Tarinoita polynomeista (osa 5)

Jukka Tuomela
Itä-Suomen yliopisto, Joensuu
jukka.tuomela@uef.fi

Kertaus

Jatketaan tässä polynomien tarkastelua hieman eri kontekstissa kuin aiemmissa kirjoituksissa [8, 9, 10, 11]. Jälleen suosittelen kirjaa [3] kaikille polynomeista kiinnostuneille. Tämän kirjoituksen laskut on helppo laskea SAGELLA [1].[1]

Helppoa polynomialgebraa

Kun lasketaan rationaalikertoimisilla polynomeilla, niin pitkissä laskuissa helposti rationaalilukujen koko kasvaa nopeasti; siis osoittajassa ja nimittäjässä voi olla hyvin suuria kokonaislukuja. Ei siis etukäteen tiedetä, kuinka monta bittiä vastauksen ja välitulosten esittämiseen tarvitaan. Tämän takia tietokonetoteutuksen pitää varautua siihen, että muistitilaa pitää kasvattaa laskun kuluessa. Olisikin paljon mukavampaa laskea siten, että kertoimien koko ei kasvaisi. Korvataan siis rationaaliluvut äärellisellä joukolla seuraavasti.

Olkoon $\mathbb{Z}_2 = \{0, 1\}$ ja määritellään tässä joukossa yhteen- ja kertolasku seuraavasti:

$+$	0	1
0	0	1
1	1	0

$*$	0	1
0	0	0
1	0	1

[1] https://www.sagemath.org/index.html

Merkitään $f \in \mathbb{Z}_2[x]$, jos

$$f = \sum_{j=0}^{n} c_j x^j, \quad c_j \in \mathbb{Z}_2.$$

Nyt voidaan esimerkiksi laskea

$$(x+1)^4 = x^4 + 1,$$
$$(x^3 + x + 1)(x^5 + x^2) = x^8 + x^6 + x^3 + x^2.$$

Jätän harjoitustehtäväksi sen pohtimisen, millä k:n arvoilla pätee $(x+1)^k = x^k + 1$.

Kaikki tavalliset polynomeihin liittyvät laskutoimitukset pätevät, koska $\mathbb{Z}_2$ on kunta. Tarkka määritelmä löytyy Metsänkylän ja Näätäsen kirjasta [5], mutta kunnassa siis voidaan laskea yhteen, kertoa ja jakaa, kuten rationaalilukujen tapauksessa on totuttu. Erityisesti siis kirjoituksessa [8] esitelty jakolaskualgoritmi toimii sellaisenaan myös renkaassa $\mathbb{Z}_2[x]$. Esimerkiksi jos $f = x^{11} + x^6 + x^4 + x$ ja $g = x^5 + x^2 + 1$, niin jakolaskualgoritmi antaa

$$f = (x^6 + x^3 + 1)g + x^4 + x^3 + x^2 + x + 1.$$

Toivoisin, että lukija laskisi tämän jakokulman avulla ja huomaisi, miten helppoa se on.

SAGEN avulla lasketaan seuraavasti.

```
R0 = PolynomialRing(GF(2), 'x');
x = R0.gen()
```

Ensimmäisellä rivillä annetaan renkaan $\mathbb{Z}_2[x]$ nimeksi R0 ja toisella rivillä kerrotaan, että kirjain x on muuttujan nimi. GF(2) on kunnan $\mathbb{Z}_2$ nimi.[2] Sitten voidaan määritellä polynomit:

```
f=x^(11)+x^6+x^4+x;
g=x^5+x^2+1
```

Nyt f voidaan jakaa tekijöihin komennolla f.factor(), mikä antaa

$$f = x(x+1)^3(x^7+x^6+x^3+x+1).$$

Nolla on siis f:n yksinkertainen nollakohta, ja yksi on kolminkertainen nollakohta. Tekijällä $x^7+x^6+x^3+x+1$ ei ole nollakohtia ollenkaan.

