PROSTE GRUPE IN DREVESA

JAKOB POGAČNIK SOUVENT

Fakulteta za matematiko in fiziko
Univerza v Ljubljani

Vsaki grupi pripada geometrijska upodobitev s Cayleyjevim grafom. V primeru prostih grup je pripadajoči graf, ob primerni izbiri generatorjev, drevo, na katerem je kanonično delovanje z levim množenjem prosto. Posledično je potrebna lastnost karakterizacije prostih grup obstoj drevesa, na katerem grupa prosto deluje. Manj očitno je, da je potrebna lastnost tudi zadostna, tj. da je vsaka grupa s prostim delovanjem na nekem drevesu prosta. Posledica te ekvivalence je dejstvo, da so podgrupe prostih grup tudi same proste.

FREE GROUPS AND TREES

Every group has a geometric representation in the form of a Cayley graph. For free groups with a proper choice of a generating set, the corresponding Cayley graph is a tree on which the group acts freely via a left translation action. Consequently a necessary condition for a group to be free is admitting a free action on a nonempty tree. Not immediately obvious is that this condition is also sufficient, meaning that having a free action on some tree is enough to characterise a group as free. A consequence of this equivalence is the fact that subgroups of a free group are themselves free.

1. Uvod

Ideja *prostega objekta* znotraj določene kategorije je matematična interpretacija generičnega objekta kategorije. Algebraična struktura nad neko množico A je prosta, če so edine vezi med elementi A vezi, ki sledijo iz aksiomov, ki definirajo algebraično strukturo. Proste strukture se naravno pojavijo na več področjih matematike v obliki vektorskih prostorov, prostih grup in tenzorskih algeber. Netrivialni problem je pokazati, da je dani objekt prost.

Geometična teorija grup ponuja orodja za analizo algebraičnih lastnosti grup preko njihovega delovanja in upodobitev v obliki geometrijskih objektov, kot so denimo grafi, ploskve ali višje dimenzionalne mnogoterosti. V članku bomo pokazali, kako je prostost grupe razvidna iz njene upodobitve v obliki Cayleyjevega grafa in njenega delovanja na grafih. Več o geometrični teoriji grup je bralcu na voljo v [1], od koder je tudi povzet pričujoči članek.

2. Cayleyjevi grafi

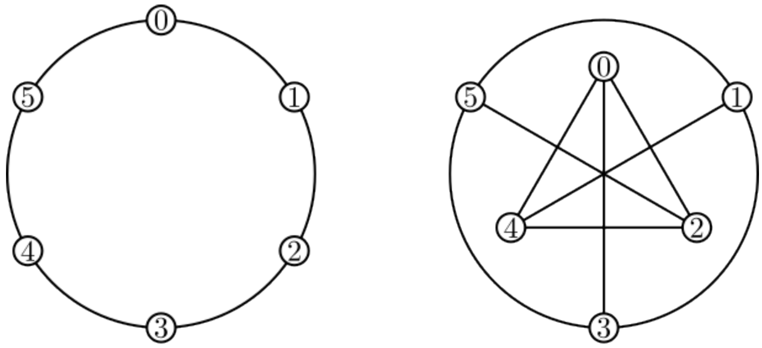
Denimo, da imamo podano neko grupo G, generirano z množico S, ki bi jo radi predstavili geometrično. Povezave med elementi glede na množico generatorjev lahko upodobimo s *Cayleyjevimi grafi*.

Definicija 1 (Cayleyjev graf). Naj bo S podmnožica, ki generira grupo G. **Cayleyjev graf** grupe G glede na množico generatorjev S je graf $Cay(G, S)$, katerega vozlišča so elementi grupe G, povezave pa so

$$\{\{g, g \cdot s\} \mid g \in G, s \in (S \cup S^{-1}) \setminus \{e\}\},$$

kjer je s $\cdot$ označeno množenje v grupi G in z e njena enota.

Dve vozlišči v Cayleyjevem grafu sta si sosednji natanko tedaj, ko se razlikujeta le za desno množenje z elementom (ali inverzom) dane množice S. Za boljšo predstavo si oglejmo Cayleyjeve grafe nekaterih znanih grup.



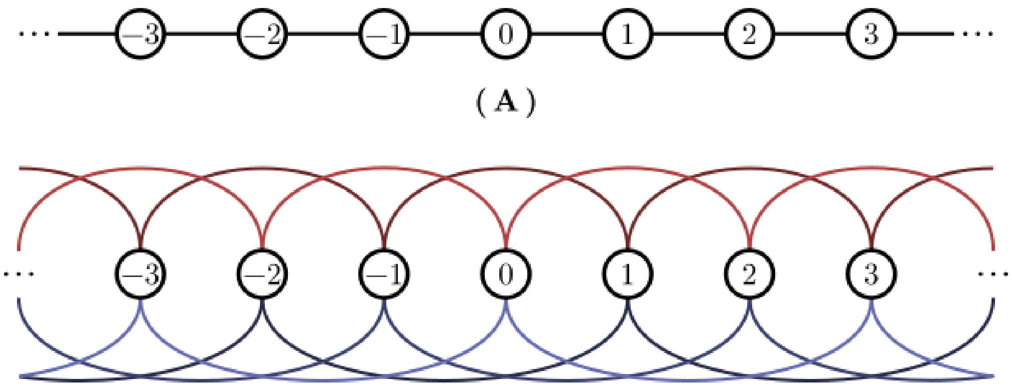
(A) **(B)**

Slika 1. $Cay(\mathbb{Z}_6, S_1)$ in $Cay(\mathbb{Z}_6, S_2)$

Zgled 1. Na sliki 1 sta Cayleyjeva grafa končne ciklične grupe $\mathbb{Z}_6$ glede na množici generatorjev $S_1 = \{1\}$ (slika 1 A) in $S_2 = \{2, 3\}$ (slika 1 B).

