b) \in E^{\mathfrak{A}^{\mathrm{II}}_{w\alpha}} \iff (p(k), p(b)) \in E^{\mathfrak{A}^{\mathrm{II}}_{w'\alpha}} \\
&\iff p(k) \in p(B) \iff p^*(k) = p(k) \in p(B) \cup \{n'\} = p^*(B \cup \{n\}) \\
&\iff (p^*(k), p^*(B \cup \{n\})) \in E^{\mathfrak{A}^{\mathrm{II}}_{w'\alpha}}
\end{aligned}$$

ja että kaikki muut tapaukset E:n kohdalla ovat ilmeisiä. Siis $p^* \in \mathrm{Part}(\mathfrak{A}^{\mathrm{II}}_{w\alpha}, \mathfrak{A}^{\mathrm{II}}_{w'\alpha})$.

Oletetaan, että $\mathfrak{A}^{\mathrm{II}}_w \equiv_m \mathfrak{A}^{\mathrm{II}}_{w'}$. Tällöin $\mathfrak{A}^{\mathrm{II}}_w \cong_m \mathfrak{A}^{\mathrm{II}}_{w'}$, joten jollakin osittaisten isomorfismien systeemillä

$$(I_0, \ldots, I_m)\colon\ \mathfrak{A}^{\mathrm{II}}_w \cong_m \mathfrak{A}^{\mathrm{II}}_{w'}.$$

Merkitään jokaisella $j = 0,\ldots,m$ $\quad I^*_j = \{\, p^* \mid p \in I_j \,\}$. Koska $I_m \neq \emptyset$, myös $I^*_m \neq \emptyset$. Jää jäljelle osoittaa, että jokaisella $j = 0,\ldots,m-1$ jokainen $r \in I^*_{j+1}$ laajenee edestakaisesti joukkoon I^*_j. Olkoon $r \in I^*_{j+1}$ mielivaltainen; tällöin $r = p^*$ jollakin $p \in I_{j+1}$. Symmetrian vuoksi riittää tarkastella vain laajentamista eteenpäin. Olkoon $a \in \mathrm{Dom}(\mathfrak{A}^{\mathrm{II}}_{w\alpha})$. Tarkastellaan eri tapauksia:

1) $a \in \mathrm{Dom}(\mathfrak{A}^{\mathrm{II}}_w)$. Koska $p \in I_{j+1}$, niin p laajenee edestakaisesti joukkoon I_j ja on siis olemassa $q \in I_j$, jolle $p \subset q$ ja $a \in \mathrm{dom}(q)$. Tällöin $q^* \in I^*_j$, $a \in \mathrm{dom}(q^*)$ ja $p^* \subset q^*$.
2) $a = n$. Valitaan $q \in I_j$, jolle $p \subset q$. Tällöin $q^* \in I^*_j$, $p^* \subset q^*$ ja $n \in \mathrm{dom}(q^*)$ triviaalisti.
3) $a = B \cup \{n\}$ jollakin $B \subset \{0,\ldots,n-1\}$. Valitaan $q \in I_j$ niin, että $p \subset q$ ja $B \in \mathrm{dom}(q)$. Tällöin $B \cup \{n\} \in \mathrm{dom}(q^*)$, $q^* \in I^*_j$ ja $p^* \subset q^*$.

Siis $(I^*_0, \ldots, I^*_m)\colon\ \mathfrak{A}^{\mathrm{II}}_{w\alpha} \equiv_m \mathfrak{A}^{\mathrm{II}}_{w'\alpha}$, mistä seuraa $\mathfrak{A}^{\mathrm{II}}_{w\alpha} \cong_m \mathfrak{A}^{\mathrm{II}}_{w'\alpha}$. $\square$

On aika sitoa langat yhteen:

2.11. Lause. (Büchin lause) *Olkoon Σ äärellinen epätyhjä merkistö ja $L \subset \Sigma^+$. Tällöin seuraavat ovat yhtäpitäviä:*

a) On olemassa sellainen invariantti joukon Σ^* ekvivalenssirelaatio $\sim$, jolla on äärellisen monta ekvivalenssiluokkaa, että L on yhdiste joistakin $\sim$:n ekvivalenssiluokista.

b) L on äärellisen automaatin tunnistama.

c) L on Mon $-\Sigma_1^1$*:ssä määriteltävä.*

d) L on MSO*:ssa määriteltävä.*

Todistus. Seuraukset a) $\Rightarrow$ b) ja b) $\Rightarrow$ c) on todistettu erillisissä lemmoissa. Kohdasta c seuraa d, koska Mon $-\Sigma_1^1$ on logiikan MSO alilogiikka. Oletetaan siis, että kohta d on voimassa, ja todistetaan kohta a.

Olkoon τ merkistöä Σ vastaava sanamallien aakkosto ja oletetaan siis, että L on MSO:ssa määriteltävä. Edellisen seurauksen perusteella tiedetään jo, että jollakin $m \in \mathbb{N}$ L on yhdiste joistakin $\sim_m$-luokista, missä $w \sim_m w' \Longleftrightarrow \mathfrak{A}_w^{\mathrm{II}} \equiv_m \mathfrak{A}_{w'}^{\mathrm{II}}$ tai $w = w' = \lambda$, kun $w, w' \in \Sigma^*$. Edellisen lemman mukaan kaikilla $w, w' \in \Sigma^+$, $\alpha \in \Sigma$, $w \sim_m w'$ pätee $w\alpha \sim_m w'$, mistä seuraa $\sim_m$:n invarianttius. □

Yhtäpitävien väitteiden listaan voitaisiin lisätä vielä:

e) L on jonkin epädeterministisen äärellisen automaatin tunnistama.

f) L on säännöllinen.

Epädeterministinen äärellinen automaatti on kuten äärellinen automaatti, mutta tilasiirtymäfunktion tilalla on tilasiirtymärelaatio. Säännölliset kielet, tai lausekkeet, ovat monista ohjelmista varsinkin UNIX-järjestelmissä tuttuja (emacs, grep). Käytännön sovelluksissa tosin säännöllisyyttä usein rajoitetaan. Kohdat e ja f on jätetty kurssin aineistosta pois yksinkertaisesti esityksen keventämisen vuoksi.

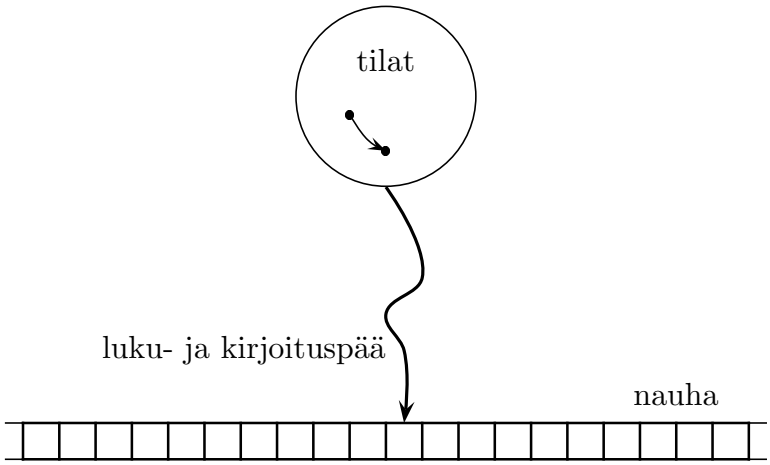
Richard Büchi todisti lauseensa vuonna 1960. Jälkikäteen asiaa tarkastellen se on ensimmäisiä deskriptiivisen vaativuusteorian tuloksia.

3. Turingin kone ja vaativuusluokat

Edellisessä luvussa nähtiin, että äärellisen automaatin kielten tunnistuskyky on varsin rajoittunut. Äärellisen automaatin kielten tunnistusvoimaa rajoittaa se, että automaatti joutuu hyväksymään tai hylkäämään syötteen yhden lukukerran jälkeen, sekä se, että automaatti ei voi hyödyntää työmuistia laskentansa aikana. Toisaalta nämä rajoitukset takaavat sen, että äärellisen automaatin laskenta on hyvin tehokasta: Syötteenä oleva merkkijono käydään läpi merkkijonon pituuteen verrannollisessa ajassa eikä ylimääräistä muistitilaa tarvita (automaatin tiloihin voi ajatella tarvittavan vakiomäärä tilaa). Turingin kone laajentaa äärellistä automaattia molemmissa edellä mainituissa suhteissa. On ehkä yllättävää, että näin yksinkertaisilla rajoituksista vapautumisilla saadaan yleisen laskennan malli, ts. yleisesti ajatellaan, että jos jokin asia on laskettavissa, niin se on laskettavissa Turingin koneella.

Äärellisen automaatin laskentamalli on niin yksinkertainen, ettei koneen käyttämään lukumekanismiin tarvitse kiinnittää erityistä huomiota; automaatti yksinkertaisesti lukee syötteen merkkejä järjestyksessä läpi. Turingin kone sen sijaan saa käydä syötettä

moneen kertaan läpi, ja sillä on myös työmuistia käytettävissä. Syötteet, työmuisti ja tulosteet sijaitsevat nauhalla (tai nauhoilla), jota käy läpi luku- ja kirjoituspää. Vaikka Turingin kone on teoreettisen tietojenkäsittelytieteen vakiintunut laskennan malli, määritelmän yksityiskohdat vaihtelevat lähteestä toiseen. Tämä johtuu ennen kaikkea mallin robustisuudesta eli siitä, että eri muunnelmia Turingin koneesta on mahdollista simuloida toisillaan. Näissä luennoissa käytettävää versiota kuvaa seuraava kaavio.



3.1. Määritelmä. *Turingin kone* on viisikko $M = (Q, \Sigma, \delta, a, F)$, missä
1) Q on äärellinen joukko *tiloja*,
2) Σ on äärellinen epätyhjä merkistö,
3) *tilasiirtymäfunktio* eli *Turingin taulu* on muotoa

$$\delta\colon Q \times (\Sigma \cup \{\Box\}) \rightharpoonup (\Sigma \cup \{\Box\}) \times Q \times \{-1, 0, 1\},$$

4) $a \in Q$ on *alkutila*,

ja

5) $F \subset Q$ on *hyväksyvien tilojen* joukko.

Tässä $\Box \notin \Sigma$ on tyhjää solua merkitsevä merkki.

