Tartu Ülikool
Matemaatikateaduskond
Arvutiteaduse Instituut

Osaliselt tsüklilise monoidi Möbiuse funktsioonist

bakalaureusetöö

Peeter Laud
juhendaja Uno Kaljulaid

Tartu, 1997

Sisukord

Sissejuhatus

Selles töös me püüame heita valgust *osaliselt tsüklilise monoidi* ehitusele ja eriti tema Möbiuse funktsioonile. Kui X on tähestik ja F *tsükliline* ternaarne seos X-l, siis X^* faktormonoidi kongruentsiga, mille genereerivad võrdused $abc = bca = cab$, kus $(a, b, c) \in F$, nimetame (F tekitatud) tsükliliseks monoidiks (üle X).

Vahendina osaliselt tsüklilise monoidi Möbiuse funktsiooni kirjeldamiseks kasutame me *naabrustähestikku*. See mõiste on pärit [Fed]-st, kus näidatakse tema kasutusvõimalusi mitmete probleemide uurimisel, kaasa arvatud *osaliselt kommutatiivse monoidi* Möbiuse funktsiooni leidmisel. Resultaat, mida ta kasutab, on käesolevas töös ära toodud lausena 2.1. Naabrustähestik, mida ta kasutab, kirjeldab sõnade kahetähelisi alamsõnu.

Me tuletame järgnevas lause 2.1 analoogi kolmetäheliste alamsõnade jaoks. Seejärel näeme, et kui tsükliline seos F on täielik, s.t. $F = X^3$, siis me suudame kirjeldada osaliselt tsüklilise monoidi Riemanni funktsiooni kui teatava formaalse rea $\mathbb{Z}\langle\langle X^* \rangle\rangle$-st loomulikku projektsiooni formaalsete ridade ringi üle osaliselt tsüklilise monoidi. Seejuures see formaalne rida on saadav kolme formaalse rea summana, mis kõik on defineeritavad „naabruste“ kaudu. Neid kolme rida suudame me pöörata, kuid vastuseta jääb küsimus, milline on nende kolme rea summa pöördväärtus ja selle projektsioon formaalsete ridade ringi üle osaliselt tsüklilise monoidi.

Me suudame anda osaliselt tsüklilise monoidi Möbiuse funktsioonile samasuguse kirjelduse ka juhul, kui vastav F on *sümmeetriline* ja *transitiivne* (see nõue on nõrgem kui täielikkuse nõudmine). Nimelt tuleb välja, et selline osaliselt tsükliline monoid sisaldab alammonoide, mis on saadud vaba monoidi täieliku tsüklilise seose tekitatud kongruentsiga faktoriseerides. Kasutades mõnda [Lal]-s toodud üsnagi elementaarset tulemust saame kirjelduse sellise osaliselt tsüklilise monoidi Möbiuse funktsioonile.

1 Põhimõisted

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

Sõna $f = x_1x_2\dots x_n$ pikkuseks nimetame tähtede arvu f-s (tähistame $|f|$). Sõnade $f = x_1x_2\dots x_n$ ja $g = y_1y_2\dots y_m$ korrutiseks nimetame sõna $f \cdot g = x_1x_2\dots x_ny_1y_2\dots y_m$. Ilmne on, et selliselt defineeritud korrutamine on assiotsiatiivne ja selle suhtes on olemas ühikelement — sõna pikkusega 0 (edaspidi tähistame seda sõna Λ-ga). Seega $(X^*, \cdot)$ on monoid. Monoidi $(X^*, \cdot)$ nimetatakse vabaks monoidiks baasiga X.
Kui tähistame $X^+ = X^* \backslash \{\Lambda\}$, siis $(X^+, \cdot)$ on poolrühm, mida nimetatakse vabaks poolrühmaks baasiga X.

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

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

ja korrutiseks rida

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

Hulk $R\langle\langle X^*\rangle\rangle$ koos niiviisi defineeritud summa ja korrutisega on (ühikuga) ring.
Formaalseid ridu ei pea tingimata vaatlema üle vaba monoidi. Tõepoolest, kui vaatame funktsioone lihtsalt mingist monoidist mingisse ringi, siis saame nende funktsioonide summa defineerida samamoodi kui seda ülalpool tehtud on. Korrutamise defineerimisega tekib raskusi, sest suvalise monoidi korral ei pruugi liidetavate arv sisemises summas lõplik olla. Kirjeldamaks teatavat monoidide klassi, mille jaoks on võimalik sellisel viisil formaalsete ridade ringi defineerida, defineerime järgmised mõisted:

Definitsioon 1.1. Olgu M monoid, olgu $x \in M$. Elemendi x *dekompositsiooniks* nimetatakse järjendit $y_1, y_2, \dots, y_m$, kus $m \geqslant 0$, $y_i \in M\backslash\{1\}$, kus 1 tähistab M ühikelementi, nii, et $x = y_1y_2\cdots y_m$.

Definitsioon 1.2. Monoid M on *lõplike dekompositsioonidega*, kui tema iga elemendi dekompositsioonide arv on lõplik.
Märkus: Vabas monoidis on tühjal sõnal üks dekompositsioon — null elemendiga.

Kui M on lõplike dekompositsioonidega monoid ja R on ühikuga ring, siis saame defineerida formaalsete ridade ringi üle M-i, sest nüüd on sel viisil defineeritud korrutamine hästi defineeritud.

Definitsioon 1.3. Monoidi M *Riemanni funktsiooniks* nimetatakse formaalset rida γ ringist $\mathbb{Z}\langle\langle M\rangle\rangle$, mille korral

$$\forall x \in M : \quad \langle \gamma, x \rangle = 1.$$

Monoidi M *Möbiuse funktsiooniks* nimetatakse formaalset rida μ ringist $\mathbb{Z}\langle\langle M\rangle\rangle$, mille korral

$$\gamma\mu = 1 \text{ ja } \mu\gamma = 1.$$

Märkus: Möbiuse funktsioon on alati olemas — saab näidata, et kui formaalne rida on üle lõplike dekompositsioonidega monoidi, siis on ta pööratav parajasti siis, kui tema vabaliikme kordaja (s.t. monoidi ühikelemendi kordaja) on kordajate ringis pööratav.

