Teknillinen korkeakoulu
Informaatio- ja luonnontieteiden tiedekunta

Luovat joukot ja Myhillin isomorfialause

Mika Göös <mgoos@cc.hut.fi>
Ohjaajana prof. Pekka Orponen

Espoossa 26.4.2009

Tiivistelmä

Laskettavuusteoria (myös: *rekursioteoria*) tutkii mekaanisen laskennan ja äärellisten menetelmien ominaisuuksia. Kurt Gödelin ja Alan Turingin tulokset mekaanisten menetelmien rajoituksista antavat laskettavuusteorialle lähtökohdan:

Perustulos. *On olemassa äärellisesti esitettäviä matemaattisia ongelmia, joihin ei voida äärellisin menetelmin vastata.*

Tässä kandidaatintyössä esitellään riippumaton johdanto näihin laskettavuusteorian perusideoihin. Tässä työssä määritellään *osittaisrekursiivisten* funktioiden luokka, jonka avulla laskettavan funktion käsitteestä tehdään täsmällinen. Keskeinen osa laskettavuusteoriaa on laskennallisten päätösongelmien luokittelu ja vertailu: päätösongelmien vaikeus formalisoidaan laskettavien funktioiden avulla ja tästä syntyvien *rekursiivisten* ja *rekursiivisesti numeroituvien* päätösongelmien perusominaisuuksia tarkastellaan.

Laskettavuusteorian voidaan katsoa irtautuneen matemaattisen logiikan tutkimuksesta 1930-luvulla. Tämän työn yksi pääteema on katsoa matemaattisen logiikan käsitteitä, kuten *todistuvuutta* ja *määriteltävyyttä*, laskettavuusteorian tarjoamassa yleisessä viitekehyksessä. Laskettavuusteorian sovellusalana matemaattinen logiikka ohjaa tutkimusta mielekkäiden päätösongelmaluokkien tarkasteluun. Näin on erityisesti *produktiivisten* ja *luovien* joukkojen kohdalla, joiden ominaisuuksia tässä työssä tutkitaan.

Vuonna 1955 John Myhill todisti merkittävän tuloksen vaikeita rekursiivisesti numeroituvia päätösongelmia koskien. Tässä työssä määritellään ja johdetaan kaikki vaadittava teoria, jotta lopulta seuraava Myhillin tulos voidaan todistaa:

Myhillin isomorfialause. *Kaikki m-täydelliset päätösongelmat ovat rekursiivisesti isomorfisia.*

Sisältö

1 Johdanto

Luovat joukot ja Myhillin tulokset koskevat erityisesti rekursiivisesti numeroituvien joukkojen luokan rakennetta.

Tässä työssä pyritään esittämään mahdollisimman riippumaton johdanto näihin aiheisiin laskettavuusteorian perusteiden kautta. Esitiedoiksi on tarkoitettu riittävän Teknillisessä korkeakoulussa luennoitavat kurssit *Tietojenkäsittelyteorian perusteet* ja *Logiikka tietotekniikassa: perusteet*, vaikkakin laskettavuusteorian formalismi johdetaan esitietoja olettamatta luvussa 2.

Laskettavuusteoria tutkii laskennallisten päätösongelmien vaikeutta. Tätä vaikeusluokittelua aletaan hahmotella luvussa 3. Esitetty teoria pohjautuu matemaattisen logiikan tutkimukseen, jonka tuotoksia tarkastellaan soveltuvin osin neljännessä luvussa.

Luvussa 5 annetaan määritelmä luoville joukoille, jotka toimivat sekä teknisenä apuvälineenä että mielenkiintoisena käsitteenä todistettaessa työn päätavoitteita, Myhillin tuloksia, luvuissa 5 ja 6.

Muutamat teknisluontoiset ja tekstin tavoitteen kannalta epäoleelliset todistukset on jätetty liitteeksi.

2 Mekaaninen laskettavuus

Mekaanisesti laskettavan funktion (myös: *efektiivisen menetelmän* tai *algoritmin*) käsite muotoutui 1930-luvulla. Laskettavuuden pohdiskeluihin ajauduttiin matematiikan perusteiden tutkimuksen kautta. Törmättiin mm. seuraavanlaisiin kysymyksiin:

K1. Mitä voidaan matemaattisesti päätellä—edes periaatteessa?
K2. Ovatko logiikan teoriat täydellisiä, eli voidaanko niissä todistaa kaikki todet väittämät?
K3. Voidaanko annetusta predikaattilogiikan lauseesta mekaanisesti päättää onko lause pätevä?

Listan viimeinen ongelma tunnetaan David Hilbertin mukaan nimellä *Entscheidungsproblem*, päätösongelma. Kysymykseen negatiivisesti vastaaminen edellytti intuitiivisen ja epämuodollisen käsitteen "olla mekaanisesti pääteltävä" täsmällistä määrittelyä. Vuonna 1936 Alonso Church, Alan Turing, Stephen Kleene ja Emil Post julkaisivat omat ehdotuksensa laskettavuuden käsitteen formalisaatioista. Määritelmät osoitettiin myöhemmin yhtä vahvoiksi ja näin *osittaisrekursiivisten* tai *laskettavien*[1] funktioiden luokka oli löytynyt [5; 7]. Kurt Gödelin sanoin

> [Laskettavuuden] käsitteen kohdalla on ensimmäistä kertaa onnistuttu antamaan absoluuttinen, eli valitusta formalismista riippumaton, määritelmä kiinnostavalle epistemologiselle käsitteelle. [5, Gödel 1946]

Seuraavassa kerrataan aluksi peruskäsitteistöä ja siirrytään sen jälkeen tutkimaan osittaisrekursiivisten funktioiden ominaisuuksia. Materiaali on suureksi osaksi jo tuttua *Tietojenkäsittelyteorian perusteet* -kurssilta [12], joskin notaatio on tässä lähempänä alkuperäisen kirjallisuuden käytäntöjä.

[1] Robert Soare on esittänyt [16], että historiallisen, mutta nykypäivänä ylikuormitetun, termin "rekursiivinen" sijasta puhuttaisiin "laskettavuudesta".

2.1 Peruskäsitteet ja notaatio

Samastetaan tässä funktiot niiden kuvaajiin, eli relaatio $f \subseteq X \times Y$ on *funktio* (tai *kuvaus*) lähtöjoukolta X maalijoukolle Y, merkitään $f : X \to Y$, jos jokaista $x \in X$ kohden löytyy korkeintaan yksi $y \in Y$, jolle $(x, y) \in f$. Tämä yksikäsitteinen arvo y on funktion arvo pisteessä x ja merkitään $f(x) = y$. Funktion määrittelyjoukko (engl. domain) on $\mathrm{Dom}\, f = \{x \in X \mid (x, y) \in f, \text{ jollakin } y \in Y\}$. Joukon $A \subseteq X$ kuvajoukko (engl. image) kuvauksessa f on $f(A) = \{f(a) \in Y \mid a \in A\}$. Funktion arvojoukko tai funktion kuva saadaan kuvaamalla koko lähtöjoukko: $\mathrm{Im}\, f = f(X)$. Joukon $A \subseteq Y$ alkukuva on $f^{-1}(A) = \{x \in X \mid (x, a) \in f, \text{ jollakin } a \in A\}$. Määritellään lisäksi funktioista $f : X \to Y$ ja $g : Y \to Z$ yhdistämällä saatu funktio $g \circ f : X \to Z$ s.e. $(g \circ f)(x) = g(f(x))$.

Funktio $f : X \to Y$ on *totaali*, jos $\mathrm{Dom}\, f = X$. Perinteisessä matematiikassa funktiot määritellään yleensä totaaleiksi, mutta laskettavuusteoriassa osoittautuu käteväksi tarkastella myös *osittaiskuvauksia* $\varphi : \mathbb{N}^n \to \mathbb{N}$, joita ei ole määritelty kaikilla $\vec{x} = (x_1, \ldots, x_n) \in \mathbb{N}^n$ ja joiden määrittelyjoukkoa ei eksplisiittisesti ilmoiteta. Jos funktiota ei ole määritelty jollakin $\vec{x} \in \mathbb{N}^n$, sanotaan, että funktion laskenta ei pysähdy tai että funktion laskenta hajaantuu tässä pisteessä ja merkitään $\varphi(\vec{x})\uparrow$. Jos taas $\varphi(\vec{x})$ on määritelty, sanotaan laskennan pysähtyvän tai suppenevan, jolloin merkitään $\varphi(\vec{x})\downarrow$. Tässä työssä käytetään pääasiassa kreikkalaisia kirjaimia $(\varphi, \psi, \tau, \ldots)$, kun on kyse osittaisista funktioista, ja latinalaisia $(f, g, h, \ldots)$, kun on kyse aidosti totaaleista funktioista.

Olkoot $\varphi, \psi : \mathbb{N}^n \to \mathbb{N}$ osittaiskuvauksia. Merkitään $\varphi(\vec{x}) \simeq \psi(\vec{x})$, jos φ ja ψ ovat molemmat määrittelemättömiä pisteessä $\vec{x} \in \mathbb{N}^n$ tai jos $\varphi(\vec{x})$ ja $\psi(\vec{x})$ ovat määriteltyjä ja $\varphi(\vec{x}) = \psi(\vec{x})$.

Määritelmä 1. *Totaali funktio $f : X \to Y$ on*

1. surjektio, *jos* $\mathrm{Im}\, f = Y$
2. injektio, *jos kaikilla* $a, b \in X$, $a \neq b \Longrightarrow f(a) \neq f(b)$
3. bijektio, *jos se on sekä surjektio että injektio*

Huomautus 1. Injektiivisen funktion käänteiskuvaus, $f^{-1} = \{(y, x) \mid (x, y) \in f\}$, on hyvin määritelty osittaisfunktio, koska jokaisella $y \in \mathrm{Im}\, f$ on yksikäsitteinen alkukuva.

2.2 Osittaisrekursiivisten funktioiden luokka

Seuraavassa on listattuna tärkeimmät formalisaatiot, joita on esitetty karakterisoimaan laskettavien funktioiden luokkaa [4, luku 3]:

M1. Herbrand-Gödel (1936), yhtälöryhmillä määritellyt funktiot.
M2. Church (1936), λ-kalkyyli.
M3. Gödel-Kleene (1936), μ-rekursiiviset funktiot.
M4. Turing (1936), Turingin koneet.
M5. Post (1943) ja Markov (1951), merkkijonomuunnosjärjestelmät.
M6. Shepherdson-Sturgis (1963), rekisterikoneet.

Kaikki yllä mainitut ovat yhtä vahvoja määritelminä ja erityisesti yhtä vahvoja kuin modernit ohjelmointikielet. Niiden kuvaamat funktiot voidaan siis ainakin periaatteessa laskea mekaanisesti. Churchin-Turingin teesinä tunnetaan käänteinen väite: kaikki intuitiivisesti laskettavat funktiot ovat laskettavia kaikissa näissä formalismeissa.

Ehkä historiallisesti tärkein ja kirjallisuudessa eniten vastaantuleva formalisaatio on Turingin laskentakoneet (M4). Niiden yksinkertaisuus ja mekaaninen luonne suostutteli aikoinaan tutkijat hyväksymään Churchin-Turingin teesin [7]. Esitetään tässä

kuitenkin Kleenen μ-rekursiivisten funktioiden määritelmä [4; 11; 17], koska se sisältää suoraan monia keinoja, joita jatkossa käytetään konstruoimaan erilaisia funktioita.

Olkoon $\ldots x \ldots$ jokin luonnollisia lukuja koskeva väite, jossa x toimii vapaana muuttujana. Merkitään lausekkeella $\mu x(\ldots x \ldots)$ pienintä lukua, jolle tämä väite pätee. Jos väite ei päde yhdellekään luonnolliselle luvulle, lauseke on määrittelemätön. Tämä on ns. *Kleenen μ-operaattori* tai *rajoittamaton minimalisaatio.*

Määritelmä 2. Osittaisrekursiivisten *(tai* laskettavien*) funktioiden luokka määritellään seuraavasti.* [11, ss. 127–128]

R1. 1. *Nollafunktio* $Z(x) = 0$ *on* osittaisrekursiivinen.
2. *Seuraajafunktio* $S(x) = x + 1$ *on* osittaisrekursiivinen.
3. *Projektiofunktiot* $Pr^m_n : \mathbb{N}^m \to \mathbb{N}$, $1 \le n \le m$ *s.e.* $Pr^m_n(x_1, \ldots, x_m) = x_n$, *ovat* osittaisrekursiivisia.

R2. Jos $\psi : \mathbb{N}^m \to \mathbb{N}$ *ja* $\tau_i : \mathbb{N}^n \to \mathbb{N}$, $0 \le i \le m$, *ovat osittaisrekursiivisia, yhdistämällä saatu funktio* $\varphi : \mathbb{N}^n \to \mathbb{N}$ *s.e.*

$$\varphi(\vec{x}) \;\simeq\; \psi(\tau_1(\vec{x}), \ldots, \tau_m(\vec{x}))$$

on osittaisrekursiivinen.

R3. Jos funktiot $\psi : \mathbb{N}^n \to \mathbb{N}$ *ja* $\tau : \mathbb{N}^{n+2} \to \mathbb{N}$ *ovat osittaisrekursiivisia, yhden muuttujan suhteen rekursiolla saatu funktio* $\varphi : \mathbb{N}^{n+1} \to \mathbb{N}$ *s.e.*

$$\begin{cases} \varphi(0, \vec{x}) \;\simeq\; \psi(\vec{x}) \\ \varphi(y+1, \vec{x}) \;\simeq\; \tau(y, \varphi(y, \vec{x}), \vec{x}) \end{cases}$$

on osittaisrekursiivinen.

R4. Jos funktio $\psi : \mathbb{N}^{n+1} \to \mathbb{N}$ *on osittaisrekursiivinen, minimalisaatiolla saatu funktio* $\varphi : \mathbb{N}^n \to \mathbb{N}$ *s.e.*

$$\varphi(\vec{x}) \;\simeq\; \mu y(\;\; \forall z \le y : \psi(z, \vec{x}){\downarrow} \;\;\wedge\;\; \psi(y, \vec{x}) = 0 \;\;)$$

on osittaisrekursiivinen.

Totaalia osittaisrekursiivista funktiota kutsutaan lyhyesti vain rekursiiviseksi funktioksi.

Esimerkki 1. Yhteenlasku on rekursiivista. Määritellään $a(x, y) = x + y$ yhdistämällä funktioita ja säännöllä *R3*:

$$\begin{cases} a(0, y) = y = Pr^1_1(y) \\ a(x+1, y) = (x+y) + 1 = S(x+y) = S(a(x, y)) = S(Pr^3_2(x, a(x, y), y)) \end{cases}$$

Määritelmä 2 on sisällytetty täydellisyyden vuoksi; koko teoriaa ei tässä voida kehittää täysin formaalisti ja jatkossa tukeudutaankin intuitiivisiin argumentteihin, eli kuvataan funktion laskenta epämuodollisesti ja vedotaan Churchin-Turingin teesiin.

Muutamia huomautuksia määritelmästä:

H1. *R3* mahdollistaa funktioiden määrittelyn induktiivisesti: laskettaessa arvoa $\varphi(n)$, saadaan käyttää aiempia arvoja $\varphi(i)$, $0 \le i < n$, hyväksi.

H2. Kohdat *R1–R3* yhdessä määrittelevät osittaisrekursiivisia funktioita suppeamman funktioluokan, *primitiivirekursiiviset* funktiot.[2] Nämä ovat aina totaaleja funktioita.

[2] Ackermannin funktio [4, s. 46], joka on määritelty rekursiolla kahden muuttujan suhteen, on esimerkki rekursiivisesta funktiosta, joka ei ole primitiivirekursiivinen.

H3. μ-operaattori $(R4)$ voi tuottaa aidosti osittain määriteltyjä kuvauksia, vaikka lähtökohtana oleva kuvaus ψ olisi totaali. Jos pienin yhtälön

$$\psi(y, \vec{x}) = 0$$

toteuttava $y \in \mathbb{N}$ on olemassa, se löytyy, kun mekaanisesti tarkastetaan luvut järjestyksessä $0, 1, 2, 3, \ldots$. Toisaalta jos yhtälöä ei toteuta mikään $y \in \mathbb{N}$, tätä tosiasiaa ei voida yleisesti selvittää, kuten tullaan huomaamaan kohdassa 2.6.

2.3 Gödel-numerointi ja koodaukset

Luonnollisten lukujen joukko $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ ja sen osajoukot ovat ensisijaisen tarkastelun kohteena tässä tutkielmassa. Luonnollisten lukujen voidaan ajatella koodaavan asiayhteydestä riippuen mitä tahansa äärellisesti esitettäviä olioita, kuten merkkijonoja, osittaisrekursiivisten funktioiden esityksiä tai vaikka predikaattilogiikan kaavoja. Luonnollisia lukuja käsittelevä teoria on siis täysin yleinen, kunhan sopivasta koodauksesta on sovittu.

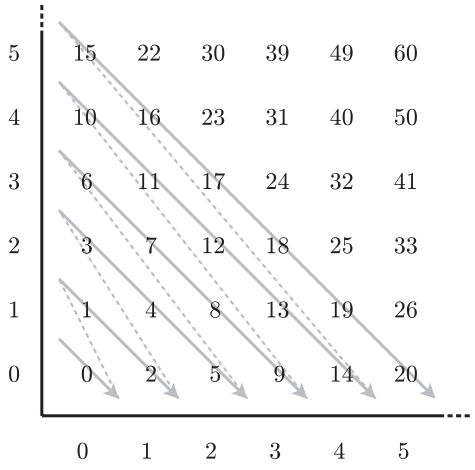
Parifunktio ja jonojen koodaus. Jo Georg Cantorilta peräisin oleva tulos koskee joukon $\mathbb{N} \times \mathbb{N}$ mahtavuutta.

Lause 1. $\mathbb{N}^2$ *on numeroituva, eli on olemassa bijektio* $\pi : \mathbb{N}^2 \to \mathbb{N}$.

Todistus. Määritellään parifunktio $\pi : \mathbb{N}^2 \to \mathbb{N}$ s.e.

$$\pi(x, y) = \frac{1}{2}(x + y)(x + y + 1) + x \tag{1}$$

Funktio π on bijektio. (Tarkempi todistus liitteenä.) □



Kuva 1. Parifunktio π numeroi $\mathbb{N} \times \mathbb{N}$ -tason.

Parifunktion π toimintaa on havainnollistettu kuvassa 1. Tietojenkäsittelyteoriassa parifunktiota käyttäville menetelmille on vakiintunut englannin kielessä termi *dovetailing*. Funktion π käänteisfunktiot ovat $\pi_1, \pi_2 : \mathbb{N} \to \mathbb{N}^2$, joille pätee $\pi(\pi_1(n), \pi_2(n)) =$

n, kaikilla $n \in \mathbb{N}$. Polynomimuotoisena π on rekursiivinen ja niin ovat myös sen käänteisfunktiot:

$$\pi_1(n) = \mu x(\exists y \le n : \pi(x,y) = n), \qquad \pi_2(n) = \mu y(\exists x \le n : \pi(x,y) = n) \ . \tag{2}$$

Tässä siis predikaatti "$\exists y \le n : \pi(x,y) = n$" voidaan pukea määritelmän vaatimaan muotoon "$f(x,n) = 0$", missä f on totaali rekursiivinen funktio, koska jokaista $x \in \mathbb{N}$ kohti riittää tarkastaa vain äärellinen määrä $y \in \{0,\ldots,n\}$ arvoja.

Tämän lisäksi huomataan, että yhdistämällä parifunktiota itsensä kanssa saadaan bijektio

$$\pi^k = \pi(\cdots\pi(\pi(x_1,x_2),x_3)\cdots,x_k) : \mathbb{N}^k \to \mathbb{N}$$

mille tahansa $k \in \mathbb{N}$. Edelleen kaikkien äärellisten jonojen joukko $\bigcup_{i\in\mathbb{N}} \mathbb{N}^i$ voidaan numeroida kuvauksella $\pi^* : \bigcup_{i\in\mathbb{N}} \mathbb{N}^i \to \mathbb{N}$ seuraavasti [13, s. 71]

$$\pi^*(\varnothing) = 0 \qquad (\text{kun } k = 0) \tag{3}$$

$$\pi^*((x_1,\ldots,x_k)) = \pi(\pi^k(x,\ldots,x_k), k-1) + 1 \tag{4}$$

Merkitään jatkossa lyhyesti $\langle x_1,\ldots,x_n\rangle = \pi^n(x_1,\ldots,x_n)$.