Komennolla f.quo_rem(g) saadaan sitten osamäärä ja jakojäännös. Vastaus on lista, jonka ensimmäinen alkio on osamäärä ja toinen on jakojäännös.

Täsmälleen samoin voidaan laskea, jos on useampia muuttujia:

$$\begin{aligned} h &= (x_1^3 + x_1x_2 + x_2^2)(x_1^2 + x_2) \\ &= x_1^5 + x_1^2x_2^2 + x_1x_2^2 + x_2^3. \end{aligned} \tag{1}$$

Skeptinen lukija kenties on samaa mieltä siitä, että laskut helpottuvat, mutta hän voi epäillä koko jutun hyödyllisyyttä ja/tai mielekkyyttä. On kuitenkin osoittautunut, että polynomeja, joitten kertoimet ovat äärellisestä kunnasta, esiintyy monilla matematiikan aloilla. Esimerkiksi:

(i) Äärellisiä kuntia ja polynomeja käytetään koodausteoriassa [13].

(ii) Jos halutaan jakaa rationaalikertoiminen polynomi tekijöihin, niin ensin suoritetaan tämä tekijöihinjako äärellisessä kunnassa, koska se on helpompaa. Tämän avulla sitten löydetään myös rationaaliset tekijät [12].

Tässä kirjoituksessa katsotaan, miten polynomien avulla voidaan helposti analysoida monimutkaisia loogisia lausekkeita. Ennen sitä pitää kuitenkin katsoa, mitä eroa on polynomeilla ja funktioilla.

Polynomit ja funktiot

Olkoon sitten $f \in \mathbb{Z}_2[x]$ jokin polynomi. Selvästi näin voidaan määritellä myös funktio $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$. Mutta nyt on varsin selvää, että polynomien ja funktioitten välillä ei ole bijektiota. Helposti löydetään polynomeja, jotka eivät ole nollapolynomeja, mutta ne ovat nollafunktioita, esimerkiksi $\hat{f} = x+x^3+x^4+x^7$. Itse asiassa kun vähän pohtii asiaa, niin on vain 4 eri funktiota $\mathbb{Z}_2 \to \mathbb{Z}_2$:

$$\begin{aligned} f_0(x) &= 0, \quad f_1(x) = 1, \\ f_2(x) &= x, \quad f_3(x) = x+1. \end{aligned} \tag{2}$$

Huomaa, että nämä ovat täsmälleen kaikki polynomit, joitten aste on korkeintaan yksi.

Jos sitten annetaan jokin mielivaltainen polynomi f, niin funktiona se vastaa jotain noista neljästä funktiosta. Tässä tietenkin tarvitaan jakolaskualgoritmia. Olkoon $g = x^2 + x$; tämä on yksinkertaisin polynomi, joka ei ole nollapolynomi, mutta on nollafunktio. Jaetaan siis g:llä, jolloin saadaan

$$f = qg + r,$$

missä r on jokin ensimmäisen asteen polynomi, koska g on toisen asteen polynomi. Siis $r = f_j$ jollekin $0 \le j \le 3$. Mutta koska $g(x) = 0$, niin

$$f(x) = q(x)g(x) + r(x) = r(x).$$

Funktiona f ja sen jakojäännös r ovat samoja, vaikka ne ovat eri polynomeja. Merkitään tätä jakojäännöstä $\mathsf{NF}(f)$.

Tämä idea yleistyy sellaisenaan monen muuttujan tapaukseen. Olkoon $x = (x_1, \ldots, x_n)$ ja olkoon edelleen $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ ja merkitään

$$x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}.$$

Mielivaltainen $f \in \mathbb{Z}_2[x_1, \ldots, x_n]$ voidaan nyt kirjoittaa muodossa

$$f = \sum_\alpha c_\alpha x^\alpha, \quad c_\alpha \in \mathbb{Z}_2.$$

Miten sitten löydettäisiin $\mathsf{NF}(f)$? Huomaa, että funktioina $x_j^k = x_j$ kaikilla $k \ge 1$, joten jokaisessa monomissa x^α voidaan α korvata indeksivektorilla β, missä

$$\beta_j = \begin{cases} 0, & \alpha_j = 0, \\ 1, & \alpha_j \ge 1. \end{cases} \tag{3}$$