Huomautus. Äärellisen automaatin pysähtyminen on ongelmaton asia, koska automaatti pysähtyy heti saatuaan syötteen luettua. Turingin koneessa syöte voidaan lukea moneen kertaan, joten pysähtyminen täytyy määritellä toisin. Siksi Turingin koneen tilasiirtymäfunktio on *osittainen* kuvaus: jos Turingin taulu ei jossain tilanteessa sisällä vastausta, miten toimia, niin Turingin kone pysähtyy, kuten myöhemmin selviää.

Turingin kone on siten äärellinen kone, joka suorittaa laskentaa lukien soluista (yhden merkin yksikkö) koostuvaa nauhaa, joka on molempiin suuntiin ääretön. Laskennan aikana jokainen nauhan solu sisältää joko merkin merkistöstä Σ tai on tyhjä, jota merkitään symbolilla $\Box$. Turingin koneen M laskenta muodostuu yksittäisistä peräkkäisistä laskenta-askeleista. Jos laskenta-askeleen aluksi kone M on tilassa q, lukee merkkiä a ja Turingin taulun sisältämä komento on $\delta(q, a) = (a', q', \varepsilon)$, niin seuraavaksi M korvaa

merkin a jollakin merkillä a', siirtää luku- ja kirjotuspäätä askeleen ε (eli solun verran oikealle, jos $\varepsilon = 1$, vasemmalle, jos $\varepsilon = -1$, tai pitää lukupään paikallaan, jos $\varepsilon = 0$) ja siirtyy tilasta q tilaan q'.

Seuraava määritelmä pyrkii kuvaamaan Turingin koneen toiminnan yksityiskohtaisesti.

3.2. Määritelmä. Tarkastellaan Turingin konetta $M = (Q, \Sigma, \delta, a, F)$.

a) *Laskennan tilanne* on kolmikko $S = (q, W, n) \in Q \times {}^{\mathbb{Z}}(\Sigma \cup \{\square\}) \times \mathbb{Z}$. Tässä q kuvaa Turingin koneen (sisäistä) tilaa, $W\colon \mathbb{Z} \to \Sigma \cup \{\square\}$ on *nauhan sisältö*, ts. kohdassa $x \in \mathbb{Z}$ on aina merkki $W(x)$, ja n on *lukupään paikka*.

b) Kun W on nauhan sisältö, merkitään $\mathrm{supt}(W) = W^{-1}[\Sigma]$, mikä on siis nauhan epätyhjien solujen joukko. Turingin koneen M *alkutilanne syötteellä* $w \in \Sigma^*$ on $(a, W_0, 0)$, missä W_0 on se yksikäsitteinen nauhan sisältö, jolle $\mathrm{supt}(W) = \{0, \ldots, |w|-1\}$ ja $W{\restriction}\{0, \ldots, |w|-1\} = w$. Epämuodollisemmin: alkutilanteessa M on (sisäisesti) alkutilassa, nauhalle on kirjoitettu syöte w ja luku- ja kirjoituspää on origossa syötteen ensimmäisen merkin kohdalla.

c) Laskenta *päättyy* tilanteessa $S = (q, W, n)$, jos $(q, W(n)) \notin \mathrm{dom}(\delta)$. Laskenta päättyy *hyväksyvään tilaan*, jos $q \in F$, ja *hylkäävään tilaan*, jos $q \notin F$.

d) Jos tilanteessa $S = (q, W, n)$ Turingin taulu komentaa $(\alpha, q', \varepsilon) = \delta(q, W(n))$, niin laskenta-askeleen aikana Turingin kone M siirtyy tilanteesta S tilanteeseen $S' = (q', W', n + \varepsilon)$, missä $W'\colon \mathbb{Z} \to \Sigma \cup \{\square\}$,

$$W'(x) = \begin{cases} \alpha, & \text{kun } x = n \\ W(x), & \text{muuten.} \end{cases}$$

Laskenta-askelta tilanteesta S tilanteeseen S' merkitään $S \vdash_M S'$.

Edellisen määritelmän avulla on arvattavissa, mitä tarkoitetaan Turingin koneen laskennalla. Jälleen on huomattavissa selkeä ero äärellisen automaatin ja Turingin koneen välillä, äärellisen automaatin laskenta nimittäin aina päättyy, Turingin koneen ei. Ero on perustavanlaatuinen, sillä pysähtymisongelma on tunnettu ns. ratkeamaton ongelma. Käytännössä tämä tarkoittaa, että jokaisen täydelliseen laskennan malliin liittyy vastaavanlainen ongelma.

3.3. Määritelmä. Olkoon $M = (Q, \Sigma, \delta, a, F)$ Turingin kone ja $\boldsymbol{S} = (S_i)_{i \in I}$ jono tilanteita, missä I on luonnollisen lukujen epätyhjä alkupätkä, ts. joko $I = \mathbb{N}$ tai $I = \{0, \ldots t\}$ jollakin $t \in \mathbb{N}$.

a) $\boldsymbol{S}$ on *laskenta syötteellä* w, jos S_0 on alkutilanne syötteellä w ja $S_i \vdash_M S_{i+1}$, kun $i, i+1 \in I$.

b) Laskenta $\boldsymbol{S}$ on *maksimaalinen*, jos sitä ei voi jatkaa, ts. joko $I = \mathbb{N}$ tai $I = \{0, \ldots, t\}$ jollakin $t \in \mathbb{N}$ ja S_t on lopputilanne eli laskenta $\boldsymbol{S}$ on päättynyt tilanteeseen S_t.

c) Maksimaalinen laskenta $\boldsymbol{S}$ on *päättyvä eli äärellinen*, jos I on äärellinen, muuten *päättymätön eli ääretön.*

d) Maksimaalinen laskenta $\boldsymbol{S}$ syötteellä w *hyväksyy syötteen* w, jos se on päättyvä ja päättyy hyväksyvään tilanteeseen. Vastaavasti $\boldsymbol{S}$ *hylkää syötteen* w, jos se on päättyvä ja päättyy hylkäävään tilanteeseen.

Turingin koneeseen M ja syötteeseen w liittyvä maksimaalinen laskenta $\boldsymbol{S}$ on selvästi *yksikäsitteinen*. Tässä esitellyt Turingin koneet toimivat siis deterministisesti.

Vaativuusluokat

Turingin koneen teoreettinen arvo laskennan mallina selittyy suurelta osin sillä, että se on niin homogeeninen: jokainen solu sisältää yhtä paljon informaatiota ja jokainen laskenta-askel on operaationa samanarvoinen. Siksi laskennan vaatimia resursseja on yksinkertaista mitata Turingin koneen avulla.

3.4. Määritelmä. Olkoon $M = (Q, \Sigma, \delta, a, F)$ Turingin kone ja $L \subset \Sigma^*$ kieli.

a) Turingin kone M *käyttää syötteen* $w \in \Sigma^*$ *käsittelyyn ajan*

$$t_M(w) = \begin{cases} t, & \text{jos } \boldsymbol{S} = (S_0, \ldots, S_t) \text{ on päättyvä} \\ \infty, & \text{jos } \boldsymbol{S} \text{ on päättymätön,} \end{cases}$$

missä $\boldsymbol{S}$ on M:n maksimaalinen laskenta syötteellä w. Vastaavasti M *suoriutuu syötteeseen* w *liittyvästä laskennasta tilassa*

$$s_M(w) = \begin{cases} \left|\bigcup_{i=0}^{t} \operatorname{supt}(W_i)\right|, & \text{jos } \boldsymbol{S} = ((q_0, W_0, n_0), \ldots, (q_t, W_t, n_t)) \text{ on päättyvä} \\ \infty, & \text{jos } \boldsymbol{S} \text{ on päättymätön.} \end{cases}$$

b) M *ratkaisee kielen* L, jos M pysähtyy kaikilla syötteillä ja

$$L = \{\, w \in \Sigma^* \mid M \text{ hyväksyy syötteen } w \,\}.$$

c) Kieli L on *polynomisessa ajassa ratkeava* eli luokassa PTIME, jos on olemassa sellainen Turingin kone M ja $\mathbb{N}$-kertoiminen polynomifunktio $P\colon \mathbb{N} \to \mathbb{N}$, että M ratkaisee kielen L ja kaikilla syötteillä $w \in \Sigma^*$ pätee $t_M(w) \leq P(|w|)$.

c) Kieli L on *polynomisessa tilassa ratkeava* eli luokassa PSPACE, jos on olemassa sellainen Turingin kone M ja $\mathbb{N}$-kertoiminen polynomifunktio $P\colon \mathbb{N} \to \mathbb{N}$, että M ratkaisee kielen L ja kaikilla syötteillä $w \in \Sigma^*$ pätee $s_M(w) \leq P(|w|)$.

Turingin koneen muunnelmat

3.5. Deterministinen/epädeterministinen: Kuten todettiin, Turingin koneesta on olemassa useita muunnelmia ja tässä esitelty Turingin kone on *deterministinen*. Nimitys tulee siitä, että missä tahansa laskennan vaiheessa koneella on korkeintaan yksi mahdollinen seuraava laskenta-askel ja siten koneeseen liittyvä maksimaalinen laskenta on yksikäsitteinen. Jos Turingin koneen määritelmässä luovutaan Turingin taulun δ funktionaalisuudesta ja sallitaan taulun olevan mikä tahansa relaatio

$$\delta \subset \big(Q \times (\Sigma \cup \{\square\})\big) \times \big((\Sigma \cup \{\square\}) \times Q \times \{-1, 0, 1\}\big),$$

niin tällöin vastaavaa Turingin konetta kutsutaan *epädeterministiseksi*.

Tällöin syötettä vastaa yleensä useampia maksimaalisia laskentoja. Epädeterministinen Turingin kone ei kuvaakaan yhtä laskentaa, vaan paremminkin perheen erilaisia laskentoja, joista osa voi pysähtyä hyväksyvään tilaan, osa hylätä syötteen ja osa olla pysähtymättä. Epädeterministisen koneen M laskentaa syötteellä w voidaan kuvata puulla, jonka juuren muodostaa kone M alkutilanteessa syötteellä w. Tässä puussa haarautuminen vastaa sitä, että kyseisessä laskennan vaiheessa koneella M on enemmän kuin yksi seuraava laskenta-askel. Syötteen hyväksyntään riittää, että jokin näistä maksimaalisista laskennoista hyväksyy syötteen.

Vaativuusteoreettisissa tarkasteluissa Turingin koneesta esitetään yleensä rinnan deterministinen ja epädeterministinen muunnelma. Epädeterministisen muunnelman avulla määritellään sitten epädeterministiset vaativuusluokat, kuten NP, joka vastaa determinististä luokkaa PTIME, ja NPSPACE, joka vastaa luokkaa PSPACE. Voidaan näyttää, että NP sisältyy luokkaan PSPACE ja NPSPACE = PSPACE.