Vidimo, da je Cayleyjev graf odvisen od izbire množice generatorjev. Cikli v Cayleyjevem grafu nosijo informacije o relacijah med generatorji. V grafu $Cay(\mathbb{Z}_6, S_2)$ cikla $(0, 2, 4)$ in $(1, 3, 5)$ ustrezata relaciji $2 + 2 + 2 = 0$, cikel $(0, 3)$ pa relaciji $3 + 3 = 0$.

Zgled 2. Za neskončno ciklično grupo $\mathbb{Z}$ dobimo naslednja Cayleyjeva grafa glede na množici generatorjev $S_1 = \{1\}$ (slika 2 A) in $S_2 = \{2, 3\}$ (slika 2 B).



(B)

Slika 2. $Cay(\mathbb{Z}, S_1)$ in $Cay(\mathbb{Z}, S_2)$

Tudi v tem grafu se v primeru množice S_2 (slika 2 B) pojavijo cikli. Cikel $(0, 3, 1, -1, -3)$ ustreza relaciji $3 - 2 - 2 - 2 + 3 = 0$ med generatorjema 2 in 3.

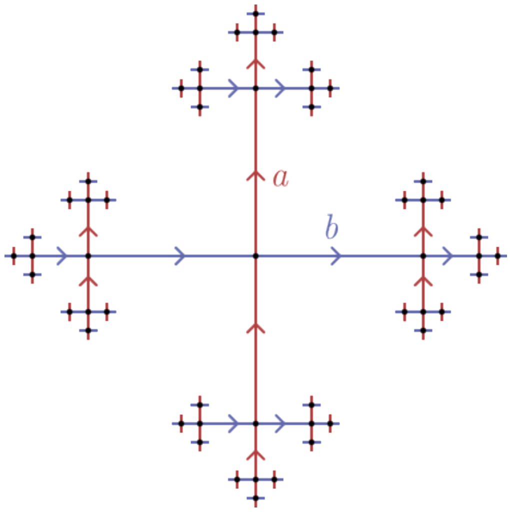
V splošnem cikel $(v_0, v_1, \ldots, v_n)$ v grafu $Cay(G, S)$ pomeni obstoj takih elementov $s_1, s_2, \ldots, s_n \in S \cup S^{-1}$, da je $v_{i-1} \cdot s_i = v_i$. Cikel $(v_0, v_1, \ldots, v_n)$ tedaj predstavlja relacijo med elementi množice S, podano z enačbo $s_0 \cdot s_1 \cdot \ldots \cdot s_n = e$.

Opazka deluje tudi v obratno smer. Če Cayleyjev graf $Cay(G, S)$ ne vsebuje ciklov, elementi množice S nimajo medsebojnih relacij. Opisana lastnost tvori graf brez ciklov z eno komponento, ki mu pravimo drevo (v splošnem neskončno). Grupe, katerih Cayleyjev graf je drevo, so tipično ti. *proste grupe*, ki so primer *prostih objektov* v kategoriji grup.

Zgled 3. Tipični primer Cayleyjevega drevesa dobimo za prosto grupo ranga 2 z generatorjema $S = \{a, b\}$, ki jo običajno označimo F_2. Njeni elementi so besede oblike $\{s_1 s_2 \ldots s_n \mid s_i \in S \cup S^{-1}\}$, grupna operacija pa je stikanje besed (z morebitnim krajšanjem, če v stiku črki sledi njen inverz).

Element $x \in F$ je v Cayleyjevem grafu $Cay(F, S)$ povezan z elementi xa, xb, xa^{-1} in xb^{-1}. Ker je grupa F nekomutativna, sta elementa xab in xba različna. Nadalje to pomeni, da je med enoto ε in elementom $s_1 s_2 \dots s_n$ natanko ena pot, ki vodi skozi vozlišča $s_1, s_1 s_2, \dots, s_1 s_2 \dots s_{n-1}$ (pri čemer privzamemo definicijo poti, v kateri se vozlišča ne ponavljajo). Če bi bili $s_1', s_2', \dots, s_n' \in S \cup S^{-1}$ elementi, ki bi opisovali drugo pot do med ε in $s_1 s_2 \dots s_n$ skozi vozlišča $s_1', s_1' s_2', \dots, s_1' s_2' \dots s_{n-1}'$, bi morala veljati enakost okrajšanih besed $s_1' s_2' s_3' \dots s_n' = s_1 s_2 s_3 \dots s_n$, kar pomeni natanko enakost posamičnih črk $s_1' = s_1, s_2' = s_2, \dots, s_n' = s_n$.

Graf $Cay(F, S)$ je torej neskončen, povezan 4-regularen graf brez ciklov. V ravnini ga lahko upodobimo z neskončnim fraktalnim drevesom, ilustriranim na sliki 3.



Slika 3. Cayleyjev graf proste grupe F_2

Cayleyjevi grafi prostih grup s primerno izbiro generatorjev so drevesa. Obratno, če je T graf, izomorfen Cayleyjevemu grafu grupe G, potem iz dejstva, da je T drevo (in določenimi predpostavkami), lahko razberemo prostost grupe G. Težava seveda nastane pri iskanju grupe G in primerne množice generatorjev S, katere Cayleyjev graf $Cay(G, S)$ je izomorfen T. V nadaljevanju bomo formalizirali opisano ekvivalenco in pokazali, kako lahko iz grafa razberemo množico generatorjev proste grupe.

3. Proste grupe

Neformalno so *prosti objekti* v neki kategoriji objekti, za katere veljajo samo zahteve (aksiomi), ki definirajo objekte te kategorije. Posledica želene lastnosti je, da morajo biti generatorji prostih objektov karseda neodvisni. Dodatno, če imamo nek morfizem proste strukture F, je slika F enolično določena s slikami množice generatorjev.

Dobro znani primeri prostih struktur so vektorski prostori. Vsak vektorski prostor V ima maksimalno nepovezano množico, ki ga generira, tj. linearno neodvisno bazo; slika poljubnega elementa prostora V pri linearni preslikavi je enolično določena s slikami baznih vektorjev.