2 Osaliselt kommutatiivsest monoidist

Enne tsüklilise monoidi defineerimist ja uurimist heidame pilgu sellele, kuidas töötab meie kasutatav tehnika osaliselt kommutatiivse monoidi korral.

Definitsioon 2.1. Olgu X tähestik, olgu θ irrefleksiivne sümmeetriline binaarne seos hulgal X. Olgu $\equiv_\theta$ monoidi X^* kongruents, mis genereeritakse seostega

$$\forall (a,b) \in \theta : \quad ab \equiv_\theta ba.$$

Faktormonoidi $M(X,\theta) = X^*/\equiv_\theta$ nimetatakse θ tekitatud *osaliselt kommutatiivseks monoidiks* üle tähestiku X. Sõna $w \in X^*$ kongruentsiklassi $\hat{w}$ nimetatakse *w jäljeks.*

Definitsioon 2.2. Olgu X tähestik. Talle vastavaks *naabrustähestikuks* nimetame hulka

$$A = \{a_{xy} \mid (x,y) \in X^2\}.$$

Vaatame formaalsete ridade ringi $\mathbb{Z}[A]\langle\langle X^*\rangle\rangle$ (siin $\mathbb{Z}[A]$ tähistab kommutatiivsete polünoomide ringi muutujatega hulgast A ja täisarvuliste kordajatega). Selles ringis defineerime:

Definitsioon 2.3. Sõna $w = x_1x_2\cdots x_n \in X^*$ *naabrusmonoomiks* nimetatakse monoomi

$$a(w) = \begin{cases} a_{x_1x_2}a_{x_2x_3}\cdots a_{x_{n-1}x_n} & \text{kui } n \geqslant 2 \\ 1 & \text{kui } n < 2 \end{cases}$$

ja *sõelpolünoomiks* nimetatakse polünoomi

$$\bar{a}(w) = \begin{cases} (a_{x_1x_2}-1)(a_{x_2x_3}-1)\cdots(a_{x_{n-1}x_n}-1) & \text{kui } n \geqslant 2 \\ 1 & \text{kui } n = 1 \\ 0 & \text{kui } n = 0 \end{cases}$$

Lause 2.1. *Kehtib järgmine võrdus ([Fed]):*

$$\sum_{w\in X^*} a(w)w = \left(1 - \sum_{w\in X^*} \bar{a}(w)w\right)^{-1}. \blacksquare$$

Olgu X ja θ sellised nagu osaliselt kommutatiivse monoidi definitsioonis. *Orientatsiooniks* θ-l nimetatakse tema alamhulka $\vec{\theta}$, mille korral θ on $\vec{\theta}$ ja $\{(x,y)|(y,x) \in \vec{\theta}\}$ lõikumatu ühend. (S.t. kui (x,y) ja (y,x) on sümmeetrilise seose θ elemendid, siis nendest täpselt üks kuulub $\vec{\theta}$-sse)

Kui me võrduses, mille kehtivust väidab lause 2.1, väärtustame muutujad $a_{xy} \in A$, siis saame mingi samasuse $\mathbb{Z}\langle\langle X^* \rangle\rangle$ elementide vahel. Sobiva väärtustuse defineerimiseks on vajalikud veel mõned tähistused.

Ütleme, et sõnal $w = x_1x_2 \cdots x_n \in X^*$ on positsioonil k *$\vec{\theta}$-naabrus*, kui $x_k\vec{\theta}x_{k+1}$. Sõna w $\vec{\theta}$-naabruste arvu tähistame $\vec{\theta}\mathrm{adj}\ w$.

Olgu $T(X,\vec{\theta})$ selliste sõnade $t_1t_2 \cdots t_n \in X^*$ hulk, mille korral $t_1\vec{\theta}t_2\vec{\theta}\cdots\vec{\theta}t_n$.

Väärtustame nüüd A elemendid. Olgu

$$a_{xy} = \begin{cases} a & \text{kui } x\vec{\theta}y \\ 1 & \text{muidu} \end{cases}$$

kus $a \in \mathbb{Z}$ on muutuja. Siis saame lausest 2.1, et

$$\sum_{w \in X^*} a^{\vec{\theta}\mathrm{adj}\ w} w = \left(1 - \sum_{t \in T(X,\vec{\theta})} (a-1)^{|t|} t \right)^{-1}.$$

Kui $\vec{\theta}$ on transitiivne (suvalisel irrefleksiivsel sümmeetrilisel binaarsel seosel ei pruugi transitiivset orientatsiooni olla), siis võttes $a = 0$ saame viimase võrduse vasakule poolele sellise formaalse rea, et iga jälje $\hat{w} \in M(X,\theta)$ korral on seal $\hat{w}$ ühe esindaja kordajaks 1 ja ülejäänud esindajate kordajaks 0 ([Fed]). Teisisõnu, kui π on loomulik projektsioon $X^* \to M(X,\theta)$ (see on laiendatav ringide homomorfismiks $\mathbb{Z}\langle\langle X^* \rangle\rangle \to \mathbb{Z}\langle\langle M(X,\theta) \rangle\rangle$), siis π rakendatuna viimase võrduse vasakule poolele annab meile $M(X,\theta)$ Riemanni funktsiooni. See aga tähendab, et kui rakendame π-d võrduse paremale poolele, siis võime sealt välja lugeda $M(X,\theta)$ Möbiuse funktsiooni.
Märkus: [Lal]-s näidatakse, milline on osaliselt kommutatiivse monoidi Möbiuse funktsioon üldjuhul.

3 Osaliselt tsüklilisest monoidist

3.1 Mõisted

Definitsioon 3.1. *Ternaarseks seoseks* hulgal X nimetatakse hulga X^3 mingit alamhulka F.