Siispä $\beta \in \mathbb{Z}_2^n$; huomaa, että erilaisia indeksivektoreita, ja vastaavia monomeja x^β, on 2^n kappaletta. Tästä edelleen seuraa, että kaikki mahdolliset funktiot $\mathbb{Z}_2^n \to \mathbb{Z}_2$ ovat muotoa

$$\tilde{f} = \sum_{\beta \in \mathbb{Z}_2^n} c_\beta x^\beta, \quad c_\beta \in \mathbb{Z}_2. \tag{4}$$

Siispä mahdollisia funktioita $\mathbb{Z}_2^n \to \mathbb{Z}_2$ on 2^{2^n} kappaletta, mikä antaa 4 kappaletta tapauksessa $n = 1$, kuten jo yllä todettiin. Polynomeja, jotka ovat muotoa (4) on tapana kutsua Zhegalkinin polynomeiksi [4].[3]

[2] Äärellistä kuntaa (finite field) sanotaan myös Galois'n kunnaksi (Galois field).

[3] Artikkeli [4] on kirjoitettu venäjäksi, mutta siinä oli ranskankielinen lyhennelmä, joten nimi kirjoitettiin ranskalaisittain Gégalkine.

Nyt vaikkapa polynomin (1) tapauksessa

$$\mathsf{NF}(h) = x_1 + x_1x_2 + x_1x_2 + x_2 = x_1 + x_2.$$

Käsin laskien on kätevä käyttää kaavaa (3), mutta tietokoneella laskiessa on näppärämpää edetä toisin. Olkoon $g_j = x_j^2 + x_j$ ja jaetaan vuorotellen jokaisen polynomin g_j suhteen:

$$\begin{aligned} f &= q_1g_1 + r_1, \\ r_1 &= q_2g_2 + r_2, \\ &\vdots \\ r_{n-1} &= q_ng_n + r_n. \end{aligned}$$

Nyt r_n on Zhegalkinin polynomi ja voidaan kirjoittaa $r_n = \mathsf{NF}(f)$. Esimerkiksi jos otetaan yhtälön (1) polynomi, niin

$$\begin{aligned} h &= (x_1^3 + x_1^2 + x_2^2 + x_1 + 1)g_1 + x_1 + x_2^3, \\ x_1 + x_2^3 &= (x_2 + 1)g_2 + x_1 + x_2, \end{aligned}$$

joten $\mathsf{NF}(h) = x_1 + x_2$, kuten äsken jo nähtiin.

Nyt voidaan sitten testata, milloin kaksi polynomia ovat funktioina samoja: f ja g ovat funktioina samoja, jos $\mathsf{NF}(f) = \mathsf{NF}(g)$ tai ekvivalentisti, jos $\mathsf{NF}(f+g) = 0$. Zhegalkin päätyi polynomeihinsa, kun hän tarkasteli loogisten lausekkeitten totuusarvoja. Katsotaan tätä seuraavaksi.

Logiikka 0

Lewis Carroll kuvaili logiikkaa seuraavasti [2]:

> ‘I know what you’re thinking about,’ said Tweedledum: ‘but it isn’t so, nohow.’
>
> ‘Contrariwise,’ continued Tweedledee, ‘if it was so, it might be; and if it were so, it would be; but as it isn’t, it ain’t. That’s logic.’

Jätän harjoitustehtäväksi sen pohtimisen, miten hyvin Carroll on tuossa tavoittanut logiikan syvimmän olemuksen. Metsänkylä ja Näätänen [5] ovat ottaneet perinteisemmän näkökulman logiikkaan. Kirjan luvussa nolla on esitelty logiikan peruskäsitteet, joten jos alempana jokin termi tai merkintä ei ole ennestään tuttu, niin tuolta löytyy lisätietoa.

