TARVITAANKO JOUKKO-OPPIA (ENÄÄ)?

Jukka Tuomela
Fysiikan ja matematiikan laitos, Itä-Suomen yliopisto

JOUKKO-OPIN NOUSU JA …

Georg Cantorin luoma joukko-oppi on tullut niin vakiintuneeksi osaksi matematiikkaa, että nykyään on ehkä vaikea kuvitella, miten joukko-oppi ja siihen liittyvät kysymykset aiheuttivat kovia riitoja matemaatikkojen keskuudessa 1800-luvun lopulla ja 1900-luvun alussa. Ennen Cantoria oli vältetty äärettömyyden käsitteen suoraa tutkimista, mutta kun Cantor osoitti, että on olemassa erilaisia äärettömyyden asteita, niin kysymystä ei enää noin vain voinut lakaista maton alle. Tunnetusti Cantorin teoriassa oli ongelmia, jotka myös joukko-opin kannattajat myönsivät. Jostain syystä ei puhuttu ristiriidoista, ehkä sitä pidettiin liian repivänä, vaan käytettiin termejä antinomi ja paradoksi.

Lopulta sitten Zermelo ja Fraenkl rakensivat aksioomasysteemin, joka on edelleen joukko-opin standardi versio: on tapana puhua ZFC-systeemistä, missä C viittaa valinta-aksioomaan. Äärettömien joukkojen asema jäi kuitenkin vaivaamaan. Yksi aksioomistahan sanoo, että äärettömiä joukkoja on olemassa. Perinteisesti aksioomien haluttiin olevan mahdollisimman ”itsestäänselviä”, mutta voiko mitään äärettömän käsitteeseen liittyvää pitää itsestäänselvänä? Tähän ongelmaan tarjottiin kahta vastausta: konstruktivisimi, johon palataan hiukan myöhemmin, ja etenkin David Hilbertin ajama näkemys, jota sitten ruvettiin kutsumaan formalismiksi.

Hilbertin idea oli, että pitäisi olla jokin systeemi, jossa ei suoraan vedottaisi äärettömyyteen, mutta jonka puitteissa kuitenkin voitaisiin käyttää niitä tuloksia ”joihin on totuttu” (Davis, P. , Hersh, R., 1980):

> The goal of my theory is to establish once and for all the certitude of mathematical methods […]. The present state of affairs where we run up against the paradoxes is intolerable. […] If mathematical thinking is defective, where are we to find truth and certitude?

Tavallaan matemaatikot yrittivät paroni von Münchhausenin esimerkkiä noudattaen vetää itsensä ylös suosta saappaanvarsista. Ehkä Münchhausenin tarinat olivat Hilbertin mielilukemistoa.

Joka tapauksessa Hilbertin unelma varmuudesta romahti, kun Kurt Gödel julkaisi kuuluisat epätäydellisyystuloksensa. Nämä tulokset osoittivat, että matematiikan perusteilta oli alun perin vaadittu aivan liikaa, ja piti tyytyä vähempään. Matematiikan perusteitten pohtiminen väheni merkittävästi, koska ei ollut oikein selkeää näkemystä, mihin suuntaan edetä. John (János) von Neumann kommentoi Gödelin tuloksia seuraavasti (von Neumann, 1947).

> I think that it [the controversy about foundations of mathematics] constitutes the best caution against taking the immovable rigour of mathematics too much for granted. This happened in our own lifetime, and I know myself how humiliatingly easily my own views regarding the absolute mathematical truth changed during this episode, and how they changed three times in succession!

Toisaalta Gödelin tulokset olivat erittäin hedelmällisiä matemaattisen logiikan kannalta, ja matemaattinen logiikkahan on edelleenkin aktiivinen tutkimusala. Siitä kuitenkin tuli ikään kuin normaali tutkimusala, kuten vaikkapa kommutatiivinen algebra. Gödelin jälkeisen ajan tyypillisen matemaatikon suhdetta matematiikan perusteisiin Davis ja Hersh kuvaavat näin (Davis, P. , Hersh, R., 1980):

> the typical working mathematician is a Platonist on weekdays and a formalist on Sundays. That is, when he is doing mathematics he is convinced that he is dealing with an objective reality whose properties he is attempting to determine. But then, when challenged to give a philosophical account of this reality, he finds it easiest to pretend that he does not believe in it after all.

Toisaalta Hilbert itsekin toimi näin: yllä olevassa lainauksessa Hilbert käytti sanaa totuus. Tämä sana on kuitenkin mielekäs vain Platonistisessa näkemyksessä.

Mielenkiintoinen tapaus on myös Bourbaki-ryhmän suhde joukko-oppiin. Voisihan kuvitella, että Bourbaki olisi pitänyt joukko-oppia erityisen tärkeänä, koska Bourbakin ideologiaan kuului, että lähdetään liikkeelle selkeistä aksioomista joiden päälle sitten matematiikka rakennetaan. Todellisuudessa joukko-oppi ei kiinnostanut Bourbakia (Mashaal, 2017):

> ce livre (théorie des ensembles) a été rédigé avec peine et sans plaisir, mais il fallait le faire.

Joukko-opin kirjoittaminen oli tuskallista, mutta se oli pakko tehdä.

Toisin sanoen ideologisista syistä kirjasarjalla piti olla jokin alkupiste, vaikka hyvin tiedettiin, että sillä ei ollut varsinaista merkitystä jatkon kannalta. Bourbakin joukko-oppi olikin alussa (1939) vain kokoelma tuloksia ja ”varsinainen” joukko-opin kirja julkaistiin vasta 1954. Bourbakin joukko-opin kirjaa onkin kritisoitu paljon, ja eräskin ranskalainen matemaatikko, joka ymmärrettävistä syistä halusi esiintyä nimettömänä, suositteli teoksen heittämistä roskikseen (Ces chapitres sont à jeter à la poubelle) (Mashaal, 2017).

