SANAYHTÄLÖIDEN PARAMETRISET RATKAISUT

Aleksi Saarela

Pro gradu -tutkielma
Marraskuu 2007

MATEMATIIKAN LAITOS
TURUN YLIOPISTO

TURUN YLIOPISTO
Matematiikan laitos

SAARELA, ALEKSI: Sanayhtälöiden parametriset ratkaisut
Pro gradu -tutkielma, 47 s.
Matematiikka
Marraskuu 2007

Työ kuuluu sanojen kombinatoriikan alaan ja siinä käsitellään sanayhtälöitä. Tarkastelun kohteena on sanayhtälöiden ratkaisujen esittäminen parametristen sanojen avulla.

Hmelevskii todisti (*Equations in free semigroups*; Proceedings of the Steklov Institute of Mathematics, 107, 1971; käännös, American Mathematical Society, 1976), että kaikkien niiden kolmen muuttujan sanayhtälöiden, joissa ei ole vakioita, ratkaisut voidaan esittää parametrisesti, mutta neljän muuttujan yhtälöille tämä ei enää pidä paikkaansa. Työn tavoitteena on näiden tulosten todistaminen.

Työssä esitetään sanojen ja sanayhtälöiden perusteet, määritellään täsmällisesti sanaparametreistä ja näiden eksponentteina olevista numeerisista parametreistä koostuvat parametriset sanat ja todistetaan joitakin tarvittavia aputuloksia. Tämän jälkeen todistetaan Hmelevskiin tulokset yhtälöiden ratkaisuiden parametrisoituvuudesta. Neljän muuttujan yhtälöiden tapaus on helpompi ja perustuu Czeizlerin yksinkertaistettuun todistukseen (*The non-parametrizability of the word equation $xyz = zvx$: a short proof*; Theoretical Computer Science, 345:296–303, 2005). Kolmen muuttujan yhtälöiden käsittely seuraa enimmäkseen Hmelevskiin todistusta ja muodostaa pääosan työstä.

Asiasanat: Sanojen kombinatoriikka, sanayhtälöt, parametriset sanat

Sisältö

1 Johdanto

Tämän työn aiheena ovat sanat eli merkkijonot yli jonkin äärellisen symbolijoukon. Sanoille voidaan määritellä laskutoimitus katenaatio, joka vastaa näiden laittamista peräkkäin. Näin syntyy algebrallinen struktuuri, joka on äärellisesti generoitu vapaa monoidi. Sanojen kombinatoriikan perusteoksia ovat Lothairen kirjat *Combinatorics on words* [5] ja *Algebraic combinatorics on words* [6].

Sanamonoidissa voidaan määritellä yhtälöt tavalliseen tapaan. Näiden ratkaiseminen on yleisesti vaikeaa. Alan merkittäviä tuloksia on Makaninin algoritmi, joka ratkaisee sen, onko annetulla yhtälöllä ratkaisuja vai ei.

Sanayhtälöillä on tyypillisesti äärettömän monta ratkaisua. Siksi ennen kysymystä yhtälön ratkaisemisesta pitää pohtia, miten nämä ratkaisut voisi esittää äärellisesti. Yksi moniin tapauksiin sopiva menetelmä on parametriset sanat. Tämä työ tarkastelee sitä, milloin kaikki ratkaisut voidaan esittää parametristen sanojen avulla.

Parametrisissä sanoissa on sanaparametrejä ja numeerisia parametrejä näiden eksponentteina. Esimerkiksi konjugointiyhtälön $xz = zy$ ratkaisut ovat

$$x = pq, \quad y = qp, \quad z = p(qp)^i \qquad \text{tai} \qquad x = y = 1, \ z = p,$$

missä sanaparametrit p ja q voivat olla mitä tahansa sanoja ja numeerinen parametri i voi olla positiivinen kokonaisluku tai nolla. Hmelevskii todisti [3], että kaikkien niiden kolmen muuttujan sanayhtälöiden, joissa ei ole vakioita, ratkaisut voidaan esittää parametristen sanojen avulla. Lisäksi hän antoi esimerkin neljän muuttujan yhtälöstä, jonka ratkaisuja ei voida esittää parametrisesti. Jatkossa oletetaan aina yhtälöiden olevan vakiottomia.

Tämä työ alkaa luvussa 2 joidenkin sanojen kombinatoriikan perusasioiden lyhyellä esittämisellä. Erityisesti käsitellään sanayhtälöitä ja todistetaan muutamia niihin liittyviä yksinkertaisia lemmoja, joita tarvitaan myöhemmin.

Luvussa 3 määritellään parametriset sanat ja joukkojen esittäminen näiden avulla, jolloin voidaan esittää täsmällisesti työn varsinaisena tavoitteena oleva Hmelevskiin tulos. Parametristen sanojen avulla voidaan myös käsitellä eksponenttiyhtälöitä, jotka ovat tärkeä osa tämän tuloksen todistusta. Luvun lopuksi todistetaan, että neljän muuttujan yhtälön $xuy = yvx$ ratkaisuja ei voida esittää parametrisesti; tämä tulos on selvästi helpompi kuin kolmen muuttujan yhtälöiden ratkaisujen parametrisoituvuuden todistaminen.

Kahdessa viimeisessä luvussa tarkastellaan kolmen muuttujan yhtälöitä. Luvussa 4 todistetaan päätulos osalle kaikista tällaisista yhtälöistä. Tämän jälkeen tavoittena on palauttaa kaikkien yhtälöiden ratkaisut näiden perus-

yhtälöiden ratkaisuihin. Tärkein menetelmä tässä ovat yhtälöiden kuvat ja θ-kuvat, joiden käsittely vie suurimman osan luvusta 4.

Luvussa 5 todistetaan luvun 4 tulosten pohjalta, että jokaisen kolmen muuttujan yhtälön ratkaisut voidaan esittää parametrisesti. Tämä tapahtuu palauttamalla yhtälöt vaiheittain toisenlaisiin yhtälöihin, jolloin muodostuu puumainen rakenne. Päätulos todistetaan osoittamalla, että jokainen yhtälö voidaan tällä tavalla palauttaa luvussa 4 käsiteltyihin perusyhtälöihin.

2 Merkintöjä ja perustuloksia

Tässä luvussa määritellään käsitteitä ja esitellään merkintöjä, perustuloksia ja joitakin myöhemmin tarvittavia lemmoja. Peruslauseitten todistukset löytyvät kirjan *Handbook of Formal Languages* luvusta *Combinatorics of words* [1]; se on muutenkin hyvä sanojen kombinatoriikan lähde.

2.1 Sanoista yleisesti

Aakkosto on mikä tahansa äärellinen epätyhjä joukko Σ. Sen alkiot ovat *kirjaimia*. *Sanat* yli tämän aakkoston ovat kaikki sen alkioista koostuvat äärelliset jonot; näiden joukosta käytetään merkitään Σ^*. Siis

$$\Sigma^* = \{a_1 \dots a_n : n \geq 0, a_1, \dots, a_n \in \Sigma\}.$$

Erityisesti joukkoon Σ^* kuuluu nollasta merkistä koostuva *tyhjä sana*, jota merkitään symbolilla 1. Lisäksi merkitään $\Sigma^+ = \Sigma^* \setminus \{1\}$.

Sanojen $u = a_1 \dots a_m$ ja $v = b_1 \dots b_n$ *katenaatio* on

$$u \cdot v = a_1 \dots a_m b_1 \dots b_n.$$

Tavalliseen tapaan piste voidaan jättää merkitsemättä ja puhua tulosta uv. Tyhjä sana 1 on neutraalialkio ja $(\Sigma^*, \cdot)$ on vapaa monoidi.

Sanan w potensseista koostuvasta joukosta $\{w^n : n = 0, 1, 2, \dots\}$ voidaan käyttää merkintää w^*.

Sanan $w = a_1 \dots a_n$ *pituus* on $|w| = n$. Kirjaimen a esiintymien lukumäärää sanassa w merkitään $|w|_a$.

Sana u on sanan w alkuosa eli *prefiksi*, jos on olemassa sellainen sana v, että $uv = w$. Tällöin merkitään $u \leq w$. Jos tässä $v \neq 1$ eli $u \neq w$, niin u on aito prefiksi ja merkitään $u < w$. Vastaavasti määritellään sanan loppuosa eli *suffiksi*.

Sanan $w = a_1 \dots a_n$ *käänteinen sana* on $w^R = a_n \dots a_1$.

Jos Σ on aakkosto ja M monoidi, niin kuvaus $h : \Sigma^* \to M$ on *morfismi*, jos $h(uv) = h(u)h(v)$ kaikilla $u, v \in \Sigma^*$. Mikä tahansa kuvaus $h : \Sigma \to M$ voidaan laajentaa yksikäsitteisellä tavalla tällaiseksi morfismiksi. Jos $\Sigma = \{a_1, \dots, a_n\}$, niin sanasta $U \in \Sigma^*$ voidaan käyttää myös merkintää $U(a_1, \dots, a_n)$, jolloin voidaan merkitä $h(U) = U(h(a_1), \dots, h(a_n))$. Jos $M = \Sigma^*$, niin morfismilla $a_1 \mapsto u$ tarkoitetaan sitä yksikäsitteistä morfismia, joka kuvaa $a_1 \mapsto u$ ja $a_i \mapsto a_i$, kun $i = 2, \dots, n$.

Sana w on *primitiivinen*, jos se ei ole aito potenssi eli jos sitä ei voi esittää muodossa t^n, missä $t \neq w$. Jokainen sana w voidaan esittää yksikäsitteisellä tavalla muodossa t^n siten, että t on primitiivinen; tällöin t on sanan w *primitiivinen juuri* ja merkitään $t = \rho(w)$.

Sanat u ja v *kommutoivat*, jos $uv = vu$. Seuraavat ehdot ovat ekvivalentit:

(i) u ja v kommutoivat,

(ii) u ja v toteuttavat epätriviaalin relaation,

(iii) on olemassa sellainen sana t, että $u, v \in t^*$,

(iv) $\rho(u) = \rho(v)$.

Sanat u ja v ovat *konjugaatteja*, jos on olemassa sellaiset sanat p ja q, että $u = pq$ ja $v = qp$. Jos $u, v \neq 1$, niin seuraavat ehdot ovat ekvivalentit:

(i) u ja v ovat konjugaatteja,

(ii) on olemassa sellainen sana z, että $uz = zv$,

(iii) on olemassa sellaiset sanat z, p, q ja luku $k \geq 0$, että $u = pq$, $v = qp$ ja $z = p(qp)^k$.

2.2 Sanayhtälöt

Seuraavassa määritellään sanayhtälöt. Yleisesti niissä voisi esiintyä tuntemattomien lisäksi vakioita, mutta tässä määritelmässä ja jatkossa käsitellään vain yhtälöitä, joissa ei ole vakioita.

Oletetaan, että on kiinnitetty aakkosto Σ ja tuntemattomien aakkosto Ξ. Tällöin yhtälö E on pari (U, V), missä $U, V \in \Xi^*$. Tätä merkitään $U = V$. Yhtälön E ratkaisuja ovat kaikki morfismit $h : \Xi^* \to \Sigma^*$, joille $h(U) = h(V)$. Jos tuntemattomat ovat järjestyksessä $x_1, \ldots, x_n$, niin voidaan puhua myös ratkaisusta $(h(x_1), \ldots, h(x_n))$ tai ratkaisusta $x_1 = h(x_1), \ldots, x_n = h(x_n)$. Jos $h(x_1), \ldots, h(x_n) \in t^*$ jollakin $t \in \Sigma^*$, niin ratkaisu h on *jaksollinen*.

Määritellään tavallisten yhtälöiden lisäksi myös yksipuoliset yhtälöt. Tässä vaaditaan, että U ja V alkavat eri kirjaimilla. Yksipuolista yhtälöä merkitään $U \rightrightarrows V$, ja sen ratkaisuja ovat ne yhtälön $U = V$ ratkaisut h, joille $h(x) \geq h(y)$, missä x on sanan U ja y sanan V ensimmäinen kirjain. Merkintä $V \lleftarrow U$ tarkoittaa samaa kuin $U \rightrightarrows V$.

Jos $x \in \Xi$ ja $U, V \in \Xi^*$, niin yhtälöillä $U = V$, $xU = xV$ ja $Ux = Vx$ on samat ratkaisut. Tämän vuoksi yhtälöitä voidaan supistaa ja kertoa vasemmalta tai oikealta. Sama on voimassa yksipuolisille yhtälöille oikealta operoinnin suhteen, mutta yksipuolisen yhtälön määrittely tekee vasemmalta operoinnin mahdottomaksi.

Edellisessä osiossa todetun nojalla saadaan ratkaisut jokaiselle kahden muuttujan yhtälölle sekä konjugointiyhtälölle $xz = zy$.

2.1 Lause. *Olkoot $U, V \in \{x, y\}^*$ eri sanoja. Oletetaan, että $|U|_x = a$, $|U|_y = b$, $|V|_x = c$ ja $|V|_y = d$. Kahden muuttujan yhtälön $U = V$ ratkaisut ovat*

$$x = t^i,\ y = t^j,$$

missä $t \in \Sigma^*$, $ai + bj = ci + dj$ ja $i, j \geq 0$

2.2 Lause. *Yhtälön $xz = zy$ ratkaisut ovat*

$$x = pq,\quad y = qp,\quad z = p(qp)^i \qquad tai \qquad x = y = 1,\ z = p,$$

missä $p, q \in \Sigma^*$ ja $i \geq 0$.

Yhtälöiden ratkaisemisessa voidaan käyttää apuna esimerkiksi edellisiä yhtälöitä, pituusargumentteja ja sijoituksia. Hyödyllisiä ovat myös kaksi seuraavaa lausetta: Finen ja Wilfin lemma sekä Graafilemma.

2.3 Lause (Fine ja Wilf)**.** *Olkoon $u, v \in \Sigma^+$, $u' < u$, $v' < v$ ja*

$$|u^m u'| = |v^n v'| \geq |u| + |v| - \mathrm{syt}(|u|, |v|).$$

Tällöin $u^m u' = v^n v'$ jos ja vain jos $uv = vu$.

2.4 Lause (Graafilemma)**.** *Olkoon E yhtälöryhmä. Muodostetaan graafi, jonka solmuja ovat tuntemattomat, ja jossa solmujen x, y välillä on kaari, jos E sisältää jonkin muotoa $x \ldots = y \ldots$ olevan yhtälön. Oletetaan, että tässä graafissa on c yhtenäistä komponenttia. Olkoon $\Xi = \{x_1, \ldots, x_n\}$ ja $h : \Xi^* \to \Sigma^*$ jokin yhtälöryhmän E ratkaisu. Nyt on olemassa sellainen c-alkioinen joukko $F \subset \Sigma^*$, että $h(x_1), \ldots, h(x_n) \in F^*$.*

Lauseesta 2.4 tulee käyttöön seuraava erikoistapaus.

2.5 Seuraus. *Olkoon $A, B, C, D \in \{x, y, z\}^*$. Kolmen muuttujan yhtälöparin $xA = yB, xC = zD$, kaikki ratkaisut h, joille $h(x), h(y), h(z) \neq 1$, ovat jaksollisia.*

Finen ja Wilfin lemmaa käytetään ensimmäisen kerran jo lemman 2.9 todistuksessa. Graafilemmaa tarvitaan vasta myöhemmin, joten esitetään sen käytöstä esimerkki.

2.6 Esimerkki. Tarkastellaan yhtälöä $xyzxzy = yzxzyx$. Koska $|h(xyz)| = |h(yzx)|$ kaikilla morfismeilla h, niin yhtälö on ekvivalentti yhtälöparin $xyz = yzx$, $xzy = zyx$ kanssa. Olkoon h tämän ratkaisu. Jos $h(y) = 1$ tai $h(z) = 1$, niin h on jaksollinen. Jos $h(x) = 1$, niin yhtälö tulee muotoon $yzzy = yzzy$. Seurauksen 2.5 mukaan yhtälöllä on näiden lisäksi vain jaksollisia ratkaisuja. Siis ratkaisut ovat

$$x = p^i,\quad y = p^j,\quad z = p^k \qquad \text{tai} \qquad x = 1,\quad y = p,\quad z = q,$$

missä $p, q \in \Sigma^*$ ja $i, j, k \geq 0$.

Seurausta 2.5 käytetään usein pituusargumentin kanssa, kuten esimerkissä 2.6: jos jokainen muuttuja esiintyy sanassa xA yhtä monesti kuin sanassa yB, niin yhtälöillä $xAxC = yBzD$ ja $xAzD = yBxC$ on vain jaksollisia ratkaisuja sekä ratkaisuja, joissa jokin muuttujista saa arvon 1.

Seuraavat lemmat antavat ratkaisut joillekin myöhemmin tarvittaville yhtälöille ja toimivat samalla esimerkkeinä yhtälöiden ratkaisemisesta. Jaksollisten ratkaisujen määrittäminen on helppoa, joten lemmoissa käsitellään vain jaksottomia ratkaisuja.

2.7 Lemma. *Yhtälön $xyz = zyx$ jaksottomat ratkaisut ovat*

$$x = (pq)^i p, \quad y = q(pq)^j, \quad z = (pq)^k p,$$

missä $p, q \in \Sigma^*$, $i, j, k \geq 0$, $pq \neq qp$ ja pq voidaan olettaa primitiiviseksi.

Todistus. Väitetyt ratkaisut toteuttavat yhtälön ja ovat jaksottomia. Jos h on jokin jaksoton ratkaisu, niin $h(xyzy) = h(zyxy)$, joten $h(xy) = t^m$ ja $h(zy) = t^n$, missä t on primitiivinen ja $m, n > 0$. Nyt $h(y) = q(pq)^j$, missä $pq = t$ ja $0 \leq j < m, n$, jolloin $h(x) = (pq)^i p$ ja $h(z) = (pq)^k p$, missä $i = m - j - 1$ ja $k = n - j - 1$. Jos p ja q kommutoisivat, niin ratkaisu olisi jaksollinen. □

2.8 Lemma. *Yhtälön $xyz = zxy$ jaksottomat ratkaisut ovat*

$$x = (pq)^i p, \quad y = q(pq)^j, \quad z = (pq)^k,$$

missä $p, q \in \Sigma^*$, $i, j, k \geq 0$ ja $pq \neq qp$.