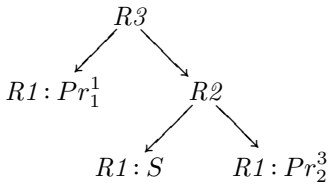
Nyt jos $\mathcal{L} = \{\alpha_1,\ldots,\alpha_n\}$ on jokin äärellinen (tai jopa numeroituvasti ääretön) aakkosto, voidaan jokaiseen merkkijonoon $\omega \in \mathcal{L}^* = \{\alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_m} \mid 1 \le i_j \le n\}$ liittää kääntäen yksikäsitteinen koodi

$$\lceil\omega\rceil = \pi^*(i_1,i_2,\ldots,i_m) \in \mathbb{N} \ . \tag{5}$$

Jos $\mathcal{L}$ koostuu esimerkiksi predikaattilogiikassa käytetyistä symboleista, voidaan formaaleihin kaavoihin viitata niiden koodilukujen eli *indeksien* eli *Gödel-lukujen* avulla. Kurt Gödel käytti vuonna 1931 tällaisia koodausmenetelmiä todistaessaan kuuluisia epätäydellisyystuloksiaan, joita käsitellään lisää luvussa 4.

Osittaisrekursiivisten funktioiden Gödel-numerointi. Jatkon kannalta erittäin tärkeä koodaus on edellä määriteltyjen osittaisrekursiivisten funktioiden standardinumerointi.

Osittaisrekursiiviset funktiot ovat äärellisiä olioita, sillä jokainen näistä funktioista saadaan koostettua äärellisellä määrällä sääntöjen *R1-R4* sovelluksia. Esimerkin 1 funktion $a(x,y)$ rakenne voidaan esittää puuna



(6)

Tämä voidaan koodata luvuksi

$$k \ = \ \Big\langle R3, \big\langle \langle R1, Pr_1^1\rangle, \langle R2, \pi^*(\langle R1, S\rangle, \langle R1, Pr_2^3\rangle)\rangle\big\rangle\Big\rangle \ \in \mathbb{N},$$

missä lähtöfunktioille (Z, S, Pr_n^m) ja säännöille $(R1\text{–}R4)$ voidaan käyttää vaikkapa koodeja $Z \to 0$, $S \to 1$, $Pr_n^m \to 2 + \langle m,n\rangle$ ja $Ri \to i$. Sanotaan, että k on funktion a indeksi, Gödel-luku tai ohjelma. Samalla tavalla voidaan koodata minkä tahansa osittaisrekursiivisen funktion rakennepuu, joten seuraava määritelmä on mielekäs.

Määritelmä 3. *Olkoon $n, m \in \mathbb{N}$. Merkitään $\varphi_n^{(m)}$:llä sitä osittaisrekursiivista funktiota $f : \mathbb{N}^m \to \mathbb{N}$, jonka indeksi on n. Jos n määrittelee laittoman rakennepuun tai funktion, jonka parametrien lukumäärä poikkeaa m:stä, olkoon $\varphi_n^{(m)} = \varnothing$.*

Merkitään lyhyemmin $\varphi_n = \varphi_n^{(1)}$. Numeroituva jono funktioita

$$\varphi_0, \ \varphi_1, \ \varphi_2, \ \varphi_3, \ \ldots$$

sisältää siis kaikki yhden muuttujan osittaisrekursiiviset funktiot. Tässä listauksessa jokainen funktio esiintyy äärettömän monta kertaa, sillä jokainen funktio voidaan määritellä äärettömän monella erilaisella rakennepuulla: Olkoon $\varphi : \mathbb{N}^n \to \mathbb{N}$ osittaisrekursiivinen. Nyt jono

$$\varphi(\vec{x}), \quad Pr_1^1(\varphi(\vec{x})), \quad Pr_1^1(Pr_1^1(\varphi(\vec{x}))), \quad Pr_1^1(Pr_1^1(Pr_1^1(\varphi(\vec{x})))), \quad \ldots,$$

antaa äärettömän monta esitystä samalle funktiolle. Sama muodollisesti: Kun n on funktion indeksi, kuvaus $n \mapsto \langle R2, \pi^*(\langle R1, Pr_1^1\rangle, n)\rangle = \langle 2, \pi^*(\langle 1, 2 + \langle 1, 1\rangle\rangle, n)\rangle$ on laskettava ja voidaankin määritellä rekursiolla

$$t'(n, z) = \begin{cases} n, & \text{jos } z = 0 \\ \langle 2, \pi^*(\langle 1, 2 + \langle 1, 1\rangle\rangle, t'(n, z-1))\rangle, & \text{jos } z \geq 1 \end{cases}. \tag{7}$$

Pienin muutoksin funktiosta t' saadaan injektiivinen myös ensimmäisen parametrinsa suhteen.

Lause 2. *Jokaiselle osittaisrekursiiviselle funktiolle $\varphi_n^{(m)}$ löytyy ääretön määrä indeksejä,*

$$\varphi_n^{(m)} = \varphi_{t(n,0)}^{(m)} = \varphi_{t(n,1)}^{(m)} = \varphi_{t(n,2)}^{(m)} = \varphi_{t(n,3)}^{(m)} = \cdots,$$

missä $t : \mathbb{N}^2 \to \mathbb{N}$ on rekursiivinen injektio.

Todistus. Liitteenä. □

Cantorin diagonaaliargumentilla saadaan välittömästi funktio, joka ei ole osittaisrekursiivinen:

$$d(x) = \begin{cases} \varphi_x(x) + 1, & \text{jos } \varphi_x(x)\downarrow \\ 0, & \text{jos } \varphi_x(x)\uparrow \end{cases} \tag{8}$$

Funktio d eroaa jokaisesta osittaisrekursiivisesta funktiosta φ_i kohdassa i: $\varphi_i(i) \neq d(i)$. Jos d-funktiota yritetään mekaanisesti lähteä laskemaan, kohdataan ongelma: Mikäli funktion φ_x laskenta ei pysähdy syötteellä x, eli $\varphi_x(x)\uparrow$, kuinka tämä tosiasia saataisiin selville, jotta funktion arvona voitaisiin tulostaa turvallisesti "0"? Tähän ns. *pysähtymisongelmaan* palataan kohdassa 2.6.

Tässä kuvattu indeksointi on vain yksi mahdollinen Gödel-numerointi osittaisrekursiivisille funktioille. Laskettavuusteorian kannalta numeroinnin teknisillä yksityiskohdilla ei ole väliä, kunhan koodaus on sellainen, jolle seuraavaksi käsitellyt lauseet ovat voimassa.

2.4 Efektiiviset operaatiot indekseillä

Osittaisrekursiivisen funktion Gödel-lukua voidaan ajatella sen ohjelmakoodina: Annettu indeksi n voidaan purkaa efektiivisesti, jolloin saadaan selville alkuperäinen rakennepuu ja ohjeistus siitä, miten funktion arvoja lasketaan. Laskenta etenee aina diskreeteissä askelissa; tässä tulkinta Turingin koneiden avulla on hyödyllinen.

Työlään ohjelmointiharjoituksen tuloksena saadaan Alan Turingin keskeinen tulos.

Lause 3 (Universaalikone [5, Turing 1936]**).** *Funktio* $U(x,y) \simeq \varphi_x(y)$ *on osittaisrekursiivinen.*

Todistus. Sivuutetaan. Ks. [11, ss. 90–96].

Sanotaan, että U on universaali funktio yksiparametrisille osittaisrekursiivisille funktioille. Tämä "ohjelmistoteollisuuden olemassaololause" [1] kertoo, ettei jokaista laskettavaa funktiota varten tarvitse rakentaa omaa fyysistä laskentakonetta, sillä U toimii virtuaalikoneena ja osaa simuloida mitä tahansa sille parametrina annettua ohjelmaa x syötteellä y.

Toinen osittaisrekursiivisten funktioiden Gödel-lukuihin liittyvä työkalu koskee funktion argumenttien upottamista funktion ohjelmakoodiin. Jos $f : \mathbb{N}^{m+n} \to \mathbb{N}$ on osittaisrekursiivinen ja $\varphi_z^{(m+n)} = f$, muunnoksessa[3]

$$\begin{array}{ccc} f(x_1,\ldots,x_m,y_1,\ldots,y_n) & \simeq & \varphi_z^{(m+n)}(x_1,\ldots,x_m,y_1,\ldots,y_n) \\ \downarrow & & \downarrow \\ f(\underbrace{S\cdots S}_{x_1 \text{ kpl}}(0),\ldots,\underbrace{S\cdots S}_{x_m \text{ kpl}}(0),\ y_1,\ldots,y_n) & \simeq & \varphi_{z'}^{(n)}(y_1,\ldots,y_n) \end{array} \tag{9}$$

alkuperäisen $(m+n)$ muuttujan funktion ohjelmakoodissa korvataan osa parametreistä vakiofunktioilla. Funktion f indeksin muutos $z \mapsto z'$ voidaan laskea efektiivisesti muuttujien $x_1,\ldots,x_m$ funktiona.

Lause 4 (Kleenen s**-**m**-**n**-lause** [13, s. 23]**).** *Kaikille* $m,n \geq 1$ *on olemassa injektiivinen rekursiivinen funktio* $s_n^m : \mathbb{N}^{m+1} \to \mathbb{N}$ *s.e. kaikille* $z,x_1,\ldots,x_m,y_1,\ldots,y_n$ *pätee*

$$\varphi^{(n)}_{s_n^m(z,x_1,\ldots,x_m)}(y_1,\ldots,y_n) \quad \simeq \quad \varphi_z^{(m+n)}(x_1,\ldots,x_m,y_1,\ldots,y_m) \tag{10}$$

Todistus. Liitteenä.

Yleisemmissä yhteyksissä osittaisrekursiivisten funktioiden Gödel-numerointi voidaan määritellä kääntäen: se on rekursiivisten funktioiden numerointi, jolle pätee lauseet 3 ja 4. Näistä lähtökohdista myös lause 2 on todistettavissa. [14, luku 4.2]

2.5 Ratkeavat ja puoliratkeavat ongelmat

Minkälaisiin kysymyksiin voidaan mekaanisesti päättelemällä vastata? Laskettavuusteoriassa tarkastellaan yksinkertaisesti päätösongelmia A, joiden instansseihin "$a \in A$?" tavoitellaan "kyllä"/"ei" vastauksia. Jos $P(x)$ on jokin luonnollisia lukuja $x \in \mathbb{N}$ koskeva väite tai ominaisuus, joukko

$$A = \{x \in \mathbb{N} \mid P(x)\}$$

määrittelee päätösongelman: Annettuna on $x \in \mathbb{N}$, onko "$x \in A$"?

Päätösongelma ratkeaa, jos pystytään konstruoimaan algoritmi, joka ratkaisee kysymyksen tyhjentävästi kaikilla syötteillä.

Määritelmä 4. *Joukko* $A \subseteq \mathbb{N}$ *on* rekursiivinen *tai* ratkeava *jos sen karakteristinen funktio*

$$\chi_A(x) = \begin{cases} 1, & \textit{jos } x \in A \\ 0, & \textit{jos } x \notin A \end{cases} \tag{11}$$

on rekursiivinen.

[3] Täsmällisemmin tässä pitäisi kirjoittaa "0" muodossa "$Z(Pr_1^n(y_1,\ldots,y_n))$" ja "$y_i$" muodossa "$Pr_i^n(y_1,\ldots,y_n)$", jotta noudatettaisiin määritelmää 2.

Selvästi A on rekursiivinen täsmälleen silloin, kun sen komplementti $\bar{A} = \mathbb{N} \setminus A$ on.

Koska luonnollisten lukujen osajoukkoja on ylinumeroituva määrä, ei jokaista niistä voida rekursiivisesti ratkaista. Laskettavuusteorian tavoitteisiin kuuluu kuitenkin löytää mahdollisimman *luonnollisia* esimerkkejä tällaisista ongelmista—sellaisia, joiden ratkeamattomuudella on jopa käytännön seurauksia.

Rekursiivisten joukkojen lisäksi määritellään myös näennäisesti (ja myöhemmin todistettavasti) laajempi joukkojen luokka.

Määritelmä 5. *Joukko $A \subseteq \mathbb{N}$ on* rekursiivisesti numeroituva *(r.n.), jos $A = \varnothing$ tai $A = \operatorname{Im} f$, jollekin totaalille rekursiiviselle funktiolle $f : \mathbb{N} \to \mathbb{N}$.*

Sanotaan myös, että n:n muuttujan predikaatti $P(x_1, \ldots, x_n)$ on *rekursiivinen* (*rekursiivisesti numeroituva*), jos

$$P = \{\langle x_1, \ldots, x_n \rangle \in \mathbb{N} \mid P(x_1, \ldots, x_n)\}$$

on rekursiivinen (rekursiivisesti numeroituva) eli samastetaan luontevasti n:n muuttujan predikaatit luonnollisten lukujen osajoukkoihin.

Tässä siis joukko A on r.n., jos sen alkioita voidaan luetella mekaanisesti kuinka pitkälle tahansa:

$$f(0),\ f(1),\ f(2),\ f(3),\ f(4),\ \ldots$$

Jos $x \in A$, tulostuu x tässä listauksessa lopulta jossakin kohdassa $n \in \mathbb{N}$, eli $x = f(n)$. Sanotaan, että rekursiivisesti numeroituvat joukot ovat *puoliratkeavia*, sillä ongelman "kyllä"-instanssien kohdalla voidaan aina vastata myöntävästi pelkästään listaamalla tarpeeksi joukon alkioita.

Nähdään heti, että kaikki rekursiiviset joukot A ovat myös rekursiivisesti numeroituvia: tapaus $A = \varnothing$ on selvä, joten otetaan $a \in A \neq \varnothing$ ja määritellään

$$f(x) = \begin{cases} x, & \text{jos } \chi_A(x) = 1 \\ a, & \text{jos } \chi_A(x) = 0 \end{cases} \tag{12}$$

joka on rekursiivinen, koska χ_A on, ja pätee $A = \operatorname{Im} f$.

Kerätään muitakin havaintoja.

Lemma 1. *Seuraavat ovat yhtäpitäviä.*

1. *A on rekursiivisesti numeroituva.*
2. *$A = \operatorname{Dom} \psi$, jollekin osittaisrekursiiviselle $\psi : \mathbb{N} \to \mathbb{N}$.*
3. *A:n puolikarakteristinen funktio*[4]

$$\widetilde{\chi_A}(x) = \begin{cases} 1, & \textit{jos } x \in A \\ \nearrow, & \textit{jos } x \notin A \end{cases}$$

   on osittaisrekursiivinen.
4. *On olemassa rekursiivinen predikaatti $P(x, y)$ s.e. $x \in A \iff \exists y : P(x, y)$.*

Todistus. (1) $\Rightarrow$ (2): Jos $A = \varnothing$, valitaan ikuiseen silmukkaan jäävä laskenta, $\psi(x) \simeq \mu z(1 = 0)$. Oletetaan siis $A = \operatorname{Im} f$. Määritellään $\psi(x) \simeq \mu z(f(z) = x)$. Selvästi $\psi(x)$ olemassa täsmälleen silloin, kun $x \in A$, joten $A = \operatorname{Dom} \psi$.

[4] Kirjoitetaan "$\nearrow$" kun funktion arvoa ei määritellä, eli laskennan annetaan hajaantua.

(2) $\Rightarrow$ *(3)*: Olkoon $A = \mathrm{Dom}\ \psi$. Puolikarakteristinen funktio saadaan ψ:n avulla:

$$\widetilde{\chi_A}(x) = \begin{cases} 1, & \text{jos } \psi(x)\downarrow \\ \nearrow, & \text{muulloin} \end{cases} \tag{13}$$

$\widetilde{\chi_A}$:n arvoja lasketaan ensin simuloimalla ψ:n laskentaa. Jos ψ pysähtyy, palautetaan 1. Jos $\psi(x)\uparrow$, tällöin myös $\widetilde{\chi_A}(x)$ on määrittelemätön. Churchin-Turingin teesin nojalla $\widetilde{\chi_A}$ on laskettava.

(3) $\Rightarrow$ *(4)*: Olkoon $\widetilde{\chi_A} = \varphi_x$ annettu. Tarkastellaan predikaattia T s.e.

$$T(x, y, z) \iff$$

"Funktion φ_x laskenta pysähtyy syötteellä y z:n askeleen jälkeen".

Tämä on *Kleenen T-predikaatti*[5] ja se on ratkeava: annettua ohjelmaa x simuloidaan äärellisen monta askelta, z, ja tarkastetaan, valmistuuko laskenta tähän mennessä. T:n avulla voidaan määritellä

$$P(x, y) \iff T(x, \pi_1(y), \pi_2(y)) \ , \tag{14}$$

missä π_1, π_2 ovat parifunktion käänteisfunktiot (2). Selvästi P on ratkeava, kun T on. Jos $z \in A$, niin $\varphi_x(z)\downarrow$ äärellisen askelmäärän, w, jälkeen. Siis $T(x, z, w)$ ja edelleen $P(x, \pi(z, w))$, joten $\exists y : P(x, y)$. Sama pätee kääntäen, joten väite seuraa.

(4) $\Rightarrow$ *(1)*: Jos $P(x, y)$ ei päde millään $x, y \in \mathbb{N}$, on $A = \varnothing$, joten oletetaan $a \in A \neq \varnothing$. Määritellään yhtälön 12 tapaan rekursiivinen f seuraavasti

$$f(x) = \begin{cases} \pi_1(x), & \text{jos } P(\pi_1(x), \pi_2(x)) \\ a, & \text{muulloin} \end{cases} \tag{15}$$

Funktion f laskenta pysähtyy jokaisella syötteellä, koska P oli ratkeava, siis f on totaali. Selvästi $A = \mathrm{Im}\ f$.

□

Jos rekursiivisesti numeroituvalle joukolle on olemassa myös tapa luetella joukon komplementin alkioita, eli joukon määräämän päätösongelman "ei"-instansseja, seuraava luonnehdinta on hyödyllinen.

Lause 5. *A on rekursiivinen jos ja vain jos A ja $\bar{A}$ ovat rekursiivisesti numeroituvia.*

Todistus. "$\Rightarrow$" Käsitelty. "$\Leftarrow$" Jos $A = \varnothing$ tai $\bar{A} = \varnothing$, väite on selvä, joten oletetaan $A \neq \varnothing \neq \bar{A}$ ja $f, g : \mathbb{N} \to \mathbb{N}$ s.e. $\mathrm{Im}\ f = A$ ja $\mathrm{Im}\ g = \bar{A}$. Koska kaikille $x \in \mathbb{N}$ joko $x \in A$ tai $x \in \bar{A}$, pätee $f(y) = x$ tai $g(y) = x$ jollekin $y \in \mathbb{N}$. Etsitään pienin tällainen $y_0 = \mu y(f(y) = x \vee g(y) = x)$ ja tarkastetaan sen avulla kumpaan joukkoon x kuuluu, eli onko $f(y_0) = x$. Saadaan

$$x \in A \qquad \iff \qquad f(\mu y(f(y) = x \vee g(y) = x)) = x \ . \tag{16}$$

Jokaiselle $x \in \mathbb{N}$ tällainen luku y lopulta löytyy, joten määrittelemällä

$$\chi_A(x) = \begin{cases} 1, & \text{jos } f(\mu y(f(y) = x \vee g(y) = x)) = x \\ 0, & \text{muulloin} \end{cases} \tag{17}$$

saadaan haluttu totaali rekursiivinen karakteristinen funktio. □

[5] [5, Kleene 1943]

Esimerkki 2. Joukko

$$K_0 = \{\ \langle x, y\rangle \in \mathbb{N} \mid \varphi_x(y)\downarrow\ \} \tag{18}$$

on rekursiivisesti numeroituva lemman 1 neljännen kohdan nojalla,

$$\langle x, y\rangle \in K_0 \iff \varphi_x(y)\downarrow \iff \exists z : T(x, y, z)\ , \tag{19}$$

missä T on rekursiivinen.

Lemman 1 toinen väittämä motivoi seuraavaan määritelmään.