Jean Dieudonné (yksi Bourbaki-ryhmän perustajajäsenistä), joka tunnetusti oli suorapuheinen, sanoo näin (Dieudonné, 1982):

> Les philosophes et logiciens ont une tendance, parfaitement naturelle et excusable, à croire que les mathématiciens s'interessent beaucoup à ce qu'ils font. Detrompez-les, ce n'est pas vrai: 95% de mathématiciens se moquent éperdumment de ce que peuvent tous les logiciens et tous les philosophes.

Filosofit ja loogikot luulevat, että matemaatikot olisivat kiinnostuneita heidän töistään. Tämä ei ole totta: 95% matemaatikoista ei voisi olla vähempää kiinnostuneita siitä, mitä loogikot ja filosofit tekevät.

Dieudonnén kirjoituksen nimi on muuten Mathématiques vides et mathématiques significatives, jonka voisi kääntää vaikkapa seuraavasti: Tyhjänpäiväistä matematiikkaa ja merkityksellistä matematiikkaa. Lukija varmaan tässä vaiheessa jo arvaa kumpaan kategoriaan logiikka ja joukko-oppi sijoittuu. Kuitenkin jos unohdetaan Dieudonnén provosoiva sävy, niin mielestäni hän vain toteaa saman, minkä jo edellä sanoin: matemaattisesta logiikasta on tullut ”tavallinen” tutkimusala, jonka tuloksilla ei automaattisesti ole merkitystä oman alan ulkopuolella.

Dieudonné antaa kaksikin syytä sille, että joukko-oppi ei ole niin tärkeää kuin voisi kuvitella. Ensinnäkin eihän tutkimuksissa oikeasti lähdetä liikkeelle matematiikan perusteista vaan aivan jostain muusta. Jos sitten havaitaan, että jokin asia ei toimi ZFC-systeemin puitteissa, niin sitten voikin olla järkevää muokata joukko-oppia siten, että haluttu tulos saadaan voimaan. Esimerkkinä Dieudonné antaa mitattomat joukot $\mathbf{R}^n$:ssä, jotka ovat pelkkä tekninen kiusa. Olisi paljon kätevämpää, jos kaikki joukot olisivat mitallisia; näin voidaankin olettaa, jos luovutaan yleisestä valinta-aksioomasta. Numeroituva valinta voidaan kuitenkin olettaa, ja Dieudonnén mielestä tämä riittää kaikkeen järkevään matematiikkaan. Tim Gowers ilmaisee asian näin (Gowers):

> Not every function is measurable but all the ones that you might actually want to integrate are.

Toisin sanoen mitattomat joukot ja funktiot ovat vain seurausta valinta-aksiooman ”holtittomasta” käytöstä, eikä niitä esiinny missään ”luonnollisessa” ongelmassa. Gowers antaa myös esimerkin Ramseyn teoriaan liittyvästä lauseesta, jossa esiintyy samantyyppinen tilanne.

> The statement is false […] because it is quite easy to use the axiom of choice to build a counterexample. But there are many mathematical contexts [… where …] the result is true. In fact, there is a precise theorem […] which comes close to saying that the only counterexamples are ridiculous ones cooked up using the axiom of choice.

Toinen syy on, ettei ole pelkästään yhtä joukko-oppia, vaan voidaan helposti rakentaa erilaisia joukko-oppeja, ehkä jopa ääretömän monta erilaista. Mikä näistä olisi "luonnollisin"? Dieudonné ottaa esimerkiksi kontinuumihypoteesin. Gödel ja Paul Cohen osoittivat, että kontinuumihypoteesi on riippumaton muista joukko-opin aksioomista, joten se voitaisiin lisätä sinne, tai jokin sen "negaatioista". Dieudonnén mielestä tämä ei kuitenkaan ole kiinnostavaa, vaan tuloksen merkitys on nimenomaan siinä,

ettei matemaatikkojen enää tarvitse vaivata päätään tällä karsealla (abominable) ja lopulta merkityksettömällä ongelmalla. Gowers puolestaan kertoo, että hänen viaton Platonisminsa päättyi tähän:

> I can date my own conversion from an unthinking childhood Platonism from the moment when I learnt that the continuum hypothesis was independent of the other axioms of set theory.

KONSTRUKTIVISMI, EPÄSTANDARDI ANALYYSI JA KATEGORIAT

ZFC-standardista on muutamia muunnelmia, jotka ovat omalla tavallaan tärkeitä. Edellä jo oli puhetta, että äärettömyyden ongelmaan tarjottiin toisenlaista ratkaisua, jota on tapana kutsua konstruktivismiksi. Tässä siis äärettömiä joukkoa ei sallittu, ja kuten Hilbert ja muut huomasivat, niin hyvin monet asiat, joihin oli totuttu, olisi pitänyt joko hylätä tai ainakin muotoilla hyvin eri tavalla kuin ennen. Konstruktivismin tunnetuin edustaja oli alussa L. E. J. Brouwer. Errett Bishop sitten 60-luvulla julkaisi tunnetun kirjan konstruktiivisestä analyysistä (Bishop, 1967) , mutta konstruktivismin asema on ollut matematiikassa marginaalinen. On ajateltu Hilbertin tavoin, että kaikenlaisesta kivasta pitäisi luopua, jos ruvettaisiin tekemään matematiikkaa konstruktiivisesti. Asia ei kuitenkaan taida olla näin yksioikoinen. Mielenkiintoisesti Andrej Bauer (Bauer, 2017) kääntää asetelman toisinpäin: hänen mukaansa konstruktivismi ei sulje ovia vaan päinvastoin avaa uusia mahdollisuuksia. Esimerkkinä hän antoi tapauksen, jossa tietyssä joukossa ei ollut pisteitä mutta siellä oli mestoja (locale)[58]. Perinteisen joukko-opin kannalta siis kyseessä oli tyhjä joukko. Mutta toisenlaisen joukko-opin mukaan se vain oli "asumaton" (uninhabited). Mestojen avulla voidaan myös ratkaista mitallisuusongelma:

> if we use locales instead of spaces, we can have both, the axiom of choice and an isometry-invariant measure on all sublocales of Rn, which agrees with the Lebesgue measure on the measurable sets.