Todistus. Väitetyt ratkaisut toteuttavat yhtälön ja ovat jaksottomia. Jos h on jokin jaksoton ratkaisu, niin $h(xy) = t^m$ ja $h(z) = t^k$, missä $m > 0, k \geq 0$. Nyt $h(y) = q(pq)^j$, missä $pq = t$ ja $0 \leq j < m$, jolloin $h(x) = (pq)^i p$ ja $h(z) = (pq)^k$, missä $i = m - j - 1$. Jos p ja q kommutoisivat, niin ratkaisu olisi jaksollinen. □

2.9 Lemma. *Olkoon $a \geq 2$. Yhtälön $xzx = y^a$ jaksottomat ratkaisut ovat*

$$x = (pq)^i p, \quad y = (pq)^{i+1} p, \quad z = qp((pq)^{i+1} p)^{a-2} pq,$$

missä $p, q \in \Sigma^*$, $i \geq 0$ ja $pq \neq qp$.

Todistus. Väitetyt ratkaisut toteuttavat yhtälön ja ovat jaksottomia. Olkoon h jokin jaksoton ratkaisu. Jos olisi $|h(x)| \geq |h(y)|$ niin lauseen 2.3 perusteella $h(xz)$ ja $h(y)$ ovat saman sanan potensseja, josta seuraa, että ratkaisu on jaksollinen. Siis $|h(x)| < |h(y)|$. Tällöin $h(y) = uh(x) = h(x)v$, missä $u, v \neq 1$, ja $h(z) = vh(y)^{a-2}u$. Nyt lauseen 2.2 perusteella $u = pq$, $v = qp$, $h(x) = (pq)^i p$, $h(y) = (pq)^{i+1} p$ ja $h(z) = qp((pq)^{i+1} p)^{a-2} pq$. Jos p ja q kommutoisivat, niin ratkaisu olisi jaksollinen. □

2.10 Lemma. *Olkoon $a \geq 2$. Yhtälön $xy^az = zy^ax$ jaksottomat ratkaisut ovat*

$$x = (pq^a)^i p, \quad y = q, \quad z = (pq^a)^j p \tag{1}$$

tai

$$\begin{cases} x &= qp((pq)^{k+1}p)^{a-2}pq(((pq)^{k+1}p)^{a-1}pq)^i, \\ y &= (pq)^{k+1}p, \\ z &= qp((pq)^{k+1}p)^{a-2}pq(((pq)^{k+1}p)^{a-1}pq)^j, \end{cases} \tag{2}$$

missä $p, q \in \Sigma^*$, $i, j, k \geq 0$ ja $pq \neq qp$.

Todistus. Väitetyt ratkaisut toteuttavat yhtälön ja ovat jaksottomia. Jos h on jokin jaksoton ratkaisu, niin lemman 2.7 perusteella

$$h(x) = u(vu)^i, \ h(y^a) = v(uv)^b, \ h(z) = u(vu)^j,$$

missä uv on primitiivinen. Jos $b = 0$, tästä saadaan muotoa (1) oleva ratkaisu. Jos $b > 1$, niin lemman 2.3 nojalla $h(y)$ ja primitiivinen sana vu kommutoivat. Tällöin välttämättä $u = 1$ tai $v = 1$ ja $h(x), h(y), h(z) \in (uv)^*$, mikä on ristiriidassa oletuksen kanssa. Jos $b = 1$, niin lemman 2.9 mukaan $h(v) = (pq)^k p$, $h(y) = (pq)^{k+1}p$ ja $h(u) = qp((pq)^{k+1}p)^{a-2}pq$. Tästä saadaan muotoa (2) oleva ratkaisu. Jos p ja q kommutoisivat, niin ratkaisut olisivat jaksollisia. □

2.11 Lemma. *Yhtälön $xyxz \rightrightarrows zx^2y$ jaksottomat ratkaisut ovat*

$$x = (pq)^i p, \quad y = pq, \quad z = qp((pq)^{i+1}p)^j pq,$$

missä $p, q \in \Sigma^*$, $i, j \geq 0$ ja $pq \neq qp$.

Todistus. Väitetyt ratkaisut toteuttavat yhtälön ja ovat jaksottomia. Jos h on jokin jaksoton ratkaisu, niin lemman 2.7 perusteella

$$h(xy) = (uv)^b u, \ h(x) = v(uv)^c, \ h(z) = (uv)^d u.$$

Koska $h(z) \leq h(x) \leq h(xy)$ ja $uv \neq vu$, niin $h(z) = u \leq h(x) = v \leq uv$. Nyt on oltava $h(z) = pq$ ja $h(x) = (pq)^i p$, jolloin $y = qp((pq)^{i+1}p)^j pq$. Jos p ja q kommutoisivat, niin ratkaisut olisivat jaksollisia. □

2.12 Lemma. *Olkoon $a, b \geq 1$ ja $U, V \in \Xi^*$. Jos h on yhtälön $x^ayU = y^bxV$ ratkaisu, niin $h(x)$ ja $h(y)$ kommutoivat.*

Todistus. Symmetrian vuoksi voidaan olettaa, että $h(x) \leq h(y)$. Tällöin $h(y) = h(x)^c t$, missä $h(x) \not\leq t$. Koska $h(x)^{a+c} \ldots = h(x)^c t \ldots$, niin $t \leq h(x)$. Nyt $h(x)^{a+c}t \ldots = h(y)^b h(x) \ldots$ ja $|h(x)^{a+c}t|, |h(y)^b h(x)| \geq |h(x)h(y)|$, joten väite seuraa lauseesta 2.3. □

2.3 Diofantoksen yhtälöt ja relaatiot

Jatkossa tarvitaan lineaarisista Diofantoksen yhtälöistä ja epäyhtälöistä koostuvia ehtoja, sekä keinoa kuvata sanat polynomeiksi.

2.13 Määritelmä. Olkoon $A = \{a_1, \ldots, a_N\}$ jokin N-alkioinen joukko ja R joukko funktioita $A \to \mathbb{N}_0 = \{0, 1, 2, \ldots\}$. Joukko R on *lineaarinen Diofantoksen relaatio*, jos on olemassa sellaiset luvut $M, K_m, C_{mn} \geq 0$ ja lineaariset polynomit $p_{mk} \in \mathbb{Z}[x_1, \ldots, x_N]$ ($m = 1, \ldots, M$; $n = 1, \ldots, N$; $k = 1, \ldots, K_m$), että $f \in R$ jos ja vain jos

$$\bigvee_{m=1}^{M} \left(\left(\bigwedge_{k=1}^{K_m} p_{mk}(f(a_1), \ldots, f(a_N)) = 0 \right) \wedge \left(\bigwedge_{n=1}^{N} f(a_n) \geq C_{mn} \right) \right). \tag{3}$$

Lineaarisen Diofantoksen relaation määrittelevä ehto (3) on siis disjunktio lineaarisista yhtälöryhmistä täydennettynä muuttujien $f(a_1), \ldots, f(a_N)$ alarajoilla.

2.14 Esimerkki. Jos määritelmän 2.13 joukossa A on vain yksi alkio a, niin ehto (3) tulee muotoon

$$\bigvee_{m=1}^{M} \left(\left(\bigwedge_{k=1}^{K_m} b_k f(a) + c_k = 0 \right) \wedge \left(\bigwedge_{n=1}^{N} f(a) \geq C_{mn} \right) \right)$$

joillakin kokonaisluvuilla b_k, c_k. Siis joko R on äärellinen joukko tai on olemassa sellainen äärellinen joukko $B \subset \mathbb{N}_0$ ja luku C, että $f \in R$ jos ja vain jos $f(a) \in B$ tai $f(a) \geq C$.

Aakkosto Ξ, jossa on k kirjainta, voidaan ajatella joukoksi $\{1, \ldots, k\}$. Tällöin voidaan määritellä funktiot $\lambda, \mu : \Xi^* \to \mathbb{Z}[X]$:

$$\begin{aligned} \lambda(w) &= X^{m+1}, \\ \mu(w) &= a_m X^m + \cdots + a_1 X + a_0 \end{aligned}$$

kaikilla $w = a_m \ldots a_0 \in \Xi^*$. Tämän voi ajatella vastaavan myös luvun n-arista esitystä, kun $n > k$: sana w esittää n-kantaisessa lukujärjestelmässä lukua, joka saadaan sijoittamalla polynomissa $\mu(w)$ muuttujan X paikalle luku n.

2.15 Esimerkki. Jos $u, v \in \Xi^*$, niin $\mu(uv) = \mu(u)\lambda(v) + \mu(v)$. Jos $w \in \Xi^+$ ja $i > 0$, niin

$$\begin{aligned} \mu(w^i) &= \mu(w)\lambda(w^{i-1}) + \mu(w)\lambda(w^{i-2}) + \cdots + \mu(w)\lambda(w) + \mu(w) \\ &= \mu(w)\left(\lambda(w)^{i-1} + \lambda(w)^{i-2} + \cdots + \lambda(w) + 1\right) \\ &= \frac{\mu(w)\,(1 - \lambda(w)^i)}{1 - \lambda(w)}. \end{aligned}$$

Toinen tapa kirjoittaa tämä on

$$\frac{\mu(w)}{1-\lambda(w)} = \frac{\mu(w^i)}{1-\lambda(w^i)}.$$

Esimerkin 2.15 kaavat ovat tärkeitä jatkossa. Kuvaus μ sanoilta polynomeille on selvästi injektiivinen, joten saadaan seuraava lause.

2.16 Lause. *Olkoon Ξ mikä tahansa aakkosto. Sanat $U, V \in \Xi^*$ ovat samat jos ja vain jos polynomit $\mu(U)$ ja $\mu(V)$ ovat samat.*

3 Parametriset ratkaisut

Tässä luvussa määritellään parametriset sanat ja joukkojen esittäminen näiden avulla. Parametristen sanojen avulla voidaan myös määritellä eksponenttiyhtälöt, jotka ovat tärkeitä jatkossa. Eksponenttiyhtälöihin liittyviä lauseita todistetaan suoraan Hmelevskiin esitystä seuraten ja edellä todetun sanojen ja polynomien yhteyden avulla. Luvun lopuksi todistetaan, että neljän muuttujan yhtälön $xuy = yvx$ ratkaisuja ei voida esittää parametrisesti.

3.1 Parametriset sanat

Määritellään parametriset sanat.

3.1 Määritelmä. Kiinnitetään *sanaparametrien* aakkosto Δ ja *numeeristen parametrien* joukko $\mathcal{N}$. Nyt *parametriset sanat* määritellään seuraavasti:

(i) jos $a \in \Delta \cup \{1\}$, niin (a) on parametrinen sana,

(ii) jos α ja β ovat parametrisiä sanoja, niin samoin on $(\alpha\beta)$,

(iii) jos α on parametrinen sana ja $i \in \mathcal{N}$, niin (α^i) on parametrinen sana,

(iv) kaikki parametriset sanat saadaan näin.

Jatkossa oletetaan aina parametrisistä sanoista puhuttaessa, että parametrijoukot ovat Δ ja $\mathcal{N}$.

Sovitaan, että funktiolla $f : \mathcal{N} \to \mathbb{N}_0$ voidaan kuvata parametrisiä sanoja seuraavien sääntöjen mukaisesti:

(i) jos $a \in \Delta \cup \{1\}$, niin $f((a)) = a$,

(ii) jos α ja β ovat parametrisiä sanoja, niin $f((\alpha\beta)) = f(\alpha)f(\beta)$,

(iii) jos α on parametrinen sana ja $i \in \mathcal{N}$, niin $f((\alpha^i)) = f(\alpha)^{f(i)}$.

Parametrinen sana siis kuvautuu joukon Δ^* sanaksi, joka saadaan antamalla numeerisille parametreille lukuarvot funktiolla f. Tämä sana voidaan edelleen kuvata morfismilla $h : \Delta^* \to \Sigma^*$ joukon Σ^* sanaksi, missä Σ on jokin aakkosto; siis annetaan sanaparametreille arvot funktiolla h. Yhdistettyä kuvausta $h \circ f$ sanotaan *arvotukseksi*. Myös f voidaan tulkita arvotukseksi joukolle Δ^*. Aina puhuttaessa arvotuksesta $h \circ f$ oletetaan, että f ja h ovat kuten edellä.

Parametriset sanat α ja β voidaan samaistaa, jos $f(\alpha) = f(\beta)$ kaikilla funktioilla $f : \mathcal{N} \to \mathbb{N}_0$. Nyt voidaan merkintöjen yksinkertaistamiseksi sopia, että potenssi sitoo kertolaskua vahvemmin, jättää turhia sulkuja pois ja lisäksi merkitä esimerkiksi $\alpha^i\alpha^j = \alpha^{i+j}$ ja $(\alpha^i)^j = \alpha^{ij}$.

3.2 Esimerkki. Olkoon $\Delta = \{a, b\}$ ja $\mathcal{N} = \{i\}$. Parametriset sanat

$$((((a)(b))^i)((a)(b))) \qquad \text{ja} \qquad ((a)((((b)(a))^i)(b)))$$

voidaan samaistaa ja kirjoittaa $(ab)^{i+1}$.

Jos määritellään parametristen sanojen α ja β tuloksi $\alpha\beta$, niin parametriset sanat muodostavat monoidin ja tavallisia sanoja voidaan kuvata parametrisiksi sanoiksi morfismeilla.

3.3 Määritelmä. Määritellään parametrisen sanan *aste*:

(i) jos $a \in \Delta \cup \{1\}$, niin sanan a aste on nolla,

(ii) jos α ja β ovat parametrisiä sanoja, niin sanan $\alpha\beta$ aste on maksimi sanojen α, β asteista,

(iii) jos $\alpha \neq 1$ on parametrinen sana ja $i \in \mathcal{N}$, niin sanan α^i aste on yhtä suurempi kuin sanan α aste.

Parametrisen sanan aste on siis suurin siinä esiintyvien sisäkkäisten numeeristen parametrien lukumäärä. Astetta nolla olevat parametriset sanat voidaan tulkita aakkoston Δ^* sanoiksi.

3.4 Määritelmä. Määritellään parametrisen sanan γ *käänteinen sana* γ^R:

(i) jos $a \in \Delta \cup \{1\}$, niin $a^R = a$,

(ii) jos α ja β ovat parametrisiä sanoja, niin $(\alpha\beta)^R = \beta^R\alpha^R$,

(iii) jos $\alpha \neq 1$ on parametrinen sana ja $i \in \mathcal{N}$, niin $(\alpha^i)^R = (\alpha^R)^i$.

Jos parametriset sanat α ja β voidaan samaistaa, niin niillä on sama aste ja sanat α^R ja β^R voidaan samaistaa, joten määritelmät ovat järkeviä ja sopivat yhteen samaistusten kanssa.

3.5 Esimerkki. Olkoon $\Delta = \{a, b\}$ ja $\mathcal{N} = \{i, j\}$. Nyt sanan $\alpha = a((b^i a)^i b^j)^j$ aste on kolme. Lisäksi $\alpha^R = (b^j(ab^i)^i)^j a$.

3.2 Yhtälöiden parametriset ratkaisut

Määritellään, milloin joukko morfismeja voidaan esittää parametrisesti; tähtäimenä on yhtälöiden ratkaisujoukkojen esittäminen.

3.6 Määritelmä. Olkoon S joukko morfismeja $\Xi^* \to \Sigma^*$, $\mathcal{N} = \{i_1, \ldots, i_k\}$, h_j morfismi joukolta Ξ^* parametrisille sanoille ja R_j lineaarinen Diofantoksen relaatio, kun $j = 1, \ldots, m$. Joukko

$$\{(h_j, R_j) : 1 \leq j \leq m\}$$

on joukon S *parametrinen esitys*, jos

$$S = \{h \circ f \circ h_j : 1 \leq j \leq m, f \in R_j\},$$

missä $h \circ f$ käy arvotuksia joukolle Σ^*. Joukko S voidaan *esittää parametrisesti*, jos sillä on parametrinen esitys.

Jos kaksi joukkoa voidaan esittää parametrisesti, niin myös niiden unioni voidaan esittää parametrisesti.

3.7 Määritelmä. Olkoot $S, S_1, \ldots, S_n$ joukkoja morfismeja $\Xi^* \to \Sigma^*$. Joukko S voidaan *esittää parametrisesti joukkojen $S_1, \ldots, S_n$ avulla*, jos on sellaiset morfismit $h_1, \ldots, h_n$ joukolta Ξ^* parametrisille sanoille, sanaparametrien aakkostona Ξ, että

$$S = \{g \circ f \circ h_j : 1 \leq j \leq n, g \in S_j\},$$

missä f käy funktioita $\mathcal{N} \to \mathbb{N}_0$.

Määritelmistä nähdään, että jos joukko S voidaan esittää parametrisesti joukkojen $S_1, \ldots, S_n$ avulla, ja jokainen S_i voidaan esittää parametrisesti joukkojen $S_{i1}, \ldots, S_{in_i}$ avulla, niin S voidaan esittää parametrisesti joukkojen S_{ij} avulla. Jos joukot S_i voidaan esittää parametrisesti, niin S voidaan esittää parametrisesti.

3.8 Määritelmä. Yhtälön E ratkaisut voidaan *esittää parametrisesti*, jos sen ratkaisujoukko voidaan esittää parametrisesti. Tämän joukon parametrinen esitys on yhtälön E *parametrinen ratkaisu*.

Nämä määritelmät voidaan luonnollisesti laajentaa myös yhtälöryhmille. Lauseista 2.1 ja 2.2 sekä lemmoista 2.7 – 2.11 saadaan niiden käsittelemien yhtälöiden parametriset ratkaisut.

3.9 Esimerkki. Konjugointiyhtälöllä $xz = zy$ on parametrinen ratkaisu $\{(h_1, R), (h_2, R)\}$, missä $\Delta = \{p, q\}$, $\mathcal{N} = \{i\}$, $h_1(x) = pq$, $h_1(y) = qp$, $h_1(z) = p(qp)^i$, $h_2(x) = h_2(y) = 1$, $h_2(z) = p$ ja R on triviaali relaatio, johon kuuluvat kaikki funktiot $f : \mathcal{N} \to \mathbb{N}_0$. Yleensä tämä kirjoitetaan tietysti vähemmän muodollisesti kuten lauseessa 2.2.

Määritelmissä esiintyvä lineaarinen Diofantoksen relaatio ei ole välttämätön, mutta tätä relaation poisjättämistä ei tässä työssä käsitellä seuraavaa esimerkkiä enempää.

