Tartu Ülikool
Matemaatikateaduskond
Arvutiteaduse Instituut

Alamsõnad ning nende loendamine

semestritöö

Peeter Laud
juhendaja Uno Kaljulaid

Tartu, 1997

Kokkuvõte

Käesolev töö on suuremas osas [Lot] kuuenda peatüki refereerimine. Teksti sisse on lisatud mõnede peatüki lõpus olevate ülesannete lahendused — mõned neist on toodud paragrahvi 2.1 lõpus, samuti on paragrahv 3.2 ülesannete järgi kirjutatud.

Töös toome kõigepealt ära vaba (sõnade) monoidi moodustamise konstruktsiooni ja formaalsete ridade ringi konstruktsiooni. Seejärel defineerime sõna alamsõna kui sõna, mis on esialgsest saadav mõningate tähtede kustutamise läbi. Alamsõna mõiste kaudu saame defineerida vabal monoidil teatava järjestuse, me näitame, et sel viisil saadud osaliselt järjestatud hulgas pole lõpmatuid antiahelaid.

Uurides, mitmel erineval viisil võime ühe sõna alamsõnana saada teise sõna, jõuame binoomkordaja mõiste üldistamiseni. Suurem osa tööst ongi pühendatud nende üldistatud binoomkordajate vaheliste seoste uurimisele.

Sisukord

0 Sissejuhatus

Olgu A lõplik hulk, mida nimetame tähestikuks ja mille elemente nimetame tähtedeks. Sõnaks üle tähestiku A nimetame lõpliku pikkusega (kaasa arvatud pikkusega 0) järjendit A elementidest. Kõigi sõnade hulka üle tähestiku A tähistame A^*.

Sõna $f = a_1 a_2 \dots a_n$ pikkuseks nimetame tähtede arvu f-s (tähistame $|f|$). Sõnade $f = a_1 a_2 \dots a_n$ ja $g = b_1 b_2 \dots b_m$ korrutiseks nimetame sõna $f \cdot g = a_1 a_2 \dots a_n b_1 b_2 \dots b_m$. Ilmne on, et selliselt defineeritud korrutamine on assiotsiatiivne ja selle suhtes on olemas ühikelement — sõna pikkusega 0 (edaspidi tähistame seda sõna Λ-ga). Seega $(A^*, \cdot)$ on monoid. Monoidi $(A^*, \cdot)$ nimetatakse vabaks monoidiks baasiga A.

Formaalseteks ridadeks üle A^* kordajatega ringist $\mathbb{Z}$ nimetame funktsioone $\phi : A^* \to \mathbb{Z}$. Funktsiooni väärtust kohal $f \in A^*$ nimetame f kordajaks reas ϕ ja tähistame $\langle \phi, f \rangle$. Formaalset rida ϕ kirjutame üles kujul $\sum_{f \in A^*} \langle \phi, f \rangle f$. Kõigi formaalsete ridade hulka üle A^* kordajatega ringist $\mathbb{Z}$ tähistame $\mathbb{Z}\langle\langle A^* \rangle\rangle$.
Formaalsete ridade ϕ ja ψ summaks nimetame rida

$$\phi + \psi = \sum_{f \in A^*} (\langle \phi, f \rangle + \langle \psi, f \rangle) f$$

ja korrutiseks rida

$$\phi \cdot \psi = \sum_{f \in A^*} \left(\sum_{g,h \in A^*, gh = f} \langle \phi, g \rangle \langle \psi, h \rangle \right) f$$

Hulk $\mathbb{Z}\langle\langle A^* \rangle\rangle$ koos niiviisi defineeritud summa ja korrutisega on (ühikuga) ring.
Formaalset rida ϕ nimetame polünoomiks, kui hulk $\{f \mid \langle \phi, f \rangle \neq 0\}$ on lõplik. Polünoomide hulka (üle A^* kordajatega ringist $\mathbb{Z}$ tähistame $\mathbb{Z}\langle A^* \rangle$. On ilmne, et $\mathbb{Z}\langle A^* \rangle$ on $\mathbb{Z}\langle\langle A^* \rangle\rangle$ alamring.

1 Jaguvuse kaudu antud järjestusest

Definitsioon 1.1. Olgu $f = a_1 a_2 \dots a_n \in A^*$. Sõna $g \in A^*$ nimetame sõna f *alamsõnaks*, kui $g = b_1 b_2 \dots b_m$ ja leiduvad sellised naturaalarvud $1 \leq i_1 < i_2 < \dots < i_m \leq n$, et $a_{i_j} = b_j \ \forall j \in [1 \dots m]$.

Teisisõnu, g on f alamsõna, kui $g = f$ või kui g on saadav f-st mõnede tähtede kustutamisega.
Alamsõna mõiste defineerib jaguvuse hulgal A^*, ütleme, et sõna g jagab sõna f (ja tähistame seda $g|f$), kui g on f alamsõna. Siis kehtib:

Lause 1.1. *Jaguvus on korrutamisega kooskõlas olev osaline järjestus hulgal A^*.*

Tõestuseks märgime, et iga sõna on iseenda alamsõna, ja et kui g on f alamsõna ja h on g alamsõna, siis h on f alamsõna — seega jaguvus on refelksiivne ja transitiivne seos. Samuti, kui g jagab f-i, siis $|g| \leq |f|$, kusjuures võrdus kehtib parajasti siis, kui $g = f$. Seega on jaguvus antisümmeetriline. See, et jaguvus on kooskõlas korrutamisega järeldub sellest, et kui g on f alamsõna ja g' on f' alamsõna, siis gg' on ff' alamsõna. ■

Osaliselt järjestatud hulk $(A^*, |)$ pole ei ülemine ega ka alumine poolvõre. Tõepoolest, olgu $A = \{a, b\}$, siis $ab|aba$ ja $ab|bab$, kuid aba ja bab on mittevõrreldavad. Samuti $ba|aba$, kuid ab ja ba on mittevõrreldavad. Jaguvusseose põhiline omadus on järgmine:

Teoreem 1.2. *Suvaline paarikaupa mittevõrreldavate sõnade hulk üle lõpliku tähestiku on lõplik.*
Teisisõnu — osaliselt järjestatud hulgas $(A^*, |)$ pole lõpmatuid antiahelaid.

Tõestus: Oletame vastuväiteliselt, et leidub lõpmatuid paarikaupa mittevõrreldavate sõnade hulki. Sel juhul on ka olemas lõpmatud sõnade *jaguvuseta* jadad — s.t. jadad $(f_i)_{i \in \mathbb{N}}$, kus $f_i \in A^*$ ja kus sellest, et $i < j$ järeldub, et $f_i \not| f_j$. Nende hulgast võime välja valida kõige „varasema“ jada, s.t. sellise jada $(f_i)_{i \in \mathbb{N}}$, kus

- f_1 on minimaalse pikkusega kõigi nende sõnade hulgas, millest algab mõni jaguvuseta jada.
- f_2 on minimaalse pikkusega kõigi nende sõnade hulgas, mille korral f_1, f_2 on mõne jaguvuseta jada esimesteks liikmeteks.
- f_3 on minimaalse pikkusega kõigi nende sõnade hulgas, mille korral f_1, f_2, f_3 on mõne jaguvuseta jada esimesteks liikmeteks.
- ja nii edasi

Kuna tähestik A on lõplik, siis leidub saadud jadas lõpmata palju selliseid liikmeid, mis kõik algavad ühe ja sama tähega. Olgu see täht a ja olgu need liikmed $f_{i_1} = ag_1, f_{i_2} = ag_2, \dots$, kus $i_1 < i_2 < \cdots$. Sel juhul saame moodustada lõpmatu jaguvuseta jada $f_1, f_2, \dots, f_{i_1-1}, g_1, g_2, \dots$, mis on „varasem" kui (f_i); aga see on vastuolus (f_i) valikuga. ■

Märgime, et kuigi $(A^*, |)$ ei sisalda lõpmatuid antiahelaid, leidub seal kuitahes suure võimsusega lõplikke antiahelaid. Tõepoolest, hulk $\{f \in A^* | \, |f| = n\}$, kus n on mingi fikseeritud naturaalarv, on antiahel.