Za razliko od vektorskih prostorov večine grup ne moremo opisati s popolnoma nepovezano množico generatorjev. Inherentne relacije so potrebne za opis določenih grup, kar je eden od razlogov, zakaj je študij grup zahtevnejši od študija vektorskih prostorov.

Definicija 2 (Prosta grupa). Naj bo S množica elementov grupe F. Pravimo, da S **prosto generira** F, če za vsako grupo G in vsako preslikavo $j\colon S \to G$ obstaja enolično določen homomorfizem $\varphi_j\colon F \to G$, ki razširi j. Če označimo z i inkluzijo $i\colon S \hookrightarrow F$ to pomeni $\varphi_j \circ i = j$.

$$
\begin{tikzcd}
S \arrow[r, "j"] \arrow[d, hook, "i"'] & G \\
F \arrow[ur, dashed, "\varphi_j"'] &
\end{tikzcd}
$$

Grupi F pravimo **prosta**, če vsebuje kakšno podmnožico, ki jo prosto generira, opisani lastnosti pa pravimo **univerzalna lastnost prostih grup**.

Preden nadaljujemo, pokažimo, da so proste grupe enolično (do izomorfizma natančno) določene z množico generatorjev.

Izrek 1 (Enoličnost prostih grup). *Naj bo S množica. Potem do izomorfizma natančno obstaja največ ena grupa, prosto generirana z S.*

Dokaz. Naj bosta F in F' prosti grupi, prosti generirani z množico S. Označimo z i in j inkluziji $i\colon S \hookrightarrow F$ ter $j\colon S \hookrightarrow F'$. Po univerzalni lastnosti prostih grup lahko inkluziji razširimo do homomorfizmov $\varphi_i\colon F' \to F$ in $\varphi_j\colon F \to F'$.

$$
\begin{tikzcd}
S \arrow[r, "j"] \arrow[d, hook, "i"'] & F' \\
F \arrow[ur, dashed, "\varphi_j"'] &
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
S \arrow[r, hook, "j"] \arrow[d, "i"'] & F' \arrow[dl, dashed, "\varphi_i"] \\
F &
\end{tikzcd}
$$

Kompozitum $\varphi_i \circ \varphi_j\colon F \to F$ je na množici S identiteta. Ker sta tako $\varphi_i \circ \varphi_j$ kot id_F razširitvi inkluzije i, mora po enoličnosti razširitev veljati $\varphi_i \circ \varphi_j = id_F$. Podobno velja $\varphi_j \circ \varphi_i = id_{F'}$, torej sta grupi F in F' izomorfni.

■

Naj bo S poljubna množica. Grupa okrajšanih besed nad abecedo S je podana z množico $F(S) = \{s_1 s_2 \dots s_n \mid n \in \mathbb{N}_0, s_i \in S \cup S^{-1}\}$ opremljeno z operacijo stikanja in krajšanja sosednjih inverzov. Takšna operacija je dobro definirana in grupa $F(S)$ je prosto generirana z množico S. Dokaza dobre definiranosti in dejstva, da je grupa prosto generirana, sta opisana v [1, Prop. 3.3.5.].

Zaradi izreka 1 sledi, da s takšno konstrukcijo dobimo natanko vse proste grupe in da vsaka množica S prosto generira neko grupo. V nadaljevanju članka bomo zato z besedno zvezo prosta grupa vedno imeli v mislih množico okrajšanih besed, ki jo bomo označili z oznako $F(S)$.

Zapis prostih grup v obliki $F(S)$ pravi, da lahko na elemente prostih grup gledamo kot formalne besede nad abecedo S. Intuitivna, a netrivialna, posledica tega pogleda je naslednja lastnost.

Lema 2. *Proste grupe ne vsebujejo elementov končnega reda.*

Dokaz. Naj bo $F(S)$ grupa, prosto generirana z množico S in naj bo $a \in F(S)$ element končnega reda. Označimo $a = a_1 a_2 \dots a_n$ za $a_1, a_2, \dots, a_n \in S$. Naj bo $j\colon S \to \mathbb{Z}$ preslikava, za katero velja $j(a_i) > 0$. Po univerzalni lastnosti prostih grup lahko preslikavo j razširimo do homomorfizma $\varphi_j\colon F(S) \to \mathbb{Z}$. Ker je φ_j homomorfizem, velja $\varphi_j(a_1 a_2 \dots a_n) = \varphi_j(a_1) + \varphi_j(a_2) + \dots + \varphi_j(a_n)$, oziroma $\varphi_j(a) > 0$. Ker bi moral red slike $\varphi_j(a)$ deliti red elementa a, vsi neničelni elementi $\mathbb{Z}$ pa nimajo končnega reda, smo prišli v protislovje.

4. Cayleyjevi grafi prostih grup

Opremljeni z natančno definicijo proste grupe se vrnimo na ugotovitev o strukturi njihovih Cayleyjevih grafov poglavja 2. Trditev, da prostim grupam ustrezajo Cayleyjevi grafi dreves, zapišemo v izrek in tudi formalno dokažemo.

Kot opombo glede notacije zabeležimo, da bomo imeli z oznako $Cay(F, S)$ v mislih prosto grupo $F = F(S)$.

Izrek 3. *Naj bo F grupa, prosto generirana z množico $S \subseteq F$. Potem je graf $Cay(F, S)$ drevo.*

Dokaz. Kot smo opazili že v drugem poglavju, lahko cikel v grafu $Cay(F, S)$ razumemo kot relacijo med elementi množice S, podano z enačbo

$$s_1 \dots s_n = \varepsilon,$$

kjer ε predstavlja prazno besedo (nevtralni element) v grupi $F(S)$.

