Kompleksnost in algoritmični problemi v teoriji krovnih grafov

Rok Požar

doktorska disertacija

predana

Fakulteti za računalništvo in informatiko

kot del izpolnjevanja pogojev za pridobitev naziva

doktor znanosti

s področja

računalništva in informatike

Ljubljana, 2013

IZJAVA

Izjavljam, da sem avtor doktorske disertacije z naslovom Kompleksnost in algoritmični problemi v teoriji krovnih grafov, ki sem jo izdal samostojno pod vodstvom mentorja in somentorja, in da slednje ne vsebuje materiala, ki bi ga kdorkoli predhodno že objavil ali oddal v obravnavo za pridobitev naziva na univerzi ali na drugem visokošolskem zavodu, razen v primerih, kjer so navedeni viri. Soglašam z javno objavo elektronske oblike doktorske disertacije, ki je identična s tiskano obliko doktorske disertacije.

— Rok Požar —

september 2013

Oddajo so odobrili

dr. Aleksander Malnič

profesor za matematiko

mentor in član ocenjevalne komisije

dr. Andrej Brodnik

docent za računalništvo in informatiko

somentor in član ocenjevalne komisije

dr. Neža Mramor Kosta

profesorica za računalništvo in informatiko

predsednica ocenjevalne komisije

dr. Martin Milanič

docent za matematiko

zunanji član ocenjevalne komisije

Univerza na Primorskem

PREDHODNA OBJAVA

Izjavljam, da so bili rezultati obravnavane raziskave predhodno objavljeni/sprejeti za objavo v recenzirani reviji ali javno predstavljeni v naslednjih primerih:

[1] A. Malnič and R. Požar. On the Split Structure of Lifted Groups. Poslano v objavo.

[2] A. Malnič and R. Požar. On the Split Liftings with Sectional Complements. Poslano v objavo.

[3] R. Požar. Sectional split extensions arising from lifts of groups. *Ars Math. Contemp.*, 6:393–408, 2013.

[4] R. Požar. Some computational aspects of solvable regular covers of graphs, Poslano v objavo.

Potrjujem, da sem pridobil pisna dovoljenja vseh lastnikov avtorskih pravic, ki mi dovoljujejo vključitev zgoraj navedenega materiala v pričujočo disertacijo. Potrjujem, da zgoraj navedeni material opisuje rezultate raziskav, izvedenih v času mojega podiplomskega študija na Univerzi v Ljubljani.

Univerza *v Ljubljani*
Fakulteta *za računalništvo in informatiko*
Rok Požar
Kompleksnost in algoritmični problemi v teoriji krovnih grafov

POVZETEK

Krovne tehnike so močno orodje v različnih vejah znanosti – poleg matematike predvsem tam, kjer se srečamo s problemom predstavitve in študija strukturnih lastnosti velikih kombinatoričnih objektov. Pomembna lastnost krovnih grafov je, da lahko vso informacijo o (običajno) velikem krovnem grafu predstavimo na (relativno) majhnem baznem grafu, ki jo zakodiramo s tako imenovanimi napetostmi na usmerjenih povezavah; študij strukturnih lastnosti krovnih grafov pa se pogosto prevede na študij distribucije napetosti na baznem grafu. Kombinatorične tehnike, razvite v ta namen, slonijo predvsem na konceptu dviga avtomorfizmov vzdolž krovnih projekcij.

Cilj disertacije je dvojen: po eni strani razviti ustrezne algoritme za reševanje nekaterih naravnih problemov v zvezi z dvigi avtomorfizmov, po drugi strani pa razviti programski paket, ki bo to omogočil v praksi. Predstavljen je učinkovit algoritem za testiranje, kdaj se dani avtomorfizem dvigne vzdolž kombinatorično podane krovne projekcije. Razviti so algoritmi za analizo strukture dvignjene grupe vzdolž regularne krovne projekcije, podane kombinatorično prek napetosti: algoritem, ki poišče prezentacijo dvignjene grupe, algoritem za testiranje razcepnosti dvignjene grupe kot razširitve grupe krovnih transformacij in algoritem za testiranje prerezne razcepnosti dvignjene grupe kot razširitve grupe krovnih transformacij. Algoritmi so zasnovani tako, da se izognejo eksplicitni konstrukciji tako krovnega grafa kot dvignjene grupe. Slednje je namreč v splošnem časovno in prostorsko zahteven problem. Predstavljene so še metode za konstrukcijo krovnih projekcij, vzdolž katerih se dana podgrupa avtomorfizmov dvigne. Posebej je opisana metoda za konstrukcijo regularnih krovnih projekcij, vzdolž katerih se dana podgrupa avtomorfizmov dvigne kot prerezna razcepna razširitev.

Ključne besede: algoritem, delovanje grupe, dvig avtomorfizma, graf, krovna projekcija, napetostna grupa, prezentacija grupe, razširitev grupe

University *of Ljubljana*
Faculty *of Computer and Information Science*
Rok Požar
Complexity and algorithmic aspects in the theory of graph covers

ABSTRACT

Apart from mathematics, covering techniques have long been known as a powerful tool in different areas of science, especially in those fields dealing with representation and analysis of large structural objects. In such a context, one of the key properties of graph covers is that all the information about a (usually) large covering graph can be encoded by means of voltages assigned to directed edges of a (relatively) small base graph. In addition, the study of structural properties of covering graphs often reduces to the study of voltage distribution on the base graph. Combinatorial techniques developed for this purpose are based on the concept of lifting automorphism along covering projections.

The aim of this Thesis is twofold. Firstly, to develop adequate algorithms for solving certain natural problems regarding lifting automorphisms. And secondly, to provide an appropriate software package for practical usage. An efficient algorithm for testing whether a given automorphism lifts along a covering projection, given in terms of voltages, is presented. Further, algorithms for analysing the structure of lifted groups along combinatorially given regular covering projection are developed: an algorithm for finding a presentation of the lifted group, an algorithm for testing whether the lifted group is a split extension, and algorithm for testing whether the lifted group is a sectional split extension. All algorithms avoid explicit constructions of the covering graph as well as of the lifted group, since such constructions are time and space consuming in general. In addition, methods for generating those covering projections along which a given group of automorphisms lifts, are presented. In particular, a method for finding regular covering projections along which a given group of automorphisms lifts as a sectional split extension, is given.

Key words: algorithm, covering projection, graph, group action, group extension, group presentation, lifting automorphism, voltage group

ZAHVALA

Iskrena hvala mentorju prof. dr. Aleksandru Malniču, somentorju dr. Andreju Brodniku, prof. dr. Marstonu Conderju in prof. dr. Primožu Potočniku!

— Rok Požar, Ljubljana, september 2013.

KAZALO

I

Uvod

Krovna projekcija $\wp\colon \tilde{X} \to X$ je surjektivni homomorfizem grafa $\tilde{X}$ na graf X, ki je lokalna bijekcija na okolicah vozlišč. Grafu $\tilde{X}$ rečemo *krovni graf* nad *baznim grafom* X. Koncept krovnega grafa se je izkazal za močno orodje v različnih vejah znanosti – poleg matematike predvsem tam, kjer se srečamo s problemom predstavitve in študija strukturnih lastnosti velikih kombinatoričnih objektov. Na področju strukturne kemije, na primer, se krovni grafi uporabljajo za predstavitev in študij kristalnih mrež [1, 2]. V računalništvu pa igrajo pomembno vlogo med drugim pri konstrukciji in analizi kod [3, 4], pri modeliranju računalniških omrežij [5–8] ter pri študiju povezav med socialnimi omrežji [9, 10].

Dve ključni lastnosti krovnih grafov sta naslednji. Prvič, vso informacijo o (običajno) velikem krovnem grafu lahko predstavimo na (relativno) majhnem baznem grafu, ki jo je mogoče zakodirati s pomočjo tako imenovanih napetosti na usmerjenih povezavah [11, 12]. In drugič, krovni graf ohranja „lokalne lastnosti“ baznega grafa – v tem smislu lahko določene lastnosti krovnega grafa analiziramo na podlagi lastnosti baznega grafa.

Če želimo, da na krovni graf vplivajo tudi kakšne „globalne lastnosti“ baznega grafa, je običajno potrebno zahtevati, da krovni graf podeduje tudi kake simetrijske lastnosti. Študij simetrijskih lastnosti krovnih grafov je mogoče prevesti na študij distribucije napetosti na baznem grafu, kombinatorične tehnike, ki so bile razvite v ta namen, pa slonijo predvsem na konceptu dviga avtomorfizmov [13–15]. Pri tem je avtomorfizem $\tilde{g}$ krovnega grafa $\tilde{X}$ *dvig* avtomorfizma g baznega grafa X vzdolž krovne projekcije $\wp\colon \tilde{X} \to X$, če velja $\wp\,\tilde{g} = g\,\wp$. To pomeni, da avtomorfizem $\tilde{g}$ vsako *vlakno* (prasliko vozlišča) bijektivno preslika na neko drugo ustrezno vlakno; preslikava vlaken porodi na baznem grafu avtomorfizem g. Iz tega lahko nazorno vidimo, kako simetrija baznega grafa porodi simetrijo krovnega grafa. Bolj splošno rečemo, da se podgrupa G avtomorfizmov grafa X dvigne, če se dvignejo vsi njeni elementi. Vsi dvigi elementov iz G tvorijo *dvig* grupe G, ki je podgrupa $\tilde{G}$ v grupi avtomorfizmov krovnega graf $\tilde{X}$. Posebej, dvig trivialne grupe je *grupa krovnih transformacij* $CT(\wp)$.

Teorija krovnih grafov je z algoritmičnega vidika še pretežno neobdelana, zato je to atraktivno raziskovalno področje. V disertaciji obravnavamo algoritmične probleme v zvezi s simetrijskimi lastnostmi krovnih grafov.

1.1 Raziskovalna motivacija in cilji

V teoretičnem smislu je področje krovnih grafov precej dobro obdelano. Motivacija za vpeljavo samega koncepta v začetku 70. let prejšnjega stoletja [16] se je prvotno navezovala na tehnike, ki so leta 1968 privedle do dokončne rešitve znamenite Heawoodove domneve iz leta 1890 o barvanju zemljevidov na sklenjenih ploskvah. Neodvisno in hkrati s tem pa so se krovne tehnike pokazale tudi kot učinkovito orodje pri proučevanju strukturnih lastnosti grafov s predpisanimi simetrijskimi lastnostmi, torej pri klasifikaciji, konstrukciji in katalogizaciji nekaterih neskončnih družin. O tem priča vrsta člankov v zadnjih dvajsetih letih, glej recimo [11, 13, 17–29] in tam citirane reference.

Kot že omenjeno, pa se je manj pozornosti doslej posvečalo algoritmičnim vidikom, tako glede kompleksnosti kot tudi njihove implementacije. Doslej znani rezultati se pretežno nanašajo na posebno podpodročje razpoznavanja krovov: ali obstaja krovna projekcija med danima grafoma? Problem je v splošnem *NP*-poln. Pomemebne rezultate v zvezi z razpoznavanjem krovov je dosegla skupina s Karlove univerze v Pragi [25, 26, 30, 31]. Precej neraziskano pa je področje algoritmov, ki bi podali odgovore na določena naravna vprašanja v zvezi s simetrijskimi lastnostmi grafov in njihovih krovov.

Eno osrednjih vprašanj v tem kontekstu se navezuje na problem dviga avtomorfizmov vzdolž krovnih projekcij: ali se dana grupa avtomorfizmov G baznega grafa X dvigne vzdolž dane krovne projekcije $\wp\colon \tilde{X} \to X$ do grupe avtomorfizmov $\tilde{G}$ krovnega grafa X? Posebne pozornosti so bili doslej deležni potrebni in zadostni pogoji za obstoj dviga v kombinatoričnem smislu [14, 15, 32, 33]. Vendar pa ti splošni rezultati ne zagotavljajo zadovoljivih tehnik, s katerimi bi lahko učinkovito reševali konkretne primere. V prvi vrsti je zato potrebno razviti algoritem za testiranje dviga avtomorfizmov vzdolž krovne projekcije, podane kombinatorično prek napetosti. Nekaj načelnih opomb o problemu dviga avtomorfizmov z algoritmičnega vidika je moč najti v [34].
Cilj I. Razvoj algoritma za testiranje, kdaj se dana grupa avtomorfizmov G baznega grafa X dvigne vzdolž dane krovne projekcije $\wp\colon \tilde{X} \to X$.

Poleg tega osnovnega problema se lahko vprašamo tudi po strukturi dvignjene grupe, ki lahko razkrije dodatne lastnosti krovnega grafa. Natančneje, če se grupa G dvigne, nas zanima prezentacija dvignjene grupe $\tilde{G}$. Ker lahko krovni graf predstavimo kombinatorično z napetosti, se porodi vprašanje, ali lahko potem poiščemo tudi prezentacijo

dvignjene grupe $\tilde{G}$ že samo preko „obnašanja“ grupe G na napetostih? Pri tem je bistveno to, da niti krovnega grafa niti dvignjene grupe ne zgradimo eksplicitno, ampak problem prevedemo na študij distribucije napetosti na baznem grafu. S tem se praviloma izboljša tako prostorska kot časovna zahtevnost. Ker je dvignjena grupa $\tilde{G}$ vedno razširitev grupe krovnih transformacij $CT(\wp)$ po grupi G, velja uporabiti nekatere ideje, ki so znane iz računske teorije grup.

Cilj II. Razvoj metode za izračun prezentacije dvignjene grupe $\tilde{G}$.

Pogosto nas zanima podroben opis delovanja dvignjene grupe in njenih lastnosti. Tedaj se je naravno vprašati po tipu razširitve dvignjene grupe. Posebni tipi razširitev namreč v veliki meri določajo strukturne lastnosti krovnega grafa. V tem kontekstu si posebno pozornost zaslužijo razcepne razširitve. Po definiciji razcepne razširitve obstaja v grupi $\tilde{G}$ komplement $\overline{G}$ k podgrupi $CT(\wp)$. Pri tem se $\overline{G}$ izomorfno projicira na G vzdolž projekcije $\wp$. To omogoča, da lahko primerjamo delovanji dveh izomorfnih grup: grupe G na baznem grafu X in komplementa $\overline{G}$ na krovnem grafu $\tilde{X}$. Seveda se lahko zgodi, da komplement ni enolično določen – še več, različni komplementi lahko porodijo različna delovanja na $\tilde{X}$. Analiza je torej lahko precej zapletena, zato bi veljalo razviti algoritem za testiranje razcepnosti razširitve.

Cilj III. Razvoj algoritma za testiranje, kdaj je dvignjena grupa $\tilde{G}$ razcepna razširitev grupe krovnih transformacij $CT(\wp)$ po grupi G.

Glede na specifična delovanja, ki jih lahko porodijo komplementi, posebej izstopajo prerezni komplementi. Komplement je *prerezni*, če ima orbito, ki seka vsako vlakno v največ enem vozlišču. Rečemo, da je razcepna razširitev *prerezna*, če obstaja kakšen prerezni komplement. Nekatera posebna vprašanja v zvezi s prereznimi razcepnimi razširitvami so obravnavana v [15, 35–37]. Poleg tega je v [37] grobo opisana tudi metoda za testiranje prerezne razcepnosti razširitve, ki pa v praksi ni učinkovita.

Cilj IV. Razvoj algoritma za testiranje, kdaj je dvignjena grupa $\tilde{G}$ prerezna razcepna razširitev grupe krovnih transformacij $CT(\wp)$ po grupi G.

Posebej težka je (eksplicitna) konstrukcija vseh tistih krovnih projekcij nad danim baznim grafov, vzdolž katerih se izbrana grupa avtomorfizmov dvigne. V zvezi s tem problemom so algoritmi poznani le v primeru, ko je krovna projekcija regularna in je grupa krovnih transformacij elementarno abelska [38, 39]. Krovna projekcija je *regularna*, če grupa krovnih transformacij deluje regularno na vlaknih.

Cilj V. Za dani bazni graf X in njegovo podgrupo avtomorfizmov G razviti algoritem za generiranje vseh krovnih projekcij nad X, vzdolž katerih se G dvigne.

Ker so v aplikacijah pomembne predvsem regularne krovne projekcije, se v doktorski disertaciji ukvarjamo predvsem z algoritmičnimi problemi v zvezi z regularnimi krovnimi projekcijami. Naš namen je dvojen: po eni strani razviti ustrezne algoritme za reševanje opisanih problemov v primeru regularnih krovnih projekcij, po drugi strani pa – ker se že nekaj časa kaže potreba po specializirani programski opremi za delo s krovnimi grafi – razviti programski paket, ki bo to omogočil v praksi. Primerno programsko okolje za implementacijo je Magma [40]. To je zelo široko zastavljen programski paket za izračunavanja v algebri, algebraični geometriji in kombinatoriki. Vsebuje tudi orodja za delo z grafi, ne vsebuje pa paketa za delo s krovnimi grafi. S to implementacijo bo ta pomanjkljivost odpravljena.

1.2 Prispevki k znanosti

Del rezultatov doktorske disertacije je vključen v naslednje znanstvene članke [41–44]. Glavni in originalni prispevki k znanosti so naslednji:

(i) *Razvoj algoritmov za testiranje dviga avtomorfizma vzdolž krovne projekcije.* Za krovno projekcijo, podano kombinatorično prek napetosti, je problem najprej obravnavan v splošnem (glej Algoritem 3.1). Podana je formalna časovna in prostorska analiza (glej Izrek 3.1.6 in Izrek 3.1.7). Nato posebej obravnavamo še regularne krovne projekcije (glej Algoritem 3.2 in Algoritem 3.3). Podana je formalna časovna in prostorska analiza v primeru elementarno abelskih regularnih krovov (glej Izrek 3.2.5).

(ii) *Razvoj metode za iskanje prezentacije dvignjene grupe vzdolž regularne krovne projekcije.* Metoda je zasnovana tako, da se izogne eksplicitni konstrukciji tako krovnega grafa kot tudi dvignjene grupe (glej Razdelek 4.1).

(iii) *Razvoj algoritmov za testiranje, ali je dvignjena grupa vzdolž regularne krovne projekcije razcepna razširitev grupe krovnih transformacij.* Predstavljena je metoda za učinkovito reševanje tega problema v primerih, ko je grupa krovnih transformacij elementarno abelska, abelska ali rešljiva (glej Algoritem 6.2 in Algoritem 6.3). V primeru elementarno abelskih regularnih krovov je podana formalna časovna in prostorska zahtevnost (glej Izrek 6.1.4), medtem ko je v primeru rešljivih regularnih krovov narejena eksperimetalna analiza (glej Razdelek 6.2 in Izrek 6.2.2).

(iv) *Razvoj algoritma za testiranje, ali je dvignjena grupa vzdolž regularne krovne projekcije prerezna razcepna razširitev grupe krovnih transformacij.* Predstavljena je metoda za učinkovito reševanje tega problema v primerih, ko je grupa krovnih transformacij elementarno abelska ali abelska (glej Algoritem 7.3). V primeru elementarno abelskih regularnih krovov je podana formalna časovna in prostorska zahtevnost (glej Izrek 7.3.6).

(v) *Konstrukcija vseh krovnih projekcij nad danim baznim grafov, vzdolž katerih se izbrana grupa avtomorfizmov dvigne.* Krovne projekcije so podane eksplicitno prek napetosti na baznem grafu. Najprej je podana metoda v splošnem (glej Algoritem 5.1), nato še za regularne krovne projekcije (glej Algoritem 5.2). V primeru regularnih krovnih projekcij so posebej obravnavane tiste, ki imajo rešljivo grupo krovnih transformacij (glej Algoritem 5.3).

(vi) *Konstrukcija vseh regularnih krovnih projekcij nad danim baznim grafom, vzdolž katerih se izbrana grupa avtomorfizmov dvigne kot prerezna razcepna razširitev.* Poleg razvoja same metode so klasificirane vse elementarno abelske regularne krovne projekcije nad polnim grafov na štirih vozliščih, vzdolž katerih se ciklična grupa reda štiri dvigne kot prerezna razcepna razširitev (glej Razdelek 7.4).

(vii) *Dostopnost algoritmov za delo s krovnimi grafi v programskem okolju* Magma. Dokumentacija vsebuje tako module za delo s krovnimi grafi nasploh kot tudi algoritme, ki se navezujejo na problem dviga avtomorfizmov. Dokumentacija je javno dostopna (glej spletno stran `http://osebje.famnit.upr.si/~rok.pozar` in priloženo zgoščenko).

Izpostavimo še, da lahko vse metode, razvite za regularne krovne projekcije, ustrezno uporabimo tudi v primeru neregularnih krovnih projekcij.