2 Alamsõnade loendamisest

2.1 Binoomkordaja mõiste

Me defineerisime sõna kui tähtede lõpliku järjendi ja mingi sõna f alamsõna kui järjendi f alamjärjendi. Paneme tähele, et kaks erinevat alamjärjendit võivad defineerida sama alamsõna. Kuna me hakkame pöörama tähelepanu sellele, mitu korda üks sõna on saadav teise sõna alamsõnana, siis omab mõtet järgmine

Definitsioon 2.1. Olgu $f, g \in A^*$. f ja g *binoomkordajaks* (tähistatakse $\binom{f}{g}$) nimetatakse järjendi f erinevate alamjärjendite arvu, mis sõnadena on võrdsed sõnaga g.

Näide 2.1. $\binom{abab}{ab} = 3$, $\binom{aabbaa}{aba} = 8$.

Nimetust „binoomkordaja" õigustab märkus, et kui tähestik $A = \{a\}$, siis $\binom{a^m}{a^n} = \binom{m}{n}$, kus $\binom{m}{n}$ on klassikaline binoomkordaja. Tõepoolest, a^n on saadav a^m alamsõnana nii mitmel viisil, kui mitmel viisil on võimalik m positsiooni hulgast välja valida n tükki (valimisjärjekorda arvestamata).

Kehtivad järgmised võrdused:

$$\forall f \in A^* \qquad \binom{f}{\Lambda} = 1 \tag{2.1}$$

Tõepoolest, iga järjend sisaldab täpselt ühe järjendi pikkusega 0. Veel kehtib

$$\forall f, g \in A^* \qquad |f| < |g| \Rightarrow \binom{f}{g} = 0, \tag{2.2}$$

sest et f ükski alamsõna pole pikem kui f ise.
Kroneckeri sümbol $\delta_{f,g}$, kus $f, g \in A^*$, on võrdne ühega parajasti siis kui $f = g$ ja nulliga kui $f \neq g$. Kehtib

Lause 2.1.

$$\forall f,g \in A^*, \forall a,b \in A: \quad \binom{fa}{gb} = \binom{f}{gb} + \delta_{a,b}\binom{f}{g} \tag{2.3}$$

Tõestus: Kui $a \neq b$, siis fa alamjärjendid, mis on võrdsed gb-ga on parajasti f alamjärjendid, mis on võrdsed gb-ga. Kui $a = b$, siis fa alamjärjend, mis on võrdne ga-ga kas sisaldab fa viimast tähte või ei sisalda. Esimesel juhul, eemaldades alamjärjendist viimase tähe, saame sõna f mingi alamjärjendi, mis on võrdne sõnaga g. Vastupidi, kui me lisame sõna f mingile alamjärjendile, mis on võrdne sõnaga g, paremalt poolt juurde tähe a, siis saame sõna fa alamjärjendi, mis on võrdne sõnaga ga. Kui fa alamjärjend ei sisalda fa viimast tähte, siis on taas tegemist sõna f alamjärjendiga (mis on võrdne ga-ga). Seega on fa alamjärjendite, mis on võrdsed ga-ga, arv võrdne f-i ga-ga või g-ga võrdsete alamjärjendite arvuga. ■

Lause 2.1 üldistab Pascali valemit $\binom{m}{n} = \binom{m-1}{n} + \binom{m-1}{n-1}$. Sarnaselt klassikalise juhuga võime väita, et

Lause 2.2. *Võrdus (2.3) koos rajatingimustega (2.1) ja (2.2) määravad binoomkordajad* $\binom{f}{g}$ *kõigi* $f,g \in A^*$ *jaoks.*

Tõestus: Induktsiooniga $|f|$ järgi. Seosed (2.1) ja (2.2) määravad $\binom{\Lambda}{g}$ iga $g \in A^*$ jaoks. Seejärel on $\binom{fa}{g}$ määratud iga $g \in A^*$ jaoks — Valemi (2.1) järgi juhuks $g = \Lambda$ ja valemi (2.3) järgi juhuks $g \neq \Lambda$. ■

Veel kehtivad järgmised võrdused:

- $$\sum_{\substack{g\in A^* \\ |g|=n}} \binom{f}{g} = \binom{|f|}{n},$$

  kus $f \in A^*$ ja $n \in \mathbb{N} \cup \{0\}$.
  Tõepoolest, ühest küljest on sõna f kõigi n-elemendiliste alamjärjendite arv $\binom{|f|}{n}$, teisest küljest on iga selline alamjärjend võrdne mingi n-tähelise sõnaga, kusjuures iga n-täheline sõna g tuleb ette täpselt $\binom{f}{g}$ korral.

- $$\sum_{g\in A^*} \binom{f}{g} = 2^{|f|},$$

kus $f \in A^*$.
Tõepoolest, eelmisest võrdusest järeldub, et

$$\sum_{g \in A^*} \binom{f}{g} = \sum_{n=0}^{\infty} \sum_{\substack{g \in A^* \\ |g|=n}} \binom{f}{g} = \sum_{n=0}^{\infty} \binom{|f|}{n} = 2^{|f|}$$

- Kõigi $f, g \in A^*$ ja $a \in A$ jaoks kehtib

$$\binom{f}{ga} = \sum_{\substack{u,v \in A^* \\ uav=f}} \binom{u}{g} \tag{2.4}$$

Selle võrduse kehtivust näitame induktsiooniga üle $|f|$. Kui $f = \Lambda$, siis $\binom{\Lambda}{ga} = 0$ valemi (2.2) põhjal ja võrduse (2.4) paremal pool seisvas summas pole ühtegi liidetavat. Kui $f' \neq \Lambda$, siis oletame, et valem (2.4) kehtib kõigi $f \in A^*$ jaoks, kui $|f| < |f'|$. Kuna $f' = fb$ mingi $f \in A^*, |f| < |f'|$ ja $b \in A$ jaoks, siis

$$\binom{fb}{ga} = \binom{f}{ga} + \delta_{b,a}\binom{f}{g} = \sum_{\substack{u,v \in A^* \\ uav=f}} \binom{u}{g} + \delta_{fa,fb}\binom{f}{g}$$

$$= \sum_{\substack{u,v \in A^* \\ ua(vb)=fb}} \binom{u}{g} + \sum_{\substack{u \in A^* \\ ua\Lambda=fb}} \binom{u}{g} = \sum_{\substack{u,v \in A^* \\ uav=fb}} \binom{u}{g}$$

Sarnaselt klassikalisele Pascali kolmnurgale võime me paigutada binoomkordajad lõpmatusse maatriksisse, mille read ja veerud on indekseeritud A^* elementidega ja kus positsioonil (f, g) seisab väärtus $\binom{f}{g}$. Nimetame seda maatriksit Pascali maatriksiks P. Kui P read ja veerud on mõlemad leksikograafiliselt järjestatud, siis on ta alumine kolmnurkmaatriks.

2.2 Magnuse teisendus ja segamiskorrutis

Definitsioon 2.2. *Magnuse teisenduseks* nimetatakse ringi $\mathbb{Z}\langle A^*\rangle$ endomorfismi μ, mis on defineeritud võrdustega:

$$\mu(a) = 1 + a \qquad \forall a \in A$$

Selle definitsiooni mõtte avab järgmine

Teoreem 2.3.

$$\mu(f) = \sum_{g\in A^*} \binom{f}{g} g \quad \forall f \in A^*$$

Tõestus: Induktsiooniga $|f|$ järgi. Võrdus kehtib $f = \Lambda$ jaoks. Kui $f \in A^*$ ja $a \in A$, siis

$$\mu(fa) = \mu(f)(1+a) = \left(\sum_{h\in A^*} \binom{f}{h} h\right)(1+a)$$
$$= \sum_{h\in A^*} \binom{f}{h} h + \sum_{h\in A^*} \binom{f}{h} ha.$$

Rühmitame esimeses summas liidetavaid järgmiselt: esiteks $h = \Lambda$; teiseks $h = ga$, kus $g \in A^*$; kolmandaks $h = gb$, kus $g \in A^*$ ja $b \in A\backslash\{a\}$. Siis saame

$$\mu(fa) = \binom{f}{\Lambda}\Lambda + \sum_{\substack{g\in A^* \\ b\in A\backslash\{b\}}} \binom{f}{gb} gb + \sum_{g\in A^*} \binom{f}{ga} ga + \sum_{h\in A^*} \binom{f}{h} ha$$