3.10 Esimerkki. Yhtälön $xy = z^2$ jaksolliset ratkaisut ovat selvästi

$$x = t^i, \quad y = t^j, \quad z = t^k,$$

missä $t \in \Sigma^*$, $i + j = 2k$ ja $i, j, k \geq 0$. Ehdosta $i + j = 2k$ päästään eroon kirjoittamalla ratkaisut toisin ja jakamalla ne kahteen osaan parametrien i ja j arvojen pariteetin mukaan:

$$x = t^{2m}, \quad y = t^{2n}, \quad z = t^{m+n} \quad \text{tai} \quad x = t^{2m+1}, \quad y = t^{2n+1}, \quad z = t^{m+n+1},$$

missä $t \in \Sigma^*$ ja $m, n \geq 0$.

Seuraava lause liittyy yksipuolisiin yhtälöihin tehtäviin sijoituksiin.

3.11 Lause. *Olkoon $U, V \in \Xi^*$, $x, y \in \Xi$ ja $x \neq y$. Olkoon h morfismi $x \mapsto yx$. Jos yhtälön $xh(U) = h(V)$ ratkaisut voidaan esittää parametrisesti, niin myös yhtälön $xU \rightrightarrows yV$ ratkaisut voidaan esittää parametrisesti.*

Todistus. Jos yhtälöllä $xh(U) = h(V)$ on parametrinen ratkaisu

$$\{(h_j, R_j) : 1 \leq j \leq m\},$$

niin yhtälöllä $xU \rightrightarrows yV$ on parametrinen ratkaisu

$$\{(h_j \circ h, R_j) : 1 \leq j \leq m\}.$$

□

3.3 Eksponenttiyhtälöt

Tarkastellaan yhtälöitä, joissa tuntemattomat ovat eksponentteja, joille haetaan mahdollisia lukuarvoja. Nämä voidaan määritellä parametristen sanojen avulla.

3.12 Määritelmä. *Eksponenttiyhtälö* on pari (α, β), missä α ja β ovat parametrisiä sanoja. Tämän ratkaisuja ovat kaikki funktiot $f : \mathcal{N} \to \mathbb{N}_0$, joille $f(\alpha) = f(\beta)$. Jos numeeriset parametrit ovat järjestyksessä $i_1, \ldots, i_n$, niin voidaan puhua myös ratkaisusta $(f(i_1), \ldots, f(i_n))$ tai ratkaisusta $i_1 = f(i_1), \ldots, i_n = f(i_n)$. Eksponenttiyhtälön *aste* on parametrisen sanan $\alpha\beta$ aste.

3.13 Esimerkki. Eksponenttiyhtälön $a^i b = (ab)^j$ ratkaisu on $i = j = 1$.

3.14 Lause. *Olkoon E eksponenttiyhtälö, jonka aste on yksi. Tällöin on olemassa sellainen lineaarinen Diofantoksen relaatio R, että funktio $f : \mathcal{N} \to \mathbb{N}_0$ on eksponenttiyhtälön E ratkaisu jos ja vain jos $f \in R$.*

Todistus. Olkoon E yhtälö $\alpha = \beta$, missä

$$\alpha = s_0 t_1^{i_1} s_1 \dots t_m^{i_m} s_m, \qquad \beta = u_0 v_1^{j_1} u_1 \dots v_n^{j_n} u_n,$$

$s_0, \dots, s_m, t_1, \dots, t_m, u_0, \dots, u_n, v_1, \dots, v_n \in \Delta^*$ ja $i_1, \dots, i_m, j_1, \dots, j_n \in \mathcal{N}$. Lauseen 2.16 mukaan funktio f on tämän ratkaisu jos ja vain jos $\mu(f(\alpha)) = \mu(f(\beta))$. Nyt $f(\alpha)$ on

$$\begin{aligned}
&\mu(s_0)\lambda(t_1)^{f(i_1)}\lambda(s_1)\dots\lambda(t_m)^{f(i_m)}\lambda(s_m) \\
&+\frac{\mu(t_1)(\lambda(t_1)^{f(i_1)}-1)}{\lambda(t_1)-1}\cdot\lambda(s_1)\dots\lambda(t_m)^{f(i_m)}\lambda(s_m) \\
&+\dots+\frac{\mu(t_m)(\lambda(t_m)^{f(i_m)}-1)}{\lambda(t_m)-1}\cdot\lambda(s_m)+\mu(s_m)
\end{aligned}$$

tai toisin kirjoitettuna

$$\begin{aligned}
&\left(\mu(s_0)+\frac{\mu(t_1)}{\lambda(t_1)-1}\right)\lambda(s_1\dots s_m)\lambda(t_1^{f(i_1)}\dots t_m^{f(i_m)}) \\
&+\sum_{k=2}^{m}\left(\mu(s_{k-1})+\frac{\mu(t_k)}{\lambda(t_k)-1}-\frac{\mu(t_{k-1})\lambda(s_{k-1})}{\lambda(t_{k-1})-1}\right)\lambda(s_k\dots s_m)\lambda(t_k^{f(i_k)}\dots t_m^{f(i_m)}) \\
&+\mu(s_m),
\end{aligned}$$

ja $\mu(f(\beta))$ on vastaavaa muotoa. Tästä nähdään, että yhtälö

$$\begin{aligned}
&(\lambda(t_1)-1)\dots(\lambda(t_m)-1)(\lambda(v_1)-1)\dots(\lambda(v_n)-1)\mu(f(\alpha)) \\
=&(\lambda(t_1)-1)\dots(\lambda(t_m)-1)(\lambda(v_1)-1)\dots(\lambda(v_n)-1)\mu(f(\beta))
\end{aligned}$$

voidaan termejä siirtämällä kirjoittaa muotoon

$$X^{P_1}+\dots+X^{P_M} = X^{Q_1}+\dots+X^{Q_N}, \tag{4}$$

missä jokainen P_k ja Q_k on lineaarinen polynomi luvuista $f(i_l)$, $f(j_l)$. Yhtälö (4) voi toteutua vain, jos $M = N$. Tällöin se on ekvivalentti kaavan

$$\bigvee_{\pi}\left((P_1 = Q_{\pi(1)})\wedge\dots\wedge(P_N = Q_{\pi(N)})\right)$$

kanssa, missä π käy kaikki N alkion permutaatiot. Väite seuraa tästä. □

3.15 Lause. *Olkoon* $\mathcal{N} = \{i\}$,

$$E : s_0 t^i s_1 \dots t^i s_m = u_0 t^i u_1 \dots t^i u_n$$

eksponenttiyhtälö, jonka aste on yksi, $s_0, \dots, s_m$, $u_0, \dots, u_n$, $t \in \Delta^*$ *ja*

$$\frac{|s_0 \dots s_m u_1 \dots u_n|}{|t|} < S.$$

Tällöin on olemassa sellainen vain luvusta S *riippuva luku* T*, että joko* f *on yhtälön ratkaisu aina, kun* $f(i) \geq T$*, tai* f *ei ole yhtälön ratkaisu millään* $f(i) \geq T$.

Todistus. Kuten lauseen 3.14 todistuksessa, päädytään yhtälöön (4). Tässä esiintyvät polynomit P_j ovat muotoa $af(i)+b$. Toisaalta ne ovat polynomien $\lambda(s_k)$, $\mu(s_k)$, $\lambda(t)$, $\lambda(t)^{f(i)}$, $\mu(t)$ tulojen termien eksponentteja. Jokainen näistä polynomeista voi esiintyä kyseisissä tuloissa korkeintaan kerran. Täten $|t|$ jakaa luvun a ja $b \leq 2|s_0 \dots s_m t|$. Vastaava on voimassa myös polynomien Q_j kertoimille. Täten yhtälö $P_j = Q_{\pi(j)}$ voidaan kirjoittaa $Af(i) = B$, missä $A = 0$ tai $|A| \geq |t|$ ja $|B| \leq 2|s_0 \dots s_m u_1 \dots u_n t^2|$. Nyt on olemassa sellainen vaadittu luku T, että yhtälöillä $P_j = Q_{\pi(j)}$ ei ole ratkaisuja $f(i) \geq T$, jollei jokin yhtälö ole triviaali. Tämä todistaa väitteen. □

Seuraava lause on lauseen 3.15 muunnelma, kun $\mathcal{N} = \{i, j\}$. Se koskee vain tietynlaisessa normaalimuodossa olevia yhtälöitä. Olkoon $t, v \in \Delta^*$ primitiivisiä sanoja, $|t| \neq |v|$ ja $s_0, \dots, s_m$, $u_0, \dots, u_n \in \Delta^*$. Tarkastellaan eksponenttiyhtälöä

$$s_0 t_1^{p_1} s_1 \dots t_m^{p_m} s_m = u_0 v_1^{q_1} u_1 \dots v_n^{q_n} u_n, \tag{5}$$

missä jokainen t_k ja v_k on joko sanan t tai sanan v konjugaatti, ja jokainen p_k ja q_k on muuttujien i, j ensimmäisen asteen polynomi. Näiden polynomien kertoimet eivät voi olla negatiivisia. Oletetaan, että sanan t_k viimeinen kirjain on erisuuri kuin sanan s_{k-1} viimeinen kirjain, ja $t_k \not\leq s_k t_{k+1}^c$ kaikilla c. Tehdään vastaavat oletukset yhtälön oikean puolen sanoille u_k ja v_k ja polynomeille q_k.

3.16 Lause. *Olkoon* E *yhtälö* (5) *edellä olevin oletuksin. Oletetaan, että* p_k *on parametrin* i *polynomi, kun* t_k *on sanan* t *konjugaatti, ja parametrin* j *polynomi, kun* t_k *on sanan* v *konjugaatti. Tehdään vastaavat oletukset yhtälön oikean puolen sanoille* v_k *ja polynomeille* q_k*. Oletetaan vielä, että*

$$\frac{|s_0 \dots s_m u_1 \dots u_n (tv)^2|}{|w^a|} < S \qquad ja \qquad \frac{b}{a} < S$$

aina, kun $w \in \{t^a, v^a\}$ *ja ainakin toinen polynomeista* $ai + b$, $aj + b$ *kuuluu joukkoon* $\{p_1, \ldots, p_m, q_1, \ldots, q_n\}$. *Tällöin on olemassa sellainen vain luvusta* S *riippuva luku* T, *että joko* f *on yhtälön* E *ratkaisu aina, kun* $f(i), f(j) \geq T$, *tai* f *ei ole yhtälön ratkaisu millään* $f(i), f(j) \geq T$.

Todistus. Todistetaan induktiolla luvun $m+n$ suhteen, että jos yhtälöllä on ratkaisu f, jolle $f(i), f(j) \geq S + 2$, niin $s_k = u_k$, $t_k = v_k$ ja $f(p_k) = f(q_k)$ kaikilla k. Jos $m + n = 0$, niin väite on selvä, joskin yhtälö on silloin astetta nolla. Jos $m = 0, n > 0$ tai päinvastoin, niin se eksponentti, joka yhtälössä esiintyy, voi saada vain pieniä arvoja. Oletetaan, että $m, n > 0$. Voidaan olettaa, että $u_0 \leq s_0$, jolloin $v_1 = BA$ ja $s_0 = u_0(BA)^k B$ joillakin A, B. Nyt $|v_1^{f(q_1)}| \geq |s_0| + |t_1^2|$ ja $|t_1^{f(p_1)}| \geq |(AB)^2|$. Siis sanojen t_1 ja AB potenssit yhtyvät vähintään pituuden $|t_1 AB|$ verran, ja lauseen 2.3 perusteella $t_1 = AB$. Siis $t_1 = v_1$, $B = 1$, $k = 0$ ja $s_0 = u_0$. Todistetaan, että $f(p_1) = f(q_1)$. Jos olisi $f(p_1) > f(q_1)$, niin olisi $t_1 = u_1 C$, missä $C \neq 1$, ja $n > 1$. Nyt $C \ldots = v_2^{f(q_2)} \ldots$ ja $C < v_2^{f(q_2)}$, koska $f(q_2)$ on riittävän suuri. Saadaan ristiriita $v_1 = t_1 < u_1 v_2^{f(q_2)}$. Tapaus $f(p_1) < f(q_1)$ on symmetrinen. Induktiivisesti seuraa, että $s_k = u_k$, $t_k = v_k$ ja $f(p_k) = f(q_k)$ kaikilla k.

Nyt nähdään, että yhtälössä $p_k = q_k$ esiintyy vain toista tuntematonta i tai j, koska $t_k = v_k$. Jos siis $f(p_k) = f(q_k)$ ja $f(i), f(j) \geq 2S$, niin on oltava $p_k = q_k$. Väite seuraa tästä. □

Lause 3.14 voidaan yleistää myös tietyn muotoisille astetta kaksi oleville eksponenttiyhtälöille.

3.17 Lause. *Olkoon* $\mathcal{N} = \{i, j\}$. *Olkoot* $s_0, \ldots, s_m$, $t_1, \ldots, t_m$, $u_0, \ldots, u_n$ *ja* $v_1, \ldots, v_n$ *astetta nolla tai yksi olevia parametrisiä sanoja, joissa ei esiinny numeerista parametriä* j. *Oletetaan, että* i *esiintyy ainakin sanoissa* $t_1, \ldots, t_m$ *ja* $v_1, \ldots, v_n$. *Merkitään*

$$\alpha = s_0 t_1^j s_1 \ldots t_m^j s_m, \qquad \beta = u_0 v_1^j u_1 \ldots v_n^j u_n.$$

Nyt on olemassa sellainen lineaarinen Diofantoksen relaatio R, *että funktio* $f : \mathcal{N} \to \mathbb{N}_0$ *on eksponenttiyhtälön* $E : \alpha = \beta$ *ratkaisu jos ja vain jos* $f \in R$.

Todistus. Käytetään jälleen lausetta 2.16. Kuten lauseen 3.14 todistuksessa, saadaan yhtälö $\mu(f(\alpha)) = \mu(f(\beta))$ nimittäjät pois kertomalla ja termejä siirtämällä muotoon

$$X^{P_1} + \cdots + X^{P_M} = X^{Q_1} + \cdots + X^{Q_N}, \tag{6}$$

missä jokainen P_k ja Q_k on muotoa $af(i)f(j) + bf(i) + c$ joillakin kokonaisluvuilla a, b, c. Yhtälö (6) voi toteutua vain jos $M = N$. Tällöin se on

ekvivalentti kaavan

$$\bigvee_{\pi} \big((P_1 = Q_{\pi(1)}) \wedge \cdots \wedge (P_N = Q_{\pi(N)})\big) \tag{7}$$

kanssa, missä π käy kaikki N alkion permutaatiot.

Tarkastellaan tässä esiintyviä yhtälöitä $P_k = Q_{\pi(k)}$. Jos

$$P_k = af(i)f(j) + bf(i) + c, \qquad Q_{\pi(k)} = df(i)f(j) + ef(i) + f$$

ja $f(i) > |c-f|$, niin yhtälö $P_k = Q_{\pi(k)}$ on ekvivalentti yhtälöparin $af(j)+b = df(j)+e$ ja $c = f$ kanssa. On siis olemassa sellainen luku L, että jos oletetaan $f(i) > L$, niin kaava (7) vastaa lineaarista Diofantoksen relaatiota. Tapauksissa $f(i) = 0, \ldots, f(i) = L$ alkuperäinen eksponenttiyhtälö muuttuu astetta yksi olevaksi eksponenttiyhtälöksi, joka on lauseen 3.14 nojalla ekvivalentti lineaarisen Diofantoksen relaation kanssa. Väite seuraa tästä. □

Seuraavassa lauseessa esiintyvät parametriset sanat tulevat lemman 2.10 yhtälön ratkaisuista.

3.18 Lause. *Olkoon $\Delta = \{p, q\}$, $\mathcal{N} = \{i, j, k\}$ ja $a \geq 2$. Olkoon*

$$\alpha = (pq^a)^i p, \quad \beta = q, \quad \gamma = (pq^a)^j p \tag{8}$$

tai

$$\begin{cases} \alpha &= qp((pq)^{k+1}p)^{a-2}pq(((pq)^{k+1}p)^{a-1}pq)^i, \\ \beta &= (pq)^{k+1}p, \\ \gamma &= qp((pq)^{k+1}p)^{a-2}pq(((pq)^{k+1}p)^{a-1}pq)^j. \end{cases} \tag{9}$$

Olkoon $A, B \in \{x, y, z\}^*$ ja h morfismi, joka kuvaa $x \mapsto \alpha, y \mapsto \beta, z \mapsto \gamma$. Nyt on olemassa sellainen lineaarinen Diofantoksen relaatio R, että funktio $f : \mathcal{N} \to \mathbb{N}_0$ on eksponenttiyhtälön $E : h(A) = h(B)$ ratkaisu jos ja vain jos $f \in R$.

Todistus. Kaavan (8) tapauksessa E on astetta yksi ja väite seuraa lauseesta 3.14. Tarkastellaan kaavan (9) tapausta. Voidaan olettaa, että yhtälö $A = B$ on supistetussa muodossa, jolloin A ja B alkavat kirjaimilla x ja z. Tarkastellaan ekvivalenttia yhtälöä $y^a A = y^a B$. Erotetaan molemmilta puolilta maksimaaliset muotoa $y^a t_1 \ldots y^a t_n$ olevat alkuosat; olkoot nämä U ja V. Näin saadaan yhtälö muotoon $UA_1 = VB_1$. Merkitään $T = ((pq)^{k+1}p)^{a-1}pq$. Nyt parametriset sanat $h(U)$ ja $h(V)$ ovat muotoa $T^{P(i,j,k)}$ ja $T^{Q(i,j,k)}$, missä P ja Q ovat numeeristen parametrien lineaarisia polynomeja.

Osoitetaan, että jos f on eksponenttiyhtälön $h(A) = h(B)$ ratkaisu, niin

$$P(f(i), f(j), f(k)) = Q(f(i), f(j), f(k)). \tag{10}$$

Oletetaan, että olisi $P(f(i), f(j), f(k)) > Q(f(i), f(j), f(k))$; toinen suunta on symmetrinen. Tällöin

$$f(T^c h(A_1)) = f(h(B_1)), \tag{11}$$

missä $c \geq 1$. Koska $\beta^{a-1}pq \leq T$, on oltava $\beta^{a-1}pq \leq h(B_1)$. Tästä seuraa, että $B_1 = y^a B_2$. Nyt yhtälö (11) supistuu yhtälöksi $f(T^{c-1}h(A_1)) = f((pq)^k p h(B_2))$. Tästä nähdään, että pitää olla $c > 1$ tai $y \leq A_1$. Molemmissa tapauksissa $(pq)^{k+1}p \leq T^{c-1}h(A_1)$, jolloin pitää olla $pq \leq h(B_2)$, mikä on mahdollista vain, jos B_2 alkaa kirjaimella x tai z. Mutta tällöin B_1 alkaa sanalla $y^a x$ tai $y^a z$, mikä on vastoin sanan V maksimaalisuusoletusta. Yhtälö (10) on siis osoitettu.