Vaikka deterministisen ja epädeterministisen Turingin koneen välillä on (otaksuttavasti) vaativuusteoreettinen ero, niin niillä voidaan laskea samat asiat – kunhan deterministisessä muunnelmassa käytetään enemmän aikaa ja tilaa.

3.6. Moninauhaisuus: Vähäisempiä muunnelmia saadaan niin, että sallitaan Turingin koneen käyttävän useampia nauhoja, jolloin tietenkin tarvitaan myös usempia luku- ja kirjoituspäitä. Tällöin eri nauhoja voidaan käyttää erikoistuneisiin tarkoituksiin: Voidaan esimerkiksi sallia, että koneella on käytössään erikseen syötenauhat ja erillisiä työnauhoja, ja syötenauhojen luku- ja kirjoituspäät voidaan rajoittaa pelkiksi lukupäiksi. *Moninauhaisia* Turingin koneita voidaan simuloida yksinauhallisella koneella siten, että simuloiva kone käyttää aikaa $p(f(|w|))$ syötteellä w, missä $p \in \mathbb{N}[x]$ on polynomi ja $f\colon \mathbb{N} \to \mathbb{N}$ on moninauhaisen koneen laskenta-aikaa rajoittava funktio. Erityisesti tästä seuraa, että luokkien PTIME, NP ja PSPACE määritelmissä voidaan sallia myös moninauhaiset Turingin koneet suhteen.

Näissä luennoissa esitelty yksinnauhainen deterministinen Turingin kone riittää siis hyvin deterministisen vähintään polynomisen aika- ja tilavaativuuden tapauksissa. Alempien tilavaativuusluokkien kohdalla tulee kuitenkin se ongelma, että yllä esitetyn määritelmän mukaan aina $s_M(w) \geq |w|$ eli tilavaativuudesta tulee vähintään lineaarinen. Erottelemalla syöte- ja työnauhat ja kieltämällä kirjoitusmahdollisuus syötenauhalla voidaan tilavaativuus määritellä uudestaan niin, että pienemmät tilavaativuudet tulevat mahdollisiksi.

Turingin koneen määritelmää voidaan edelleen liberalisoida niin, että samaa nauhaa lukemaan voi olla käytettävissä usempia luku- ja kirjoituspäitä, joista osa voi siis olla pelkkiä luku-, toiset kirjoituspäitä.

3.7. Nauhojen päät: Puhtaasti teknisluonteisista eroista mainittakoon, että joskus vaaditaan, että nauhalla täytyy olla alkupää, jolloin nauha on siis vain oikealle päin rajoittamaton.

4. Kiintopistelogiikat

Ensimmäisen kertaluvun logiikassa ei pystytä ilmaisemaan kaikkia laskennallisesti yksinkertaisia asioita, kuten mallin – edes järjestetyn mallin – koon parillisuutta. Samoin verkon yhtenäisyys on mahdotonta ilmaista FO:ssa. vaikka yhtenäisyyden laskentaan liittyviä vaiheita on mahdollista kuvata FO:ssa.

4.1. Esimerkki. Määritellään verkkojen aakkoston $\{E\}$ kaavat $\delta_i(x,y)$, $i \in \mathbb{N}$, rekursiivisesti seuraavasti:

$$\delta_0(x,y) \text{ on } x = y$$

ja

$$\delta_{i+1}(x,y) \text{ on } \delta_i(x,y) \vee \exists z\,(\delta_i(x,z) \wedge E(z,y)).$$

Induktiolla on helppo osoittaa, että kun $\mathbb{G}$ on verkko, $a, b \in \mathrm{Dom}(\mathbb{G})$ ja $i \in \mathbb{N}$, niin $\mathbb{G} \models \delta_i[a/x, b/y]$, jos ja vain jos solmujen a ja b etäisyys on korkeintaan i eli solmusta a on solmuun b polku, jonka pituus on korkeintaan i. Edelleen verkko $\mathbb{G}$ on yhtenäinen, jos ja vain jos $\mathbb{G} \models \chi$, missä $\chi = \forall x\,\forall y \bigvee_{i\in\mathbb{N}} \delta_i(x,y)$.

Kuitenkaan χ ei ole FO:n lause, sillä siinä esiintyy ääretön disjunktio. Tavallisesti sidottuja muuttujia korvattaessa tilalle otetaan jatkuvasti uusia muuttujia. Jos sen sijasta muuttujien y ja z roolit vaihdetaankin, jokaisessa kaavassa δ_i onkin kaikkiaan vain kolme muuttujaa. Esimerkiksi $\delta_2(x,y)$ on

$$x = y \vee \exists z\,(x = z \wedge E(z,y)) \vee \exists z\,\Big(\big(x = z \vee \exists y\,(x = y \wedge E(y,z))\big) \wedge E(z,y)\Big).$$

Tällöin kaavat δ_i ovat paitsi FO:ssa, myös kolmen muuttujan kaavoja ja siten χ on FVL^3:ssa.

Toisaalta χ on aivan erityislaatuinen FVL:n lause, koska kaavat δ_i määräytyvät toisistaan hyvin siistin rekursiivisen säännön mukaan. Tämän analysoimiseksi merkitään

$$\varphi = C(y) \vee y = x \vee \exists z\,(C(z) \wedge E(z,y)).$$

Siis $\varphi \in \mathrm{FO}[\{E, C, x, y\}]$. Tarkastellaan tilannetta kiinteässä äärellisessä verkossa $\mathbb{G}$, jonka solmujoukko on $V = \mathrm{Dom}(\mathbb{G})$. Kun $a \in V$, merkitään $B_i(a)$:lla niiden solmujen b joukkoa, joiden etäisyys solmusta a on korkeintaan i, ts. $B_i(a) = \{\, b \in V \mid \mathbb{G} \models \delta_i[a/x, b/y] \,\}$. Tällöin seuraavat ovat yhtäpitäviä:

$$\begin{aligned}
&\mathbb{G} \models \varphi[B_i(a)/C, a/x, b/y],\\
&\mathbb{G} \models C(y) \vee \exists z\,(C(z) \wedge E(z,y)[B_i(a)/C, a/x, b/y],\\
&\mathbb{G} \models \delta_i(x,y) \vee \exists z\,(\delta_i(x,z) \wedge E(z,y)[a/x, b/y],\\
&\mathbb{G} \models \delta_i(x,y)[a/x, b/y] \text{ ja}\\
&b \in B_{i+1}(a).
\end{aligned}$$

Jos siis kiinnitetään $a \in V$ ja määritellään operaattori $F_\varphi\colon \mathcal{P}(V) \to \mathcal{P}(V)$,

$$F_\varphi(B) = \{\, b \in V \mid \mathbb{G} \models \varphi[B/C, a/x, b/y] \,\},$$

niin kaikilla $i \in \mathbb{N}$ pätee $F_\varphi(B_i(a)) = B_{i+1}(a)$. Lisäksi huomataan, että $F_\varphi(\emptyset) = \{a\} = B_0(a)$.

Yleistetään edellisen esimerkin tilannetta ja tarkastellaan joukon M operaattoreita $F\colon \mathcal{P}(M) \to \mathcal{P}(M)$. Operaattoriin voidaan liittää iteroimalla saadut vaiheet $S_0(F) = \emptyset$, $S_{i+1}(F) = F(S_i(F))$, kun $i \in \mathbb{N}$, ts. $S_i(F) = F^i(\emptyset) = \underbrace{F(\cdots(F}_{i \text{ kpl}}(\emptyset))\cdots)$.

4.2. Määritelmä. Kuvaus $F\colon \mathcal{P}(M) \to \mathcal{P}(M)$ on *inflatorinen*, jos kaikilla $X \subset M$ pätee $X \subset F(X)$.

4.3. Lemma. *Olkoon M äärellinen joukko ja $F\colon \mathcal{P}(M) \to \mathcal{P}(M)$. Tällöin jono $(S_i(F))_{i\in\mathbb{N}}$ on lopulta jaksollinen eli on olemassa sellaiset $m \in \mathbb{N}$ ja $t \in \mathbb{Z}_+$, että $S_i(F) = S_{i+t}(F)$ kaikilla $i \in \mathbb{N}$, $i \geq m$. Luku m voidaan valita niin, että $m < 2^{|M|}$. Jos F on inflatorinen, niin jokin $S_m(F)$, missä $m \in \mathbb{N}$ ja $m \leq |M|$, on kuvauksen F kiintopiste, ts. luvut m ja t yllä voidaan valita niin, että $m < |M|$ ja $t = 1$.*

Todistus. Tulos perustuu yksinkertaisesti laatikkoperiaatteeseen. Koska $|\mathcal{P}(M)| = 2^{|M|}$, niin jonossa $(S_0(F), \ldots, S_{2^{|M|}}(F))$ on pakko olla toistoa, joten on olemassa sellaiset indeksit m ja $m{+}t$, että $m \in \mathbb{N}$, $t \in \mathbb{Z}_+$, $m{+}t \leq 2^{|M|}$ ja $S_m(F) = S_{m+t}(F)$. Soveltamalla yhtälöön puolittain kuvausta F saadaan induktiolla $S_i(F) = S_{i+t}(F)$ kaikilla $i \in \mathbb{N}$, $i \geq m$.

Jos F on inflatorinen, niin jono $(S_i(F))_{i\in\mathbb{N}}$ on kasvava, joten myös jono $(|S_i(F)|)_{i\in\mathbb{N}}$ on kasvava. Jälkimmäinen jono on kuitenkin rajoitettu, sillä kaikilla $i \in \mathbb{N}$ pätee $|S_i(F)| \leq |M|$ ja M on äärellinen. Siis jollain $m \in \mathbb{N}$, missä $m < |M|$, pätee $|S_m(F)| = |S_{m+1}(F)|$, mikä inflatorisuuden vuoksi tarkoittaa, että $S_m(F) = S_{m+1}(F)$. Tästä seuraa induktiolla $S_i(F) = S_{i+1}(F)$ kaikille $i \in \mathbb{N}$, $i \geq m$. □

Lemman perusteella on järkevää merkitä $S_\infty(F) = S_m(F)$, jos jokin $S_m(F)$, $m \in \mathbb{N}$, on kuvauksen F kiintopiste. Jos tällaista kiintopistettä ei ole, merkitään $S_\infty(F) = \emptyset$.