Nüüd:

- $$\binom{f}{\Lambda}\Lambda = 1\cdot\Lambda = \binom{fa}{\Lambda}\Lambda$$

- $$\sum_{\substack{g\in A^* \\ b\in A\backslash\{b\}}} \binom{f}{gb} gb = \sum_{\substack{g\in A^* \\ b\in A\backslash\{b\}}} \binom{fa}{gb} gb$$

- $$\sum_{g\in A^*} \binom{f}{ga} ga + \sum_{h\in A^*} \binom{f}{h} ha = \sum_{g\in A^*} \left(\binom{f}{ga} + \binom{f}{g}\right) ga = \sum_{g\in A^*} \binom{fa}{ga} ga$$

Millest järeldub

$$\mu(fa) = \sum_{g\in A^*} \binom{fa}{g} g. \qquad \blacksquare$$

Teoreemi 2.3 võib teisiti sõnastada järgmiselt:

$$\forall f,g \in A^* \qquad \langle \mu(f), g\rangle = \binom{f}{g}$$

Sellest ja sellest, et Magnuse teisendus on endomorfism, saame

Järeldus 2.4.

$$\forall f,g,h \in A^* \quad \binom{fh}{g} = \sum_{\substack{u,v\in A^*\\ uv=g}} \binom{f}{u}\binom{h}{v}$$

Tõestus: Võrduse vasakul poolel seisab $\langle \mu(fh), g\rangle$, paremal poolel $\langle \mu(f)\mu(h), g\rangle$. Kuna μ on homomorfism, siis on need kaks suurust võrdsed. ■

Näeme, et rea $\mu(f)$ kordajad saame Pascali maatriksi reast märgendiga f. Järgnevalt näitame, kuidas saada sõnast f rida, mille kordajad saadakse Pascali maatriksi veerust märgendiga f.

Definitsioon 2.3. *Segamiskorrutiseks* nimetatakse binaarset operatsiooni (aditiivsel rühmal) $\mathbb{Z}\langle\langle A^*\rangle\rangle$, mida tähistame $\circ$-ga ja mis määratakse induktiivselt seostest

- $$\forall f \in A^* \quad f\circ\Lambda = \Lambda\circ f = f \tag{2.5}$$

- $$\forall f,g \in A^*, \forall a,b\in A \quad fa\circ gb = (f\circ gb)a + (fa\circ g)b \tag{2.6}$$

- $$\forall s,t \in \mathbb{Z}\langle\langle A^*\rangle\rangle \quad s\circ t = \sum_{f,g\in A^*} \langle s,f\rangle\langle t,g\rangle(f\circ g) \tag{2.7}$$

Kui $f,g \in A^*$, siis $f\circ g$ on homogeenne $|f|+|g|$-astme polünoom (induktsiooniga üle $|f|+|g|$). Tänu sellele on kahe rea segamiskorrutis hästi defineeritud, olgugi et definitsioonis on kirjas lõpmatu summeerimine. Intuitiivselt võib kahe sõna segamiskorrutist kirjeldada järgmiselt: sõna h kordaja sõnade f ja g segamiskorrutises on võrdne erinevate võimaluste arvuga valida sõnast h kaks alamjärjendit, mis oleksid teineteise täienditeks ja millest esimene oleks võrdne sõnaga f ja teine sõnaga g.

Segamiskorrutise omaduste näitamiseks läheb meil vaja paari lemmat:

Lemma 2.5. *Olgu* $s, t \in \mathbb{Z}\langle\langle A^*\rangle\rangle$, *olgu* $x, y \in A$. *Siis*

$$sx \circ ty = (s \circ ty)x + (sx \circ t)y.$$

Tõestus: Valemi (2.7) järgi $sx \circ ty = \sum_{f,g \in A^*} \langle sx, f\rangle\langle ty, g\rangle f \circ g$. Kuna reas sx saavad nullist erinevad kordajad olla vaid sõnadel, mis lõpevad x-ga (sama mõttekäik ty jaoks), siis

$$\begin{aligned} sx \circ ty &= \sum_{f,g \in A^*} \langle sx, fx\rangle\langle ty, gy\rangle(fx \circ gy) \\ &= \sum_{f,g \in A^*} \langle sx, fx\rangle\langle ty, gy\rangle((fx \circ g)y + (f \circ gy)x) \\ &= \left(\sum_{f,g \in A^*} \langle sx, fx\rangle\langle t, g\rangle(fx \circ g)\right) y + \left(\sum_{f,g \in A^*} \langle s, f\rangle\langle ty, gy\rangle(f \circ gy)\right) x \\ &= (sx \circ t)y + (s \circ ty)x, \end{aligned}$$

sest $\langle sx, fx\rangle = \langle s, f\rangle$ ja $\langle ty, gy\rangle = \langle t, g\rangle$, kui $s, t \in \mathbb{Z}\langle\langle A^*\rangle\rangle$,$f, g \in A^*$, $x, y \in A$. ■

Lemma 2.6. *Olgu* $s, t \in \mathbb{Z}\langle\langle A^*\rangle\rangle$, *olgu* $u, v \in \mathbb{Z}\langle A^*\rangle$ *homogeensed esimese astme polünoomid. Siis:*

$$su \circ tv = (s \circ tv)u + (su \circ t)v$$

Tõestus: Meil on $u = \sum_{x \in A} \langle u, x\rangle x$ ja $v = \sum_{y \in A} \langle v, y\rangle y$. Nüüd

$$\begin{aligned} su \circ tv &= s \cdot \left(\sum_{x \in A} \langle u, x\rangle x\right) \circ t \cdot \left(\sum_{y \in A} \langle v, y\rangle y\right) \\ &= \sum_{x,y \in A} \langle u, x\rangle\langle v, y\rangle(sx \circ ty) = \sum_{x,y \in A} \langle u, x\rangle\langle v, y\rangle((sx \circ t)y + (s \circ ty)x \\ &= \sum_{y \in A} \left(s \cdot \left(\sum_{x \in A} \langle u, x\rangle x\right) \circ t\right) \langle v, y\rangle y \\ &+ \sum_{x \in A} \left(s \circ t \cdot \left(\sum_{y \in A} \langle v, y\rangle y\right)\right) \langle u, x\rangle x = (su \circ t)v + (s \circ tv)u \end{aligned}$$ ■

Lause 2.7. *Segamiskorrutis on kommutatiivne ja assiotsiatiivne tehe.*

Tõestus: Tõestame mõlemad omadused A^* elementide jaoks. Seejärel laiendab seos (2.7) mõlemad omadused $\mathbb{Z}\langle\langle A^*\rangle\rangle$-le.
(Assiotsiatiivsus) Olgu $f, g, h \in A^*$. Teeme induktsiooni $|f| + |g| + |h|$ järgi. Kui mõni nendest sõnadest on tühi sõna, siis on ilmne, et $(f \circ g) \circ h = f \circ (g \circ h)$ (järeldub seosest (2.5)). Olgu nüüd $a, b, c \in A$, siis

$$
\begin{aligned}
(fa \circ gb) \circ hc &= ((f \circ gb)a + (fa \circ g)b) \circ hc \\
&= (f \circ gb)a \circ hc + (fa \circ g)b \circ hc \\
&= ((f \circ gb) \circ hc)a + ((f \circ gb)a \circ h)c + ((fa \circ g) \circ hc)b + ((fa \circ g)b \circ h)c \\
&= ((f \circ gb) \circ hc)a + ((fa \circ g) \circ hc)b + (((f \circ gb)a + (fa \circ g)b) \circ h)c \\
&= ((f \circ gb) \circ hc)a + ((fa \circ g) \circ hc)b + ((fa \circ gb) \circ h)c
\end{aligned}
$$

Nüüd kasutame induktsiooni eeldust ja saame

$$
\begin{aligned}
&(fa \circ gb) \circ hc \\
&= (f \circ (gb \circ hc))a + (fa \circ (g \circ hc))b + (fa \circ (gb \circ h))c \\
&= (f \circ ((gb \circ h)c + (g \circ hc)b))a + (fa \circ (g \circ hc))b + (fa \circ (gb \circ h))c \\
&= (f \circ (gb \circ h)c)a + (fa \circ (gb \circ h))c + (f \circ (g \circ hc)b)a + (fa \circ (g \circ hc))b \\
&= fa \circ (gb \circ h)c + fa \circ (g \circ hc)b \\
&= fa \circ ((gb \circ h)c + (g \circ hc)b) = fa \circ (gb \circ hc)
\end{aligned}
$$