Merkitään isoilla kirjaimilla joitain väitteitä, kuten X on väite, että reaaliluku $a \geq 1$. Tämän negaatio $\neg X$ on väite $a < 1$. Tarkkaavainen lukija kenties huomaa, että tässä ollaan heti heikoilla jäillä, koska voisihan ajatella, että eräänlainen negaatio olisi väite: a ei ole reaaliluku. Väitteillä pitää tavallaan olla jokin konteksti, mutta tämä konteksti varmaankin on selvä esimerkeissä, ja joka tapauksessa tätä kontekstia ei puhtaan loogisesti edes tarvita. Matematiikassahan voidaan määritellä tiettyjä asioita riippumatta niitten merkityksestä.

Kun esitetään jokin väite, niin se voi olla matematiikassa joko tosi tai epätosi. Todellisessa elämässähän väitteet ovat usein epämääräisiä ja/tai epäilyttäviä, mutta keskitytään tässä vain matemaattisiin väitteisiin.

Jos on siis annettu jokin väite X, joka voi olla tosi tai epätosi, niin sehän on oikeasti jokin funktio, jonka arvojoukko on $\mathbb{Z}_2$: funktion arvo on 0, jos X on epätosi, ja 1, jos se on tosi. Laitetaan siis väitettä X vastaamaan muuttuja x, jolloin voidaan sanoa, että X määrittää funktion f_2, joka oli yhtälössä (2).

Olkoon sitten $\mathbb{E}$ väite, joka on epätosi, ja $\mathbb{T}$ väite, joka on tosi; tällöin väitettä $\mathbb{E}$ vastaa nollafunktio ja väitettä $\mathbb{T}$ vastaa funktio, joka aina saa arvon yksi. Lopuksi vielä negaatiota $\neg X$ vastaa yhtälön (2) funktio $f_3 = 1+x$. Voidaan siis kirjoittaa:

$$\begin{aligned} \mathbb{E} &\longleftrightarrow 0, \\ \mathbb{T} &\longleftrightarrow 1, \\ X &\longleftrightarrow x, \\ \neg X &\longleftrightarrow 1 + x. \end{aligned}$$

Huomaa, että oikealla puolella on täsmälleen yhtälössä (2) annetut yhden muuttujan Zhegalkinin polynomit.

Logiikassa on kuitenkin tyypillisesti useampia väitteitä. Jos on annettu väitteet X ja Y, niin liitetään näihin vastaavat muuttujat x ja y. Kuten yllä todettiin, niin on $2^{2^2} = 16$ eri kahden muuttujan Zhegalkinin polynomia, joten mikä tahansa kahden väitteen lauseke voidaan esittää näitten avulla. Koska yhden muuttujan tapaus on erikoistapaus kahden muuttujan tapauksesta, niin jäljelle jää vain 10 aidosti kahta väitettä kuvaavaa funktiota.

Logiikassa on tapana käyttää seuraavia merkintöjä näille funktioille:

$$\begin{aligned} X \vee Y &\longleftrightarrow x + y + xy, \\ X \wedge Y &\longleftrightarrow xy, \\ X \;\Rightarrow\; Y &\longleftrightarrow 1 + x + xy, \\ Y \;\Rightarrow\; X &\longleftrightarrow 1 + y + xy, \\ X \;\Leftrightarrow\; Y &\longleftrightarrow 1 + x + y. \end{aligned} \tag{5}$$

Kun otetaan vielä näitten negaatiot, niin saadaan kaikki 10 funktiota. Tämä muuten selittää logiikassa käytettävien merkintöjen lukumäärän. Yhden väitteen tapauksessa on kätevää käyttää symbolia ¬, koska silloin kaikki Zhegalkinin polynomeja vastaavat lausekkeet voidaan esittää lyhyesti. Kahden väitteen tapauksessa lyhyet esitysmuodot Zhegalkinin polynomeille saadaan, kun otetaan käyttöön lisäksi ∨, ∧, ⇒ ja ⇔. Puhtaan loogisesti vähempikin symbolimäärä riittäisi, mutta tällöin lausekkeista tulisi paljon vaikeammin hahmotettavia.