Myös epästandardi analyysi voidaan tulkinta eräänlaiseksi ZFC-systeemin muunnelmaksi. Erityisen selvä tämä on Nelsonin muotoilemassa sisäjoukko-opissa (internal set theory) (Nelson, 1977). Nelson yksinkertaisesti lisää ZFC-aksioomiin muutaman lisäaksiooman, joitten avulla infinitesimaalit voidaan ottaa käyttöön. Tämän jälkeen voidaan osoittaa, että jos ZFC-systeemi on ristiriidaton, niin myös sisäjoukko-oppi on ristiriidaton. Toisin sanoen infinitesimaaleja voidaan käyttää siinä missä reaalilukujakin.

Tunnetusti myös kategoriateoriassa tavallinen joukko-oppi ei riitä vaan pitää lähteä muulta pohjalta liikkeelle. Kuitenkin ehkä päällisin puolin voisi ajatella, että kategoriateoriassa vain "vähän" laajennetaan joukon käsitettä, mutta tämä laajennus on pikemminkin tekninen riesa eikä itse kategoriateorian keskeinen asia.

Kaiken kaikkiaan siis joukko-oppi, tai tarkemmin ZFC-systeemi, on säilyttänyt ase-

[58] En tiedä mitä locale on tai pitäisi olla suomeksi, mutta minusta mesta kuulostaa hyvältä.

mansa tai ainakin maineensa eräänlaisena matematiikan perustana, vaikka hyvin tiedetään, että sen merkitys ei ole lopulta niin iso kuin voisi kuvitella. Tietysti alkeisjoukko-opin merkinnät ja käytännöt ovat sinänsä hyödyllisiä, ja kun vuosikymmenien aikana niihin on totuttu, niin tuntuisi vaikealta luopua niistä. Miten muuten asiat sitten voisi ilmaista kuin joukko-opin avulla? Olkoon $x \in \subset \mathbf{R}^n$; tämäntapaisia kaavoja esiintyy lukemattomissa yhteyksissä. Entä jos $\mathbf{R}^n$ ei olisikaan joukko, miten tämä ajatus pitäisi ilmaista? Gowers sanoo näin:

> Is the set-theoretic language dispensable to an ordinary mathematician? I think it often is, but I wouldn't want to go too far - after all, I would certainly feel hampered if I couldn't use it myself.

Luonnollisesti tärkeämpi kysymys on miksi joukko-opista ja sen merkinnöistä ylipäätään pitäisi luopua, jos ei ole mitään erityistä tarvetta siihen? Voevodskyn mielestä tarvetta kuitenkin oli.

VOEVODSKYN EREHDYS JA HUOLI

Vladimir Voevodsky sai Fieldsin mitalin vuonna 2002 homotopiateorioihin liittyvistä töistä. Voevodsky kiinnostui 90-luvun lopulla todistusassistenteista, koska tietyissä hänen tutkimuksensa kannalta tärkeissä todistuksissa oli virheitä ja epäselvyyksiä. Voevodsky kertoo kiinnostuksensa taustoista seuraavasti (Voevodsky, 2014):

> The field of motivic cohomology was considered at that time [1991] to be highly speculative and lacking firm foundation. The groundbreaking 1986 paper (Bloch, 1986) was [...] found [...] to contain a mistake in the proof of Lemma 1.1. The proof could not be fixed, and almost all of the claims of the paper were left unsubstantiated.
>
> A new proof, which replaced one paragraph from the original paper by thirty pages of complex arguments, was not made public until 1993, and it took many more years for it to be accepted as correct.
>
> The approach to motivic cohomology that [...] circumvented Bloch's lemma by relying instead on (Voevodsky, 2000) which was written [...] in 1992–93. Only in 1999–2000 [...] did I discover that the proof of a key lemma [...] contained a mistake [...]. A corrected sequence of arguments was published in 2006.

Blochin artikkelin julkaisemisen jälkeen kesti siis parikymmentä vuotta ennen kuin asiaan saatiin selvyys. Borgdin mielestä tämä on eräs esimerkki eräänlaisesta referointikriisistä (Borgd, 2021). Toinen tunnettu tapaus on abc-konjektuuri; vuonna 2012 Shinichi Mochizuki väitti todistaneensa konjektuurin käyttäen uutta matemaattista teoriaa, jota hän kutsui nimellä inter-universal Teichmüller theory. Konjektuurin status on edelleen kiistanalainen, ja lopulta Mochizuki päätti julkaista artikkelinsa lehdessä, jossa hän on itse päätoimittaja (Mochizuki, 2021). Joka tapauksessa Voevodsky päätti, että tämänkaltainen vuosikausia kestävä epämääräisyys ei käy vaan tarvitsisi tehdä jotain.

> I didn't have the tools to explore the areas where curiosity was leading me and the areas that I considered to be of value and of interest and of beauty.
>
> So I started to look into what I could do to create such tools. And it soon became clear that the only long-term solution was somehow to make it possible for me to use computers to verify my abstract, logical, and mathematical constructions.