(Kommutatiivsus) Olgu $f, g \in A^*$. Teeme induktsiooni $|f| + |g|$ järgi. Kui $f = \Lambda$ või $g = \Lambda$, siis saame seosest (2.5), et $f \circ g = g \circ f$. Olgu nüüd $a, b \in A$, siis

$$fa \circ gb = (f \circ gb)a + (fa \circ g)b = (gb \circ f)a + (g \circ fa)b = gb \circ fa \quad \blacksquare$$

Järgenvalt tähistame $\mathbf{A}^*$-ga A^*-i karakteristlikku rida, s.t. $\mathbf{A}^* = \sum_{f \in A^*} 1 \cdot f$. Analoogiliselt olgu $\mathbf{A}^+ = \sum_{f \in A^+} 1 \cdot f$ ja $\mathbf{A} = \sum_{x \in A} 1 \cdot x$, kus $A^+ = A^* \setminus \{\Lambda\}$. Näeme, et $1 + \mathbf{A}^+ = \mathbf{A}^*$ ja $\mathbf{A}^+ = \mathbf{A} \cdot \mathbf{A}^* = \mathbf{A}^* \cdot \mathbf{A}$, kus 1 tähistab rida $1 \cdot \Lambda$. Kehtib järgmine

Lemma 2.8. *Iga $g \in A^*$ ja iga $a \in A$ korral*

$$ga \circ \mathbf{A}^* = (g \circ \mathbf{A}^*)a\mathbf{A}^*$$

Tõestus:

$$
\begin{aligned}
ga \circ \mathbf{A}^* &= ga \circ (1 + \mathbf{A}^*\mathbf{A}) = ga \circ 1 + ga \circ (\mathbf{A}^*\mathbf{A}) \\
&= (g \circ 1)a + (ga \circ \mathbf{A}^*)\mathbf{A} + (g \circ \mathbf{A}^+)a = (g \circ \mathbf{A}^*)a + (ga \circ \mathbf{A}^*)\mathbf{A}
\end{aligned}
$$

Seega oleme saanud

$$ga \circ \mathbf{A}^* = (g \circ \mathbf{A}^*)a + (ga \circ \mathbf{A}^*)\mathbf{A},$$

millest

$$(ga \circ \mathbf{A}^*)(1 - \mathbf{A}) = (g \circ \mathbf{A}^*)a$$

Korrutades seda võrdust paremalt $\mathbf{A}^*$-ga saame soovitu, sest $(1-\mathbf{A})\mathbf{A}^* = 1$. ■

Nüüd võime formuleerida tulemuse, milleni me tahtsime jõuda segamiskorrutist defineerides.

Teoreem 2.9. *Kõigi sõnade $g \in A^*$ jaoks kehtib*

$$g \circ \mathbf{A}^* = \sum_{f \in A^*} \binom{f}{g} f.$$

Viimase väite võime kirja panna kujul

$$\forall f, g \in A^* \qquad \langle g \circ \mathbf{A}^*, f \rangle = \binom{f}{g},$$

mis tähendab, et segamine $\mathbf{A}^*$-ga on duaalne Magnuse teisendusega.
Järgneb teoreemi

Tõestus: Teeme induktsiooni üle $|g|$. Olgu $f \in A^*$. Kui $g = \Lambda$, siis

$$\langle \Lambda \circ \mathbf{A}^*, f \rangle = \langle \mathbf{A}^*, f \rangle = 1.$$

Kehtigu nüüd $\langle h \circ \mathbf{A}^*, f \rangle = \binom{f}{h}$, kus $f, h \in A^*$ kõigi h-de korral, kus $|h| \leq |g|$. Olgu $a \in A$, siis

$$\begin{aligned}\langle ga \circ \mathbf{A}^*, f \rangle = \langle (g \circ \mathbf{A}^*)a\mathbf{A}^*, f \rangle &= \sum_{\substack{u,v \in A^* \\ uav=f}} \langle g \circ \mathbf{A}^*, u \rangle \langle \mathbf{A}^*, v \rangle \\ &= \sum_{\substack{u,v \in A^* \\ uav=f}} \langle g \circ \mathbf{A}^*, u \rangle = \sum_{\substack{u,v \in A^* \\ uav=f}} \binom{u}{g} = \binom{f}{ga},\end{aligned}$$

kus viimane võrdus kehtib tänu valemile (2.4). ■

3 Sõna Magnuse teisendusest

3.1 Mõned kombinatoorsed samasused

Teoreemist 2.3 võime saada täiendavaid samasusi, muuhulgas pöörata Pascali maatriksi. Nimelt kehtib järgmine

Lause 3.1. *Kõigi $f, g \in A^*$ jaoks kehtib*

$$\sum_{h \in A^*} (-1)^{|f|+|h|} \binom{f}{h} \binom{h}{g} = \delta_{f,g}.$$

Tõestus: Olgu π ringi $\mathbb{Z}\langle A^* \rangle$ endomorfism, mis on defineeritud järgmiselt:

$$\forall a \in A \qquad \pi(a) = a - 1$$

Seega, kui $a \in A$, siis $\pi(a) = -\mu(-a)$, ning teoreemist 2.3 ja sellest, et μ on homomorfism, järeldub, et

$$\pi(f) = (-1)^{|f|} \sum_{h \in A^*} (-1)^{|h|} \binom{f}{h} h.$$

Kuna $\forall a \in A$ jaoks $\mu(\pi(a)) = a = \pi(\mu(a))$, siis on π ja μ teineteise pöördteisendused. Seega

$$\begin{aligned} f = \mu(\pi(f)) &= (-1)^{|f|} \sum_{h \in A^*} (-1)^{|h|} \binom{f}{h} \mu(h) \\ &= (-1)^{|f|} \sum_{h \in A^*} (-1)^{|h|} \binom{f}{h} \left(\sum_{g \in A^*} \binom{h}{g} g \right) \\ &= (-1)^{|f|} \sum_{f,g \in A^*} (-1)^{|h|} \binom{f}{h} \binom{h}{g} g, \end{aligned}$$

millest saame

$$f = \sum_{g \in A^*} \left(\sum_{h \in A^*} (-1)^{|f|+|h|} \binom{f}{h} \binom{h}{g} \right) g$$

Siin on tegemist võrdusega formaalsete ridade vahel. Arvestades, et kaks formaalset rida on võrdsed parajasti siis, kui nende kordajad on võrdsed, saame soovitud võrduse. ■

Viimasest lausest järeldub, et Pascali maatriksi P pöördmaatriksiks on maatriks Q, mille read ja veerud on indekseeritud A^* elementidega ja milles positsioonil (f,h) seisab väärtus $\binom{f}{h}$. Tõepoolest, lause 3.1 väidab, et

$$\forall f,g \in A^* : \sum_{h\in A^*} [P]_{f,h}[Q]_{h,g} = \begin{cases} 1, & \text{kui } f = g \\ 0, & \text{kui } f \neq g \end{cases}$$

Kus $[M]_{i,j}$ tähistab maatriksi M positisioonil (i,j) asuvat elementi.
Kuna maatriksi pöördmaatriksi transponeeritud maatriks on selle maatriksi transponeeritud maatriksi pöördmaatriks, siis saame

Järeldus 3.2. *Kõigi $f,g \in A^*$ jaoks kehtib*

$$\sum_{h\in A^*} (-1)^{|g|+|h|} \binom{f}{h} \binom{h}{g} = \delta_{f,g}. \quad \blacksquare$$

Nendest seostest võime teha järgmise järelduse.