Nyt eksponenttiyhtälö $h(UA_1) = h(VB_1)$ on ekvivalentti yhtälöparin $h(U) = h(V)$, $h(A_1) = h(B_1)$ kanssa. Näistä yhtälöistä ensimmäinen on ekvivalentti lineaarisen Diofantoksen yhtälön (10) kanssa. Jälkimmäinen on alkuperäistä yhtälöä lyhyempi ja siihen voidaan soveltaa samaa menettelyä induktiivisesti. Näin saadaan väite todistettua. □

3.4 Neljän muuttujan yhtälöt

Neljän muuttujan yhtälöiden ratkaisuja ei voida yleisesti esittää parametrisesti. Hmelevskii osoitti tämän käyttämällä vastaesimerkkinä yhtälöä $xuy = yvx$. Esitetään tämän yhtälön ratkaisujen parametrisoitumattomuudelle yksinkertaistettu todistus, joka on Czeizlerin artikkelista [2]. Todistuksessa tarvitaan Fibonaccin sanoja ja erityisesti tietoa siitä, että niillä ei ole tekijöinä neljänsiä potensseja.

3.19 Määritelmä. *Fibonaccin sanat* F_n määritellään rekursiivisesti seuraavasti: $F_0 = a$, $F_1 = ab$ ja $F_n = F_{n-1}F_{n-2}$, kun $n \geq 2$.

Jono $F_0, F_1, F_2, F_3, F_4, \ldots$ on siis $a, ab, aba, abaab, abaababa, \ldots$. Seuraava lause on todistettu Karhumäen artikkelissa [4].

3.20 Lause. *Fibonaccin sanoilla ei ole tekijänä minkään epätyhjän sanan neljättä potenssia.*

Sanoilla $F_1, F_3, F_5, \ldots$ on suffiksi ab ja sanoilla $F_2, F_4, F_6, \ldots$ suffiksi ba. Merkitään $H_n = ab$, kun n on pariton, ja $H_n = ba$, kun n on parillinen. Tällöin voidaan merkitä $F_n = G_n H_n$ kaikilla $n \geq 1$. Nyt $G_n = G_{n-1}H_{n-1}G_{n-2}$ kaikilla $n \geq 3$. Seuraava lemma antaa joitakin ratkaisuja yhtälölle $xuy = yvx$.

3.21 Lemma. *Jos $n \geq 2$, niin $G_n H_n G_{n-1} = G_{n-1} H_{n-1} G_n$.*

Todistus. Tapaus $n = 2$ on selvä. Jos $G_n H_n G_{n-1} = G_{n-1} H_{n-1} G_n$, niin kertomalla vasemmalta sanalla $G_n H_n$ saadaan rekursiokaavojen avulla yhtäsuuruus $G_n H_n G_{n+1} = G_{n+1} H_{n-1} G_n$. Väite seuraa induktiolla, koska $H_{n-1} = H_{n+1}$. □

3.22 Lemma. *Olkoon $p, q, s, t \in \Delta^*$. Jos $spt = tqs$, niin $p = q$ tai jokainen sanan st kirjain esiintyy myös sanassa pq.*

Todistus. Jos $|s| = |t|$, niin $s = t$ ja $p = q$. Jatkossa voidaan symmetrian vuoksi olettaa, että $|s| > |t|$.

Jos $|s| \leq |tq| = |pt|$, niin $s = tq' = p't$, missä q' on sanan q prefiksi ja p' on sanan p suffiksi. Sanat p' ja q' ovat konjugaatteja, joten voidaan käyttää lausetta 2.2. Siitä nähdään, että jokainen sanan st kirjain esiintyy sanoissa p', q' ja siten sanassa pq.

Jos $|s| > |tq|$, niin $s = (tq)^k s'$, missä $s' < tq$. Nyt yhtälö supistuu muotoon $s'pt = tqs'$. Jos $tq = 1$, niin myös $p = 1$ ja siis $p = q$. Muuten tämä yhtälö on samaa muotoa kuin alkuperäinen yhtälö, mutta lyhyempi. Tätä voidaan jatkaa induktiivisesti, kunnes päädytään johonkin aiemmista tapauksista, jolloin joko $p = q$ tai sanan $s't$ jokainen kirjain esiintyy myös sanassa pq, josta väite seuraa. □

3.23 Lause. *Yhtälön $xuy = yvx$ ratkaisuja ei voida esittää parametrisesti.*

Todistus. Oletetaan vastoin väitettä, että $\{(h_j, R_j) : 1 \leq j \leq m\}$ on yhtälön parametrinen ratkaisu. Nyt jollekin h_j ja arvotukselle $\varphi = h \circ f$ on $\varphi \circ h_j$ lemmasta 3.21 saatava ratkaisu. Tällöin $(\varphi \circ h_j)(u) = ab$ ja $(\varphi \circ h_j)(v) = ba$. Pitää siis olla $|\varphi(c)| \leq 2$ kaikilla sanojen $h_j(u)$ ja $h_j(v)$ kirjaimilla $c \in \Delta$. Koska $ab \neq ba$, niin lemman 3.22 mukaan $|\varphi(c)| \leq 2$ myös kaikilla sanojen $h_j(x)$ ja $h_j(y)$ kirjaimilla c. Koska $(\varphi \circ h_j)(x) = G_k$, niin lauseen 3.20 mukaan $\varphi(i) < 4$ kaikilla sanassa $h_j(x)$ esiintyvillä parametreillä $i \in \mathcal{N}$, paitsi mahdollisesti tekijöiden α^i, $\varphi(\alpha) = 1$, tapauksessa. Siis sanojen $(\varphi \circ h_j)(x)$ pituus on rajoitettu, mikä on ristiriita, kun k ja siten sanan G_k pituus on riittävän suuri. □

Hmelevskii antaa kaikki yhtälön $xuy = yvx$ ratkaisut. Nämä koostuvat parametrisesti esitettävistä ratkaisuista tapauksessa $u = v$ ja hieman sanojen G_n tapaan määriteltävistä ratkaisuista.

4 Kolmen muuttujan yhtälöt

Kahdessa viimeisessä luvussa tarkastellaan kolmen muuttujan yhtälöitä. Tuntemattomien aakkostona on $\Xi = \{x, y, z\}$. Yhtälöistä voidaan olettaa, että niiden vasen puoli alkaa kirjaimella x. Samoin voidaan olettaa, että x esiintyy myös yhtälön toisella puolella, mutta ei ensimmäisenä. Yhtälön yleinen muoto on näillä oletuksilla

$$xU(x, y, z) = V(y, z)xW(x, y, z).$$

Tässä siis $V \in \{y, z\}^*$. Sama on voimassa myös yksipuolisille yhtälöille.

Jos kolmen muuttujan yhtälöllä on ratkaisu h, jolle $h(z) = 1$, niin h on muuttujien x ja y yhtälön ratkaisu. Tällöin h on jaksollinen tai jokainen morfismi g, jolle $g(z) = 1$, on yhtälön ratkaisu. Tällaiset ratkaisut on helppo esittää parametrisesti. Ratkaisut, jotka ovat jaksollisia tai joissa jokin muuttuja saa arvon 1, ovat *triviaaleja*. Tarvittaessa voidaan keskittyä vain epätriviaaleihin ratkaisuihin.

Lopullisena tavoitteena on todistaa, että kaikkien kolmen muuttujan yhtälöiden ratkaisut voidaan esittää parametrisesti; tämä tavoite saavutetaan luvun 5 lopussa. Lemmat ja lauseet seuraavat läheisesti Hmelevskiin esitystä, joskin joitakin todistuksia on hieman yksinkertaistettu. Ainakin seurauksen 2.5 käyttö lyhentää todistuksia, joskus myös merkinnälliset seikat, kuten morfismin käsitteen käyttö.

4.1 Perusyhtälöt

Aloitetaan määrittelemällä perusyhtälöt ja todistamalla ratkaisujen parametrisoituvuus niille.

4.1 Määritelmä. Yhtälö on *perusyhtälö*, jos se on triviaali yhtälö $U = U$, missä $U \in \Xi^*$, jos sillä on vain triviaaleja ratkaisuja, tai jos se on jotakin seuraavista muodoista, missä $a, b \geq 1$, $c \geq 2$ ja $t \in \{x, z\}$:

P1. $x^a y \ldots = y^b x \ldots$

P2. $x^2 \ldots \rightrightarrows y^a x \ldots$

P3. $xyt \ldots \rightrightarrows zxy \ldots$

P4. $xyt \ldots \rightrightarrows zyx \ldots$

P5. $xyz \ldots = zxy \ldots$

P6. $xyz \ldots = zyx \ldots$

P7. $xy^c z \ldots = zy^c x \ldots$

P8. $xyt \ldots \rightrightarrows z^a xy \ldots$

P9. $xyxz \ldots \rightrightarrows zx^2 y \ldots$

Määritelmä 4.1 pitää tulkita muuttujien uudelleennimeämistä vaille. Esimerkiksi yhtälö $y^2zx = zyxy$ on perusyhtälö P1. Sama koskee muitakin jatkossa esitettäviä määritelmiä.

4.2 Lemma. *Olkoon $S, T, U, V \in \Xi^*$. Oletetaan, että yhtälöllä $S = T$ on parametrinen ratkaisu $\{(h_j, R_j) : j = 1, \ldots, m\}$, missä parametrijoukot ovat $\Delta = \{p, q\}$ ja $\mathcal{N} = \{i_1, \ldots, i_k\}$. Oletetaan, että eksponenttiyhtälöt $h_j(U) = h_j(V)$ ovat ekvivalentteja lineaaristen Diofantoksen relaatioiden kanssa. Tällöin yhtälöparin $S = T, U = V$ ratkaisut voidaan esittää parametrisesti.*

Todistus. Olkoon $h_j(U) = h_j(V)$ ekvivalentti lineaarisen Diofantoksen relaation R'_j kanssa. Osoitetaan, että yhtälöparin ratkaisuilla on parametrinen esitys

$$\big\{(h_j, R_j \cap R'_j) : j = 1, \ldots, m\big\} \cup A,$$

missä A on yhtälöparin jaksollisten ratkaisujen parametrinen esitys.

Jos $\varphi = h \circ f$ on arvotus, jolle $f \in R_j \cap R'_j$, niin $\varphi \circ h_j$ on yhtälön $S = T$ ratkaisu ja f on eksponenttiyhtälön $h_j(U) = h_j(V)$ ratkaisu, jolloin $\varphi \circ h_j$ on myös yhtälön $U = V$ ratkaisu.

Jos taas g on yhtälöparin $S = T, U = V$ jaksoton ratkaisu, niin $g = \varphi \circ h_j$ jollakin sellaisella luvulla j ja arvotuksella $\varphi = h \circ f$, että $f \in R_j$. Pitää vielä näyttää, että f on eksponenttiyhtälön $h_j(U) = h_j(V)$ ratkaisu. Morfismi h on kahden muuttujan yhtälön $f(h_j(U)) = f(h_j(V))$ ratkaisu, mutta se ei voi olla jaksollinen, koska g ei ole jaksollinen. Siis $f(h_j(U))$ ja $f(h_j(V))$ ovat sama sana. □

4.3 Lause. *Perusyhtälöiden ratkaisut voidaan esittää parametrisesti*

Todistus. Yhtälöille $U = U$ ja yhtälöille, joilla on vain triviaaleja ratkaisuja, väite on selvä. Todistetaan se yhtälöille P1–P9. Redusoidaan ensin yhtälöitä toisiksi lauseen 3.11 perusteella. Yhtälö P2 redusoituu sijoituksella $x \mapsto yx$ yhtälöksi $xyx \ldots = y^a x \ldots$, joka on muotoa P1. Yhtälöt P3 ja P4 redusoituvat sijoituksella $x \mapsto zx$ yhtälöiksi $xyz \ldots = zxy \ldots$ ja $xyz \ldots = yzx \ldots$, jotka ovat muotoa P5. Yhtälö P8 redusoituu sijoituksella $x \mapsto zx$ yhtälöksi $xyzA = z^a xyB$ joillakin $A, B \in \Xi^*$. Tämä on lemman 2.12 perusteella ekvivalentti muotoa P5 olevan yhtälön $xyzxyzA = zxyz^a xyB$ kanssa.

Riittää siis tarkastella yhtälöitä P1, P5, P6, P7 ja P9. Käytetään lemmaa 4.2. Tässä lemmassa esiintyvänä yhtälönä $U = V$ voivat olla nämä yhtälöt

itse ja yhtälönä $S = T$ yhtälöt $xy = yx$, $xyz = zxy$, $xyz = zyx$, $xy^c z = zy^c x$ sekä $xyxz \rightrightarrows zx^2y$. Yhtälön P1 tapauksessa tämä seuraa lemmasta 2.12, muuten pituusargumentilla. Lemmojen 2.8, 2.10 ja 2.11 mukaan näiden ratkaisut saadaan tietyistä parametrisistä sanoista yli sanaparametrien p, q ja numeeristen parametrien i, j, k. Nähdään että lemman 4.2 eksponenttiyhtälö tulee yhtälöiden P1, P5 ja P6 tapauksessa olemaan astetta yksi, jolloin voidaan käyttää lausetta 3.14, yhtälön P9 tapauksessa lauseen 3.17 tyyppiä ja yhtälön P7 tapauksessa lauseen 3.18 tyyppiä. Se on siis kaikissa tapauksissa ekvivalentti lineaarisen Diofantoksen relaation kanssa ja väite seuraa lemmasta 4.2. □

4.2 Yhtälöiden kuvat

Olkoon $t_1, \ldots, t_n \in \{y, z\}$ ja $V = t_1 \ldots t_n$. Merkitään $t_{n+1} = t_1$. Jos morfismi h on yhtälön $E : xU \rightrightarrows VxW$ ratkaisu, niin

$$h(x) = h(V^k t_1 \ldots t_i)u \tag{12}$$

joillakin luvuilla k, i ja sanalla u, jotka toteuttavat ehdot $k \geq 0$, $0 < i \leq n$ ja $h(t_{i+1}) \not\leq u$.

Kaavan (12) toteuttava morfismi h puolestaan on yhtälön E ratkaisu jos ja vain jos

$$uh(U) = h(t_{i+1} \ldots t_n t_1 \ldots t_i)uh(W).$$

Voidaan kirjoittaa $h = g \circ f$, missä f on morfismi $x \mapsto V^k t_1 \ldots t_i x$ ja g morfismi, jolle $g(x) = u$, $g(y) = h(y)$ ja $g(z) = h(z)$. Nyt h on yhtälön E ratkaisu jos ja vain jos g on yhtälön

$$xf(U) \leftleftarrows f(t_{i+1} \ldots t_n t_1 \ldots t_i)xf(W). \tag{13}$$

ratkaisu.

4.4 Määritelmä. Yhtälön

$$xU(x, y, z) \rightrightarrows V(y, z)xW(x, y, z)$$

kuva morfismissa $x \mapsto V^t Px$, missä $t \geq 0$, $V = PQ$ ja $Q \neq 1$, on

$$xU(V^t Px, y, z) \leftleftarrows QPxW(V^t Px, y, z).$$

Jos sanassa V esiintyy vain toista kirjaimista y, z tai jos $P = 1$, niin kuva on *degeneroitunut*.

Edellä todetun nojalla yhtälön ratkaisut saadaan helposti sen kuvien ratkaisuista, joten riittää tarkastella näitä kuvia. Kuvia on ääretön määrä, mutta muuttamalla jokin kuva yksipuolisesta yhtälöstä tavalliseksi yhtälöksi voidaan rajoittua äärelliseen määrään yhtälöitä. Seuraava määritelmä koskee tätä.

4.5 Määritelmä. Yhtälö E *redusoituu yhtälöiksi* $E_1, \ldots, E_n$ *n-tuplalla sijoituksia*, jos E on muotoa

$$xU(x,y,z) \rightrightarrows t_1 \ldots t_k x V(x,y,z),$$

missä $1 \leq n \leq k$ ja $t_1, \ldots, t_k \in \{y, z\}$, yhtälö E_i on

$$xU(t_1 \ldots t_i x, y, z) \lessdot t_{i+1} \ldots t_k t_1 \ldots t_i x V(t_1 \ldots t_i x, y, z),$$

kun $1 \leq i < n$, ja yhtälö E_n on

$$xU(t_1 \ldots t_n x, y, z) = t_{n+1} \ldots t_k t_1 \ldots t_n x V(t_1 \ldots t_n x, y, z).$$

Edellä olevista tarkasteluista seuraa nyt lauseen 3.11 yleistys.

4.6 Lause. *Jos yhtälö E redusoituu yhtälöiksi $E_1, \ldots, E_n$ n-tuplalla sijoituksia, ja yhtälöiden $E_1, \ldots, E_n$ ratkaisut voidaan esittää parametrisesti, niin yhtälön E ratkaisut voidaan esittää parametrisesti.*

4.7 Määritelmä. Yhtälö

$$xU(x,y,z) \rightrightarrows V(y,z)xW(x,y,z)$$

on *tyyppiä I*, jos molemmat muuttujat y, z esiintyvät sanassa V. Yhtälö

$$xy^bU(x,y,z) \rightrightarrows z^c x V(x,z) y W(x,y,z),$$

missä $b, c \geq 1$, on *tyyppiä II*, jos $b > 1$ tai $V \neq 1$.

4.8 Lause. *Tyypin I yhtälön ratkaisut voidaan esittää parametrisesti joidenkin sen äärellisen monen kuvan ratkaisujen avulla.*

Todistus. Tarkastellaan yhtälöä

$$E : xU(x,y,z) \rightrightarrows V(y,z)xW(x,y,z)$$

missä molemmat kirjaimista y, z esiintyvät sanassa V, ja sen kuvia

$$E_{P,i} : xU(V^iPx, y, z) \lessdot QPxW(V^iPx, y, z), \tag{14}$$

missä $i \geq 0$, $V = PQ$ ja $Q \neq 1$. Osoitetaan, että on olemassa sellainen luku T, että jos P ja Q ovat kiinteät, niin yhtälöillä (14) on kaikilla $i \geq T$ samat ratkaisut.