Työkalu, jota Voevodsky tarvitsi, oli todistusassistentti; noihin aikoihin eräs tunnetuimmista oli Coq (The Coq proof assistant). Thierry Coquand ja Gérard Huet tekivät ensimmäiset versiot tästä ohjelmasta jo 80-luvulla (Coquand, T. , Huet, G., 1987). Voevodsky ryhtyi siis formalisoimaan matematiikaa Coqin avulla, ja jatkoi tätä työtä aina kuolemaansa saakka 2017. Voevodskyn työtä on jatketaan edelleen HoTT-projektissa (homotopy type theory) (HoTT).

TYYPPITEORIA

Tekninen ja myös psykologinen vaikeus formalisoinnissa oli, että Coq ei perustunut joukko-oppiin vaan tyyppiteoriaan. Joukko-opista ja kategoriateoriasta luopuminen oli Voevodskylle vaikeaa.

> It is extremely difficult to accept that mathematics is in need of a completely new foundation. [...] Overcoming the appeal of category theory as a candidate for new foundations of mathematics was for me personally the most challenging.

Kategoriateoria on siinä mielessä luonnollinen laajennus joukko-opille, että voidaan määritellä kategoria SET, jonka objektit ovat joukkoja ja morfismit kuvauksia; joukko-oppi ikään kuin upotetaan kategoriateoriaan.

Mutta miksi sitten todistusassistentit kannattaa rakentaa nimenomaan tyyppiteorian pohjalta? Voisihan ajatella, että todistuksia voisi formalisoida myös joukko-opin tai kategoriateorian avulla. Jossain määrin näin voidaankin tehdä, kuten Metamath osoittaa (Metamath). Mutta tavallaan intuitiivisesti voisi sanoa, että joukko-oppi on liian köyhä rakennelma, että sen varaan voisi rakentaa kunnollisia todistusassistentteja. Samoin kategoriateoria ei kelpaa, koska se ei tässä mielessä ole juuri sen parempi kuin joukko-oppi.

Tästähän ei sinänsä suoraan seuraa, että tyyppiteoria olisi sen parempi. On kuitenkin osoittautunut, että tyyppiteorian puitteissa voidaan sanoa, että todistukset ja laskenta vastaavat tietyllä tavalla toisiaan. Tämän asian tarkempi muotoilu tunnetaan nimellä Curry-Howard-isomorfismi (de Groote, 1995). Ne, kuten minä, jotka eivät ole tämän alan spesialisteja, voivat saada asiasta tarkemman tai ainakin jonkinlaisen käsityksen perehtymällä esitelmään Curry-Howard isomorphism for dummies (Pédrot, 2015). Tämän isomorfismin takia voidaan siis olla varmoja, että ainakin teoriassa tyyppiteorian avulla voidaan järkevästi ilmaista todistusassistenteissa vaadittavia rakenteita. Pédrot tiivistää asian näin:

> Proofs in a given subset of mathematics are exactly programs from a particular language.
>
> The statement of a theorem corresponds to the type of the corresponding program

Mutta mikä oikeastaan on tyyppiteoria? Hyvin intuitiivisella tasolla se on jopa helppo hahmottaa. Jokainen, joka on ohjelmoinut edes vähän tietää, että useissa ohjelmointikielissä pitää määritellä muuttujien tyyppi: esimerkiksi INTEGER, REAL (oikeastaan liukuluku) tai STRING. Tietyntyyppi-sille muuttujille on sallittu vain tietynlaisia operaatioita, eikä eri tyyppien sekoittaminen ole useinkaan mielekästä.

Matematiikassa kuitenkin usein implisiittisesti sallitaan, että erilaisia elementtejä voidaan pitää samoina (Grayson, 2018) :

> In set theory, the equation $\mathbf{N} = \{x \in \mathbf{Z} \,|\, x \geq 0\}$ is false, The statement is false because the elements of the two sets are different. The strongest thing that can be said is that there is an isomorphism $\mathbf{N} \simeq \{x \in \mathbf{Z} \,|\, x \geq 0\}$. Nevertheless, a mathematician may identify the two sets and expect not to get into trouble.

Tämänkaltaisia identifiointeja tehdään jatkuvasti: aina puhutaan L^2-funktioista eikä ekvivalenssi-luokista. Edelleen, kyseessä oleva ”funktio” samaistetaan sitä vastaavaan distribuutioon. Tyyppiteoriassa pitää olla tarkempi ja jos halutaan identifioida kaksi asiaa, niin tämä samaistus pitää sitten eksplisiittisesti konstruoida.

Joukko-opin kaavaa $a \in B$ vastaa tyyppiteoriassa ajatuksellisesti $a : B$ joka luetaan: termi a on tyyppiä B. Sen sijaan osajoukolle $A \subset B$ ei ole oikein mitään suoraa vastinetta vaan tässä tapauksessa pitäisi konstruoida upotus $A \to B$. Tämän takia myös operaatioilla $A \cap B$ ja $A \cup B$ ei ole mitään suoraa vastinetta tyyppiteoriassa. Tyyppiteorian sisällä voidaan kuitenkin määritellä tyyppi, jota voidaan kutsua joukoksi. Tämä ei tietysti ole täsmälleen sama asia kuin joukko-opin joukko, mutta ehkäpä *matemaatikko voi identifioida nämä kaksi asiaa joutumatta kovin pahoihin vaikeuksiin.*

Vaikeampi/ mielenkiintoisempi asia on, että samaa merkintää käytetään sekä funktiolle että implikaatiolle. Tästä saadaan (Grayson, 2018):

> If X and Y are types, there will be a type whose elements serve as functions from X to Y; the notation for it is $X \to Y$. This allows us to introduce the surprising mathematical pun $f : X \to Y$, which says that f is an element of the type $X \to Y$, and which can be read traditionally as saying that f is a function from X to Y.