Määritelmä 6. *Olkoon $x \in \mathbb{N}$. Merkitään $W_x = \mathrm{Dom}\ \varphi_x$.*

Näin saadaan standardinumerointi kaikille rekursiivisesti numeroituville joukoille,

$$W_0,\ W_1,\ W_2,\ W_3,\ W_4,\ \ldots\ .$$

Lemman 1 neljäs kohta tunnetaan projektiolauseena [13, luku 5.4]. Laskennan vaativuusteoriassa tarkasteltu päätösongelmaluokka NP voidaan karakterisoida analogisella tavalla: luokka NP koostuu päätösongelmista A, joille on olemassa polynomisessa ajassa laskettava ja polynomisesti tasapainoinen[6] predikaatti $P(x, y)$, jolle

$$x \in A \iff \exists y : P(x, y)\ . \tag{20}$$

Ns. P vs. NP -ongelma on yhä avoin kysymys laskennan vaativuusteoriassa; Laskettavuusteorian vastine tälle ongelmalle kysyy onko rekursiivisten joukkojen ja rekursiivisesti numeroituvien joukkojen luokat samat. Ongelma laskettavuusteoriassa ratkesi jo syntyessään, kuten seuraavaksi nähdään.

2.6 Pysähtymisongelma

Esimerkin 2 joukko K_0 kuvaa *pysähtymisongelmaa* (engl. halting problem):

$$\langle x, y\rangle \in K_0 \iff \varphi_x(y)\downarrow \iff y \in W_x \tag{21}$$

> "Annettuna on funktion indeksi x ja syöte y. Pysähtyykö funktion φ_x laskenta tällä syötteellä?"

Seuraavan laskettavuusteorian perustuloksen todisti yleisessä muodossa Alan Turing [5, Turing 1936], vaikkakin tutkijat Post 1922, Gödel 1931, Kleene 1936 ja Church 1936 [5] esittivät kukin vastaavia tuloksia omissa formalisaatioissaan. Todistus on klassinen diagonaaliargumentin sovellus.

Lause 6. *K_0 ei ole rekursiivinen.*

Todistus. Tehdään vastaoletus: χ_{K_0} on rekursiivinen. Tällöin funktio

$$\psi(x) = \begin{cases} \nearrow, & \text{jos } \chi_{K_0}(\langle x, x\rangle) = 1 \\ 0, & \text{jos } \chi_{K_0}(\langle x, x\rangle) = 0 \end{cases} \tag{22}$$

on osittaisrekursiivinen. Valitaan sellainen $n \in \mathbb{N}$, että $\varphi_n = \psi$. Ristiriita saadaan aikaan päättelyketjulla

$$\begin{aligned} \langle n, n\rangle \in K_0 &\iff \varphi_n(n)\downarrow && (K_0\text{:n määritelmä}) \\ &\iff \psi(n)\downarrow && (\text{luvun } n \text{ valinta}) \\ &\iff \chi_{K_0}(\langle n, n\rangle) = 0 && (\psi\text{:n määritelmä}) \\ &\iff \langle n, n\rangle \notin K_0 && (\chi_{K_0}\text{:n määritelmä}) \end{aligned}$$

□

[6] Tietoa laskennan vaativuusteorissa käytetyistä termeistä löytyy Sipserin teoksesta [15].

Sanotaan, että kahden muuttujan predikaatti "$\varphi_x(y)\downarrow$" on ratkeamaton. Esimerkin 2 avulla tehdään välittömästi seuraava huomio.

Seuraus 1. *K_0 on rekursiivisesti numeroituva, mutta ei rekursiivinen.*

Lauseesta 5 taas seuraa, että $\bar{K}_0$ ei voi olla r.n., koska muuten K_0 olisi rekursiivinen.

Seuraus 2. *$\bar{K}_0$ ei ole rekursiivisesti numeroituva.*

Vaikka lause 6 näytettiin todeksi vastaoletuksen kautta, todistus on jossain mielessä konstruktiivinen, sillä todistuksessa funktio ψ voidaan rakentaa konkreettiseksi vastaesimerkiksi mille tahansa yritykselle muotoilla funktion χ_{K_0} laskeva algoritmi. Myöhemmin esimerkissä 7 tämä päättely tehdään tarkemmin. Edelleen luvussa 4 vastaavanlainen tarkastelu tehdään päättelyjärjestelmien tapauksessa ja tätä efektiivistä tapaa löytää vastaesimerkki käytetään määriteltäessä *luovien joukkojen* käsitettä luvussa 5.

2.7 Yhteenveto

Tässä luvussa esiteltiin laskettavuusteorian lähtökohdat:

1. Osittaisrekursiiviset funktiot ovat formaali vastine mekaanisen laskettavuuden intuitiiviselle käsitteelle.
2. Gödel-numeroinnin avulla osittaisrekursiiviselle funktiolle voidaan määrittää indeksi, joka koodaa funktion laskevan algoritmin rakenteen.
3. Osittaisrekursiivisen funktion indeksin avulla funktion laskentaa voidaan efektiivisesti simuloida osittaisrekursiivisella universaalifunktiolla U (Lause 3) ja funktion argumentteja voidaan upottaa sen ohjelmakoodiin Kleenen s-m-n-lauseen (Lause 4) avulla.
4. Tärkeimmät päätösongelmaluokat ovat
   - *Rekursiiviset joukot* $A \subseteq \mathbb{N}$, joihin liittyvä predikaatti "$x \in A$" on ratkeava.
   - *Rekursiivisesti numeroituvat (r.n.) joukot* $B \subseteq \mathbb{N}$, joihin liittyvä predikaatti "$x \in B$" on puoliratkeava, eli vain ongelman "kyllä"-instansseihin voidaan taata korrekti vastaus.
5. Pysähtymisongelman K_0 avulla nähdään, että kaikki r.n. joukot eivät ole rekursiivisia.

Seuraavaksi lähdetään tarkastelemaan päätösongelmien vaikeuseroja rekursiivisten palautusten avulla.

3 Rekursiiviset palautukset

Tässä luvussa käsitellään yksinkertaisia tapoja luokitella päätösongelmia laskettavuusteoriassa. Rekursiivisesti numeroituvien joukkojen luokittelun pani alulle Emil Post [5, Post 1944], jolta ovat peräisin myös kohdassa 3.2 esitellyt vahvat palautukset.

3.1 Isomorfiatyypit [13, luku 4]

Laskettavuusteoria tutkii laskennallisten ongelmien ominaisuuksia, jotka ovat *rekursiivisesti invariantteja*. Selvennetään mitä tällä tarkoitetaan.

Tarkastellaan *rekursiivisten permutaatioiden* joukkoa

$$\mathcal{G} = \{f : \mathbb{N} \to \mathbb{N} \mid f \text{ rekursiivinen bijektio}\} \ . \tag{23}$$

Joukon $\mathcal{G}$ alkiot ovat laskettavia funktioita, jotka järjestävät luonnolliset luvut uuteen järjestykseen. Itse asiassa $\mathcal{G}$ on ryhmä[7] funktioiden yhdistämisen suhteen:

G1. Jos $f, g \in \mathcal{G}$, myös $f \circ g \in \mathcal{G}$, koska osittaisrekursiivisten funktioiden luokka on suljettu yhdistämisen suhteen (*R2*) ja bijektioiden yhdiste on edelleen bijektio.
G2. Funktioiden yhdistäminen on liitännäistä: $(g \circ f) \circ h = g \circ (f \circ h)$.
G3. Identiteettikuvaus $\mathrm{id}(x) = Pr^1_1(x) = x$, jolle $\mathrm{id} \circ f = f \circ \mathrm{id} = f$ kaikilla $f \in \mathcal{G}$, on rekursiivinen permutaatio.
G4. Rekursiivisen permutaation käänteiskuvaus on myös rekursiivinen. Olkoon $f \in \mathcal{G}$. Tällöin
$$f^{-1}(x) = \mu y(f(y) = x) \tag{24}$$
määrittelee totaalin funktion, sillä f:n surjektiivisuuden nojalla jokaiselle $x \in \mathbb{N}$ löytyy jokin alkukuva y.

Päätösongelmat A ja B ovat yhtä mielenkiintoisia tai niillä on laskettavuusteorian kannalta sama rakenne, jos joukot voidaan kuvata toisiinsa rekursiivisen permutaatioryhmän $\mathcal{G}$ toiminnoilla.

Määritelmä 7. *Joukot $A, B \subseteq \mathbb{N}$ ovat* rekursiivisesti isomorfisia *(tai lyhyesti* isomorfisia*), merkitään $A \equiv B$, jos A saadaan rekursiivisesti permutoimalla B:tä:*

$$A \equiv B \quad \Longleftrightarrow \quad A = f(B), \ \textit{jollekin } f \in \mathcal{G} \ . \tag{25}$$

Rekursiivisten permutaatioiden ryhmäominaisuuksista nähdään, että relaatio $\equiv$ on

E1. *Refleksiivinen.* Kaikilla $A \subseteq \mathbb{N}$, $A \equiv A$, koska $A = \mathrm{id}(A)$.
E2. *Symmetrinen.* Kaikilla $A, B \subseteq \mathbb{N}$, $A \equiv B \Rightarrow B \equiv A$, koska jos $A = f(B)$, niin $B = f^{-1}(A)$.
E3. *Transitiivinen.* Kaikilla $A, B, C \subseteq \mathbb{N}$, $A \equiv B$ ja $B \equiv C \Rightarrow A \equiv C$, koska jos $A = f(B)$ ja $B = g(C)$, niin $A = (f \circ g)(C)$.

Kohdat E1-E3 yhdessä tekevät $\equiv$-relaatiosta *ekvivalenssirelaation*[8], joka osittaa luonnollisten lukujen osajoukot eri *ekvivalenssiluokkiin*, eli eri *isomorfiatyyppeihin*. Tämän avulla voidaan samastaa rakenteellisesti identtiset joukot eli voidaan abstrahoida päätösongelmien koodaukselliset yksityiskohdat pois: kaksi päätösongelmaa ovat isomorfisia, jos ne kuvaavat laskennallisessa mielessä samat ongelmat. Nämä isomorfiatyypit ovat laskettavuusteorian peruselementtejä ja vaaditaankin yleisesti, että laskettavuusteorian käsitteet (kuten rekursiiviset joukot, universaalit funktiot, funktioiden Gödel-numeroinnit, jne.) kunnioittavat isomorfiatyyppejä seuraavalla tavalla.

Määritelmä 8. *Luonnollisten lukujen osajoukkoja koskeva ominaisuus P on* rekursiivisesti invariantti*, jos se pätee keskenään isomorfisille joukoille yhtäaikaisesti:*

$$A \equiv B \qquad \Longrightarrow \qquad (P(A) \Leftrightarrow P(B)) \ . \tag{26}$$

[7] Algebran perusteita käsitellään esimerkiksi teoksessa [2].
[8] Ekvivalenssirelaatioista tarkemmin materiaalissa [12, luku 1.3] tai [2, luku 1].

Esimerkki 3. Rekursiivisesti numeroituvien joukkojen käsite on rekursiivisesti invariantti. Olkoon A ja B isomorfisia joukkoja, $A \equiv B$, eli $A = f(B)$, jollekin $f \in \mathcal{G}$. Koska $\equiv$-relaatio on symmetrinen, riittää näyttää vain toinen implikaatio, joten olkoon B r.n. ja g sellainen, että Im $g = B$ (tapaus $B = \varnothing$ selvä). Tällöin $A = f(\text{Im } g) = \text{Im } f \circ g$, joten A on myös rekursiivisesti numeroituva.

Laskettavuusteoriassa kaikki yksittäisiä päätosongelmia koskevat tulokset (joissa vedotaan vain rekursiivisesti invariantteihin ominaisuuksiin) voidaan heti yleistää koskemaan kokonaista isomorfiatyyppiä.

3.2 Vahvat palautukset

Päätösongelmien luokittelussa kahden ongelman keskinäisen vaikeuden vertaaminen on keskeistä. Intuitiivisesti ongelma B on vaikeampi tai yhtä vaikea kuin A, jos B:n ratkaisevasta algoritmista voidaan johtaa myös A:lle algoritmi. Toisin sanoen ongelman A ratkaisemiseksi riittää ratkaista B. Sanotaan, että ongelma A *palautuu* ongelmaan B.

Esimerkki 4. Edellisessä luvussa määriteltiin pysähtymisongelma K_0, jolle $\langle x, y\rangle \in K_0 \Leftrightarrow \varphi_x(y)\downarrow$. Tarkastellaan joukon K_0 diagonaalileikkausta, pysähtymisongelman variaatiota

$$K = \{x \in \mathbb{N} \mid \varphi_x(x)\downarrow\} \ . \tag{27}$$

Ongelma K on korkeintaan yhtä vaikea kuin K_0, sillä ratkaistaessa predikaattia "$x \in K$" riittää tarkastaa ehto "$\langle x, x\rangle \in K_0$".

m-palautukset. Päätösongelmien palautuvuus voidaan formalisoida eri tavoin. Tarkastelemme tässä työssä ns. *vahvoja palautuksia* (engl. strong reducibilities), jotka lopulta osoittautuvat yksinkertaisimmiksi mahdollisiksi palautuksiksi (Luku 6).

Määritelmä 9. *Joukko $A \subseteq \mathbb{N}$ voidaan* monta-yhteen[9] palauttaa *(tai lyhyemmin* m-palauttaa*) joukkoon $B \subseteq \mathbb{N}$, merkitään $A \leq_m B$, jos on olemassa rekursiivinen $f : \mathbb{N} \to \mathbb{N}$ s.e.*

$$x \in A \qquad \Longleftrightarrow \qquad f(x) \in B \ . \tag{28}$$

Jos $A \leq_m B$ kuvauksella $f : \mathbb{N} \to \mathbb{N}$, kirjoitetaan lyhyesti $f : A \leq_m B$. Huomataan heti, että $\leq_m$-relaatio on

- *Refleksiivinen.* $A \leq_m A$, identiteettikuvauksella.
- *Transitiivinen.* Jos $f : A \leq_m B$ ja $g : B \leq_m C$, niin $g \circ f : A \leq_m C$.

Huomautus 2. Palautukset toimivat myös luonnollisella tavalla seuraavasti. Jos $f : A \leq_m B$ ja B on rekursiivinen (r.n.), niin A on rekursiivinen (r.n.). Tämä seuraa siitä, että $\chi_A = \chi_B \circ f$ ($\widetilde{\chi_A} = \widetilde{\chi_B} \circ f$).

Esimerkissä 4 nähtiin, että $x \mapsto \langle x, x\rangle : K \leq_m K_0$. Itse asiassa väite pätee kääntäenkin.

Lemma 2. *$K_0 \leq_m K$.*

[9] Funktiot ovat monta-yhteen-relaatioita (engl. many-one relation), koska jokaista kuvajoukon alkiota vastaa monta alkiota lähtöpuolella. Terminologia on tässä hieman kankea, ja esimerkiksi Sipser [15, luku 5.3] on ottanut käyttoon termin *mapping reducibility*.

Todistus. Määritellään osittaisrekursiivinen funktio

$$\psi(x,y) = \begin{cases} 1, & \text{jos } \varphi_{\pi_1(x)}(\pi_2(x))\downarrow \\ \nearrow, & \text{jos } \varphi_{\pi_1(x)}(\pi_2(x))\uparrow \end{cases} \tag{29}$$

Funktio ψ käyttää laskennassaan implisiittisesti funktiota U (Lause 3) simuloidessaan parametrina saatua ohjelmaa $\pi_1(x)$. Huom! funktion ψ arvo ei riipu ollenkaan toisesta parametristaan y.

Kleenen *s-m-n*-lause antaa nyt rekursiivisen $s : \mathbb{N} \to \mathbb{N}$ s.e. $\varphi_{s(x)}(y) \simeq \psi(x,y)$.[10] Kun merkitään lyhyesti $z = \langle x, y\rangle$, päätellään

$$\begin{aligned} z = \langle x,y\rangle \in K_0 &\iff \varphi_x(y)\downarrow \iff \varphi_{\pi_1(z)}(\pi_2(z))\downarrow \\ &\iff \psi(z,s(z))\downarrow \iff \varphi_{s(z)}(s(z))\downarrow \iff s(z) \in K \ . \end{aligned}$$

Saatiin $K_0 \leq_m K$ kuvauksella s. □

Koska $K \leq_m K_0$ ja $K_0 \leq_m K$, ongelmat K ja K_0 ovat m-palautusten mielessä yhtä vaikeat. Annetaan tälle ekvivalenssille oma merkintä: $K \equiv_m K_0$.

Määritelmä 10. *Joukot $A, B \subseteq \mathbb{N}$ ovat* m-ekvivalentteja*, merkitään $A \equiv_m B$, jos $A \leq_m B$ ja $B \leq_m A$.*

Määritelmä 10 on rekursiivisesti invariantti ($A \equiv B \Rightarrow A \equiv_m B$) ja relaatio $\equiv_m$ on todella ekvivalenssirelaatio, kuten $\leq_m$-relaation refleksiivisyydestä ja transitiivisuudesta nähdään.

Päätösongelmaan A liittyvää ekvivalenssiluokkaa eli *m-astetta* (engl. m-degree) merkitään

$$\mathrm{d}_m(A) = \{B \subseteq \mathbb{N} \mid A \equiv_m B\} \ . \tag{30}$$

Kaikkien m-asteiden luokan

$$\boldsymbol{\mathcal{D}}_m = \{\mathrm{d}_m(A) \mid A \subseteq \mathbb{N}\} \tag{31}$$

rakenne on laskettavuusteorian kannalta oleellinen. Kun laajennetaan $\leq_m$-relaatio luonnollisesti m-asteiden luokkaan $\boldsymbol{\mathcal{D}}_m$, eli määritellään $\mathrm{d}_m(A) \leq_m \mathrm{d}_m(B) \Leftrightarrow A \leq_m B$,[11] saadaan relaatiosta $\leq_m$ lisäksi antisymmetrinen tässä luokassa: jos $\mathbf{a}, \mathbf{b} \in \boldsymbol{\mathcal{D}}_m$ ja pätee $\mathbf{a} \leq_m \mathbf{b}$ ja $\mathbf{b} \leq_m \mathbf{a}$, niin seuraa $\mathbf{a} = \mathbf{b}$.

Kootaan tähänastiset huomiot yhteen.

Lemma 3. *$(\boldsymbol{\mathcal{D}}_m, \leq_m)$ on osittain järjestetty joukko (engl. poset), eli $\leq_m$ on refleksiivinen, antisymmetrinen ja transitiivinen.*

Teknisemmin pätee lisäksi, että $(\boldsymbol{\mathcal{D}}_m, \leq_m)$ on join-puolihila[12], mutta tämän työn tavoitteen kannalta Lemman 3 luonnehdinta riittää.

Jo triviaalitapaukset osoittavat, että on olemassa joukkoja, joita ei voida vertailla keskenään: $\varnothing \not\leq_m \mathbb{N}$ ja $\mathbb{N} \not\leq_m \varnothing$. Relaatio $\leq_m$ ei siis ole lineaarinen järjestys. Mielenkiintoisempi tapaus saadaan pysähtymisongelman kohdalla.

Lemma 4. *K_0 ja $\bar{K}_0$ ovat vertailemattomia.*

---

[10] Tarkemmin: jos $z \in \mathbb{N}$ on sellainen, että $\varphi_z^{(2)} \simeq \psi$ *s-m-n*-lause antaa rekursiivisen $s_1^1 : \mathbb{N}^2 \to \mathbb{N}$ s.e. $\varphi_{s_1^1(z,x)}(y) \simeq \psi(x,y)$. Määritellään $s(x) = s_1^1(z,x)$.

[11] Laajennus on hyvin määritelty. Jos $A \equiv_m A'$, $B \equiv_m B'$ ja $A \leq_m B$, niin $A' \leq_m A \leq_m B \leq_m B'$, josta $A' \leq_m B'$.

[12] Kahden m-asteen $\mathrm{d}_m(A)$ ja $\mathrm{d}_m(B)$ pienin yhteinen yläraja on $\mathrm{d}_m(A \oplus B)$, missä $A \oplus B = \{2x \in \mathbb{N} \mid x \in A\} \cup \{2x+1 \in \mathbb{N} \mid x \in B\}$. [4, s. 164]

Todistus. $\bar{K_0} \not\leq_m K_0$**:** Jos olisi $\bar{K_0} \leq_m K_0$, saataisiin joukosta $\bar{K_0}$ rekursiivisesti numeroituva huomautuksen 2 nojalla, mikä on ristiriidassa seurauslauseen 2 kanssa.
$K_0 \not\leq_m \bar{K_0}$**:** Jos $f : K_0 \leq_m \bar{K_0}$, eli $x \in K_0 \Leftrightarrow f(x) \in \bar{K_0}$, on tämä yhtäpitävää sen kanssa, että $x \notin K_0 \Leftrightarrow f(x) \notin \bar{K_0}$ eli $x \in \bar{K_0} \Leftrightarrow f(x) \in K_0$ ja ristiriita saadaan samalla tavalla kun edellisessä tapauksessa.