Järeldus 3.3. *Olgu s ja t funktsioonid $A^* \to \mathbb{R}$, olgu*

$$\forall f \in A^* \quad s(f) = \sum_{g\in A^*} (-1)^{|g|} \binom{f}{g} t(g),$$

siis

$$\forall g \in A^* \quad t(g) = \sum_{f\in A^*} (-1)^{|f|} \binom{g}{f} s(f).$$

Tõestus: Tõepoolest, olgu $g \in A^*$, siis

$$\sum_{f\in A^*} (-1)^{|f|} \binom{g}{f} s(f) = \sum_{f,h\in A^*} (-1)^{|f|+|h|} \binom{g}{f} \binom{f}{h} t(h)$$
$$= \sum_{h\in A^*} \delta_{g,h} t(h) = t(g) \quad \blacksquare$$

3.2 Vaba rühma Magnuse esitusest

Olgu A hulk, vaatame vaba monoidi $(A\dot{\cup}A^{-1})^*$, kus $A^{-1} = \{a^{-1} | \ a \in A\}$ (siin „a^{-1}“ on lihtsalt tähistus). Olgu $\equiv$ monoidi $(A\dot{\cup}A^{-1})^*$ kongruents, mis on defineeritud seostega

$$\forall a \in A \quad aa^{-1} \equiv \Lambda \text{ ja } a^{-1}a \equiv \Lambda.$$

Olgu $F(A) = (A\dot\cup A^{-1})^*/\equiv$. Ilmne on, et $F(A)$ on rühm. $F(A)$-d nimetatakse vabaks rühmaks moodustajate süsteemiga A.

Tuleb välja, et

Lause 3.4. *Magnuse teisendus $\mu : A^* \to \mathbb{Z}\langle A^*\rangle$ on laiendatav injektiivseks homomorfismiks $F(A) \to \mathbb{Z}\langle\langle A^*\rangle\rangle$.*

Tõestus: Meil tuleb kindlaks teha, millega võrdub $\mu(a^{-1})$, kus $a \in A$. Tuleb välja, et

$$\forall a \in A: \quad \mu(a^{-1}) = \sum_{n=0}^{\infty}(-1)^n a^n$$

Tõepoolest, sel juhul

$$\mu(a)\mu(a^{-1}) \;=\; (1 + a)\sum_{n=0}^{\infty}(-1)^n a^n \;=\; \sum_{n=0}^{\infty}(-1)^n a^n - \sum_{n=1}^{\infty}(-1)^n a^n \;=\; 1$$

Seega on μ laiendatav homomorfismiks $F(A) \to \mathbb{Z}\langle\langle A^*\rangle\rangle$. Näitame nüüd, et see homomorfism on injektiivne. Selleks piisab näidata, et $\operatorname{Ker}\mu = \{\Lambda\}$. Olgu $f \in F(A)$. Kui $f \neq \Lambda$, siis leiduvad sellised $k > 0$, $a_1, \ldots a_k \in A$, kus kõigi $i \in [1, k-1]$ jaoks kehtib $a_i \neq a_{i+1}$, samuti leiduvad sellised $\epsilon_1, \ldots, \epsilon_k \in \mathbb{Z}\backslash\{0\}$ nii, et

$$f = a_1^{\epsilon_1} a_2^{\epsilon_2} \ldots a_k^{\epsilon_k}$$

μ definitsiooni tõttu kehtib kõigi $i \in [1, k]$ jaoks

$$\mu(a_i^{\epsilon_i}) = 1 + \epsilon_i a_i + h_i,$$

kus h_i on rida kujul

$$h_i = \sum_{n=2}^{\infty} c_{i,n} a_i^n,\;\; c_{i,n} \in \mathbb{Z}.$$

Uurime nüüd, mis on $a_1 a_2 \ldots a_k$ kordajaks $\mu(f)$-s. Kuna

$$\mu(f) = (1 + \epsilon_1 a_1 + h_1)(1 + \epsilon_2 a_2 + h_2)\ldots(1 + \epsilon_k a_k + h_k)$$

ja $a_1 \neq a_2 \neq \ldots \neq a_k$, siis tuleb selleks, et saada monoomi $a_1 a_2 \ldots a_k$ valida igast sulust liige, mis ei ole 1. Seega oleme saanud

$$\langle \mu(f), a_1 a_2 \ldots a_k\rangle = \epsilon_1 \epsilon_2 \ldots \epsilon_k.$$

Kuna $\epsilon_1\epsilon_2\ldots\epsilon_k \neq 0$, siis $\mu(f) \neq 1$. ■

Olgu $u, v \in F(A)$. Elementi $[u, v] = u^{-1}v^{-1}uv$ nimetatakse u ja v *kommutaatoriks.* Kui G on rühm, siis G *alumine keskmine rida* $(G_n)_{n\in\mathbb{N}}$ on defineeritud järgmiselt:

$$G_1 = G, \text{ kui } n \leq 1, \text{ siis } G_{n+1} = [G_n, G],$$

kus $[U, V]$ $(U, V \leq G)$ on elementide $[u, v]$, kus $u \in U$ ja $v \in V$, genereeritud alamrühm.
Olgu (F_n) $F(A)$ alumine keskmine rida.
Rea $s \in \mathbb{Z}\langle\langle A^*\rangle\rangle$ *valuatsiooniks* (tähistame $\mathrm{val}(s)$) nimetatakse vähimat täisarvu n, mille korral s sisaldab nullist erineva kordajaga n-astme monoomi. Kokkuleppeliselt $\mathrm{val}(0) = +\infty$. Olgu

$$D_n = \{w \in F(A) | \ \mathrm{val}(\mu(w) - 1) \geq n\}, \text{ kus } n \geq 1.$$

Üsnagi ilmne on, et kehtib järgmine

Lause 3.5. *D_n on $F(A)$ alamrühm.*

Tõestus: Olgu $u, v \in D_n$. Siis

$$\mu(uv) - 1 = \mu(u)\mu(v) - 1 = (\mu(u) - 1)(\mu(v) - 1) + (\mu(u) - 1) + (\mu(v) - 1).$$

Selles summas on kõigi liidetavate valuatsioon n või suurem, seega $\mathrm{val}(\mu(uv) - 1) \geq n$ ja D_n on kinnine korrutamise suhtes. Ka saame, et

$$\begin{aligned}\mu(u^{-1}) - 1 = (\mu(u))^{-1} - 1 = (1 + (\mu(u) - 1))^{-1} - 1 \\ = \sum_{k=0}^{\infty}(-1)^k(\mu(u) - 1)^k - 1 = \sum_{k=1}^{\infty}(-1)^k(\mu(u) - 1)^k\end{aligned}$$

ja seega $\mathrm{val}(\mu(u^{-1}) - 1) \geq n$, s.t. D_n on kinnine pöördelemendi võtmise suhtes. ■

D_n definitsioonist järeldub, et kui $u, v \in F(A)$ ja $n \in \mathbb{N}$, siis $\mathrm{val}(\mu(u) - \mu(v)) \geq n$ parajasti siis kui $uv^{-1} \in D_n$. Tõepoolest, kui $\mathrm{val}(\mu(u) - \mu(v)) \geq n$, siis

$$n \leq \mathrm{val}(\mu(u) - \mu(v)) = \mathrm{val}((\mu(u) - \mu(v))\mu(v^{-1})) = \mathrm{val}(\mu(uv^{-1}) - 1)$$

ning paremast poolest vasaku järeldumist saab samamoodi näidata.
Näitame nüüd, et

Lause 3.6. *Kõigi $n \in \mathbb{N}$ jaoks kehtib $F_n \leq D_n$.*

Tõestus: Viime läbi induktsiooni n järgi. Kui $n = 1$, siis $D_1 = F = F_1$ ja seega $F_1 \leq D_1$. Olgu nüüd $F_k \leq D_k$, kõigi $k \leq n$ jaoks. Iga F_{n+1} element avaldub kujul $u^{-1}v^{-1}uv$, kus $u \in F_n$ ja $v \in F$. Siis

$$\begin{aligned}
&\mu(u^{-1}v^{-1}uv) - 1 = \mu(u^{-1})\mu(v^{-1})\mu(u)\mu(v) - 1 \\
&= (\mu(u^{-1}) - 1)\mu(v^{-1})(\mu(u) - 1)\mu(v) + \mu(v^{-1})(\mu(u) - 1)\mu(v) + \mu(u^{-1}) - 1.
\end{aligned}$$