Zapisana relacija bi bila protislovna s prostostjo grupe $F(S)$, saj je grupa prosta natanko tedaj, ko elementi množice, ki jo prosto generira, nimajo medsebojnih povezav. ∎

Pri formalnem dokazu obrata se stvari nekoliko zakomplicirajo. Ker so Cayleyjevi grafi neusmerjeni, nam težavo delajo cikli dolžine 2, ki v primeru majhnih grup tvorijo Cayleyjev graf, ki ustreza definiciji drevesa. Tako je naprimer graf $Cay(\mathbb{Z}_2, \{1\})$ drevo, čeprav je za grupo $\mathbb{Z}_2$ očitno, da ni prosto generirana. Za obrat potrebujemo tako v splošnem, poleg drevesne strukture, dodati predpostavko, da elementi množice S ne tvorijo ciklov dolžine 2.

Izrek 4. *Naj bo G grupa in naj bo $S \subseteq G$ množica generatorjev grupe G. Dodatno naj za vsaka elementa $s, t \in S$ velja $s \cdot t \neq e$. Če je Cayleyjev graf $Cay(G, S)$ drevo, potem S prosto generira G.*

Dokaz. Naj bo G grupa in množica $S \subseteq G$ takšna, da velja predpostavka izreka. Dokažimo izomorfizem grup G in $F(S)$.

Ker je $F(S)$ prosto generirana z S, nam univerzalna lastnost prostih grup že nudi obetavnega kandidata za izomorfizem: to je homomorfizem φ_j, ki ga dobimo z razširitvijo vložitve $j\colon S \hookrightarrow G$. Ker po predpostavki S generira G, sledi, da je φ_j surjektiven.

Injektivnost preslikave φ_j dokazujemo s protislovjem. Denimo, da homomorfizem φ_j ni injektiven. Potem obstaja neka okrajšana beseda, ki se slika v enoto. Naj bo $s_1 \dots s_n \in F(S) \setminus \{\varepsilon\}$ najkrajša beseda, ki se slika v enoto $\varphi_j(s_1 \dots s_n) = e$. Ker je φ_j na S identiteta, v grupi G velja $s_1 \dots s_n = e$.

Ločimo primere.

1. Če je $n = 1$, velja $e \in S$, kar je v nasprotju s predpostavko.
2. Če je $n = 2$, potem
$$s_1 s_2 = e.$$
Po definiciji grupe $F(S)$ velja $s_1, s_2 \in S \cup S^{-1}$. Držati mora ena izmed naslednjih možnosti:
   (a) Ali $s_1, s_2 \in S$, kar je v protislovju s predpostavko, da za vsak $s, t \in S\colon s \cdot t \neq e$.
   (b) Ali $s_1, s_2 \in S^{-1}$, kar pomeni $s_1^{-1}, s_2^{-1} \in S$ in velja $s_2^{-1} s_1^{-1} = e$, kar je nemogoče kot v prejšnji točki.
   (c) Ali $s_1 \in S$ in $s_2 \in S^{-1}$, zato $s_2 = s_1^{-1}$ in dosežemo protislovje z dejstvom, da je $s_1 s_2$ okrajšana beseda.

3. Če je $n \geq 3$, v $Cay(G, S)$ začnemo v vozlišču e ter se po povezavah $s_1, \ldots, s_n$ sprehodimo preko vozlišč $g_0, \ldots, g_n$ kjer

$$g_0 = e,$$
$$g_i = g_{i-1}s_i.$$

Ker je $s_1 \ldots s_n$ najkrajša okrajšana beseda, so vozlišča $g_0, \ldots, g_n$ različna. Če bi za neka $i < j$ veljajo $g_i = g_j$, bi sledilo

$$g_i = g_i s_{i+1} s_{i+2} \ldots s_j,$$
$$e = s_{i+1} s_{i+2} \ldots s_j$$

in beseda $s_{i+1}s_{i+2} \ldots s_j$ bi bila krajša beseda, ki se slika v enoto. Zaporedje vozlišč $g_0, \ldots, g_n$ je torej cikel, kar je protislovno s predpostavko, da je $Cay(G, S)$ drevo.

Torej je φ_j injektiven in kot tak res izomorfizem med grupama G in $F(S)$.

■

5. Delovanje grup na grafih

Izrek 4 nam pove, da je grupa G prosta natanko tedaj, ko lahko izberemo množico generatorjev S, da je pripadajoči Cayleyjev graf $Cay(G, S)$ drevo, vendar velja še več. Preden formuliramo naš glavni izrek, potrebujemo še pojem delovanja grupe na grafu.

Definicija 3 (Delovanje na grafu). Naj bo G grupa in X graf. **Delovanje** grupe G na grafu X je homomorfizem grup $\rho\colon G \to Aut(X)$, ki vsakemu elementu $g \in G$ priredi ustrezni avtomorfizem $\rho_g\colon X \to X$, da velja

$$\rho_g \circ \rho_h = \rho_{gh}$$

za poljubna $g, h \in G$. Standardna oznaka za delovanje je $g \cdot v = \rho_g(v)$.

Za takšno delovanje pravimo, da je **prosto**, če za vsak $g \in G \setminus \{e\}$ velja:

- za vsak $v \in V\colon \rho_g(v) \neq v$ in
- za vsak $\{v, v'\} \in E\colon \{\rho_g(v), \rho_g(v')\} \neq \{v, v'\}$

tj. če za avtomorfizem prirejen poljubnemu elementu g nobeno vozlišče in nobena povezava ni slikana sama vase.

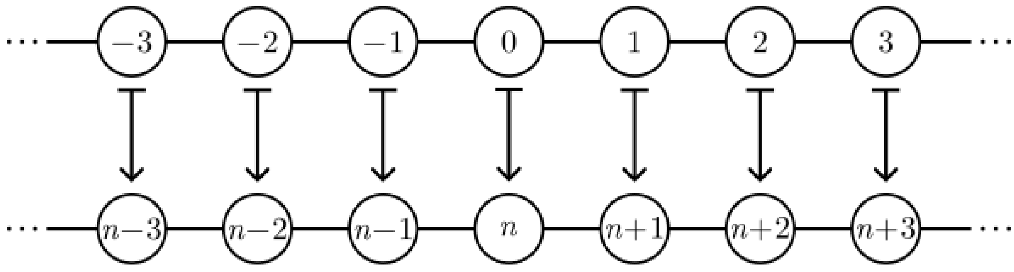
Tekom članka bomo sprva za namene formalizma koristili oznako ρ_g, kasneje pa preskočili na splošno uporabljeno standardno oznako.