□

Huomautus 3. Huomautuksen 2 avulla nähdään, että jos $A \in \mathbf{a} \in \boldsymbol{\mathcal{D}}_m$ on rekursiivinen (r.n.), jokainen $B \in \mathbf{a}$ on niin ikään rekursiivinen (r.n.). Tämän vuoksi on mielekästä puhua rekursiivisista tai rekursiivisesti numeroituvista m-asteista.

1-palautukset. Aavistuksen verran rajoittuneempi palautustyyppi saadaan, kun vaaditaan määritelmässä 9 palautusfunktiolta injektiivisyyttä.

Määritelmä 11. *Joukko $A \subseteq \mathbb{N}$ voidaan* yksi-yhteen palauttaa *(tai lyhyemmin* 1-palauttaa*) joukkoon $B \subseteq \mathbb{N}$, merkitään $A \leq_1 B$, jos on olemassa rekursiivinen injektio $f : \mathbb{N} \to \mathbb{N}$ s.e.*

$$x \in A \qquad \Longleftrightarrow \qquad f(x) \in B \ . \tag{32}$$

Täysin analogisesti m-palautusten kanssa voidaan määritellä käsitteet 1-ekvivalenssi ($\equiv_1$), 1-asteet ($\mathrm{d}_1(\cdot)$) ja 1-asteiden luokka $\boldsymbol{\mathcal{D}}_1$, jolle $\leq_1$ on osittainjärjestys.

Koska 1-palautukset ovat m-palautusten erikoistapauksia, saadaan

$$A \equiv_1 B \qquad \Longrightarrow \qquad A \equiv_m B \ .$$

Tämä voidaan tulkita siten, että yksi m-aste koostuu useista 1-asteista. Tutkitaan seuraavaksi 1- ja m-palautusten suhdetta.

3.3 Sylinterit [13, luku 7.6]

On tilanteita, joissa m-palautusta $f : A \leq_m B$ ei voida muokata injektiiviseksi 1-palautukseksi $f' : A \leq_1 B$. Ongelmia voi tulla siitä, ettei joukossa B tai sen komplementissa ole tilaa erotella palautuksen f ei-injektiivisiä kohtia $a \neq b$, $f(a) = f(b)$, eri alkioiksi kuvapuolella. Tai voi olla, ettei tätä tilaa löydetä rekursiivisesti. Helppona esimerkkinä

$$\{1,2\} \leq_m \{3\}, \qquad \text{mutta} \qquad \{1,2\} \not\leq_1 \{3\} \ .$$

Jos päätösongelmalla A on sellainen rakenne, että jokaista sen instanssia "$x \in A$" kohden voidaan muodostaa jono erilaisia instansseja

$$\text{“}h_x(0) \in A\text{”}, \quad \text{“}h_x(1) \in A\text{”}, \quad \text{“}h_x(2) \in A\text{”}, \quad \text{“}h_x(3) \in A\text{”}, \quad \ldots \ , \tag{33}$$

missä $h_x : \mathbb{N} \to \mathbb{N}$ on rekursiivinen injektio ja kaikilla $y \in \mathbb{N}$

$$x \in A \quad \Longleftrightarrow \quad h_x(y) \in A \ , \tag{34}$$

m-palautukset $B \leq_m A$ saadaan efektiivisesti muunnettua injektiivisiksi. Tehdään tämä täsmällisesti.

Määritelmä 12. *Joukko $A \subseteq \mathbb{N}$ on* sylinteri*, jos on olemassa $C \subseteq \mathbb{N}$ s.e.*

$$A \ \equiv_1 \ C \otimes \mathbb{N} \ , \tag{35}$$

missä joukkojen C ja $\mathbb{N}$ tulo määritellään

$$C \otimes \mathbb{N} = \pi(C \times \mathbb{N}) = \{\langle x, y\rangle \in \mathbb{N} \mid x \in C, y \in \mathbb{N}\} \ . \tag{36}$$

Lause 7. *Jos A on sylinteri ja $B \leq_m A$, niin $B \leq_1 A$.*

Todistus. Koska $A \equiv_1 C \otimes \mathbb{N}$, riittää näyttää $B \leq_1 C \otimes \mathbb{N}$. Yhä 1-ekvivalenssin nojalla oletuksesta $B \leq_m A$ saadaan $f : B \leq_m C \otimes \mathbb{N}$, jollekin rekursiiviselle f. Funktio $g : \mathbb{N} \to \mathbb{N}$ s.e.

$$g(x) = \langle \pi_1(f(x)), x \rangle \tag{37}$$

on rekursiivinen injektio: jos $x \neq x'$, niin $\langle \cdots, x \rangle \neq \langle \cdots, x' \rangle$ eli $g(x) \neq g(x')$. Toisaalta

$$\begin{aligned} x \in B \quad &\iff \quad f(x) \in C \otimes \mathbb{N} \quad \iff \quad \langle \pi_1(f(x)), \pi_2(f(x)) \rangle \in C \otimes \mathbb{N} \\ &\iff \quad \langle \pi_1(f(x)), x \rangle \in C \otimes \mathbb{N} \quad \iff \quad g(x) \in C \otimes \mathbb{N} \ , \end{aligned}$$

joten $g : B \leq_1 C \otimes \mathbb{N}$. □

Huomautus 4. Jos $A \equiv_1 C \otimes \mathbb{N}$, eli $f : A \leq_1 C \otimes \mathbb{N}$ ja $g : C \otimes \mathbb{N} \leq_1 A$, niin kaavoihin 33–34 liittyvät pohdinnat pätevät funktiolla $h_x(y) = g(\langle \pi_1(f(x)), y \rangle)$.

Esitellään sylintereille heti konkreettinen käyttötarkoitus.

Lemma 5. *K_0 on sylinteri.*

Todistus. Osoitetaan $K_0 \equiv_1 K_0 \otimes \mathbb{N}$. Ensimmäinen suunta on helppo: $x \mapsto \langle x, 0 \rangle : K_0 \leq_1 K_0 \otimes \mathbb{N}$. Toiseenkin suuntaan työt on jo tehty, sillä lauseen 2 t-funktio antaa injektiivisen palautuksen.

$$\langle \langle x, y \rangle, z \rangle \in K_0 \otimes \mathbb{N} \quad \iff \quad \langle x, y \rangle \in K_0 \quad \iff \quad \langle t(x, z), y \rangle \in K_0 \ .$$

□

Lemman 2 todistuksessa nähtiin, että $s : K_0 \leq_m K$, mutta koska s oli saatu lauseella 4, s on injektio ja pätee edelleen $K_0 \leq_1 K$. Lisäksi tiedetään äskeisen lemman perusteella (tai suoraan esimerkin 4 palautuksellakin), että $K \leq_1 K_0$, joten saadaan seurauslause:

Seuraus 3. *$K \equiv_1 K_0$ ja molemmat K ja K_0 ovat sylintereitä.*

3.4 Täydelliset joukot

Mitkä rekursiivisesti numeroituvat päätösongelmat ovat vaikeimpia? Pysähtymisongelma K_0 osoittautuu tässäkin pohdinnassa keskeiseksi, nimittäin K_0 on vähintään yhtä vaikea kuin mikä tahansa r.n. ongelma.

Lause 8. *Olkoon $B \subseteq \mathbb{N}$ rekursiivisesti numeroituva. Tällöin $B \leq_m K_0$.*

Todistus. Jos B on r.n., $B = W_x$ jollekin $x \in \mathbb{N}$. Nyt

$$y \in B \quad \iff \quad y \in W_x \quad \iff \quad \varphi_x(y)\downarrow \quad \iff \quad \langle x, y \rangle \in K_0 \ ,$$

joten $y \mapsto \langle x, y \rangle : B \leq_m K_0$. □

Määritelmä 13. *Rekursiivisesti numeroituva joukko $A \subseteq \mathbb{N}$ on* m-täydellinen (1-täydellinen)*, jos jokainen r.n. joukko voidaan m-palauttaa (1-palauttaa) siihen.*

Joukko K_0 on m-täydellinen ja koska $K \equiv_m K_0$, myös K on. Itse asiassa m-aste $\mathrm{d}_m(K)$ sisältää tasan m-täydelliset joukot ja se on maksimi rekursiivisesti numeroituvien m-asteiden luokassa. Merkitään tätä m-täydellisten joukkojen m-astetta symbolilla $\mathbf{0}'_m = \mathrm{d}_m(K)$.

Analysoidaan lopuksi $\boldsymbol{\mathcal{D}}_m$-luokan rakennetta rekursiivisesti numeroituvien joukkojen osalta. Tähän mennessä tiedetään, että

$$A \equiv B \implies A \equiv_1 B \qquad \text{ja} \qquad A \equiv_1 B \implies A \equiv_m B \ ,$$

eli 1-asteet koostuvat isomorfiatyypeistä ja m-asteet koostuvat 1-asteista. Koska kaikille joukoille A pätee[13] $A \equiv_m A \otimes \mathbb{N}$, on $A \otimes \mathbb{N} \in \mathrm{d}_m(A)$ ja koska $A \otimes \mathbb{N}$ on sylinteri, kaikille $B \in \mathrm{d}_m(A)$ saadaan $B \leq_1 A \otimes \mathbb{N}$. Tämä tarkoittaa sitä, että jokaisen m-asteen $\mathrm{d}_m(A)$ sisällä on maksimi 1-aste $\mathrm{d}_1(A \otimes \mathbb{N})$ relaation $\leq_1$ suhteen.

Rekursiiviset joukot jakaantuvat kolmeen m-asteeseen. Löytyy kaksi triviaalitapausta, $\mathbf{o} = \mathrm{d}_m(\varnothing) = \{\varnothing\}$ ja $\mathbf{n} = \mathrm{d}_m(\mathbb{N}) = \{\mathbb{N}\}$, ja loput rekursiiviset joukot asettuvat m-asteeseen, jonka edustajaksi kelpaa esimerkiksi joukko $\{1\}$ (jolloin $\chi_A : A \leq_m \{1\}$), merkitään $\mathbf{0}_m = \mathrm{d}_m(\{1\})$.

Onko olemassa muita rekursiivisesti numeroituvia m-asteita jo lueteltujen $\mathbf{o}, \mathbf{n}, \mathbf{0}_m$ ja $\mathbf{0}'_m$ lisäksi? Tällaisia rekursiivisesti numeroituvia, ei-rekursiivisia ja ei-m-täydellisiä joukkoja on olemassa, mutta niiden konstruoiminen on hieman teknistä, eikä näitä esiinny luonnollisesti klassisissa sovelluksissa [10]. Helpoimpana esimerkkinä toimivat Postin ns. *yksinkertaiset joukot*[14], joiden m-asteet sijoittuvat asteiden $\mathbf{0}_m$ ja $\mathbf{0}'_m$ välille [5, Post 1944].

Kuvaan 2 on hahmoteltu m-asteiden $\boldsymbol{\mathcal{D}}_m$ rakennetta, missä harmaaksi väritetylle alueelle asettuvat asteista $\mathbf{o}, \mathbf{n}, \mathbf{0}_m$ ja $\mathbf{0}'_m$ poikkeavat r.n. m-asteet.

Luvuissa 5 ja 6 yksinkertaistetaan joitain tässä määriteltyjä käsitteitä. Jätetään kuitenkin palautuvuustarkastelut hetkeksi ja lähdetään seuraavassa luvussa tutkimaan ratkeavuuskysymyksiä matemaattisessa logiikassa, josta lopulta *luovien joukkojen* käsite kumpuaa luonnollisesti.

4 Otteita matemaattisesta logiikasta

David Hilbertin johtaman koulukunnan tavoitteena oli 1920-luvulla perustaa klassinen matematiikka täsmälliselle ja ristiriidattomalle formalismille. Cantorin tuomista äärettömyyden käsitteistä oli nimittäin 1900-luvun vaihteessa löytynyt huolestusta herättäviä paradokseja, jotka uhkasivat horjuttaa matematiikan perusteita. Hilbertin ohjelman tarkoituksena oli kitkeä nämä ongelmakohtien aiheuttajat (määritelmien monitulkinnallisuudet ja luonnollisen kielen epämääräisyydet) pois matemaattisesta päättelystä. Ratkaisuyritteenä oli kehittää formaali kieli, jossa matematiikan todistuksia voitaisiin johtaa äärellisin menetelmin, eli mekaanisesti, ilman ulkopuolista tulkintaa.

Ensimmäisen kertaluvun predikaattilogiikka antaa pohjan tällaisille päättelyjärjestelmille. Esimerkiksi moderni lähtökohta joukko-opille on Zermelon-Fraenkelin (ZF) aksiomatisointi, joka on ensimmäisen kertaluvun teoria. [3]

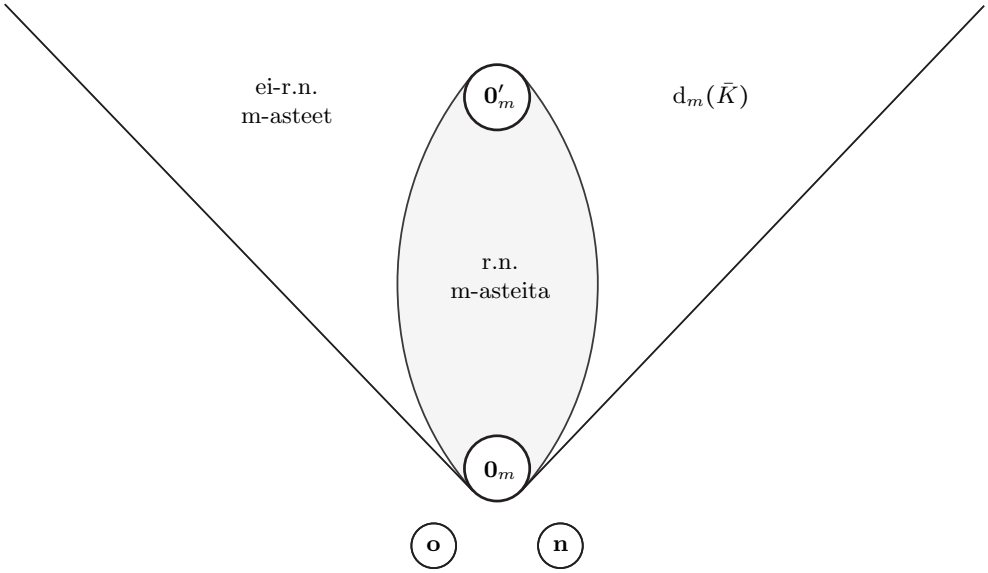
Loogisilta teorioilta[15] T vaaditaan kaksi keskeistä ominaisuutta.

---

[13] $x \mapsto \langle x, 0\rangle : A \leq_m A \otimes \mathbb{N}$ ja $\pi_1 : A \otimes \mathbb{N} \leq_m A$.

[14] *Yksinkertaiset joukot* ovat sellaisia r.n. joukkoja, joilla on ääretön komplementti, joka ei sisällä ainuttakaan ääretöntä r.n. joukkoa.

[15] Predikaattilogiikassa teoriat T ovat yksinkertaisesti predikaattilogiikan lauseista koostuvia aksioomajoukkoja.



Kuva 2. m-asteiden osittain järjestetyn joukon $(\boldsymbol{\mathcal{D}}_m, \leq_m)$ rakenne. Rekursiivisesti numeroituvia m-asteita ovat $\mathbf{o}, \mathbf{n}, \mathbf{0}_m$ ja $\mathbf{0}'_m$ sekä harmaalle alueelle jäävät asteet $\mathbf{a}$, joille $\mathbf{0}_m \leq_m \mathbf{a} \leq_m \mathbf{0}'_m$. Asteet $\mathbf{0}'_m$ ja $\mathrm{d}_m(\bar{K})$ ovat keskenään vertailemattomia. (Kirjasta [4, s. 163].)

T1. *Virheettömyys.* Teoria ei saa todistaa ristiriitoja.

$$\text{Kaikille lauseille } \sigma, \quad \mathrm{T} \nvdash \sigma \wedge \neg\sigma$$

T2. *Täydellisyys.* Teorian tulee ottaa kantaa jokaisen lauseen totuuteen.

$$\text{Kaikille lauseille } \sigma, \quad \mathrm{T} \vdash \sigma \quad \text{tai} \quad \mathrm{T} \vdash \neg\sigma$$

Kurt Gödel osoitti vuonna 1931 [5, Gödel 1931], että kaikki matemaattisesti mielenkiintoiset päättelyjärjestelmät ovat oleellisella tavalla epätäydellisiä (eivät toteuta ehtoja T1–T2 yhtäaikaisesti). Seurataan Gödelin esimerkkiä ja katsotaan, miksei matematiikan formalisointi tule onnistumaan Hilbertin mielessä.

Seuraavassa oletetaan ensimmäisen kertaluvun predikaattilogiikan perusteet tunnetuiksi ja käytetään pitkälti *Logiikka tietotekniikassa: perusteet* -kurssilta [8] tuttua terminologiaa.

4.1 Lukuteorian standardimalli

Jokaisen matematiikkaa formalisoivan teorian tulisi vähintään pystyä kuvaamaan luonnollisten lukujen rakennetta.

ZF-teoriassa luonnolliset luvut rakennetaan epäsuorasti joukkojen avulla, mutta esimerkiksi Peanon aritmetiikka (PA) antaa suoraan aksioomat lukuteorian aakkoston $\mathcal{L}_{\mathcal{N}} = \{+, \times, 0, 1\}$ symbolien[16] manipuloinnille, missä teorian mallien universumien ajatellaan koostuvan luonnollisista luvuista.

$\mathcal{L}_{\mathcal{N}}$-struktuuri

$$\mathcal{N} = (\mathbb{N}, +, \times, 0, 1) \ ,$$

[16] Tässä "+" ja "×" ovat kahden muuttujan funktiosymboleita, "0" ja "1" vakiosymboleita.

missä aakkoston $\mathcal{L}_{\mathcal{N}}$ symboleille on annettu tavalliset tulkinnat luonnollisten lukujen joukossa, on *lukuteorian standardimalli* ja samalla Peanon aritmetiikan (eräs) malli.

Olemassaolevien teorioiden (PA, ZF) yksityiskohdat eivät ole tässä tarkasteltujen tuloksien kannalta oleellisia. Tavoitteena on selventää, miksei mikään hyväksyttävä teoria (esim. PA tai ZF) voi täysin mallintaa struktuurin $\mathcal{N}$ rakennetta predikaattilogiikan tarjoamalla ilmaisuvoimalla.

4.2 Aksiomatisoituvat teoriat

Jos valitaan teoriaksi T lukuteorian standardimallissa todet $\mathcal{L}_{\mathcal{N}}$-lauseet, eli

$$T = \operatorname{Th} \mathcal{N} = \{\sigma \mid \sigma \text{ on } \mathcal{L}_{\mathcal{N}}\text{-lause ja } \mathcal{N} \vDash \sigma\} \ ,$$

saadaan triviaalisti ehdot T1–T2 toteuttava teoria. Tämä ei kuitenkaan ole Hilbertin mielessä tyydyttävä ratkaisu: ei ole ilmeistä kuinka annetulle $\mathcal{L}_{\mathcal{N}}$-lauseelle σ voitaisiin päättää kumpi väitteistä "$\sigma \in T$" vaiko "$\sigma \notin T$" pätee.

Tässä kohtaa luvun 2 tarkastelut ohjaavat mielekkääseen määritelmään. Muistetaan, että merkkijonoihin σ voidaan liittää Gödel-luku $\ulcorner\sigma\urcorner \in \mathbb{N}$ kaavan 5 tapaan. Kiinnitetään predikaattilogiikan kieli, eli $\mathcal{L}_{\mathcal{N}}$-kaavojen joukko

$$\mathcal{L}^*_{\mathcal{N}} = \{\sigma \mid \sigma \text{ on } \mathcal{L}_{\mathcal{N}}\text{-kaava}\} \tag{38}$$

ja sille jokin Gödel-numerointi $\ulcorner\cdot\urcorner : \mathcal{L}^*_{\mathcal{N}} \to \mathbb{N}$.