1.3 Pregled vsebine

Disertacija je vsebinsko razdeljena na osem poglavij. V drugem poglavju so razloženi osnovni koncepti, ki so potrebni za razumevanje vsebine. Poglavje začnemo s pregledom osnovnih pojmov v teoriji grup, teoriji grafov in posebej krovnih grafov. Zaključimo z osnovami analize algoritmov in izračunljivosti.

V tretjem poglavju se posvetimo osnovnemu vprašanju, kdaj se dani avtomorfizem baznega grafa dvigne vzdolž krovne projekcije, podane kombinatorično prek napetosti. Najprej predstavimo učinkovite algoritme v splošnem primeru, nato pa posebno pozornost namenimo še regularnim krovom.

V četrtem poglavju začnemo z analizo strukture dvignjene grupe vzdolž regularne krovne projekcije. Predstavimo metodo, ki prek informacije o distribuciji napetosti poišče prezentacijo dvignjene grupe. Opišemo tudi kombinatorično rekonstrukcijo kompozicije oziroma dekompozicije regularne krovne projekcije.

V petem poglavju opišemo metode za generiranje krovnih projekcij, vzdolž katerih se dana podgrupa avtomorfizmov baznega grafa dvigne. Posebno pozornost namenimo regularnim krovnim projekcijam.

V šestem poglavju nadaljujemo z natančnejšo analizo regularnega dviga. Razvijemo algoritem za testiranje razcepnosti razširitve dvignjene grupe vzdolž regularne krovne projekcije, podane prek napetosti. Poleg tega algoritem eksperimentalno ovrednotimo.

Sedmo poglavje je namenjeno posebnemu primeru prereznih razcepnih razširitev. Najprej razvijemo algoritem za testiranje prerezne razcepnosti razširitve dvignjene grupe vzdolž regularne krovne projekcije. Nato razvijemo metodo za generiranje regularnih krovnih projekcij, vzdolž katerih se dana grupa avtomorfizmov baznega grafa dvigne kot prerezna razcepna razširitev. Metodo ilustriramo na konkretnem zgledu: klasificiramo vse elementarno abelske regularne krovne projekcije nad polnim grafov na štirih vozliščih, vzdolž katerih se ciklična grupa reda štiri dvigne kot prerezna razcepna razširitev.

Povzetek vsebine disertacije in ovrednotenje rezultatov podamo v zadnjem poglavju. Izpostavimo tudi odprte probleme in ideje za nadaljnje delo.

2

Osnovni koncepti

V tem poglavju podamo notacijo in povzamemo osnovne koncepte, ki so potrebni za razumevanje vsebine. Začnemo s pregledom osnovnih pojmov v teoriji grup. Nato podamo formalno definicijo grafa in njegove fundamentalne grupe. Ker je krovni graf tesno povezan z delovanjem fundamentalne grupe, si pogledamo tudi osnovne pojme, povezane z delovanji grup nasploh. Nato podamo formalno definicijo krovnih grafov ter njihove osnovne lastnosti. Poudarek je na kombinatoričnem opisu krovnih grafov, kar nam v nadaljevanju omogoči študij z algoritmičnega vidika. Nadaljujemo s konceptom dviga avtomorfizmov, zaključimo pa z analizo algoritmov in izračunljivostjo.

Osnovne pojme teorije grup, ki jih tu ne bomo navedli, si lahko bralec prebere v [45]. Bolj poglobljeno razlago o delovanjih grup lahko bralec najde v [45, 46]. Več o konceptu krovnega grafa in dviga avtomorfizmov je moč najti v [15, 16]. Standardni vir, ki pokriva področje algoritmov, je [47].

2.1 Grupa

Grupa je množica G skupaj z binarno operacijo $\cdot : G \times G \to G$, ki zadošča naslednjim lastnostim:

(i) za vse $g, h \in G$, velja $g \cdot h \in G$ (*zaprtost*);
(ii) za vse $g, h, k \in G$, velja $(g \cdot h) \cdot k = g \cdot (h \cdot k)$ (*asociativnost*);
(iii) obstaja element $e \in G$, da za vsak $g \in G$ velja $e \cdot g = g \cdot e = e$ (*identiteta*);
(iv) za vsak $g \in G$ obstaja tak element h, da velja $g \cdot h = h \cdot g = e$ (*inverz*).

Grupa je *končna*, če ima množica G končno mnogo elementov. V tem primeru številu elementov v grupi rečemo *moč* ali *red* grupe, ki ga označimo z $|G|$. V poljubni grupi G za vsak poljuben element g definiramo *red elementa* g kot tisto najmanjše naravno število n, da velja $g^n = e$. V kolikor tak n ne obstaja, pravimo, da je g *neskončnega reda*. Grupa ja *abelska* oziroma *komutativna*, če zadošča dodatnemu pogoju: za vse $g, h \in G$, velja $g \cdot h = h \cdot g$ (*komutativnost*). *Elementarno abelska grupa* je abelska grupa, v kateri je vsak netrivialni element reda p, kjer je p praštevilo.

Grupe v disertaciji so bodisi:

(i) multiplikativne grupe, kjer ponavadi opuščamo znak $\cdot$ za operacijo (pišemo gh namesto $g \cdot h$), identiteto označujemo z 1 namesto e, medtem ko z g^{-1} označujemo inverz elementa g; bodisi

(ii) aditivne grupe, kjer znak za operacijo $\cdot$ zamenjamo z znakom $+$, identiteto označujemo z 0, inverz elementa g pa z $-g$.

Aditivne grupe so vedno komutativne, multiplikativne grupe pa so lahko komutativne ali pa tudi ne. Poleg tega v disertaciji obravnavamo le končne grupe.

Podmnožica H grupe G je *podgrupa* v G, če je H, skupaj s podedovano operacijo iz grupe G, tudi grupa. Oznaka $H \leq G$ pomeni, da je H podgrupa v G. Naj bo S poljubna podmnožica grupe G. Podgrupa $\langle S \rangle$ v G, *generirana* s podmnožico S, je najmanjša podgrupa v G, ki vsebuje S. Posebej rečemo, da množica S generira grupo G, če velja $G = \langle S \rangle$. Naj bo $x \in G$. Potem je *desni odsek* po podgrupi H podmnožica $Hx = \{hx \mid h \in H\}$ grupe G. Podobno definiramo *levi odsek*. *Indeks* $[G : H]$ podgrupe H v grupi G je moč množice desnih (oziroma levih) odsekov po podgrupi H v grupi G – ki je lahko v splošnem bodisi končen bodisi neskončen – in je enak $|G|/|H|$, če je G končna. Množici predstavnikov desnih odsekov po H v G rečemo *desna transverzala*, *levo transverzalo* definiramo podobno.

Podgrupa N v grupi G je *edinka* v G, če velja $xN = Nx$ za vse $x \in G$. Dejstvo, da je N podgrupa edinka v G označimo z $N \lhd G$. Tipična primera podgrup edink sta komutatorska podgrupa in normalno zaprtje. *Komutatorska podgrupa* $[G, G]$ v G je podgrupa generirana z vsemi *komutatorji* $g^{-1}h^{-1}gh$, $g, h \in G$. *Normalno zaprtje* A^G podmnožice A v grupi G je presek vseh podgrup edink v G, ki vsebujejo A. Drugače rečeno, normalno zaprtje je najmanjša podgrupa edinka v G, ki vsebuje A. Za vsako podgrupo edinko N velja pomembna lastnost, da produkt poljubnega elementa $n_1 g$ iz odseka Ng s poljubnim elementom $n_2 h$ iz odseka Nh leži v odseku Ngh. Zato je $(Ng)(Nh) = Ngh$ in množica desnih odsekov Ng po N v G tvori multiplikativno grupo reda $[G : N]$. To grupo označimo z G/N in ji rečemo *kvocientna* oziroma *faktorska* grupa po edinki N.

Naj bosta G in H grupi. *Homomorfizem* ϕ iz grupe G v grupo H je preslikava $\phi\colon G \to H$, za katero velja $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$ za vse $g_1, g_2 \in G$. *Jedro* $\mathrm{Ker}(\phi)$ homomorfizma ϕ je množica vseh elementov iz G, ki se preslikajo v 1; to je

$$\mathrm{Ker}(\phi) = \{g \in G \mid \phi(g) = 1\}.$$

Ni se težko prepričati, da je $\mathrm{Ker}(\phi)$ vedno podgrupa edinka v G. Homomorfizem ϕ je *monomorfizem*, *epimorfizem* oziroma *izomorfizem*, če je injektiven, surjektiven oziroma bijektiven, zaporedoma. Homomorfizmu, ki slika iz G v G, rečemo *endomorfizem*,

izomorfizmu iz G v G pa *avtomorfizem* . Avtomorfizmi grupe G skupaj z operacijo komponiranja tvorijo grupo, ki jo označimo z $\mathsf{Aut}(G)$. Grupi G in H sta *izomorfni*, če obstaja izomorfizem $\phi\colon G \to H$.

Naj bo S podmnožica grupe F. Grupa F je *prosta* grupa na množici S, če za vsako grupo G in preslikavo $\theta\colon S \to G$ obstaja tak enolično definiran homomorfizem $\theta'\colon F \to G$ z lastnostjo, da velja $\theta'(s) = \theta(s)$ za vse $s \in S$. Moč $|S|$ množice S je *rang* proste grupe F na množici S. Nizu $w = s_1 s_2 \dots s_r$, kjer je vsak s_i iz množice S, rečemo *beseda* nad S. Število $|w| = r$ je *dolžina* besede w.

Grupe so pogosto opisane kot kvocientne grupe prostih grup: $G = F/N$. Če je F prosta grupa na podmnožici S in je $N = R^F$ normalno zaprtje podmnožice R v F, potem rečemo, da je $\langle S \,|\, R\rangle$ *prezentacija* grupe G. Za vsak element s v S naj $\bar{s}$ označuje njegovo sliko v grupi G. Potem množica $\bar{S} = \{\bar{s} \,|\, s \in S\}$ generira grupo G. Če $r = r(s_1, s_2, \dots, s_n)$ leži v R, potem velja enakost $r(\bar{s}_1, \bar{s}_2, \dots, \bar{s}_n) = 1$ v G. Ponavadi govorimo kar o množici S kot množici *generatorjev* za G. Poleg tega enakosti $r = 1$, $r \in R$ rečemo *relacija*, elementu r pa *relator*.

Naj bo N podgrupa edinka v grupi G. Potem rečemo, da je grupa G (grupna) *razširitev* grupe N po faktorski grupi G/N. S pomočjo pojma razširitve lahko definiramo rešljivo grupo. Grupa je *rešljiva*, če jo lahko konstruiramo iz abelskih grup z rekurzivno uporabo razširitev. V nadaljevanju pomembno vlogo igrajo razcepne razširitve. Če obstaja v grupi G tudi podgrupa K, da velja $NK = G$ in $N \cap K = 1$, je razširitev *razcepna*. V tem primeru podgrupo K imenujemo *komplement* grupe N v G.

Za dani grupi N in K lahko razcepne razširitve N po K konstruiramo na naslednji način. Denimo, da je dan homomorfizem $\theta\colon K \to \mathsf{Aut}(K)$. *Poldirektni produkt* grupe N po grupi K glede na homomorfizem θ je množica $N \times K$ opremljena z množenjem

$$(n,k)(n',k') = (n\theta_k(n'), kk')$$

za $n, n' \in N$ in $k, k' \in K$. Standardna oznaka za poldirektni produkt je $N \rtimes_\theta K$ oziroma $N \rtimes K$, če je homomorfizem θ razviden iz konteksta. Ni se težko prepričati, da je podgrupa $(N, 1)$ edinka in je $(1, K)$ njen komplement v $N \rtimes K$. Poleg tega je vsaka razcepna razširitev poldirektni produkt. V tem smislu lahko zato pojma razcepne razširitve in poldirektnega produkta enačimo. Grupi $H \rtimes_{id} \mathsf{Aut}(H)$ rečemo *holomorf* grupe H in ga označimo s $\mathrm{Hol}(H)$.

2.2 Graf in njegova fundamentalna grupa

Graf je urejen par $X = (V, \sim)$, kjer je $V(X) = V$ neprazna množica *vozlišč* in $\sim$ irefleksivna simetrična relacija na V, ki jo imenujemo relacija *sosednosti*. Vozlišči u in v sta *sosednji*, če velja $u \sim v$. Neurejenemu paru uv sosednjih vozlišč u, v rečemo *povezava*, množico vseh povezav grafa X pa označimo z $E(X)$. Če želimo poudariti, da so povezave predstavljene z neurejenimi pari, potem grafu rečemo tudi *neusmerjen* graf. Hkrati rečemo, da sta vozlišči u in v *krajišči* povezave uv. Urejenemu paru (u, v) sosednjih vozlišč u, v rečemo *lok*, množico vseh lokov grafa X pa označimo z $A(X)$. Vsaka povezava uv določa dva med seboj *nasprotna* loka: (u, v) in (v, u). Če vsaki povezavi dodelimo natanko enega izmed pripadajočih lokov, dobimo *orientacijo* grafa X, ki jo označimo z $A^+(X)$. *Okolica* vozlišča u je množica vseh sosedov vozlišča u v X in jo označimo z $N(u)$. Njeno moč imenujemo *stopnja* ali *valenca* vozlišča u. Graf je *končen*, če sta množici $V(X)$ in $E(X)$ končni.

Po definiciji graf ne vsebuje zank; *zanka* je „povezava“, ki ima obe krajišči v istem vozlišču. Poleg tega ne vsebuje niti *večkratnih povezav*, torej več različnih „povezav“, ki imajo za svoja krajišča isti par vozlišč. Kadar želimo poudariti, da graf ne vsebuje zank in večkratnih povezav, mu rečemo *enostaven* graf. V *multigrafu* dopuščamo tudi zanke in večkratne povezave.

Če povezave definiramo kot urejene pare vozlišč, potem govorimo o *usmerjenem grafu*. Podobno lahko definiramo *usmerjen multigraf*. Urejenemu paru (u, v) rečemo tudi *usmerjena povezava*. Čeprav so v nadaljevanju omenjeni tudi usmerjeni multigrafi (glej Razdelek 3.1), je v disertaciji poudarek na enostavnih neusmerjenih grafih, razen tam, kjer bo omenjeno drugače. Poleg tega v disertaciji študiramo le končne grafe, zato bo beseda „graf“ vedno pomenila končen graf.

Podgraf grafa X je graf na podmnožici vozlišč in povezav grafa X. Podgrafu na množici vseh vozlišč grafa X rečemo *vpeti* podgraf. *Sprehod* $W : u \to v$ dolžine $n \geq 0$ od vozlišča $u_0 = u$ do vozlišča $u_n = v$ je zaporedje vozlišč $W = (u_0, u_1, \ldots, u_n)$, kjer sta u_{i-1} in u_i sosednji vozlišči za vse $1 \leq i \leq n$. Zaporedje (u) je *trivialen sprehod* dolžine 0 v vozlišču u. *Pot* v grafu je sprehod, ki vsebuje le različna vozlišča grafa. Očitno so poti dolžine 1 natanko loki. *Obhod* je sklenjen sprehod; to pomeni, da končno vozlišče sovpada z začetnim. *Cikel* je obhod, v katerem se ponovita zgolj začetno in končno vozlišče. Graf je *povezan*, če obstaja sprehod med poljubno izbranim parom vozlišč. Povezan graf brez ciklov je *drevo*.

Homomorfizem iz grafa X v graf X' je funkcija $f: V(X) \to V(X')$, ki preslika sosednja vozlišča v sosednja vozlišča (to je, f ohranja sosednost). Homomorfizme komponiramo z desne proti levi – tako kot funkcije. Surjektivni homomorfizem grafov imenujemo *epimorfizem*, medtem ko bijektivnemu homomorfizmu rečemo *izomorfizem* . *Avtomorfizem grafa* je izomorfizem grafa samega nase. Vsi avtomorfizmi grafa X skupaj z operacijo komponiranja tvorijo grupo avtomorfizmov $\mathsf{Aut}(X)$ grafa X.

Za dani sprehod $W = (u_0, u_1, \dots, u_n)$ definiramo njegov *nasprotni sprehod* kot $W^{-1} = (u_n, u_{n-1}, \dots, u_0)$. Vsakemu sprehodu W priredimo *reduciran sprehod* $\underline{W}$ tako, da iz sprehoda zaporedoma odstranimo vse podsprehode oblike (u, v, u). Sprehoda $W, W': u \to v$ sta *homotopna*, če sta njuna reducirana sprehoda ista. Sprehod je *skrčljiv*, če je homotopen trivialnemu sprehodu. *Homotopija* je ekvivalenčna relacija na množici vseh sprehodov. Homotopske razrede sprehodov označimo z $[W]$. *Produkt sprehodov* $W: u \to v$ in $W': v \to w$ definiramo kot sprehod $W \cdot W': u \to w$, ki ga dobimo s spojitvijo zaporedij. Takšna definicija porodi produkt $[W][W'] = [W \cdot W']$ homotopskih razredov.

Naj bo X povezan graf in izberimo poljubno vozlišče u v X. Množica homotopskih razredov obhodov $W: u \to u$ skupaj z zgornjim produktom definira *fundamentalno grupo* $\pi(X, u)$ z vozliščem u. Do izomorfizma natanko je grupa $\pi(X, u)$ neodvisna od izbire vozlišča u. Drugače rečeno, za poljubni vozlišči u in v sta grupi $\pi(X, u)$ in $\pi(X, v)$ izomorfni. Še več, vse fundamentalne grupe $\pi(X, u)$, $u \in V(X)$, so izomorfne prosti grupi ranga $|E(X)| - |V(X)| + 1$. Število $\beta(X) = |E(X)| - |V(X)| + 1$ imenujemo *Bettijevo število* oziroma tudi *rang* povezanega grafa X. Nadalje, naj bo T poljubno vpeto drevo grafa X in $X - T$ *kodrevo*, to je podgraf v X, ki mu odstranimo vse povezave iz T. Vsak lok (v, w) kodrevesa $X - T$ skupaj z enolično določenima potema $P: u \to v$ in $Q: u \to w$ v drevesu T določa *fundamentalni obhod* $W^{(v,w)} = P(v, w)Q^{-1}$ v vozlišču u. Množica $\{[W^{(v,w)}] \mid (v, w) \in A(X - T)\}$ homotopskih razredov fundamentalnih obhodov v vozlišču u generira grupo $\pi(X, u)$. Minimalno število generatorjev, ki generirajo grupo $\pi(X, u)$, dobimo tako, da za vsako povezavo v kodrevesu $X - T$ izberemo natanko en lok. *Abelizacijo* $\pi(X, u)/[\pi(X, u), \pi(X, u)]$ fundamentalne grupe $\pi(X, u)$ imenujemo (prva) *homološka grupa* grafa X in jo označimo s $H_1(X)$.

2.3 Delovanje grup

Množico vseh permutacij na neprazni množici Ω skupaj z množenjem permutacij od desne proti levi imenujemo *leva simetrična grupa* in jo označimo s simbolom $\mathsf{Sym}_{\mathrm{L}}(\Omega)$.

Ker so permutacije preslikave, sliko poljubnega elementa $\omega \in \Omega$ pri permutaciji $g \in \mathrm{Sym}_{\mathrm{L}}(\Omega)$ pišemo z $g(\omega)$, kot smo to vajeni pri preslikavah. Opozorimo, da smo grupo avtomorfizmov $\mathrm{Aut}(X)$ grafa X definirali kot podgrupo leve simetrične grupe $\mathrm{Sym}_{\mathrm{L}}(\Omega)$, kjer je $\Omega = V(X)$ množica vozlišč.

Podobno pa lahko definiramo še *desno simetrično grupo* $\mathrm{Sym}_{\mathrm{R}}(\Omega)$, kjer permutacije množimo od leve proti desni. V tem primeru sliko elementa $w \in \Omega$ pri permutaciji $g \in \mathrm{Sym}_{\mathrm{R}}(\Omega)$ pišemo z eksponentnim zapisom w^g. Če je Ω kar množica naravnih števil $[n] = \{1, 2, \ldots, n\}$, potem desno simetrično grupo označimo s simbolom S_n. Podgrupi grupe $\mathrm{Sym}_{\mathrm{L}}(\Omega)$ oziroma $\mathrm{Sym}_{\mathrm{R}}(\Omega)$ rečemo *permutacijska grupa*.