Siin esimese liidetava valuatsioon on vähemalt $2n$, mis on vähemalt sama palju kui $n + 1$. Ülejäänu annab

$$\begin{aligned}
\mu(v^{-1})(\mu(u) - 1)\mu(v) + \mu(u^{-1}) - 1 = \mu(v^{-1})(\mu(u) - 1)\mu(v) - (\mu(u) - 1) \\
+ \sum_{n=2}^{\infty} (-1)^n (\mu(u) - 1)^n
\end{aligned}$$

eelmise tõestuse põhjal. Siin summamärgi all olevate avaldiste valuatsioonid on kõik vähemalt $2n$, mis on vähemalt sama palju kui $n+1$. Ülejäänu annab

$$\begin{aligned}
&\mu(v^{-1})(\mu(u) - 1)\mu(v) - (\mu(u) - 1) \\
&= \mu(v^{-1})(\mu(u) - 1)\mu(v) - (\mu(u) - 1)\mu(v) + (\mu(u) - 1)\mu(v) - (\mu(u) - 1) \\
&= (\mu(v^{-1}) - 1)(\mu(u) - 1)\mu(v) + (\mu(u) - 1)(\mu(v) - 1)
\end{aligned}$$

siin mõlema liidetava valuatsioon on vähemalt $n + 1$. ∎

Magnus, Karass ja Solitar näitavad [MKS]-s, et kehtib

Lause 3.7. *Kõigi $n \in \mathbb{N}$ korral $F_n = D_n$.* ∎

Seega kui $u, v \in F(A)$ ja $n \in \mathbb{N}$, siis $\mathrm{val}(\mu(u) - \mu(v)) \geq n$ parajasti siis kui $uv^{-1} \in F_n$.

Definitsioon 3.1. *Morse-Thue jadadeks* nimetatakse jadasid $(u_n)_{n\in\mathbb{N}}$ ja $(v_n)_{n\in\mathbb{N}}$ üle vaba monoidi $\{a, b\}^*$, mis on defineeritud järgmiselt:

$$\begin{aligned}
u_1 &= a, & v_1 &= b, \\
u_{n+1} &= u_n v_n, & v_{n+1} &= v_n u_n,
\end{aligned}$$

kui $n \geq 1$.

Neid jadasid iseloomustab, et

Lause 3.8. *Olgu $f \in \{a,b\}^*$ ja $n \in \mathbb{N}$. Kui $|f| < n$, siis $\binom{u_n}{f} = \binom{v_n}{f}$.*

Tõestus: Lause väide on samaväärne sellega, et

$$\sum_{\substack{f\in\{a,b\}^*\\|f|<n}} \left(\binom{u_n}{f} f - \binom{v_n}{f} f\right) = 0,$$

mis on omakorda samaväärne sellega, et $\mathrm{val}(\mu(u_n) - \mu(u_n)) \geq n$. Viimane väide on tõene parajasti siis kui $u_n v_n^{-1} \in F_n$, kus F_n on vaba rühma $F(\{a,b\})$ alumise keskmise jada n-s liige.
$u_1 v_1^{-1}$ kuulub triviaalselt F_1-e, sest F_1 võrdub terve vaba rühmaga. Oletame nüüd, et $u_n v_n^{-1} \in F_n$. Siis

$$u_{n+1}v_{n+1}^{-1} = u_n v_n u_n^{-1} v_n^{-1} = (u_n v_n^{-1}) v_n (v_n u_n^{-1}) v_n^{-1} \in F_{n+1}$$

alumise keskmise jada definitsiooni põhjal, sest $v_n u_n^{-1} = (u_n v_n^{-1})^{-1} \in F_n$ ja $v_n^{-1} \in F(\{a,b\})$. ■

Seejuures leidub iga n jaoks selline $f \in \{a,b\}^*$, et $|f| = n$ ja $\binom{u_n}{f} \neq \binom{v_n}{f}$. Et seda näidata, defineerime sõnade jadad $(\hat{a}_n)_{n\in\mathbb{N}}$ ja $(\hat{b}_n)_{n\in\mathbb{N}}$ järgmiselt:

$$\hat{a}_1 = a, \qquad \hat{a}_{n+1} = \begin{cases} \hat{a}_n a, & \text{kui } n \text{ on paaris} \\ \hat{a}_n b, & \text{kui } n \text{ on paaritu} \end{cases}$$

$$\hat{b}_1 = b, \qquad \hat{b}_{n+1} = \begin{cases} \hat{b}_n b, & \text{kui } n \text{ on paaris} \\ \hat{b}_n a, & \text{kui } n \text{ on paaritu} \end{cases}$$

Näitame nüüd induktsiooniga n järgi, et

$$\binom{u_n}{\hat{a}_n} > \binom{v_n}{\hat{a}_n} \text{ ja } \binom{u_n}{\hat{b}_n} < \binom{v_n}{\hat{b}_n}$$

Kui $n = 1$, siis $\binom{u_1}{\hat{a}_1} = \binom{v_1}{\hat{b}_1} = 1$ ja $\binom{u_1}{\hat{b}_1} = \binom{v_1}{\hat{a}_1} = 0$. Ka kehtib $\binom{u_2}{\hat{a}_2} = \binom{v_2}{\hat{b}_2} = 1$ ja $\binom{u_2}{\hat{b}_2} = \binom{v_2}{\hat{a}_2} = 0$.Kehtigu need võrratused nüüd mingi fikseeritud $n \geq 2$ korral. Siis järeldusest 2.4 saame, et $\binom{u_{n+1}}{\hat{a}_{n+1}} > \binom{v_{n+1}}{\hat{a}_{n+1}}$ parajasti siis kui

$$\sum_{\substack{f,g\in\{a,b\}^*\\fg=\hat{a}_{n+1}}} \binom{u_n}{f}\binom{v_n}{g} > \sum_{\substack{f,g\in\{a,b\}^*\\fg=\hat{a}_{n+1}}} \binom{v_n}{f}\binom{u_n}{g}, \tag{3.1}$$

Viimase lause põhjal kui $|f| < n$ ja $|g| < n$, siis $\binom{u_n}{f}\binom{v_n}{g} = \binom{v_n}{f}\binom{u_n}{g}$, seega on (3.1)-ga samaväärne

$$\binom{u_n}{\hat{a}_{n+1}}\binom{v_n}{\Lambda} + \binom{u_n}{\hat{a}_n}\binom{v_n}{x} + \binom{u_n}{a}\binom{v_n}{\hat{b}_n} + \binom{u_n}{\Lambda}\binom{v_n}{\hat{a}_{n+1}} > \binom{v_n}{\hat{a}_{n+1}}\binom{u_n}{\Lambda} + \binom{v_n}{\hat{a}_n}\binom{u_n}{x} + \binom{v_n}{a}\binom{u_n}{\hat{b}_n} + \binom{v_n}{\Lambda}\binom{u_n}{\hat{a}_{n+1}},$$

kus x on $\hat{a}_{n+1}$ viimane täht. Koondades siit sarnased liikmed ja arvestades, et $\binom{u_n}{a} = \binom{u_n}{x} = \binom{v_n}{a} = \binom{v_n}{x}$ (sest $n \geq 2$), saame samaväärse võrratuse

$$\binom{u_n}{\hat{a}_n} + \binom{v_n}{\hat{b}_n} > \binom{v_n}{\hat{a}_n} + \binom{u_n}{\hat{b}_n},$$

mis on induktsiooni eelduse järgi tõene. Samamoodi saab näidata, et $\binom{v_{n+1}}{\hat{b}_{n+1}} > \binom{u_{n+1}}{\hat{b}_{n+1}}$.

4 Ridade Hadamardi ja infiltratsioonikorrutisest

Uute binoomkordajaid siduvate samasuste saamiseks osutub kasulikuks defineerida uus korrutis $\mathbb{Z}\langle\langle A^*\rangle\rangle$-l, nimelt

Definitsioon 4.1. *Infiltratsioonikorrutiseks* nimetatakse binaarset operatsiooni (aditiivsel rühmal) $\mathbb{Z}\langle\langle A^*\rangle\rangle$, mida tähistame $\uparrow$-ga ja mis määratakse induktiivselt seostest

- $$\forall f \in A^* \quad f \uparrow \Lambda = \Lambda \uparrow f = f \tag{4.1}$$

- $$\forall f, g \in A^*, \forall a, b \in A \quad fa \uparrow gb = (f \uparrow gb)a + (fa \uparrow g)b + \delta_{a,b}(f \uparrow g)a \tag{4.2}$$

- $$\forall s, t \in \mathbb{Z}\langle\langle A^*\rangle\rangle \quad s \uparrow t = \sum_{f,g \in A^*} \langle s, f\rangle\langle t, g\rangle(f \uparrow g) \tag{4.3}$$

Analoogiliselt segamiskorrutisega on ka kahe rea infiltratsioonikorrutis hästi defineeritud, hoolimata lõpmatust summast. Samuti on võimalik infiltratsiooni intuitiivselt kirjeldada — sõna h kordaja korrutises $f \uparrow g$ on selliste h alamjärjendite paaride arv, mis: esiteks on nende ühend võrdne terve järjendiga h; ja teiseks on esimene neist võrdne f-ga ja teine g-ga.