Määritelmä 14. [9, s. 18] *Teoria T on* (rekursiivisesti) aksiomatisoituva *jos on olemassa teoria S s.e. joukko*

$$\ulcorner S\urcorner = \{\ulcorner\sigma\urcorner \in \mathbb{N} \mid \sigma \in S\}$$

on rekursiivinen ja S aksiomatisoi *T:n, eli* $\operatorname{Cn} S = \operatorname{Cn} T$.[17] *Sanotaan lisäksi, että teoria T on ratkeava, jos* $\ulcorner \operatorname{Cn} T \urcorner$ *on rekursiivinen.*

Jotta teoria T olisi aksiomatisoituva, vaaditaan, että löytyy jokin rekursiivinen joukko aksioomia S, josta kaikki teorian T seuraukset ovat johdettavissa. Tässä on Churchin-Turingin teesiin nojautuen kirjoitettu auki se vaatimus, minkä Hilbert intuitiivisesti vaati päättelyjärjestelmiltään.

Predikaattilogiikan päättelysäännöt[18] ovat lisäksi sellaiset, että niitä voidaan soveltaa mekaanisesti (eli rekursiivisesti). Kääntäen voitaisiin vaatia, että mikä tahansa hyväksyttävä looginen päättelyjärjestelmä on sellainen, joka toimii laskettavia sääntöjä noudattaen.

Gödelin alkuperäisessä artikkelissa johdettiin Principia Mathematica (PM) -järjestelmän johdannaiselle formalismille seuraavat tulokset, jotka modernissa laskettavuusteorian käsittelyssä voitaisiin ottaa aikaisempien huomioiden nojalla melkeinpä annettuina. Otetaan käyttöön lyhennysmerkintöjä $\mathcal{L}_{\mathcal{N}}$-termeille.

Määritelmä 15. *Olkoon $n \in \mathbb{N}$. Merkitään $\underline{n} = 1 + 1 + \cdots + 1 \in \mathcal{L}^*_{\mathcal{N}}$ (n kpl).*[19] *Näin $\mathcal{L}_{\mathcal{N}}$-termin $\underline{n}$ tulkinta struktuurissa $\mathcal{N}$ on juuri luku n.*

---

[17] Teoriasta T todistuvien lauseiden joukko on $\operatorname{Cn} T = \{\sigma \mid T \vdash \sigma\}$.

[18] Luentomonisteessa [8] esitellään semanttisten taulujen menetelmää. Lähteissä [9; 17] käytetään perinteisempiä Hilbertin mallisia päättelysääntöjä.

[19] Täsmällisemmin $+(1, +(1, \cdots + (1, 0)\cdots))$.

Lemma 6. *Olkoon S $\mathcal{L}_\mathcal{N}$-teoria, jolle $\lceil S \rceil$ on rekursiivinen. Seuraavat luonnollisia lukuja koskevat predikaatit ovat rekursiivisia.*[20]

$$Prf_S(a,b) \iff \begin{array}{l} b \text{ koodaa todistuksen teoriasta } S \text{ lauseelle, jonka} \\ \text{Gödel-luku on } a. \end{array}$$

$$Sub(a,b,c) \iff \begin{array}{l} a \text{ on Gödel-luku kaavalle, joka saadaan sijoittamalla} \\ b\text{:n koodaaman kaavan vapaisiin muuttujiin termi } \underline{c}. \end{array}$$

Todistus. Hahmotellaan tilannetta predikaattilogiikan tapauksessa.

- $Prf_S(a,b)$: Todistus on on äärellinen $\mathcal{L}_\mathcal{N}$-kaavajono, joka päättyy lauseeseen mikä oli todistettavissa. (Jonoja voidaan koodata funktiolla π^*, s. 5.) Jonon jokainen kaava σ on joko
  1. S:n aksiooma, jolloin predikaatti "$\lceil \sigma \rceil \in \lceil S \rceil$" on oletuksen nojalla ratkeava.
  2. predikaattilogiikan aksiooma, jolloin se voidaan myös tunnistaa rekursiivisesti.
  3. saatu päättelysäännöllä (esim. *modus ponens*) jonon aiemmista kaavoista, mikä on niin ikään rekursiivista.
- $Sub(a,b,c)$: Käydään läpi merkkijonoa, jonka Gödel-luku on b, ja korvataan kaikki vapaat muuttujaesiintymät termillä $\underline{c}$. Lopuksi verrataan saadun merkkijonon Gödel-lukua lukuun a. □

Predikaatin $Prf_S(a,b)$ rekursiivisuus vastaa täsmälleen Hilbertin toiveita: kun joku väittää todistaneensa uuden matemaattisen tuloksen, formaalin todistuksen oikeellisuus tulisi voida mekaanisesti tarkistaa.

Projisoimalla saadaan

Lause 9. *Jos T on aksiomatisoituva, joukko $\lceil \mathrm{Cn}\ T \rceil$ on rekursiivisesti numeroituva.*

Todistus. Olkoon S sellainen, että $\lceil S \rceil$ on rekursiivinen ja $\mathrm{Cn}\ S = \mathrm{Cn}\ T$. Edellisen lemman nojalla $Prf_S(a,b)$ on rekursiivinen. Nyt jos $\lceil \sigma \rceil$ on kaavan σ Gödel-luku, pätee

$$\begin{aligned} \exists b : Prf_S(\lceil \sigma \rceil, b) &\iff S \vdash \sigma \iff \sigma \in \mathrm{Cn}\ S \\ &\iff \sigma \in \mathrm{Cn}\ T \iff \lceil \sigma \rceil \in \lceil \mathrm{Cn}\ T \rceil\ , \end{aligned}$$

mistä nähdään projektiolauseen (Lemma 1, kohta 4) perusteella, että $\lceil \mathrm{Cn}\ T \rceil$ on r.n.. □

4.3 Määriteltävyys lukuteoriassa

Kuinka ilmaisuvoimainen predikaattilogiikan kieli on? Muotoillaan kysymys toisin: millaiset rakenteet ovat *määriteltävissä* predikaattilogiikan kielellä?

Määritelmä 16. *Relaatio $X \subseteq \mathbb{N}^n$ on* määriteltävä lukuteorian standardimallissa $\mathcal{N}$*, jos on olemassa $\mathcal{L}_\mathcal{N}$-kaava $\sigma(v_1, \ldots, v_n)$, jolle pätee*

$$(x_1, \ldots, x_n) \in X \qquad \iff \qquad \mathcal{N} \vDash \sigma(\underline{x_1}, \ldots, \underline{x_n})\ . \tag{39}$$

Esimerkki 5. Alkulukujen joukko on määriteltävä.

$$p \text{ on alkuluku} \iff \mathcal{N} \vDash \exists k : (\underline{2} + k = \underline{p}) \wedge \forall n \forall m : (n \times m = \underline{p} \to (n = 1 \vee m = 1))\ .$$

[20] Itse asiassa Gödel osoitti predikaatit primitiivirekursiivisiksi (s. 3, H2). Vuonna 1931 rekursiivisten funktioiden käsite ei ollut vielä muotoutunut.

Funktiot $f : \mathbb{N}^n \to \mathbb{N}$ ovat relaatioita, $f \subseteq \mathbb{N}^n \times \mathbb{N} = \mathbb{N}^{n+1}$, joten voidaan puhua myös funktioiden määriteltävyydesta.

Esitellään aputulos, jonka todistus vaatii hieman lukuteoreettista huolenpitoa.

Lemma 7 (Gödelin β-funktiolemma). *On olemassa struktuurissa $\mathcal{N}$ määriteltävä funktio $\beta : \mathbb{N}^2 \to \mathbb{N}$ s.e. kaikille $n \in \mathbb{N}$ ja kaikille jonoille $(x_0, \ldots, x_{n-1}) \in \mathbb{N}^n$ löytyy $z \in \mathbb{N}$ s.e. $\beta(z, i) = x_i$, kaikilla $0 \leq i \leq n-1$.*

Todistus. Liitteenä. □

Lemman β-funktio purkaa äärellisten jonojen koodeja samalla tavalla kuin luvun 2 π^*-funktion käänteiskuvaus, mutta näin muotoiltuna se on helpompi ottaa käyttöön seuraavassa tärkeässä tuloksessa.

Lause 10. *Osittaisrekursiiviset funktiot ovat määriteltäviä lukuteoriassa.*

Todistus. Käydään läpi määritelmä 2 ja näytetään, että määriteltävien funktioiden luokka sisältää lähtöfunktiot (*R1*) ja on suljettu operaatioiden *R2–R4* suhteen.

R1. Lähtöfunktiot ovat määriteltäviä.

$$\begin{aligned} Z(x) = y &\iff \mathcal{N} \vDash 0 = \underline{y} \\ S(x) = y &\iff \mathcal{N} \vDash \underline{x} + 1 = \underline{y} \\ Pr_n^m(x_1, \ldots, x_n) = y &\iff \mathcal{N} \vDash \underline{x_m} = \underline{y} \end{aligned}$$

R2. Oletetaan, että kaavat $\sigma_\psi(v_1, \ldots, v_m, u)$ ja $\sigma_{\tau_i}(v_1, \ldots, v_n, u)$, $0 \leq i \leq m$, määrittelevät osittaisfunktiot $\psi : \mathbb{N}^m \to \mathbb{N}$ ja $\tau_i : \mathbb{N}^n \to \mathbb{N}$. Tällöin kaava $\sigma_\varphi(v_1, \ldots, v_m, u)$ s.e.

$$\begin{aligned} \sigma_\varphi(v_1, \ldots, v_n, u) \;=\; \exists z_1 \cdots \exists z_m : (&\sigma_{\tau_1}(v_1, \ldots, v_n, z_1) \wedge \cdots \wedge \sigma_{\tau_m}(v_1, \ldots, v_n, z_m) \\ &\wedge \sigma_\psi(z_1, \ldots, z_m, u)) \end{aligned}$$

määrittelee osittaisfunktion $\varphi(\vec{x}) \simeq \psi(\tau_1(\vec{x}), \ldots, \tau_m(\vec{x}))$.

R3. Oletetaan, että kaavat $\sigma_\psi(v_1, \ldots, v_n, u)$ ja $\sigma_\tau(t_1, t_2, v_1, \ldots, v_n, u)$ määrittelevät osittaisfunktiot $\psi : \mathbb{N}^n \to \mathbb{N}$ ja $\tau : \mathbb{N}^{n+2} \to \mathbb{N}$. Olkoon $\varphi : \mathbb{N}^{n+1} \to \mathbb{N}$ saatu näistä rekursiolla:

$$\begin{cases} \varphi(0, \vec{x}) \;\simeq\; \psi(\vec{x}) \\ \varphi(y+1, \vec{x}) \;\simeq\; \tau(y, \varphi(y, \vec{x}), \vec{x}) \end{cases}$$

Sovelletaan lemman 7 β-funktiota kirjoitettaessa kaavaa $\sigma_\varphi(t, v_1, \ldots, v_2, u)$. Etsitään jonon $(\varphi(0, \vec{x}), \varphi(1, \vec{x}), \ldots, \varphi(t, \vec{x}))$ koodaavaa lukua z, jonka avulla voidaan tarkastaa arvon $\varphi(t, \vec{x})$ laskennan oikeellisuus. Ilmeisillä lyhennysmerkinnöillä saadaan[21]

$$\begin{aligned} \sigma_\varphi(t, v_1, \ldots, v_n, u) \;=\; \exists z : (&\sigma_\psi(v_1, \ldots, v_n, \beta(z, 0)) \;\wedge \\ &\forall y < t : \sigma_\tau(y, \beta(z, y), v_1, \ldots, v_n, \beta(z, y+1)) \;\wedge \\ &\beta(z, t) = u) \end{aligned}$$

joka määrittelee funktion φ.

[21] Jos $\sigma_\beta(v_1, v_2, u)$ määrittelee funktion β, yllä on kirjoitettu esimerkiksi $\sigma_\beta(z, t, u)$ muodossa $\beta(z, t) = u$ ja $\exists k : (\sigma_\beta(z, 0, k) \wedge \sigma_\psi(v_1, \ldots, v_n, k))$ muodossa $\sigma_\psi(v_1, \ldots, v_n, \beta(z, 0))$. Lisäksi lyhennys $\forall y < t : (\cdots)$ voidaan laventaa kaavaksi $\forall y : (y < t \to (\cdots))$, missä $y < t$ tarkoittaa $\exists l : (y + l = t) \wedge \neg(y = t)$.

R4. Oletetaan, että kaava $\sigma_\psi(t, v_1, \ldots, v_n, u)$ määrittelee osittaisfunktion $\psi : \mathbb{N}^{n+1} \to \mathbb{N}$. Jos osittaisfunktio $\varphi : \mathbb{N}^n \to \mathbb{N}$ on saatu minimalisaatiolla

$$\varphi(\vec{x}) \simeq \mu y(\ \forall z \le y : \psi(z, \vec{x})\downarrow \ \wedge\ \psi(y, \vec{x}) = 0\ )\ ,$$

funktion määrittelevä kaava σ_φ saadaan (lyhennysmerkinnöillä) seuraavasti:

$$\begin{aligned}\sigma_\varphi(v_1, \ldots, v_n, u) \ =\ & \forall k < u : \exists z \neq 0 : \sigma_\psi(k, v_1, \ldots, v_n, z) \ \wedge \\ & \sigma_\psi(u, v_1, \ldots, v_n, 0)\end{aligned}$$

□

Esimerkki 6. Jos $A \neq \varnothing$ on r.n. joukko eli $A = \operatorname{Im} f$, saadaan lauseen 10 avulla kaava

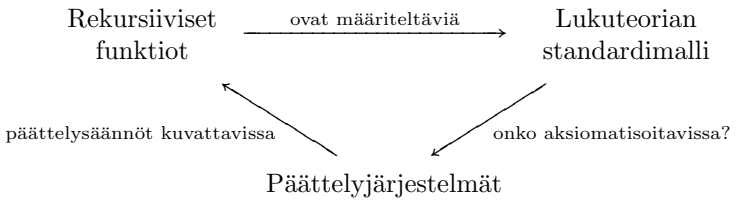
$$\sigma_A(x) = \exists y : \sigma_f(y, x)\ ,$$

jolloin $x \in A \Leftrightarrow \mathcal{N} \vDash \sigma_A(\underline{x})$.

Lukuteorian $\mathcal{L}_\mathcal{N}$-lauseilla voidaan siis viitata laskettavuusteorian käsitteistöön. Tämä ilmaisuvoima osoittautuu ongelmalliseksi, kun lukuteoriaa pyritään rekursiivisesti aksiomatisoimaan.

4.4 Gödelin epätäydellisyyslause

Päättelyjärjestelmät noudattavat laskettavia sääntöjä ja nämä säännöt ovat määriteltävissä lukuteoriassa: sanotaan, että päättelyjärjestelmien toiminta on näin *aritmetisoitu*. Seuraava kaavio kuvaa tilannetta.



Gödelin neronleimaus oli käyttää formaalin kielen ilmaisuvoimaa itseään vastaan ja konstruoida $\mathcal{L}_\mathcal{N}$-lause G, joka viittaa itseensä ja jonka tulkinta luonnolliselle kielelle kuuluu

$$G = \text{“}\textit{Tämä lause ei ole todistettavissa teoriasta } T\text{”}\ ,$$

missä G voidaan konstruoida mille tahansa aksiomatisoituvalle teorialle T. Lause G saadaan ns. *Gödelin kiintopistelauseen* [9, s. 19] sovelluksena.

Lause 11. [5, Gödel 1931] *Olkoon T aksiomatisoituva. On olemassa $\mathcal{L}_\mathcal{N}$-lause G s.e.*

$$\mathcal{N} \vDash G \qquad \Longleftrightarrow \qquad T \nvdash G\ . \tag{40}$$

Todistus. Kun T on aksiomatisoituva, lauseen 9 nojalla $\lceil \operatorname{Cn} T \rceil$ on r.n., joten olkoon (esimerkin 6 avulla) $\phi(x) = \neg\sigma_{\lceil \operatorname{Cn} T \rceil}(x)$. Kaikille $\mathcal{L}_\mathcal{N}$-kaavoille σ pätee

$$\begin{aligned}\mathcal{N} \vDash \phi(\underline{\lceil\sigma\rceil}) \ &\Longleftrightarrow\ \mathcal{N} \vDash \neg\sigma_{\lceil \operatorname{Cn} T \rceil}(\underline{\lceil\sigma\rceil}) \ \Longleftrightarrow\ \mathcal{N} \nvDash \sigma_{\lceil \operatorname{Cn} T \rceil}(\underline{\lceil\sigma\rceil}) \\ &\Longleftrightarrow\ \lceil\sigma\rceil \notin \lceil \operatorname{Cn} T \rceil \ \Longleftrightarrow\ \sigma \notin \operatorname{Cn} T \ \Longleftrightarrow\ T \nvdash \sigma\ .\end{aligned}$$

Muistetaan, että lemman 6 $Sub(a,b,c)$-predikaatti on rekursiivinen, joten olkoon $\sigma_{Sub}(v_1,v_2,v_3)$ sen määrittelevä $\mathcal{L}_{\mathcal{N}}$-kaava. Tarkastellaan kaavaa

$$\widetilde{G}(y) = \exists x : (\phi(x) \wedge \sigma_{Sub}(x,y,y)) \ ,$$

jonka tulkinta luonnolliselle kielelle voisi olla

$$\widetilde{G}(y) \quad = \quad \textit{“Lause, joka on saatu } y\textit{:n koodaamasta kaavasta vapaat muuttujat termillä } \underline{y} \textit{ korvaten, ei ole todistuva } T\textit{:stä”}$$

Määritellään lopulta lause G:

$$G \ = \ \widetilde{G}(\underline{\lceil \widetilde{G}(y) \rceil}) \ = \ \exists x : (\phi(x) \wedge \sigma_{Sub}(x, \underline{\lceil \widetilde{G}(y) \rceil}, \underline{\lceil \widetilde{G}(y) \rceil})) \ .$$

G on saatu kaavasta $\widetilde{G}(y)$ vapaat muuttujat termillä $\underline{\lceil \widetilde{G}(y) \rceil}$ korvaten—mutta tämähän tarkoittaa juuri sitä, että $Sub(\lceil G \rceil, \lceil \widetilde{G}(y) \rceil, \lceil \widetilde{G}(y) \rceil)$ pätee!

$$x = \lceil G \rceil \iff Sub(x, \lceil \widetilde{G}(y) \rceil, \lceil \widetilde{G}(y) \rceil) \iff \mathcal{N} \vDash \sigma_{Sub}(\underline{x}, \underline{\lceil \widetilde{G}(y) \rceil}, \underline{\lceil \widetilde{G}(y) \rceil})$$

Siispä tulos saadaan päättelemällä

$$\begin{aligned}
\mathcal{N} \vDash G \quad &\iff \quad \mathcal{N} \vDash \exists x : (\phi(x) \wedge \sigma_{Sub}(x, \underline{\lceil \widetilde{G}(y) \rceil}, \underline{\lceil \widetilde{G}(y) \rceil})) \\
&\iff \quad \text{jollakin } x \in \mathbb{N} : \quad \mathcal{N} \vDash \phi(\underline{x}) \quad \text{ja} \quad \mathcal{N} \vDash \sigma_{Sub}(\underline{x}, \underline{\lceil \widetilde{G}(y) \rceil}, \underline{\lceil \widetilde{G}(y) \rceil}) \\
&\iff \quad \text{jollakin } x \in \mathbb{N} : \quad \mathcal{N} \vDash \phi(\underline{x}) \quad \text{ja} \quad x = \lceil G \rceil \\
&\iff \quad \mathcal{N} \vDash \phi(\underline{\lceil G \rceil}) \\
&\iff \quad T \nvdash G
\end{aligned}$$

□

Seuraus 4 (Gödelin 1. epätäydellisyyslause). *Teoria* Th $\mathcal{N}$ *ei ole aksiomatisoituva.*

Todistus. Olkoon T mikä tahansa rekursiivisesti aksiomatisoituva $\mathcal{L}_{\mathcal{N}}$-teoria. Konstruoidaan $\mathcal{L}_{\mathcal{N}}$-lause G kuten yllä. Kaksi tapausta:

1. $T \vdash G$: Lause G todistuu teoriasta T, mutta on silloin epätosi lukuteorian standardimallissa ja tällöin T todistaa epätosia väittämiä!

$$G \in \text{Cn } T \setminus \text{Th } \mathcal{N} \qquad \Longrightarrow \qquad \text{Cn } T \neq \text{Th } \mathcal{N}$$

2. $T \nvdash G$: Tällöin lause G on tosi väite, mutta T ei todista sitä.

$$G \in \text{Th } \mathcal{N} \setminus \text{Cn } T \qquad \Longrightarrow \qquad \text{Cn } T \neq \text{Th } \mathcal{N}$$

Teorioille, jotka todistavat vain tosia lauseita, pätee lisäksi $T \nvdash \neg G$. Tällöin sanotaan, että lause G on *riippumaton* teoriasta T.