Desno delovanje grupe G na množici Ω je funkcija

$$\Omega \times G \to \Omega, \quad (\omega, g) \mapsto \omega^g,$$

ki zadošča pogojema $\omega^{1_G} = \omega$ in $\omega^{gh} = (\omega^g)^h$ za vse $\omega \in \Omega$ in $g, h \in G$. Desno delovanje grupe G na Ω lahko enakovredno opišemo kot homomorfizem iz grupe G v desno simetrično grupo $\mathrm{Sym}_{\mathrm{R}}(\Omega)$. Namreč, za vsak $g \in G$ delovanje porodi permutacijo $\chi(g)\colon \omega \mapsto \omega^g$ in posledično tudi homomorfizem χ s predpisom $g \mapsto \chi(g)$. Obratno, ni se težko prepričati, da poljuben homomorfizem $\chi\colon G \to \mathrm{Sym}_{\mathrm{R}}(\Omega)$ porodi desno delovanje grupe G na Ω s predpisom $(\omega, g) \mapsto \omega^{\chi(g)}$. Če desno delovanje grupe G na Ω predstavimo kot homomorfizem $\chi\colon G \to \mathrm{Sym}_{\mathrm{R}}(\Omega)$, potem homomorfizmu χ rečemo *desna permutacijska reprezentacija* grupe G na Ω. Čeprav so v disertaciji omenjena tudi *leva delovanja*, bomo v naslednjih definicijah privzeli, da grupe delujejo na množicah z desne. Pojme, povezane z levimi delovanji, definiramo podobno.

Naj grupa G deluje na množici Ω, grupa G' pa na množici Ω'. *Morfizem delovanj* (oziroma permutacijskih reprezentacij) je par preslikav (f, ϕ), kjer je $f\colon G \to G'$ homomorfizem grup in $\phi\colon \Omega \to \Omega'$ taka preslikava množic, da velja $\phi(\omega^g) = \phi(\omega)^{f(g)}$ za vse $\omega \in \Omega$ in $g \in G$. Povedano drugače, če sta $\chi\colon G \to \mathrm{Sym}_{R}(\Omega)$ in $\chi'\colon G' \to \mathrm{Sym}_{R}(\Omega')$ pripadajoči permutacijski reprezentaciji, potem naslednji diagram

$$\begin{array}{ccc} \Omega & \xrightarrow{\chi(g)} & \Omega \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi} \\ \Omega' & \xrightarrow{\chi'(f(g))} & \Omega' \end{array}$$

komutira za vsak $g \in G$.

Morfizmu (f, ϕ) rečemo *monomorfizem*, če sta f in ϕ injektivna, *epimorfizem*, če sta f in ϕ surjektivna, oziroma *izomorfizem*, če sta f in ϕ bijekciji. Če je $G = G'$ in je $f = id$, potem izomorfizmu rečemo *ekvivalenca delovanj*. Intuitivno vzeto pomeni ekvivalenca delovanj tako preoznačitev množice, ki „ne spremeni“ delovanja. Naj grupa G deluje na množici Ω z n elementi in naj bo $\phi: \Omega \to [n]$ poljubno oštevilčenje množice Ω z naravnimi števili. Potem pripadajoča permutacijska reprezentacija $\chi: G \to \mathrm{Sym}_R(\Omega)$ porodi ekvivalentno permutacijsko reprezentacijo $G \to S_n$ glede na to oštevilčenje, ki jo zaradi poenostavitve notacije prav tako označimo s χ.

Jedro delovanja je jedro $\mathrm{Ker}(\chi)$ permutacijske reprezentacije χ. Če je $\mathrm{Ker}(\chi) = 1$, potem rečemo, da je delovanje (oziroma reprezentacija) *zvesto* (zvesta). Kadar je delovanje zvesto, je slika $\mathrm{Im}(\chi)$ izomorfna grupi G.

Množico $G_\omega = \{g \in G \mid \omega^g = \omega\}$ vseh elementov grupe G, ki ohranjajo element $\omega \in \Omega$ negiben, imenujemo *stabilizator* elementa ω pri delovanju grupe G, množici slik $\omega^G = \{\omega^g \mid g \in G\}$ pa rečemo *orbita* elementa ω. Delovanje grupe je *polregularno*, če so vsi stabilizatorji trivialni. V primeru, da obstaja samo ena orbita, je delovanje *tranzitivno*; to pomeni, da za poljubna elementa ω in ω' v Ω obstaja grupni element g v G, da velja $\omega' = \omega^g$. Stabilizatorji v isti orbiti so med seboj konjugirani. Tranzitivno in polregularno delovanje je *regularno*.

Oglejmo si delovanji, ki bosta v nadaljevanju igrali pomembno vlogo. Naj bo G poljubna grupa. Potem lahko definiramo (desno) delovanje grupe G na množici $\Omega = \{H \mid H \leq G\}$ vseh njenih podgrup s konjugacijo: $H^g := g^{-1}Hg$ za $H, g^{-1}Hg \in \Omega$ in $g \in G$. Grupo $g^{-1}Hg$ imenujemo *konjugiranka* podgrupe H z elementom g. Razen v izrojenih primerih, to delovanje ni tranzitivno. Orbita podgrupe H je množica $H^G = \{g^{-1}Hg \mid g \in G\}$ vseh konjugirank podgrupe H oziroma *konjugiranostni razred* podgrupe H. Stabilizator podgrupe H pa je

$$G_H = \{g \in G \mid g^{-1}Hg = H\};$$

to je največja podgrupa v grupi G, ki vsebuje H kot podgrupo edinko. Rečemo mu tudi *normalizator* podgrupe H v grupi G in ga označimo z $N_H(G)$.

Definirajmo še (desno) delovanje grupe G na množici $H|G = \{Hx \mid x \in G\}$ vseh desnih odsekov po podgrupi H z desnim množenjem: $(Hx)^g := Hxg$ za $Hx, Hxg \in \Omega$ in $g \in G$. Pripadajočo permutacijsko reprezentacijo označimo s $\chi_H: G \to \mathrm{Sym}_R(H|G)$.

Jedro tega delovanja je

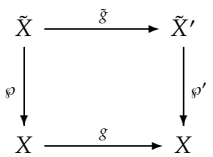
$$\mathrm{Ker}(\chi_H) = \bigcap_{g \in G} g^{-1} H g,$$

ki je največja podgrupa edinka v G, vsebovana v H. To jedro imenujemo tudi *sredica* podgrupe H v grupi G in jo označimo s $\mathrm{core}_G(H)$. V splošnem reprezentacija χ_H ni zvesta. Ni se težko prepričati, da je to delovanje vedno tranzitivno. Iz tega sledi, da je slika $\mathrm{Im}(\chi_H)$ tranzitivna podgrupa v $\mathsf{Sym}_R(H|G)$. Poleg tega je stabilizator odseka Hx konjugiranka $x^{-1}Hx$ podgrupe H z elementom x. V primeru, da je H podgrupa edinka, so vsi stabilizatorji in tudi sredica $\mathrm{core}_G(H)$ očitno enaki kar H. Tedaj je slika $\mathrm{Im}(\chi_H)$ regularna podgrupa v $\mathsf{Sym}_R(H|G)$. V posebnem primeru, ko za H vzamemo trivialno grupo, grupa G deluje nase regularno in zvesto z desnim množenjem. Pripadajočemu homomorfizmu rečemo *desna regularna reprezentacija*. Dodajmo, da je vsako tranzitivno (desno) delovanje grupe G na Ω ekvivalentno (desnemu) delovanju grupe G na (desnih) odsekih po stabilizatorju G_w elementa $w \in \Omega$. In še, tranzitivni delovanji sta ekvivalentni natanko tedaj, ko sta stabilizatorja konjugirana.

2.4 Krovni graf

Krovna projekcija grafov je epimorfizem $\wp\colon \tilde{X} \to X$, ki preslika okolico $N(\tilde{u})$ poljubnega vozlišča $\tilde{u}$ v $\tilde{X}$ bijektivno na okolico $N(\wp(\tilde{u}))$ slike $\wp(\tilde{u})$ vozlišča $\tilde{u}$ v X (endomorfizem $\wp$ je lokalno bijektiven na okolicah vozlišč). Pravimo, da je $\tilde{X}$ *krovni graf* oziroma krov nad *baznim grafom* X. Prasliko $\wp^{-1}(u)$ za $u \in V(X)$, imenujemo *vlakno vozlišča* u. Krovne projekcije, ki so posebej pomembne pri študiju simetrijskih lastnosti grafov in njihovih krovov, so regularne krovne projekcije. Krovna projekcija $\wp\colon \tilde{X} \to X$ je *regularna*, če obstaja polregularna grupa $C \leq \mathsf{Aut}(\tilde{X})$, katere orbite vozlišč sovpadajo z vlakni vozlišč. Z drugimi besedami, grupa C deluje regularno na vsakem vlaknu (od tod tudi ime). Tedaj graf $\tilde{X}$ imenujemo *regularen krovni graf* oziroma regularen krov.

Krovne projekcije navadno študiramo do ekvivalence ali do izomorfizma natanko (kar je precej težje). Krovni projekciji $\wp\colon \tilde{X} \to X$ in $\wp'\colon \tilde{X}' \to X$ sta *izomorfni*, če obstajata avtomorfizem $g \in \mathsf{Aut}(X)$ in izomorfizem $\tilde{g}\colon \tilde{X} \to \tilde{X}'$, da naslednji diagram



komutira. Posebej, projekcij sta *ekvivalentni*, če je $g = id$.

Iz definicije krovne projekcije neposredno sledi, da za vsak sprehod $W\colon u \to v$ v baznem grafu X in poljubno vozlišče $\tilde{u}$ v vlaknu $\wp^{-1}(u)$ obstaja natanko en sprehod $\tilde{W}^{\tilde{u}}$ v krovnem grafu $\tilde{X}$ z začetkom v $\tilde{u}$, ki se projicira na W: $\wp(\tilde{W}^{\tilde{u}}) = W$. Sprehod $\tilde{W}^{\tilde{u}}$ imenujemo *dvignjeni sprehod*. Slednje je znano kot *lastnost enoličnega dviga sprehoda*. Pri predpostavki, da je X povezan graf (kar bo brez škode za splošnost naša standardna predpostavka), imajo potemtakem vsa vlakna isto moč. Če je moč vlakna enaka n, rečemo, da je krovna projekcija *n-listna*, krovni graf $\tilde{X}$ pa imenujemo *n-listni krov* nad X. Poleg tega je očitno, da se homotopski sprehodi dvignejo do homotopskih sprehodov in da predpis

$$\tilde{u}^{[W]} := \text{končno vozlišče dvignjenega sprehoda } \tilde{W}^{\tilde{u}}$$

definira „desno delovanje“ homotopskih razredov na množici vozlišč krovnega grafa $\tilde{X}$ prek enoličnega dviga sprehoda. Posebej, fundamentalna grupa $\pi(X, u)$ deluje z desne na vlaknu $\wp^{-1}(u)$. To je natanko delovanje, ki določa strukturne lastnosti krovov. Krovni graf $\tilde{X}$ je povezan natanko tedaj, ko fundamentalna grupa $\pi(X, u)$ deluje tranzitivno na vlaknu $\wp^{-1}(u)$. Tedaj je to delovanje ekvivalentno delovanju grupe $\pi(X, u)$ na desnih odsekih po stabilizatorju $\pi(X, u)_{\tilde{u}}$, $\tilde{u} \in \wp^{-1}(u)$. Obratno, vsaka podgrupa $H \leq_n \pi(X, u)$ indeksa n porodi do ekvivalence natanko n-listno povezano krovno projekcijo tako, da je stabilizator pripadajočega delovanja natanko H. Ta vidik bo igral pomembno vlogo v nadaljevanju pri generiranju krovov.

Opazimo, da krovna projekcija $\wp$ inducira preslikavo $\pi(\tilde{X}, \tilde{u}) \to \pi(X, u)$, ki je monomorfizem grup, in da je stabilizator natanko monomorfna slika grupe $\pi(\tilde{X}, \tilde{u})$ v $\pi(X, u)$. Stabilizator torej vsebuje natanko tiste reducirane sprehode $[W] \in \pi(X, u)$, ki imajo sklenjen dvig $\tilde{W}$ z začetkom v $\tilde{u}$. V povezanem krovnem grafu $\tilde{X}$ so si stabilizatorji različnih vozlišč v splošnem konjugirani in so med seboj enaki natanko tedaj, ko je krovna projekcija regularna. Drugače povedano, krovna projekcija povezanih grafov je regularna natanko tedaj, ko so vsi stabilizatorji delovanja grupe $\pi(X, u)$ na vlaknu $\wp^{-1}(u)$ enaki jedru delovanja. Poleg tega sta krovni projekciji $\wp\colon \tilde{X} \to X$ in $\wp'\colon \tilde{X}' \to X$ ekvivalentni natanko tedaj, ko sta za poljubno vozlišče u v X delovanji fundamentalne grupe $\pi(X, u)$ na vlaknih $\wp^{-1}(u)$ in $\wp'^{-1}(u)$ ekvivalentni.

Krovne grafe lahko kombinatorično opišemo na naslednji način. Naj bo Γ poljubna (abstraktna) grupa, ki z desne deluje na neki množici Ω. Nadalje naj bo $\zeta\colon X \to \Gamma$

funkcija na povezanem grafu X, ki nasprotnim lokom priredi inverzne elemente grupe:

$$\zeta(v,u) = (\zeta(u,v))^{-1} \quad \text{za vse loke } (u,v) \text{ v } X.$$

Tedaj pravimo, da je Ω *abstraktno vlakno*, Γ *napetostna grupa*, ζ *napetostna funkcija* na X, $\zeta(u,v)$ pa *napetost* na loku (u,v). S temi podatki lahko definiramo *izpeljani graf* $X \times_\zeta \Omega$ na množici vozlišč $V(X) \times \Omega$ in relacijo sosednosti

$$(u,\omega) \sim (v,\omega^{\zeta(u,v)}) \quad \text{za } u \sim v \text{ v } X.$$

Izkaže se, da je projekcija na prvo komponento

$$\wp_\zeta \colon X \times_\zeta \Omega \to X, \quad \wp_\zeta(u,f) = u \tag{2.1}$$

krovna projekcija. Rečemo ji *izpeljana krovna projekcija*. Če na množici Ω deluje grupa $\Gamma = \mathsf{Sym}_{\mathrm{R}}(\Omega)$, govorimo o *permutacijski napetostni funkciji* in *permutacijskih napetostih*, če pa je $\Omega = \Gamma$ (grupa Γ deluje nase regularno z desnim množenjem), pa o *regularni napetostni funkciji* in *regularnih napetostih*. Napetostna funkcija je *končna*, brž ko je Ω končna. Očitno je napetostna funkcija natanko definirana s predpisom napetosti le na izbrani orientaciji grafa X.

Po drugi strani lahko vsako n-listno krovno projekcijo $\wp \colon \tilde{X} \to X$ do ekvivalence natanko rekonstruiramo recimo s permutacijskimi napetostmi. Označimo vozlišča vsakega vlakna poljubno z naravnimi števili $\{1,2,\dots,n\}$: naj bo $\wp^{-1}(u) = \{u_1,u_2,\dots,u_n\}$ vlakno za vsako vozlišče u v X in naj število i označuje vozlišče u_i. Potem je permutacijska napetost $\zeta(u,v) \in S_n$ loka (u,v) v X definirana na naslednji način: $i^{\zeta(u,v)} = j$ natanko tedaj, ko je vozlišče u_i v vlaknu $\wp^{-1}(u)$ povezano z vozliščem v_j v vlaknu $\wp^{-1}(v)$. To informacijo zakodiramo na X s funkcijo $\zeta \colon X \to S_n$, ki porodi izpeljano krovno projekcijo $\wp_\zeta \colon X \times_\zeta [n] \to X$, ekvivalentno krovni projekciji $\wp$.

Regularne krove dobimo kot izpeljane grafe z regularnimi napetostmi. V tem primeru je namreč izpeljana krovna projekcija $\wp_\zeta$ iz (2.1) regularna – polregularno grupo C dobimo, če na $C = \Gamma$ pogledamo kot na podgrupo avtomorfizmov krovnega grafa $\tilde{X}$, ki na drugi koordinati deluje na sebi z levim množenjem: element $c \in \Gamma$ preslika vozlišče (u,x) v vozlišče (u,cx).

Obratno, vsako regularno krovno projekcijo $\wp \colon \tilde{X} \to X$ lahko do ekvivalence natanko rekonstruiramo z regularnimi napetostmi. Naj bo C polregularna grupa iz definicije regularne krovne projekcije. Ker C deluje regularno na vsakem vlaknu, lahko označimo vozlišča v $\tilde{X}$ z elementi iz $\Gamma = C$ dosledno z njenim delovanjem. V vsakem vlaknu

$\wp^{-1}(u)$ izberimo poljubno vozlišče $\tilde{u}$ in za vsak $c \in \Gamma$ označimo vozlišče $c(\tilde{u})$ v vlaknu $\wp^{-1}(u)$ z (u, c). Na ta način so vozlišča vsakega vlakna $\wp^{-1}(u)$ označena bijektivno z $\{u\}\times\Gamma$. Za poljuben lok (u, v) v X naj bo (v, x) oznaka vozlišča v $\wp^{-1}(v)$, ki je povezano z vozliščem v $\wp^{-1}(u)$ z oznako $(u, 1)$. Potem je poljubno vozlišče v $\wp^{-1}(v)$, ki je povezano z vozliščem v $\wp^{-1}(v)$ z oznako recimo (u, c), označeno z (v, cx). To informacijo zakodiramo na X z regularno napetostno funkcijo $\zeta\colon X \to \Gamma$ s predpisom $\zeta(u, v) = x$. Pripadajoča izpeljana regularna krovna projekcija $\wp_\zeta$ je ekvivalentna projekciji $\wp$.

Pri rekonstrukciji krovne projekcije imamo precej svobode pri izbiri lokov, ki jim lahko predpišemo trivialne napetosti. Različne izbire nam dajo različne, toda *ekvivalentne* napetostne funkcije. Drugače povedano, pripadajoče izpeljane krovne projekcije so ekvivalentne. Preprost način, kako dani napetostni funkciji ζ poiščemo ekvivalentno napetostno funkcijo, je ta, da spremenimo napetosti na lokih, ne da bi pri tem spremenili napetosti fundamentalnih obhodov z začetkom v u. To lahko dosežemo z izbiro poljubnega vpetega drevesa T v X in definicijo nove napetostne funkcije $\zeta^{(T,u)}$, ki vsakemu loku (v, w) v drevesu T predpiše trivialno napetost, medtem ko vsakemu loku (v, w) v kodrevesu $X - T$ predpiše napetost $\zeta(W^{(v,w)})$ fundamentalnega obhoda $W^{(v,w)}$ v vozlišču u. Tako funkcijo imenujemo (T, u)- *reducirana napetostna funkcija*.

Naj bo X povezan graf in $\zeta\colon X \to \Gamma$ napetostna funkcija, kjer Γ deluje na množici Ω. Potem lahko funkcijo ζ naravno razširimo na poljuben sprehod $W = (u_0, u_1, \dots, u_n)$ v X s predpisom $\zeta(W) = \zeta(u_0, u_1)\cdots\zeta(u_{n-1}, u_n)$. Očitno imata homotopna sprehoda isto napetost, zato lahko napetosti priredimo homotopnim razredom. Še več, inducirana preslikava $\pi(X, u) \to \Gamma$ je homomorfizem grup, ki jo zaradi poenostavitve notacije prav tako označimo s ζ. Obratno, vsak homomorfizem $\pi(X, u) \to \Gamma$ porodi napetostno funkcijo na grafu X: lokom v izbranem vpetem drevesu dodelimo trivialne napetosti, medtem ko ostalim lokom dodelimo slike pripadajočih generatorjev grupe $\pi(X, u)$ glede na ta homomorfizem. Homomorfno sliko $\zeta(\pi(X, u))$ imenujemo *lokalna napetostna grupa* v vozlišču u in jo označimo z Loc_u. Opozorimo, da so lokalne napetostne grupe v različnih vozliščih v splošnem konjugirane podgrupe; v primeru (T, u)-reducirane napetostne funkcije ζ pa so vse lokalne napetostne grupe enake $\mathrm{Loc} = \mathrm{Loc}_v$, $v \in V(X)$. Opazimo še, da velja

$$(u, \omega)^{[W]} = (u, \omega^{\zeta([W])}),$$

zato lahko rečemo, da je delovanje lokalne napetostne grupe Loc_u na abstraktnem vlaknu Ω usklajeno z delovanjem grupe $\pi(X, u)$ na vlaknu $\wp_\zeta^{-1}(u) = \{(u, w) | w \in \Omega\}$

v naslednjem smislu. Če sta $\chi\colon \pi(X,u) \to \mathrm{Sym}_R(\wp_\zeta^{-1}(u))$ in $\chi'\colon \mathrm{Loc}_u \to \mathrm{Sym}_R(\Omega)$ pripadajoči permutacijski reprezentaciji, potem komutira diagram

$$\begin{array}{ccc} \wp_\zeta^{-1}(u) & \xrightarrow{\chi([W])} & \wp_\zeta^{-1}(u) \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi} \\ \Omega & \xrightarrow{\chi'(\zeta([W]))} & \Omega, \end{array}$$

kjer je preslikava $\phi\colon \wp_\zeta^{-1}(u) \to \Omega$, definirana s predpisom $(u,w) \mapsto w$, bijekcija. Torej je izpeljani krovni graf $X \times_\zeta \Omega$ povezan natanko tedaj, ko je $\chi'(\mathrm{Loc}_u)$ tranzitivna podgrupa v $\mathrm{Sym}_R(\Omega)$. Tedaj rečemo, da je napetostna funkcija ζ *povezana*. Poleg tega povezane regularne krovne projekcije $\wp_\zeta$ spoznamo kot tiste, za katere je $\chi'(\mathrm{Loc}_u)$ regularna podgrupa v $\mathrm{Sym}_R(\Omega)$. Posebej, v primeru permutacijskih napetosti je krovna projekcija $\wp_\zeta$ povezana natanko tedaj, ko je Loc_u tranzitivna podgrupa v $\mathrm{Sym}_R(\Omega)$, in regularna natanko tedaj, ko je Loc_u regularna podgrupa v $\mathrm{Sym}_R(\Omega)$. V primeru regularnih napetosti pa je krovni graf $X \times_\zeta \Gamma$ povezan natanko tedaj, ko je $\mathrm{Loc}_u = \Gamma$, kar pomeni, da napetosti fundamentalnih obhodov v izbranem vozlišču u generirajo grupo Γ.