Näide 4.1.

$$
\begin{aligned}
ab \uparrow ab &= ab + 2aab + 2abb + 4aabb + 2abab \\
ab \uparrow ba &= aba + bab + 2abba + 2baab + baba
\end{aligned}
$$

Lause 4.1. *Infiltratsioonikorrutis on kommutatiivne ja assiotsiatiivne.*

Tõestus: Nii nagu segamiskorrutise puhulgi, näitame infiltratsiooni kommutatiivsust ja assiotsiatiivsust kõigepealt A^* elementide jaoks. Seejärel saame valemist (4.3) nende omaduste kehtivuse terve $\mathbb{Z}\langle\langle A* \rangle\rangle$ jaoks. Kommutatiivsus on ilmne seosest (4.2), kui arvestada, et $\delta_{a,b}a = delta_{a,b}b$. Uurime assiotsiatiivsust. Olgu $f, g, h \in A^*$. Kui mõni nendest sõnadest on tühi, siis on valemist (4.1) ilmne, et $(f \uparrow g) \uparrow h = f \uparrow (g \uparrow h)$. Seega olgu $a, b, c \in A$, siis on

$$
\begin{aligned}
(fa \uparrow gb) \uparrow hc &= ((f \uparrow gb)a) \uparrow hc + (fa \uparrow g)b) \uparrow hc + \delta_{a,b}((f \uparrow g)a) \uparrow hc \\
&= ((f \uparrow gb) \uparrow hc)a + (((f \uparrow gb)a) \uparrow h)c + \delta_{a,c}((f \uparrow gb) \uparrow h)a \\
&\quad + ((fa \uparrow g) \uparrow hc)b + (((fa \uparrow g)b) \uparrow h)c + \delta_{b,c}((fa \uparrow g) \uparrow h)b \\
&\quad + \delta_{a,b}\big[((f \uparrow g) \uparrow hc)a + (((f \uparrow g)a) \uparrow h)c + \delta_{a,c}((f \uparrow g) \uparrow h)a\big] \\
&= ((f \uparrow gb) \uparrow hc)a + ((fa \uparrow g) \uparrow hc)b \\
&\quad + \big[(((f \uparrow gb)a) \uparrow h)c + (((fa \uparrow g)b) \uparrow h)c + \delta_{a,b}(((f \uparrow g)a) \uparrow h)c\big] \\
&\quad + \delta_{a,c}((f \uparrow gb) \uparrow h)a + \delta_{b,c}((fa \uparrow g) \uparrow h)b \\
&\quad + \delta_{a,b}((f \uparrow g) \uparrow hc)a \\
&\quad + \delta_{a,b}\delta_{b,c}((f \uparrow g) \uparrow h)a
\end{aligned}
$$

arvestades nüüd, et

- kandilistes sulgudes olev avaldis on võrdne $((fa \uparrow gb) \uparrow h)c$-ga
- $\delta_{x,y}x = \delta_{x,y}y$, kus $x, y \in \{a, b, c\}$
- $\delta_{a,b}\delta_{b,c} = \delta_{a,b}\delta_{b,c}\delta_{c,a}$

- sulgudes olevatele avaldistele võib rakendada induktsiooni eeldust (eeldame, et kui $|f'|+|g'|+|h'| < |fa|+|gb|+|hc|$, kus $f',g',h' \in A^*$, siis $(f' \uparrow g') \uparrow h' = f' \uparrow (g' \uparrow h')$

saame, et oleme $(fa \uparrow gb) \uparrow hc$ avaldanud kujul, mis on sümmeetriline f,g ja h suhtes, nii nagu ka a,b ja c suhtes. ■

Kuna (4.3) tagab liitmise distributiivsuse infiltratsiooni suhtes, siis on $(\mathbb{Z}\langle\langle A^*\rangle\rangle, +, \uparrow)$ kommutatiivne (ühikuga) ring.
Kui $s \in \mathbb{Z}\langle A^*\rangle$, siis $\deg s$ tähistab s astet. Esimese kirjelduse infiltratsioonile annab järgmine

Lemma 4.2. *Olgu $f,g \in A^*$. Siis $\deg(f \uparrow g) = |f|+|g|$. Täpsemalt võib $f \uparrow g$ üles kirjutada kujul*

$$f \uparrow g = P'(f,g) + f \circ g \text{ kus } \deg P'(f,g) < |f|+|g| \tag{4.4}$$

Kui $|f| \geq |g|$, siis kehtib ka

$$f \uparrow g = \binom{f}{g} f + P''(f,g) \text{ kus } |f| < \mathrm{val}(P''(f,g)) \tag{4.5}$$

Tõestus: Valem (4.4) on tõestatav induktsiooniga üle $|f|+|g|$. Tõepoolest, kui $f=\Lambda$ või $g=\Lambda$, siis $f \uparrow g = f \circ g$. Viime nüüd läbi induktsioonisammu. Olgu $a,b \in A$. Siis

$$\begin{aligned} fa \uparrow gb = (f \uparrow gb)a + (fa \uparrow g)b + \delta_{a,b}(f \uparrow g)a = \\ (f \circ gb)a + P'(f,gb)a + (fa \circ g)b + P'(fa,g)b + \delta_{a,b}(f \uparrow g)a = \\ fa \circ gb + P'(fa,gb), \end{aligned}$$

kus

$$P'(fa,gb) = aP'(f,gb) + bP'(fa,g) + \delta_{a,b}(f \uparrow g)a$$

Rakendades siin induktsiooni eeldust $P'(f,gb)$ ja $P'(fa,g)$ jaoks ja arvestades, et induktsiooni eelduse järgi $f \uparrow g$ on $|f|+|g|$ astme polünoom, saame et $\deg P'(fa,gb) < |fa|+|gb|$.
Samamoodi võime tõestada ka (4.5). Kui $g=\Lambda$, siis (4.5) ilmselt kehtib iga $f \in A^*$ korral. Olgu nüüd $a,b \in A$. Siis

$$fa \uparrow gb = (f \uparrow gb)a + (fa \uparrow g)b + \delta_{a,b}(f \uparrow g)a.$$

Esimene juhtum. $|f| \geq |gb|$. Induktsiooni eelduse kohaselt siis

$$\begin{aligned} fa \uparrow gb = &\left(\binom{f}{gb} f + P''(f, gb)\right) a + \left(\binom{fa}{g} fa + P''(fa, g)\right) b \\ &+ \delta_{a,b} \left(\binom{f}{g} f + P''(f, g)\right) a \\ &= \left(\binom{f}{gb} + \delta_{a,b}\binom{f}{g}\right) fa + P''(fa, gb), \end{aligned}$$

kus

$$P''(fa, gb) = aP''(f, gb) + bP''(fa, g) + \delta_{a,b} aP''(f, g) + \binom{fa}{g} fab.$$

Seega induktsiooni eelduse kohaselt $\mathrm{val}(P''(fa, gb)) > |fa|$ ja valemi (2.3) tõttu on fa kordaja $fa \uparrow gb$-s $\binom{fa}{gb}$.
Teine juhtum. $|f| < |g|$. Siis $|f| = |g|$ ja

$$\begin{aligned} fa \uparrow gb = &\left(\binom{gb}{f} gb + P''(gb, f)\right) a + \left(\binom{fa}{g} fa + P''(fa, g)\right) b \\ &+ \delta_{a,b} \left(\binom{f}{g} f + P''(f, g)\right) a \\ &= \delta_{a,b}\binom{f}{g} fa + P''(fa, gb), \end{aligned}$$

kus

$$P''(fa, gb) = aP''(gb, a) + bP''(fa, g) + \delta_{a,b} aP''(f, g) + \binom{gb}{f} gba + \binom{fa}{g} fab.$$