Nyt voidaan helposti laskea esimerkiksi, että

$$\begin{aligned} \neg\big(X \vee Y\big) &\longleftrightarrow 1 + x + y + xy = (1 + x)(1 + y) \\ &\longleftrightarrow \neg X \wedge \neg Y. \end{aligned} \tag{6}$$

Yllä esitellyt merkinnät on tapana lukea seuraavasti:

$$\begin{aligned} X \vee Y &: \mathsf{X\ tai\ Y}, \\ X \wedge Y &: \mathsf{X\ ja\ Y}, \\ X \Rightarrow Y &: \mathsf{X:stä\ seuraa\ Y}, \\ X \Leftrightarrow Y &: \mathsf{X\ ja\ Y\ ovat\ ekvivalentteja}. \end{aligned}$$

Sivupolku

René Thom eräässä kirjoituksessaan [7] analysoi muun muassa logiikan soveltuvuutta luonnollisen kielen analyysiin, ja tekee siinä mielestäni hauskan havainnon. Thom antaa esimerkkejä tapauksista, joissa sanojen JA ja TAI käyttö poikkeaa logiikan käytännöistä. Tarkastellaan väitettä:

> Suomen lippu on sininen ja valkoinen.[4]

Luulisin, että kaikki pitävät väitettä totena. Mutta logiikan mukaan tällöin myös väite ”Suomen lippu on sininen” on tosi. Kuitenkin jos joku esittäisi tällaisen väitteen, niin vastaus todennäköisesti olisi: ”ei se ole sininen, sehän on sininen ja valkoinen”. Thomin ajatus on, että lippu ajatellaan pintana ja sana JA ei viittaa varsinaisesti logiikkaan, vaan siihen, että siniset ja valkoiset alueet ovat geometrisesti lähekkäin.

Tavallaan tässä ollaan tilanteessa, joka on hyvin erilainen kuin mitä logiikassa normaalisti opetetaan. Yleensähän ajatellaan, että JA tarkoittaa, että kaksi eri asiaa on voimassa yhtä aikaa. Lipun tapauksessa kuitenkin vain jompikumpi asioista on voimassa: jokainen lipun piste on joko sininen TAI valkoinen.

Joukko-opillisesti JA usein yhdistetään leikkaukseen. Lipun tapauksessa JA kuitenkin vastaa yhdistettä, koska Suomen lippu on yhdiste valkoisista ja sinisistä alueista.

Jacques Prévertin runo *Composition française* (ranskalainen ainekirjoitus) [6] alkaa näin:

> Tout jeune, Napoléon était très maigre et officier d'artillerie.
>
> Nuorena Napoleon oli hyvin laiha ja tykistöupseeri.

Tämä taas on loogisesti (ja varmaankin myös historiallisesti) täysin oikein, mutta kielellisesti väärin, koska ei ole tapana yhdistää adjektiivia ja substantiivia JA-sanalla. Geometrisesti tämän voisi ajatella niin, että adjektiivit ja substantiivit ovat kategorioina niin ”kaukana” toisistaan, että niitten yhdistäminen tällä tavalla ei ole mielekästä.

Alkeislogiikka on siis varsin hyödytön työkalu luonnollisen kielen analyysiin.

Logiikka 1

Palataan sitten logiikan kaavoihin. Zhegalkin sai idean polynomien käyttämisestä logiikassa lukiessaan Whiteheadin ja Russellin kuuluisaa kirjaa *Principia Mathematica* [14].[5] Ensimmäisen osan sivuilla 98–126 on kymmeniä ellei peräti satoja alkeislogiikan aputuloksia. Tarkkaa lukumäärää on hiukan hankala määrittää, koska lauseet on numeroitu niin epäloogisesti. Kirjan ensimmäisessä osassa myös luvun 5 jälkeen seuraa luku 9. Jotenkin tuntuisi, että tämänkaltaiset käytännöt eivät olisi hyvää mainosta logiikkaa käsittelevälle teokselle. Joka tapauksessa kaikki nuo logiikan kaavat voidaan helposti todistaa polynomien avulla, kuten Zhegalkin huomasi.