□

Gödelin lause on matemaattisen logiikan merkittävin tulos. Sen katsotaan romahduttaneen Hilbertin ohjelman: mistään aksiomatisoinnista ei voida johtaa kaikkia matematiikan totuuksia ja vain niitä. Tässä Gödelin lause muotoiltiin predikaattilogiikan $\mathcal{L}_{\mathcal{N}}$-teorioille; usein se esitetään yleisemmässäkin muodossa:

> Mikään virheetön päättelyjärjestelmä, joka kykenee käsittelemään aritmetiikkaa, ei ole täydellinen. [6, s. 16]

Vaikka Gödelin G-lause on keinotekoisesti rakennettu, filosofisen merkityksensä lisäksi lause koskettaa matemaatikkoja käytännössäkin. Esimerkiksi Zermelon-Fraenkelin aksiomatisoinnin epätäydellisyys tulee vastaan jo yksinkertaisia olemassaolokysymyksiä pohdittaessa, sillä ns. valinta-aksiooma (engl. axiom of choice) on riippumaton ZF-aksioomista. Jos ZF-teoriaan lisätään valinta-aksiooma (ZFC), Gödelin tulos takaa tässäkin järjestelmässä riippumattomien väitteiden olemassaolon. Edelleen Cantorilta ratkaisematta jääneen ongelman, kontinuumihypoteesin, todisti ZFC:stä riippumattomaksi Paul Cohen. [3]

4.5 Produktiiviset joukot

Edellä nähtiin, että jokainen yrite T aksiomatisoida lukuteoria epäonnistuu. Olipa T millainen tahansa, ajatellaan, että tällainen aksiomatisointiyritys voidaan antaa rekursiivisesti numeroituvan joukon indeksinä x, s.e. $\lceil \mathrm{Cn}\ T \rceil = W_x$. Jos T todistaa vain tosia väittämiä ($\mathrm{Cn}\ T \subseteq \mathrm{Th}\ \mathcal{N}$), voidaan konstruoida $\mathcal{L}_{\mathcal{N}}$-lause G, joka on tosi ($G \in \mathrm{Th}\ \mathcal{N}$) mutta ei todistuva ($G \notin \mathrm{Cn}\ T$):

$$\text{Annettuna } x \text{ s.e. } W_x \subseteq \lceil \mathrm{Th}\ \mathcal{N} \rceil \xrightarrow{\text{Gödelin konstruktio}} \lceil G \rceil \in \lceil \mathrm{Th}\ \mathcal{N} \rceil \setminus W_x$$

Tosien lauseiden joukko on *efektiivisesti ei-rekursiivisesti numeroituva*, sillä kuvaus, joka muodostaa annetusta r.n. aksiomatisoinnista W_x siitä riippumattoman lauseen G, eli kuvaus $x \mapsto \lceil G \rceil$, on mekaanisesti laskettavissa. Vielä kerran: vastaesimerkki, joka on todiste aksioomien vaillinaisuudelle, voidaan muodostaa konstruktiivisesti lähtemällä aksioomista. Formalisoidaan tämä.

Määritelmä 17. *Joukko $A \subseteq \mathbb{N}$ on* produktiivinen*, jos on olemassa osittaisrekursiivinen funktio $\rho : \mathbb{N} \to \mathbb{N}$ s.e.*

$$W_x \subseteq A \quad \Longrightarrow \quad \rho(x)\!\downarrow \quad \textit{ja} \quad \rho(x) \in A \setminus W_x \ .$$

Joukko $\lceil \mathrm{Th}\ \mathcal{N} \rceil$ on produktiivinen ja sen *produktiofunktio* ρ saadaan seuraamalla todistuksen 11 vaiheita. Tilannetta on havainnollistettu kuvassa 3.

Viedään tätä abstraktiota eteenpäin seuraavassa luvussa.

5 Luovat joukot

Luvuissa 2 ja 3 nähtiin, että joukko K (tai K_0) on rekursiivisesti numeroituva mutta ei rekursiivinen. Lisäksi pääteltiin, että K:n komplementti $\bar{K}$ ei voi olla r.n., koska se tekisi joukosta K rekursiivisen.

Oletetaan, että r.n. joukko W_x luettelee joukon $\bar{K}$ alkioita, eli $W_x \subseteq \bar{K}$. Koska $\bar{K} \neq W_x$, täytyy jokin alkio $k \in \bar{K} \setminus W_x$ jäädä luettelematta. Joukon $\bar{K}$ määritelmän perusteella

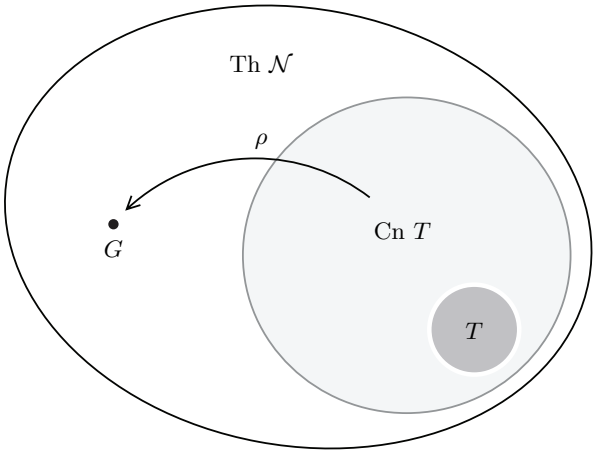
$$x \in W_x \quad \Longleftrightarrow \quad \varphi_x(x)\!\downarrow \quad \Longleftrightarrow \quad x \notin \bar{K} \ , \tag{41}$$

joten jos $x \in W_x$ olisi $W_x \not\subseteq \bar{K}$ vastoin oletusta, eli täytyy olla $x \notin W_x$ ja $x \in \bar{K}$. Saatiin kaikille x:

$$W_x \subseteq \bar{K} \quad \Longrightarrow \quad x \in \bar{K} \setminus W_x \ . \tag{42}$$

Luku x on itsessään konkreettinen todiste tosiasialle $W_x \neq \bar{K}$, ja siten $\bar{K}$ on produktiivinen produktiofunktiolla $\rho(x) = x$. Sanotaan, että K on *luova*.

Määritelmä 18. [5, Post 1944] *Rekursiivisesti numeroituva joukko $A \subseteq \mathbb{N}$ on* luova*, jos $\bar{A}$ on produktiivinen.*



Kuva 3. Lukuteorian tosien lauseiden joukko Th $\mathcal{N}$ (tai tarkemmin $\lceil \text{Th } \mathcal{N} \rceil$) on produktiivinen: jokaisesta sen rekursiivisesti numeroituvasta osajoukosta Cn T (missä T aksiomatisoi Cn T:n), voidaan produktiofunktiolla ρ laskea uusi alkio G, jolle $G \in \text{Th } \mathcal{N} \setminus \text{Cn } T$.

5.1 Luovien joukkojen ominaisuuksia

Aluksi on helppo nähdä, ettei mikään luova joukko A voi olla rekursiivinen, koska joukon komplementti $\bar{A}$ ei ole produktiivisena joukkona rekursiivisesti numeroituva.

Vaikka $\bar{A}$ ei ole r.n., sille saadaan rakennettua ääretön r.n. osajoukko.

Lause 12. *Olkoon $A \subseteq \mathbb{N}$ luova. On olemassa ääretön r.n. joukko B s.e. $B \subseteq \bar{A}$.*

Todistus. Olkoon $\rho : \mathbb{N} \to \mathbb{N}$ produktiivinen osittaisrekursiivinen funktio joukolle $\bar{A}$. Tietenkin $\varnothing \subseteq \bar{A}$, joten jos $e_1 \in \mathbb{N}$ on tyhjän funktion indeksi ($W_{e_1} = \varnothing$), saadaan $\rho(e_1) \in \bar{A} \setminus W_{e_1}$. Edelleen $\{\rho(e_1)\} \subseteq \bar{A}$, joten kun $e_2 \in \mathbb{N}$ on sellainen, että $W_{e_2} = \{\rho(e_1)\}$ saadaan uusi alkio $\rho(e_2) \in \bar{A} \setminus W_{e_1}$ ja joukko $\{\rho(e_1), \rho(e_2)\} \subseteq \bar{A}$. Seuraavaksi etsitään $e_3 \in \mathbb{N}$, jolle $W_{e_3} = \{\rho(e_1), \rho(e_2)\}$, ja sovelletaan taas produktiofunktiota. Kuvattu prosessi on mekaaninen ja näin jatkamalla syntyy ääretön $B = \{\rho(e_1), \rho(e_2), \rho(e_3), \ldots\} \subseteq \bar{A}$.

Muodollisempi johto on annettu liitteenä. □

Tämä tulos kertoo muun muassa sen, etteivät luovat joukot voi olla *yksinkertaisia joukkoja* Postin mielessä (s. 17). Lisäksi koska edellinen tulos pätee mille tahansa produktiiviselle joukolle, sen voi tulkita päättelyjärjestelmien tapauksessa niinkin, että aksiomatisoituja teorioita $T \subseteq \text{Th } \mathcal{N}$ voidaan laajentaa lisäämällä ääretön määrä uusia aksioomia rekursiivisesti numeroituvalla tavalla. Tätä asiaa tutki mm. Turing (1939) [5].

Seuraavaksi tavoitteena on näyttää:

Lause 13. *Jos $A \subseteq \mathbb{N}$ on luova, $B \subseteq \mathbb{N}$ rekursiivisesti numeroituva ja $A \leq_m B$, joukko B on myös luova.*

Tarvitaan kuitenkin ensin apuväite:

Lemma 8. *Jos $f : \mathbb{N} \to \mathbb{N}$ on osittaisrekursiivinen funktio, on olemassa rekursiivinen $h : \mathbb{N} \to \mathbb{N}$ s.e. $W_{h(x)} = f^{-1}(W_x)$.*

Todistus. Kun $f : \mathbb{N} \to \mathbb{N}$ on annettu, määritellään $\psi : \mathbb{N}^2 \to \mathbb{N}$ s.e.

$$\psi(x, y) = \begin{cases} 1, & \text{jos } f(y) \in W_x \\ \nearrow, & \text{muulloin} \end{cases} \tag{43}$$

Koska predikaatti "$f(y) \in W_x$" ($\Leftrightarrow (\varphi_x \circ f)(y)\downarrow$) on r.n., ψ on laskettava. Kleenen s-m-n-lause antaa funktion $h : \mathbb{N} \to \mathbb{N}$ s.e. $\varphi_{h(x)}(y) \simeq \psi(x, y)$, mikä määrittelyjoukkojen puolella tarkoittaa

$$W_{h(x)} = \text{Dom } \varphi_{h(x)} = \text{Dom } \psi(x, \cdot) = \text{Dom } \varphi_x \circ f = f^{-1}(W_x) \ .$$

□

Todistus (Lauseelle 13). Olkoon A luova produktiofunktiolla ρ, B r.n. ja $f : A \leq_m B$. Koska B on jo oletuksen nojalla r.n., riittää näyttää joukko $\bar{B}$ produktiiviseksi.

Väitetään, että $f \circ \rho \circ h$ on produktiofunktio $\bar{B}$:lle, missä $h : \mathbb{N} \to \mathbb{N}$ on saatu edellisellä lemmalla funktiosta f. Kaavio selventänee.

$$\begin{array}{ccc} W_{h(x)} \subseteq \bar{A} & \xleftarrow{\quad h \quad} & W_x \subseteq \bar{B} \\ \Big\downarrow{\scriptstyle \rho} & & \Big\downarrow{\scriptstyle f \circ \rho \circ h} \\ (\rho \circ h)(x) \in \bar{A} \setminus W_{h(x)} & \xrightarrow{\quad f \quad} & (f \circ \rho \circ h)(x) \in \bar{B} \setminus W_x \end{array}$$

1. Olkoon $W_x \subseteq \bar{B}$. Joukko $f^{-1}(W_x)$ on joukon $\bar{A}$ r.n. osajoukko, koska f on palautus. Joukon $f^{-1}(W_x)$ indeksi $h(x)$ saatiin efektiivisesti edellisellä lemmalla.
2. Nyt $f^{-1}(W_x) = W_{h(x)} \subseteq \bar{A}$, joten käytetään $\bar{A}$:n produktiofunktiota ja saadaan $\rho(h(x)) \in \bar{A}$, mutta $\rho(h(x)) \notin W_{h(x)}$.
3. Käytetään vielä palautusta f, jolloin $f(\rho(h(x))) \in \bar{B}$. Jos olisi $f(\rho(h(x))) \in W_x$, niin olisi myös $\rho(h(x)) \in f^{-1}(W_x) = W_{h(x)}$, ristiriita. Siis $f(\rho(h(x))) \notin W_x$ ja saatiin funktiosta $f \circ \rho \circ h$ produktiofunktio joukolle $\bar{B}$.

□

Äskeinen tulos kertoo, että luovuus periytyy ylöspäin rekursiivisesti numeroituvien joukkojen luokassa osittainjärjestyksen $\leq_m$ suhteen. Koska K on luova ja se voidaan palauttaa mihin tahansa m-täydelliseen joukkoon, saadaan seurauslause

Seuraus 5. *A on m-täydellinen $\implies$ A on luova.*

Tämän luvun yksi tavoite on näyttää, että tässä implikaatio pätee toiseenkin suuntaan.

5.2 Kleenen kiintopistelause

Gödelin G-lauseen konstruktiossa käytettiin implisiittisesti yleisempää periaatetta, Gödelin kiintopistelausetta, jolla mille tahansa yhden vapaan muuttujan $\mathcal{L}_\mathcal{N}$-kaavalle $\phi(x)$ voidaan rakentaa $\mathcal{L}_\mathcal{N}$-lause σ, jolle pätee

$$\mathcal{N} \vDash \sigma \qquad \Longleftrightarrow \qquad \mathcal{N} \vDash \phi(\underline{\lceil \sigma \rceil}) \ ,$$

eli σ väittää "Tämän lauseen Gödel-luvulla on lukuteoreettinen ominaisuus ϕ". Lause σ on näin määritelty itseviittaavasti.

Laskettavuusteorian analogia tälle on *Kleenen kiintopistelause* tai *rekursiolause*. Sen avulla osittaisrekursiivisia funktioita voidaan määritellä itseviittaavasti siinä mielessä, että funktion määritelmässä saadaan viitata funktion omaan Gödel-lukuun. Väitteen voi tulkita myös niin, että laskettavalla ohjelmalla on tällä tavalla pääsy omaan lähdekoodiinsa.

Lause voidaan esittää monilla eri tavoilla. Käytetään tässä työn jatkon kannalta riittävää muotoilua.

Lause 14 (Kleenen kiintopistelause). *Olkoon $\psi : \mathbb{N}^3 \to \mathbb{N}$ osittaisrekursiivinen funktio. On olemassa rekursiivinen injektio $k : \mathbb{N} \to \mathbb{N}$ s.e. kaikilla $x, z \in \mathbb{N}$:*

$$\varphi_{k(x)}(z) \simeq \psi(k(x), x, z) \ .$$

Todistus. [13, luku 11.2] Määritellään osittaisrekursiivinen $\tau : \mathbb{N}^3 \to \mathbb{N}$ seuraavasti

$$\tau(u,x,z) = \begin{cases} \varphi_{\varphi_u^{(2)}(u,x)}(z), & \text{jos } \varphi_u^{(2)}(u,x)\downarrow \\ \nearrow, & \text{jos } \varphi_u^{(2)}(u,x)\uparrow \end{cases} \tag{44}$$

Voidaan merkitä lyhyesti $\tau(u,x,z) \simeq \varphi_{\varphi_u^{(2)}(u,x)}(z)$, kun lausekkeella $\varphi_{\varphi_u^{(2)}(u,x)}$ tarkoitetaan funktiota joka hajaantuu, jos $\varphi_u^{(2)}(u,x)$ hajaantuu tai jos $\varphi_u^{(2)}(u,x) = i$ suppenee ja φ_i hajaantuu. Olkoon $h : \mathbb{N}^2 \to \mathbb{N}$ sellainen injektio, että $\varphi_{h(u,x)}(z) = \tau(u,x,z)$ (s-m-n-lauseella). Tähän mennessä ollaan saatu

$$\varphi_{h(u,x)} = \varphi_{\varphi_u^{(2)}(u,x)} \ . \tag{45}$$

Olkoon sitten $\psi : \mathbb{N}^3 \to \mathbb{N}$ annettuna ja konstruoidaan $k : \mathbb{N} \to \mathbb{N}$. Ensin olkoon $s : \mathbb{N}^2 \to \mathbb{N}$ s.e.

$$\varphi_{s(x,y)}(z) \simeq \psi(x,y,z) \tag{46}$$

ja $v \in \mathbb{N}$ funktion $(u,x) \mapsto s(h(u,x),x)$ Gödel-luku,

$$\varphi_v^{(2)}(u,x) \simeq s(h(u,x),x) \ . \tag{47}$$

Nyt

$$k(x) = h(v,x) \tag{48}$$

on totaali rekursiivinen injektio, koska funktio h on. Tarkistetaan, että tämä todella toteuttaa väittämän:

$$\begin{aligned} \varphi_{k(x)}(z) &\simeq \varphi_{h(v,x)}(z) \simeq \varphi_{\varphi_v^{(2)}(v,x)}(z) \\ &\simeq \varphi_{s(h(v,x),x)}(z) \simeq \varphi_{s(k(x),x)}(z) \simeq \psi(k(x),x,z) \end{aligned}$$

□

Esimerkki 7. Lauseella 13 saataisiin produktiofunktio joukolle $\bar{K}_0$ suoraan palautuksen $K \leq_m K_0$ kautta, mutta kokeillaan konstruoida tällainen kiintopistelauseen avulla.

Määritellään

$$\psi(x,y,z) = \begin{cases} 1, & \text{jos } \langle x,z\rangle \in W_y \\ \nearrow, & \text{muulloin} \end{cases} \tag{49}$$

jolloin käyttämällä kiintopistelausetta saadaan $k : \mathbb{N} \to \mathbb{N}$ s.e.

$$\varphi_{k(x)}(z) \simeq \psi(k(x),x,z) = \begin{cases} 1, & \text{jos } \langle k(x),z\rangle \in W_x \\ \nearrow, & \text{muulloin} \end{cases} \tag{50}$$

Nythän $\varphi_{k(x)}(0)\!\downarrow \Leftrightarrow \langle k(x),0\rangle \in W_x$ eli kun $W_x \subseteq \bar{K}_0$ on annettu, funktio, jonka indeksi on $k(x)$, kysyy laskentansa aikana joukolta W_x "Hajaantuuko ohjelman $k(x)$ laskenta?" tai toisin sanoen "Hajaantuuko tämän ohjelman laskenta?". Ohjelma $k(x)$ todella hajaantuu esimerkiksi syötteellä 0, mutta W_x ei pysty kertomaan tätä: jos olisi $\langle k(x),0\rangle \in W_x$, ohjelma $k(x)$ saisi tämän selville ja pysähtyisi heti. Siis $\langle k(x),0\rangle \in \bar{K}_0 \setminus W_x$ ja kuvaus $\rho(x) = \langle k(x),0\rangle$ on produktiofunktio joukolle $\bar{K}_0$.

Jos haetaan analogiaa edellisen luvun tarkasteluiden kanssa, voitaisiin sanoa, että lause "$\langle k(x),0\rangle \in \bar{K}_0$" on tosi väite, joka ei kuitenkaan ole todistuva aksiomatisoinnista W_x, joka todistaa vain tosia väittämiä ($W_x \subseteq \bar{K}_0$).

5.3 Luovien joukkojen 1-täydellisyys

Aloitetaan teknisellä lemmalla.