Olkoon h yhtälön $E_{P,i}$ ratkaisu. Tällöin eksponenttiyhtälöön

$$h(x)U(h(V)^i h(Px), h(y), h(z)) = h(QPx)W(h(V)^i h(Px), h(y), h(z)),$$

missä i ajatellaan tuntemattomaksi, voidaan soveltaa lausetta 3.15. Tässä esiintyvä raja S ei riipu morfismista h, koska molemmat kirjaimista y, z esiintyvät sanassa V ja $h(x) \leq h(y)$ tai $h(x) \leq h(z)$. On siis olemassa sellainen morfismista h riippumaton luku T, että h joko on ratkaisu kaikilla $i \geq T$ tai ei millään $i \geq T$. Siis yhtälöillä $E_{P,T}, E_{P,T+1}, E_{P,T+2}, \ldots$ on samat ratkaisut, kun P on kiinteä.

Nyt lauseessa vaadituiksi kuviksi kelpaavat yhtälöt $E_{P,j}$, missä $P < V$ ja $j \leq T$. Yhtälön E ratkaisut saadaan nimittäin kaavasta

$$g \circ f \circ h',$$

missä joko h' on morfismi $x \mapsto V^j Px$, g käy vastaavan kuvan $E_{P,j}$ ratkaisut, f ei tee mitään ja $j < T$, tai sitten h' on morfismi $x \mapsto V^{T+i}Px$, i on numeerinen parametri, g käy kuvan $E_{P,T}$ ratkaisut ja f antaa muuttujalle i arvoja joukosta $\mathbb{N}_0$. □

Seuraava esimerkki osoittaa, että tyypin II yhtälöille lauseen 4.8 todistuksessa esiintyvä väite luvun T olemassaolosta ei yleisesti pidä paikkaansa.

4.9 Esimerkki. Yhtälön $xy \rightrightarrows zx^2$ kuvat ovat $xy \leftleftarrows zxz^t x$. Nyt $x = a$, $y = ba(ab)^N a$, $z = ab$ on tällaisen kuvan ratkaisu jos ja vain jos $t = N$. Siis kaikilla kuvilla on erilaiset ratkaisujoukot.

Tarkastellaan tyypin II yhtälöä

$$xy^b A(x, y, z) \rightrightarrows z^c xB(x, z)yC(x, y, z), \tag{15}$$

missä $b, c \geq 1$ ja $b > 1$ tai $B \neq 1$. Tämän kuvat ovat degeneroituneita ja muotoa

$$xy^b A(z^i x, y, z) \leftleftarrows z^c xB(z^i x, z)yC(z^i x, y, z). \tag{16}$$

Lause 4.8 on voimassa myös osalle yhtälöistä 15.

4.10 Lause. *Jos $B = z^d$, $d \geq 1$, niin yhtälön (15) ratkaisut voidaan esittää parametrisesti joidenkin sen äärellisen monen kuvan ratkaisujen avulla.*

Todistus. Yhtälö (16) redusoituu sijoituksella $z \mapsto xz$ yhtälöksi

$$y^b A((xz)^i x, y, xz) = (zx)^c (xz)^d y C((xz)^i x, y, xz). \tag{17}$$

Olkoon h tämän ratkaisu. Merkitään $D = h((zx)^c(xz)^d)$ ja $h(y) = D^j Y$, missä $Y < D$, jolloin saadaan yhtälö

$$Y(D^j Y)^{b-1} A(h((xz)^i x), D^j Y, h(xz)) = DYC(h((xz)^i x), D^j Y, h(xz)). \tag{18}$$

Kääntäen jos yhtälö (18) on voimassa, niin h on yhtälön (17) ratkaisu ja siitä saadaan yhtälön (16) ratkaisu. Lauseeen väite seuraa, kun osoitetaan, että on olemassa sellainen morfismista h riippumaton raja T, että jos yhtälö (18) on voimassa jollakin $i \geq T$, niin se on voimassa kaikilla $i \geq T$. Tällöin nimittäin voidaan rajoittua niihin kuviin (16), joissa $i \leq T$, kuten lauseen 4.8 todistuksessa.

Jos j kiinnitetään, niin yhtälö (18) voidaan ajatella muuttujan i eksponenttiyhtälöksi, ja voidaan soveltaa lausetta 3.15. Morfismista h riippumattoman rajan S olemassaolo seuraa siitä, että $|Y| < (d + c)|h(xz)|$. Pitää vielä käsitellä tapaukset, joissa j on suuri. Sovelletaan lausetta 3.16. Siinä esiintyviksi sanoiksi t ja v kelpaavat sanojen $h(xz)$ ja D primitiiviset juuret. Jos nämä olisivat yhtä pitkät, niin olisi $t = v$ ja $h(xz) = h(zx)$, jolloin päädyttäisiin jaksolliseen ratkaisuun. Voidaan siis olettaa, että $|t| \neq |v|$. Nyt yhtälö (18) saadaan lauseen 3.16 vaatimaan muotoon: siirretään ensin sanojen t ja v potensseja mahdollisimman paljon vasemmalle muuttamalla t ja v aina sopiviksi konjugaateikseen, ja yhdistetään sitten mahdollisimman paljon kustakin potenssista oikealle olevaa osaa kyseiseen potenssiin. Tämä voi edellyttää muuttujien i ja j korvaamista muuttujilla $i' = i - a$ ja $j' = j - b$ joillakin luvuilla a, b. Lauseen 2.3 perusteella sanojen $h(xz)$ ja D konjugaattien potenssit voivat yhtyä korkeintaan pituuden $|h(xz)D|$ verran, joten voidaan valita $a, b \leq c + d + 1$, ja muuttujat i' ja j' voidaan ottaa käyttöön jos i ja j ovat riittävän suuria. Koska sanat $h(xz)$ ja D muodostuvat sanoista $h(x)$ ja $h(z)$ ja $Y < D$, niin lauseen 3.16 raja S ei riipu morfismista h. □

4.3 Yhtälöiden θ-kuvat

Yhtälöiden kuvien tarkastelu ei yksinkertaisimmassa muodossaan riitä; siksi määritellään korkeamman kertaluvun kuvat ja erityisesti θ-kuvat. Nämä mahdollistavat lauseen 4.8 yleisemmän vastineen todistamisen.

4.11 Määritelmä. Jono yhtälöitä $E_0, \ldots, E_n$ on *ketju*, jos E_i on yhtälön E_{i-1} kuva kaikilla i, $1 \leq i \leq n$. Tällöin E_n on yhtälön E_0 *kertaluvun n kuva*. Jos jokainen E_i on degeneroitunut kuva, niin ketju on degeneroitunut ja E_n on degeneroitunut kertaluvun n kuva.

4.12 Määritelmä. Määritellään tyyppien I ja II yhtälöiden *θ-kuvat*. Tyypin I yhtälön θ-kuvat ovat kaikki sen kuvat. Tyypin II yhtälön θ-kuvat ovat sen degeneroituneet kertaluvun 2 kuvat ja degeneroitumattomat kertaluvun 3 kuvat.

4.13 Lemma. *Yhtälön* (15) *ne ratkaisut h, joille $|h(y)| \leq |h(z)|$, voidaan esittää parametrisesti joidenkin sen äärellisen monen kuvan ratkaisujen avulla.*

Todistus. Väite todistetaan kuten lause 4.8. Olkoon E_i yhtälö (16) ja h tämän ratkaisu. Tällöin eksponenttiyhtälöön

$$\begin{aligned} &h(xy^b)A(h(z)^i h(x), h(y), h(z)) \\ =&h(z^c x)B(h(z)^i h(x), h(z))yC(h(z)^i h(x), h(y), h(z)), \end{aligned}$$

missä i ajatellaan tuntemattomaksi, voidaan soveltaa lausetta 3.15. Tässä esiintyvä raja S ei riipu morfismista h, koska $h(x), h(y) \leq h(z)$. On siis olemassa sellainen morfismista h riippumaton T, että h joko on ratkaisu kaikilla $i \geq T$ tai ei millään $i \geq T$. Siis yhtälöillä $E_T, E_{T+1}, E_{T+2}, \ldots$ on samat ratkaisut. Kuten lauseen 4.8 todistuksessa, vaadituiksi kuviksi kelpaavat yhtälöt E_j, missä $j \leq T$. □

4.14 Lemma. *Yhtälön* (15) *ne ratkaisut h, joille $|h(y)| \leq |h(z)|$, voidaan esittää parametrisesti joidenkin sen äärellisen monen θ-kuvan ratkaisujen avulla.*

Todistus. Kutsutaan kyseessä olevia ratkaisuja τ-ratkaisuiksi. Olkoon E_i yhtälö (16). Lemman 4.13 perusteella τ-ratkaisut voidaan esittää parametrisesti yhtälöiden $E_0, \ldots, E_T$ τ-ratkaisujen avulla jollakin T. Olkoon P_i yhtälön E_i niiden τ-ratkaisujen h joukko, joille $|h(z)| \geq |h(xy)|$, ja Q_i yhtälön E_i niiden τ-ratkaisujen h joukko, joille $|h(y)| \leq |h(z)| \leq |h(xy)|$.

Olkoon E_i' yhtälön E_i kuva morfismissa $z \mapsto xz$ ja E_i'' yhtälön E_i' kuva morfismissa $y \mapsto zy$. Pituusehdosta $|h(y)| \leq |h(z)| \leq |h(xy)|$ seuraa, että joukko Q_i voidaan esittää parametrisesti yhtälön (15) kolmannen kertaluvun degeneroitumattoman kuvan E_i'' ratkaisujen avulla.

Tarkastellaan joukkoa P_i. Yhtälö (16) on tyyppiä I, joten sen ratkaisut voidaan esittää joidenkin sen äärellisen monen kuvan ratkaisujen avulla. Joukon P_i määritelmän ehdon $|h(z)| \geq |h(xy)|$ vuoksi näistä voidaan jättää pois kuva morfismissa $z \mapsto xz$. Olkoon näin saatava kuvien joukko F_i. Joukko P_i voidaan esittää parametrisesti joukon F_i yhtälöiden ratkaisujen avulla. Jaetaan F_i degeneroituneiden ja degeneroitumattomien kuvien joukkoihin G_i ja H_i. Joukon H_i yhtälöt ovat tyyppiä I, joten niiden ratkaisut voidaan esittää

äärellisen monen niiden kuvan ratkaisujen avulla. Nämä kuvat ovat alkuperäisen yhtälön (15) kolmannen kertaluvun degeneroitumattomia kuvia. Joukon G_i yhtälöt ovat toisen kertaluvun degeneroituneita kuvia. Siis myös joukko P_i voidaan esittää parametrisesti yhtälön (15) äärellisen monen θ-kuvan ratkaisujen avulla. □

4.15 Lemma. *Olkoon $A, B, C \in \Xi^*$ ja $i, k, a, p, a_1, \ldots, a_n \geq 0$ ja $c, q > 0$. Oletetaan, että kaikki kirjaimet x, y, z esiintyvät sanassa A, $y \not\leq A$, $0 < q \leq n$ ja $a_q + c + 2 \leq k \leq i - c - |A|$. Merkitään*

$$D_1(x,z) = (zx)^c((xz)^{i+a_1}x)\ldots((xz)^{i+a_{q-1}}x)xz,$$
$$D_2(x,z) = (xz)^{i-k+a_q}x((xz)^{i+a_{q+1}}x)\ldots((xz)^{i+a_n}x)(xz)^p.$$

Nyt yhtälöillä

$$y(D_1B)^aA((xz)^ix, D_1B, xz) \leftrightarrows zD_2D_1C(x,y,z) \tag{19}$$
$$y(D_1B)^aA((xz)^ix, D_1B, xz) \leftrightarrows D_2D_1C(x,y,z) \tag{20}$$

on vain triviaaleja ratkaisuja.

Todistus. Ensimmäinen yhtälö redusoituu sijoituksella $z \mapsto yz$ yhtälöksi

$$(D_1(x,yz)B')^aA((xyz)^ix, D_1(x,yz)B', xyz) = zD_2(x,yz)D_1(x,yz)C'.$$

Jos $a > 0$, niin yhtälö on muotoa

$$(yzx)^cx\ldots = (zxy)^{i-k}\ldots.$$

Koska $c > 0$ ja $i - k \geq c + 1$, niin tällä yhtälöllä on seurauksen 2.5 mukaan vain triviaaleja ratkaisuja. Jos $a = 0$ ja $z^my \leq A$, $m > 0$, niin yhtälö on muotoa

$$(xyz)^my\ldots = (zxy)^{i-k}\ldots.$$

Koska $i - k \geq m + 1$, niin tällä yhtälöllä on seurauksen 2.5 mukaan vain triviaaleja ratkaisuja. Jos $a = 0$ ja $z^mx \leq A$, $m \geq 0$, niin yhtälö on muotoa

$$(xyz)^{m+i}\ldots = (zxy)^{i-k+a_q}zxxyz\ldots,$$

paitsi jos $n = q$ ja $p = 0$, jolloin se on muotoa

$$(xyz)^{m+i}\ldots = (zxy)^{i-k+a_q}zx(yzx)^cxyz\ldots.$$

Koska $i-k+a_q > 0$ ja $i > i-k+a_q+c+1$, niin tällä yhtälöllä on seurauksen 2.5 mukaan molemmissa tapauksissa vain triviaaleja ratkaisuja.

Toinen yhtälö käsitellään samoin. Se redusoituu sijoituksella $x \mapsto yx$ yhtälöksi

$$\begin{aligned}&(D_1(yx,z)B')^a A((yxz)^i yx, D_1(yx,z)B', yxz)\\ =&x(zyx)^{i-k+a_q}((yxz)^{i+a_{q+1}}yx)\dots((yxz)^{i+a_n}yx)(yxz)^p D_1(yx,z)C'.\end{aligned}$$

Jos $a > 0$, niin yhtälö on muotoa

$$(zyx)^c y \dots = (xzy)^{i-k} \dots .$$

Koska $c > 0$ ja $i - k \geq c + 1$, niin tällä yhtälöllä on seurauksen 2.5 mukaan vain triviaaleja ratkaisuja. Jos $a = 0$ ja $z^m y \leq A$, $m > 0$, niin yhtälö on muotoa

$$(yxz)^m z \dots = (xzy)^{i-k} \dots .$$

Koska $i - k \geq m + 1$, niin tällä yhtälöllä on seurauksen 2.5 mukaan vain triviaaleja ratkaisuja. Jos $a = 0$ ja $z^m x \leq A$, $m \geq 0$, niin yhtälö on muotoa

$$(yxz)^{m+i} \dots = (xzy)^{i-k+a_q} xyx \dots ,$$

paitsi jos $n = q$ ja $p = 0$, jolloin se on muotoa

$$(yxz)^{m+i} \dots = (xzy)^{i-k+a_q} x(zyx)^c yx \dots .$$

Koska $i-k+a_q > 0$ ja $i > i-k+a_q+c+1$, niin tällä yhtälöllä on seurauksen 2.5 mukaan molemmissa tapauksissa vain triviaaleja ratkaisuja. □

4.16 Lemma. *Jos x esiintyy sanassa B, niin yhtälön* (15) *ne jaksottomat ratkaisut h, joille $|h(y)| \geq |h(z)|$, sekä joitakin jaksollisia ratkaisuja voidaan esittää parametrisesti joidenkin sen äärellisen monen θ-kuvan ratkaisujen avulla.*

Todistus. Yhtälön (15) kuvat ovat yhtälöt (16). Ehdon $|h(y)| \geq |h(z)|$ vuoksi tämän kuvista riittää tarkastella kuvaa morfismissa $z \mapsto xz$:

$$y^b A((xz)^i x, y, xz) \rightrightarrows (zx)^c B((xz)^i x, xz) y C((xz)^i x, y, xz). \tag{21}$$

Pituusehto tulee tälle yhtälölle muotoon $|h(y)| \geq |h(xz)|$. Yhtälö (21) on yhtälön (15) toisen kertaluvun degeneroitumaton kuva. Käytetään merkintää $D = (zx)^c B((xz)^i x, xz)$. Nyt yhtälön (21) kuva morfismissa $y \mapsto D^j D_1 y$, missä $j \geq 0$, $D_1 < D$ ja $D^j D_1 \neq 1$, on

$$\begin{aligned}&y(D^j D_1 y)^{b-1} A((xz)^i x, D^j D_1 y, xz)\\ \leftleftarrows&D_2 D_1 B((xz)^i x, xz) y C((xz)^i x, D^j D_1 y, xz),\end{aligned} \tag{22}$$

missä $D_1 D_2 = D$.

Voidaan kirjoittaa $D = (zx)^c((xz)^{i+a_1}x)\dots((xz)^{i+a_n}x)(xz)^p$, missä $n \geq 1$, $p \geq 0$ ja $a_1, \dots, a_n \geq 0$. Olkoon $M = \max\{a_l + c + 1 + |A| : 1 \leq l \leq n\}$. Jos D_1 "leikkaa" tekijän $(xz)^i$ sanassa D, niin

$$D_1 = (zx)^c((xz)^{i+a_1}x)\dots((xz)^{i+a_{q-1}}x)(xz)^k,$$
$$D_2 = (xz)^{i-k+a_q}x((xz)^{i+a_{q+1}}x)\dots((xz)^{i+a_n}x)(xz)^p$$

tai

$$D_1 = (zx)^c((xz)^{i+a_1}x)\dots((xz)^{i+a_{q-1}}x)(xz)^{k-1}x,$$
$$D_2 = z(xz)^{i-k+a_q}x((xz)^{i+a_{q+1}}x)\dots((xz)^{i+a_n}x)(xz)^p,$$

missä $0 < k \leq t$ ja $0 < q \leq n$. Jos $M \leq k \leq t - M$, niin lemman 4.15 mukaan yhtälöllä (22) on vain triviaaleja ratkaisuja.

Yhtälön (15) kaikki jaksottomat ratkaisut h, joille $|h(y)| \geq |h(z)|$, saadaan yhtälön (22) ratkaisuista. Jaetaan alkuperäisen yhtälön jaksottomat ratkaisut joukkoihin P ja Q sen mukaan, saadaanko ne yhtälöstä (22), kun $i \leq 2M$ tai kun $i \geq 2M$. Pitää osoittaa, että nämä joukot sekä joitakin jaksollisia ratkaisuja voidaan esittää äärellisen monen yhtälön (22) ratkaisujen avulla.

Olkoon $U \leftleftarrows V$ yhtälö (22) ja h jokin tämän ratkaisu. Jos i on kiinteä, niin yhtälö $h(U) = h(V)$ voidaan ajatella eksponenttiyhtälöksi, missä j on numeerinen parametri. Sovelletaan lausetta 3.15. Tämän mukaan on olemassa sellainen morfismista h riippumaton T, että h joko on ratkaisu kaikilla $j \geq T$ tai ei millään $j \geq T$. Voidaan olettaa, että sama T käy kaikille arvoille $i \leq 2M$. Kuten lauseen 4.8 todistuksessa, nähdään, että joukko P sekä joitakin jaksollisia ratkaisuja voidaan esittää niiden yhtälöiden (22) avulla, joissa $i \leq 2M$ ja $j \leq T$.