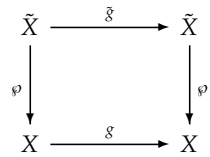
Naj bosta $\wp\colon \tilde{X} \to X$ in $\wp'\colon \tilde{X}' \to X$ krovni projekciji končnih povezanih grafov. V primeru, da krovne grafe rekonstruiramo s permutacijskimi napetostmi, se testiranje ekvivalence prevede na reševanje sistema permutacijskih enačb. Denimo, da $\zeta\colon X \to \mathrm{Sym}_R(\Omega)$ in $\zeta'\colon X \to \mathrm{Sym}_R(\Omega)$ rekonstruirata projekciji $\wp$ oziroma $\wp'$. Potem sta projekciji $\wp$ in $\wp'$ ekvivalentni natanko tedaj, ko za poljubno izbrano vozlišče u v X obstaja permutacija τ v grupi $\mathrm{Sym}_R(\Omega)$, za katero je

$$\tau^{-1}\zeta([W])\tau = \zeta'([W]), \quad [W] \in \pi(X,u). \tag{2.2}$$

Zgornjo enačbo je dovolj preveriti za generatorje grupe $\pi(X,u)$. Na drugi strani se kriterij za ekvivalenco regularnih krovnih projekcij v smislu regularnih napetostnih funkcij prevede na naslednjega: povezani regularni napetostni funkciji ζ in ζ' z vrednostmi v Γ sta ekvivalentni natanko tedaj, ko obstaja avtomorfizem τ napetostne grupe Γ, ki preslika napetost $\zeta(W)$ v napetost $\zeta'(W)$ za vsak obhod W v $\pi(X,u)$ (glej [33]). Pogoj je dovolj preveriti za generatorje grupe $\pi(X,u)$.

2.5 Dvigi avtomorfizmov

Avtomorfizem g baznega grafa X se *dvigne vzdolž* krovne projekcije $\wp\colon \tilde{X} \to X$, če obstaja avtomorfizem $\tilde{g}$ krovnega grafa $\tilde{X}$, da naslednji diagram



komutira. Avtomorfizem $\tilde{g}$ se potem *projicira* na g. Podgrupa G avtomorfizmov grafa X se dvigne, če se dvignejo vsi njeni elementi. Takšni krovni projekciji rečemo G-*dopustna*. Vsi dvigi elementov iz G tvorijo podgrupo $\tilde{G}$ avtomorfizmov krovnega graf $\tilde{X}$, *dvig* grupe G. Posebej, dvig trivialne grupe je *grupa krovnih transformacij* $CT(\wp)$. Poleg tega je dvignjena grupa $\tilde{G}$ razširitev grupe $CT(\wp)$ po grupi G. Torej ima vsak $g \in G$ natanko $|CT(\wp)|$ različnih dvigov, ki tvorijo odsek podgrupe $CT(\wp)$ v grupi $\tilde{G}$. Pri predpostavki, da je krovni graf $\tilde{X}$ povezan, grupa krovnih transformacij $CT(\wp)$ deluje polregularno na $\tilde{X}$. Tedaj je vsak dvig $\tilde{g}$ avtomorfizma $g \in \mathrm{Aut}(X)$, če obstaja, enolično določen s sliko enega vozlišča. Od zdaj naprej bomo predpostavili, da sta grafa X in $\tilde{X}$ povezana.

Posebej, grupa $CT(\wp)$ deluje polregularno na poljubnem vlaknu $\wp^{-1}(u)$, zato velja neenakost $|CT(\wp)| \leq |\wp^{-1}(u)|$. Enakost nastopi natanko tedaj, ko grupa $CT(\wp)$ deluje tudi tranzitivno in zato regularno na vlaknu $\wp^{-1}(u)$. V tem primeru je polregularna grupa C iz definicije regularne krovne projekcije natanko $C = CT(\wp)$ in regularna napetostna funkcija $\zeta\colon X \to \Gamma$, ki rekonstruira projekcijo, ima pravzaprav vrednosti v $\Gamma \cong CT(\wp)$ (kjer $CT(\wp)$ vidimo kot abstraktno grupo). Rečemo, da je regularna krovna projekcija *elementarno abelska, abelska* oziroma *rešljiva*, če je grupa $CT(\wp)$ elementarno abelska, abelska oziroma rešljiva, zaporedoma.

Ker se G dvigne vzdolž dane krovne projekcije $\wp$ natanko tedaj, ko se dvigne vzdolž katerekoli krovne projekcije, ki je ekvivalentna projekciji $\wp$, lahko dvige avtomorfizmov študiramo kombinatorično preko napetosti. V primeru permutacijskih napetosti se testiranje dviga avtomorfizma prevede na reševanje sistema permutacijskih enačb (primerjaj s testiranjem ekvivalence). Če je $\zeta\colon X \to \mathrm{Sym}_R(\Omega)$ permutacijska napetostna funkcija, ki rekonstruira krovno projekcijo $\wp$, potem se po *osnovni lemi o dvigu* (glej [14, 15]) avtomorfizem $g \in G$ dvigne vzdolž projekcije $\wp$ natanko tedaj, ko za

poljubno izbrano vozlišče u v X obstaja permutacija τ v grupi $\mathrm{Sym}_R(\Omega)$, za katero je

$$\tau^{-1}\zeta([W])\tau = \zeta(g([W])), \quad [W] \in \pi(X,u). \tag{2.3}$$

Zgornji pogoj je dovolj preveriti zgolj za generatorje grupe $\pi(X,u)$.

Oglejmo si interpretacijo permutacije τ v zgornjem sistemu. Recimo, da se g dvigne. Za poljuben dvig $\tilde{g}$ označimo s $\tau_{v,\tilde{g}}$ permutacijo v $\mathrm{Sym}_R(\Omega)$, ki pripada restrikciji $\tilde{g}\colon \wp^{-1}(v) \to \wp^{-1}(g(v))$ na drugi komponenti:

$$\tilde{g}(v,w) = (g(v), w^{\tau_{v,\tilde{g}}}).$$

Potem je permutacija $\tau_{u,\tilde{g}}$ natanko rešitev sistema. Obratno, vsaka rešitev sistema porodi natanko en dvig, zato so vse rešitve sistema v bijektivni korespondenci z vsemi dvigi. Poleg tega velja naslednja zveza med poljubno permutacijo $\tau_{v,\tilde{g}}$ in permutacijo $\tau_{u,\tilde{g}}$:

$$\tau_{v,\tilde{g}} = \zeta(Q)\,\tau_{u,\tilde{g}}\,\zeta(g(Q))^{-1}, \tag{2.4}$$

kjer je $Q\colon v \to u$ poljuben sprehod.

V primeru regularne krovne projekcije, dane s (T,u)-reducirano permutacijsko napetostno funkcijo, se sistem (2.3) prevede na pogoj, da obstaja avtomorfizem $g^{\#_u}$ lokalne napetostne grupe Loc, definiran lokalno v vozlišču u s predpisom

$$g^{\#_u}(\zeta([W])) = \zeta(g([W])), \quad [W] \in \pi(X,u).$$

Za dvig $\tilde{g}$, ki preslika vozlišče $(u,1)$ v vozlišče $(g(u),w)$, je pripadajoča permutacija $\tau_{u,\tilde{g}}$ oblike

$$\tau_{u,\tilde{g}}\colon 1^\nu \mapsto w^{g^{\#_u}(\nu)}, \quad \nu \in \mathrm{Loc}. \tag{2.5}$$

V nadaljevanju bomo potrebovali naslednjo oceno.

Lema 2.5.1: Naj bo $\wp_\zeta\colon X \times_\zeta [n] \to X$ povezana n-listna regularna krovna projekcija, dana s (T,u)-reducirano permutacijsko napetostno funkcijo ζ. Če se avtomorfizem g baznega grafa X dvigne, potem obstaja rešitev $\tau \in S_n$ sistema permutacijskih enačb (2.3), katerega red je navzgor omejen z $n-1$.

Dokaz: Ker se g dvigne vzdolž regularne krovne projekcije, obstaja dvig, ki preslika vozlišče $(u,1)$ v vozlišče $(g(u),1)$. Po (2.5) je pripadajoča permutacija $\tau \in S_n$, ki je rešitev sistema (2.3), oblike $\tau\colon 1^\nu \mapsto 1^{g^{\#_u}(\nu)}, \nu \in \mathrm{Loc}$. Sledi, da je

$$\tau^k\colon 1^\nu \mapsto 1^{(g^{\#_u})^k(\nu)}, \quad k \in \mathbb{N}.$$

Ker lokalna napetostna grupa Loc deluje regularno na $[n]$, ni težko videti, da je red permutacije $\tau \in S_n$ enak redu $g^{\#_u}$ v $\mathrm{Aut}(\mathrm{Loc})$. Zdaj uporabimo izrek Horoševskega (glej [48, Izrek 2]), ki pove, da ima vsak avtomorfizem grupe moči n red navzgor omejen z $n-1$. Ker je $|\mathrm{Loc}| = n$, je red avtomorfizma $g^{\#_u}$ in zato red permutacije τ navzgor omejen z $n-1$. □

Recimo, da je napetostna funkcija $\zeta\colon X \to \Gamma$ regularna (ne nujno (T,u)-reducirana). Tedaj je $g^{\#_u}$ avtomorfizem napetostne grupe Γ, permutacija $\tau_{u,\tilde{g}} \in \mathrm{Sym}_R(\Gamma)$ pa je oblike

$$\tau_{u,\tilde{g}}\colon c \mapsto t\,g^{\#_u}(c), \quad c \in \Gamma, \tag{2.6}$$

kjer $\tilde{g}$ preslika vozlišče $(u,1)$ v vozlišče $(g(u),t)$. Kadar želimo poudariti, da $\tilde{g}$ preslika vozlišče $(u,1)$ v vozlišče $(g(u),t)$, pišemo $\tilde{g}_t$. Poleg tega se zveza (2.4) prepiše v

$$\tau_{v,\tilde{g}}\colon c \mapsto c^{\tau_{u,\tilde{g}}}\, g^{\#_u}(\zeta(Q))\,\zeta(g(Q))^{-1}. \tag{2.7}$$

Opazimo tudi, da so avtomorfizmi $g^{\#_u}$, definirani lokalno v različnih vozliščih, med seboj konjugirani in da funkcija $G \to \mathrm{Aut}(\Gamma)$, definirana s predpisom $g \mapsto g^{\#_u}$, v splošnem ni grupni homomorfizem. Toda, če je regularna krovna projekcija abelska, potem avtomorfizem $g^{\#} = g^{\#_u}$ ni odvisen od u in funkcija $G \to \mathrm{Aut}(\Gamma)$ je homomorfizem grup.

2.5.1 *Elementarno abelski regularni krovi*

Problem iskanja takšnih elementarno abelskih regularnih krovov grafa X, da se avtomorfizem g dvigne vzdolž pripadajočih krovnih projekcij, so učinkovito rešili Malnič in soavtorji (glej [39]). Ključno vlogo pri tem igra prva (mod p)-homološka grupa $H_1(X;\mathbb{Z}_p) = H_1(X)/pH_1(X)$, ki je izomorfna elementarno abelski grupi $\mathbb{Z}_p^r$, kjer je p praštevilo in r rang grafa X. Namreč, če je v splošnem krovna projekcija porojena s homomorfizmom $\pi(X,u) \to \Gamma$, pa je v posebnem primeru, ko je $\Gamma = \mathbb{Z}_p^d$ elementarno abelska grupa, regularna krovna projekcija natanko določena s homomorfizmom $H_1(X;\mathbb{Z}_p) \to \mathbb{Z}_p^d$. Še več, ker lahko vsako elementarno abelsko grupo identificiramo z vektorskim prostorom nad poljem praštevilske karakteristike, lahko na zgornji homomorfizem gledamo kot na linearno preslikavo.

Naj bo T vpeto drevo in $A^+(X) = \{a_1, a_2, \dots, a_t\}$ urejena orientacija grafa X, kjer so $a_1, a_2 \dots, a_r$ loki v kodrevesu $X-T$, $a_{r+1}, a_{r+2}, \dots, a_t$ pa loki v drevesu T. Označimo z $B_T = \{[W^{a_1}], [W^{a_2}], \dots, [W^{a_r}]\}$ pripadajočo (urejeno) bazo prostora $H_1(X;\mathbb{Z}_p)$, ki

je določena z loki $a_1, a_2 \dots, a_r$. Vsak element $[W] \in H_1(X; \mathbb{Z}_p)$ ima enoličen razvoj $[W] = \sum_{i=1}^{r} \lambda_i [W^{a_i}]$ po bazi B_T, zato lahko $[W]$ identificiramo s stolpičnim vektorjem

$$(\lambda_1, \lambda_2, \dots, \lambda_r)^t.$$

Podobno lahko vsak element v $\mathbb{Z}_p^d$ identificiramo s stolpičnim vektorjem v $\mathbb{Z}_p^{d\times 1}$ glede na standardno bazo.

Ker avtomorfizem g slika sklenjene obhode v sklenjene obhode, obstaja naravno (levo) delovanje avtomorfizma g na grupi $H_1(X; \mathbb{Z}_p)$, ki porodi linearno transformacijo $g^{\#}$ na $H_1(X; \mathbb{Z}_p)$. Njeno matrično reprezentacijo glede na bazo B_T predstavimo z matriko $M_g = [g_{ij}] \in \mathbb{Z}_p^{r\times r}$, katere koeficiente g_{ij} dobimo iz razvoja

$$g^{\#}([W^{a_i}]) = \sum_{j=1}^{r} g_{ji} [W^{a_j}].$$

Poleg tega dani regularni napetostni funkciji $\zeta\colon X \to \mathbb{Z}_p^d$ na grafu X priredimo matriko napetosti

$$M_\zeta = \begin{bmatrix} \zeta(W^{a_1})^t \\ \zeta(W^{a_2})^t \\ \vdots \\ \zeta(W^{a_r})^t \end{bmatrix} \in \mathbb{Z}_p^{r\times d},$$

kjer napetosti $\zeta(W^{a_r})$ identificiramo s stolpičnimi vektorji v $\mathbb{Z}_p^{d\times 1}$ glede na standardno bazo prostora $\mathbb{Z}_p^d$. Opozorimo, da je ζ povezana natanko tedaj, ko je rang matrike M_ζ enak d. V tem primeru se avtomorfizem g dvigne vzdolž izpeljane krovne projekcije $\wp_\zeta\colon X \times_\zeta \mathbb{Z}_p^d \to X$ natanko tedaj, ko stolpci

$$M_\zeta^{(1)}, M_\zeta^{(2)}, \dots, M_\zeta^{(d)}$$

matrike M_ζ tvorijo bazo d-razsežnega podprostora $S(\zeta) \leq \mathbb{Z}_p^{r\times 1}$, ki je invarianten za matriko M_g^t. Če je ζ' druga napetostna funkcija z vrednostmi v $\mathbb{Z}_p^d$, ki tudi zadošča zgornjemu pogoju, potem sta napetostni funkciji ζ in ζ' ekvivalentni natanko tedaj, ko velja $S(\zeta') = S(\zeta)$.

Torej lahko do ekvivalence natanko poiščemo vse regularne napetostne funkcije grafa X, ki porodijo povezane g-dopustne elementarno abelske regularne krovne projekcije, na naslednji način. Najprej poiščemo bazo $\{u_1, u_2 \dots, u_d\}$ za vsak podprostor

$U \leq \mathbb{Z}_p^{r\times 1}$, ki je invarianten za matriko M_g^t. Nato za vsako bazo $\{u_1, u_2 \dots, u_d\}$ zgradimo matriko $M_U \in \mathbb{Z}_p^{r\times d}$ s stolpci $u_1, u_2, \dots, u_d$ in definiramo regularno napetostno funkcijo $\zeta\colon X \to \mathbb{Z}_p^{d\times 1}$ na grafu X, ki loku a_i v kodrevesu $X - T$ priredi transponirano i-to vrstico matrike M_U, medtem ko vsakemu loku v drevesu T priredi ničelni vektor v $\mathbb{Z}_p^{d\times 1}$. Poleg tega lahko do ekvivalence krovnih projekcij natanko vpeto drevo skupaj z orientacijo grafa, kot tudi urejeno bazo invariantnega prostora, izberemo poljubno. Posledično se problem iskanja povezanih g-dopustnih elementarno abelskih regularnih krovnih projekcij prevede na problem iskanja invariantnih podprostorov matrične grupe.

V tem kontekstu naj bo $A \in \mathbb{Z}_p^{n\times n}$ matrika nad poljem $\mathbb{Z}_p$, ki deluje kot linearna transformacija na prostoru $\mathbb{Z}_p^{n\times 1}$. Nadalje, naj bo $\kappa_A(x) = f_1(x)^{n_1} f_2(x)^{n_2} \cdots f_k(x)^{n_k}$ njen karakteristični polinom, $m_A(x) = f_1(x)^{s_1} f_2(x)^{s_2} \cdots f_k(x)^{s_k}$ pa njen minimalni polinom, kjer so polinomi f_i paroma različni in nerazcepni nad $\mathbb{Z}_p$. Potem lahko prostor $\mathbb{Z}_p^{n\times 1}$ zapišemo kot direktno vsoto A-invariantnih podprostorov

$$\mathbb{Z}_p^{n\times 1} = \mathrm{Ker} f_1(A)^{s_1} \oplus \mathrm{Ker} f_2(A)^{s_2} \oplus \cdots \oplus \mathrm{Ker} f_k(A)^{s_k}.$$

Poleg tega so vsi A-invariantni podprostori direktne vsote nekaterih A-invariantnih podprostorov v $\mathrm{Ker} f_i(A)^{s_i}$.

Pogosto lahko pri iskanju invariantnih prostorov matrične grupe uporabimo Maschkejev izrek, ki pravi, da je njena reprezentacija popolnoma razcepna, če karakteristika polja ne deli reda grupe. V tem primeru moramo pravzaprav poiskati le minimalne invariantne podprostore. Posebej, če red matrike A ni deljiv s p, potem je vsak A-invarianten podprostor direktna vsota minimalnih. Za podrobnejši opis iskanja invariantnih prostorov glej [49].

2.6 Analiza algoritmov in izračunljivost

V tem kratkem pregledu se bomo izognili formalni definiciji algoritma kot Turingovega stroja (glej na primer [47]). Neformalno je *algoritem* postopek za reševanje problema, ki na začetku dobi določene *podatke*, na koncu svojega delovanja pa vrne *rezultat*. Podatkom algoritma pravimo tudi *vhodni parametri*, rezultatu pa *izhodni parametri*. Pomembno je, da je rezultat pri vseh podatkih enolično določen.

Časovna zahtevnost algoritma je določena z največjim številom računskih korakov, ki jih algoritem potrebuje za rešitev problema pri dani velikosti problema. Podamo jo

kot funkcijo velikosti vhodnih parametrov. Podobno definiramo tudi *prostorsko zahtevnost*. Računske korake merimo v osnovnih operacijah računalnika, ki izvaja algoritem. Ocena je seveda odvisna od tega, kako definiramo ceno operacije. V splošnem se uporabljata dva modela:

(i) model z enakomerno ceno – posamezna operacija ima konstantno ceno ne glede na velikost operandov;
(ii) model z logaritemsko ceno – posamezna operacija ima ceno, ki je odvisna od velikosti operandov.