Ennen kuin katsotaan tätä tarkemmin tarvitaan vielä yksi käsite: tautologia. Olkoon F jokin looginen lauseke, jossa esiintyy väitteitä X ja Y. F on siis jokin mielekäs kombinaatio merkinnöistä, jotka ovat yhtälössä (5) vasemmalla puolella. Olkoon f vastaava polynomi, joka saadaan käyttämällä yhtälön (5) oikeaa puolta; siis $f \in \mathbb{Z}_2[x, y]$. Nyt sanotaan, että F on tautologia, jos $\mathsf{NF}(f) = 1$.

Tarkastellaan lauseketta

$$F = \big(\neg(X \vee Y)\big) \Leftrightarrow \big(\neg X \wedge \neg Y\big).$$

Yhtäsuuruusmerkki tulkitaan tässä niin, että F on yhtäsuuruusmerkin oikealla puolella oleva merkkijono, joka voidaan muuttaa polynomiksi f käyttämällä vastaavuuksia (5). Nyt F on muotoa $F = F_0 \Leftrightarrow F_1$, joten $f = 1 + f_0 + f_1$. Mutta yhtälössä (6) laskettiin, että $f_0 = f_1$, joten $f = 1$ mistä seuraa, että F on tautologia.

Logiikan tulokset hyvin usein muotoillaan niin, että sanotaan, että jokin lauseke on tautologia. Esimerkiksi suurin osa (tai ehkä kaikki) Principian sivuilla 98–126 olevista tuloksista on tautologioita. Yleisesti ottaen loogisia lausekkeita voidaan sieventää, kun lasketaan lauseketta vastaava Zhegalkinin polynomi. Olkoon

$$\begin{aligned} F &= \Big(X \vee \big(Y \Rightarrow \neg X\big) \wedge \Big(\big(\neg Y \vee \neg X\big) \Rightarrow \big(\neg X \Rightarrow Y\big)\Big) \\ &= F_0 \wedge F_1 = (X \vee F_2) \wedge (F_3 \Rightarrow F_4). \end{aligned}$$

[4] Vaikka Thom ei puhu Suomen lipusta, hänen esimerkissään tosiaan on sinivalkoinen lippu.

[5] Nämä ovat myös netissä:
https://archive.org/details/dli.ernet.247278/page/n1/mode/2up
https://archive.org/details/PrincipiaMathematicaVol2/mode/2up
https://archive.org/details/in.ernet.dli.2015.220247/mode/2up

Vastaavat polynomit ovat

$$\begin{aligned} f_2 &= 1 + y + (1 + x)y, \\ f_3 &= 1 + xy, \\ f_4 &= 1 + 1 + x + (1 + x)y, \\ f_0 &= x + f_2 + xf_2, \\ f_1 &= 1 + f_3 + f_3f_4, \\ f &= f_0f_1 \\ &= x^4y^3 + x^4y^2 + x^3y^2 + x^2y^3 + x^3y + x + y. \end{aligned}$$

Nyt laskemalla jakojäännökset tai käyttämällä kaavaa (3) saadaan $\mathsf{NF}(f) = x+y+xy$. Voidaan siis sanoa, että F sieveni muotoon $X \vee Y$, ja tämä voidaan ilmaista niin, että

$$F \;\Leftrightarrow\; X \vee Y$$

on tautologia.

Jos sitten on enemmän väitteitä, niin otetaan käyttöön enemmän muuttujia. Esimerkiksi pitäisi osoittaa, että seuraava lauseke on tautologia [5, s. 3, kaava (3)], [14, vol. 1, s. 118, lause 4·4]:

$$F = \big(X \wedge (Y \vee Z)\big) \;\Leftrightarrow\; \big((X \wedge Y) \vee (X \wedge Z)\big).$$

Tätä vastaa polynomi $f \in \mathbb{Z}_2[x, y, z]$; käyttämällä kaavoja (5) saadaan

$$\begin{aligned} f &= 1 + x(y + z + yz) + xy + xz + x^2yz \\ &= 1 + xyz + x^2yz. \end{aligned}$$

Koska $x^2 + x$ on nollafunktio, niin $\mathsf{NF}(f) = 1$, joten F on tautologia.