Kaikkein tärkein tyyppi on Graysonin mukaan yhtäsuuruustyyppi (equality type tai identity type). Per Martin-Löf (Martin-Löf, 1971) huomasi 70-luvulla, että yhtäsuuruustyyppi voidaan määritellä induktiivisesti, hiukan samaan tapaan kuin Peanon systeemissä positiiviset kokonaisluvut määritellään induktiivisesti. Tämä kuulostaa tietysti varsin kummalliselta, mutta on osoittautunut, että Martin-Löfin idea on tärkeä tyyppiteoriassa. Graysonin artikkelissa (Grayson, 2018) asiaa selvitetään tarkemmin,

mutta katsotaan tähän liittyvä esimerkki. Jos x ja y ovat tyyppiä B, niin Martin-Löfin mukaan on aina olemassa tyyppi $x = y$. Voidaan siis kirjoittaa $T : x = y$, ja tämä voidaan lukea: T on todistus sille, että x on y. Tässä siis $x = y$ on lause, ja T on todistus/ ohjelma, joka on lauseen tyyppiä.

Kuten jo näistä yksinkertaisista huomioista nähdään, niin tyyppiteoriassa asiat pitää ilmaista aivan eri tavalla kuin on totuttu. Vaikka Martin-Löf ei itse ollut kehittämässä todistusassistentteja, niin hän oli kiinnostunut tyyppiteorian ja laskennan vuorovaikutuksesta; hänen mielestään tyyppiteoriaa voidaan jopa pitää eräänlaisena hyvin korkean tason ohjelmointikielenä (Martin-Löf, 1982). Martin-Löfiin liittyy hauska muisto: osallistuin erääseen konferenssiin Mittag-Lefflerissä 80-luvulla, ja Martin-Löf oli yksi puhujista. Luulen, että hän puhui nimenomaan tyyppiteoriasta; esitelmä on kuitenkin jäänyt mieleen juuri sen takia, etten ymmärtänyt siitä mitään.

Mielenkiintoista on myös, että tyyppiteoria ja todistusassistentit voidaan rakentaa enemmän tai vähemmän konstruktiiviseksi. Valinta-aksiooma voidaan ottaa käyttöön, jos halutaan. Voidaan siis hyvin tarkasti kontrolloida, millaisia asioita todistuksessa sallitaan tai ei sallita. Tämän avulla lauseiden sisältökin saa tarkemman muodon, kun pidetään kirjaa, mitä kaikkea todistuksessa tarvitaan.

Jotta asiat eivät olisi liian yksinkertaisia, niin tyyppiteorioita on tietysti erilaisia. Ehkäpä ensimmäinen tyyppiteoreettinen systeemi oli Alfred North Whiteheadin ja Bertrand Russellin yritys rakentaa matematiikan perusteita (Whitehead, A. N. , Russell, B., 1910). Teoksessa käytettiin tyyppiteoriaa muun muassa siihen, että päästiin eroon joukko-opin kiusallisista itseensä viittaavista kaavoista kuten $A \in A$. Tyyppiteoriassa $A : A$ ei ole syntaktisesti mahdollinen. Tämähän on luonnollista, jos ajattelee ohjelmointikieliä: jos a : INTEGER, niin tietenkään a itse ei voi olla INTEGER.

En tiedä tuliko Whiteheadille ja Russellille mieleen, että heidän työllään voisi olla merkitystä tietokoneitten kannalta. Tämä olisi ainakin teoriassa ollut mahdollista, koska Charles Babbage ja Ada Lovelace olivat jo 1800-luvun puolella selkeästi hahmotelleet tietokoneen idean, vaikka Babbagen yritys rakentaa tietokone (analytical engine) jäikin kesken (Babbage, C. , Lovelace, A., 1842).

Nykyään monet todistusassistentit, kuten Coq, Agda (Agda) ja LEAN (LEAN) , käyttävät ”riippuvaa” tyyppiteoriaa (dependent type theory), mutta kuitenkin Isabelle (Isabelle) käyttää “yksinkertaista” (simple) tyyppiteoriaa. En ole varma, kuinka merkittävä yksinkertaisen ja riippuvan tyyppiteorian ero on, mutta kaiketi yksinkertaisellakin versiolla aika pitkälle päästään (Bordg, A. , Paulson, L. , Li, W., 2021). RedPRL (RedPRL) puolestaan käyttää versiota, jonka nimi on Cartesian cubical computational type theory. Myös Voevodsky loi oman version riippuvasta tyyppiteoriasta; hän käytti näin syntyneestä systeemistä nimeä *Univalent foundations* (Grayson, 2018). Näyttäisi siis siltä, että tyyppiteorioita on jatkossakin monenlaisia, eikä

kaiketi ole selvää alan spesialisteillekaan stabiloituuko tilanne lähiaikoina vai ei.

Todistusassistenttien avulla voidaan siis kirjoittaa "parempia" tai ainakin varmempia tai tarkempia (rigorous) todistuksia kuin muuten olisi mahdollista. Kaiketi on varsin selvää, että kun asiat tehdään huolellisesti, niin koneet tekevät vähemmän virheitä kuin ihmiset, joten matemaattisten tulosten luotettavuus kasvaa, jos todistusassistentit yleistyvät. Artikkelien referointikin voisi merkittävästi helpottua ajan myötä, ja näin myös vältyttäisiin Borgdin kuvaamalta referointikriisiltä. Ongelma on tietenkin se, että tulokset ja artikkelit pitäisi muotoilla tyyppiteorian mukaisesti, siis tavallisille matemaatikoille aivan uudella ja vieraalla tavalla, joten tietysti tämä ei ole vielä käytännössä mahdollista pitkään aikaan. Periaatteessa kuitenkin tämä voisi olla jonain päivänä toimiva systeemi.