V disertaciji uporabljamo prvi model. Poleg tega nas zanima zgolj hitrost rasti zahtevnosti algoritma in ne točna vrednost, zato definirajmo pojem reda velikosti, ki ga predstavimo v $\mathcal{O}$-zapisu . Za dani funkciji $f, g\colon \mathbb{N} \to \mathbb{R}$ rečemo, da je g kvečjemu *reda* f, če obstajata taki pozitivni konstanti C in n_0, da velja $|g(n)| \leq C|f(n)|$ za vsak $n > n_0$. Tedaj pišemo $g(n) = \mathcal{O}(f(n))$. Časovno in prostorsko zahtevnost ponavadi podamo v $\mathcal{O}$-zapisu.

Za učinkovito izvedbo algoritma moramo skrbno izbrati *podatkovno strukturo*, s katero predstavimo podatke. V disertaciji grafe predstavimo s seznamom sosedov, kjer za vsako vozlišče podamo seznam njegovih sosedov. Kar zadeva predstavitve grup, ločimo naslednja primera:

(i) grupa G je dana kot prezentacija $\langle S_G \,|\, R_G \rangle$ – izračunamo lahko vsak element grupe G, znamo izračunati inverze in produkte elementov, ni pa nujno, da znamo določiti, ali reprezentaciji dveh elementov definirata isti element;
(ii) grupa G je dana kot permutacijska grupa, definirana s poljubno množico generatorjev – kot v primeru (i), le da znamo določiti, ali reprezentaciji dveh elementov definirata isti element.

Za dano grupo je osnovni cilj ta, da jo prevedemo v obliko, ki omogoča učinkovito nadaljnjo računanje s to grupo. Če je grupa G dana s prezentacijo $\langle S_G \,|\, R_G \rangle$ – ob dodatni predpostavki, da je končna – potem lahko naredimo njeno regularno reprezentacijo z uporabo Todd-Coxeterjevega algoritma za preštevanje odsekov (glej recimo [50, Poglavje 5]). Obratno, za permutacijsko grupo, dano na množici generatorjev, je včasih potrebno izračunati njeno prezentacijo. To lahko dosežemo z Modificiranim Todd-Coxeterjevim algoritmom, ki poišče prezentacijo grupe za dano množico generatorjev (glej recimo [50, Poglavje 5]).

Kar zadeva samo analizo kompleksnosti algoritmov, ki vključujejo računanje z grupami, moramo izpostaviti naslednje. Če imamo opraviti s permutacijskimi grupami, potem lahko kompleksnost takšnih algoritmov teoretično analiziramo. Precej težja pa je analiza kompleksnosti, kadar računamo s prezentacijami grup. Veliko problemov, ki so povezani s takšnimi grupami, namreč nima algoritmičnih rešitev. Obstajajo postopki za reševanje nekaterih tovrstnih problemov, vendar pa se le-ti ustavijo samo v primerih, kadar ima rešitev določeno obliko. V ostalih primerih se postopek v končnem številu korakov ne ustavi. V tem primeru kompleksnosti ni mogoče teoretično analizirati. Čeprav nimamo primernega teoretičnega ozadja, pa se je še vedno potrebno odločiti, katere tehnike uporabiti. Ponavadi nam ostane zgolj možnost eksperimentalne analize, kjer na množici testnih podatkov primerjamo rezultate posameznih metod.

Eno od vprašanj, ki si ga naravno zastavimo pri računanju s prezentacijami grup, je naslednje: ali je grupa $G = \langle S_G | R_G \rangle$ končna? Problem je teoretično dokazano nerešljiv. Posledično je nerešljiv tudi problem preštevanja odsekov. Če je namreč odsekov neskončno, bo vsak algoritem tekel neskončno časa. Po drugi strani pa velja naslednje: čeprav v splošnem ne moremo določiti, ali je grupa $G = \langle S_G | R_G \rangle$ končna, pa lahko – če se izkaže, da je končna – to preverimo. Drugače rečeno, Todd-Coxeterjev algoritem za preštevanje odsekov se ustavi po končno korakih natanko tedaj, ko je grupa končna. Posledica opisanih dejstev je, da za slednji algoritem ne obstaja izračunljiva zgornja meja za časovno zahtevnost. Kljub temu pa je Todd-Coxeterjev algoritem presenetljivo uporaben že vse od tridesetih let prejšnjega stoletja – učinkovit tudi brez uporabe računalnika.

3

Testiranje dviga avtomorfizmov

V tem poglavju se posvetimo razvoju algoritmov, ki odgovorijo na osnovno vprašanje, kdaj se dani avtomorfizem baznega grafa dvigne vzdolž krovne projekcije, podane z napetostno funkcijo. Za permutacijske napetosti problem najprej prevedemo na poseben primer testiranja izomorfizma grafov in nato predstavimo znane algoritme za reševanje slednjega problema. V primeru regularnih napetosti pa uporabimo standarden rezultat iz računske teorije grup.

3.1 Permutacijske napetosti

Naj bo X končen povezan graf in $\zeta\colon X \to S_n$ povezana permutacijska napetostna funkcija. Izberimo vpeto drevo T s korenom v baznem vozlišču u in urejeno orientacijo $A^+(X) = \{a_1, a_2, \dots, a_t\}$ grafa X tako, da so $a_1, a_2 \dots, a_r$ loki v kodrevesu $X - T$, $a_{r+1}, a_{r+2}, \dots, a_t$ pa loki v drevesu T. Za testiranje, ali se avtomorfizem g grafa X dvigne vzdolž izpeljane krovne projekcije $\wp\colon X \times_\zeta [n] \to X$, je po osnovni lemi o dvigu dovolj preveriti, ali ima sistem enačb

$$\begin{aligned} \tau^{-1}\zeta(W^{a_1})\tau &= \zeta(g(W^{a_1})) \\ \tau^{-1}\zeta(W^{a_2})\tau &= \zeta(g(W^{a_2})) \\ &\vdots \\ \tau^{-1}\zeta(W^{a_r})\tau &= \zeta(g(W^{a_r})) \end{aligned} \tag{3.1}$$

rešitev v simetrični grupi S_n, kjer je W^{a_i} fundamentalni obhod v vozlišču u, določen z drevesom T in lokom a_i. Napetosti $\zeta(W^{a_i})$ in $\zeta(g(W^{a_i}))$ lahko učinkovito izračunamo s pregledom grafa v širino (s korenom v u).

Da si poenostavimo notacijo, pišimo $\alpha_i = \zeta(W^{a_i})$ in $\alpha_i' = \zeta(g(W^{a_i}))$ za $i = 1, 2, \dots, r$. Spomnimo, da permutacije α_i generirajo lokalno napetostno grupo Loc_u v u, medtem ko permutacije α_i' generirajo lokalno napetostno grupo $\mathrm{Loc}_{g(u)}$ v preslikanem vozlišču $g(u)$, saj je g avtomorfizem. Poleg tega so vse lokalne napetostne grupe tranzitivne, ker je napetostna funkcija povezana.

Oglejmo si najprej poseben primer zgornjega sistema, ko je $\alpha_i' = \alpha_i$ za vse indekse i; v tem primeru iščemo centralizator $\mathrm{C}_{S_n}(\mathrm{Loc}_u)$ lokalne napetostne grupe Loc_u v S_n. Ker je Loc_u tranzitivna grupa, je centralizator $\mathrm{C}_{S_n}(\mathrm{Loc}_u)$ polregularen, zato je njegova moč $|\mathrm{C}_{S_n}(\mathrm{Loc}_u)| \leq n$. Še več, centralizator $\mathrm{C}_{S_n}(\mathrm{Loc}_u)$ je pravzaprav izomorfen grupi krovnih transformacij $CT(\wp)$.

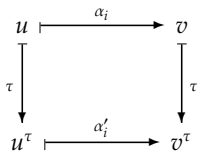
Recimo, da je $\tau \in S_n$ poljubna rešitev sistema (3.1) in $c \in \mathrm{C}_{S_n}(\mathrm{Loc}_u)$. Potem velja

$$(c\tau)^{-1}\alpha_i(c\tau) = \tau^{-1}c^{-1}\alpha_i c\tau = \tau^{-1}\alpha_i\tau = \alpha_i',$$

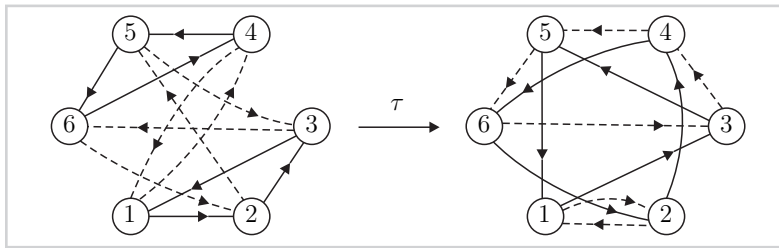
zato so vse rešitve oblike $c\,\tau$. Drugače rečeno, če je sistem (3.1) rešljiv, je število vseh rešitev enako moči $|\mathrm{C}_{S_n}(\mathrm{Loc}_u)|$ centralizatorja. Slednje je reformulacija trditve, da ima avtomorfizem g, če se dvigne, natanko $|CT(\wp)|$ različnih dvigov.

Zgornji sistem (3.1) ima lepo interpretacijo v jeziku teorije grafov. Opazimo, da lahko permutacijo $\alpha \in S_n$ predstavimo z usmerjenim grafom na množici vozlišč $[\,n\,]$, kjer so usmerjene povezave oblike (k, k^c), $k \in [\,n\,]$. Uporabimo to idejo za predstavitev zaporedja $(\alpha_1, \alpha_2, \dots, \alpha_r)$ permutacij. *Barvni permutacijski graf* $X(\alpha_1, \alpha_2, \dots, \alpha_r)$ je usmerjen multigraf na množici vozlišč $[\,n\,]$, kjer obstaja usmerjena povezava (k, k') z barvo i natanko tedaj, ko velja $k^{\alpha_i} = k'$. Po definiciji je usmerjen graf *krepko povezan*, če za poljubni vozlišči $k = k_0$ in $k' = k_n$ obstaja *usmerjen sprehod* od k do k', to je, zaporedje vozlišč $(k_0, k_1, \dots, k_n)$, kjer je (k_{i-1}, k_i) usmerjena povezava za vse $1 \le i \le n$. Hitro se lahko prepričamo, da je barvni permutacijski graf $X(\alpha_1, \alpha_2, \dots, \alpha_r)$ krepko povezan natanko tedaj, ko je grupa $\langle \alpha_1, \alpha_2, \dots, \alpha_r \rangle$ tranzitivna. Poleg tega lahko definicijo izomorfizma grafov posplošimo na barvne permutacijske grafe. *Izomorfizem* barvnih permutacijskih grafov $X(\alpha_1, \alpha_2, \dots, \alpha_r)$ in $X(\alpha_1', \alpha_2', \dots, \alpha_r')$, ki *ohranja barve*, je taka permutacija $\tau \in S_n$, da za vsak par vozlišč k, k' v $X(\alpha_1, \alpha_2, \dots, \alpha_r)$ velja: (k, k') je usmerjena povezava v $X(\alpha_1, \alpha_2, \dots, \alpha_r)$ z barvo i natanko tedaj, ko je $(k^\tau, (k')^\tau)$ usmerjena povezava v $X(\alpha_1', \alpha_2', \dots, \alpha_r')$ z barvo i.

Prepišimo sedaj zgornje enačbe v obliko $\alpha_i\tau = \tau\alpha_i'$, to je, oglejmo si komutativni diagram



za vsak $i = 1, 2, \dots, r$. Iz definicije barvnih permutacijskih grafov in njihovih izomorfizmov takoj sledi, da vsaka permutacija τ, ki reši zgornji sistem, natanko ustreza izomorfizmu grafov $X(\alpha_1, \alpha_2, \dots, \alpha_r)$ in $X(\alpha_1', \alpha_2', \dots, \alpha_r')$, ki ohranja barve. Torej velja naslednja trditev.



Slika 3.1

Barvna permutacijska grafa.

Trditev 3.1.1: Pri zgornji notaciji ima sistem permutacijskih enačb $\tau^{-1}\alpha_i\tau = \alpha_i'$, $i = 1, 2, \dots, r$, rešitev natanko tedaj, ko obstaja tak izomorfizem med barvnima permutacijskima grafoma $X(\alpha_1, \alpha_2, \dots, \alpha_r)$ in $X(\alpha_1', \alpha_2', \dots, \alpha_r')$, ki ohranja barve. Poleg tega so vse rešitve sistema v bijektivni korespondenci z vsemi takšnimi izomorfizmi.

Primer 3.1.2: Oglejmo si naslednji sistem permutacijskih enačb v grupi S_6:

$$\begin{aligned}\tau^{-1}(1,2,3)(4,5,6)\tau &= (1,3,5)(2,4,6)\\ \tau^{-1}(1,4)(2,5,3,6)\tau &= (1,2)(3,4,5,6).\end{aligned}$$

Njegova grafična interpretacija je predstavljena na Sliki 3.1 s permutacijskima grafoma $X((1,2,3)(4,5,6),(1,4)(2,5,3,6))$ (levo) in $X((1,3,5)(2,4,6),(1,2)(3,4,5,6))$ (desno).

Problem smo iz teorije grup tako prevedli na vprašanje, ali obstaja izomorfizem med permutacijskima grafoma $X(\alpha_1, \alpha_2, \dots, \alpha_r)$ in $X(\alpha_1', \alpha_2', \dots, \alpha_r')$, ki ohranja barve. Slednje vprašanje je prvič obravnavano v [51], kjer je predstavljen polinomski algoritem za testiranje, ali obstaja izomorfizem med danima permutacijskima grafoma, ki ohranja barve. Osnovna ideja je naslednja. Naj bo τ izomorfizem med permutacijskima grafoma $X(\alpha_1, \alpha_2, \dots, \alpha_r)$ in $X(\alpha_1', \alpha_2', \dots, \alpha_r')$, ki ohranja barve; vozlišče k naj preslika v vozlišče k^τ. Ker τ ohranja barve, se za vsak α_i vozlišče k^{α_i} preslika v vozlišče $(k^\tau)^{\alpha_i'}$. Zaradi krepke povezanosti grafov $X(\alpha_1, \alpha_2, \dots, \alpha_r)$ in $X(\alpha_1', \alpha_2', \dots, \alpha_r')$ po indukciji sledi, da je izomorfizem τ natanko določen s sliko enega vozlišča. Kot posledico te opazke dobimo naslednjo trditev.

Trditev 3.1.3: [51, Poglavje 6, Posledica 2] Če sta $X(\alpha_1, \alpha_2, \dots, \alpha_r)$ in $X(\alpha_1', \alpha_2', \dots, \alpha_r')$ krepko povezana permutacijska grafa na n vozliščih, potem lahko v $\mathcal{O}(n^2 r)$ korakih

testiramo, ali obstaja izomorfizem med grafoma $X(\alpha_1, \alpha_2, \dots, \alpha_r)$ in $X(\alpha'_1, \alpha'_2, \dots, \alpha'_r)$, ki ohranja barve.

Dokaz: Naj bo k poljubno vozlišče grafa $X(\alpha_1, \alpha_2, \dots, \alpha_r)$. Za vsako vozlišče k' v grafu $X(\alpha'_1, \alpha'_2, \dots, \alpha'_r)$ lahko v $\mathcal{O}(nr)$ korakih preverimo, ali preslikava, ki preslika vozlišče k v vozlišče k', določa izomorfizem. Ker je moč množice vozlišč grafa $X(\alpha'_1, \alpha'_2, \dots, \alpha'_r)$ enaka n, trditev sledi. □

Poleg tega opazimo, da potrebujemo $\mathcal{O}(rn)$ prostora za testiranje, ali obstaja izomorfizem med grafoma $X(\alpha_1, \alpha_2, \dots, \alpha_r)$ in $X(\alpha'_1, \alpha'_2, \dots, \alpha'_r)$, ki ohranja barve. Nekaj let kasneje je v [52] predstavljen učinkovitejši algoritem, ki reši problem izomorfizma permutacijskih grafov v $\mathcal{O}(nr \log(nr))$ korakih, uporabljajoč $\mathcal{O}(nr)$ prostora. Še vedno pa ostaja odprto vprašanje, ali obstaja algoritem z boljšo časovno zahtevnostjo. Z drugimi besedami, ali je $\mathcal{O}(nr \log(nr))$ spodnja meja?

Lahko pa precej več povemo v primeru, ko s permutacijskimi napetostmi rekonstruiramo regularno krovno projekcijo povezanih grafov. Poleg tega se nam niti ni potrebno sklicevati na rezultat iz [52]. Tedaj je namreč lokalna napetostna grupa Loc_u regularna, zato je centralizator $\mathrm{C}_{S_n}(\mathrm{Loc}_u)$ regularen. Drugače povedano, brž ko je sistem (3.1) rešljiv, potem za poljubno izbrana $k, k' \in [n]$ obstaja taka rešitev τ, za katero velja $k^\tau = k'$. V luči Trditve 3.1.3 in zgornje opazke dobimo v primeru regularni krovov naslednjo posledico.

Posledica 3.1.4: Pri zgornji notaciji in predpostavki, da permutacijska napetostna funkcija $\zeta\colon X \to S_n$ rekonstruira regularno krovno projekcijo povezanih grafov, lahko v $\mathcal{O}(nr)$ korakih testiramo, ali obstaja izomorfizem med permutacijskima grafoma $X(\alpha_1, \alpha_2, \dots, \alpha_r)$ in $X(\alpha'_1, \alpha'_2, \dots, \alpha'_r)$, ki ohranja barve.

Povežimo sedaj vsa opažanja iz zgornje diskusije med sabo, pa dobimo algoritem za testiranje dviga avtomorfizmov. Formalna koda je podana v Algoritmu 3.1.

Izrek 3.1.5: Za dano povezano permutacijsko napetostno funkcijo $\zeta\colon X \to S_n$ na končnem povezanem grafu X ranga r Algoritem 3.1 testira, ali se dani avtomorfizem g dvigne.

Izrek 3.1.6: Za povezano permutacijsko napetostno funkcijo $\zeta\colon X \to S_n$ na končnem povezanem grafu X ranga r obstaja algoritem, ki reši problem testiranja dviga avtomorfizma v $\mathcal{O}(|V(X)| + n|E(X)| + nr \log(nr))$ korakih, uporabljajoč $\mathcal{O}(|V(X)| + n|E(X)|)$ prostora.

Algoritem 3.1: Testiranje dviga – permutacijske napetosti

Vhodni parametri: povezana permutacijska napetostna funkcija $\zeta\colon X \to S_n$ na končnem povezanem grafu X ranga r, avtomorfizem g grafa X

Izhodni parametri: true, če se g dvigne, false sicer

1: izračunaj napetosti $\alpha_i = \zeta(W^{a_i})$ in $\alpha'_i = \zeta(g(W^{a_i}))$ za $i = 1, 2, \dots, r$;
2: testiraj, ali obstaja izomorfizem med permutacijskima grafoma $X(\alpha_1, \alpha_2, \dots, \alpha_r)$ in $X(\alpha'_1, \alpha'_2, \dots, \alpha'_r)$, ki ohranja barve;
3: *if* obstaja izomorfizem *then*
4: *return* true;
5: *else*
6: *return* false;

Dokaz: V Algoritmu 3.1 lahko napetosti α_i in α'_i izračunamo s pregledom grafa v širino, kjer je cena vsake povezave $\mathcal{O}(n)$; skupaj to vzame $\mathcal{O}(|V(X)| + n|E(X)|)$ korakov. Nadalje, obstaja algoritem, ki v $\mathcal{O}(nr \log(nr))$ korakih testira, ali obstaja izomorfizem med permutacijskima grafoma $X(\alpha_1, \alpha_2, \dots, \alpha_r)$ in $X(\alpha'_1, \alpha'_2, \dots, \alpha'_r)$, ki ohranja barve. Torej lahko testiramo, ali se dani avtomorfizem dvigne v $\mathcal{O}(|V(X)| + n|E(X)| + nr \log(nr))$ korakih.

Za predstavitev grafa X s seznamom sosedov potrebujemo $\mathcal{O}(|V(X)| + |E(X)|)$ prostora, za poljubno permutacijo v S_n pa $\mathcal{O}(n)$ prostora. Torej lahko napetostno funkcijo ζ predstavimo z $\mathcal{O}(|V(X)| + n|E(X)|)$ prostora, avtomorfizem g pa z $\mathcal{O}(|V(X)|)$. Med pregledom grafa v širino potrebujemo $\mathcal{O}(n|E(X)|)$ dodatnega prostora, za izračun napetosti α_i ter α'_i, medtem ko pri testiranju izomorfizma potrebujemo še $\mathcal{O}(nr)$ dodatnega prostora. Prostorska zahtevnost je zato enaka $\mathcal{O}(|V(X)| + n|E(X)|)$. □

V primeru regularnih krovnih projekcij se časovna zahtevnost izboljša. Tedaj lahko namreč za testiranje, ali obstaja izomorfizem permutacijskih grafov, ki ohranja barve, uporabimo kar rezultat iz Posledice 3.1.4.