Vsaka grupa deluje sama nase z levim množenjem $\rho_g(v) = gv$ za $v \in G$. Delovanje grupe G nase se tako naravno razširi na delovanje grupe G na svojem Cayleyjevem grafu $Cay(G, S)$.

Zgled 4. Oglejmo si naravno delovanje grupe $\mathbb{Z}_6$ na grafih $Cay(\mathbb{Z}_6, S_1)$ in $Cay(\mathbb{Z}_6, S_2)$, ki smo ju obravnavali v zgledu 1. V obeh primerih je delovanje defnirano kot $\rho_n(v) = n + v$. Delovanje na $Cay(\mathbb{Z}_6, S_1)$ si lahko predstavljamo kot rotacijo grafa za kot $n\frac{\pi}{3}$. Očitna posledica je dejstvo, da delovanje na $Cay(\mathbb{Z}_6, S_1)$ nima stacionarnih vozlišč ali povezav. Na grafu $Cay(\mathbb{Z}_6, S_1)$ analogija z rotacijo za kot $n\frac{2\pi}{3}$ deluje za $n = 0, 2, 4$ medtem ko v primeru $n = 1, 3$ zamenjamo notranji in zunanji krog grafa, pri čemer povezave $\{0, 3\}$, $\{1, 4\}$ in $\{2, 5\}$ slikamo same vase.

Dejstvo, da je delovanje prosto, torej ni vedno izpolnjeno. Videli bomo, da je to močna lastnost, ki opisuje pomembno vrsto delovanj, značilno za proste grupe.

Zgled 5. Naravno delovanje grupe $\mathbb{Z}$ na grafih $Cay(\mathbb{Z}, S_1)$ in $Cay(\mathbb{Z}, S_2)$ je podano z isto formulo kot v prejšnjem zgledu. S preprostim izračunom se prepričamo, da velja $\rho_n(v) = v$ natanko v primeru $n = 0$. Grafično si delovanje lahko predstavljamo kot translacijo Cayleyjevega grafa (slika 4) za n mest v desno.



Slika 4. Delovanje $\mathbb{Z}$ na $Cay(\mathbb{Z}, \{1\})$

Ker v obeh primerih velja $\{\rho_n(a), \rho_n(b)\} = \{n + a, n + b\} \neq \{a, b\}$ za poljubno povezavo $\{a, b\}$, tudi to delovanje nima stacionarnih vozlišč ali povezav.

Zgled 6. Naj prosta grupa $F(S)$ deluje na grafu $Cay(F, S)$ z levim množenjem. Ker je beseda gx vedno različna od besede x, če le beseda g ni prazna beseda ε, delovanje ne fiksira vozlišč. Podobno, če bi ρ_g povezavo $\{x, y\}$ slikal vase, bi to pomenilo, da je $gx = y$ in $gy = x$ oziroma $g^2 y = y$, torej $g^2 = \varepsilon$, kar pa ne more držati, saj proste grupe ne vsebujejo elementov končnega reda.

Zadnji zgled nam pove, da je delovanje z levo translacijo na Cayleyjevih grafih prostih grup vedno prosto, medtem ko je za neproste grupe prostost naravnega delovanja na Cayleyjevih grafih odvisna od izbrane množice generatorjev. Če pri tvorjenju Cayleyjevega grafa množica S vsebuje element s reda 2, bomo pri kanoničnem delovanju z elementom s fiksirali povezavo $\{e, s\}$ in delovanje ne bo prosto. Premišljena zahteva je potrebna in tudi zadostna, da naravno delovanje postane prosto.

Izrek 5. *Naj bo G grupa in S neka množica generatorjev grupe G. Delovanje G na $Cay(G, S)$ z levo translacijo $g \cdot v = gv$ je prosto natanko tedaj, ko S ne vsebuje elementov reda 2.*

Dokaz. Ker velja $gv = v \iff g = e$, je naravno delovanje grupe G na vozliščih $Cay(G, S)$ vedno prosto. Dovolj je torej, da dokažemo ekvivalenco drugega dela definicije.

Najprej pokažimo, da iz tega, da v S obstaja element reda 2, sledi, da delovanje ni prosto. Naj bo $s \in S$ reda 2. Pri delovanju G na $Cay(G, S)$ velja

$$s \cdot \{e, s\} = \{s \cdot e, s \cdot s\} = \{s, s^2\} = \{s, e\}.$$

Pokažimo še, da v primeru, ko delovanje ni prosto, S vsebuje element reda 2. Naj bo $g \in G$ in naj bo $\{v, v'\}$ povezava v $Cay(G, S)$, za katero velja $\{v, v'\} = \{g \cdot v, g \cdot v'\}$. Iz enakosti množic ločimo dva primera:

1. Če je $g \cdot v = v$ in $g \cdot v' = v'$, to implicira $g = e$.

2. Če je $g \cdot v = v'$ in $g \cdot v' = v$, po definiciji sosednosti v $Cay(G, S)$ obstaja $s \in (S \cup S^{-1}) \setminus \{e\}$, da je $v' = vs$. Sledi:

$$v = g \cdot v' = g \cdot (vs) = g(vs) = (gv)s = (g \cdot v)s = (v')s = (vs)s = vs^2$$

Če zdaj z leve množimo z v^{-1}, dobimo želeno enakost $e = s^2$. Torej je s iskani element reda 2.

■

S teorijo, ki smo jo do sem izpeljali, smo že skoraj pripravljeni podati opis prostih grup z njihovim delovanjem na drevesih. Od zaključka nas loči le še naslednji pojem.