Huomautus. On tietenkin mahdollista, että kuvauksella $F\colon \mathcal{P}(M) \to \mathcal{P}(M)$ on kiintopiste, vaikka mikään $S_m(F)$, $m \in \mathbb{N}$, ei sellainen olisikaan. Yksinkertaisin esimerkki saadaan, kun $M = \{0, 1\}$, $F(\emptyset) = M$, $F(M) = \emptyset$, $F(\{0\}) = \{0\}$ ja $F(\{1\}) = \{0\}$.

Tämän valmistelun jälkeen voidaan ryhtyä rakentamaan kiintopistelogiikoita. Tarkoituksena on määritellä kaavanmuodostussääntö, joka toteuttaa edellisen esimerkin kaltaisten iteraation.

Kun φ on lause, X on relaatiosymboli, jonka paikkaluku on $k = \#(X)$, ja $\boldsymbol{x} = (x_0, \ldots, x_{k-1})$ on jono vakiosymboleita, niin lauseesta φ muodostetaan *kiintopistekvantifionnilla* lause $\exists X(\boldsymbol{x})\, \varphi$, jonka aakkosto on $\tau(\exists X(\boldsymbol{x})\, \varphi) = (\tau(\varphi) \setminus \{X\}) \cup \{x_0, \ldots, x_{k-1}\}$. (Epätriviaaleissa tapauksissa yleensä $\{x_0, \ldots, x_{k-1}\} \subset \tau(\varphi)$, jolloin aakkosto palautuu yksinkertaisesti muotoon $\tau(\exists X(\boldsymbol{x})\, \varphi) = (\tau(\varphi) \setminus \{X\})$.)

Kiintopistekvantifionnille voi määritellä kaksi vaihtoehdoista semantiikka. Olkoon $\mathfrak{A}$ aakkoston σ malli, missä $\tau(\exists X(\boldsymbol{x})\,\varphi) \subset \sigma$. Lause φ ja malli $\mathfrak{A}$ määräävät operaattorit $F_\varphi\colon \mathcal{P}(\mathrm{Dom}(\mathfrak{A})^k) \to \mathcal{P}(\mathrm{Dom}(\mathfrak{A})^k)$,

$$F_\varphi(S) = \{\, (a_0, \ldots, a_{k-1}) \in \mathrm{Dom}(\mathfrak{A})^k \mid \mathfrak{A} \models \varphi[a_0/x_0, \ldots, a_{k-1}/x_{k-1}, S/X] \,\}$$

ja $G_\varphi\colon \mathcal{P}(\mathrm{Dom}(\mathfrak{A})^k) \to \mathcal{P}(\mathrm{Dom}(\mathfrak{A})^k)$,

$$G_\varphi(S) = S \cup \{\, (a_0, \ldots, a_{k-1}) \in \mathrm{Dom}(\mathfrak{A})^k \mid \mathfrak{A} \models_{\mathrm{IFP}} \varphi[a_0/x_0, \ldots, a_{k-1}/x_{k-1}, S/X] \,\}.$$

Tällöin *inflatorisen semantiikan* mukaan

$$\mathfrak{A} \models_{\mathrm{IFP}} \exists X(\boldsymbol{x})\,\varphi, \text{ jos ja vain jos } (x_0^{\mathfrak{A}}, \ldots, x_{k-1}^{\mathfrak{A}}) \in S_\infty(G_\varphi),$$

kun taas *luonnollisen semantiikan* mukaan

$$\mathfrak{A} \models \exists X(\boldsymbol{x})\,\varphi, \text{ jos ja vain jos } (x_0^{\mathfrak{A}}, \ldots, x_{k-1}^{\mathfrak{A}}) \in S_\infty(F_\varphi).$$

4.4. Määritelmä. *Inflatorinen kiintopistelogiikka* IFP *ja osittainen kiintopistelogiikka* PFP ovat pienimpiä logiikoita, jotka sisältävät atomilauseet ja ovat suljettuja negaation, konjunktion, eksistenssikvantifionnin ja kiintopistekvantifioinnin suhteen. Semantiikka määritellään logiikoissa eri tavoilla: logiikassa PFP on käytössä luonnollinen semantiikka, kun sen sijaan logiikassa IFP kiintopistekvantifiointi noudattaa inflatorista semantiikkaa.

Huomautus. 1) On tärkeää havaita, että kuvaus inflatorisen semantiikan määrittelyssä käytetyt operaattorit G_φ ovat aina inflatorisia, joten vastaavat kiintopiste ovat olemassa. Sen sijaan operaattoreilla F_φ ei välttämättä ole kiintopistettä, ja vielä useammin käy niin, että sellainen ei löydy iteratiivisella prosessilla, vaikka kiintopiste olisikin olemassa, mistä nimi osittainen kiintopistelogiikka.

2) Jos $\mathfrak{A}$ on aakkoston $\tau(\varphi) \setminus \{X, x_0, \ldots, x_{k-1}\}$ malli, mutta tilanne muuten kuten semantiikan määrittelyssä yllä, niin inflatorisen semantiikan määritelmä saadaan kaavamuotoon

$$\mathfrak{A} \models_{\mathrm{IFP}} \exists X(\boldsymbol{x})\,\varphi[a_0/x_0, \ldots, a_{k-1}/x_{k-1}], \text{ jos ja vain jos } (a_0, \ldots, a_{k-1}) \in S_\infty(G_\varphi).$$

Samanlainen kaavamuoto saadaan tietenkin myös PFP:lle.

3) Kiintopistekvantifionnille tässä valittu symboli $\exists$ rinnastaa sen tavanomaisiin ensimmäisen ja toisen kertaluvun kvantifiointiin, mutta ei ole yleisessä käytössä. Kvantifionnille $\exists X(\boldsymbol{x})$ käytetään mm. merkintöjä $\mathrm{IFP}_{\boldsymbol{x},X}$, $\mathrm{PFP}_{\boldsymbol{x},X}$. Useissa lähteissä kvantifiointi myös esitellään suoraan niin, että lauseesta φ muodostetaan lause $[\exists X(\boldsymbol{x})\,\varphi]\boldsymbol{t}$, missä $\boldsymbol{t} = (t_0, \ldots, t_{k-1})$ on jono termejä. Tämän lauseen voi kuitenkin ymmärtää lyhennysmerkinnäksi lauseelle

$$\exists x_0 \cdots \exists x_{k-1} \left(\exists X(\boldsymbol{x})\,\varphi \wedge \bigwedge_{i=0}^{k} x_i = t_i \right).$$

4.5. Esimerkki. Esimerkin 4.1 analyysista seuraa nyt vaivatta, että IFP:n lause

$$\forall x \forall y \, \dashv C(x) \big(y = x \vee \exists z \, (C(z) \wedge E(z, y)) \big)$$

määrittelee kera verkkoaksioomien verkon yhtenäisyyden. Olkoon φ nimittäin kuten mainitussa esimerkissä, ts. iteroitava alikaava, ja tarkastellaan tapausta, jossa äärellinen verkko on $\mathbb{G}$ ja x tulkitaan solmuksi a, jolloin vastaava operaattori on $G_\varphi \colon \mathcal{P}(V) \to \mathcal{P}(V)$, $G_\varphi(B) = \{\, b \in V \mid \mathbb{G} \models \varphi[B/C, a/x, b/y] \,\}$. Esimerkin 4.1 merkinnöin verkossa $\mathbb{G}$ saadaan iteroinnin vaiheiksi $S_0(G_\varphi) = \emptyset$ ja $S_{i+1}(G_\varphi) = B_i(a)$, kun $i \in \mathbb{N}$. Siis $\mathbb{G} \models_{\mathrm{IFP}} \dashv C(x) \, \varphi[a/x, b/y]$, jos ja vain jos solmusta b on polku solmuun a. Siis $\mathbb{G} \models_{\mathrm{IFP}} \forall x \forall y \, \dashv C(x) \, \varphi$, jos ja vain jos $\mathbb{G}$ on yhtenäinen. Myös $\exists x \forall y \, \dashv C(x) \, \varphi$ kelpaisi yhtenäisyyden ilmaisemiseen, edellinen lausehan kertoo, että kaikki solmut ovat samassa komponentissa, jälkimmäinen, että jonkin solmun komponentti on koko solmujoukko.

4.6. Lause. *Jokaista logiikan* IFP *lausetta φ vastaa logiikan* PFP *lause φ^*, jolla on sama aakkosto ja samat mallit siinä mielessä, että kaikilla aakkoston $\tau(\varphi)$ äärellisillä malleilla pätee $\mathfrak{A} \models_{\mathrm{IFP}} \varphi$ täsmälleen silloin, kun $\mathfrak{A} \models \varphi^*$.*

Todistus. Rakennetaan $*$-käännös induktiolla IFP:n lauseen φ rakenteen suhteen.

1) Jos φ on atomilause, niin $\varphi^* = \varphi$.
2) $(\neg\varphi)^* = \neg\varphi^*$ ja $(\vartheta \wedge \psi)^* = \vartheta^* \wedge \psi^*$.
3) $(\exists x \, \vartheta)^* = \exists x \, \vartheta^*$.
4) $(\dashv X(\boldsymbol{x}) \, \vartheta)^* = \dashv X(\boldsymbol{x}) \, (X(\boldsymbol{x}) \vee \vartheta^*)$.