Lemma 9. *Luovien joukkojen määritelmässä 18 voidaan osittaisrekursiivinen produktiofunktio $\rho : \mathbb{N} \to \mathbb{N}$ korvata injektiivisellä rekursiivisella produktiofunktiolla $p : \mathbb{N} \to \mathbb{N}$.*

Todistus. Konstruoidaan annetusta osittaisrekursiivisesta produktiofunktiosta ρ ensin totaalinen produktiofunktio p' ja lopuksi täydennetään se injektiiviseksi funktioksi p.

Olkoon A luova, $\rho : \mathbb{N} \to \mathbb{N}$ produktiofunktio sen komplementille ja W_x annettuna. Kuvaillaan rekursiivisen funktion $p' : \mathbb{N} \to \mathbb{N}$ laskenta epämuodollisesti. Kaksi mahdollisuutta.

1. $W_x \subseteq \bar{A}$: Tällöin $\rho(x)\!\downarrow$ oletuksen nojalla, joten voidaan asettaa $p'(x) = \rho(x)$.
2. $W_x \nsubseteq \bar{A}$: W_x ($\neq \varnothing$) ja A ($\neq \varnothing$) ovat r.n. joukkoja, joten tässä $W_x \cap A \neq \varnothing$. Listataan molempien joukkojen alkioita ja jossain vaiheessa löydetään jokin $k \in W_x \cap A$. Asetetaan vaikka $p'(x) = 0$.

Lasketaan kohtia 1 ja 2 rinnakkain. Jompikumpi näistä prosesseista pysähtyy ensimmäisenä, joten näin määritelty p' on totaali funktio ja yhä produktiofunktio joukolle $\bar{A}$.

Jotta produktiofunktiosta saataisiin lisäksi injektiivinen, määritellään $p : \mathbb{N} \to \mathbb{N}$ funktion p' avulla rekursiivisesti: Pohjatapauksena asetetaan $p(0) = p'(0)$. Kun $x \geq 1$ on annettu, kuvaillaan funktion arvon $p(x)$ laskenta. Olkoon $D = \{p(0), p(1), \ldots, p(x-1)\}$ funktion aiemmat arvot sisältävä joukko. Jos $p'(x) \notin D$, asetetaan $p(x) = p'(x)$. Muulloin $p'(x) = p(i)$ jollakin $0 \leq i \leq x-1$, jolloin käytetään tuttua tekniikkaa: Otetaan sellainen $e_1 \in \mathbb{N}$, että $W_{e_1} = \{p(i)\}$ ja lasketaan jonon $S = \{p'(e_1), p'(e_2), p'(e_3), \ldots\}$ alkioita, missä $e_{n+1} \in \mathbb{N}$ valitaan aina siten, että

$$W_{e_{n+1}} = \{p'(e_1), \ldots, p'(e_n)\}$$

aivan kuten lauseen 12 todistuksessa. Tilanne jakautuu kahteen tapaukseen.

1. Jos oli $W_x \subseteq \bar{A}$ eli $p'(x) = p(i) \in \bar{A}$, jonoa S laskemalla löydetään lopulta käypä $p'(e_N) \in \bar{A} \setminus W_x$, missä $p'(e_N) \notin D$ ja $N \leq |D| + 1$, koska jonon S alkiot ovat keskenään erisuuria. Asetetaan $p(x) = p'(e_N)$.
2. Toisaalta jos $W_x \nsubseteq \bar{A}$ eli $p(i) \notin \bar{A}$, on mahdollista että jonon S laskennassa törmätään kahteen yhtäsuureen alkioon. Jos näin käy, tiedetään siis, että $W_x \nsubseteq \bar{A}$ ja funktion arvoksi $p(x)$ voidaan valita mitä tahansa, kunhan ei rikota funktion injektiivisyyttä, esimerkiksi $p(x) = \max D + 1$.

Näin rakennettuna funktio p on lopulta injektiivinen kaikilla $x \in \mathbb{N}$ ja toteuttaa produktiofunktion vaatimukset. □

Seuraavaksi siirrytään tarkastelemaan lauseita, jotka John Myhill on todistanut vuonna 1955 artikkelissaan "Creative sets" [10]. Ensimmäisenä katsotaan, kuinka mikä tahansa r.n. ongelma voidaan 1-palauttaa mielivaltaiseen luovaan joukkoon.

Lause 15 (Myhill). *A on luova $\implies$ A on 1-täydellinen.*

Todistus. Olkoon A luova ja edellisen lemman nojalla $p : \mathbb{N} \to \mathbb{N}$ totaali injektiivinen produktiofunktio joukolle $\bar{A}$. Kun B on r.n. joukko, täytyy näyttää $B \leq_1 A$.

Määritellään $\psi : \mathbb{N}^3 \to \mathbb{N}$ s.e.

$$\psi(x, y, z) = \begin{cases} 1, & \text{jos } y \in B \text{ ja } z = p(x) \\ \nearrow, & \text{muulloin} \end{cases} \tag{51}$$

Funktio ψ on laskettava, sillä se on r.n. predikaatin "$y \in B \wedge z = p(x)$" puolikarakteristinen funktio. Kun tähän sovelletaan kiintopistelausetta, saadaan $\varphi_{k(x)}(z) \simeq \psi(k(x), x, z)$, mikä on määrittelyjoukkojen avulla ilmaistuna

$$W_{k(x)} = \text{Dom } \psi(k(x), x, \cdot) = \begin{cases} \{p(k(x))\}, & \text{jos } x \in B \\ \varnothing, & \text{muulloin} \end{cases} \tag{52}$$

Kaksi tapausta.

1. $x \in B$: Jos olisi $p(k(x)) \notin A$ eli $W_{k(x)} = \{p(k(x))\} \subseteq \bar{A}$, niin produktiofunktiolla $p(k(x)) \in \bar{A} \setminus \{p(k(x))\}$, ristiriita! Siis $p(k(x)) \in A$.
2. $x \notin B$: Tällöin $W_{k(x)} = \varnothing \subseteq \bar{A}$, jolloin produktiofunktiolla $p(k(x)) \in \bar{A}$ eli $p(k(x)) \notin A$.

Nähtiin, että $x \in B \iff (p \circ k)(x) \in A$ eli koska p ja k ovat injektioita, $p \circ k : B \leq_1 A$. □

Luovien joukkojen kautta saadaan kaunis karakterisaatio 1- ja m-täydellisille joukoille. Vaikka $A \equiv_m B \Rightarrow A \equiv_1 B$ ei yleisesti ole voimassa, m-täydellisten joukkojen tapauksessa tilanne on yksinkertainen.

Seuraus 6. *A on 1-täydellinen $\iff$ A on m-täydellinen $\iff$ A on luova.*

Todistus. "A on 1-täydellinen $\Rightarrow$ A on m-täydellinen" suoraan määritelmästä. Implikaatio "A on m-täydellinen $\Rightarrow$ A on luova" saatiin seurauslauseena 5 ja juuri nähtiin "A on luova $\Rightarrow$ A on 1-täydellinen". □

Erityisesti jokainen luova joukko on 1-ekvivalentti pysähtymisongelman K kanssa. Koska K on sylinteri, kaikki m-täydelliset joukot ovat myös sylintereitä. Viimeisessä luvussa esiteltävä Myhillin isomorfialause luonnehtii m-täydellisten joukkojen luokan $\mathbf{0}'_m$ rakennetta vielä tätäkin tarkemmin.

6 Myhillin isomorfialause

Onko olemassa vielä vahvempaa päätösongelmien palautuvuuskäsitettä kuin 1-palautukset? Myhillin isomorfialause tarjoaa tähän kysymykseen negatiivisen vastauksen.

Lause 16 (Myhill [10]**).** *Kaikille $A, B \subseteq \mathbb{N}$ pätee $A \equiv_1 B \implies A \equiv B$.*

Keskenään 1-ekvivalentit joukot ovat rekursiivisesti isomorfisia, eli 1-asteiden luokka $\boldsymbol{\mathcal{D}}_1$ muodostuu täsmälleen eri isomorfiatyypeistä, laskettavuusteorian peruselementeistä.

Ennen kuin lauseelle 16 annetaan todistus, etsitään motivaatiota tälle perinteisen joukko-opin tuloksista. Luvun lopuksi muotoillaan vielä yhteenvetona matemaattisen logiikan tulkintaa Myhillin lauseelle.

6.1 Cantor-Schröder-Bernstein lause

Mille tahansa joukoille X ja Y kirjoitetaan $|X| = |Y|$, jos joukot X ja Y ovat yhtä mahtavat eli on olemassa bijektio $h : X \to Y$. Lisäksi merkitään $|X| \leq |Y|$, jos on olemassa injektio $f : X \to Y$. Cantorin-Schröderin-Bernsteinin tulos oikeuttaa tämän notaation käytön.

Lause 17 (Cantor-Schröder-Bernstein). *Jos* $|X| \leq |Y|$ *ja* $|Y| \leq |X|$, *niin* $|X| = |Y|$.

Kun annettuna on injektiot $f : X \to Y$ ja $g : Y \to X$, lauseen todistus vaatii bijektion $h : X \to Y$ konstruointia. Todistuksen ideana on osittaa molemmat joukot X ja Y kahteen pistevieraaseen osajoukkoon

$$X = X_1 \cup X_2 \qquad \text{ja} \qquad Y = Y_1 \cup Y_2 \tag{53}$$

siten, että kuvausten f ja g^{-1} rajoittumat sopiviin osajoukkoihin olisivat bijektioita:

$$f : X_1 \to Y_1 \ \textit{bijektio} \qquad \text{ja} \qquad g^{-1} : X_2 \to Y_2 \ \textit{bijektio} \ . \tag{54}$$

Tällöin voitaisiin määritellä $h : X \to Y$ seuraavasti

$$h(x) = \begin{cases} f(x), & \text{jos } x \in X_1 \\ g^{-1}(x), & \text{jos } x \in X_2 \end{cases} \tag{55}$$

Ongelmana on siis löytää toimivat ositukset.

Jos funktiolle $f \circ g : Y \to Y$ kirjoitetaan $(f \circ g)^{(0)} = \mathrm{id}$ ja $(f \circ g)^{(n+1)} = (f \circ g) \circ (f \circ g)^{(n)}$, esimerkiksi lähteessä [2, ss. 26–27] on annettu lauseelle 17 todistus, jossa valitaan

$$Y_2 = \{(f \circ g)^{(n)}(y) \in Y \mid n \in \mathbb{N},\ y \in Y \setminus f(X)\} \tag{56}$$

ja $X_2 = g(Y_2)$. Valitettavasti tämä konstruktio yleisille X ja Y ei ole riittävän efektiivinen: vaikka kuvaukset f ja g olisivat rekursiivisia funktioita, näin määriteltynä predikaatti "$x \in X_2$" ei silti ole rekursiivinen, eikä todistusta voida suoraan soveltaa Myhillin lauseen tapauksessa. Tarvitaan toisenlaista lähestymistapaa.

6.2 Myhillin isomorfialause

Kun injektiot $f : A \leq_1 B$ ja $g : A \leq_1 B$ ovat annettuina, kuinka näistä voitaisiin rakentaa rekursiivinen bijektio $h : \mathbb{N} \to \mathbb{N}$, jolle myös $h : A \leq_1 B$?

Lähdetään konstruoimaan funktiota h vaiheittain äärellisten vastaavuuksien avulla.

Määritelmä 19. *Äärellinen osittaisfunktio*

$$\theta = \{(x_1, y_1), (x_2, y_2), \ldots, (x_k, y_k)\} : \mathbb{N} \to \mathbb{N} \tag{57}$$

on äärellinen vastaavuus joukolta A joukolle B, *jos* θ *on injektiivinen ja*

$$x_i \in A \quad \Longleftrightarrow \quad \theta(x_i) = y_i \in B \ . \tag{58}$$

Äärellisiä osittaisfunktioita voidaan käsitellä laskennallisesti koodaamalla pareja parifunktiolla ja äärellisiä joukkoja esimerkiksi kuvauksella

$$\{a_1, \ldots, a_k\} \longmapsto \sum_{i=1}^{k} 2^{a_i} \ . \tag{59}$$

Lemma 10. *Olkoon $\theta = \{(x_1, y_1), \ldots, (x_k, y_k)\}$ äärellinen vastaavuus joukolta A joukolle B, $A \leq_1 B$ ja $n \in \mathbb{N}$ mielivaltainen. Tällöin voidaan efektiivisesti etsiä $m \in \mathbb{N}$ s.e. $\theta \cup \{(n, m)\}$ on myös äärellinen vastaavuus joukkojen A ja B välillä.*

Todistus. Olkoon θ annettu kuten yllä, $f : A \leq_1 B$ ja $n \in \mathbb{N}$. Jos $n = x_i$ jollakin $1 \leq i \leq k$, väite on selvä, joten oletetaan $n \neq x_i$ kaikilla $1 \leq i \leq k$.

Lasketaan ensiksi $f(n)$. Jos $f(n) \neq y_i$ kaikilla $1 \leq i \leq k$, voidaan valita $m = f(n)$, jolloin laajennettu joukko $\theta \cup \{(n, m)\}$ on yhä vastaavuus, koska f on palautus: $n \in A \Leftrightarrow m = f(n) \in B$. Toisaalta jos $f(n) = y_{i_0}$ jollakin $1 \leq i_0 \leq k$, lasketaan seuraavaksi $f(x_{i_0})$. Huomataan, että

$$n \in A \Leftrightarrow f(n) = y_{i_0} \in B \Leftrightarrow x_{i_0} \in A \Leftrightarrow f(x_{i_0}) \in B \ , \tag{60}$$

joten jos $f(x_{i_0}) \neq y_j$ kaikilla $1 \leq j \leq k$, voidaan valita $m = f(x_{i_0})$. Jos vieläkin $f(x_{i_0}) = y_{i_1}$ jollakin $1 \leq i_1 \leq k$, lasketaan seuraavaksi $f(x_{i_1})$. Tätä prosessia jatkamalla syntyy jono $i_0, i_1, i_2 \ldots$ indeksejä, missä päättelyä (60) toistamalla saadaan

$$n \in A \Leftrightarrow f(x_i) \in B \text{ kaikilla } i = i_0, i_1, \ldots \ . \tag{61}$$

Joko löydetään $m = f(x_{i_N})$ s.e. $m \neq y_j$ kaikilla $1 \leq j \leq k$ tai jonoa laskettaessa törmätään kahteen samaan indeksiin: $i_p = i_q$, $p \neq q$. Osoitetaan, että näin ei voi käydä.

Jos olisi $i_p = i_q$, $p < q$, saataisiin $y_{i_p} = y_{i_q}$ eli $f(x_{i_{p-1}}) = f(x_{i_{q-1}})$ ja koska f on injektiivinen, $x_{i_{p-1}} = x_{i_{q-1}}$ eli $i_{p-1} = i_{q-1}$. Jatkamalla samaa päättelyä päädytään identiteettiin $i_0 = i_{q-p} = i_l$, $l > 0$. Nythän $f(n) = y_{i_0} = y_{i_l} = f(x_{i_{l-1}})$, josta f:n injektiivisyydellä seuraa $n = x_{i_{l-1}}$, mikä oli vastoin oletusta $n \neq x_j$ kaikilla $1 \leq j \leq k$. □

Todistus (Myhillin isomorfialause). Olkoon $A \equiv_1 B$ palautuksilla $f : A \leq_1 B$ ja $g : B \leq_1 A$. Tarkoituksena on rakentaa rekursiivinen permutaatio $h : \mathbb{N} \to \mathbb{N}$, jolle $h(A) = B$. Käytetään toistuvasti edellistä lemmaa ja määritellään induktiivisesti jono $\theta_0 \subseteq \theta_1 \subseteq \theta_2 \subseteq \cdots$ äärellisiä vastaavuuksia joukkojen A ja B välille. Tarkastellaan rakentuvaa vastaavuutta θ_i vuorotellen lähtö- ja kuvapuolelta.

1. θ_0: Asetetaan

$$\theta_0 = \begin{cases} \{(0,0)\}, & \text{jos } f(0) = 0 \text{ tai } g(0) = 0 \\ \{(0, f(0)), (g(0), 0)\}, & \text{muulloin} \end{cases} \tag{62}$$

   Selvästi θ_0 on äärellinen vastaavuus.

2. θ_{2n-1}, $n \geq 1$: Oletetaan, että θ_{2n-2} on konstruoitu. Käytetään edellistä lemmaa kääntäen:

$$\hat{\theta}_{2n-2} = \{(y_i, x_i) \in \mathbb{N} \times \mathbb{N} \mid (x_i, y_i) \in \theta_{2n-2}\}$$

   on äärellinen vastaavuus joukolta B joukolle A, joten palautuksella g saadaan efektiivisesti laajennettu vastaavuus $\hat{\theta}_{2n-1} = \hat{\theta}_{2n-2} \cup \{(n, m)\}$ jollekin $m \in \mathbb{N}$. Lopulta asetetaan

$$\theta_{2n-1} = \{(x_i, y_i) \in \mathbb{N} \times \mathbb{N} \mid (y_i, x_i) \in \hat{\theta}_{2n-1}\} \ .$$

3. θ_{2n}, $n \geq 1$: Oletetaan, että θ_{2n-1} on konstruoitu. Käyttämällä palautusta f löydetään efektiivisesti $m \in \mathbb{N}$ s.e. $\theta_{2n} = \theta_{2n-1} \cup \{(n, m)\}$ on äärellinen vastaavuus.

Tässä kaikilla $n \in \mathbb{N}$ pätee $n \in \text{Dom } \theta_{2n}$ ja $n \in \text{Im } \theta_{2n}$, joten jos määritellään funktio $h : \mathbb{N} \to \mathbb{N}$ s.e.

$$h(x) = \theta_{2x}(x) \ , \tag{63}$$

saadaan rekursiivinen funktio, koska äärellisen vastaavuuden θ_{2x} konstruointi on rekursiivista jokaiselle kiinteälle luvulle x. Lisäksi

$$h = \bigcup_{n \in \mathbb{N}} \theta_n \ , \tag{64}$$

joten $\text{Im } h = \text{Dom } h = \mathbb{N}$ ja koska h on konstruktion nojalla injektiivinen, h on rekursiivinen permutaatio. Äärelliset vastaavuudet takaavat, että h on palautus. Siis $f(A) = B$ ja $A \equiv B$. □

Seuraus 7. *Olkoon $A \subseteq \mathbb{N}$. Seuraavat ovat yhtäpitäviä.*

1. *A on 1-täydellinen.*
2. *A on m-täydellinen.*
3. *A on luova.*
4. *$A \equiv K$.*

Nähtiin, että m-täydellisten joukkojen luokka $\mathbf{0}'_m$ on isomorfiatyyppi, laskettavuusteorian kannalta yksinkertaisin mahdollinen. Jokainen vaikea r.n. päätösongelma on instanssien laskennallista uudelleenjärjestämistä vaille identtinen pysähtymisongelman kanssa.

6.3 Loppusanat

Luvun 2 johdannossa esiteltiin Hilbertin *Entscheidungsproblem*:

K3. Voidaanko annetusta predikaattilogiikan lauseesta mekaanisesti päättää onko lause pätevä?

Matemaattisen logiikan tarkastelut auttavat nyt tarkentamaan kysymystä lukuteorian yhteydessä. Peanon aritmetiikan tapauksessa voidaan kysyä

K3*. Annettuna on $\mathcal{L}_{\mathcal{N}}$-lause σ. Mikä seuraavista pätee?
   (a) $\text{PA} \vdash \sigma$, eli lause on todistuva Peanon aksioomista.
   (b) $\text{PA} \vdash \neg\sigma$, eli lauseen negaatio on todistuva.
   (c) $\text{PA} \nvdash \sigma$ ja $\text{PA} \nvdash \neg\sigma$, eli lause on riippumaton teoriasta PA.

Gödelin lause jätti auki mahdollisuuden sille, että ensimmäisen kertaluvun aksiomatisoituvat teoriat olisivat niin triviaaleja, että vaikka ne eivät kykene todistamaan kaikkia lukuteorian standardimallissa tosia väittämiä, voitaisiin silti mekaanisesti päättää milloin annettu $\mathcal{L}_{\mathcal{N}}$-lause on todistumaton.