Definicija 4 (Vpeto drevo delovanja). Naj grupa G deluje na povezanem grafu X. **Orbita** vozlišča $v \in X$ tega delovanja je množica

$$G \cdot v = \{g \cdot v \mid g \in G\}.$$

Vpeto drevo delovanja grupe G na X je podgraf $T \subseteq X$, ki je drevo in vsebuje natanko eno vozlišče iz vsake orbite vozlišč.

Izrek 6. *Vsako delovanje grupe na povezanem grafu ima vpeto drevo delovanja.*

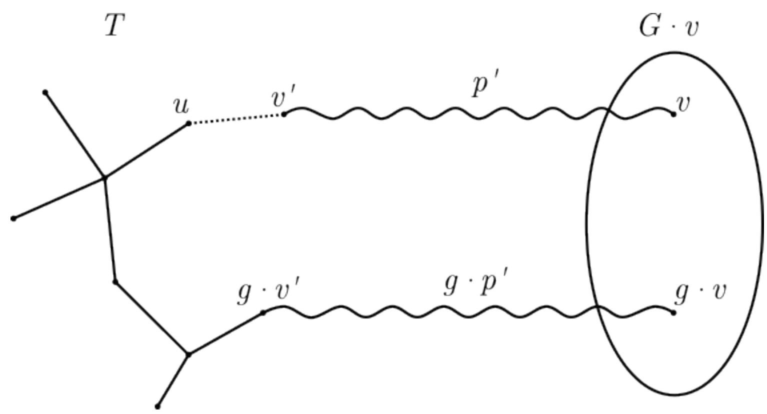
Dokaz. Naj bo G grupa, ki deluje na povezanem grafu X. Brez škode za splošnost je X neprazen, saj je drugače prazno drevo iskano vpeto drevo delovanja. Naj bo T_G družina poddreves X, ki vsebujejo največ en element vsake orbite delovanja G. Družina T_G je delno urejena za relacijo podgrafa, neprazna (vsebuje prazno drevo), vsaka veriga v T_G pa ima zgornjo mejo (unijo vseh elementov verige). Po Zornovi lemi sledi, da T_G vsebuje maksimalni element T. Ker je X neprazen, je tudi T neprazen.

Denimo, da T ni vpeto drevo delovanja. Naj bo potem v_0 vozlišče, za katerega noben element orbite $G \cdot v_0$ ni v T in ima soseda $u \in T$. Takšno vozlišče obstaja zaradi naslednjega sklepa.

Ker smo predpostavili, da T ni vpeto drevo delovanja, mora obstajati vozlišče v, za katero nobeno od vozlišč v orbiti $G \cdot v$ ni vsebovano v T. Ker je X povezan obstaja pot p, ki povezuje neko vozlišče $u \in T$ z v. Naj bo v' prvo vozlišče v poti p, da $v' \notin T$. Ločimo dva primera:

1. Nobeno izmed vozlišč v $G \cdot v'$ ni v T. Lahko vzamemo $v_0 := v'$.

2. Obstaja $g \in G$, da $g \cdot v' \in T$. Označimo s p' pot med v' in v, ter z $g \cdot p'$ pot med $g \cdot v'$ in $g \cdot v$, kjer smo vsako vozlišče poti p' "premaknili" z delovanjem g. Ker je tako premaknjen $g \cdot v' \in T$, pot $g \cdot p'$ pa krajša od poti p, lahko postopek induktivno nadaljujemo, dokler ne najdemo želenega vozlišča (vozlišče zagotovo najdemo, ker za v noben element $G \cdot v$ ni v T).



Slika 5. Konstrukcija poti $g \cdot p'$

Če drevesu T dodamo vozlišče v_0 in povezavo $\{u, v_0\}$, dobimo drevo v T_G, ki vsebuje T kot pravo poddrevo, kar je protislovno s trditvijo Zornove leme, da je T maksimalno. Torej je T vpeto drevo delovanja grupe G na povezanem grafu X.

■

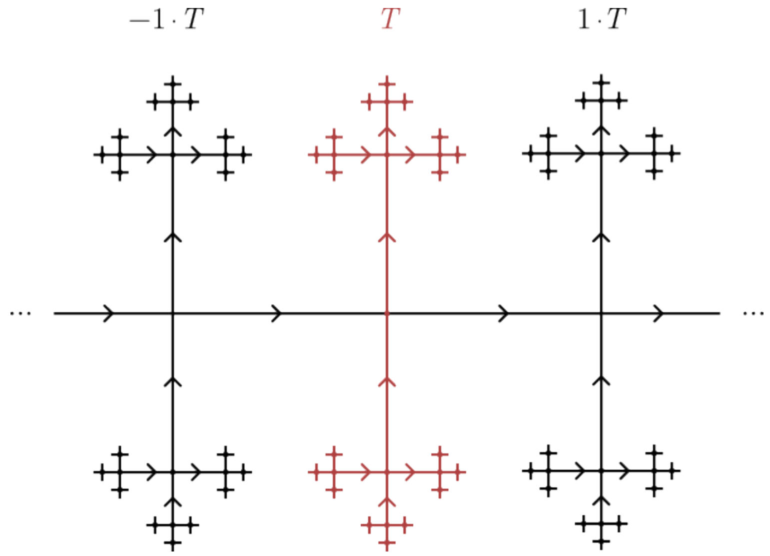
Izrek nam zagotovi obstoj vpetega drevesa delovanja, vendar ne pove, kako takšno drevo najdemo. Za boljšo predstavo si oglejmo nekaj primerov.

Zgled 7. Naj bo $F(S)$ prosta grupa ranga 2 generirana z množico $S = \{a, b\}$. Naj $F(S)$ deluje na svoj Cayleyjev graf $Cay(F, S)$ z levim množenjem. Za vsak element $s \in F(S) \setminus \{\varepsilon\}$ velja $s \cdot \varepsilon = s$, torej ima delovanje samo eno orbito $F(S) \cdot \varepsilon = F(S)$. Vpeto drevo delovanja je torej $T = \{s\}$, kjer je s poljuben element grupe $F(S)$.