Induktiolla pitää myös osoittaa, että kaikilla aakkoston $\tau(\varphi)$ äärellisillä malleilla pätee $\mathfrak{A} \models_{\mathrm{IFP}} \varphi$ täsmälleen silloin, kun $\mathfrak{A} \models \varphi^*$. Kohtia 1–3 vastavat induktioaskeleet ovat ilmeisiä, joten oletetaan, että induktio-oletus pätee lauseelle ϑ ja tarkastellaan lauseena φ lausetta $\dashv X(\boldsymbol{x}) \, \vartheta$. Merkitään $k = |\boldsymbol{x}|$. Olkoon $\mathfrak{A}$ aakkoston $\tau(\varphi)$ äärellinen malli. Liitetään lauseeseen φ operaattorit F_{ϑ^*} ja G_ϑ kuten semantiikan määritelmässä. Tällöin induktio-oletuksesta seuraa suoraan, että kaikilla $S \subset \mathrm{Dom}(\mathfrak{A})^k$ pätee $G_\vartheta(S) = S \cup F_{\vartheta^*}(S) = F_{X(\boldsymbol{x}) \vee \vartheta^*}$. Siis seuraavat ovat yhtäpitäviä:

$$\begin{aligned}
&\mathfrak{A} \models_{\mathrm{IFP}} \dashv X(\boldsymbol{x}) \, \vartheta, \\
&(x_0^{\mathfrak{A}}, \ldots, x_{k-1}^{\mathfrak{A}}) \in S_\infty(G_\vartheta), \\
&(x_0^{\mathfrak{A}}, \ldots, x_{k-1}^{\mathfrak{A}}) \in S_\infty(F_{X(\boldsymbol{x}) \vee \vartheta^*}) \text{ ja} \\
&\mathfrak{A} \models \dashv X(\boldsymbol{x}) \, (X(\boldsymbol{x}) \vee \vartheta^*),
\end{aligned}$$

joten induktiotodistus menee läpi. □

5. PTIME:n karakterisointi

Büchin lauseen myötä on tullut selväksi kuvailevan vaativuusteorian perusasetelma: Erityisissä tilanteissa laskentaa suorittavia koneita – epämuodollisemmin voisi puhua ohjelmista tai algoritmeista – vastaavat tiettyjen logiikkojen lauseet. Büchin lauseessa koneet ovat äärellisiä automaatteja ja lauseet MSO:n lauseita, joten tämä tulos rinnastaa äärellisten automaattien laskennan ja siten säännölliset kielet sekä logiikan MSO. Teoreettisten koneiden syötteet ovat sanoja, kun taas logiikan lauseet ovat tosia tai epätosia malleissa, joten vastaavuus edellyttää mekanismin, joka rinnastaa malleja ja sanoja. Büchin lauseessa tietenkin yhteys muodostetaan sanojen ja vastaavien sanamallien välille. Malliteoreettisesti tulos on hyvin voimakkaasti rajaava, koska tulos käsittelee vain sanamalleja.

Kuvailevan vaativuusteorian perustavanlaatuisimmissa tuloksissa rinnastetaan vaativuusluokkia ja logiikoita. Ihanteellisessa tapauksessa tulos koskee kaikkia äärellisiä malleja, joiden aakkosto on äärellinen, mutta yleensä tulokset joudutaan rajaamaan järjestettyihin malleihin. Esimerkkinä tällaisesta tuloksesta on vaativuusluokan PTIME karakterisointi logiikan IFP avulla.

Kuten mainittiin, kuvailevan vaativuusteorian tulokset edellyttävät mallien ja sanojen välisen vastaavuuden. Luonnolliset tavat koodata malli sanaksi edellyttävät mallin perusjoukon alkioiden luettelemista jossain järjestyksessä. Yksinkertaisinta on siis, jos malli on valmiiksi järjestetty.

Olkoon $n \in \mathbb{Z}_+$ ja R joukon $\{0, \ldots, n-1\}$ k-paikkainen relaatio. Olkoon $\{\boldsymbol{a}_0, \ldots, \boldsymbol{a}_{n^k-1}\}$ joukon $\{0, \ldots, n-1\}^k$ luettelo sanakirjajärjestyksessä. Tällöin relaatiota R koodaava sana on

$$\text{koodi}(R) = b_0 \cdots b_{n^k-1} \in \{0,1\}^*,$$

missä

$$b_i = \begin{cases} 1, & \text{kun } \boldsymbol{a}_i \in R \\ 0, & \text{kun } \boldsymbol{a}_i \notin R. \end{cases}$$

Olkoon $\mathfrak{A}$ äärellisen aakkoston τ järjestetty malli. Tällöin on olemassa yksikäsitteinen $\mathfrak{A}^* \cong \mathfrak{A}$, jolle $\text{Dom}(\mathfrak{A}^*) = \text{Dom}(\mathfrak{A})$ ja $\leq^{\mathfrak{A}^*}$ on luonnollinen joukon $\{0, \ldots, n-1\}$ järjestys, missä $n = \text{card}(\mathfrak{A})$. Liitetään aakkostoon τ jokin kiinteä tapa luetella sen symbolit:

$$\tau = \{R_0, \ldots, r_{t-1}, f_0, \ldots, f_{u-1}, c_0, \ldots, c_{v-1}\},$$

ts. ensin luetellaan relaatiosymbolit (t kappaletta), sitten funktiosymbolit (u kappaletta) ja lopuksi vakiosymbolit (v kappaletta). Asetetaan

$$w_{\mathfrak{A}} = 1^n 0\, \text{koodi}(R_0^{\mathfrak{A}^*}) \cdots \text{koodi}(R_{t-1}^{\mathfrak{A}^*})\, \text{koodi}(f_0^{\mathfrak{A}^*}) \cdots \text{koodi}(f_{u-1}^{\mathfrak{A}^*})\, \text{koodi}(\{c_0^{\mathfrak{A}^*}\}) \cdots \text{koodi}(\{c_{v-1}^{\mathfrak{A}^*}\}),$$

missä funktioiden koodit muodostetaan samastamalla ne kuvaajansa kanssa.

Malliluokaksi kutsutaan isomorfian suhteen suljettua luokkaa yhteisen aakkoston malleja. Olkoon K malliluokka järjestettyjä malleja, missä yhteinen aakkosto τ on äärellinen. Asetetaan

$$L(K) = \{\, w_{\mathfrak{A}} \mid \mathfrak{A} \in K \,\} \subset \{0,1\}^*.$$

PTIME:n karakterisointi on nyt muotoiltavissa.

5.1. Lause. *Olkoon K malliluokka äärellisen aakkoston τ järjestettyjä malleja. Tällöin seuraavat ovat yhtäpitäviä:*

a) K on logiikassa IFP *määriteltävissä, ts. on olemassa sellainen lause $\varphi \in \mathrm{IFP}[\tau]$, että*

$$K = \{\, \mathfrak{M} \mid \mathfrak{M} \text{ on aakkoston } \tau \text{ äärellinen malli, } \mathfrak{M} \models \varphi \,\}.$$

b) $L(K)$ on ratkaistavissa luokassa PTIME. □

Tulos esitetään todistuksetta, mutta lyhyen todistushahmotelman kera. Toiseen suuntaan (kohdasta a seuraa kohta b) kyse on teknisestä induktiotodistuksesta: Jokaiseen lauseeseen φ liitetään induktiolla lauseen rakenteen suhteen Turingin kone M_φ. Tämän puolen todistuksen algoritminen sisältö on varsin selvä, sillä IFP:n lauseiden totuus äärellisessä mallissa voidaan laskea käyttämällä silmukoita, jotka eivät ole pitkiä. Toiseen suuntaan todistus on syvällisempi: Olkoon M kielen $L(K)$ ratkaiseva polynomisessa ajassa toimiva Turingin kone. Osoittautuu, että syötettä $w_{\mathfrak{A}}$ vastaavassa mallissa $\mathfrak{A}$ voidaan simuloida Turingin koneen M toimintaa niin, että tilanteet ja laskenta kuvaillaan $\mathrm{Dom}(\mathfrak{A})$:n relaationa, jotka ovat kiintopisteiteraatiolla määriteltävissä. Polynomiaikaisuus on tässä oleellista, jotta kuvaus onnistuisi.

Harjoituksia osaan IV

1. Rakenna joukon $\Sigma = \{a, b, c\}$ sanoja lukevat äärelliset automaatit, jotka tunnistavat seuraavat kielet.

a) $L_0 = \{\, w \in \Sigma^* \mid$ Sanassa w on viidellä jaollinen määrä kirjaimia $\}$.

b) $L_1 = \{\, w = \alpha_0 \dots a_{l-1} \in \Sigma^* \mid$ Kaikilla $j = 0, \dots, l-2$ pätee $\alpha_j \neq \alpha_{j+1} \,\}$.

c) $L_2 = \{\, w \in \Sigma^* \mid$ Joillakin $k, l, m \in \mathbb{Z}_+$ pätee $w = a^k b^l c^m \,\}$ eli kieli L_2 koostuu niistä sanoista, joissa on alussa kirjainta a, keskellä b:tä ja lopussa c:tä, kutakin ainakin yhden merkin verran.

2. Olkoon $L \subset \Sigma^*$ äärellinen. Osoita, että jokin äärellinen automaatti tunnistaa kielen L.

3. Olkoon $\tau = \{\leq\} \cup \{\, U_\alpha \mid \alpha \subset \Sigma \,\}$ merkkijoukkoa Σ vastaavien sanamallien aakkosto. Aakkoston τ lauseen φ sanotaan *määrittelevän* kielen $L \subset \Sigma^+$, jos

$$L = \{\, w \in \Sigma^+ \mid \mathfrak{A}_w \models \varphi \,\}.$$

Etsi ensimmäisen kertaluvun lauseet, jotka määrittelevät tehtävän 3 kielet L_1 ja L_2.

4. Osoita, että kieli $L_0 \setminus \{\lambda\}$, missä $\lambda = ()$ ja L_0 kuten tehtävässä 3, ei ole määriteltävissä ensimmäisen kertaluvun logiikassa. (Vihje: Tarkastele niitä kielen sanoja, joissa esiintyy vain yhtä kirjainta, ja näitä vastaavia sanamalleja. Käytä sitten tuttuja tuloksia lineaarijärjestysten välisistä EF-peleistä.)

5. Olkoon $k \in \mathbb{Z}_+$. Osoita, että toisen kertaluvun logiikassa voidaan ilmaista, että äärellisen mallin mahtavuus on jaollinen luvulla k. Toisin sanoen: On olemassa sellainen $\varphi \in \mathrm{SO}[\emptyset]$, että kaikissa äärellisissä malleissa $\mathfrak{A}$

$$\mathfrak{A} \models \varphi, \text{ jos ja vain jos } k \mid \mathrm{card}(\mathfrak{A}).$$

6. Osoita, että monadisessa toisen kertaluvun logiikassa MSO voidaan ilmaista, että äärellisen *järjestetyn* mallin mahtavuus on parillinen.

7. Verkko $\mathbb{G} \in \mathrm{Str}(\{E\})$ on *kaksiosainen*, jos on olemassa sellainen $U \subset \mathrm{Dom}(\mathbb{G})$, että verkon kaikki särmät ovat joukkojen U ja $\mathrm{Dom}(\mathbb{G}) \setminus U$ välisiä. Osoita, että kaksiosaisuus on logiikassa MSO ilmaistavissa.