LEAN

Katsotaan tarkemmin LEANia. Leonardo de Moura aloitti tämän systeemin kehittämisen Microsoftilla vuonna 2013. Systeemin tarkoituksena oli tarkistaa, että tietokoneohjelmissa ei ole virheitä, eikä sitä mitenkään alun perin ollut tarkoitettu matemaatikoille. Mutta itse asiassa ohjelman osoittaminen virheettömäksi on oikeastaan hyvin lähellä lauseen todistamista; ehkäpä Curry-Howard-isomorfismin ansiosta voidaan jopa sanoa, että ne ovat sama asia; tai ainakin että matemaatikko voi identifioida nämä kaksi asiaa joutumatta kovin pahoihin vaikeuksiin. Matemaatikot siis huomasivat, että LEAN soveltuisi hyvin myös todistusassistentiksi, ja jonkin ajan kuluttua siitä tehtiin versio nimenomaan matematiikan tarpeita ajatellen. Tämän jälkeen ohjelmiston ympärille on kasvanut yhteisö, joka pikkuhiljaa formalisoi kaikkea matematiikkaa lähtien perusasioista liikkeelle (Hartnett, 2020).

Luonnollisesti tehtävä on valtava, mutta asiat etenevät ja esimerkiksi perusreaalianalyysiä on formalisoitu niin paljon, että tyyppiteoriaa voitaisiin jo käyttää opetuksessa. Toisin sanoen joukko-oppi voitaisiin unohtaa yliopistojen peruskursseilla, ja lähteä opiskelemaan matematiikkaa LEANin avulla. Kevin Buzzard[59] on jo jonkin verran kokeillut tällaista Imperial Collegessa, samoin Patrick Massot Université Paris-Sudissä.[60] Buzzard kertoo tästä, ja muutenkin matematiikan formalisoinnista esitelmässä, jonka hän piti Microsoftilla (Buzzard, 2019). Buzzard kiinnostui todistusassistenteista osittain samasta syystä kuin Voevodsky: eräät tulokset, joita hän halusi käyttää tutkimuksessa, olivat epäselviä ja epävarmoja.

Todistusassistenttien ja tyyppiteorian käyttö opetuksessa herättää mielenkiintoisia kysymyksiä. Mitä matematiikkaa pitäisi opettaa ja miksi? Vaikka tyyppiteoria tuntuu nyt vieraalta, niin luulisin, että opiskelijan näkökulmasta se ei ole sen vaikeampi tai helpompi kuin joukko-oppi. Todistus-assistenttien avulla opiskelijat pystyisivät tekemään

[59] https://www.imperial.ac.uk/people/k.buzzard

[60] https://www.imo.universite-paris-saclay.fr/~pmassot/index.html

tarkkoja todistuksia, mutta todistukset olisivat hyvin erilaisia kuin mitä nykyään opetetaan. Mutta haittaisiko se? Ja jos ei haluta opettaa mahdollisimman tarkkoja todistuksia, niin mitä oikeastaan halutaan?

LEANiin voi jokainen helposti tutustua Buzzardin ja Mohammad Pedramfarin suunnitteleman Natural number gamen avulla (Buzzard, Natural number game). Tässä lähdetään liikkeelle ilman mitään esitietoja, ja minusta se oli kiinnostavasti tehty. Helppojen tehtävien avulla saa ainakin jonkinlaisen kuvan, miten formalisointi toimii. Luonnollisesti tässä tulee vastaan ne tavanomaiset turhautumiset, kun pitää opetella uusi syntaksi. Mielenkiintoista on, että prosessi etenee vaiheittain. Kun todistus jotenkin on saatu alkuun, niin **LEAN** automaattisesti etenee mahdollisimman pitkälle, ja kertoo sitten käyttäjälle, mitä seuraavaksi pitäisi tehdä. Siis käyttäjän ei tarvitse etukäteen pilkkoa lausetta ”pienemmiksi” lemmoiksi, vaan ohjelma tekee tämän. Tätä on ehkä vaikea hahmottaa, jos ei ole itse kokeillut tuollaista systeemiä, joten suosittelen Natural number gamen testaamista!

Katsotaan sitten vielä toinen esimerkki, jossa todistusassistenttia on käytetty aivan lähiaikoina huippututkimuksessa; tätä varten käännytään toisen Fields-mitalistin puoleen

TIIVISTETTY MATEMATIIKKA

Peter Scholze sai Fieldsin mitalin vuonna 2018 aritmeettiseen algebralliseen geometriaan liittyvistä töistä. Viime aikoina hän on Dustin Clausenin kanssa ruvennut luomaan uudenlaista matematiikan alaa: tiivistettyä matematiikkaa (condensed mathematics) (Scholze). Tässä keskeinen käsite on tiivistetty joukko (condensed set) (Scholze, 2021).

> **Määritelmä**. Condensed sets *are sheaves on the pro-étale site of a point*.

Palataan hiukan myöhemmin siihen, miten tämä pitäisi ymmärtää, koska ainakaan minulle itse määritelmä ei juuri valaise asiaa. Joka tapauksessa tiivistettyyn matematiikkaan liittyy joitain joukko-opillisia ongelmia:

> [There are] set-theoretic problems. […] Let me gloss over this point here; it is not essential for any of the following discussion.

Toisin sanoen ZFC-systeemi ei riitä tässä, mutta Scholzen mielestä tämä on oikeastaan epäoleellista. Scholzen rakennelmassa oli muutama erittäin tekninen lause, jotka hän luuli todistaneensa, mutta hälventääkseen viimeiset epäilyt, hän päätti ryhtyä projektiin, jossa nämä keskeiset tulokset formalisoitaisiin ja todistettaisiin LEANin avulla. Scholze ei itse ruvennut ohjelmoimaan LEANilla, vaan luotiin Johan Commelinin johtama ryhmä tätä tarkoitusta varten. Scholze oli kuitenkin jatkuvasti yhteydessä ryhmään. Projektin nimeksi tuli *Liquid tensor experiment*, kaiketi kahdesta syystä: toisaalta nesteet varmaankin ovat jonkinlainen kontrasti tiiviydelle, ja toisaalta Scholzen ja Commelinin suosikkibändi on nimeltään *Liquid tension experiment*.[61] Ryhmä aloitti työt loppuvuonna 2020, ja jo

[61] https://www.wikiwand.com/en/Liquid_Tension_Experiment

kesällä 2021 projekti oli edennyt jo niin pitkälle, että Scholze jo siinä vaiheessa piti projektia onnistuneena (Castelvecchi, 2021). Esimerkiksi ne tekniset tulokset, jotka Scholzea erityisesti huolestutti, oli saatu pakettiin.