Definitsioon 3.2. Ternaarset seost F nimetatakse *tsükliliseks seoseks*, kui $\forall a, b, c \in X$ korral sellest, et $(a, b, c) \in F$, järeldub $(b, c, a) \in F$.
Märkus: ... ja sel juhul ka $(c, a, b) \in F$.

Definitsioon 3.3. Olgu F tsükliline (ternaarne) seos hulgal X. Olgu $\equiv_F$ monoidi X^* kongruents, mille genereerivad võrdused $abc = bca$, kus $(a, b, c) \in F$. Olgu $C(X, F) = X^*/\equiv_F$. Monoidi $C(X, F)$ nimetame F poolt tekitatud *tsükliliseks monoidiks*.
Edaspidi me uurime tsükliliste seoste poolt tekitatud tsüklilisi monoide. Kuna tekitatav monoid ei muutu, kui lisame või eemaldame seosest elemente kujul (x, x, x), kus $x \in X$, siis loeme edaspidi, et kõik sellisel kujul olevad elemendid kuuluvad seosesse.

Lause 3.1. *$C(X, F)$ on lõplike dekompositsioonidega.*

Tõestus: Me võime defineerida $\hat{w} \in C(X, F)$ jaoks $\hat{w}$ *pikkuse* — olgu $|\hat{w}| = |w|$, kus w on $\hat{w}$ suvaline esindaja. See definitsioon on ilmselt korrektne — $\equiv_F$ definitsiooni järgi kui $w_1 \equiv_F w_2$, siis $|w_1| = |w_2|$.
Kuna hulk $\{\hat{w} \in C(X, F) | \; |\hat{w}| < l\}$, kus l on mingi naturaalarv või 0, on lõplik ning kuna $\hat{w}$ dekompositsiooniks olevates järjendites on kõigi elementide pikkused väiksemad kui $|\hat{w}|$ ja suuremad kui 0, siis peab $\bar{w}$-l kõigest lõplik arv dekompositsioone olema.
Märkus: [Lal]-s näidatakse, et osaliselt kommutatiivne monoid on lõplike dekompositsioonidega.

Edaspidi me seame tsüklilisele seosele veel teatavaid kitsendusi, siinkohal toome ära veel paar definitsiooni:

Definitsioon 3.4. Tsüklilist seost nimetatakse *sümmeetriliseks*, kui $\forall a, b, c \in X$ korral sellest, et $(a, b, c) \in F$, järeldub $(b, a, c) \in F$.
Märkus: Juhul kui F on tsükliline sümmeetriline seos, siis järeldub mingi kolmiku (a, b, c) kuulumisest F-i selle kolmiku kõikvõimalike permutatsioonide kuulumine F-i. Seega võib tsüklilise sümmeetrilise seose elemente vaadelda järjestamata kolmikutena $\{a, b, c\}$.

Definitsioon 3.5. Tsüklilist seost nimetatakse *transitiivseks*, kui $\forall a, b, c, d \in X$ korral sellest, et $(a, b, c) \in F$ ja $(c, d, a) \in F$, järeldub $(b, c, d) \in F$.
Märkus: ... ja siis ka $(d, a, b) \in F$

3.2 Sõnade genereerimine kolmetäheliste naabruste järgi

Siin tõestame me lause 2.1 analoogi kolmetäheliste naabruste jaoks. Selle formuleeerimiseks on mõistlik ümber defineerida naabrustähestik (ja ühes sellega naabrusmonoom ja sõelpolünoom). Seega olgu:

Definitsioon 3.6. Tähestiku X *naabrustähestikuks* nimetatakse hulka $A = \{a_{xyz} \mid (x, y, z) \in X^3\}$.

Definitsioon 3.7. Sõna $w \in X^*$, $w = x_1 x_2 \cdots x_n$, *naabrusmonoomiks* nimetatakse monoomi

$$a(w) = \begin{cases} a_{x_1x_2x_3} a_{x_2x_3x_4} \cdots a_{x_{n-2}x_{n-1}x_n} & \text{kui } n \geqslant 3 \\ 1 & \text{kui } n < 3 \end{cases}$$

ja *sõelpolünoomiks* polünoomi

$$\bar{a}(w) = \begin{cases} 0 & \text{kui } |w| = 0 \\ 1 & \text{kui } |w| = 1 \\ 0 & \text{kui } |w| = 2 \\ \big(\bar{a}(x_1x_2 \cdots x_{n-1}) + \bar{a}(x_1x_2 \cdots x_{n-2})\big) \cdot (a_{x_{n-2}x_{n-1}x_n} - 1) & \text{kui } |w| \geqslant 3 \end{cases}$$

Sellisel juhul kehtib:

Teoreem 3.2. *Naabruste järgi genereeritakse X^* sõnad järgmiselt:*

$$\sum_{w \in X^*} a(w)w = \left(1 - \sum_{w \in X^*} \bar{a}(w)w\right)^{-1}$$

Tõestus: Korrutades selle võrduse mõlemaid pooli $(1 - \sum_{w \in X^*} \bar{a}(w)w)$-ga saame, et tõestatav võrdus on samaväärne võrdusega

$$\sum_{w \in X^*} a(w)w - \sum_{w \in X^*} \left(\sum_{u,v \in X^*, uv = w} a(u)\bar{a}(v) \right) w = 1 \tag{3.1}$$

ja seega tuleks näidata, et iga mittetühja sõna $w \in X^*$ jaoks kehtib

$$a(w) = \sum_{u,v \in X^*, uv=w} a(u)\bar{a}(v) \tag{3.2}$$

(kui $w = \Lambda$, siis on w kordajad (3.1) vasakul ja paremal poolel ilmselt võrdsed).
Teeme induktsiooni üle $|w|$.
Baas. Kui $|w| = 1$ või $|w| = 2$, siis (3.2) ilmselt kehtib.
Samm. Iga sõna, mille pikkus on vähemalt 3, avaldub kujul $wxyz$, kus $w \in X^*$ ja $x, y, z \in X$. Kehtigu (3.2) sõnade jaoks, mille pikkus on väiksem kui $|wxyz|$, siis