8. Todista seuraava **pumppauslemma**: Olkoon $L \subset \Sigma^*$ äärellisen automaatin tunnistama kieli. Tällöin on olemassa sellainen $m \in \mathbb{N}$, että jokainen $s \in \Sigma^*$, $|s| \geq m$ jakautuu seuraavalla tavalla kolmeen osaan $u, v, w \in \Sigma^*$. 1) $s = uvw$, 2) $|uv| \leq m, v \neq \lambda$ ja 3) kaikilla $k \in \mathbb{N}$ ja $t \in \Sigma^*$ on voimassa

$$uvt \in L, \text{ jos ja vain jos } uv^k t \in L.$$

9. Olkoon Σ äärellinen merkkijoukko, jossa on vähintään kaksi alkiota. Olkoon $L \subset \Sigma^*$ joukon Σ *palindromien* joukko, ts. $w = \alpha_0 \dots \alpha_{l-1} \in L$, jos

ja vain jos $\alpha_i = \alpha_j$, kun $i + j = l - 1$, $i, j \in \mathbb{N}$. Voiko kielen L tunnistaa äärellisellä automaatilla?

10. Olkoot A ja B sellaisia joukkoja, että joukot A, B, $\mathcal{P}(A)$ ja $\mathcal{P}(B)$ ovat erillisiä. Tarkastellaan $\{U, V, E\}$-malleja $\mathfrak{A}$ ja $\mathfrak{B}$, missä $\#(U) = \#(V) = 1$ ja $\#(E) = 2$ sekä

$$\begin{gathered}\mathrm{Dom}(\mathfrak{A}) = A \cup \mathcal{P}(A),\ \mathrm{Dom}(\mathfrak{B}) = B \cup \mathcal{P}(B),\\ U^{\mathfrak{A}} = A,\ U^{\mathfrak{B}} = B,\ V^{\mathfrak{A}} = \mathcal{P}(A),\ V^{\mathfrak{B}} = \mathcal{P}(B),\\ E^{\mathfrak{A}} = \{\, (x, X) \mid x \in A,\ X \in \mathcal{P}(A),\ x \in X \,\},\\ E^{\mathfrak{B}} = \{\, (x, X) \mid x \in B,\ X \in \mathcal{P}(B),\ x \in X \,\}.\end{gathered}$$

(Luentojen merkinnöin siis $\mathfrak{A} = \langle A \rangle^{\mathrm{II}}$ ja $\mathfrak{B} = \langle B \rangle^{\mathrm{II}}$.) Oletetaan, että $|A| = 4$ ja $|B| = 5$. Etsi suurin $k \in \mathbb{N}$, jolle Elinalla on voittostrategia pelissä $\mathrm{EF}_k(\mathfrak{A}, \mathfrak{B})$.

11. Olkoot $k \in \mathbb{N}$ ja $\mathfrak{A}, \mathfrak{A}', \mathfrak{B}, \mathfrak{B}'$ saman äärellisen aakkoston τ äärellisiä järjestettyjä malleja, joille $\mathfrak{A} \cong_k \mathfrak{A}'$ ja $\mathfrak{B} \cong_k \mathfrak{B}'$. Osoita, että järjestetyille summille pätee

$$\mathfrak{A} \triangleleft \mathfrak{B} \cong_k \mathfrak{A}' \triangleleft \mathfrak{B}'.$$

12. Kieli $L \subset \{a, b\}^+$ sisältäköön täsmälleen ne sanat w, joissa a esiintyy useammin kuin b. Osoita, että L ei ole määriteltävissä ensimmäisen kertaluvun logiikassa.

13. Olkoon $\tau = \{\leq, A, B\}$, missä symbolit ovat relationaalisia ja $\#(\leq) = 2$, $\#(A) = \#(B) = 1$. Olkoon K sellaisten äärellisten järjestettyjen mallien $\mathfrak{M} \in \mathrm{Str}(\tau)$ luokka, että järjestyksen $\leq^{\mathfrak{M}}$ kääntävä kuvaus f on rajoittuman $\mathfrak{M}{\restriction}\{A, B\}$ automorfismi. Tässä siis f on se yksikäsitteinen bijektio $f\colon \mathrm{Dom}(\mathfrak{M}) \to \mathrm{Dom}(\mathfrak{M})$, jolle pätee $a \leq^{\mathfrak{M}} b$, jos ja vain jos $f(b) \leq^{\mathfrak{M}} f(a)$, kun $a, b \in \mathrm{Dom}(\mathfrak{M})$. Onko olemassa sellaista $\varphi \in \mathrm{MSO}[\tau]$, että kaikilla τ-malleilla $\mathfrak{M}$ pätee $\mathfrak{M} \in K$, jos ja vain jos $\mathfrak{M} \models \varphi$? (vrt. palindromiharjoitukseen IV.9)

14. Olkoon $\tau = \{\leq, A, B\}$, missä symbolit ovat relationaalisia ja $\#(\leq) = 2$, $\#(A) = \#(B) = 1$. Olkoon K sellaisten (äärellisten) järjestettyjen τ-mallien $\mathfrak{M}$ luokka, että $\left|A^{\mathfrak{M}}\right| = \left|B^{\mathfrak{M}}\right|$. Osoita, että äärellisen mallin luokkaan K kuuluminen ei ole MSO:ssa ilmaistavissa.

15. Verkko $\mathbb{G} \in \mathrm{Str}(\{E\})$ on *kaksiosainen*, jos on olemassa sellainen $V_0 \subset \mathrm{Dom}(\mathbb{G})$, että kaikilla $(a, b) \in E^{\mathbb{G}}$ pätee $(a, b) \in V_0 \times (\mathrm{Dom}(\mathbb{G}) \setminus V_0)$ tai $(b, a) \in V_0 \times (\mathrm{Dom}(\mathbb{G}) \setminus V_0)$. Kaksiosainen verkko on *tasapainoinen*, jos em. V_0 voidaan valita niin, että $|V_0| = |\mathrm{Dom}(\mathbb{G}) \setminus V_0|$.

a) Osoita, että kaksiosaisuus on logiikassa MSO ilmaistavissa.

b) Osoita, että äärellisten verkkojen tasapainoisuus ei sen sijaan ole ilmaistavissa logiikassa MSO. (Palauta ongelma edelliseen tehtävään. Liitä merkistön $\{a, b\}$ sanamalliin $\mathfrak{A}_w$ luonnollisella tavalla kaksijakoinen verkko $\mathbb{G}_w$, ja näytä, että jos $\mathbb{G}_w$:n tasapainoisuus olisi ilmaistavissa, niin edellisen tehtävänkin luokka K' olisi MSO:ssa.)

16. Olkoon $L \subset \Sigma^*$ äärellisen automaatin tunnistama kieli. Todista, että on olemassa Turingin kone M, joka hyväksyy saman kielen L.

17. Rakenna aakkoston $\{0,1\}$ Turingin kone, joka hyväksyy täsmälleen muotoa $w = 1^n$, $n \in \mathbb{Z}_+$, olevat sanat ja jonka pysähtyessä hyväksyvään tilaan nauhalla on kirjoitettuna n binäärimuodossa.

18. Osoita, että logiikassa IFP voidaan ilmaista, että
a) äärellisen järjestetyn joukon mahtavuus on parillinen ja
b) verkko on yhtenäinen.

19. Todista, että jokaista inflatorisen kiintopistelogiikan lausetta $\varphi \in \mathrm{IFP}[\tau]$ vastaa käännös äärellisen monen muuttujan logiikassa $\varphi^* \in \mathrm{FVL}[\tau]$, ts. kaikilla äärellisillä $\mathfrak{M} \in \mathrm{Str}(\tau)$ pätee $\mathfrak{M} \models \varphi$, jos ja vain jos $\mathfrak{M} \models \varphi^*$.

20. Olkoon $\tau = \{\leq, A, B\}$, missä symbolit ovat relationaalisia ja $\#(\leq) = 2$, $\#(A) = \#(B) = 1$. Olkoon K sellaisten äärellisten järjestettyjen mallien $\mathfrak{M} \in \mathrm{Str}(\tau)$ luokka, että järjestyksen $\leq^{\mathfrak{M}}$ kääntävä kuvaus f on rajoittuman $\mathfrak{M}{\restriction}\{A,B\}$ automorfismi. Tässä siis f on se yksikäsitteinen bijektio $f\colon \mathrm{Dom}(\mathfrak{M}) \to \mathrm{Dom}(\mathfrak{M})$, jolle pätee $a \leq^{\mathfrak{M}} b$, jos ja vain jos $f(b) \leq^{\mathfrak{M}} f(a)$, kun $a, b \in \mathrm{Dom}(\mathfrak{M})$. Onko olemassa sellaista $\varphi \in \mathrm{MSO}[\tau]$, että kaikilla τ-malleilla $\mathfrak{M}$ pätee $\mathfrak{M} \in K$, jos ja vain jos $\mathfrak{M} \models \varphi$?

21. Esitä esimerkki logiikan IFP lauseesta, joka ei ole loogisesti ekvivalentti minkään logiikan FO lauseen kanssa.

22. Esitä esimerkki logiikan FVL lauseesta, jonka aakkosto äärellinen ja joka ei ole loogisesti ekvivalentti minkään logiikan IFP lauseen kanssa.

23. Osoita, että minmax-algoritmi on seuraavassa mielessä inflationaarisessa kiintopistelogiikassa määriteltävissä: Kutsutaan relationaalisen aakkoston $\tau = \{R, V, H\}$ $(\#(R) = 2, \#(V) = \#(H) = 1)$ mallia $\mathcal{T}$ *pelipuuksi*, jos $\mathcal{T}_0 = \mathcal{T}{\restriction}\{R\}$ on suunnattu äärellinen puu, $V^{\mathcal{T}}$ ja $H^{\mathcal{T}}$ ovat erillisiä sekä $V^{\mathcal{T}} \cup H^{\mathcal{T}}$ on suunnatun puun $\mathcal{T}_0$ lehtien joukko. Määritellään induktiivisesti voitto- ja häviöjoukot

$$V_0 = V^{\mathcal{T}},\ H_0 = H^{\mathcal{T}}$$
$$V_{n+1} = V_n \cup \{\, t \in \mathrm{Dom}(\mathcal{T}) \mid \text{solmun } t \text{ seuraajista jokin on joukossa } H_n \,\}$$
$$H_{n+1} = V_n \cup \{\, t \in \mathrm{Dom}(\mathcal{T}) \mid \text{solmun } t \text{ seuraajat ovat kaikki joukossa } V_n \,\}.$$

Osoita, että on olemassa $\varphi \in \mathrm{IFP}[\tau]$, joka on totta pelipuussa $\mathcal{T}$, jos ja vain jos tämän juuri on joukossa $\bigcup_{n\in\mathbb{N}} V_n$.