Siis varsin lyhyessä ajassa pystyttiin formalisoimaan ja todistamaan tuloksia, jotka ovat hyvin monimutkaisia, joten selvästi todistusassistenteilla voidaan tehdä jotain järkevää aivan matematiikan tutkimuksen eturintamassa. Lisäksi todistusassistenttien laatu koko ajan paranee, koska kaikki uudet formalisoidut käsitteet ja tulokset ovat ikään kuin valmiina kirjastossa tulevaa käyttöä varten, joten käytössä olevien työkalujen määrä kasvaa koko ajan.

Tuloksen formalisoinnissa tiivistetty joukko ei tietysti ole joukko, vaan tyyppi, tai termi, joka on tiettyä tyyppiä. Uskoisin kuitenkin, että tästä huolimatta Scholze ja Clausen käyttävät jatkossa joukko-opin merkintöjä tavallisissa matemaattisissa teksteissä. Tässä siis siirretään tuloksia kahden erilaisen matemaattisen maailman välillä, käyttäen jo hyväksi havaittua filosofiaa, että matemaatikko (toivoo, että hän) voi sopivasti identifioida kaksi eri asiaa joutumatta kovin pahoihin vaikeuksiin.

Mutta miksi nämä tiivistetyt joukot sitten ovat niin tärkeitä? Itse asiassa Scholze väittää, että niillä voisi olla laajempaakin käyttöä matematiikassa. Lause johon Scholze seuraavassa viittaa on juuri se tulos, joka piti formalisoida.

> With this theorem, the hope that the condensed formalism can be fruitfully applied to real functional analysis stands or falls. I think the theorem is of utmost foundational importance, so being 99.9% sure is not enough.

Jos nyt katsoo uudelleen tuota tiivistetyn joukon määritelmää, niin voisi varsin helposti tulla siihen johtopäätökseen, että sillä ei ole mitään tekemistä reaalisen funktionaalianalyysin kanssa. En tiedä miten Scholze ja Clausen aikovat tehdä tuloksensa ymmärrettäviksi sellaisille matemaatikoille, jotka tuntevat funktionaalianalyysiä, mutta eivät ole perehtyneet algebralliseen geometriaan ja kategoriateoriaan. Ehkäpä heillä on tekeillä teos *Condensed sets for dummies*. Mutta itse asiassa tiivistetyn joukon merkitys on Scholzen mukaan vieläkin suurempi:

> I want to make the strong claim that in the foundations of mathematics, one should replace topological spaces with condensed sets. […] This claim is only tenable if condensed sets can also serve their purpose within real functional analysis.

Kun nyt on jo totuttu ajatukseen, että joukko-opista luovutaan tai ainakin voitaisiin luopua, niin kukaan ei kai enää järkyty, kun topologiset avaruudetkin pitää korvata paremmalla rakenteella, siis tiivistetyillä joukoilla. Jäänkin odottamaan Scholzen ja Clausenin kirjaa niin voin sitten muuttaa kurssini *Johdatus topologiaan* kurssiksi *Johdatus tiivistettyihin joukkoihin*.

TULEVAISUUS

Charles Hoskinson opiskeli nuorempana matematiikkaa mutta innostui sitten kryptovaluutoista, ja rikastui niitten avulla. Viime

syksynä hän lahjoitti 20 miljoonaa dollaria Carnegie Mellon -yliopistolle, jotta sinne perustettaisiin Hoskinson center for formal mathematics. Yksikön johtajaksi tulee Jeremy Avigad, joka on ollut aktiivisesti mukana LEANissa. Avigad kertoo yksikön tavoitteista seuraavasti (Avigad, 2021):

> The center's mission is to support the work being done by the LEAN community, to promote the use of LEAN and its libraries, and to seek out ways of using the technology to make mathematics accessible and enjoyable to as wide an audience as possible.

Tähän mennessä LEAN on toiminut yhteisönä varsin epämuodollisesti. Hoskinson center todennäköisesti varmistaa toiminnan jatkuvuuden siinä mielessä, että yhteisö ei pääse jotenkin ”vahingossa” hajoamaan.

Kuten on nähty, niin LEAN on tietysti vain yksi mahdollinen systeemi. Angelika Koutsoukou-Argyraki on kerännyt erilaisia ajatuksia ja mielipiteitä matematiikan formalisoinnista ja sen merkityksestä tulevaisuudessa, riippumatta siitä mitä todistusassistenttia käytetään (Koutsoukou-Argyraki, 2022). Lopuksi ehkä on vielä syytä mainita, että luonnollisesti tarkoitus ei ole korvata kaikkea matematiikkaa formalisoidulla matematiikalla, vaan ideana on, että todistusassistenttien ja tyyppiteorian käyttö on eräs mahdollinen ja mielenkiintoinen tapa tehdä matematiikkaa. Massot ilmaisee asian näin (Massot, 2021):

> I think a key point is that formalized mathematics brings a lot of fun. […] Of course fun is not the only reason why people collaborate on building libraries of formalized mathematics. This is also an exhilarating experience where contributors feel they could have a real impact on the mathematical community, without removing anything we love, only adding new possibilities.