Todistus etenee aina samalla tavalla:

(i) Olkoon annettu jokin logiikan kaava F, joka sisältää väitteitä $X_1, \ldots, X_n$.

(ii) Muodostetaan kaavaa F vastaava polynomi $f \in \mathbb{Z}_2[x_1, \ldots, x_n]$ käyttäen vastaavuuksia (5).

(iii) Lasketaan polynomia f vastaava Zhegalkinin polynomi $\mathsf{NF}(f)$. Jos $\mathsf{NF}(f) = 1$, niin F on tautologia.

Tulkitaan tämä vielä hiukan toisin. Yllä mainittu polynomi f on myös funktio $\mathbb{Z}_2^n \to \mathbb{Z}_2$, ja sitä vastaava Zhegalkinin polynomi $\mathsf{NF}(f)$ on kanoninen muoto tälle funktiolle. Huomaa, että logiikan oppikirjoissa ei käytetä sanaa funktio, vaan totuusarvotaulu(kko).

Katsotaan vielä eräs esimerkki [14, vol. 1, s. 113, lause 3·47]. Pitäisi osoittaa, että seuraava lauseke on tautologia. Whitehead ja Russell sanovat, että tämä tulos on peräisin Leibnizilta.

$$F = \big((A \;\Rightarrow\; X) \wedge (B \;\Rightarrow\; Y)\big) \;\Rightarrow\; \big(A \wedge B \;\Rightarrow\; X \wedge Y\big).$$

Jaetaan taas lauseke osiin:

$$\begin{aligned} F &= F_0 \;\Rightarrow\; F_1, \\ F_0 &= (A \;\Rightarrow\; X) \wedge (B \;\Rightarrow\; Y), \\ F_1 &= A \wedge B \;\Rightarrow\; X \wedge Y. \end{aligned}$$

ja lasketaan vastaavat polynomit:

$$\begin{aligned} f_0 &= (1 + a + ax)(1 + b + by), \\ f_1 &= 1 + ab + abxy, \\ f &= 1 + f_0 + f_0f_1, \\ &= a^2b^2x^2y^2 + a^2b^2x^2y + a^2b^2xy^2 + a^2bx^2y + \\ &\quad ab^2xy^2 + a^2b^2x + a^2b^2y + a^2bxy + ab^2xy + \\ &\quad a^2b^2 + a^2bx + ab^2y + abxy + a^2b + ab^2 + ab + 1. \end{aligned}$$

Laskemalla jakojäännökset nähdään, että $\mathsf{NF}(f) = 1$, joten F on tautologia. Tämä esimerkki oli jo hiukan työläs käsin laskien, mutta Sagen avulla hyvin helppo:

```
R1 = PolynomialRing(GF(2), 'a, b, x,y');
a,b,x,y = R1.gens();
f0=(1+a+a*x)*(1+b+b*y);
f1=1+a*b+a*b*x*y; f=1+f0+f0*f1;
g0=a^2+a; g1=b^2+b;
g2=x^2+x; g3=y^2+y;
qr=f.quo_rem(g0);r1=qr[1];
qr=r1.quo_rem(g1);r2=qr[1];
qr=r2.quo_rem(g2);r3=qr[1];
qr=r3.quo_rem(g3);r4=qr[1];
```

Polynomi r4 on $\mathsf{NF}(f)$, ja yllä olevat laskut antavat $\mathsf{NF}(f) = 1$.

Metsänkylän ja Näätäsen kirjassa [5] on sivulla 3 lueteltu 12 tautologiaa. Lukija voi harjoitustehtävänä tarkistaa, että todistukset polynomien avulla ovat hyvin helppoja.