Izrek 3.1.7: Če funkcija $\zeta\colon X \to S_n$ rekonstruira povezano regularno krovno projekcijo, potem obstaja algoritem, ki reši problem testiranja v $\mathcal{O}(|V(X)| + n|E(X)|)$ korakih, uporabljajoč $\mathcal{O}(|V(X)| + n|E(X)|)$ prostora.

Nazadnje spomnimo, da se testiranje ekvivalence krovnih projekcij, rekonstruiranih

s permutacijskimi napetostmi, prav tako prevede na reševanje sistema permutacijskih enačb. Natančneje, če je $\zeta' : X \to S_n$ neka druga povezana permutacijska napetostna funkcija, potem je potrebno rešiti sistem enačb $\alpha_i^{-1} \tau \alpha_i = \alpha_i'$, kjer je $\alpha_i' = \zeta'(W^{a_i})$, $i = 1, 2, \ldots, r$.

3.2 Regularne napetosti

Naj bo Γ končna napetostna grupa, dana s prezentacijo $\langle S_\Gamma | R_\Gamma \rangle$, in $\zeta : X \to \Gamma$ povezana regularna napetostna funkcija. Prvi način za testiranje, ali se avtomorfizem g dvigne, je ta, da regularne napetosti prevedemo v permutacijske napetosti in rešujemo sistem permutacijskih enačb, opisan v prejšnjem razdelku. Napetosti prevedemo v permutacijske z uporabo Todd-Coxeterjevega algoritma za preštevanje odsekov, s katerim lahko izračunamo regularno permutacijsko reprezentacijo grupe Γ. Drugi način bomo opisali v tem razdelku.

Osnovna ideja temelji na naslednjem standardnem rezultatu iz računske teorije grup, ki poda učinkovit test, ali je preslikava Θ iz grupe H v grupo K homomorfizem.

Izrek 3.2.1: [50, Izrek 2.53] Naj bo $H = \langle S_H | R_H \rangle$ prezentacija končne grupe in $\Theta : S_H \to K$ preslikava iz množice generatorjev S_H v končno grupo K. Potem se preslikava Θ razširi do homomorfizma grup natanko tedaj, ko velja $\Theta(s_1)\Theta(s_2) \cdots \Theta(s_k) = 1$ za vse relatorje $w = s_1 s_2 \cdots s_k \in R_H$. Ta razširitev je enolična, če obstaja.

Spomnimo, da se v primeru regularnih napetosti avtomorfizem g dvigne natanko tedaj, ko obstaja avtomorfizem $g^{\#_u}$ napetostne grupe Γ, lokalno definiran v vozlišču u s predpisom

$$g^{\#_u}(\zeta(W^{a_i})) = \zeta(g(W^{a_i})), \quad i = 1, 2, \ldots, r, \tag{3.2}$$

kjer je W^{a_i} fundamentalni obhod z začetkom v u. Ker je napetostna funkcija povezana, napetosti fundamentalnih obhodov $\zeta(W^{a_i})$ kot tudi napetosti preslikanih fundamentalnih obhodov $\zeta(g(W^{a_i}))$ generirajo napetostno grupo Γ. Torej je vsak endomorfizem napetostne grupe Γ, ki je lokalno definiran v vozlišču u z zgornjim predpisom (3.2), dejansko epimorfizem in zaradi končnosti grupe Γ avtomorfizem. Zato je dovolj preveriti, ali se predpis

$$\zeta(W^{a_i}) \mapsto \zeta(g(W^{a_i})) \tag{3.3}$$

iz množice generatorjev $\{\zeta(W^{a_i}) | i = 1, 2, \ldots, r\}$ v grupo Γ razširi do endomorfizma grupe. Po Izreku 3.2.1 moramo torej poiskati prezentacijo grupe Γ na množici ge-

neratorjev $\{\zeta(W^{a_i}) | i = 1, 2, \dots, r\}$. To lahko dosežemo z uporabo tako imenovanega Modificiranega Todd-Coxeterjevega algoritma, ki poišče prezentacijo grupe za dano množico generatorjev.

Zgornja opažanja porodijo algoritem, ki reši problem dviga avtomorfizma v primeru regularnih napetosti. Formalna koda je podana v Algoritmu 3.2.

Algoritem 3.2: Testiranje dviga – regularne napetosti

Vhodni parametri: povezana regularna napetostna funkcija $\zeta: X \to \Gamma$ na končnem povezanem grafu X ranga r, kjer je Γ končna grupa, dana s prezentacijo $\langle S_\Gamma | R_\Gamma \rangle$,
avtomorfizem g grafa X

Izhodni parametri: true, če se g dvigne, false sicer

1: izračunaj napetosti $\alpha_i = \zeta(W^{a_i})$ in $\alpha'_i = \zeta(g(W^{a_i}))$ za $i = 1, 2, \dots, r$;
2: izračunaj prezentacijo $\langle \alpha_1, \alpha_2, \dots, \alpha_r | R \rangle$ grupe Γ na množici generatorjev $\{\alpha_i | i = 1, 2, \dots, r\}$ z Modificiranim Todd-Coxeterjevim algoritmom;
3: *dvig* ← true;
4: *for* $r \in R$ *do*
5: predpostavimo, da je $r = \alpha_{k_1} \cdots \alpha_{k_l}$;
6: *if* $\alpha'_{k_1} \cdots \alpha'_{k_l} \neq 1_\Gamma$ *then*
7: *dvig* ← false;
8: break;
9: *return dvig*;

Izrek 3.2.2: Za dano povezano regularno napetostno funkcijo $\zeta: X \to \Gamma$ na končnem povezanem grafu X ranga r Algoritem 3.2 testira, ali se dani avtomorfizem g dvigne.

Kot v primeru permutacijskih napetosti lahko tudi tu opisano metodo uporabimo za testiranje ekvivalence regularnih krovnih projekcij. Če je $\zeta': X \to \Gamma$ tudi povezan regularna napetostna funkcija, potem napetosti $\zeta(g(W^{a_i}))$ nadomestimo z napetostmi $\zeta'(W^{a_i})$.

3.2.1 *Elementarno abelski regularni krovi*

Posebej omembe vredne so elementarno abelske regularne krovne projekcije. Vemo že, da lahko v tem primeru napetostno grupo Γ identificiramo z vektorskim prostorom,

njene avtomorfizme pa z obrnljivimi linearnimi preslikavami. Tedaj je potrebno testirati, ali se preslikava (3.3) razširi do endomorfizma vektorskega prostora, kar je – kot bomo videli v nadaljevanju – precej enostavnejše.

Naj bo torej $\Gamma = \mathbb{Z}_p^d$, kjer je p praštevilo. Množica generatorjev S_Γ predstavlja standardno bazo vektorskega prostora $\mathbb{Z}_p^d$ nad $\mathbb{Z}_p$. Iz linearne algebre vemo, da se vsaka preslikava, definirana na baznih vektorjih, enolično razširi do endomorfizma vektorskega prostora. Opozorimo, da je zaradi povezanosti krovnega grafa razsežnost d navzgor omejena z rangom r. Torej množica $\{\zeta(W^{a_i}) | i = 1, 2, \dots, r\}$ v splošnem ni baza, je pa ogrodje prostora Γ.

Test, ali se preslikava, definirana na ogrodju, razširi do endomorfizma, lahko naredimo z uporabo Gaussovega postopka. Identificirajmo napetostni $\zeta(W^{a_i})$ in $\zeta(g(W^{a_i}))$ s stolpičnimi vektorji v $\mathbb{Z}_p^{d\times 1}$ glede na standardno bazo prostora $\mathbb{Z}_p^d$ in si oglejmo matriki napetosti

$$M_\zeta = \begin{bmatrix} \zeta(W^{a_1})^t \\ \vdots \\ \zeta(W^{a_r})^t \end{bmatrix} \in \mathbb{Z}_p^{r\times d} \quad \text{ter} \quad M_{\zeta\circ g} = \begin{bmatrix} \zeta(g(W^{a_1}))^t \\ \vdots \\ \zeta(g(W^{a_r}))^t \end{bmatrix} \in \mathbb{Z}_p^{r\times d}.$$

Tedaj velja naslednji izrek.

Izrek 3.2.3: Pri zgornji notaciji in predpostavkah se predpis $\zeta(W^{a_i}) \mapsto \zeta(g(W^{a_i}))$ razširi do endomorfizma vektorskega prostora natanko tedaj, ko ima razširjena matrika

$$\left[M_\zeta \;\middle|\; M_{\zeta\circ g} \right] \in \mathbb{Z}_p^{r\times 2d}$$

rang d.

Dokaz: Brez škode za splošnost lahko predpostavimo, da vektorji

$$\zeta(W^{a_1}), \zeta(W^{a_2}), \dots, \zeta(W^{a_d})$$

tvorijo bazo. Potem se predpis $\zeta(W^{a_i}) \mapsto \zeta(g(W^{a_i}))$ razširi do endomorfizma natanko tedaj, ko za vsak $i = d+1, d+2, \dots, r$ velja: če je $\zeta(W^{a_i}) = \lambda_1\zeta(W^{a_1}) + \lambda_2\zeta(W^{a_2}) + \cdots + \lambda_d\zeta(W^{a_d})$, potem je $\zeta(g(W^{a_i})) = \lambda_1\zeta(g(W^{a_1})) + \lambda_2\zeta(g(W^{a_2})) + \cdots + \lambda_d\zeta(g(W^{a_d}))$. Toda ta pogoj je ekvivalenten zahtevi, da ima razširjena matrika rang d. □

V luči zgornje razprave in Izreka 3.2.3 se torej g dvigne vzdolž povezane elementarno abelske regularne krovne projekcije natanko tedaj, ko ima razširjena matrika

$\left[M_\zeta \;\middle|\; M_{\zeta\circ g}\right]$ rang d. Na kriterij za dvig pa lahko pogledamo tudi prek invariantnih podprostorov.

Naj bo $g^\#$ linearna transformacija na $H_1(X;\mathbb{Z}_p)$, inducirana z delovanjem avtomorfizma g na $H_1(X;\mathbb{Z}_p)$, in $M_g \in \mathbb{Z}^{r\times r}$ njena matrična upodobitev glede na bazo prostora $H_1(X;\mathbb{Z}_p)$, porojeno z loki $a_1, a_2, \dots, a_r$. Spomnimo, da se g dvigne natanko tedaj, ko stolpci

$$M_\zeta^{(1)}, M_\zeta^{(2)}, \dots, M_\zeta^{(d)}$$

matrike M_ζ tvorijo bazo d-razsežnega podprostora v $\mathbb{Z}_p^{r\times 1}$, ki je invarianten za matriko M_g^t. Opazimo, da velja $M_g^t \cdot M_\zeta = M_{\zeta\circ g}$. Posebej, slika stolpca $M_\zeta^{(i)}$ je enaka stolpcu $M_g^t \cdot M_\zeta^{(i)} = M_{\zeta\circ g}^{(i)}$. Torej je potrebno preveriti, ali lahko vsak stolpec $M_{\zeta\circ g}^{(i)}$ zapišemo kot linearno kombinacijo stolpcev matrike M_ζ. Ni se težko prepričati, da je slednje ekvivalentno testiranju, ali so linearni sistem

$$M_\zeta \cdot x = M_{\zeta\circ g}^{(i)}$$

rešljivi za $i = 1, 2, \dots, r$. Ker je rang matrike M_ζ enak d, imajo sistemi rešitev natanko tedaj, ko imajo razširjene matrike

$$\left[M_\zeta \;\middle|\; M_{\zeta\circ g}^{(i)}\right]$$

tudi rang d. To pa je natanko pogoj, da ima razširjena matrika $\left[M_\zeta \;\middle|\; M_{\zeta\circ g}\right]$ rang d.

Kar smo povedali zgoraj, porodi algoritem za testiranje dviga avtomorfizma v primeru, ko je napetostna grupa elementarno abelska. Formalna koda je podana v Algoritmu 3.3.

Izrek 3.2.4: Za dano povezano regularno napetostno funkcijo $\zeta\colon X \to \mathbb{Z}_p^d$ na končnem povezanem grafu X ranga r Algoritem 3.3 testira, ali se avtomorfizem g dvigne.

Izrek 3.2.5: Za povezano regularno napetostno funkcijo $\zeta\colon X \to \mathbb{Z}_p^d$ na končnem povezanem grafu X ranga r obstaja algoritem, ki reši problem testiranja dviga avtomorfizma v $\mathcal{O}(|V(X)| + d|E(X)| + r^2 d)$ korakih, uporabljajoč $\mathcal{O}(|V(X)| + d|E(X)|)$ prostora.

Dokaz: Napetosti α_i in α_i' v Algoritmu 3.3 izračunamo s pregledom grafa v širino, kjer je cena vsake povezave $\mathcal{O}(d)$; skupaj to vzame $\mathcal{O}(|V(X)| + d|E(X)|)$ korakov. Nadalje, v $\mathcal{O}(r^2 d)$ korakih lahko z Gaussovim postopkom izračunamo rang matrike $\left[M_\zeta \;\middle|\; M_{\zeta\circ g}\right] \in \mathbb{Z}_p^{r\times 2d}$. Skupaj je torej potrebnih $\mathcal{O}(|V(X)| + d|E(X)| + r^2 d)$ korakov.

Algoritem 3.3: Testiranje dviga – elementarno abelske regularne napetosti

Vhodni parametri: povezana regularna napetostna funkcija $\zeta\colon X \to \mathbb{Z}_p^d$ na končnem povezanem grafu X ranga r, avtomorfizem g grafa X

Izhodni parametri: true, če se g dvigne, false sicer

1: izračunaj napetosti $\alpha_i = \zeta(W^{a_i})$ in $\alpha_i' = \zeta(g(W^{a_i}))$ za $i = 1, 2, \dots, r$;
2: $M_\zeta \leftarrow \left[\alpha_1^t \quad \cdots \quad \alpha_r^t\right]^t$, $M_{\zeta\circ g} \leftarrow \left[(\alpha_1')^t \quad \cdots \quad (\alpha_r')^t\right]^t$;
3: *if* rang$\left(\left[M_\zeta \mid M_{\zeta\circ g}\right]\right)$ == d *then*
4: *return* true;
5: *else*
6: *return* false;

Za predstavitev grafa X s seznamom sosedov potrebujemo $\mathcal{O}(|V(X)| + |E(X)|)$ prostora, za poljubno vektor v $\mathbb{Z}_p^d$ pa $\mathcal{O}(d)$ prostora. Torej lahko napetostno funkcijo ζ predstavimo z $\mathcal{O}(|V(X)| + d|E(X)|)$ prostora, avtomorfizem g pa z $\mathcal{O}(|V(X)|)$. Med pregledom grafa v širino potrebujemo $\mathcal{O}(d|E(X)|)$ dodatnega prostora, da shranimo napetosti. Skupna prostorska zahtevnost je torej $\mathcal{O}(|V(X)| + d|E(X)|)$. □

4

Struktura regularnega dviga in regularnih krovnih projekcij

V tem poglavju začnemo z analizo strukture regularnega dviga – za grupo, ki se dvigne vzdolž regularne krovne projekcije, podane z regularno napetostno funkcijo na baznem grafu, poiščemo prezentacijo dvignjene grupe. Prva možnost je ta, da najprej eksplicitno konstruiramo krovni graf skupaj z dvignjeno grupo in nato uporabimo znane metode za iskanje prezentacije grupe. Ker so eksplicitne konstrukcije potratne, bi se jim radi izognili. Ali lahko zgolj z informacijo o napetostih na baznem grafu in poznavanjem prezentacije osnovne grupe poiščemo prezentacijo dvignjene grupe? Na to vprašanje odgovorimo v prvem razdelku. V ostalih dveh razdelkih opišemo še kombinatorično rekonstrukcijo regularne kompozicije oziroma dekompozicije, kar v nadaljevanju omogoča natančnejšo obravnavo strukture dviga.

4.1 Prezentacija dviga vzdolž regularne projekcije

Naj bo X končen povezan graf, Γ končna napetostna grupa, podana s prezentacijo $\langle S_\Gamma | R_\Gamma \rangle$, in $\zeta\colon X \to \Gamma$ povezana regularna napetostna funkcija. Naj se dana podgrupa G avtomorfizmov grafa X dvigne vzdolž regularne krovne projekcije $\wp\colon X \times_\zeta \Gamma \to X$. V tem razdelku predstavimo metodo, kako poiskati prezentacijo dvignjene grupe $\tilde{G}$, ne da bi eksplicitno konstruirali krovni graf $X \times_\zeta \Gamma$ niti grupo $\tilde{G}$.

Dejstvo, da je grupa $\tilde{G}$ razširitev grupe $CT(\wp)$ po grupi G, omogoča, da lahko uporabimo splošne metode za iskanje prezentacije razširitve. V ta namen moramo najprej poiskati prezentacijo $\langle S_G \mid R_G \rangle$ grupe G. V praksi je G končna permutacijska grupa, dana z množico generatorjev, zato lahko uporabimo znane metode za izračun njene prezentacije (glej na primer [50, Poglavje 6]).

Spomnimo, da je vsak dvig enolično določen s sliko enega vozlišča. Naj bo

$$\tilde{S}_\Gamma = \{\tilde{id}_c \,|\, c \in S_\Gamma\}$$

množica krovnih transformacij, ki je porojena iz množice generatorjev S_Γ in

$$\tilde{R}_\Gamma = \{\tilde{\lambda} \,|\, \lambda \in R_\Gamma\}$$

množica besed nad generatorji $\tilde{S}_\Gamma$, ki jo dobimo iz relatorjev v R_Γ tako, da vsak generator c zamenjamo s pripadajočo krovno transformacijo $\tilde{id}_c$, kadarkoli se le-ta pojavi. Označimo s

$$\tilde{S}_G = \{\tilde{g}_1 \,|\, g \in S_G\}$$

še množico predstavnikov algebraične transverzale podgrupe $CT(\wp)$ v grupi $\tilde{G}$, kjer je $\tilde{g}_1$ tisti dvig avtomorfizma g, ki preslika $(u,1)$ v $(g(u),1)$. Nadalje, za vsak relator $r \in R_G$ naj bo $\tilde{r}$ beseda nad $\tilde{S}_G$, ki jo dobimo iz r tako, da vsak g zamenjamo z $\tilde{g}_1$, kadarkoli se la-ta pojavi. Tedaj za vsak $\tilde{r}$ velja $\wp_{\tilde{c}}(\tilde{r}) = id$, zato je $\tilde{r}$ v $CT(\wp)$. Vsak element $\tilde{r}$ lahko torej zapišemo kot besedo nad $\tilde{S}_\Gamma$, recimo

$$\tilde{id}_{n_{i_1}} \tilde{id}_{n_{i_2}} \cdots \tilde{id}_{n_{i_r}} = \tilde{id}_{w_r},$$

kjer se hitro prepričamo, da je $w_r = n_{i_1} n_{i_2} \cdots n_{i_r}$ beseda nad S_Γ. Definirajmo

$$\tilde{R}_G = \{\tilde{r}\, \tilde{id}_{w_r}^{-1} \mid r \in R_G\}.$$

Podobno, ker je $CT(\wp)$ podgrupa edinka v $\tilde{G}$, je za vse $g \in S_G$, $c \in S_\Gamma$ konjugiranec $\tilde{g}_1^{-1}\, \tilde{id}_c\, \tilde{g}_1$ element grupe $CT(\wp_{\tilde{c}})$; lahko ga zapišemo kot besedo nad $\tilde{S}_\Gamma$, recimo $\tilde{id}_{w_{g,c}}$, kjer je $w_{g,c}$ beseda nad S_Γ. Definirajmo še

$$\tilde{T} = \{\tilde{g}_1^{-1}\, \tilde{id}_c\, \tilde{g}_1\, \tilde{id}_{w_{g,c}}^{-1} \mid g \in S_G, c \in S_\Gamma\}.$$

Tako dobimo reformulacijo standardnega rezultata v jeziku krovnih grafov.

Trditev 4.1.1: [50, Trditev 2.55] Pri zgornji notaciji in predpostavkah je

$$\langle \tilde{S}_\Gamma \cup \tilde{S}_G \mid \tilde{R}_\Gamma \cup \tilde{R}_G \cup \tilde{T} \rangle$$

prezentacija dvignjene grupe $\tilde{G}$.

V konkretnih primerih je potrebno še eksplicitno poiskati besede w_r in $w_{g,c}$ nad S_Γ, ki določajo krovne transformacije $\tilde{r}$ in $\tilde{g}_1^{-1}\, \tilde{id}_c\, \tilde{g}_1$, zaporedoma. Pomagamo si lahko z rekurzivno uporabo formul (2.6) in (2.7). Preden pa jih sploh lahko uporabimo, moramo konstruirati avtomorfizem $g^{\#_u}$ napetostne grupe Γ. Očitno je dovolj podati slike $g^{\#_u}(c)$ za generatorje $c \in S_\Gamma$.