Lähdeluettelo

Agda. (ei pvm). Noudettu osoitteesta https://wiki.portal.chalmers.se/agda/pmwiki.php

Avigad, J. (2021). Noudettu osoitteesta https://leanprover-community.github.io/blog/posts/hoskinson-center-announced/

Babbage, C. , Lovelace, A. (1842). The sketch of the analytical engine. Noudettu osoitteesta https://www.fourmilab.ch/babbage/sketch.html

Bauer, A. (2017). Five stages of accepting constructive mathematics. Bulletin of AMS, 481-498. doi: https://doi.org/10.1090/bull/1556

Bishop, E. (1967). Foundations of constructive analysis. McGraw Hill.

Bloch, S. (1986). Algebraic cycles and higher K-theory. Adv. in Math., 267-304.

Bordg, A. , Paulson, L. , Li, W. (2021). Simple Type Theory is not too Simple: Grothendieck's Schemes without Dependent Types. arXiv. doi:10.48550/ARXIV.2104.09366

Borgd, A. (2021). A replication crisis in mathematics? Math. Intelligencer, vol. 43, 48-52. doi:10.1007/s00283-020-10037-7

Buzzard, K. (2019). The Future of Mathematics? Noudettu osoitteesta https://www.youtube.com/watch?v=Dp-mQ3HxgDE

Buzzard, K. (ei pvm). Natural number game. Noudettu osoitteesta https://www.ma.imperial.ac.uk/~buzzard/xena/natural_number_game/

Castelvecchi, D. (2021). Mathematicians welcome computer-assisted proof in ‘grand unification’ theory. Nature. doi:https://doi.org/10.1038/d41586-021-01627-2

Coquand, T. , Huet, G. (1987). Concepts mathématiques et informatiques formalisés dans le calcul des constructions. Teoksessa Logic colloquium '85 (Orsay, 1985) (ss. 123-146). North-Holland.

Davis, P. , Hersh, R. (1980). Mathematical experience. Birkhäuser.

de Groote, P. (Toim.). (1995). The Curry-Howard isomorphism. Cahiers du Centre de Logique. vol. 8. Academia-Erasme, Louvain-la-Neuve.

Dieudonné, J. (1982). Mathématiques vides et mathématiques significatives. Teoksessa Penser les mathématiques (ss. 15-38). Éditions du Seuil.

Gowers, T. (ei pvm). Does mathematics need philosophy? Noudettu osoitteesta https://www.dpmms.cam.ac.uk/~wtg10/philosophy.html

Grayson, D. (2018). An introduction to univalent foundations for mathematicians. Bulletin of AMS, 427-450. doi: https://doi.org/10.1090/bull/1616

Hartnett, K. (2020). Building the Mathematical Library of the Future. Quanta Magazine . Noudettu osoitteesta https://www.quantamagazine.org/building-the-mathematical-library-of-the-future-20201001/

HoTT. (ei pvm). Noudettu osoitteesta https://homotopytypetheory.org/

Isabelle. (ei pvm). Noudettu osoitteesta https://isabelle.in.tum.de/

Koutsoukou-Argyraki, A. (2022). What Can Formal Systems Do For Mathematics? A Discussion Through The Lens Of Proof Assistants: Some Recent Advances. Noudettu osoitteesta https://www.researchgate.net/publication/359592051_What_Can_Formal_Systems_-Do_For_Mathematics_A_Discussion_Through_The_Lens_Of_Proof_Assistants_Some_Recent_Advances

LEAN. (ei pvm). Noudettu osoitteesta https://leanprover-community.github.io/index.html

Martin-Löf, P. (1971). Hauptsatz for the intuitionistic theory of iterated inductive definitions. Proceedings of the Second Scandinavian Logic Symposium (ss. 179-216). North-Holland.

Martin-Löf, P. (1982). Constructive mathematics and computer programming. Teoksessa Logic, methodology and philosophy of science, VI, (Hannover 1979) (ss. 153-175). North-Holland.

Mashaal, M. (2017). Bourbaki, Une société secrète de mathématiciens. Éditions Belin.

Massot, P. (2021). Why formalize mathematics? Noudettu osoitteesta https://www.imo.universite-paris-saclay.fr/~pmassot/en/exposition/

Metamath. (ei pvm). Noudettu osoitteesta http://us.metamath.org/

Mochizuki, S. (2021). Inter-universal Teichmüller theory, 1 - 4. Publ. Res. Inst. Math. Sci., 3 -723.

Nelson, E. (1977). Internal set theory: a new approach to nonstandard analysis. Bulletin of AMS, 1165-1198. doi:10.1090/S0002-9904-1977-14398-X

Pédrot, P.-M. (2015). Curry-Howard isomorphism for dummies. Noudettu osoitteesta https://www.pédrot.fr/slides/inria-junior-02-15.pdf

RedPRL. (ei pvm). Noudettu osoitteesta https://redprl.org/

Scholze, P. (ei pvm). Noudettu osoitteesta http://www.math.uni-bonn.de/people/scholze/Notes.html

Scholze, P. (2021). Liquid tensor experiment. Experimental mathematics. doi: 10.1080/10586458.2021.1926016

The Coq proof assistant. (ei pvm). Noudettu osoitteesta The Coq proof assistant: https://coq.inria.fr/

Whitehead, A. N. , Russell, B. (1910). Principia mathematica. Cambridge Univ. Press.

Voevodsky, V. (2000). Cohomological theory of presheaves with transfers. Teoksessa Cycles, transfers, and motivic homology theories (ss. 87-137). Princeton Univ. Press.

Voevodsky, V. (2014). The Origins and motivations of univalent foundations. Noudettu osoitteesta https://www.ias.edu/ideas/2014/voevodsky-origins

von Neumann, J. (1947). The mathematician. Teoksessa The Works of the Mind (ss. 180-196). University of Chicago Press.