Tarkastellaan sitten joukkoa Q. Nyt voidaan kirjoittaa $i = 2M + m$. Kirjoitetaan yhtälössä (22) tekijöiden $(xz)^i$ paikalle $(xz)^M(xz)^m(xz)^M$. Tämän jälkeen sana D_1 ei voi enää "leikata" tekijää $(xz)^m$, jos olemme kiinnostuneita vain yhtälöistä, joilla on jaksottomia ratkaisuja. Siis sanalle D_1 on vain rajoitettu määrä vaihtoehtoja luvun m arvosta riippumatta. Kiinnitetään D_1 ja ratkaisu h. Nyt yhtälö $h(U) = h(V)$ voidaan ajatella eksponenttiyhtälöksi, missä j ja m ovat numeeriset parametrit. Kiinnitetään myös parametrin m arvo, jolloin voidaan käyttää lausetta 3.15. Nähdään, että olemassa sellainen morfismista h ja parametrin m arvosta riippumaton raja L, että h joko on ratkaisu kaikilla $j \geq L$ tai ei millään $j \geq L$. Kiinnitetään sitten vuorostaan j ja ajatellaan $h(U) = h(V)$ eksponenttiyhtälöksi, jossa tuntemattomana parametrinä on m. Nyt lauseen 3.15 avulla nähdään, että olemassa sellainen morfismista h riippumaton raja N_j, että h joko on ratkaisu kaikilla $m \geq N_j$

tai ei millään $m \geq N_j$. Voidaan olettaa, että tämä raja on kasvava luvun j suhteen. Yhdistämällä nämä tarkastelut nähdään, että h joko on ratkaisu kaikilla $j \geq L$, $m \geq N_L$ tai ei millään $j \geq L$, $m \geq N_L$. Joukko Q sekä joitakin jaksollisia ratkaisuja voidaan siis esittää niiden yhtälöiden (22) avulla, joissa $i \leq 2M + N_L$ ja $j \leq L$. Tämä todistaa lauseen. □

4.17 Lemma. *Jos x esiintyy sanassa B, niin yhtälön* (15) *jaksottomat ratkaisut, sekä joitakin jaksollisia, voidaan esittää parametrisesti joidenkin sen äärellisen monen θ-kuvan ratkaisujen avulla.*

Todistus. Vaaditut θ-kuvat saadaan yhdistämällä lemmojen 4.14 ja 4.16 joukot. □

4.18 Lemma. *Jos $B = z^d$, missä $d \geq 1$, niin yhtälön* (15) *ratkaisut voidaan esittää parametrisesti joidenkin sen äärellisen monen θ-kuvan ratkaisujen avulla.*

Todistus. Yhtälön kaikki kuvat ovat degeneroituneita; näistä voidaan valita äärellisen monta lauseen 4.10 mukaan. Nämä kuvat ovat tyyppiä I, joten niiden kuvista voidaan lauseen 4.8 mukaan valita äärellisen monta. Näistä toisen kertaluvun kuvista degeneroitumattomat ovat tyyppiä I, joten niiden kuvista voidaan jälleen valita äärellisen monta. Yhdistämällä nämä degeneroitumattomat kolmannen kertaluvun kuvat degeneroituneisiin toisen kertaluvun kuviin saadaan vaadittu joukko θ-kuvia. □

4.19 Määritelmä. Määritellään *täydellinen joukko yhtälön E θ-kuvia.* Jos E on tyypin I yhtälö, niin se on lauseen 4.8 joukko. Jos E on yhtälö (15), niin se on lemman 4.14 joukko, jos $B = 1$, lemman 4.17 joukko, jos x esiintyy sanassa B, ja lemman 4.18 joukko, jos $B = z^d$, $d \geq 1$.

Kaikilla tyyppien I ja II yhtälöillä on siis täydellinen joukko θ-kuvia. Seuraava lause on tämän osion tavoite.

4.20 Lause. *Jos yhtälöt $E_1, \ldots, E_n$ muodostavat täydellisen joukon yhtälön E θ-kuvia ja jokaisen yhtälön E_i ratkaisut voidaan esittää parametrisesti, niin yhtälön E ratkaisut voidaan esittää parametrisesti.*

Todistus. Tyypin I yhtälöille väite seuraa lauseesta 4.8. Tarkastellaan tyypin II yhtälöä (15). Jos $B \neq 1$, niin väite seuraa lemmoista 4.17 ja 4.18. Oletetaan, että $B = 1$. Lemman 4.14 vuoksi riittää osoittaa, että yhtälön (15) ne ratkaisut h, joille $|h(y)| \geq |h(z)|$, voidaan esittää parametrisesti. Olkoon h tällainen ratkaisu. Tällöin $h(x) = h(z)^m u$ joillakin $m \geq 1$ ja $u \leq h(z)$,

$h(z) = uv$ jollakin v ja $y = vuw$ jollakin w. Nähdään, että $h = g \circ f$, missä f ja g ovat morfismeja, $f(x) = (xz)^m x$, $f(y) = zxy$, $f(z) = xz$ ja g on yhtälön

$$yzx \ldots = (zx)^c y \ldots . \tag{23}$$

ratkaisu; toisaalta kaikki näin saatavat morfismit h ovat yhtälön 15 ratkaisuja. Lemman 2.12 perusteella g on myös yhtälön $yzx = zxy$ ratkaisu. Nyt voidaan käyttää lemmaa 2.8 ja lemmaa 4.2; näiden mukaan yhtälön (23) ratkaisut g voidaan esittää parametrisesti. Tulkitsemalla myös morfismissa f esiintyvä eksponentti m numeeriseksi parametriksi, saadaan parametrinen esitys vaadituille ratkaisuille h. □

5 Kolmen muuttujan yhtälöiden puut

Tässä viimeisessä luvussa todistetaan, että jokaisen kolmen muuttujan yhtälön ratkaisut voidaan esittää parametrisesti. Tämä tapahtuu palauttamalla yhtälöt vaiheittain toisenlaisiin yhtälöihin, jolloin muodostuu puu, jonka solmut ovat yhtälöitä. Todistetaan, että jokaisella yhtälöllä on tällainen puu, jonka lehtisolmut ovat perusyhtälöitä.

5.1 Yhtälöiden ympäristöt

Tarkastellaan erilaisia tapoja palauttaa yhtälön ratkaiseminen muiden yhtälöiden ratkaisemiseen. Eräs näistä tavoista vaatii kaksi lemmaa.

5.1 Lemma. *Olkoot u, v, w sanoja, $0 < |w| \leq |u|$ ja $c \geq 1$. Jos*

$$wu^{c+1}v\ldots = u^{c+1}vu\ldots \qquad tai \qquad w(uv)^c u^2\ldots = (uv)^c u^2\ldots,$$

niin $uv = vu$.

Todistus. Merkitään $u = wt$. Yhtälöstä $wu^{c+1}v\ldots = u^{c+1}vu\ldots$ saadaan nyt supistamalla

$$(wt)^{c+1}v\cdots = t(wt)^c vwt\ldots$$

ja tästä ottamalla alkuosat edelleen

$$(wt)^{c+1}v = t(wt)^c vw.$$

Yhtälöstä $w(uv)^c u^2\ldots = (uv)^c u^2\ldots$ taas saadaan

$$(wtv)^c wtwt\cdots = tv(wtv)^{c-1}wtwt\ldots$$

ja tästä ottamalla alkuosat edelleen

$$(wtv)^c wt = tv(wtv)^{c-1}wtw.$$

Molemmissa tapauksissa viimeisten yhtälöiden alku- ja loppuosista saadaan $wt = tw$ ja $wtv = tvw$. Siis $\rho(w) = \rho(t) = \rho(tv) = \rho(v) = \rho(u)$. □

5.2 Lemma. *Olkoon E_0 yhtälö*

$$xy^a zy^p s\ldots \rightrightarrows zy^b xy^q t\ldots,$$

missä $s, t \in \{x, z\}$ ja $a + p \neq b + q$. Olkoon lisäksi $k \geq 8 + |p - q|$ parillinen, E_k yhtälö $xP \rightrightarrows zQ$ ja $E_0, \ldots, E_k$ degeneroitunut ketju. Tällöin yhtälön E_k ne ratkaisut, joissa $y \neq 1$, toteuttavat yhtälön

$$xy^a zy^b \rightrightarrows zy^b xy^a.$$

Todistus. Oletetaan, että E_{i+1} on yhtälön E_i kuva morfismissa $f_i : x \mapsto (zy^b)^{c_i}x$, kun i on parillinen, ja morfismissa $f_i : z \mapsto (xy^a)^{c_i}z$, kun i on pariton. Koska $f_0(x)$ ja $f_0(z)$ ja siten $f_0(s)$ ja $f_0(t)$ alkavat kirjaimella z, on yhtälö E_k muotoa

$$xy^azy^pr\ldots \rightrightarrows zy^bxy^qr\ldots,$$

missä

$$r = (f_k \circ \cdots \circ f_1)(z) = (f_k \circ \cdots \circ f_4)((((xy^a)^{c_3}zy^b)^{c_2}xy^a)^{c_1}(xy^a)^{c_3}).$$

Merkitään $f = f_k \circ \cdots \circ f_4$. Helposti nähdään, että xy^a ja zy^b esiintyvät sanan $f(xy^a)$ tekijöinä ainakin $k-4$ kertaa. Jos nyt h on yhtälön E_k ratkaisu, niin

$$\begin{aligned}||h(xy^azy^p)| - |h(zy^bxy^q)|| &\leq |a+p-b-q||h(y)| \\ &\leq (a+b)|h(y)| + |p-q||h(y)| \\ &\leq (1+|p-q|)|h(xy^azy^b)| \\ &\leq (k-7)|h(xy^azy^b)| \\ &\leq |h(f(xy^a))|.\end{aligned}$$

On siis voimassa yhtäsuuruus

$$w((u^{c_3}v)^{c_2}u)^{c_1}u^{c_3}\ldots = ((u^{c_3}v)^{c_2}u)^{c_1}u^{c_3}\ldots,$$

missä $u = h(f(xy^a))$, $v = h(f(zy^b))$ ja $|w| \leq |u|$. Nyt lemman 5.1 mukaan pitää olla $w = 1$ tai $uv = vu$ eli $h(xy^azy^p) = h(zy^bxy^q)$ tai $h(xy^azy^b) = h(zy^bxy^a)$. Ensimmäinen tapaus ei ole mahdollinen oletuksien $h(y) \neq 1$ ja $a+p \neq b+q$ perusteella. □

Seuraavaksi määritellään yhtälöiden ympäristöt.

5.3 Määritelmä. Yhtälöt $E_1, \ldots, E_n$ muodostavat yhtälön E *ympäristön*, jos jokin seuraavista ehdoista on voimassa:

Y1. yhtälöt $E_1, \ldots, E_n$ muodostavat täydellisen joukon yhtälön E θ-kuvia,

Y2. E redusoituu yhtälöiksi $E_1, \ldots, E_n$ jollakin n-tuplalla sijoituksia,

Y3. E on yhtälö $U = V$, U ja V alkavat eri kirjaimilla, $n = 2$ ja E_1 sekä E_2 ovat yhtälöt $U \rightrightarrows V$ sekä $V \rightrightarrows U$,

Y4. $n = 1$ ja $E_1 = E^R$,

Y5. E on yhtälö $SU = TV$, kukin kirjaimista x, y, z esiintyy kummassakin sanassa S ja T yhtä monta kertaa, $n = 1$ ja E_1 on yhtälö $US = VT$,

Y6. $n = 1$ ja E_1 on E supistettuna vasemmalta tai kerrottuna oikealta jollakin kirjaimista x, y, z,

Y7. $n = 1$ ja lemman 5.2 oletuksin E on yhtälö $xP \rightrightarrows zQ$ ja E_1 yhtälö $xy^a zy^b xP \rightrightarrows zy^b xy^a zQ$.

Ehdot Y1 ja Y2 ovat jatkossa tärkeimmät. Ehto Y3 mahdollistaa tarkastelujen siirtämisen yksipuolisiin yhtälöihin. Ehdon Y6 vuoksi voidaan tarvittaessa olettaa yhtälöiden olevan supistettuja vasemmalta ja jatkuvan riittävän pitkälle oikealle. Muut ehdot tulevat käyttöön joissakin erikoistapauksissa. Seuraava lause perustelee ympäristön määritelmän järkevyyden.

5.4 Lause. *Jos yhtälöt $E_1, \ldots, E_n$ muodostavat yhtälön E ympäristön ja niiden ratkaisut voidaan esittää parametrisesti, niin myös yhtälön E ratkaisut voidaan esittää parametrisesti.*

Todistus. Käydään läpi eri tapaukset sen mukaan, minkä määritelmän 5.3 ehdoista yhtälöt $E_1, \ldots, E_n$ täyttävät:

Y1. Seuraa lauseesta 4.20.

Y2. Seuraa lauseesta 4.6.

Y3. Yhtälön $U = V$ ratkaisujoukko on yhtälöiden $U \rightrightarrows V$ ja $V \rightrightarrows U$ ratkaisujoukkojen unioni.

Y4. Jos $\{(h_j, R_j) : 1 \leq j \leq m\}$ on yhtälön E^R parametrinen ratkaisu, niin $\left\{(h_j^R, R_j) : 1 \leq j \leq m\right\}$, missä $h_j^R(t) = h_j(t)^R$, kun $t \in \Xi$, on yhtälön E parametrinen ratkaisu.

Y5. Yhtälö $SU = TV$ on ekvivalentti yhtälöparin $S = T$, $U = V$ kanssa, ja tämä on edelleen ekvivalentti yhtälön $US = VT$ kanssa.

Y6. Yhtälöt E_1 ja E ovat ekvivalentit.

Y7. Yhtälö E_1 on ekvivalentti yhtälöparin $xy^a zy^b \rightrightarrows zy^b xy^a$, E kanssa. Lemman 5.2 mukaan yhtälön E ratkaisut ovat tämän yhtälöparin ratkaisut sekä ratkaisut, joissa $y = 1$. Nämä voidaan esittää parametrisesti

□

5.2 Yhtälöiden puut

Ympäristöjen avulla voidaan määritellä yhtälöiden puut.

5.5 Määritelmä. Suunnattu syklitön graafi, jonka solmut ovat yhtälöitä, on yhtälön E puu, jos seuraavat ehdot täyttyvät:

(i) ainoa solmu, johon ei tule kaarta, on yhtälö E,

(ii) jokaiseen muuhun solmuun tulee tarkalleen yksi kaari,

(iii) jos solmusta E_0 lähtee kaaret tarkalleen solmuihin $E_1, \ldots, E_n$, niin nämä yhtälöt muodostavat yhtälön E_0 ympäristön.

Sama yhtälö voi esiintyä puussa useampana eri solmuna. Jos solmusta ei lähde yhtään kaarta, se on *lehtisolmu*.

5.6 Määritelmä. Puu, jonka kaikki lehtisolmut ovat perusyhtälöitä, on *peruspuu*.

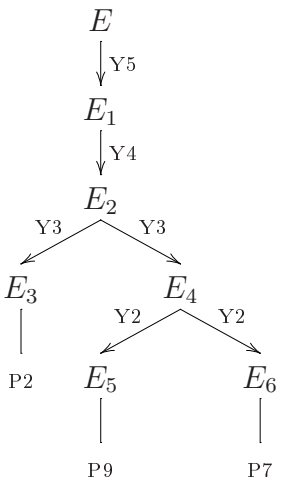
Jos tyypin I tai II yhtälön E jokaisella θ-kuvalla on peruspuu, niin yhtälöllä E on peruspuu, koska sillä on täydellinen joukko θ-kuvia. Ympäristön määritelmän kohtaa Y1 käytetään yleensä juuri näin käsittelemällä kaikkia θ-kuvia tietyn täydellisen joukon valitsemisen sijaan.

Tavoitteena on osoittaa, että kaikilla kolmen muuttujan yhtälöillä on peruspuu. Tähän tulokseen johtaa sarja lemmoja, joista ensimmäiseen eli lemmaan 5.7 liittyvä peruspuu on kuvassa 1. Tämän lemman todistuksessa puun muodostuminen on myös selitetty esimerkin omaisesti hieman huolellisemmin kuin jatkossa.

5.7 Lemma. *Yhtälöllä* $E : xyz^2A(x,y,z) = yz^2xB(x,y,z)$ *on peruspuu.*

Todistus. Käytetään määritelmän 5.3 kohtaa Y5, jolloin saadaan yhtälö $E_1 : Axyz^2 = Byz^2x$, ja tämän jälkeen kohtaa Y4, jolloin saadaan yhtälö $E_2 : z^2yxA^R = xz^2yB^R$. Jaetaan tämä yksipuolisiksi yhtälöiksi $E_3 : z^2yxA^R \rightrightarrows xz^2yB^R$ ja $E_4 : z^2yxA^R \lleftarrow xz^2yB^R$ kohdan Y3 nojalla. Näistä ensimmäinen on perusyhtälö muotoa P2. Jälkimmäiseen käytetään kohtaa Y2; yhtälö redusoituu parilla sijoituksia $x \mapsto zx$, $x \mapsto z^2x$ yhtälöiksi $E_5 : zyzx\ldots \rightrightarrows xz^2y\ldots$ ja $E_6 : yz^2x\ldots = xz^2y\ldots$. Nämä ovat perusyhtälöitä muotoa P9 ja P7. Näin saadaan väitetty peruspuu. □

5.8 Lemma. *Yhtälöllä* $x^2yz\ldots \rightrightarrows zyxy\ldots$ *on peruspuu.*



Kuva 1: Lemman 5.7 yhtälön peruspuu.