Izberimo vpeto drevo T s korenom v vozlišču u in urejeno orientacijo $A^+(X) = \{a_1, a_2, \ldots, a_t\}$ grafa X tako, da so $a_1, a_2 \ldots, a_r$ loki v kodrevesu $X - T$, $a_{r+1}, a_{r+2}, \ldots, a_t$ pa loki v drevesu T. Spomnimo, da je $g^{\#_u}$ lokalno definiran v vozlišču u s predpisom slik $g^{\#_u}(\zeta(W^{a_i}))$, kjer je W^{a_i} fundamentalni obhod v vozlišču u, določen z vpetim drevesom T in lokom a_i. Če želimo poiskati slike $g^{\#_u}(c)$ za generatorje $c \in S_\Gamma$, moramo torej vsak c zapisati kot besedo nad generatorji $\zeta(W^{a_1}), \zeta(W^{a_2}), \ldots, \zeta(W^{a_r})$. Drugi

način pa je ta, da poiščemo prezentacijo napetostne grupe Γ na množici generatorjev $\{\zeta(W^{a_i}) | i = 1, 2, \dots, r\}$ in od začetka delamo s slednjo prezentacijo ter ekvivalentno (T, u)-reducirano napetostno funkcijo $\zeta^{(T,u)}: X \to \Gamma$. Tedaj lahko namreč $g^{\#_u}$ podamo s predpisom slik $g^{\#_u}(\zeta(W^{a_i}))$. Dodajmo še, da nam je takšna prezentacija že dana, če smo prej testirali, ali se avtomorfizem g dvigne, kot je to opisano v Razdelku 3.2.

4.2 Kompozicija regularnih krovnih projekcij

Naj bosta Γ_1 in Γ_2 končni grupi, dani s prezentacijama $\Gamma_1 = \langle S_{\Gamma_1} \mid R_{\Gamma_1} \rangle$ oziroma $\Gamma_2 = \langle S_{\Gamma_2} \mid R_{\Gamma_2} \rangle$. Nadalje naj bo $\zeta_1: X \to \Gamma_1$ povezana regularna napetostna funkcija na končnem povezanem grafu X in $\zeta_2: X \times_{\zeta_1} \Gamma_1 \to \Gamma_2$ povezana regularna napetostna funkcija na izpeljanem krovu $X \times_{\zeta_1} \Gamma_1$. Označimo s $\wp_1$ in $\wp_2$ pripadajoči izpeljani krovni projekciji. Opozorimo, da je kompozicija $\wp = \wp_2 \circ \wp_1$ regularna krovna projekcija natanko tedaj, ko se grupa krovnih transformacij $CT(\wp_1)$ dvigne vzdolž $\wp_2$ (glej [53, 54]). Predpostavimo torej, da se grupa $CT(\wp_1)$ dvigne. V tem razdelku predstavimo metodo, s katero poiščemo regularno napetostno funkcijo $\zeta: X \to \Gamma$, ki rekonstruira kompozicijo $\wp$, ne da bi eksplicitno zgradili krovni graf $(X \times_{\zeta_1} \Gamma_1) \times_{\zeta_2} \Gamma_2$.

Ta problem je bil teoretično že obravnavan v [53], vendar pa ta rezultat ne zagotavlja metode, ko se moramo spopasti z implementacijo in konkretnimi primeri. Postopek, ki ga bomo predstavili, temelji na uporabi prezentacije razširitve grupe.

Spomnimo namreč, da lahko za napetostno grupo Γ vzamemo kar grupo krovnih transformacij $CT(\wp)$, ki je pravzaprav dvig grupe $CT(\wp_1)$ vzdolž $\wp_2$. Torej je napetostna grupa Γ razširitev grupe $CT(\wp_2)$ po grupi $CT(\wp_1)$, zato lahko uporabimo rezultat iz prejšnjega razdelka in poiščemo njeno prezentacijo v obliki

$$\Gamma = \langle \tilde{S}_{\Gamma_1} \cup \tilde{S}_{\Gamma_2} \mid \tilde{R}_{\Gamma_1} \cup \tilde{R}_{\Gamma_2} \cup \tilde{T} \rangle.$$

Nadalje, izberimo bazno vozlišče u v grafu X in naj

$$(\tilde{I}_h)_k \in \Gamma, \quad h \in \Gamma_1, k \in \Gamma_2,$$

označuje dvig krovne transformacije $I_h = i\tilde{d}_h \in CT(\wp_1)$ vzdolž projekcije $\wp_2$, ki preslika vozlišče $((u, 1), 1)$ v vozlišče $(I_h(u, 1), k) = ((u, h), k)$. Posebej, za generatorje $h_i \in S_{\Gamma_1}, k_i \in S_{\Gamma_2}$ dobimo generatorje $(\tilde{I}_{h_i})_1 \in \tilde{S}_{\Gamma_1}, (\tilde{I}_1)_{k_i} \in \tilde{S}_{\Gamma_2}$ grupe Γ. Očitno lahko vsako krovno transformacijo $(\tilde{I}_h)_k$ zapišemo kot besedo nad generatorji grupe Γ.

Natančneje, če sta $h = h_{i_1} \cdots h_{i_n}$ in $k = k_{j_1} \cdots k_{j_m}$ besedi nad generatorji S_{Γ_1} oziroma S_{Γ_2}, zaporedoma, potem velja

$$(\tilde{I}_h)_k = (\tilde{I}_1)_k \cdot (\tilde{I}_h)_1 = (\tilde{I}_1)_{k_{j_1}} \cdots (\tilde{I}_1)_{k_{j_m}} \cdot (\tilde{I}_{h_{i_1}})_1 \cdots (\tilde{I}_{h_{i_n}})_1.$$

V vsakem vlaknu $\wp^{-1}(v)$ izberimo vozlišče $((v,1),1)$ in za vsak $(\tilde{I}_h)_k \in \Gamma$ označimo vozlišče $(\tilde{I}_h)_k((v,1),1)$ v vlaknu $\wp^{-1}(v)$ z $(v,(\tilde{I}_h)_k)$. Na ta način so vozlišča vlaken $\wp^{-1}(v)$ označena bijektivno z $\{v\} \times \Gamma$. Za poljuben lok (v,w) v X bi radi določili napetost $\zeta(v,w)$. Očitno je napetost $\zeta(v,w)$ enaka drugi komponenti oznake tistega vozlišča v vlaknu $\wp^{-1}(w)$, ki je povezano z vozliščem $((v,1),1)$. Hitro se lahko prepričamo, da je vozlišče v vlaknu $\wp^{-1}(w)$, ki je povezano z $((v,1),1)$, enako

$$((w,\zeta_1(v,w)),\zeta_2((v,1),(w,\zeta_1(v,w)))). \tag{4.1}$$

Torej je iskana napetost $\zeta(v,w)$ enaka tisti krovni transformacija $(\tilde{I}_h)_k$, ki preslika vozlišče $((w,1),1)$ v vozlišče, dano z (4.1). Z uporabo formul (2.6) in (2.7) izpeljemo, da poljubna krovna transformacija $(\tilde{I}_h)_k$ preslika vozlišče $((w,1),1)$ v vozlišče

$$((w,h),k \cdot I_h^{\#_{(u,1)}}(\zeta_2(Q)) \cdot \zeta_2^{-1}(I_h(Q))), \tag{4.2}$$

kjer je $Q\colon (w,1) \to (u,1)$ poljuben sprehod v grafu $X \times_{\zeta_1} \Gamma_1$. Primerjajmo (4.1) in (4.2), pa dobimo

$$h = \zeta_1(v,w) \text{ in } k = \zeta_2((v,1),(w,\zeta_1(v,w))) \cdot \zeta_2(I_{\zeta_1(v,w)}(Q)) \cdot (I_{\zeta_1(v,w)}^{\#_{(u,1)}}(\zeta_2(Q)))^{-1}.$$

Opozorimo še, da sta h in k besedi nad generatorji S_{Γ_1} oziroma S_{Γ_2} in da smo avtomorfizme $I_{h_i}^{\#_{(u,1)}}$ naračunali že pri iskanju same prezentacije grupe Γ.

4.3 *Dekompozicija regularne krovne projekcije*

V tem razdelku zgodbo obrnemo. Za regularno napetostno funkcijo $\zeta\colon X \to \Gamma$ si oglejmo, kako kombinatorično rekonstruiramo dekompozicijo regularne krovne projekcije $\wp\colon X \times_\zeta \Gamma \to X$, porojene do ekvivalence natanko iz podgrupe edinke N v napetostni grupi Γ.

Naj bo $q\colon \Gamma \to \Gamma/N$ naravna kvocientna preslikava. Na grafu X definirajmo regularno napetostno funkcijo $\zeta_q\colon X \to \Gamma/N$ kot kompozicijo $\zeta_q = q \circ \zeta$ ter z

$$\wp_q\colon X \times_{\zeta_q} \Gamma/N \to X$$

označimo njeno izpeljano regularno krovno projekcijo. Nadalje, naj bo T množica vseh predstavnikov desnih odsekov po podgrupi N v Γ. Spomnimo, da lahko vsak element $a \in \Gamma$ enolično zapišemo kot produkt $a = nt$ za neka $n \in N$ in $t \in T$. Za vsak $t \in T$ in $(u, v) \in A(X)$ izberimo v množici T tisti element, ki je predstavnik desnega odseka $Nt\zeta(u, v)$, in ga označimo z $s_{t,\zeta(u,v)}$, to je, $Nt\zeta(u, v) = Ns_{t,\zeta(u,v)}$. Nato na izpeljanem grafu $X \times_{\zeta_q} \Gamma/N$ definiramo regularno napetostno funkcijo $\bar{\zeta}_q \colon X \times_{\zeta_q} \Gamma/N \to N$ s predpisom

$$\bar{\zeta}_q((u, Nt), (v, Nt\zeta_q(u, v))) = t\,\zeta(u, v)\,s^{-1}_{t,\zeta(u,v)}.$$

Hitro se lahko prepričamo, da so napetosti nasprotnih lokov enake inverznim napetostim, zato je $\bar{\zeta}_q$ dobro definirana. Označimo z

$$\bar{\wp}_q \colon (X \times_{\zeta_q} \Gamma/N) \times_{\bar{\zeta}_q} N \to X \times_{\zeta_q} \Gamma/N$$

njeno izpeljano regularno krovno projekcijo. Naslednja trditev pove, da je dekompozicija projekcije $\wp$ do ekvivalence natanko podana kot $\bar{\wp}_q \circ \wp_q$.

Trditev 4.3.1: Pri zgornji notaciji je regularna krovna projekcija $\wp$ ekvivalentna kompoziciji $\bar{\wp}_q \circ \wp_q$ regularnih krovnih projekcij $\bar{\wp}_q$ in $\wp_q$.

Dokaz: Pokazati moramo obstoj takega izomorfizma $\alpha \colon X \times_\zeta \Gamma \to (X \times_{\zeta_q} \Gamma/N) \times_{\bar{\zeta}_q} N$, da naslednji diagram

$$\begin{array}{ccc} X \times_\zeta \Gamma & \xrightarrow{\alpha} & (X \times_{\zeta_q} \Gamma/N) \times_{\bar{\zeta}_q} N \\ \downarrow{\scriptstyle \wp} & & \downarrow{\scriptstyle \bar{\wp}_q} \\ X & \xrightarrow{\wp_q} & X \times_{\zeta_q} \Gamma/N \end{array}$$

komutira. Definirajmo α s predpisom $(u, nt) \mapsto ((u, Nt), n)$ in pokažimo, da je homomorfizem grafov. Očitno α slika vozlišča v vozlišča. Preverimo še, da ohranja sosednost. Vzemimo poljubno povezavo $(u, nt) \sim (v, nt\zeta(u, v))$ v $X \times_\zeta \Gamma$, kjer je $u \sim v$ povezava v X. Ker je grupni element $nt\zeta(u, v)$ vsebovan v $Nt\zeta(u, v) = Ns_{t,\zeta(u,v)}$, obstaja tak $n' \in N$, da je $nt\zeta(u, v) = n's_{t,\zeta(u,v)}$. Potem se vozlišče $(v, nt\zeta(u, v))$ z α preslika v vozlišče $((v, Ns_{t,\zeta(u,v)}), n')$. Pokažimo, da velja $((u, Nt), n) \sim ((v, Ns_{t,\zeta(u,v)}), n')$. Res. Ker je $u \sim v$ in

$$Nt\zeta_q(u, v) = NtN\zeta(u, v) = Nt\zeta(u, v) = Ns_{t,\zeta(u,v)},$$

velja $(u, Nt) \sim (v, Ns_{t,\zeta(u,v)})$. Upoštevajmo še definicijo napetostne funkcije $\bar{\zeta}_q$, pa dobimo

$$n\bar{\zeta}_q((u, Nt), (v, Ns_{t,\zeta(u,v)})) = n\bar{\zeta}_q((u, Nt), (v, Nt\zeta_q(u, v))) = nt\,\zeta(u, v)s^{-1}_{t,\zeta(u,v)} = n'.$$

Zato je $((u, Nt), n) \sim ((v, Ns_{t,\zeta(u,v)}), n')$. Da je α bijekcija in da zadošča zgornjemu diagramu, pa očitno sledi iz njene definicije. □

Opomba 4.3.2: Napetostni grupi Γ/N in N sta natanko grupi Γ_1 oziroma Γ_2, zaporedoma, iz Razdelka 4.2.

Naj bo sedaj $\wp$ regularna krovna projekcija, ki je G-dopustna. Pogosto moramo projekcijo $\wp$ dekomponirati tako, da je projekcija $\wp_q$ tudi G-dopustna. Če je N le edinka v napetostni grupi Γ, potem to v splošnem ne bo res. Pri predpostavki, da je N karakteristična podgrupa v Γ, pa velja naslednji izrek (primerjaj z [39, 54]).

Izrek 4.3.3: Pri zgornji notaciji in predpostavki, da je N karakteristična grupa v Γ, se grupa G dvigne vzdolž projekcije $\wp$ natanko tedaj, ko se G dvigne vzdolž projekcije $\wp_q$ in se njen dvig dvigne vzdolž projekcije $\bar{\wp}_q$.

5

Konstrukcija krovnih grafov

Naj bo G dana podgrupa grupe avtomorfizmov končnega povezanega grafa X. V tem poglavju predstavimo metode za iskanje napetostnih funkcij grafa X, ki porodijo G-dopustne krovne projekcije. Najprej obravnavamo permutacijske napetosti, nato pa še regularne napetosti v primeru rešljivih regularnih krovnih projekcij.

5.1 Dopustne krovne projekcije

Naj bo n dano naravno število in $g_1, g_2, \dots, g_s$ generatorji grupe G. V tem razdelku se posvetimo konstrukciji vseh permutacijskih napetostnih funkcij grafa X, ki porodijo paroma neekvivalentne n-listne povezane G-dopustne krovne projekcije.

Izberimo vpeto drevo T s korenom v baznem vozlišču u in urejeno orientacijo $A^+(X) = \{a_1, a_2, \dots, a_t\}$ grafa X tako, da so $a_1, a_2 \dots, a_r$ loki v kodrevesu $X - T$, $a_{r+1}, a_{r+2}, \dots, a_t$ pa loki v drevesu T. Za konstrukcijo n-listnega krova grafa X je – do ekvivalence krovnih projekcij natanko – dovolj vzeti zaporedje $\alpha_1, \alpha_2, \dots, \alpha_r$ permutacij v simetrični grupi S_n in potem definirati (T, u)-reducirano permutacijsko napetostno funkcijo na grafu X tako, da loku a_j predpišemo napetost α_j, $j = 1, 2, \dots, r$. Očitno ima potem fundamentalni obhod W^{x_j} napetost α_j. Torej bo pripadajoči krovni graf povezan natanko tedaj, ko bo lokalna napetostna grupa $\Gamma = \mathrm{Loc}_u = \langle \alpha_1, \alpha_2, \dots \alpha_r \rangle$ tranzitivna. Takšno zaporedje imenujemo *tranzitivno napetostno zaporedje*.

Naj bo (T, u)-reducirana permutacijska napetostna funkcija na grafu X porojena s tranzitivnim napetostnim zaporedjem $\alpha_1, \alpha_2, \dots \alpha_r$. Ker lahko napetost poljubnega obhoda v X izrazimo kot besedo nad $\alpha_1, \alpha_2, \dots, \alpha_r$, označimo z $w_{ij}(\alpha_1, \alpha_2, \dots, \alpha_r)$ napetost preslikanega fundamentalnega obhoda $g_i(W_j)$, $i = 1, 2, \dots, s$. Nadalje naj bo Δ grupa, dana s prezentacijo

$$\Delta = \langle \mathbf{a}_1, \dots, \mathbf{a}_r, \tau_1, \dots, \tau_s \mid \tau_i^{-1} \mathbf{a}_j \tau_i = w_{i,j}(\mathbf{a}_1, \dots, \mathbf{a}_r),\ 1 \le i \le s, 1 \le j \le r \rangle.$$

Podgrupa $\Pi = \langle \mathbf{a}_1, \dots, \mathbf{a}_r \rangle$ je očitno edinka v Δ in je izomorfna fundamentalni grupi $\pi(X, u)$. Dovolj smo pripravili, da med sabo povežemo n-listne povezane G-dopustne krovne projekcije in delovanja grupe Δ na desnih odsekih po nekaterih njenih podgrupah indeksa n.

Spomnimo, da se grupa G dvigne natanko tedaj, ko ima naslednji sistem permutacijskih enačb

$$\tau_i^{-1} \alpha_j \tau_i = w_{ij}(\alpha_1, \alpha_2, \dots, \alpha_r), \quad j = 1, 2, \dots, r, \tag{5.1}$$

rešitev v S_n za vsak $i = 1, 2, \dots, s$. Ob predpostavki, da se G dvigne, izberimo, za vsak indeks i, po eno rešitev τ_i zgornjega sistema za vsak indeks i. Potem se preslikava

$\chi\colon \Delta \to S_n$, definirana s predpisoma $\mathbf{a}_j \mapsto \alpha_j$ in $\tau_i \mapsto \tau_i$, očitno razširi do homomorfizma grup. Z drugimi besedami, χ je tranzitivna permutacijska reprezentacija grupe Δ z $\hat{\Gamma} = \chi(\Delta)$ in $\Gamma = \chi(\Pi)$. Torej je ta reprezentacija grupe Δ porojena z delovanjem Δ na desnih odsekih po podgrupi $H = \chi^{-1}(\hat{\Gamma}_1)$ (kjer $\hat{\Gamma}_1$ označuje stabilizator elementa 1), ki je indeksa n v Δ. Ker je Γ tranzitivna, mora imeti vsak odsek podgrupe H netrivialen presek s podgrupo Π. Zato ima presek $\Pi \cap H$ indeks n v Π.

Obratno, naj bo $H \leq_n \Delta$ taka podgrupa indeksa n, da je presek $\Pi \cap H \leq_n \Pi$ prav tako indeksa n v Π. Oglejmo si delovanje grupe Δ na desnih odsekih podgrupe H in označimo s $\chi_H\colon \Delta \to S_n$ pripadajočo tranzitivno permutacijsko reprezentacijo. Definirajmo (T, u)-reducirano permutacijsko napetostno funkcijo na grafu X tako, da loku x_j predpišemo napetost $\alpha_j = \chi_H(\mathbf{a}_j)$, $j = 1, 2, \dots, r$. Potem je lokalna napetostna grupa enaka $\Gamma = \chi_H(\Pi)$ in $\hat{\Gamma} = \chi(\Delta)$. Očitno je Γ tranzitivna natanko tedaj, ko je delovanje grupe Π na desnih odsekih podgrupe H v Δ tranzitivno. Toda vsak odsek podgrupe H ima netrivialen presek s Π, ker velja $[\Delta : H] = [\Pi : \Pi \cap H] = n$. Torej je Γ tranzitivna in zato pripadajoči krovni graf povezan. Poleg tega se grupa G dvigne, saj vsaka permutacija $\tau_i = \chi_H(\tau_i)$ zadošča sistemu permutacijskih enačb (5.1), $i = 1, 2, \dots, s$. Vse, kar smo povedali zgoraj, strnimo v naslednji izrek.