24. Olkoon Σ äärellinen epätyhjä merkistö ja $f\colon \Sigma^* \to \{0,1\}^*$ injektio ja sanahomomorfismi, ts. kaikilla $w, w' \in \Sigma^*$ pätee $f(ww') = f(w)f(w')$. Olkoon edelleen $L \subset \Sigma^*$ polynomisessa ajassa tunnistettavissa oleva kieli. Näytä, että myös $f[L]$ on polynomisessa ajassa tunnistettavissa.

25. Olkoon $k \in \mathbb{N}$, $k \geq 2$, sekä olkoot $\mathcal{T}$ ja $\mathcal{T}'$ juurellisia puita, joissa jokaisella solmulla on korkeintaan k seuraajaa (erityisesti aste on korkeintaan $k+1$). Todista, että $\mathcal{T} \equiv \mathcal{T}'$ (FVL^k), jos ja vain jos $\mathcal{T} \cong \mathcal{T}'$.

V 0–1-lait

Satunnaisuus on äärellisten mallien kannalta monella tavalla tärkeätä. Deskriptiivisen vaativuusteorian näkökulmasta katsoen on oleellista, että syötemalleilla on tietty tilastollinen jakauma, ts. syöte on itse asiassa satunnaismalli. Vaativuusteoriassa onkin tarkasteltu pahimman tapauksen vaativuuden lisäksi keskimääräistä vaativuutta ja siihen liittyviä vaativuusluokkia. Todennäköisyyslaskennalliset ideat ovat levinneet muihinkin osiin laskennasta: algoritmeja on satunnaistettu, ja tulosteenkin saatetaan hyväksyä olevan virheellinen pienellä todennäköisyydellä.

Toisaalta satunnaisuudesta on kiinnostuttu myös puhtaasti teoreettisena konstruktiomenetelmänä. Joissakin tapauksissa haluttujen esimerkkimallien konstruoiminen perinteisellä tavalla käsin, osat yksitellen määrittäen, on hyvin työlästä, kun taas malli arpomalla voidaan päästä suoraan tulokseen. Tapaa rakentaa malli ainakin osittain satunnaisista osista kutsutaan *satunnaismenetelmäksi*. Parhaimmillaan menetelmässä yhdistellään deterministisyyttä ja satunnaisuutta hyvin epätriviaaleilla tavoilla.

Tässä lyhyessä osassa satunnaismallien rikkaaseen teoriaan tutustutaan vain hyvin ohuesti. Tarkastelun pelkistämiseksi satunnaismalleista tarkastellaan vain satunnaisverkkoja, mikä sinänsä ei ole kovin ihmeellinen rajoitus. Enemmän menetetään siinä, että satunnaisverkoista tarkastellaan vain sellaisia, joissa särmätodennäköisyys on verkon koosta riippumaton vakio. Tällaisille satunnaisverkoille todistetaan ensimmäisen kertaluvun 0–1-laki, joka on tärkeä ja jossain määrin yllättävä ilmiö, mutta sittenkin paljastaa vain jäävuoren huipun satunnaismallien teoriasta. 0–1-lailla tarkoitetaan, että asymptoottisesti melkein varmasti verkkojen kielen lause on satunnaisverkoissa totta tai asymptoottisesti melkein varmasti epätotta. Käsitteitä täsmennetään tarkastelun edetessä.

Kun A on joukko ja $k \in \mathbb{N}$, merkitään $[A]^k = \{\, B \subset A \mid |B| = k \,\}$.

Olkoon $n \in \mathbb{Z}_+$ ja $p \in [0,1]$. Epämuodollisesti $\mathbb{G}_{n,p}$ on satunnaisverkko, jonka perusjoukkona on kiinteä n solmun joukko, vaikkapa $\mathrm{Dom}(\mathbb{G}_{n,p}) = \{0,\ldots,n-1\}$, ja solmuparien välillä arvotaan toisistaan riippumatta, onko niiden välillä särmää (todennäköisyys p) vai ei (todennäköisyys $1-p$).

Muodollisemmin $\mathbb{G}_{n,p}$ on satunnaismuuttuja, jonka arvot $\mathbb{G}_{n,p}(\omega)$ ovat verkkoja. Jokaisella alkeistapauksella $\omega \in \Omega$ perusjoukko on sama $\mathrm{Dom}(\mathbb{G}_{n,p}(\omega)) = V = \{0,\ldots,n-1\}$. (Termiä satunnaismuuttuja käytetään tässä siis yleisemmin kuin todennäköisyyslaskennan peruskursseilla, joissa satunnaismuuttujat ovat aina reaalisia tai kompleksisia.) Muodostetaan ensin asiaan liittyvä todennäköisyyskenttä $(\Omega, \mathcal{P}(\Omega), \mathbb{P})$. Jokaista paria $e = \{a,b\} \in [V]^2$ kohti arvotaan, tuleeko solmujen a ja b välille särmä vai ei. Tätä arvontaa vastaa todennäköisyyskenttä $(\Omega_e, \mathcal{P}(\Omega_e), \mathbb{P}_e)$, missä $\Omega_e = \{0,1\}$ ja $\mathbb{P}_e\{1\} = p$. Lopullinen todennäköisyyskenttä $(\Omega, \mathcal{P}(\Omega), \mathbb{P})$ on tulokenttä, ts. $\Omega = \prod_{e\in[V]^2} \Omega_e$ ja $\mathbb{P}\{\omega\} = \prod_{e\in[V]^2} \mathbb{P}_e(\omega(e))$. Alkeistapaus $\omega \in \Omega$ on siis kuvaus $\omega\colon [V]^2 \to \{0,1\}$. Satunnaisverkko $\mathbb{G}_{n,p}$ on nyt satunnaismuuttuja, jolle

$$E^{\mathbb{G}_{n,p}(\omega)} = \{\, (a,b) \in V \times V \mid a \neq b,\ \omega(\{a,b\}) = 1 \,\}$$

ja kuten jo todettiin, $\mathrm{Dom}(\mathbb{G}_{n,p}(\omega)) = V = \{0,\ldots,n-1\}$.

Jatkossa tätä muodollista määritelmää ei tarvita, vaan ainoastaan seuraavia faktoja: Merkitään jokaisella $e = \{a, b\} \in [V]^2$

$$\begin{aligned} A_e &= \{(a,b) \in E^{\mathbb{G}_{n,p}}\} \qquad \text{(todennäköisyyslaskennan tapahtumamerkinnöin)} \\ &= \{\, \omega \in \Omega \mid (a,b) \in E^{\mathbb{G}_{n,p}(\omega)} \,\}. \end{aligned}$$

Tällöin tapahtumat A_e, $e \in [V]^2$, ovat keskenään riippumattomia ja $\mathbb{P}(A_e) = p$ jokaisella $e \in [V]^2$.

0–1-lain todistus voidaan jakaa kahteen osaan. Ensiksi pyritään kuvailemaan, millainen satunnaisverkko melkein varmasti on. Kuvailu onnistuu ns. laajennusaksioomilla. Toisessa vaiheessa lasketaan laajennusaksioomien todennäköisyyksiä.

1.1. Määritelmä. Olkoon $k, \ell, m \in \mathbb{N}$. Merkitään $\eta_{\ell,m}$:llä FO:n lausetta

$$\forall x_0 \ldots \forall x_{\ell-1} \forall y_0 \ldots \forall y_{m-1} \Bigg(\bigwedge_{i=0}^{\ell-1} \bigwedge_{j=0}^{m-1} x_i \neq y_j \rightarrow \exists z \Big(\bigwedge_{i=0}^{\ell-1} E(x_i, z) \wedge \bigwedge_{j=0}^{m-1} (y_j \neq z \wedge \neg E(y_j, z)) \Big) \Bigg).$$

Tällöin *k-laajennusaksioomaksi* kutsutaan lausetta

$$\eta_k = \bigwedge_{\ell=0}^{k} \eta_{\ell,k-\ell}.$$

Aksioomaa voi kutsuta myös $k+1$ *muuttujan laajennusaksioomaksi*, sillä paitsi, että $\eta_k \in \mathrm{FO}[\{E\}]$, myös $\eta_k \in \mathrm{FVL}^{k+1}[\{E\}]$.

Olkoon $\mathbb{G}$ verkko, jonka perusjoukko on $V = \mathrm{Dom}(\mathbb{G})$ ja jolle $\mathrm{card}(\mathbb{G}) > \ell + m$. Huomataan, että $\mathbb{G} \models \eta_{\ell,m}$, jos ja vain jos erillisiä $A \in [V]^\ell$ ja $B \in [V]^m$ aina vastaa $c \in V \setminus (A \cup B)$, joka on yhteydessä jokaiseen joukon A solmuun muttei yhteenkään B:n solmuun.

Todistetaan seuraavaksi, että laajennusaksiooma kuvailee verkon täydellisesti $k+1$ muuttujan suhteen.

1.2. Lemma. *Olkoot $k \in \mathbb{N}$ ja $\mathbb{G}$, $\mathbb{H}$ verkkoja, joille $\mathbb{G}, \mathbb{H} \models \eta_k$. Tällöin $\mathbb{G} \cong^{k+1} \mathbb{H}$.*

Todistus. Merkitään $I = \{\, p \in \mathrm{Part}(\mathbb{G}, \mathbb{H}) \mid |p| \leq k+1 \,\}$. Osoitetaan, että $I \colon \mathbb{G} \cong^{k+1} \mathbb{H}$. On selvää, että riittää tarkastaa edestakaisia laajennuksia koskeva ehto.

Olkoon $p \in I$, $|p| \leq k$ ja $d \in \mathrm{Dom}(\mathbb{H})$. Voidaan olettaa, että $d \notin \mathrm{rg}(p)$. Merkitään

$$A' = \{\, b \in \mathrm{rg}(p) \mid (b,d) \in E^{\mathbb{H}} \,\}$$

ja

$$B' = \{\, b \in \mathrm{rg}(p) \mid (b,d) \notin E^{\mathbb{H}} \,\}$$

sekä $A = p^{-1}[A']$ ja $B = p^{-1}[B']$. Tällöin A ja B ovat erillisiä sekä $A \cup B = \mathrm{dom}(p)$ ja siis $|A \cup B| \leq k$. Koska $\mathbb{G} \models \eta_k$, on olemassa $c \in \mathrm{Dom}(\mathbb{G})$, jolle $(a,c) \in E^{\mathbb{G}}$ ja $(b,c) \notin E^{\mathbb{G}}$, kun $a \in A$ ja $b \in B$. Nyt on selvää, että $q = p \cup \{(c,d)\}$ on osittainen isomorfismi, jolle $|q| \leq k+1$, joten $q \in I$ ja p laajenee taaksepäin joukkoon I. Vaihtamalla $\mathbb{G}$:n ja $\mathbb{H}$:n roolit saadaan, että p laajenee myös eteenpäin. Siis $I \colon \mathbb{G} \cong^{k+1} \mathbb{H}$. □

Seuraavaksi todistetaan, että laajennusaksioomien asymptoottinen todennäköisyys on yksi.