Vuoden 1936 artikkeleissaan Alonso Church ja Alan Turing antoivat esimerkkejä aksiomatisoituvista teorioista T, jotka eivät olleet ratkeavia määritelmän 14 mielessä. Eräs muotoilu tälle tulokselle on

Lause 18 (Churchin lause [5, Church 1936]**).** *Hilbertin entscheidungsproblem on ratkeamaton: jos $\mathcal{L}$ on riittävän rikas predikaattilogiikan aakkosto, predikaatti "$\varnothing \vdash \sigma$", missä σ on annettu $\mathcal{L}$-lause, ei ole ratkeava.*

Todistus. Ks. [9] □

Esimerkiksi Peanon aritmetiikka on niin vahva teoria, että joukko $\lceil \text{Cn PA} \rceil$ ei ole rekursiivinen. Itse asiassa

Lause 19. *Rekursiiviset funktiot ovat* esitettäviä *Peanon aritmetiikassa, eli jokaiselle rekursiiviselle funktiolle* $f : \mathbb{N}^n \to \mathbb{N}$ *ja kaikille* $\vec{x} \in \mathbb{N}^n$ *ja* $y \in \mathbb{N}$ *pätee*

$$\begin{aligned} f(\vec{x}) = y \quad &\Longrightarrow \quad \mathrm{PA} \vdash \sigma_f(\underline{x_1}, \ldots, \underline{x_n}, \underline{y}) \\ f(\vec{x}) \neq y \quad &\Longrightarrow \quad \mathrm{PA} \vdash \neg\sigma_f(\underline{x_1}, \ldots, \underline{x_n}, \underline{y}) \ , \end{aligned}$$

missä $\sigma_f(x, y)$ *on funktion* f *määrittelevä* $\mathcal{L}_{\mathcal{N}}$*-kaava.*

Todistus. Ks. [9] □

Peanon aritmetiikassa voidaan todistaa rekursiivisten funktioiden arvoja. Olkoon $f : \mathbb{N} \to \mathbb{N}$ rekursiivinen s.e. Im $f = K$ ja $\sigma_f(x, y)$ tämän määrittelevä $\mathcal{L}_{\mathcal{N}}$-kaava. Nythän

$$x \in K \quad \Longleftrightarrow \quad \mathrm{PA} \vdash \exists y : \sigma_f(\underline{x}, y) \quad \Longleftrightarrow \quad \lceil \exists y : \sigma_f(\underline{x}, y) \rceil \in \lceil \mathrm{Cn\ PA} \rceil \ , \tag{65}$$

joten $x \mapsto \lceil \exists y : \sigma_f(\underline{x}, y) \rceil : K \leq_m \lceil \mathrm{Cn\ PA} \rceil$. Jos merkkijonojen koodauksista ei niin huolehdita, voidaan sanoa, että

Seuraus 8. *Joukko* Cn PA *on m-täydellinen.*

Kaikki matemaattisesti mielenkiintoiset teoriat—PA:n lisäksi esimerkiksi ZFC tai PM—voidaan todistaa m-täydellisiksi tämäntyyppisillä palautuksilla: nämä teoriat ovat riittävän vahvoja puhuakseen (osittais)rekursiivisista funktioista. Myhill korosti artikkelissaan, että koska kaikki luonnolliset todistusjärjestelmät ovat m-täydellisiä, ne ovat isomorfialauseen nojalla laskennallisessa mielessä notaatiota vaille samat. [10]

Emil Postin mielestä matematiikka on *luovaa*, koska matematiikkaa ei voida mekanisoida ja jokaiselle riittävän vahvalle aksiomatisoinnille löydetään efektiivisesti sellaisia matemaattisia totuuksia, joita nämä aksiomatisoinnit eivät todista. Näin onkin selvää, miksi Post kutsui Cn PA-tyyppisiä joukkoja juuri *luoviksi*. [5, Post 1944]

Millään mekaanisella päättelyllä ei voida ratkaista kaikkia matematiikan äärellisesti esitettäviä ongelmia. Jälkiviisaana on helppo todeta Hilbertin optimismin olleen ennenaikaista: matematiikkaa ei voida aksiomatisoida.

Wir müssen wissen. Wir werden wissen.

David Hilbert (1862-1943)

Lähteet

[1] S. Aaronson, *Great Ideas in Theoretical Computer Science*, Luentomuistiinpanot, 2008. https://stellar.mit.edu/S/course/6/sp08/6.080/.

[2] P. Bhattacharya, S. Jain, and S. Nagpaul, *Basic Abstract Algebra*, Cambridge University Press, 1994.

[3] P. Cohen, *Set Theory and the Continuum Hypothesis*, Addison Wesley Publishing Company, 1966.

[4] N. Cutland, *Computability: An Introduction to Recursive Function Theory*, Cambridge University Press, 1980.

[5] M. Davis, *The Undecidable: Basic Papers on Undecidable Propositions, Unsolvable Problems, and Computable Functions*, Courier Dover Publications, 2004. Viitatut artikkelit:

Gödel 1931 On Formally Undecidable Propositions of the Principia Mathematica and Related Systems. I

Gödel 1946 Remarks Before the Princeton Bicentennial Conference on Problems in Mathematics

Church 1936 An Unsolvable Problem of Elementary Number Theory

Turing 1936 On Computable Numbers, with an Application to the Entscheidungsproblem

Turing 1939 Systems of Logic Based on Ordinals

Kleene 1936 General Recursive Functions of Natural Numbers

Kleene 1943 Recursive Predicates and Quantifiers

Post 1936 Finite Combinatory Processes. Formulation I

Post 1944 Recursively Enumerable Sets of Positive Integers and Their Decision Problems

[6] T. Franzén, *Gödel's theorem: An Incomplete Guide to Its Use and Abuse*, A K Peters, Ltd., 2005.

[7] R. Gandy, *The Confluence of Ideas in 1936*, teoksessa The Universal Turing Machine: A Half-Century Survey, R. Herken, toim., Oxford University Press, USA, 1988.

[8] T. Janhunen, *Logiikka tietotekniikassa: perusteet*, Luentomoniste. TKK, Tietojenkäsittelytieteen laitos, 2008.

[9] B. Kim, *Complete Proofs of Gödel's Incompleteness Theorems*. Luentomoniste. http://math.yonsei.ac.kr/bkim/goedel.pdf.

[10] J. Myhill, *Creative sets*, Zeitschrift fur mathematische Logik und Grundlagen der Mathematik, 1 (1955).

[11] P. Odifreddi, *Classical Recursion Theory. The Theory of Functions and Sets of Natural Numbers*, Studies in Logic and the Foundations of Mathematics, 125 (1989).

[12] P. Orponen, *Tietojenkäsittelyteorian perusteet*, Luentomoniste, 2005.

[13] H. Rogers, *Theory of Recursive Functions and Effective Computability*, McGraw-Hill, 1967.

[14] A. Shen and N. Vereshchagin, *Computable Functions*, American Mathematical Society, 2003.

[15] M. Sipser, *Introduction to the Theory of Computation*, PWS Publishing Company, 1997.

[16] R. Soare, *Computability and Recursion*, The Bulletin of Symbolic Logic, 2 (1996), ss. 284–321. http://www.people.cs.uchicago.edu/~soare/History/compute.pdf.

[17] J. Väänänen, *Matemaattinen logiikka*, Gaudeamus, 1988.

Liitteet

Lause 1. $\pi(x,y) = \frac{1}{2}(x+y)(x+y+1)+x$ *on bijektio.*

Todistus. π **on injektio:** Jos $a+b<a'+b'$, niin

$$\begin{aligned}\pi(a,b) &= \tfrac{1}{2}(a+b)(a+b+1)+a \le \tfrac{1}{2}(a+b+1)^2+\tfrac{1}{2}(a+b)\\ &< \tfrac{1}{2}(a'+b')^2+\tfrac{1}{2}(a'+b') = \tfrac{1}{2}(a'+b')(a'+b'+1)\\ &\le \tfrac{1}{2}(a'+b')(a'+b'+1)+a' = \pi(a',b')\end{aligned}$$

Siis jos $\pi(a,b)=\pi(a',b')$, niin täytyy olla $a+b=a'+b'$. Tällöin $0=\pi(a,b)-\pi(a',b')=a-a'$, josta $a=a'$ ja edelleen $b=b'$.

π **on surjektio:** Olkoon $n\in\mathbb{N}$. Valitaan $k\in\mathbb{N}$ siten että

$$\tfrac{1}{2}k(k+1) \le n < \tfrac{1}{2}(k+1)(k+2).$$

Olkoon x s.e. $\frac{1}{2}k(k+1)+x=n$ (lisäksi pätee $x\in\{0,\dots,k\}$) ja lopuksi $y=k-x$. Saadaan $\pi(x,y)=n$.

□

Lause 2. *Jokaiselle osittaisrekursiiviselle funktiolle* $\varphi_n^{(m)}$ *löytyy ääretön määrä indeksejä,*

$$\varphi_n^{(m)} = \varphi_{t(n,0)}^{(m)} = \varphi_{t(n,1)}^{(m)} = \varphi_{t(n,2)}^{(m)} = \varphi_{t(n,3)}^{(m)} = \cdots,$$

missä $t:\mathbb{N}^2\to\mathbb{N}$ *on rekursiivinen injektio.*

Todistus. [13, s. 86] Sivulla 6 konstruoitiin jo funktio t', jolle pätee kaikilla $n\in\mathbb{N}$

$$y\neq y' \qquad\Longrightarrow\qquad t'(n,y)\neq t'(n,y')\ . \tag{66}$$

Varmistetaan vielä injektiivisyys ensimmäisen muuttujan suhteen.

Määritellään apufunktio $h:\mathbb{N}\to\mathbb{N}$, jonka laskennassa käytetään apuna parifunktiota palauttamaan kahden muuttujan tilanne yksiulotteiseksi, jolloin funktion arvot voidaan määritellä rekursiolla. Merkitään lyhyesti $x=\pi_1(z)$ ja $y=\pi_2(z)$.

$$h(z)=h(\langle x,y\rangle)=\begin{cases} t'(0,0), & \text{jos } \langle x,y\rangle=\langle 0,0\rangle \text{ eli } z=0\\ t'(x,\mu k(t'(x,k)>h(z-1))), & \text{muulloin}\end{cases}$$

Minimalisaatio $\mu k(t'(x,k)>h(z-1))$ pysähtyy kaikilla x ja z, sillä kaavan 66 nojalla $t'(x,k)$ saa mielivaltaisen suuria arvoja, kun k kasvaa.

Funktio h on aidosti kasvava funktio ja siksi injektiivinen. Asetetaan lopuksi $t(x,y)=h(\langle x,y\rangle)$, jolloin funktiolla $t:\mathbb{N}^2\to\mathbb{N}$ on halutut ominaisuudet. □

Lause 4 (Kleenen s**-**m**-**n**-lause).** *Kaikille* $m,n\ge 1$ *on olemassa injektiivinen rekursiivinen funktio* $s_n^m:\mathbb{N}^{m+1}\to\mathbb{N}$ *s.e. kaikille* $z,x_1,\dots,x_m,y_1,\dots,y_n$ *pätee*

$$\varphi^{(n)}_{s_n^m(z,x_1,\dots,x_m)}(y_1,\dots,y_n) \quad\simeq\quad \varphi_z^{(m+n)}(x_1,\dots,x_m,y_1,\dots,y_m)$$

Todistus. Kuvaillaan epämuodollisesti s_n^m-funktion laskeva algoritmi. Huolehditaan vasta lopuksi kuvauksen injektiivisyydestä.

Olkoot z ja $x_1,\dots,x_m$, $m\ge 1$ annettuja. Jos z ei koodaa laillista rakennepuuta tai koodaa rakennepuun funktiolle, joka ottaa vähemmän parametrejä kuin $m+1$,

asetetaan $s_n^m(z,\vec{x}) = 0$ (tyhjän funktion indeksi). Oletetaan siis, että z koodaa $(m+n)$-parametrisen funktion rakennepuun jollekin $n \geq 1$. Puun lehtisolmuissa vain on *R1*-säännöllä saatuja funktioita ja koska $m+n > 1$, täytyy ne olla muotoa Pr_i^{m+n}, jollakin $1 \leq i \leq m+n$. Korvataan lehtisolmujen koodeja seuraavasti:

$$\begin{aligned} \text{Jos } 1 \leq i \leq m: \quad & Pr_i^{m+n} \quad \longmapsto \quad \overbrace{S\cdots S}^{x_i \text{ kpl}}(Z(Pr_1^n)) \\ \text{Jos } m+1 \leq i \leq m+n: \quad & Pr_i^{m+n} \quad \longmapsto \quad Pr_{i-m}^n \end{aligned}$$

Saatu rakennepuu kuvaa nyt n-muuttujan funktiota, jolla on selvästi halutut ominaisuudet. Konstruktio on Churchin-Turingin teesin nojalla rekursiivista ja s_n^m on totaalinen.

Jos funktiosta halutaan lisäksi injektiivinen, voidaan käyttää lauseen 2 t-funktiota. Täydennetään s_n^m injektiiviseksi funktioksi $\widehat{s_n^m}$ määrittelemällä

$$\widehat{s_n^m}(z,x_1,\ldots,x_m) = t(s_n^m(z,x_1,\ldots,x_m), \langle z,x_1,\ldots,x_m\rangle) \ .$$

□

Lemma 7 (Gödelin β-funktiolemma). *On olemassa struktuurissa $\mathcal{N}$ määriteltävä funktio $\beta : \mathbb{N}^2 \to \mathbb{N}$ s.e. kaikille $n \in \mathbb{N}$ ja kaikille jonoille $(x_0,\ldots,x_{n-1}) \in \mathbb{N}^n$ löytyy $z \in \mathbb{N}$ s.e. $\beta(z,i) = x_i$, kaikilla $0 \leq i \leq n-1$.*

Todistus. [11, s. 29] Oletetaan tunnetuksi kiinalainen jakojäännöslause: jos $m_0,\ldots,m_{n-1} \in \mathbb{N}$ ovat pareittain suhteellisia alkulukuja, luonnollinen kuvaus[22] $f : \mathbb{N} \to \mathbb{N}_{m_0} \times \cdots \times \mathbb{N}_{m_{n-1}}$ s.e. $f(x) = (x \bmod m_0,\ldots,x \bmod m_{n-1})$ on surjektio.

Olkoon $(x_0,\ldots,x_{n-1}) \in \mathbb{N}^n$ annettuna. Jos löydetään pareittain suhteelliset alkuluvut $m_0,\ldots,m_{n-1}$, joille $m_i > x_i$, kiinalaisen jakojäännöslauseen nojalla on olemassa luku $k \in f^{-1}(x_0,\ldots,x_{n-1})$, jolloin komponenttifunktion $f_i : \mathbb{N} \to \mathbb{N}_{m_i}$ avulla $f_i(k) = k \bmod m_i = x_i$. Riittää siis löytää riittävän isot pareittain suhteelliset alkuluvut m_i.

Olkoon $d = \max\{x_0,\ldots,x_{n-1},n\}$. Tarkastellaan jonoa

$$1+d!, \quad 1+2d!, \quad 1+3d!, \quad \ldots, \quad 1+(n+1)d! \ .$$

Jos määritellään $m_i = 1+(i+1)d!$ (Huom! $m_i > d \geq x_i$) saadaan n kpl pareittain suhteellisia alkulukuja: Jos alkuluku p jakaa luvut m_i ja m_j $(m_i > m_j)$, p jakaa myös näiden erotuksen $m_i - m_j = 1+(i+1)d! - 1 - (j+1)d! = (i-j)d!$. Jos p jakaa luvun $i-j$, jakaa se myös luvun $d!$, sillä $i-j < n \leq d$. Siis p jakaa luvun $d!$, mutta silloin p jakaa edelleen erotuksen $m_i - (i+1)d! = 1$, joten $p = 1$ ja m_i, m_j ovat suhteellisia alkulukuja.

Määritellään

$$\beta(z,i) = \pi_1(z) \bmod 1+(i+1)\pi_2(z) \ . \tag{67}$$

Edellä esitetyn päättelyn tuloksena kaikille $(x_0,\ldots,x_{n-1}) \in \mathbb{N}^n$ löytyy $d!$ ja k, jolla

$$\beta(\langle k,d!\rangle,i) = k \bmod 1+(i+1)d! = k \bmod m_i = f_i(k) = x_i \quad \text{kaikilla } 0 \leq i \leq n-1$$

eli $\exists z : \forall i \leq n-1 : \beta(z,i) = x_i$.

Jäljellä on katsoa, miksi β on määriteltävä struktuurissa $\mathcal{N}$.

[22] Merkitään $\mathbb{N}_n = \{0,\ldots,n-1\}$.

– Jakojäännös on määriteltävä:

$$x \bmod y = z \quad \Longleftrightarrow \quad \exists k : (k \times \underline{y} + \underline{z} = \underline{x}) \wedge \exists l : (\underline{z} + l = \underline{y}) \wedge \neg(\underline{z} = \underline{y}) \\ = \sigma_{\mathrm{mod}}(\underline{x}, \underline{y}, \underline{z})$$

– Parifunktio on määriteltävä.

$$\pi(x, y) = z \quad \Longleftrightarrow \quad \exists k : (\underline{2} \times k = (\underline{x} + \underline{y}) \times (\underline{x} + \underline{y} + 1) \wedge \underline{z} = k + \underline{x}) \\ = \sigma_{\pi}(\underline{x}, \underline{y}, \underline{z})$$

– Parifunktion käänteisfunktiot ovat määriteltäviä.

$$\pi(z)_1 = x \quad \Longleftrightarrow \quad \exists y : \sigma_{\pi}(\underline{x}, y, \underline{z}) = \sigma_{\pi_1}(\underline{z}, \underline{x}) \\ \pi(z)_2 = y \quad \Longleftrightarrow \quad \exists x : \sigma_{\pi}(x, \underline{y}, \underline{z}) = \sigma_{\pi_2}(\underline{z}, \underline{y})$$

– β-funktio on määriteltävä.

$$\beta(z, i) = x \quad \Longleftrightarrow \quad \exists p_1 : \exists p_2 : (\sigma_{\pi_1}(\underline{z}, p_1) \wedge \sigma_{\pi_2}(\underline{z}, p_2) \ \wedge \\ \sigma_{\mathrm{mod}}(p_1, 1 + (1 + \underline{i}) \times p_2, \underline{x}))$$

□

Lause 12. *Olkoon $A \subseteq \mathbb{N}$ luova. On olemassa ääretön r.n. joukko B s.e. $B \subseteq \bar{A}$.*

Todistus. Toistetaan sivun 25 päättely eksplisiittisemmin. Ensin huomioidaan, että r.n. joukkojen yhdiste on r.n. ja yhdistejoukon indeksi saadaan efektiivisesti lähtöjoukkojen indekseistä: Määritellään osittaisrekursiivinen funktio

$$\psi(x, y, z) = \begin{cases} 1, & \text{jos } \varphi_x(z)\downarrow \text{ tai } \varphi_y(z)\downarrow \\ \nearrow, & \text{muulloin} \end{cases} \tag{68}$$

Funktion ψ laskenta etenee simuloimalla funktioiden φ_x ja φ_y laskentaa yhtäaikaisesti (Lause 3) ja katsomalla pysähtyykö näistä kumpikaan. (Vielä tarkemmin voitaisiin käyttää Kleenen T-predikaattia (s. 9).) Kleenen s-m-n-lause antaa rekursiivisen $u : \mathbb{N}^2 \to \mathbb{N}$ s.e. $\varphi_{u(x,y)}(z) \simeq \psi(x, y, z)$, mikä määrittelyjoukkojen puolella tarkoittaa

$$W_{u(x,y)} = W_x \cup W_y \ .$$

Määritellään vielä $\varphi_{s(x)}(y) \simeq \mu z(y = x)$, jolloin $W_{s(x)} = \{x\}$. (Käytettiin implisiittisesti s-m-n-lausetta.)

Olkoon $e \in \mathbb{N}$ s.e. $W_e = \varnothing$. Kun ρ on joukon $\bar{A}$ osittaisrekursiivinen produktiofunktio, saadaan rekursiolla totaalinen funktio s.e.

$$f(x) = \begin{cases} e, & \text{jos } x = 0 \\ u(f(x-1), s(\rho(f(x-1)))), & \text{jos } x > 1 \end{cases} \tag{69}$$

Tässä pätee kaikilla $i \in \mathbb{N}$, $W_{f(i+1)} = W_{f(i)} \cup \{\rho(f(i))\}$, mikä antaa jonon $W_{f(0)} \subsetneq W_{f(1)} \subsetneq W_{f(2)} \subsetneq \cdots \subseteq \bar{A}$ ja lopulta $\mathrm{Im}\, \rho \circ f \subseteq \bar{A}$ on etsitty ääretön r.n. joukko. □