$$\begin{aligned}
a(wxyz) &= a(wxy)a_{xyz} = a(wxy) + a(wxy)(a_{xyz} - 1) \\
&= a(wxy) + (a(wxy) - a(wx) + a(wx))(a_{xyz} - 1) \\
&= a(wxy)\bar{a}(z) + \Big(\sum_{u,v \in X^*, uv=wxy} a(u)\bar{a}(v) - a(wx)\bar{a}(y) \\
&\qquad + \sum_{u,v \in X^*, uv=wx} a(u)\bar{a}(v) \Big)(a_{xyz} - 1) \\
&= a(wxy)\bar{a}(z) + \Big(\sum_{u,v \in X^*, uv=w} a(u)\bar{a}(vxy) \\
&\qquad + \sum_{u,v \in X^*, uv=w} a(u)\bar{a}(vx) \Big)(a_{xyz} - 1) \\
&= a(wxy)\bar{a}(z) + \sum_{u,v \in X^*, uv=w} a(u)\bar{a}(vxyz) = \sum_{u,v \in X^*, uv=wxyz} a(u)\bar{a}(v),
\end{aligned}$$

sest $\bar{a}(z) = \bar{a}(y) = 1$ ja $\bar{a}(xy) = \bar{a}(\Lambda) = \bar{a}(yz) = 0$. ■

3.3 Täielik tsükliline seos

Olgu X tähestik, olgu F täielik ternaarne seos X-l, s.t. $F = X^3$. Selleks et kirjeldada $C(X, F)$ Möbiuse funktsiooni, üritame kõigepealt kirjeldada $C(X, F)$ ennast. Osutub, et kehtib

Lause 3.3. *Olgu $w = x_1x_2 \cdots x_n$ ja $\bar{w} = \bar{x}_1\bar{x}_2 \cdots \bar{x}_m$ sõnad üle tähestiku X. Siis $w \equiv_F \bar{w}$, kus F on täielik ternaarne seos X-l, parajasti siis, kui*

- $n = m$

- *leidub selline hulga $\{1, \ldots, n\}$ paarispermutatsioon σ, et iga $i \in \{1, \ldots, n\}$ jaoks kehtib $x_i = \bar{x}_{\sigma(i)}$*

Tõestus: Ilmne on, et kui $w \equiv_F \bar{w}$, siis $|w| = |\bar{w}|$. Samuti võime sel juhul leida sõnade järjendi $w = w_0, w_1, \ldots, w_p = \bar{w}$ nii, et $\forall i \in \{1, \ldots p\}$ jaoks leiduvad $u, v \in X^*$ ja $a, b, c \in X$ nii, et $w_{i-1} = uabcv$ ja $w_i = ubcav$ ($\equiv_F$ definitsiooni põhjal). Seega tähtede järjend w_i on saadav tähtede järjendist w_{i-1} paarispermutatsiooni (täpsemalt öeldes kolmese tsükli) abil ja järelikult on tähtede järjend $\bar{w}$ saadav tähtede järjendist w paarispermutatsioonide korrutise — s.t. paarispermutatsiooni — abil.
Oletame nüüd, et $|w| = |\bar{w}| = n$ ja tähtede järjend $\bar{w}$ on saadav tähtede järjendist w mingi paarispermutatsiooni σ abil. Ilmne on, et hulga $\{1, \ldots n\}$ paarispermutatsioonide rühm A_n on moodustatud kolmeliste tsüklite $(1\ 2\ 3), (2\ 3\ 4), \ldots, (n-2\ n-1\ n)$ poolt. Seega võib σ avaldada kujul $\sigma = \sigma_1 \sigma_2 \cdots \sigma_p$, kus $\sigma_1, \ldots, \sigma_p$ on ülaltoodud kujuga kolmelised tsüklid. Seega saame moodustada sõnade järjendi $w = w_0, w_1, \ldots, w_p = \bar{w}$, kus iga $i \in \{1, \ldots, p\}$ korral on tähtede järjend w_i saadud tähtede järjendist w_{i-1} permutatsiooni σ_i abil. σ_i kuju tõttu leiduvad siis $u, v \in X^*$ ja $a, b, c \in X$, et $w_{i-1} = uabcv$ ja $w_i = ubcav$. Kuna $(a, b, c) \in F$, siis $w_{i-1} \equiv_F w_i$ iga $i \in \{1, \ldots, p\}$ korral ja seega $w \equiv_F \bar{w}$. ■

Olgu tähestik X lineaarselt järjestatud. Siis iga $\hat{w} \in C(X, F)$ kuulub täpselt ühte kolmest järgnevast klassist:

1. $\hat{w}$ esindajais X^*-s esineb mõni täht mitmekordselt. Sel juhul kui $w \in X^*$ on $\hat{w}$ esindaja, siis w on kongruentne $\equiv_F$ järgi kõigi oma permutatsioonidega — paaritule permutatsioonile võime lisada transpositsiooni, mis vahetab ära positsioonid, millel seisvad tähed on võrdsed.

2. $\hat{w}$ esindajais X^*-s ei ole ühtegi tähte mitu korda ning ta esindajate hulgas leidub selline sõna $x_1 x_2 \cdots x_n$, et $x_1 < x_2 < \cdots < x_n$.

3. $\hat{w}$ esindajais X^*-s ei ole ühtegi tähte mitu korda ning ta esindajate hulgas leidub selline sõna $x_1 x_2 \cdots x_n$, et $x_1 < x_2 < \cdots < x_{n-1}$, $x_{n-1} > x_n$ ja kui $n \geqslant 3$, siis $x_{n-2} < x_n$.