Todistus. Tämä yhtälö redusoituu parilla sijoituksia $x \mapsto zx$ ja $x \mapsto zyx$ yhtälöiksi $xzxyz\ldots \leftleftarrows yzxy\ldots$ ja $xzyxyz\ldots = zyxy\ldots$. Jälkimmäinen on perusyhtälö muotoa P5 ja ensimmäisestä tulee sijoituksella $y \mapsto xy$ yhtälö $zx^2yz\ldots = yzx^2y\ldots$, johon voidaan käyttää lemmaa 5.7. □

5.9 Lemma. *Jokaisella yhtälön $xy^2z\ldots \rightrightarrows zy^2x\ldots$ degeneroitumattomalla θ-kuvalla on peruspuu.*

Todistus. Kyseessä on tyypin I yhtälö, joten sen degeneroitumattomat θ-kuvat ovat muotoa $xy^2z\ldots \leftleftarrows y^2zx\ldots$ tai muotoa $xy^2z\ldots \leftleftarrows yzyx\ldots$. Ensimmäinen näistä on perusyhtälö P2 ja jälkimmäinen perusyhtälö P8. □

5.10 Lemma. *Jokaisella yhtälön $xyztA(x,y,z) \rightrightarrows zx^2yB(x,y,z)$, missä $t \neq z$, degeneroitumattomalla θ-kuvalla on peruspuu.*

Todistus. Yhtälö on tyyppiä II. Muotoa $xyz\ldots \rightrightarrows zx\ldots$ olevan yhtälön kuvat ovat degeneroituneita ja muotoa $xyz\ldots \leftleftarrows zx\ldots$. Toisen kertaluvun degeneroituneet kuvat ovat jälleen muotoa $xyz\ldots \rightrightarrows zx\ldots$. Alkuperäisen yhtälön toisen kertaluvun degeneroitumattomat kuvat ovat

$$yxzg(h(tA)) \rightrightarrows zx((xy)^jxz)^ixyg(h(B)), \tag{24}$$

missä h on morfismi $x \mapsto z^ix$ ja g on morfismi $z \mapsto (xy)^jxz$. Edellä todetun perusteella degeneroitumattomat θ-kuvat ovat yhtälön (24) kuvat; tarkastellaan erikseen tapauksia $j = 0$ ja $j > 0$ ja käytetään merkintää $C = tA$.

Olkoon ensin $j = 0$. Yhtälön (24) kuvat ovat

$$yxzC((xz)^i x, D^k D_1 y, xz) \leftleftarrows D_2 D_1 y B((xz)^i x, D^k D_1 y, xz), \tag{25}$$

missä $D = D_1 D_2 = zx(xz)^i x$, $D \neq D_1$ ja $D^k D_1 \neq 1$. Jos $D_2 D_1$ alkaa jollakin sanoista x^2, xzx, zxz, niin yhtälö (25) on perusyhtälö. Muuten $D_2 D_1$ alkaa välttämättä sanalla zx^2, $D_1 = 1$ ja $k > 0$. Tällöin yhtälö (25) on

$$yxzC((xz)^i x, D^k y, xz) \leftleftarrows zx(xz)^i xy B((xz)^i x, D^k y, xz).$$

Tämä redusoituu sijoituksella $z \mapsto yz$ yhtälöksi

$$xyzC((xyz)^i x, E^k y, xyz) = zx(xyz)^i xy B((xyz)^i x, E^k y, xyz),$$

missä $E = yzx(xyz)^i x$. Tämä on ekvivalentti jonkin seuraavista yhtälöpareista kanssa:

(a) $xyzx = zxxy$ ja $y \ldots = z \ldots$, jos $t = x$,

(b) $xyzyzxx = zxxyzxy$ ja $y \ldots = z \ldots$, jos $t = y$ ja $i > 1$,

(c) $xyzyzxx = zxxyzxy$ ja $y \ldots = x \ldots$, jos $t = y$, $i = 1$ ja $y \not\leq B$,

(d) $xyzyzxx = zxxyzxy$ ja $(yzx)y \ldots = (yzx)x \ldots$, jos $t = y$, $i = 1$ ja $y \leq B$.

Kaikissa tapauksissa yhtälöparilla on seurauksen 2.5 mukaan vain triviaaleja ratkaisuja.

Olkoon sitten $j \geq 0$. Jos $t = x$, niin yhtälö (24) on

$$yxz((xy)^j xz)^i xg(h(A)) \rightrightarrows zx((xy)^j xz)^i xyg(h(B)).$$

Tämä on ekvivalentti yhtälöparin $yxzx \rightrightarrows zxxy$, $y \ldots = x \ldots$ kanssa, joten sillä on seurauksen 2.5 mukaan vain triviaaleja ratkaisuja. Jos $t = y$, niin yhtälö (24) on

$$yxzy \ldots \rightrightarrows zxxy(xy)^{j-1} xzxy \ldots.$$

Tämän tyypin I yhtälön jokainen kuva on jotakin muodoista

$$yx \ldots \leftleftarrows x^2 \ldots, \quad yxz \ldots \leftleftarrows xzx \ldots, \quad yxzzx^2 s \ldots \leftleftarrows zx^2 yxzx \ldots,$$

missä $s \neq x$. Kaksi ensimmäistä ovat perusyhtälöitä P2 ja P3. Kolmas on ekvivalentti yhtälöparin $yxzzx^2 \leftleftarrows zx^2 yxz$, $s \ldots = x \ldots$ kanssa, joten sillä on seurauksen 2.5 mukaan vain triviaaleja ratkaisuja. □

5.3 Tukiyhtälöt

Tässä osiossa määritellään tukiyhtälöt ja todistetaan välituloksena, että niillä on aina peruspuu.

5.11 Määritelmä. Olkoon $1 \leq a, b \leq 2$, $d \geq 1$ ja $t \neq y$. *Tukiyhtälö* on muotoa

$$x^a y^b t \ldots \rightrightarrows zyx \ldots \qquad \text{tai} \qquad x^a y^b t \ldots \rightrightarrows zxy \ldots, \tag{26}$$

tai muotoa

$$x^a y^b t \ldots \rightrightarrows z(yz)^d x \ldots, \tag{27}$$

oleva yhtälö.

5.12 Määritelmä. Puu, jonka jokainen lehtisolmu on perusyhtälö, kaavan (26) tukiyhtälö tai yhtälö $x^2yt \ldots \rightrightarrows zyzxy \ldots$, missä $t \neq y$, on *tukipuu*.

5.13 Lemma. *Olkoon $E_0, \ldots, E_3$ ketju yhtälön*

$$E_0 : xy^a tA(x,y,z) \rightrightarrows z^c xB(x,z)yC(x,y,z)$$

kuvia, missä $a, c \geq 1$, $A, C \neq 1$ ja $t \neq y$. Oletetaan ensin, että E_2 on degeneroitunut kuva. Nyt

1. *E_2 on muotoa $xy^a z \ldots \rightrightarrows zx \ldots$;*
2. *jos $a = 2$, $c = 1$, $B = 1$ ja $y \not\leq C$, niin E_2 on muotoa $xy^2 z \ldots \rightrightarrows zxyx \ldots$;*
3. *jos $a = 2$, $c = 1$ ja $B = x$, niin E_2 on muotoa $xy^2 z \ldots \rightrightarrows zx^2 y \ldots$;*
4. *jos $a = 1$, niin E_2 on perusyhtälö P3 tai muotoa $xyzs \ldots \rightrightarrows zx^2 y \ldots$, missä $s \neq z$.*

Oletetaan sitten, että E_2 on degeneroitumaton kuva. Nyt

1. *E_3 on tukiyhtälö;*
2. *jos $a = 2$, $c = 1$, $B = 1$ ja $y \not\leq C$, niin E_3 on perusyhtälö tai muotoa $yxzy \ldots \rightrightarrows zxzy \ldots$;*
3. *jos $a = 2$, $c = 1$ ja $B = x$, niin E_3 on kaavan (26) tukiyhtälö tai muotoa $x^2 ys \ldots \rightrightarrows zyzxy$, missä $s \neq y$;*
4. *jos $a = 1$, niin E_3 on kaavan (26) tukiyhtälö.*

Todistus. Yhtälö E_1 on muotoa

$$xy^a zA_1(x,y,z) \leftleftarrows z^c xB(z^i x,z)C(z^i x,y,z),$$

missä $i > 0$ ja $A_1 \neq 1$. Tämän kuvana E_2 on muotoa

$$D_2 D_1 zA_2(x,y,z) \rightrightarrows zh(z^{c-1} xB(z^i x,z)C(z^i x,y,z)),$$

missä h on morfismi $z \mapsto (xy^a)^j D_1 z$, $j \geq 0$, $D_1 < xy^a$, $(xy^a)^j D_1 \neq 1$, $D_1 D_2 = xy^a$ ja $z \not\leq A_2 \neq 1$.

Yhtälö E_2 on degeneroitunut kuva jos ja vain jos $D_1 = 1$. Tällöin neljä ensimmäistä väitettä ovat tosia. Jos $D_1 \neq 1$, niin laskemalla E_3 erikseen kolmessa tapauksessa $t = 0$, $D_1 = x$, ja $t > 0$, $D_1 = x$, ja $t \geq 0$, $D_1 = xy^b$, $1 \leq b < a$, nähdään viimeiset neljä väitettä tosiksi. □

5.14 Lemma. *Olkoon $s, t \neq y$. Yhtälön $xy^2 s \ldots \rightrightarrows zxyt \ldots$ jokaisella degeneroitumattomalla θ-kuvalla on peruspuu. Yhtälön $xy^2 z \ldots \rightrightarrows zx^2 y \ldots$ jokaisella degeneroitumattomalla θ-kuvalla on tukipuu.*

Todistus. Jälkimmäiselle yhtälölle väite seuraa lemman 5.13 kohdasta 3. Ensimmäiselle yhtälölle se taas seuraa kohdasta 2, koska siinä esiintyvä yhtälö $yxzy \ldots \rightrightarrows zxzy \ldots$ redusoituu sijoituksella $y \mapsto zy$ lemman 5.7 yhtälöksi. □

5.15 Lemma. *Olkoon $s \neq x$ ja $t \neq y$. Yhtälöistä*

(a) $xy^2 z \ldots \rightrightarrows zx^2 y \ldots$

(b) $xyzs \ldots \rightrightarrows zx^2 y \ldots$

(c) $xy^2 z \ldots \rightrightarrows zxyt \ldots$

(d) $xyzt \ldots \rightrightarrows zy^2 x \ldots$

(e) $xyz \ldots \rightrightarrows zy^2 x \ldots$

ensimmäisellä on tukipuu ja muilla peruspuu.

Todistus. Olkoon E_0 jokin yhtälöistä (a)–(d). Se voidaan kirjoittaa muotoon $xy^a zy^p u \ldots \rightrightarrows zy^b xy^q v \ldots$, missä $u, v \neq y$. Tässä aina $a + p \neq b + q$. Olkoon $l \geq 8 + |p - q|$ parillinen. Muodostetaan yhtälölle E_0 täydellinen joukko θ-kuvia, näille täydellinen joukko θ-kuvia, ja niin edelleen l kertaa. Nämä θ-kuvat muodostavat ketjuja $E_0, \ldots, E_l$. Osoitetaan, että jokaisessa tällaisessa ketjussa on yhtälö, jolla on vaadittu tuki- tai peruspuu; tämä todistaa lemman väitteen.

Tarkastellaan ensin degeneroituneiden θ-kuvien ketjuja. Tällaista ketjua vastaa tavallisten kuvien degeneroitunut ketju ja voidaan käyttää ympäristön määritelmän kohtaa Y7. Tällöin yhtälö E_l korvautuu jollakin seuraavista yhtälöistä:

(a') $xy^2z\ldots \rightrightarrows zxy^2\ldots$

(b') $xyz\ldots \rightrightarrows zxy\ldots$

(c') $xy^2z\ldots \rightrightarrows zxy^2\ldots$

(d') $xyzy\ldots \rightrightarrows zy^2x\ldots$.

Yhtälö (b') on perusyhtälö P3. Yhtälöt (a') ja (c') redusoituvat sijoituksella $x \mapsto zx$ lemman 5.7 yhtälöksi. Yhtälö (d') redusoituu tällä sijoituksella yhtälöksi $xyzyP = y^2zxQ$, joka saadaan ympäristön määritelmän ehdoilla Y5 ja Y4 muotoon $yzyx\ldots = xzy^2\ldots$, jolla on lemman 5.7 mukaan peruspuu.

Tarkastellaan sitten degeneroitumattomia ketjuja. Tällaisesta ketjusta voidaan erottaa degeneroitunut alkuosa $E_0, \ldots, E_{j-1}$ ja olettaa, että E_j on yhtälön E_{j-1} degeneroitumaton θ-kuva. Jos E_0 on muotoa (a) – (c), niin E_{j-1} on vastaavaa muotoa, ja yhtälöllä E_j on vaadittu perus- tai tukipuu lemman 5.14 tai lemman 5.10 perusteella. Jos E_0 on muotoa (d), niin kaikki yhtälöt $E_0, \ldots, E_{j-1}$ ovat tyyppiä I. Olkoon $0 \leq i < j$. Jos i on parillinen, niin E_i on muotoa $xyz\ldots \rightrightarrows zy^2x\ldots$. Jos i on pariton, niin E_i on muotoa $zy^2x\ldots \rightrightarrows xyz\ldots$. Oletetaan ensin, että j on parillinen. Tällöin E_j on muotoa $yxzr\ldots \rightrightarrows zy^2x\ldots$, missä $r \neq z$. Tämä on yhtälö (b). Oletetaan sitten, että j on pariton. Tällöin E_j on muotoa $y^2\ldots \rightrightarrows xy\ldots$ tai $yzy\ldots \rightrightarrows xyz\ldots$. Nämä ovat perusyhtälöitä P2 ja P3.

Väite on todistettu yhtälöille (a)–(d). Yhtälö (e) on joko muotoa (d) tai muotoa (d'), joten silläkin on peruspuu. □

5.16 Lemma. *Kaavan* (26) *tukiyhtälöillä on peruspuu.*

Todistus. Tarkastellaan ensin yhtälöä $x^ay^bt\ldots \rightrightarrows zyx\ldots$, missä $1 \leq a, b \leq 2$ ja $t \neq y$. Jos $a = b = 1$, niin tämä on perusyhtälö P4. Jos $a = 1$ ja $b = 2$, niin yhtälö on tyyppiä I ja sen kuvat ovat muotoa $zyx\ldots \rightrightarrows xy^2z\ldots$ tai $yzxs\ldots \rightrightarrows xy^2z\ldots$, missä $s \neq x$. Näillä on peruspuu lemman 5.15 perusteella. Oletetaan, että $a = 2$. Nyt yhtälö redusoituu sijoituksilla $x \mapsto zx$, $x \mapsto zyx$ yhtälöiksi $xzxy\ldots \leftleftarrows yzxs\ldots$ ja $xzy\ldots = zyx\ldots$, missä $s \neq x$. Jälkimmäinen on perusyhtälö P5. Jos ensimmäisessä $s = y$, niin se redusoituu sijoituksella $y \mapsto xy$ lemman 5.7 yhtälöksi. Jos taas $s = z$, niin kyseisen yhtälön kuvat ovat muotoa $yzxz\ldots \leftleftarrows Dy$, missä D on sanan xzx konjugaatti. Jos $D = xzx$, niin tämä kuva on perusyhtälö P4. Jos $D = zx^2$, niin se on lemman 5.15 yhtälö (c). Jos $D = x^2z$, niin se on lemman 5.8 yhtälö.

Tarkastellaan sitten yhtälöä $x^a y^b t \ldots \rightrightarrows zxy \ldots$, missä $1 \leq a, b \leq 2$ ja $t \neq y$. Jos $a = 2$ tai $a = b = 1$, niin tämä on perusyhtälö P2 tai P3. Oletetaan, että $a = 1$ ja $b = 2$. Jos nyt yhtälön oikean puolen neljäs kirjain on y, niin yhtälö redusoituu sijoituksella $x \mapsto zx$ lemman 5.7 yhtälöksi $xy^2z \ldots = zxy^2 \ldots$. Muuten yhtälön θ-kuvat ovat lemman 5.13 kohdan 2 mukaan perusyhtälöitä tai yhtälöitä muotoa $xy^2z \ldots \rightrightarrows zxyx \ldots$ tai $yxzy \ldots \rightrightarrows zxzy \ldots$. Ensimmäisellä on peruspuu lemman 5.15 mukaan, jälkimmäinen redusoituu sijoituksella $y \mapsto zy$ lemman 5.7 yhtälöksi. □

5.17 Lemma. *Yhtälöllä $x^2yt \ldots \rightrightarrows zyzxy \ldots$, missä $t \neq y$, on peruspuu.*

Todistus. Tämän tyypin I yhtälön kaikilla kuvilla on lemman 5.16 perusteella peruspuu lukuunottamatta kuvaa morfismissa $x \mapsto zx$:

$$xzxyz \ldots \leftleftarrows yz^2xy \ldots.$$

Tämä redusoituu sijoituksella $y \mapsto xy$ yhtälöksi $zx^2yz \ldots = yz^2x^2 \ldots$. Tarkastellaan vastaavia yksipuolisia yhtälöitä.

Tyypin II yhtälön

$$zx^2yz \ldots \rightrightarrows yz^2x^2 \ldots \tag{28}$$

kuvat ovat muotoa $zx^2yy^iz \ldots \leftleftarrows yzy^izx^2 \ldots$, ja tämän kuvat morfismeissa $y \mapsto zy$, $y \mapsto zxy$, $y \mapsto zx^2y$ ja muissa morfismeissa puolestaan

$$x^2(zy)^{i+1} \ldots \rightrightarrows yz(zy)^izx^2 \ldots, \tag{29}$$

$$xzx \ldots \rightrightarrows yz^2x \ldots, \tag{30}$$

$$zx^2yzx \ldots \rightrightarrows yz^2x^2y \ldots, \tag{31}$$

$$Dyzx \ldots \rightrightarrows yz^2x^2z \ldots, \tag{32}$$

missä D on sanan zx^2 konjugaatti. Kaksi viimeistä voidaan jakaa yhtälöpareiksi $zx^2yz \rightrightarrows yz^2x^2$, $x \ldots = y \ldots$ ja $Dyz \rightrightarrows yz^2x^2$, $x \ldots = z \ldots$, joilla on seurauksen 2.5 mukaan vain triviaaleja ratkaisuja. Riittää tarkastella kahta ensimmäistä yhtälöä. Ne ovat degeneroitumattomia kuvia, joten niiden kuvat ovat yhtälön 28 θ-kuvia. Nämä ovat lemman 5.16 yhtälöitä lukuunottamatta yhtälön 29 kuvaa morfismissa $x \mapsto yx$:

$$xyx(zy)^{i+1} \ldots \leftleftarrows z^2(yz)^i(yx)^2 \ldots.$$

Kaikki tämän tyypin I yhtälön kuvat ovat jälleen lemman 5.16 yhtälöitä lukuunottamatta kuvaa morfismissa $z \mapsto xz$:

$$yx(xzy)^{i+1} \ldots \rightrightarrows zxz(yxz)^i(yx)^2 \ldots.$$

Tämä puolestaan redusoituu sijoituksella yhtälöksi

$$yx(xz^2y)^{i+1}\ldots = xz(zyxz)^i(zyx)^2\ldots,$$

joka voidaan jakaa yhtälöpariksi $yx^2z^2 = xz^2yx$, $y\ldots = z\ldots$, jolla on seurauksen 2.5 mukaan vain triviaaleja ratkaisuja. Siis yhtälöllä (28) on peruspuu.