Argument iz zgornjega zgleda ne velja samo za proste grupe. Enako velja, da ima naravno delovanje poljubne grupe G na svoj Cayleyjev graf $Cay(G, S)$ samo eno orbito. Vpeto drevo naravnega delovanja je torej eno samo vozlišče.

Zgled 8. Oglejmo si delovanje grupe $\mathbb{Z}$ na Cayleyjev graf proste grupe z dvema generatorjema $Cay(F, S)$, kot v prejšnjem zgledu, podano s predpisom $n \cdot s = b^n s$. Orbita elementa x so vsi elementi oblike $b^n x$. Opazimo tudi, da so elementi $\{a^m x \mid m \in \mathbb{Z} \setminus \{0\},\ x \in F(S)\}$ v različnih orbitah. Če bi bila elementa $a^m x$ in $a^k y$ v isti orbiti, bi namreč veljalo $b^n a^m x = a^k y$ za nek $n \neq 0$, kar je očitno protislovno, saj sta prvi črki besed različni. Če imamo v mislih neskončno drevesno strukturo Cayleyjevega grafa $Cay(F, S)$, ki smo jo ilustrirali v zgledu 3, elementi opisane množice sestavljajo natanko tisti del neskončnega drevesa, ki se iz prazne besede ε razteza v navpični smeri (slika 6).

Zgoraj zapisano množico označimo s T in se prepričajmo, da je T vpeto drevo opisanega delovanja. Hitro je razvidno, da vozlišča množice T opisujejo drevo, delovanje elementa $n \in \mathbb{Z}$ na drevo T pa je natanko horizontalna translacija drevesa. Z ustrezno translacijo lahko dosežemo vse elemente $Cay(F, S)$ (vsak element $F(S)$ ima obliko $a^n b^m x$ za nek $x \in F(S)$), torej imamo res natanko en element iz vsake orbite in T je vpeto drevo opisanega delovanja.



Slika 6. Orbite delovanja $\mathbb{Z}$ na $Cay(F, S)$

6. Delovanje prostih grup na drevesih

Glavna opazka prejšnjega poglavja je trdila, da je delovanje prostih grup na pripadajočih Cayleyjevih grafih vedno prosto. Ker vemo, da so Cayleyjevi grafi prostih grup ob primerni izbiri generatorjev drevesa, opazka pravi, da za vsako prosto grupo obstaja neprazno drevo, na katerem grupa prosto deluje. Bolj presenetljivo dejstvo je, da ta lastnost ni le potrebna, temveč tudi zadostna za prepoznavanje prostih grup.

Natančneje, če imamo grupo G, za katero obstaja neprazno drevo, na katerem lahko definiramo prosto delovanje, je grupa G prosta. Še več, če poznamo vpeto drevo tega delovanja, nam dokaz pove, kako najdemo množico S, ki prosto generira G.

Izrek 7. *Grupa je prosta natanko tedaj, ko ima neko prosto delovanje na nepraznem drevesu.*

Dokaz. Najprej dokažimo, da ima vsaka prosta grupa prosto delovanje na nepraznem drevesu. Naj bo F prosta grupa, prosto generirana z množico $S \subset F$. Po izreku 3 je njen Cayleyjev graf $Cay(F, S)$ (neprazno) drevo. Po izreku 5 je delovanje F na $Cay(F, S)$ z levo translacijo prosto natanko tedaj, ko v S ni elementa reda 2. Ker proste grupe ne vsebujejo elementov končnega reda, sledi, da je delovanje proste grupe F na drevesu $Cay(F, S)$ z levo translacijo prosto.

Dokažimo še obrat. Naj ima grupa G neko prosto delovanje na drevesu T in naj bo T' vpeto drevo tega delovanja, ki ga zagotavlja izrek 6. Z besedno zvezo **bistvene povezave** drevesa T poimenujmo povezave $\{u, v\}$, za katere je natanko en element v drevesu T'.

V naslednjem koraku dokaza bomo konstruirali množico $S \subset G$, ki bo prosto generirala G. Naj bo $b = \{u, v\}$ bistvena povezava drevesa T, za katero je $u \in T'$ in $v \notin T'$. Ker je T' vpeto drevo delovanja, obstaja element $g_b \in G$, da je $g_b^{-1} \cdot v \in T'$. Dodatno, ker orbita $G \cdot v$ vsebuje natanko en element v T' in ker G prosto deluje na T, sledi, da je g_b enolično določen. Zaradi dejstva, da T' vsebuje natanko en element iz orbite $G \cdot u$, velja tudi $g_b^{-1} \cdot u \notin T'$.

Definirajmo
$$\widetilde{S} := \{g_b \in G \mid b \text{ je bistvena povezava } T\}.$$

Za množico $\widetilde{S}$ velja:

1. Po konstrukciji enota grupe G ni vsebovana v $\widetilde{S}$.

2. $\widetilde{S}$ ne vsebuje elementov reda 2.

   Če je $g_b \in \widetilde{S}$ prirejen bistveni povezavi $b = \{u, v\}$ reda 2, tj. $g_b^{-1} = g_b$, povezavo b slika v $g_b \cdot b = \{g_b \cdot u, g_b \cdot v\}$, kjer je $g_b \cdot v \in T'$

   (a) Če je $g_b \cdot v = u$, mora veljati tudi $v = g_b \cdot (g_b \cdot v) = g_b \cdot u$. Sledi $g_b \cdot b = b$, kar je v nasprotju s predpostavko o prostem delovanju.

   (b) Če je $g_b \cdot v \neq u$, znotraj T' obstaja pot med u in $g_b \cdot v$, znotraj $g_b \cdot T'$ pa obstaja pot med $g_b \cdot u$ in v. V kombinaciji s povezavama b in $g_b \cdot b$ to implicira cikel v T, kar je v nasprotju s predpostavko, da je T drevo.