Olgu π loomuliku projektsiooni $X^* \to C(X, F)$ laiend $\mathbb{Z}\langle\langle X^* \rangle\rangle$-le ($\pi$ on sääraselt laiendatav, sest iga $C(X, F)$ elemendi esindajate arv X^*-s on lõplik). Defineerime $W_1, W_2, W_3 \in \mathbb{Z}\langle\langle X^* \rangle\rangle$ järgmiselt:

- $$W_1 = \sum_{w \in X^*} a(w)w,$$

  kus naabrustähestiku A tähed on väärtustatud järgmiselt:

  $$a_{xyz} = \begin{cases} 1 & \text{kui } x \leqslant y \leqslant z \\ 0 & \text{muidu} \end{cases}$$

- $$W_2 = \sum_{w \in X^*} a(w)w,$$

  kus naabrustähestiku A tähed on väärtustatud järgmiselt:

  $$a_{xyz} = \begin{cases} 1 & \text{kui } x < y,\ x < z,\ y \neq z \\ 0 & \text{muidu} \end{cases}$$

- $$W_3 = \sum_{w \in X^*} a(w)w,$$

  kus naabrustähestiku A tähed on väärtustatud järgmiselt:

  $$a_{xyz} = \begin{cases} 1 & \text{kui } x < y < z \\ 0 & \text{muidu} \end{cases}$$

Teoreem 3.4. *$\pi(W_1 + W_2 - W_3)$ on $C(X, F)$ Riemanni funktsioon.*

Tõestus: Kirjeldame sõna $w = x_1 x_2 \cdots x_n$ kordajaid W_1-s, W_2-s ja W_3-s. Ilmselt kehtivad järgmised väited:

- Kui $|w| \leqslant 2$, siis $\langle W_1, w\rangle = \langle W_2, w\rangle = \langle W_3, w\rangle = 1$ (naabrusmonoomi definitsiooni kohaselt). Kui $|w| \geqslant 3$, siis:
- $\langle W_1, w\rangle = 1$ parajasti siis, kui $x_1 \leqslant x_2 \leqslant \cdots \leqslant x_n$. Tõepoolest, kui mingi i korral $x_{i-1} > x_i$ siis kui $i < |w|$, siis $a(w)$ sisaldab tegurit $a_{x_{i-1}x_i x_{i+1}} = 0$, muidu sisaldab $a(w)$ tegurit $a_{x_{i-2}x_{i-1}x_i} = 0$.
- $\langle W_2, w\rangle = 1$ parajasti siis, kui $x_1 < x_2 < \cdots < x_{n-1}$, $x_{n-2} < x_n$ ja $x_{n-1} \neq x_n$. Tõepoolest, kui mingi i korral $x_{i-1} = x_i$, siis mingi tegur $a(w)$-s võrdub 0-ga. Samuti, kui mingi $i < |w|$ korral $x_{i-1} > x_i$, siis $a(w)$ sisaldab tegurit $a_{x_{i-1}x_i x_{i+1}} = 0$.

- $\langle W_3, w\rangle = 1$ parajasti siis, kui $x_1 < x_2 < \cdots < x_n$. Põhjendada saab seda sarnaselt üleeelmise juhuga.

Seega oleme ära kirjeldanud W_1, W_2 ja W_3 *kandjad* (formaalse rea $r \in \mathbb{Z}\langle\langle M\rangle\rangle$, kus M on monoid (üle mille on defineeritav formaalsete ridade ring), kandjaks nimetatakse hulka $\operatorname{supp} r = \{x \in M | \ \langle r, x\rangle \neq 0\}$).
Uurime, millega võrduvad $\hat{w} \in C(X, F)$ kordajad $\pi(W_1)$-s, $\pi(W_2)$-s ja $\pi(W_3)$-s. Kui $|\hat{w}| \leqslant 2$, siis on $\hat{w}$-l täpselt üks esindaja X^*-s ning selle esindaja kordaja on nii W_1-s, W_2-s kui ka W_3-s võrdne ühega. Muidu:

1. Kui $\hat{w}$ kuulub esimesse eelpool toodud kolmest klassist, siis on kõigi tema esindajate kordajad W_2-s ja W_3-s ilmselt võrdsed nulliga. Olgu w mingi $\hat{w}$ esindaja, siis on $\hat{w}$ esindajateks täpselt kõik w permutatsioonid. Nendest permutatsioonidest on täpselt üks selline, kus tähtede järjekord on mittekahanev. Eelpool toodud W_1 kandja kirjelduse põhjal on selle sõna kordajaks W_1-s 1 ja kõigi ülejäänud w permutatsioonide kordajaks 0.
   Kokkuvõttes oleme saanud, et
   $\langle\pi(W_1), \hat{w}\rangle = 1$ ja $\langle\pi(W_2), \hat{w}\rangle = \langle\pi(W_3), \hat{w}\rangle = 0$.

2. Kui $\hat{w}$ kuulub teise eelpool toodud kolmest klassist, siis on tema esindajate hulgas mingi sõna $w = x_1x_2\cdots x_n$, mille korral $x_1 < x_2 < \cdots < x_n$ ja $\hat{w}$ ülejäänud esindajad on selle sõna paarispermutatsioonid. Siis $\langle W_1, w\rangle = \langle W_2, w\rangle = \langle W_3, w\rangle = 1$ ja kõigi ülejäänud w paarispermutatsioonide kordajad W_1-s, W_2-s ja W_3-s on nullid. (Ka sõna $x_1\cdots x_{n-2}x_nx_{n-1}$ kordaja W_2-s on 1, kui see sõna pole $\hat{w}$ esindaja).
   Kokkuvõttes oleme saanud, et
   $\langle\pi(W_1), \hat{w}\rangle = \langle\pi(W_2), \hat{w}\rangle = \langle\pi(W_3), w\rangle = 1$.