Tyypin I yhtälön $zx^2yz\ldots \leftleftarrows yz^2x^2\ldots$ kuvat ovat jotakin muodoista

$$x^2zyz\ldots \rightrightarrows yz^2x^2\ldots, \tag{33}$$

$$xzxyz\ldots \rightrightarrows yz^2x^2\ldots, \tag{34}$$

$$zx^2yz\ldots \rightrightarrows yz^2x^2\ldots. \tag{35}$$

Yhtälön (34) kuvat ovat lemman 5.16 yhtälöitä. Yhtälö (35) on muota (28). Yhtälön (33) kuvat ovat lemman 5.16 yhtälöitä lukuunottamatta kuvaa morfismissa $x \mapsto yx$:

$$xyxzyz\ldots \leftleftarrows z^2(yx)^2\ldots.$$

Kaikki tämän yhtälön kuvat ovat jälleen lemman 5.16 yhtälöitä lukuunottamatta kuvaa morfismissa $z \mapsto xz$:

$$yx^2zyxz\ldots \rightrightarrows zxz(yx)^2\ldots.$$

Tämä puolestaan redusoituu sijoituksella yhtälöksi

$$yx^2z^2yxz\ldots = xz(zyx)^2\ldots,$$

joka voidaan jakaa yhtälöpariksi $yx^2z^2 = xz^2yx$, $y\ldots = z\ldots$, jolla on seurauksen 2.5 mukaan vain triviaaleja ratkaisuja. □

Lemmat 5.16 ja 5.17 todistavat, että jos yhtälöllä on tukipuu, niin sillä on myös peruspuu.

5.18 Lause. *Jokaisella tukiyhtälöllä on peruspuu.*

Todistus. Lemman 5.16 vuoksi riittää tarkastella yhtälöitä (27).

Jos $a = b = 1$, niin kyseessä on yhtälö $xyt\ldots \rightrightarrows z(yz)^dx\ldots$. Tämän tyypin I yhtälön jokainen kuva on lemman 5.16 yhtälö.

Jos $a = 1$ ja $b = 2$, niin kyseessä on yhtälö $xy^2t\ldots \rightrightarrows z(yz)^dx\ldots$. Tämän tyypin I yhtälön kuvat ovat jotakin seuraavista muodoista:

$$xy^2z\ldots \leftleftarrows zyz\ldots, \tag{36}$$

$$xy^2z\ldots \leftleftarrows yzy\ldots, \tag{37}$$

$$xy^2z\ldots \leftleftarrows yz^2s\ldots, \tag{38}$$

$$xy^2z\ldots \leftleftarrows z^2yt\ldots, \tag{39}$$

missä $s \neq z$, $t \neq y$. Tyypin I yhtälön (36) kaikki kuvat ovat kaavan (26) tukiyhtälöitä. Tyypin II yhtälön (37) kaikki θ-kuvat ovat lemman 5.13 kohdan 4 mukaan perusyhtälöitä, kaavan (26) tukiyhtälöitä tai lemman 5.15 yhtälöitä (b). Tyypin II yhtälön (38) kaikki θ-kuvat ovat lemman 5.13 kohdan 3 mukaan lemmojen 5.15, 5.16 ja 5.17 yhtälöitä. Tyypin I yhtälön (39) kaikki kuvat ovat kaavan (26) tukiyhtälöitä lukuunottamatta kuvaa morfismissa $z \mapsto xz$, joka on lemman 5.17 yhtälö.

Jos $a = 2$, niin kyseessä on yhtälö $x^2y^bt\ldots \rightrightarrows z(yz)^dx\ldots$. Tämän tyypin I yhtälön kuvat ovat kaavan (26) tukiyhtälöitä lukuunottamatta kuvaa morfismissa $x \mapsto zx$:

$$xzxy\ldots \rightrightarrows (yz)^dzx\ldots.$$

Jos $d \geq 1$, niin tämän tyypin I yhtälön kaikki kuvat ovat kaavan (26) tukiyhtälöitä. Jos $d = 1$, niin kyseessä on yhtälö (27), missä $a = 1$ ja $b = 2$. □

5.4 Päätulos

Tässä osiossa saadaan neljän lemman jälkeen todistettua peruspuun olemassaolo kaikille yhtälöille ja siten myös päätulos kolmen muuttujan yhtälöiden parametrisista ratkaisuista.

5.19 Lemma. *Yhtälöllä $xy^azy^ps\ldots \rightrightarrows zy^bxy^qt\ldots$, missä $a > 0$, $a+p \neq b+q$ ja $s, t \neq y$, on peruspuu.*

Todistus. Jos $a = 1$ ja $b = 0$, niin yhtälö on perusyhtälö P8. Tarkastellaan muita tapauksia. Yhtälö redusoituu sijoituksilla $x \mapsto zy^cx$ $(c = 0, \ldots, b)$ yhtälöiksi

$$xy^az\ldots \leftleftarrows y^{b-c}zy^cx\ldots \qquad (c = 0, \ldots, b-1), \tag{40}$$

$$xy^azy^psP = zy^bxy^qtQ. \tag{41}$$

Kun $b-c > 1$, niin yhtälö (40) on perusyhtälö P2. Kun $b-c = 1$, niin tyypin II yhtälön (40) θ-kuvilla on peruspuu lemman 5.13 kohdan 4 sekä lemmojen 5.15 ja 5.16 mukaan.

Jos $a = b$, niin yhtälö (41) on perusyhtälö P6 tai P7. Oletetaan, että $a \neq b$. Unohtamalla oletus $a > 0$ voidaan symmetrian vuoksi olettaa, että $a < b$. Käyttämällä ympäristön määritelmän ehtoja Y5 ja Y4 päädytään yhtälöön muotoa $y^dzy^ax\ldots = xy^bz\ldots$, missä $d = b - a \geq 1$. Jaetaan tämä yksipuolisiksi yhtälöiksi

$$y^dzy^ax\ldots \rightrightarrows xy^bz\ldots, \tag{42}$$

$$y^dzy^ax\ldots \leftleftarrows xy^bz\ldots. \tag{43}$$

Jos $d > 1$, niin yhtälö (42) on perusyhtälö P2. Jos $d = 1$, niin sen θ-kuvilla on peruspuu lemman 5.13 kohdan 4 sekä lemmojen 5.15 ja 5.16 mukaan. Yhtälö (43) redusoituu sijoituksilla $x \mapsto y^c x$ $(c = 1, \ldots, d)$ yhtälöiksi

$$y^{d-c}zy^{a+c}x \ldots \rightrightarrows xy^b z \ldots \qquad \text{ja} \qquad zy^{a+d}x \ldots = xy^b z \ldots .$$

Jälkimmäinen on perusyhtälö P6 tai P7, ensimmäinen muotoa (42). □

5.20 Lemma. *Yhtälöllä $xy^a z \ldots \rightrightarrows zy^b x \ldots$, missä $a > 0$, on peruspuu.*

Todistus. Yhtälö voidaan kirjoittaa muotoon

$$E_0 : xy^a zy^p u \ldots \rightrightarrows zy^b xy^q v \ldots ,$$

missä $u, v \neq y$. Jos $a+p = b+q$, niin väite seuraa lemmasta 5.19. Oletetaan, että $a + p \neq b + q$. Olkoon $l \geq 8 + |p - q|$ parillinen. Kuten lemmassa 5.15, muodostetaan yhtälölle E_0 täydellinen joukko θ-kuvia, näille täydellinen joukko θ-kuvia, ja niin edelleen l kertaa. Nämä θ-kuvat muodostavat ketjuja $E_0, \ldots, E_l$. Osoitetaan, että jokaisessa tällaisessa ketjussa on yhtälö, jolla on peruspuu; tämä todistaa lemman väitteen.

Tarkastellaan ensin degeneroituneiden θ-kuvien ketjuja. Tällaista ketjua vastaa tavallisten kuvien degeneroitunut ketju ja voidaan käyttää ympäristön määritelmän kohtaa Y7. Tällöin yhtälö E_l korvautuu lemman 5.19 yhtälöllä $xy^a zy^b xP \rightrightarrows zy^b xy^a zQ$.

Tarkastellaan sitten degeneroitumattomia ketjuja. Tällaisesta ketjusta voidaan erottaa degeneroitunut alkuosa $E_0, \ldots, E_{j-1}$ ja olettaa, että E_j on yhtälön E_{j-1} degeneroitumaton θ-kuva. Jos $b = 0$, niin yhtälö E_0 on muotoa $xy^a z \ldots \rightrightarrows zx \ldots$, ja E_{j-1} on samaa muotoa. Nyt lemman 5.13 kohdan 1 mukaan E_j on tukiyhtälö, joten sillä on peruspuu. Jos $b > 0$, niin E_0 on muotoa $xy^a z \ldots \rightrightarrows zy^b x \ldots$. Yhtälö E_{j-1} on joko samaa muotoa tai muotoa, jossa yhtälön puolet ovat vaihtaneet paikkaa. Symmetrian vuoksi riittää tarkastella ensimmäistä tapausta. Nyt E_j on muotoa $y^c zy^d x \ldots \rightrightarrows xy^a z \ldots$, missä $c + d = a$ ja $c \geq 1$. Jos $c > 1$, niin E_j on perusyhtälö P2. Jos $c = 1$, niin yhtälöllä E_j on peruspuu lemman 5.13 kohdan 4 sekä lemmojen 5.15 ja 5.16 perusteella. □

5.21 Lemma. *Yhtälöllä $xy^a t \ldots \rightrightarrows z^c xB(x, z)y \ldots$, missä $a, c \geq 1$ ja $t \neq y$, on peruspuu.*

Todistus. Lemman 5.13 kohdan 1 mukaan tämän tyypin II yhtälön kaikki θ-kuvat ovat tukiyhtälöitä tai lemman 5.20 yhtälöitä. □

5.22 Lemma. *Yhtälöllä $x^n y^m t \ldots \rightrightarrows zyA(y, z)x \ldots$, missä $n, m \geq 1$ ja $t \neq y$, on peruspuu.*

Todistus. Yhtälö on tyyppiä I; todistetaan, että kaikilla sen kuvilla on peruspuu. Jos $n = 1$, yhtälön jokainen kuva on muotoa

$$xy^m z \ldots \leftleftarrows Dx \ldots, \tag{44}$$

missä D on sanan zyA konjugaatti. Jos $n > 1$, niin yhtälön kuva morfismissa $x \mapsto zx$ on

$$x(zx)^{n-1} y \ldots \leftleftarrows yAzx \ldots, \tag{45}$$

ja kaikki muut kuvat ovat muotoa

$$xzy \ldots \leftleftarrows Dx \ldots, \tag{46}$$

missä D on sanan zyA konjugaatti.

Tarkastellaan yhtälöä (44). Jos $y^2 \leq D$, niin tämä on perusyhtälö P2. Jos $yz \leq D$, niin tämä on lemman 5.21 yhtälö. Jos $z \leq D$, niin tämä on muotoa

$$x^a y^b s \ldots \rightrightarrows zy^d x \ldots, \tag{47}$$

missä $a, b, d \geq 1$ ja $s \neq y$. Yhtälö (46) voidaan käsitellä samalla tavalla kuin yhtälö (44). Yhtälö (45) on muotoa

$$x^a y^b s \ldots \rightrightarrows z(yz)^d x \ldots, \tag{48}$$

missä $a, b, d \geq 1$ ja $s \neq y$. Riittää todistaa, että yhtälöillä (47) ja (48) on peruspuu.

Tarkastellaan yhtälöä (47). Oletetaan ensin, että $a = 1$. Nyt jokainen tämän tyypin I yhtälön kuva on muotoa $xy^b z \ldots \leftleftarrows Dx$, missä D on sanan zy^d konjugaatti. Jos $z \leq D$, niin tämä on lemman 5.20 yhtälö. Jos $y^2 \leq D$, niin tämä on perusyhtälö P2. Jos $yz \leq D$, niin tämä on lemman 5.21 yhtälö. Oletetaan sitten, että $a > 1$. Nyt tämän tyypin I yhtälön kuva morfismissa $x \mapsto zx$ on $x(zx)^{a-1} y \ldots \leftleftarrows y^d zx \ldots$, ja kaikki muut kuvat ovat muotoa $xzy \ldots \leftleftarrows Dx \ldots$, missä D on sanan zy^d konjugaatti. Ensimmäinen näistä on tyyppiä I ja kaikilla sen kuvilla on peruspuu lauseen 5.18 mukaan. Jälkimmäinen on lemman 5.21 yhtälö, jos $zy \leq D$; muutoin sen kaikilla kuvilla on peruspuu lauseen 5.18 mukaan.

Tarkastellaan yhtälöä (48). Oletetaan ensin, että $a = 1$. Nyt jokainen tämän tyypin I yhtälön kuva on muotoa $xy^b z \ldots \leftleftarrows Dx$, missä D on sanan $z(yz)^d$ konjugaatti. Jos $yz \leq D$, niin tämä on lemman 5.21 yhtälö. Muuten Dx on muotoa $z^c ys$, missä $1 \leq c \leq 2$ ja $s \neq y$, jolloin tämä kuva on muotoa (47) ja sillä on peruspuu. Oletetaan sitten, että $a > 1$. Nyt tämän tyypin I yhtälön kuva morfismissa $x \mapsto zx$ on $x(zx)^{a-1} y \ldots \leftleftarrows (yz)^d zx \ldots$, ja kaikki muut kuvat ovat muotoa $xzy \ldots \leftleftarrows Dx \ldots$, missä D on sanan $z(yz)^d$ konjugaatti. Ensimmäinen näistä palautuu yhtälön (48) tapaukseen $a = 1$. Jälkimmäisellä on peruspuu lemman 5.16 mukaan. □

5.23 Lause. *Jokaisella kolmen muuttujan yhtälöllä on peruspuu.*

Todistus. Triviaali yhtälö $U = U$ on perusyhtälö. Kaikki muut yhtälöt voidaan vasemmalta supistamisen jälkeen jakaa yksipuolisiksi yhtälöiksi. Riittää siis todistaa väite kaikille yksipuolisille yhtälöille. Jokainen näistä saadaan kertomalla oikealta sopivilla muuttujilla johonkin muodoista

$$x^2 \ldots \rightrightarrows y^c x \ldots \tag{49}$$

$$xy \ldots \rightrightarrows y^c x \ldots \tag{50}$$

$$xz^a t \ldots \rightrightarrows y^c x B(x,y) z \ldots \tag{51}$$

$$x^a y^b s \ldots \rightrightarrows y^c z B(y,z) x \ldots \tag{52}$$

$$x^a z^b t \ldots \rightrightarrows y z B(y,z) x \ldots \tag{53}$$

$$x^a z^b t \ldots \rightrightarrows y^d z B(y,z) x \ldots, \tag{54}$$

missä $a, b, c \geq 1$, $d > 1$, $t \neq z$ ja $s \neq y$. Todistetaan, että kaikilla näillä on peruspuu.

Yhtälö (49) on perusyhtälö P2. Yhtälö (50) redusoituu sijoituksella $x \mapsto yx$ yhtälöksi $xy \ldots = y^c x \ldots$, joka on perusyhtälö P1. Yhtälö (51) on lemman 5.21 yhtälö. Yhtälö (53) on lemman 5.22 yhtälö.

Yhtälö (52) on tyyppiä I ja sen kuvat ovat muotoa $xy \ldots \leftleftarrows Dx \ldots$, missä D on sanan $y^c z B$ konjugaatti. Jos $y^2 \leq D$, niin tämä kuva on muotoa (49), jos $yz \leq D$, niin muotoa (51), ja jos $z \leq D$, niin muotoa (53). Siis yhtälön (52) kaikilla kuvilla ja siten myös yhtälöllä itsellään on peruspuu.

Yhtälö (54) on tyyppiä I ja sen kuvat ovat muotoa $x(y \ldots)^{a-1} z^b y \ldots \leftleftarrows Dx \ldots$, missä D on sanan $y^d z B$ konjugaatti. Jälleen nähdään, että tämä kuva on muotoa (49), (51) tai (53). Siis yhtälön (54) kaikilla kuvilla ja siten myös yhtälöllä itsellään on peruspuu. □

5.24 Lause. *Jokaisen kolmen muuttujan yhtälön ratkaisut voidaan esittää parametrisesti.*

Todistus. Lauseen 5.23 mukaan jokaisella kolmen muuttujan yhtälöllä E on peruspuu. Lauseen 4.3 mukaan yhtälön E peruspuun lehtisolmujen ratkaisut voidaan esittää parametrisesti. Nyt lauseesta 5.4 seuraa, että kaikkien puun solmuina olevien yhtälöiden ratkaisut voidaan esittää parametrisesti. Siis erityisesti juurisolmun E ratkaisut voidaan esittää parametrisesti. □

Kolmen muuttujan yhtälöiden ratkaisujen parametrisoituvuus on nyt todistettu. Tulos on efektiivinen eli parametrinen ratkaisu voitaisiin periaatteessa löytää algoritmisesti, vaikka tätä näkökulmaa ei ole työssä tarkasteltu. Tulos voitaisiin yleistää myös yhtälöryhmille, sillä Hmelevskii antaa tavan muuttaa yhtälöryhmä yksittäiseksi yhtälöksi.

Viitteet

[1] C. Choffrut, J. Karhumäki: *Combinatorics of words*. Kirjassa G. Rozenberg, A. Salomaa (eds): *Handbook of Formal Languages*, Springer, 1997.

[2] E. Czeizler: *The non-parametrizability of the word equation $xyz = zvx$: a short proof*. Theoretical Computer Science, 345:296–303, 2005.

[3] J. Hmelevskii: *Equations in free semigroups*. Proceedings of the Steklov Institute of Mathematics, 107, 1971. Käännös, American Mathematical Society, 1976.

[4] J. Karhumäki: *On cube-free ω-words generated by binary morphisms*. Discrete Applied Mathematics, 5:279–297, 1983.

[5] M. Lothaire: *Combinatorics on words*. Addison-Wesley, 1983.

[6] M. Lothaire: *Algebraic combinatorics on words*. Cambridge University Press, 2002.