Induktsiooni eelduse kohaselt siin $val(P''(fa, gb)) > |fa|$. Uurime, mis on fa kordaja $fa \uparrow gb$-s. Kui $f = g$ ja $a = b$, siis $\delta_{a,b}\binom{f}{g} = 1 = \binom{fa}{gb}$. Ka vastupidisel juhul $\delta_{a,b}\binom{f}{g} = 0 = \binom{fa}{gb}$. ■

Järeldus 4.3.

$$\forall f, g \in A^* \quad \langle f \uparrow g, f\rangle = \binom{f}{g} \tag{4.6}$$

Selleks, et formuleerida järgmist teoreemi, on vajalik järgmine

Definitsioon 4.2. Ridade $s, t \in \mathbb{Z}\langle\langle A^*\rangle\rangle$ *Hadamardi korrutiseks* nimetatakse rida

$$s \odot t = \sum_{f \in A^*} \langle s, f\rangle\langle t, f\rangle f$$

Hadamardi korrutist võib vaadelda hulkade ühisosa üldistusena (s.t. kordsusega hulkade), näiteks kahe hulga karakteristlike ridade Hadamardi korrutis on nende hulkade ühisosa karakteristlik rida.

Teoreem 4.4. *Kõigi $f, g \in A^*$ jaoks kehtib*

$$(f \circ \mathbf{A}^*) \odot (g \circ \mathbf{A}^*) = (f \uparrow g) \circ \mathbf{A}^* \tag{4.7}$$

Tõestus: Valemist (4.3) saame, et kui $f, g, h \in A^*$, siis

$$(f \uparrow g) \uparrow h = \sum_{w,v \in A^*} \langle f \uparrow g, w\rangle \delta_{h,v}(w \uparrow v) = \sum_{w \in A^*} \langle f \uparrow g, w\rangle (w \uparrow h)$$

ja

$$f \uparrow (g \uparrow h) = \sum_{w,v \in A^*} \delta_{f,w}\langle g \uparrow h, v\rangle (w \uparrow v) = \sum_{v \in A^*} \langle g \uparrow h, v\rangle (f \uparrow v),$$

millest saame

$$\forall f, g, h, u \in A^* : \ \langle (f \uparrow g) \uparrow h, u\rangle = \sum_{w \in A^*} \langle f \uparrow g, w\rangle\langle w \uparrow h, u\rangle \tag{4.8}$$

ja

$$\forall f, g, h, u \in A^* : \ \langle f \uparrow (g \uparrow h), u\rangle = \sum_{v \in A^*} \langle g \uparrow h, v\rangle\langle f \uparrow v, u\rangle. \tag{4.9}$$

Võttes (4.8)-s $u = h$ ja kasutades valemit (4.6) saame

$$\forall f, g, h \in A^* : \ \langle (f \uparrow g) \uparrow h, h\rangle = \sum_{w \in A^*} \langle f \uparrow g, w\rangle \binom{h}{w}$$

Võtame ka (4.9)-s $u = h$ ja paneme seejärel tähele, et kõigi f, g, h, v korral $\langle g \uparrow h, v\rangle\langle f \uparrow v, h\rangle = 0$, kui $v \neq h$ (lemmast 4.2 järeldub, et kui $|v| < |h|$ või $|v| = |h|$, kuid $v \neq h$, siis $\langle g \uparrow h, v\rangle = 0$; samasugune mõttekäik on läbi viidav teise teguri suhtes). Seega saame (kasutame taas valemit (4.6))

$$\forall f, g, h \in A^* : \ \langle f \uparrow (g \uparrow h), h\rangle = \binom{h}{g}\binom{h}{f}$$

Nüüd saame kõigi $f, g, h \in A^*$ jaoks välja kirjutada

$$\begin{aligned}\langle (f \uparrow g) \circ \mathbf{A}^*, h\rangle &= \sum_{w \in A^*} \langle f \uparrow g, w\rangle \langle w \circ \mathbf{A}^*, h\rangle \\ &= \sum_{w \in A^*} \langle f \uparrow g, w\rangle \binom{h}{w} = \langle (f \uparrow g) \uparrow h, h\rangle = \langle f \uparrow (g \uparrow h), h\rangle \\ &= \binom{h}{f}\binom{h}{g} = \langle f \circ \mathbf{A}^*, h\rangle \langle g \circ \mathbf{A}^*\rangle = \langle (f \circ \mathbf{A}^*) \odot (g \circ \mathbf{A}^*), h\rangle\end{aligned}$$

ja teoreem on tõestatud. ■

Viimase teoreemi ja järelduse 3.3 abil saame otseselt välja kirjutada monoomide kordajad kahe sõna infiltratsioonikorrutises. Tõepoolest, olgu $f, g, h \in A^*$, siis on

$$\langle (f \uparrow g) \circ \mathbf{A}^*, h\rangle = \sum_{w \in A^*} (-1)^{|w|} \binom{h}{w} (-1)^{|w|} \langle f \uparrow g, w\rangle$$

Siit saame järelduse 3.3 abil, et

$$\begin{aligned}\langle f \uparrow g, h\rangle &= (-1)^{|h|} \sum_{w \in A^*} (-1)^{|w|} \binom{h}{w} \langle (f \uparrow g) \circ \mathbf{A}^*, w\rangle \\ &= (-1)^{|h|} \sum_{w \in A^*} (-1)^{|w|} \binom{h}{w} \langle (f \circ \mathbf{A}^*) \odot (g \circ \mathbf{A}^*), w\rangle,\end{aligned}$$

millest saame

Järeldus 4.5. *Kõigi $f, g, h \in A^*$ jaoks kehtib*

$$\langle f \uparrow g, h\rangle = \sum_{w \in A^*} (-1)^{|h|+|w|} \binom{h}{w} \binom{w}{f} \binom{w}{g} \quad ■$$

Resume

In this paper we come to the notion of binomial coefficients of words by defining the word as a finite sequence of letters and the subword of a word as its sub-sequence. If f and g are words, then the binomial coefficient of f and g is defined as the number of ways one can choose a sub-sequence of f that

equals g. This terminology is justified by the fact, that in case of one-letter alphabet (let the letter be denoted by a) there are $\binom{m}{n}$ sub-sequences of a^m that equal a^n.

The rest of the paper is devoted to exploring the identities between those binomial coefficients. The first formula that we derive, is an analogue to Pascal's formula. This formula and the formulas $\binom{f}{\Lambda} = 1$ and $\binom{\Lambda}{f} = 0$, where f is any word (any nonempty word in the latter case) and Λ denotes empty word, allow us to compute $\binom{f}{g}$ for any words f and g.

Next we define a homomorphism, called Magnus transformation, from the monoid of words A^* to $\mathbb{Z}\langle A^*\rangle$, the algebra of polynomials of noncommuting variables in A with coefficients in $\mathbb{Z}$. We extend this mapping to algebra endomorphism of $\mathbb{Z}\langle A^*\rangle$. We note that the coefficients of the polynomials obtained as the maps of words under this transformation are indeed binomial coefficients, and this fact together with the fact, that the Magnus transformation is a homomorphism, allows us to get new identities.

We also define several binary operations on the algebra of formal power series of noncommuting variables in A with coefficients in $\mathbb{Z}$, that can be intuitively described with the help of the idea of shuffling objects. We define shuffle product and infiltration product and see that the additive group of formal power series, equipped with any of these, becomes a commutative and associative algebra. The coefficients of the shuffle of a word with the characteristic series of A^* turn outto be binomial coefficients again, and after proving a theorem that binds both products and also the Hadamard product, we obtain an explicit formula for the coefficients of an infiltration product by means of binomial coefficients.

Viited

[Lot] Lothaire. Combinatorics on Words. Encyclopedia of Mathematics, Vol 17, Addison-Wesley, 1983

[MKS] Wilhelm Magnus, Abraham Karass, Donald Solitar. Combinatorial Group Theory. Presentations of Groups in Terms of Generators and Relations. Interscience publishers, 1966