3. Kui $\hat{w}$ kuulub kolmandasse eelpool toodud kolmest klassist, siis on tema esindajate hulgas mingi sõna $w = x_1x_2\cdots x_n$, mille korral $x_1 < x_2 < \cdots < x_{n-1} \neq x_n$ ja $x_{n-2} < x_n$. Sel juhul $\langle W_1, w\rangle = \langle W_3, w\rangle = 0$ ja $\langle W_2, w\rangle = 1$. $\hat{w}$ ülejäänud esindajate (ehk w ülejäänud paarispermutatsioonide) kordajad kõigis kolmes reas on võrdsed nulliga.
   Kokkuvõttes oleme saanud, et
   $\langle\pi(W_1), \hat{w}\rangle = \langle\pi(W_3), \hat{w}\rangle = 0$ ja $\langle\pi(W_2), \hat{w}\rangle = 1$.

Seega oleme saanud, et iga $\hat{w} \in C(X, F)$ jaoks $\langle\pi(W_1)+\pi(W_2)-\pi(W_3), \hat{w}\rangle = 1$. ■

Lahendamata probleem: Leida $(\pi(W_1)+\pi(W_2)-\pi(W_3))^{-1}$.
Teoreem 3.2 lubab meil leida W_1^{-1}, W_2^{-1} ja W_3^{-1}, aga $(W_1+W_2-W_3)^{-1}$ kuju pole teada, nii nagu ka tema projektsioon $C(X,F)$-i.

3.4 Tsükliline sümmeetriline transitiivne seos

Lause 3.5. *Olgu F tsükliline seos hulgal X. F on sümmeetriline ja transitiivne parajasti siis, kui leidub hulga X selline tükeldus $X = X_1\dot\cup X_2\dot\cup\cdots\dot\cup X_m$, et*

$$F = {X_1}^3 \cup {X_2}^3 \cup \cdots \cup {X_m}^3$$

Tõestus: Ilmne on, et kui hulgal X selline tükeldus leidub siis F on sümmeetriline ja transitiivne.
Olgu F tsükliline sümmeetriline transitiivne seos hulgal X. Olgu $a\in X$. Olgu $F(a)=\{x\in X \mid \exists y\in X \text{ nii, et } \{a,x,y\}\in F\}$. Olgu $x_1,x_2,x_3\in F(a)$. Näitame, et siis $(x_1,x_2,x_3)\in F$

$$\begin{gathered}
(y_i,a,x_i)\in F,\ (x_i,a,y_i)\in F \implies (a,x_i,a)\in F,\ \text{kus } i=1,2,3\\
(a,x_1,a)\in F,\ (a,x_2,a)\in F \implies (x_1,a,x_2)\in F \implies (a,x_1,x_2)\in F\\
(a,x_2,a)\in F,\ (a,x_3,a)\in F \implies (x_2,a,x_3)\in F \implies (x_2,x_3,a)\in F\\
(a,x_1,x_2)\in F,\ (x_2,x_3,a)\in F \implies (x_1,x_2,x_3)\in F
\end{gathered}$$

Olgu $a,b\in X$. Näitame, et kui $b\in F(a)$, siis $F(b)\subseteq F(a)$. Olgu $c\in F(b)$. Siis $(b,c,b)\in F$ (sest et $\forall x\in X:\ x\in F(x)$) ja $(b,a,b)\in F$. Transitiivsuse tõttu nüüd $(a,b,c)\in F$, seega $c\in F(a)$.
Teisest küljest, kui $b\in F(a)$, siis $a\in F(b)$ ja $F(a)=F(b)$.
Olgu $a,b\in X$. Näitame, et $F(a)\cap F(b)=\emptyset$ või $F(a)=F(b)$. Olgu $F(a)\cap F(b)\neq\emptyset$, olgu $c\in F(a)\cap F(b)$. Siis $F(a)=F(c)=F(b)$.
Seega on $\{F(x)\mid x\in X\}$ hulga X tükeldus. Kuna $\forall x\in X:\ (F(x))^3\subseteq F$ ja juhul kui $a,b\in X$ kuuluvad erinevatesse tükkidesse, siis $\neg\exists c\in X:\ (a,b,c)\in X$, siis see tükeldus rahuldab lause tingimusi. ■

Olgu X tähestik, olgu F tsükliline sümmeetriline transitiivne seos X-l, olgu $X_1,X_2,\ldots,X_m$ eelmises lauses kirjeldatud F tekitatud X tükeldus. Kirjeldame taas $C(X,F)$-i. Defineerime sõna $w\in X^*$ jaoks hulgad

$$L(w)=\{x\in X \mid \exists u\in X^*:\ xu\equiv_F w\}$$

ja

$$R(w) = \{x \in X \mid \exists u \in X^* : \ ux \equiv_F w\}$$

Kehtib järgmine

Lemma 3.6. *Olgu $w_1, w_2 \in X^*$. Kui F ei sisalda elemente kujul $\{a, b, c\}$, kus $a \in R(w_1)$, $b \in L(w_2)$ ja $c \in X$, siis $w_1w_2/\equiv_F$ koosneb täpselt sõnadest kujul $\bar{w}_1\bar{w}_2$, kus $w_1 \equiv_F \bar{w}_1$ ja $w_2 \equiv_F \bar{w}_2$.*

Tõestus: Ilmne on, et kõik sellised sõnad $\bar{w}_1\bar{w}_2$ on kongruentsed w_1w_2-ga Oletame vastuväiteliselt, et $w \equiv_F \bar{w}$ ja $\bar{w}$ ei avaldu lemma sõnastuses kirjeldatud kujul. Siis leidub järjend $w = w_0, w_1, \ldots, w_p = \bar{w}$, et iga j, kus $1 \leqslant j \leqslant p$, korral leiduvad sellised $u, v \in X^*$ ja $a, b, c \in X$, et $w_{j-1} = uabcv$ ja $w_j = ubcav$. Olgu j' vähim selline indeks, et $w_{j'}$ ei avaldu lemma sõnastuses kirjeldatud kujul. Olgu j'-le vastavad u, v, a, b, c vastavalt u', v', a', b', c'. Kui $u'a'b'c'$ oleks mõne w_1-ga kongruentse sõna prefiksiks või $a'b'c'v'$ oleks mõne w_2-ga kongruentse sõna sufiksiks, siis $w_{j'}$ avalduks lemma sõnastuses kirjeldatud kujul. Seega kas $u'a'b' \equiv_F w_1$ ja $c'v' \equiv_F w_2$ või $u'a' \equiv_F w_1$ ja $b'c'v' \equiv_F w_2$. See tähendab, et kas $b' \in R(w_1)$ ja $c' \in L(w_2)$ või $a' \in R(w_1)$ ja $b' \in L(w_2)$. Seega peaks $\{a', b', c'\} \in F$. Kuid see räägib vastu lemma eeldustele. Seega ei saa sellist indeksit j' leiduda. ∎