3. Če sta b in b' bistveni povezavi, za kateri sta $g_b = g_{b'}$, potem $b = b'$. Podobno kot v (b) zgoraj, če sta b in b' različni povezavi med T' in $g_b \cdot T' = g_{b'} \cdot T'$, to implicira cikel v drevesu T.

4. Če je $g \in \widetilde{S}$, denimo $g = g_b$ za neko bistveno povezavo b, potem je tudi $g^{-1} \cdot b$ bistvena povezava in $g^{-1} = g_{g^{-1} \cdot b} \in \widetilde{S}$.

   Z drugimi besedami, obstaja podmnožica $S \subset \widetilde{S}$, da velja:

$$S \cap S^{-1} = \emptyset \qquad \text{in} \qquad |S| = \frac{|\widetilde{S}|}{2} = \frac{1}{2} \cdot \text{ število bistvenih povezav } T.$$

Pokazati moramo še, da $\widetilde{S}$ (in posledično S) *generira* G. Naj bo $g \in G$ poljuben element in $v \in T'$ poljubno vozlišče. Ker je T povezan, v njem med vozliščema v in $g \cdot v$ obstaja pot p. Pot p gre skozi več kopij T'. Označimo s $g_0 \cdot T', \ldots, g_n \cdot T'$ zaporedne kopije T', skozi katere vodi p, tako da velja $g_0 = e$, $g_n = g$ in $g_i \neq g_{i+1}$ za vsak $i \in \{0, \ldots, n-1\}$. Kopiji $g_j \cdot T'$ in $g_{j+1} \cdot T'$, kjer $j \in \{0, \ldots, n-1\}$, sta povezani z neko povezavo b_j. Če označimo $b_j = \{g_j \cdot u, g_{j+1} \cdot v\}$ za neka $u, v \in T'$, vidimo, da je $g_j^{-1} \cdot b_j = \{u, g_j^{-1} g_{j+1} \cdot v\}$ bistvena povezava, kateri smo v $\widetilde{S}$ priredili element
$$s_j = g_j^{-1} g_{j+1}.$$

Velja

$$\begin{aligned} g = g_n &= g_0^{-1} g_n \\ &= g_0^{-1} g_1 g_1^{-1} g_2 \cdots g_{n-1}^{-1} g_n \\ &= s_0 s_1 \cdots s_{n-1}, \end{aligned}$$

torej g pripada podgrupi generirani z elementi $\widetilde{S}$. Ker je bil g poljuben, sledi, da $\widetilde{S}$ generira G.

V konstrukciji smo uporabili bijekcijo med elementi grupe G in kopijami drevesa $g \cdot T'$, da smo v drevesu T prepoznali strukturo Cayleyjevega grafa $Cay(G, \widetilde{S}) = Cay(G, S)$. Ostane nam le še premislek, da $S \subset \widetilde{S}$, ki smo ga definirali zgoraj, *prosto* generira G. Po izreku 4 zadošča dokazati, da $Cay(G, S)$ ne vsebuje ciklov (predpostavki da za vsak $s, t \in S$: $s \cdot t \neq e$ smo zadostili z izbiro podmnožice $S \subset \widetilde{S}$).

Denimo, da obstaja $n \in \mathbb{N}$, $n \geq 3$, za katerega v $Cay(G, S)$ obstaja cikel $g_1, \ldots, g_n$. Povezava $\{g_i, g_{i+1}\}$ nam pove, da je element $s_i := g_i^{-1} g_{i+1}$ v množici $\widetilde{S}$. Posebej, zaradi povezave $\{g_n, g_0\}$ velja, da je $s_n := g_n^{-1} g_0$ v $\widetilde{S}$. Po definiciji množice $\widetilde{S}$ za vsak $s \in \widetilde{S}$ obstaja povezava med T' in $s \cdot T'$ v drevesu T. Natančneje, za vsak $i \in \{0, \ldots, n\}$ obstaja povezava med T' in $s_i \cdot T'$, ki ima obliko $\{u, s_i \cdot v\} = \{u, g_i^{-1} g_{i+1} \cdot v\}$ za neka $u, v \in T'$. Z delovanjem z g_i se ta povezava preslika v povezavo $g_i \cdot \{u, g_i^{-1} g_{i+1} \cdot v\} = \{g_i \cdot u, g_{i+1} \cdot v\}$ med drevesoma $g_i \cdot T'$ in $g_{i+1} \cdot T'$. Posebej za $i = n$ dobimo povezavo med $g_n \cdot T'$ in $g_0 \cdot T'$. Ker so drevesa povezana, konstruirani cikel med kopijami drevesa T' inducira cikel elementov v drevesu T, kar vodi v protislovje.

■

Izpeljani izrek poda zelo elegantno orodje za opis podgrup proste grupe F. Na prvi pogled struktura podgrup F ni tako očitna, naključno izbrana množica generatorjev podgrupe H bo v splošnem imela medsebojne relacije. Kljub temu pa je prostost podgrup razvidna, če upoštevamo, da podgrupa H podeduje prosto delovanje.

Posledica 8. *Podgrupe prostih grup so proste.*

Dokaz. Naj bo F prosta grupa in $H \subseteq F$ njena podgrupa. Ker je grupa F prosta, ima neko prosto delovanje na nepraznem drevesu T. Inducirano delovanje podgrupe H na drevesu T mora biti prav tako prosto, kar je po izreku 7 ekvivalentno temu, da je H prosta grupa.

■

Angleško-slovenski slovar strokovnih izrazov

Cayley graph Cayleyjev graf

essential edge bistvena povezava

free action prosto delovanje

free generating set množica, ki prosto generira

free group prosta grupa

group action delovanje grupe

universal property univerzalna lastnost

reduced word okrajšana beseda

spanning tree of an action vpeto drevo delovanja

LITERATURA

[1] Clara Löh. *Geometric Group Theory: An Introduction.* Springer International Publishing, 2017.