1.3. Lemma. *Kun $k \in \mathbb{N}$ ja $p \in]0,1[$, niin*

$$\lim_{n\to\infty} \mathbb{P}\{\mathbb{G}_{n,p} \models \eta_k\} = 1.$$

Todistus. Olkoot $\ell, m \in \mathbb{N}$, $\ell + m = k$. Merkitään $\xi(\boldsymbol{x}, \boldsymbol{y}, z)$:llä kaavaa

$$\bigwedge_{i=0}^{\ell-1} E(x_i, z) \wedge \bigwedge_{j=0}^{m-1} (y_j \neq z \wedge \neg E(y_j, z))$$

Olkoon $n \in \mathbb{N}$, $n > k$. Merkitään $V = \{0, \ldots, n-1\}$. Kun $\boldsymbol{a} \in V^\ell$, $\boldsymbol{b} \in V^m$ ja $c \in V$ ovat erillisiä ja toistottomia, niin

$$\mathbb{P}\{\mathbb{G}_{n,p} \models \xi[\boldsymbol{a}/\boldsymbol{x}, \boldsymbol{b}/\boldsymbol{y}, c/z]\} = p^\ell (1-p)^m$$

Eri arvoilla c nämä tapahtumat $\{\mathbb{G}_{n,p} \models \xi[\boldsymbol{a}/\boldsymbol{x}, \boldsymbol{b}/\boldsymbol{y}, c/z]\}$ ovat riippumattomia, joten

$$\mathbb{P}\{\mathbb{G}_{n,p} \not\models \exists z \xi[\boldsymbol{a}/\boldsymbol{x}, \boldsymbol{b}/\boldsymbol{y}]\} = (1 - p^\ell (1-p)^m)^{n-k}.$$

Kun $A \in [V]^\ell$ ja $B \in [V]^m$ ovat erillisiä, merkitään $E_{A,B}$:llä tapahtumaa $\{\mathbb{G}_{n,p} \not\models \exists z \xi[\boldsymbol{a}/\boldsymbol{x}, \boldsymbol{b}/\boldsymbol{y}]\}$, missä $A = \mathrm{rg}(\boldsymbol{a})$ ja $B = \mathrm{rg}(\boldsymbol{b})$. ($E_{A,B}$ ei tietenkään riipu jonojen $\boldsymbol{a}$ ja $\boldsymbol{b}$ valinnasta eli komponenttien järjestyksestä.) Tällöin siis $\mathbb{P}(E_{A,B}) = (1 - p^\ell (1-p)^m)^{n-k}$ ja

$$\begin{aligned}
\mathbb{P}\{\mathbb{G}_{n,p} \not\models \eta_{\ell,m}\} &= \mathbb{P}\Big(\bigcup_{\substack{A \in [V]^\ell,\, B \in [V]^m \\ A \cup B = \emptyset}} E_{A,B} \Big) \\
&\leq \sum_{\substack{A \in [V]^\ell,\, B \in [V]^m \\ A \cup B = \emptyset}} \mathbb{P}(E_{A,B}) = \binom{n}{\ell} \binom{n-\ell}{m} (1 - p^\ell (1-p)^m)^{n-k} \\
&= P(n) \cdot a^n,
\end{aligned}$$

missä $P(n) = \binom{n}{\ell}\binom{n-\ell}{m}(1 - p^\ell(1-p)^m)^{-k}$ on luvun n polynomi ja $a = 1 - p^\ell(1-p)^m \in]0,1[$, joten termi a^n on eksponentiaalisesti vähenevä. Siis

$$\lim_{n\to\infty} \mathbb{P}\{\mathbb{G}_{n,p} \not\models \eta_{\ell,m}\} = 0,$$

mistä seuraa

$$\lim_{n\to\infty} \mathbb{P}\{\mathbb{G}_{n,p} \not\models \eta_k\} = \lim_{n\to\infty} \mathbb{P}\Big(\bigcup_{\ell=0}^{k} \{\mathbb{G}_{n,p} \not\models \eta_{\ell,k-\ell}\} \Big) = 0.$$

Siis $\lim_{n\to\infty} \mathbb{P}\{\mathbb{G}_{n,p} \models \eta_k\} = 1$. □

1.4. Lause. *Olkoon* $\varphi \in \mathrm{FVL}[\{E\}]$. *Tällöin*

$$\lim_{n\to\infty} \mathbb{P}\{\mathbb{G}_{n,p} \models \varphi\} \in \{0, 1\}.$$

Todistus. Tarkastelu jakautuu hyvin luonnollisella tavalla kahteen osaan. Merkitään $k = |\mathrm{bv}(\varphi)|$.

1) On olemassa verkko $\mathbb{G}$, jolle $\mathbb{G} \models \eta_k \wedge \varphi$. Tällöin jokaisella verkolla $\mathbb{H} \models \eta_k$ pätee $\mathbb{H} \models \varphi$, sillä lemman 1.2 mukaan $\mathbb{G} \cong^{k+1} \mathbb{H}$ eli $\mathbb{G} \equiv \mathbb{H}\,(\mathrm{FVL}^{k+1})$ (pelikarakterisaation nojalla) ja $\varphi \in \mathrm{FVL}^{k+1}$. Siis $\{\mathbb{G}_{n,p} \models \eta_k\} \subset \{\mathbb{G}_{n,p} \models \varphi\}$, joten

$$\mathbb{P}\{\mathbb{G}_{n,p} \models \eta_k\} \leq \mathbb{P}(\{\mathbb{G}_{n,p} \models \varphi\}) \leq 1.$$

Lemmasta 1.3 seuraa nyt $\lim_{n\to\infty} \mathbb{P}(\{\mathbb{G}_{n,p} \models \varphi\}) = 1$.

2) Kaikille verkkoille $\mathbb{G} \models \eta_k$ pätee $\mathbb{G} \not\models \varphi$. Siis $\{\mathbb{G}_{n,p} \models \eta_k\} \cap \{\mathbb{G}_{n,p} \models \varphi\} = \emptyset$, joten

$$0 \leq \mathbb{P}\{\mathbb{G}_{n,p} \models \varphi\} \leq \mathbb{P}\{\mathbb{G}_{n,p} \not\models \eta_k\}$$

Lemmasta 1.3 seuraa tässä tapauksessa $\lim_{n\to\infty} \mathbb{P}\{\mathbb{G}_{n,p} \models \varphi\} = \lim_{n\to\infty} \mathbb{P}\{\mathbb{G}_{n,p} \not\models \eta_k\} = 0$. □

Harjoituksia osaan V

1. Määritä
a) $\lim_{n\to\infty} \mathbb{P}\{\mathbb{G}_{n,1/2} \text{ on yhtenäinen}\}$ ja
b) $\lim_{n\to\infty} \mathbb{P}\{\mathbb{G}_{n,1/2} \text{ on kaksiosainen}\}$.

2. Olkoon $k \in \mathbb{Z}_+$ ja K sisältäköön kaikki ne verkot, joihin uppoavat kaikki k solmun verkot. Osoita, että $\lim_{n\to\infty} \mathbb{P}\{\mathbb{G}_{n,1/2} \in K\} = 1$.

3. Olkoon $k \in \mathbb{Z}_+$. Todista, että ei ole ole FVL:n lausetta φ, jolle pätisi kaikilla verkoilla $\mathbb{G}$, että $\mathbb{G} \models \varphi$, jos ja vain jos $\mathbb{G} \models \eta_k$ ja $\mathbb{G}$:ssä on parillinen määrä särmiä.

4. Osoita, että on olemassa sellainen $c > 0$, että jokaisella $k \in \mathbb{Z}_+$ laajennusaksioomalla η_k on malli, jossa on enintään c^k alkiota.

5. Olkoon $\alpha > 0$ ja $k \in \mathbb{Z}_+$. Merkitään $c(n)$:llä klikkien lukumäärän odotusarvoa satunnaisverkossa $\mathbb{G}_{n,n^{-\alpha}}$, kun $n \in \mathbb{Z}_+$. Laske $\lim_{n\to\infty} c(n)$.

6. Olkoon U yksipaikkainen relaatiosymboli. Kun $n \in \mathbb{Z}_+$, merkitään K_n:llä niiden järjestettyjen $\{\leq, U\}$-mallien $\mathfrak{M}$ luokkaa, joille $\mathrm{Dom}(\mathfrak{M}) = \{0, \ldots, n-1\}$. Olkoon $\mathfrak{M}_n$ umpimähkään valittu luokan K_n malli. Merkitään T:llä ensimmäisen kertaluvun lauseiden $\mathrm{FO}[\{\leq, U\}]$ asymptoottisten todennäköisyyksien joukkoa, ts. $t \in T$, jos ja vain jos on olemassa sellainen $\varphi \in \mathrm{FO}[\{\leq, U\}]$, että

$$t = \lim_{n\to\infty} \mathbb{P}\{\mathfrak{M}_n \models \varphi\}.$$

Osoita, että T on tiheä joukossa $[0, 1]$.

Kirjallisuutta

[EF95] Heinz-Dieter Ebbinghaus and Jörg Flum. *Finite model theory.* Perspectives in Mathematical Logic. Springer-Verlag, Berlin, 1995.

[Hel97] Lauri Hella. Lectures on finite model theory. Kalvot, 1997. Saatavilla osoitteesta http://mathstat.helsinki.fi/logic/people/lauri.hella/Aix97.ps.

[Imm99] Neil Immerman. *Descriptive complexity.* Graduate Texts in Computer Science. Springer-Verlag, New York, 1999.

[Lib04] Leonid Libkin. *Elements of finite model theory.* Texts in Theoretical Computer Science. An EATCS Series. Springer-Verlag, Berlin, 2004.

[Vää94] Jouko Väänänen. A short course on finite model theory, 1994. Saatavilla osoitteesta http://mathstat.helsinki.fi/logic/people/jouko.vaananen/shortcourse.pdf.

Hakemisto