1 + 1 = 2

Jos googlettaa hakusanoilla ”principia mathematica 1+1=2”, niin saa yli 300000 osumaa. Tällä viitataan usein kuvassa 1 olevaan lauseeseen 54·43, jossa ei kuitenkaan vielä varsinaisesti todisteta, että $1 + 1 = 2$, vaan vasta pohjustetaan tätä.

***54·43.** $\vdash :. \alpha, \beta \in 1 . \supset : \alpha \cap \beta = \Lambda . \equiv . \alpha \cup \beta \in 2$

Dem.

$\vdash . *54·26 . \supset \vdash :. \alpha = \iota`x . \beta = \iota`y . \supset : \alpha \cup \beta \in 2 . \equiv . x \neq y .$

$[*51·231] \qquad \equiv . \iota`x \cap \iota`y = \Lambda .$

$[*13·12] \qquad \equiv . \alpha \cap \beta = \Lambda \qquad (1)$

$\vdash . (1) . *11·11·35 . \supset$

$\vdash :. (\exists x, y) . \alpha = \iota`x . \beta = \iota`y . \supset : \alpha \cup \beta \in 2 . \equiv . \alpha \cap \beta = \Lambda \qquad (2)$

$\vdash . (2) . *11·54 . *52·1 . \supset \vdash .$ Prop

From this proposition it will follow, when arithmetical addition has been defined, that $1 + 1 = 2$.

Kuva 1: Whiteheadin ja Russellin kuuluisa lause.

Oleellisesti lause sanoo, että jos $A = \{p\}$, $B = \{q\}$ ja $p \neq q$, niin joukossa $A \cup B = \{p, q\}$ on kaksi alkiota.[6]

Kyseinen lause on sivulla 362, ja koko kirjassa on yli 700 sivua, mutta Lauseeseen $110 \cdot 643$, jossa $1 + 1 = 2$ sitten lopulta todistetaan, päästään kuitenkin vasta kirjasarjan toisessa osassa, sivulla 83. Tarkkaan ottaen merkkiä + ei käytetä, vaan jostain syystä on valittu muoto $1 +_\circ 1 = 2$. Kirjoittajat huomauttavat lauseen todistuksen jälkeen:

> The above proposition is occasionally useful.

En tiedä, missä vaiheessa kertolasku määritellään, vai päästäänkö edes niin pitkälle.

Viitteet

[1] G. V. Bard, *Sage for undergraduates*, 2nd ed., American Mathematical Society, 2022.

[2] L. Carroll, *Through the looking-glass, and what Alice found there*, 1871.

[3] D. A. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms*, 4th ed., Undergraduate Texts in Mathematics, Springer, Cham, 2015, An introduction to computational algebraic geometry and commutative algebra.

[4] I. I. Gégalkine, *Sur le calcul des propositions dans la logique symbolique*, Mat. Sb. **34** (1927), no. 1, 9–28.

[5] T. Metsänkylä and M. Näätänen, *Algebra*, 2010, https://matematiikkalehtisolmu.fi/2010/algebra.pdf.

[6] J. Prévert, *Paroles*, Gallimard, 1976.

[7] R. Thom, *"Modern" mathematics: An educational and philosophic error?*, American Scientist **59** (1971), no. 6, 695–699.

[8] J. Tuomela, *Tarinoita polynomeista (osa 1)*, Solmu (2022), no. 2.

[9] _____, *Tarinoita polynomeista (osa 2)*, Solmu (2022), no. 3.

[10] _____, *Tarinoita polynomeista (osa 3)*, Solmu (2023), no. 2.

[11] _____, *Tarinoita polynomeista (osa 4)*, Solmu (2023), no. 3.

[12] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, 3rd ed., Cambridge University Press, 2013.

[13] J. Walker, *Codes and curves*, Student Mathematical Library, vol. 7, American Mathematical Society, 2000.

[14] A. N. Whitehead and B. Russell, *Principia mathematica, vols. I–III*, 2nd ed., Cambridge University Press, 1925-27.

[6] Lausetta ja sen todistusta on tarkemmin pohdittu täällä: https://blog.plover.com/math/PM.html