Lause 3.7. *Olgu $w \in X^*$. Olgu $w = w_1w_2 \cdots w_k$ nii, et leiduvad sellised $i_1, \ldots, i_k$ nii, et $1 \leqslant i_1, \ldots, i_k \leqslant m$ ja $\forall j \in \{1, \ldots, k-1\} : \ i_j \neq i_{j+1}$ ja $\forall j \in \{1, \ldots, k\} : \ w_j \in X_{i_j}^+$. Olgu $\bar{w} \in X^*$. Siis $w \equiv_F \bar{w}$ parajasti siis, kui leiduvad sellised $\bar{w}_1, \ldots, \bar{w}_k \in X^+$, et $\bar{w} = \bar{w}_1\bar{w}_2 \cdots \bar{w}_k$ ja $\forall j \in \{1, \ldots, k\}$ jaoks kehtib $w_j \equiv_F \bar{w}_j$.*

Tõestus: „Ainult siis“ pool on ilmne.
„Siis“ poole näitame induktsiooniga üle k. Tõestame natuke tugevama väite — lisaks lauses väidetule näitame veel, et $R(w) = R(w_k)$.
Baas. $k = 1$. Sel juhul ilmselt lause väide kehtib ja $R(w) = R(w_1)$.
Samm. Kehtigu mingi k korral lause väide ja $R(w) = R(w_k)$. Vaatame sõna ww_{k+1}, kus $w_{k+1} \in X_{i_{k+1}}^+$, kus $1 \leqslant i_{k+1} \leqslant m$ ja $i_k \neq i_{k+1}$. Sel juhul on w ja w_{k+1} jaoks täidetud eelmise lemma eeldused ($R(w) = R(w_k) \subseteq X_{i_k}$ ja $L(w_{k+1}) \subseteq X_{i_{k+1}}$). Seega kui $w' \equiv_F ww_{k+1}$, siis leiduvad sellised $\bar{w}$ ja $\bar{w}_{k+1}$, et $w \equiv_F \bar{w}$ ja $w_{k+1} \equiv_F \bar{w}_{k+1}$ ning $w' = \bar{w}\bar{w}_{k+1}$. Induktsiooni eelduse kohaselt avaldub siis $\bar{w}$ kujul $\bar{w}_1 \cdots \bar{w}_k$, kus $w_1 \equiv_F \bar{w}_1, \ldots, w_k \equiv_F \bar{w}_k$. Kuna w' sufiksiks on mingi w_{k+1}-ga kongruentne sõna, siis saame, et $R(ww_{k+1}) = R(w_{k+1})$. ∎

Järgmine lemma on tõestatud [Lal]-s.

Lemma 3.8. *Olgu M lõplike dekompositsioonidega monoid, olgu $x \in M$, olgu $\delta_0(x)$ x-i selliste dekompositsioonide arv, milles on paarisarv komponente, ja $\delta_1(x)$ tema selliste dekompositsioonide arv, milles on paaritu arv komponente. Kui μ on M Möbiuse funktsioon, siis $\mu(x) = \delta_0(x) - \delta_1(x)$.* ■

Siit järeldub järgmine

Lemma 3.9. *Olgu $w_1, w_2 \in X^+$. Kui F ei sisalda elemente kujul $\{a, b, c\}$, kus $a \in R(w_1)$, $b \in L(w_2)$ ja $c \in X$, siis monoidis $C(X, F)$ $\mu(\hat{w}_1\hat{w}_2) = 0$.*

Tõestus: Lemma 3.6 järgi on $\hat{w}_1\hat{w}_2$ iga dekompositsioon $\hat{y}_1, \hat{y}_2, \ldots, \hat{y}_n$ (täpselt) ühel kujul kahest võimalikust:
Esimest tüüpi dekompositsioon: Leidub selline i, $0 \leqslant i \leqslant n$, et $\hat{y}_1 \cdots \hat{y}_i = \hat{w}_1$ ja $\hat{y}_{i+1} \cdots \hat{y}_n = \hat{w}_2$.
Teist tüüpi dekompositsioon: Sellist i-d nagu eelmisel korral ei leidu, kuid leidub selline i ($1 \leqslant i \leqslant n$) ja sellised $\hat{z}_1, \hat{z}_2 \in C(X, F)$, et $\hat{y}_1 \cdots \hat{y}_{i-1}\hat{z}_1 = w_1$, $\hat{z}_2\hat{y}_{i+1} \cdots \hat{y}_n = w_2$ ja $\hat{z}_1\hat{z}_2 = \hat{y}_i$. Seejuures on $\hat{z}_1$ ja $\hat{z}_2$ üheselt määratud.
Seame iga esimest tüüpi dekompositsiooniga vastavusse teist tüüpi dekompositsiooni ja vastupidi, iga teist tüüpi dekompositsiooniga vastavusse esimest tüüpi dekompositsiooni järgmiselt:
Kui $\hat{y}_1, \ldots, \hat{y}_n$ on esimest tüüpi, siis seame temaga vastavusse dekompositsiooni $\hat{y}_1, \ldots, \hat{y}_{i-1}, \hat{y}_i\hat{y}_{i+1}, \hat{y}_{i+2}, \ldots, \hat{y}_n$, kus i on määratud nii nagu esimest tüüpi dekompositsiooni kirjelduses.
Kui $\hat{y}_1, \ldots, \hat{y}_n$ on teist tüüpi, siis seame temaga vastavusse dekompositsiooni $\hat{y}_1, \ldots, \hat{y}_{i-1}, \hat{z}_1, \hat{z}_2, \hat{y}_{i+1}, \ldots, \hat{y}_n$, kus i, $\hat{z}_1$ ja $\hat{z}_2$ on määratud nii nagu teist tüüpi dekompositsiooni kirjelduses.
Ilmne on, et toodud vastavused on teineteise pöördvastavused, seega oleme me $\hat{w}_1\hat{w}_2$ dekompositsioonid paarideks jaganud. Seejuures on igas paaris ühes dekompositsioonis paarisarv ja teises paaritu arv komponente, s.t. $\delta_0(\hat{w}_1\hat{w}_2) = \delta_1(\hat{w}_1\hat{w}_2)$. ■

Nüüd võime kirjeldada $C(X, F)$ Möbiuse funktsiooni. Tuletame meelde, et $X_1, \ldots, X_m$ oli X klassijaotus, mille tekitas seos F lause 3.5 järgi.

Lause 3.10. *Olgu $\hat{w} \in C(X, F)$, olgu $w \in X^*$ mingi $\hat{w}$ esindaja. Kui leidub selline i, et $w \in X_i^*$, siis on $\mu(\hat{w})$ võrdne monoidi $C(X_i, X_i^3)$ Möbiuse funktsiooni väärtusega kohal $\hat{w}$ (siin X_i^3 tähistab täielikku tsüklilist seost üle X_i). Kui sellist i-d ei leidu, siis $\mu(\hat{w}) = 0$.*

Tõestus: Kui selline i leidub, siis on $\hat{w} \in C(X, F)$ ja $\hat{w} \in C(X_i, X_i^3)$ dekompositsioonide vahel ilmselt loomulik üksühene vastavus. Vastasel juhul ütleb viimane lemma, et $\mu(\hat{w}) = 0$. ■

Viited

[Fed] Jean-Marc Fedou. Adjacencies in Words. Advances in Applied Mathematics **16** (1995), pp206–218

[Lal] Gerard Lallement. Semigroups and Combinatorial Applications. John Wiley & Sons Inc., 1979

About the Möbius function of partially cyclic monoid

Peeter Laud

Resume

Let X be a finite alphabet, and let F be a ternary relation over X. We call F *cyclic*, if for every $a, b, c \in X$ $(a, b, c) \in F$ implies $(b, c, a) \in F$ (and this, in turn, implies that $(c, a, b) \in F$). Define a congruence $\equiv_F$ on X^* by the relations $abc \equiv_F bca \equiv_F cab$ for every $(a, b, c) \in F$. We denote the factormonoid $X^*/\equiv_F$ by $C(X, F)$ and call it *partially cyclic monoid over* X *generated by* F.

For the alphabet X we define *the adjacency alphabet* $A = \{a_{xyz} | \, (x, y, z) \in X^3\}$. For every word $w = x_1 \cdots x_n \in X^*$ we define *the adjacency monomial* $a(w) = a_{x_1x_2x_3}a_{x_2x_3x_4} \cdots a_{x_{n-2}x_{n-1}x_n}$, if $n \geqslant 3$ and $a(w) = 1$ otherwise. We also define *the sieve polynomial* $\bar{a}(w) = (\bar{a}(w') + \bar{a}(w''))(a_{x_{n-2}x_{n-1}x_n} - 1)$, where $w' = x_1 \cdots x_{n-1}$ and $w'' = x_1 \cdots x_{n-2}$. If $n < 3$ then we let $\bar{a}(w) = 1$ when $n = 1$ or $\bar{a}(w) = 0$ otherwise. In $\mathbb{Z}[A]\langle\langle X^*\rangle\rangle$ holds

$$\sum_{w \in X^*} a(w)w = \left(1 - \sum_{w \in X^*} \bar{a}(w)w\right)^{-1}$$

Let X be totally ordered. Let W_1, W_2, W_3 be series in $\mathbb{Z}\langle\langle X^*\rangle\rangle$ defined by: $W_i = \sum_{w \in X^*} a(w)w$, $i = 1, 2, 3$, where the variables $a_{xyz} \in A$ are assigned the following values:

- for W_1: $a_{xyz} = 1$ iff $x \leqslant y \leqslant z$. Otherwise $a_{xyz} = 0$
- for W_2: $a_{xyz} = 1$ iff $x < y$, $y < z$ and $y \neq z$. Otherwise $a_{xyz} = 0$
- for W_3: $a_{xyz} = 1$ iff $x < y < z$. Otherwise $a_{xyz} = 0$.

Let F be the total ternary relation over X (i.e. $F = X^3$), let π be the natural projection $X^* \to C(X, F)$ (which can be extended to formal power series). We show then, that $\pi(W_1 + W_2 - W_3)$ is the Riemann function of $C(X, F)$. We would like to find the Möbius function of $C(X, F)$, but so far we can find

neither $(W_1 + W_2 - W_3)^{-1}$ nor its projection to $C(X, F)$, we can only invert the series W_i.

The cyclic relation F is called *symmetric*, if for every $a, b, c \in X$ $(a, b, c) \in F$ implies $(b, a, c) \in F$. It is called *transitive*, if for every $a, b, c, d \in X$ $(a, b, c) \in F$ and $(c, d, a) \in F$ implies $(b, c, d) \in F$ (and also $(d, a, b) \in F$). We show that F is symmetric and transitive iff there exists such partitioning of X $X_1, \ldots, X_m$, that $F = X_1^3 \cup \cdots \cup X_m^3$. This gives us, that if F is a symmetric and transitive cyclic relation over X then $\mu(w)$ for $w \in C(X, F)$ equals $\mu(w)$ in $C(X_i, X_i^3)$, if the representatives of w are the words over X_i; if there isn't such i then $\mu(w) = 0$.