Izrek 5.1.1: Pri zgornji notaciji naj bo $H \leq_n \Delta$ taka podgrupa končnega indeksa n, da velja $\Pi \cap H \leq_n \Pi$. Poleg tega naj bo $\chi_H\colon \Delta \to S_n$ tranzitivna permutacijska reprezentacija. Potem (T, u)-reducirana permutacijska napetostna funkcija na grafu X z napetostmi $\alpha_j = \chi_H(\mathbf{a}_j)$ na lokih a_j, $j = 1, \dots, r$, porodi n-listno povezano G-dopustno krovno projekcijo. Obratno, vsaka n-listna povezana G-dopustna krovna projekcija je porojena, do ekvivalence natanko, na tak način.

Opomba 5.1.2: Grupi Δ rečemo tudi „univerzalna grupa“ za podgrupo G avtomorfizmov baznega grafa X v smislu, da porodi vsako G-dopustno krovno projekcijo.

Opomba 5.1.3: Pri predpostavki, da velja $[\Delta : H] = [\Pi : \Pi \cap H] = n$, je preslikava $\phi\colon (\Pi \cap H)|\Pi \to H|\Delta$, definirana s predpisom $(\Pi \cap H)x \mapsto Hx$, bijekcija. Poleg tega naslednji diagram

$$\begin{array}{ccc} (\Pi \cap H)|\Pi & \xrightarrow{\chi_{\Pi\cap H}(\mathbf{a})} & (\Pi \cap H)|\Pi \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi} \\ H|\Delta & \xrightarrow{\chi_H(\mathbf{a})} & H|\Delta \end{array}$$

komutira. Torej se delovanje grupe Π na desnih odsekih po $\Pi \cap H$ naravno vloži v delovanje grupe Δ na desnih odsekih po H. Drugače povedano, prvo delovanje je ekvivalentno delovanju grupe Π, ki je inducirano z restrikcijo delovanja Δ na desnih odsekih po H.

Spomnimo, da je n-listna povezana krovna projekcija do ekvivalence natanko določena z delovanjem Π na desnih odsekih po podgrupi indeksa n v Π. Po Izreku 5.1.1 je n-listna povezana G-dopustna krovna projekcija do ekvivalence natanko določena z delovanjem Π (pravzaprav z delovanjem Δ) na desnih odsekih po podgrupi $H \leq \Delta$ z lastnostjo $[\Delta : H] = [\Pi : \Pi \cap H] = n$. Rečemo, da je krovna projekcija *porojena z reprezentacijo* $\chi_H \colon \Delta \to S_n$.

Trditev 5.1.4: Naj bosta $H, H' \leq_n \Delta$ taki podgrupi končnega indeksa n v Δ, da imata $\Pi \cap H$ in $\Pi \cap H'$ indeks n v Π. Potem sta krovni projekciji, porojeni z reprezentacijama $\chi_H \colon \Delta \to S_n$ in $\chi_{H'} \colon \Delta \to S_n$, ekvivalentni natanko tedaj, ko sta podgrupi $\Pi \cap H$ in $\Pi \cap H'$ konjugirani v Π. Posebej, če sta H in H' konjugirani v Δ, potem sta pripadajoči projekciji ekvivalentni.

Dokaz: Prvi del trditve očitno sledi iz zgornje diskusije. Naj bo sedaj $H' = x^{-1}Hx$. Ker je $[\Delta : H] = [\Pi : (\Pi \cap H)]$, velja $Hx = Ha$ za nek $a \in \Pi$. Torej je $xa^{-1} \in H$ in zato $H' = a^{-1}Ha$. Posledično velja $\Pi \cap H' = a^{-1}\Pi a \cap a^{-1}Ha = a^{-1}(\Pi \cap H)a$. Po prvem delu trditve sta zato pripadajoči projekciji ekvivalentni. □

Opomba 5.1.5: Po Trditvi 5.1.4 je dovolj gledati podgrupe v Δ do konjugiranosti natanko. Seveda lahko dve nekonjugirani podgrupi še vedno porodita ekvivalentna krova.

Iz zgornje diskusije sledi, da je za generiranje vseh n-listnih povezanih G-dopustnih krovnih projekcij potrebno preučiti delovanje grupe Δ na desnih odsekih po vseh takšnih podgrupah H indeksa n v Δ, da imajo preseki $\Pi \cap H$ tudi indeks n v Π. V praksi pravzaprav dobimo do ekvivalence natanko vse k-listne povezane G-dopustne krovne projekcije za $k \leq n$.

Natančneje, po Trditvi 5.1.4 najprej poiščemo seznam $\mathscr{L}$ predstavnikov konjugiranostnih razredov vseh podgrup do indeksa n v grupi Δ. Dobimo jo z uporabo algoritma za iskanje podgrup majhnega indeksa. Nato za vsako podgrupo $H \leq \Delta$ indeksa $k \leq n$ na seznamu $\mathscr{L}$ izračunamo permutacijsko reprezentacijo $\chi_H \colon \Delta \to S_k$. Da preverimo, ali je pripadajoči krov povezan (torej, da velja $[\Pi : (\Pi \cap H)] = [\Delta : H]$), moramo

testirati, ali je podgrupa, generirana z $\alpha_1 = \chi(\mathbf{a}_1), \alpha_2 = \chi(\mathbf{a}_2), \ldots, \alpha_r = \chi(\mathbf{a}_r)$, tranzitivna. Nazadnje, nekatere izmed porojenih krovnih projekcij so lahko ekvivalentne po Opombi 5.1.5. Uporabimo algoritem opisan v Razdelku 3.1 in poiščemo paroma neekvivalentne krovne projekcije. Formalna koda za generiranje paroma neekvivalentnih k-listnih povezanih G-dopustnih krovnih projekcij je podana v Algoritmu 5.1.

Algoritem 5.1: G-dopustne krovne projekcije

Vhodni parametri: univerzalna grupa Δ za podgrupo G avtomorfizmov končnega povezanega grafa X,
poljubno naravno število n

Izhodni parametri: seznam $\mathscr{C}$ permutacijskih napetostnih funkcij grafa X, ki porodijo vse paroma neekvivalentne k-listne povezane G-dopustne krovne projekcije za vse $k \leq n$

1: $\mathscr{C} \leftarrow \emptyset$;
2: konstruiraj seznam $\mathscr{L}$ vseh podgrup do indeksa n v grupi Δ;
3: *for* $H \in \mathscr{L}$ *do*
4: izračunaj reprezentacijo $\chi_H : \Delta \to S_k$;
5: *if* grupa $\chi_H(\langle \mathbf{a}_1, \mathbf{a}_2, \ldots \mathbf{a}_r \rangle)$ je tranzitivna *then*
6: konstruiraj pripadajočo permutacijsko napetostno funkcijo ζ;
7: *if* ζ ni ekvivalentna nobeni krovni projekciji v $\mathscr{C}$ *then*
8: dodaj ζ v $\mathscr{C}$;
9: *return* $\mathscr{C}$;

Izrek 5.1.6: Za naravno število n, končen povezan graf X in njegovo podgrupo avtomorfizmov G Algoritem 5.1 generira vse paroma neekvivalentne k-listne povezane G-dopustne krovne projekcije, kjer je $k \leq n$.

5.2 Dopustne regularne krovne projekcije

V tem razdelku se posvetimo konstrukciji vseh permutacijskih napetostnih funkcij grafa X, ki porodijo paroma neekvivalentne n-listne povezane G-dopustne regularne krovne projekcije. Naslednji izrek sledi neposredno iz splošne teorije o krovni grafih in Opombe 5.1.3.

Izrek 5.2.1: Naj bo $H \leq_n \Delta$. Potem permutacijska reprezentacija $\chi_H\colon \Delta \to S_n$ porodi n-listno povezano G-dopustno regularno krovno projekcijo natanko tedaj, ko je $\Pi \cap H \lhd_n \Pi$ podgrupa edinka indeksa n v grupi Π.

Prva možnost za generiranje vseh povezanih G-dopustnih regularnih krovnih projekcij je, da v vrstici 6 Algoritma 5.1 naredimo dodaten test, ali je grupa $\chi_H(\langle \mathbf{a}_1, \ldots, \mathbf{a}_r \rangle)$ polregularna. Toda ta pristop vključuje veliko odvečnega dela, ker je večina krovov neregularnih. V luči dejstva, da je podgrup edink v splošnem precej manj v primerjavi z vsemi podgrupami, se porodi naslednje vprašanje. Ali je možno shajati že samo s podgrupami edinkami? Modifikacija Algoritma 5.1 v takšnega, da upoštevamo zgolj podgrupe edinke, očitno ni dobra možnost, ker lahko nekatere krove izgubimo. Potreben je drugačen pristop. Vendar bomo morali tedaj upoštevati podgrupe edinke v Δ, ki imajo indeks večji kot n.

Naj bo $H \leq_n \Delta$ taka podgrupa indeksa n, da je $\Pi \cap H$ podgrupa edinka v Π. Tedaj permutacijska reprezentacija $\chi_H\colon \Delta \to S_n$ porodi n-listno povezano G-dopustno regularno krovno projekcijo. Namesto da na to projekcijo gledamo kot na projekcijo, porojeno z reprezentacijo χ_H, najprej faktoriziramo grupo Δ po sredici $\mathrm{core}_\Delta(H)$ in nato vzamemo primerno reprezentacijo kvocientne grupe, ki porodi ekvivalentno krovno projekcijo.

Izrek 5.2.2: Naj reprezentacija $\chi_H\colon \Delta \to S_n$ porodi n-listno povezano G-dopustno regularno krovno projekcijo. Potem je sredica $\mathrm{core}_\Delta(H)$ maksimalna med podgrupami edinkami $N \lhd \Delta$, ki so vsebovane v grupi H in zadoščajo pogoju $\Pi \cap N = \Pi \cap H$. Poleg tega velja:

(i) $K = H/N$ je komplement (indeksa n) k grupi $\underline{\Pi} = \Pi N/N \cong \Pi/(\Pi \cap N)$ v grupi $\underline{\Delta} = \Delta/N$.

(ii) Reprezentacija $\chi_K\colon \underline{\Delta} \to S_n$ porodi krovno projekcijo, ki je ekvivalentna krovni projekciji, porojeni z reprezentacijo $\chi_H\colon \Delta \to S_n$.

(iii) Reprezentacija $\chi_K\colon \underline{\Delta} \to S_n$ je zvesta natanko tedaj, ko je $N = \mathrm{core}_\Delta(H)$.

Dokaz: Da je sredica $\mathrm{core}_\Delta(H)$ maksimalna med podgrupami edinkami z zahtevano lastnostjo, je dovolj pokazati, da zadošča pogoju $\Pi \cap \mathrm{core}_\Delta(H) = \Pi \cap H$. Poglejmo si delovanje grupe Π na desnih odsekih po podgrupi $\Pi \cap H$ in delovanje grupe Δ na

desnih odsekih po podgrupi H. V luči Opombe 5.1.3 se prvo delovanje vloži v drugo delovanje. Torej se jedro $\mathrm{core}_\Pi(\Pi \cap H)$ preslika v podgrupo jedra $\mathrm{core}_\Delta(H)$. Ker je po Trditvi 5.2.1 presek $\Pi \cap H$ podgrupa edinka v Π, velja $\mathrm{core}_\Pi(\Pi \cap H) = \Pi \cap H$. Torej je $\Pi \cap H \leq \mathrm{core}_\Delta(H)$ in zato $\Pi \cap H \leq \Pi \cap \mathrm{core}_\Delta(H)$. Neenakost v drugo stran je očitna.

(i) Naj bo $N \lhd \Delta$ taka podgrupa edinka, vsebovana v grupi H, da velja $\Pi \cap N = \Pi \cap H$. Ker χ_H porodi povezan krov, imata grupi $\Pi \cap H$ in H isti indeks v Π oziroma Δ, zaporedoma. Torej je $\Pi \cdot H = \Delta$, zato velja $\underline{\Pi} \cdot H/N = \underline{\Delta}$. Ker imata podgrupi $\underline{\Pi}$ in H/N trivialen presek, je H/N komplement k grupi $\underline{\Pi}$ (indeksa n).

(ii) Opazimo, da preslikava ϕ s predpisom $Hx \mapsto K \cdot Nx$ porodi bijekcijo med množico desnih odsekov podgrupe H v Δ in množico desnih odsekov podgrupe $K = H/N$ v $\underline{\Delta} = \Delta/N$. Poleg tega velja $(K \cdot Nx) \cdot N\delta = K \cdot Nx\delta$ za vse $x, \delta \in \Delta$, zato naslednji diagram

$$\begin{array}{ccc} H|\Delta & \xrightarrow{\chi_H(\delta)} & H|\Delta \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi} \\ K|\underline{\Delta} & \xrightarrow{\chi_K(N\delta)} & K|\underline{\Delta} \end{array}$$

komutira. Torej je delovanje grupe Δ na desnih odsekih po H usklajeno z delovanjem grupe $\underline{\Delta}$ na desnih odsekih po podgrupi K, zato so napetosti, porojene z reprezentacijo χ_H oziroma χ_K, bodisi enake (če so odseki v Δ in $\underline{\Delta}$ oštevilčeni usklajeno z bijekcijo ϕ) bodisi simultano konjugirane z isto permutacijo (če so odseki oštevilčeni poljubno). Pripadajoči krovni projekciji sta zato ekvivalentni.

(iii) Dokaz je očiten. □

Poglejmo si sedaj poljubno podgrupo edinko $N \lhd \Delta$ končnega indeksa. Povezana G-dopustna regularna krovna projekcija bo vsekakor obstajala, če bo obstajala podgrupa $H \leq \Delta$, ki bo vsebovala N ter zadoščala pogojema $\Pi \cap H = \Pi \cap N$ in $[\Delta : H] = [\Pi : (\Pi \cap H)]$. V luči Izreka 5.2.2 lahko tedaj projekcijo konstruiramo prek kvocientne grupe Δ/N. Zadosten pogoj za to poda naslednji izrek.

Izrek 5.2.3: Naj bo $N \lhd \Delta$ podgrupa edinka končnega indeksa. Predpostavimo, da ima kvocientna grupa $\underline{\Pi} = \Pi N/N \cong \Pi/(\Pi \cap N)$ komplement K indeksa n v grupi $\underline{\Delta} = \Delta/N$. Potem velja naslednje:

(i) Reprezentacija $\chi_K\colon \underline{\Delta} \to S_n$ porodi n-listno povezano G-dopustno regularno krovno projekcijo.

(ii) Različni komplementi k podgrupi $\underline{\Pi}$ v grupi $\underline{\Delta}$ porodijo ekvivalentne regularne krovne projekcije.

Dokaz: (i) Označimo s $q\colon \Delta \to \underline{\Delta}$ naravno kvocientno preslikavo in naj bo $H = q^{-1}(K)$ praslika komplementa K. Očitno je podgrupa H indeksa n v grupi Δ. Poleg tega je grupa $\underline{\Pi}$ moči n, zato ima presek $\Pi \cap N$ indeks n v grupi Π. Velja tudi $q(\Pi \cap H) \subseteq q(\Pi) \cap q(H) = \underline{\Pi} \cap K = 1$. Torej je $\Pi \cap H$ podgrupa v grupi N, zato je $\Pi \cap H$ tudi podgrupa v grupi $\Pi \cap N$. Po drugi strani je očitno, da je $\Pi \cap N$ podgrupa v grupi $\Pi \cap H$, zato je $\Pi \cap H = \Pi \cap N$ podgrupa edinka indeksa n v grupi Π. Po Trditvi 5.2.1 reprezentacija $\chi_H\colon \Delta \to S_n$ porodi n-listno povezano G-dopustno regularno krovno projekcijo. Toda potem reprezentacija $\chi_K\colon \underline{\Delta} \to S_n$ po Izreku 5.2.2 porodi ekvivalentno projekcijo.

(ii) Naj bosta K in K' komplementa k podgrupi $\underline{\Pi}$ v $\underline{\Delta}$. Potem je $q^{-1}(K) \cap \Pi = q^{-1}(K') \cap \Pi$ in trditev sledi po prvem delu in Trditvi 5.1.4. □

Naj bo $N \lhd \Delta$ podgrupa edinka indeksa m. Če je K kot v Izreku 5.2.3 komplement k $\underline{\Pi}$ indeksa n v $\underline{\Delta}$, potem očitno n deli m. Poglejmo si reprezentacijo $\chi_K\colon \underline{\Delta} \to S_n$. Slika $\hat{\Gamma} = \chi_K(\underline{\Delta})$ je izomorfna grupi $\underline{\Delta}/\mathrm{core}_{\underline{\Delta}}(K)$ moči $m/|\mathrm{core}_{\underline{\Delta}}(K)|$. Reprezentacija χ_K preslika podgrupo edinko $\underline{\Pi}$ (moči n) izomorfno na podgrupo $\Gamma \lhd \hat{\Gamma}$. Torej je podgrupa $\hat{\Gamma}$ vsebovana v normalizatorju podgrupe Γ v grupi S_n. Ker je Γ regularna podgrupa, je njen normalizator holomorf $\mathrm{Hol}(\Gamma) \cong \Gamma \rtimes \mathrm{Aut}(\Gamma)$. Zato $m/|\mathrm{core}_{\underline{\Delta}}(K)|$ deli $|\Gamma| \cdot |\mathrm{Aut}(\Gamma)|$, od koder sledi, da m deli $n \cdot |\mathrm{core}_{\underline{\Delta}}(K)| \cdot |\mathrm{Aut}(\Gamma)|$.

V luči Izrekov 5.2.2 in 5.2.3 ter zgornji oceni za m lahko zdaj opišemo drugo možnost za generiranje vseh povezanih G-dopustnih regularnih krovnih projekcij. Prvi korak k temu cilju bi bila konstrukcija vseh podgrup edink v grupi Δ do indeksa

$$\max_{k \le n, |\Gamma| = k} (k \cdot |\mathrm{Aut}(\Gamma)|).$$

V praksi lahko za ta namen uporabimo algoritem za iskanje podgrup edink majhnega indeksa. V oceni smo upoštevali dejstvo, da je dovolj gledati samo zveste reprezentacije χ_K (za natančnejšo razlago glej dokaz Izreka 5.2.5). Ker pa je zgornja ocena odvisna od moči grupe $\mathrm{Aut}(\Gamma)$, ki je lahko ogromna tudi za majhne napetostne grupe, se zdi, da je to skoraj brezupno.

Če pa se omejimo na dvig samo enega generatorja, potem lahko povemo precej več. Ne nazadnje lahko potem posebej naredimo dodaten test, ali se tudi ostali generatorji dvignejo.

Izrek 5.2.4: Naj se avtomorfizem g baznega grafa X dvigne vzdolž n-listne povezane regularne krovne projekcije $\wp\colon \tilde{X} \to X$. Potem v grupi $\Delta = \langle \mathbf{a}_1, \dots, \mathbf{a}_r, \tau \mid \tau^{-1}\mathbf{a}_j\tau = w_j(\mathbf{a}_1, \dots, \mathbf{a}_r), 1 \le j \le r\rangle$ obstaja podgrupa H z lastnostjo $[\Delta : \mathrm{core}_\Delta(H)] \le n(n-1)$, ki porodi regularno krovno projekcijo, ekvivalentno projekciji $\wp$.

Dokaz: Naj (T, u)-reducirana permutacijska napetostna funkcija ζ, ki loku a_j predpiše napetost α_j, $j = 1, 2, \dots, r$, rekonstruira projekcijo $\wp$. Ker ima g natanko n različnih dvigov, naj bodo $\tau_1, \tau_2, \dots, \tau_n$ vse rešitve pripadajočega sistema permutacijskih enačb $\tau^{-1}\alpha_j\tau = w_j(\alpha_1, \dots, \alpha_r)$, $1 \le j \le r$. Naj bo $\tau \in \{\tau_1, \tau_2, \dots, \tau_n\}$ permutacija reda največ $n-1$, ki obstaja po Lemi 2.5.1. Oglejmo si homomorfizem $\chi\colon \Delta \to S_n$, definiran s predpisoma $\mathbf{a}_j \mapsto \alpha_j$ in $\tau \mapsto \tau$. Nadalje naj bo $H = \chi^{-1}(\langle \mathrm{Loc}, \tau\rangle)$. Kot smo že pokazali v diskusiji pred Izrekom 5.1.1, reprezentacija $\chi_H\colon \Delta \to S_n$ porodi krovno projekcijo, ki je ekvivalentna izpeljani projekciji $\wp_\zeta$. Očitno je grupa $\langle \mathrm{Loc}, \tau\rangle$ izomorfna grupi $\Delta/\mathrm{core}_\Delta(H)$. Poleg tega velja $|\langle \mathrm{Loc}, \tau\rangle| \le n(n-1)$, ker permutacija τ normalizira podgrupo Loc. Torej je indeks sredice $\mathrm{core}_\Delta(H)$ v Δ največ $n(n-1)$. □

Izrek 5.2.5: Pri zgornji notaciji in predpostavkah Algoritem 5.2 generira vse paroma neekvivalentne k-listne povezane g-dopustne regularne krovne projekcije, kjer je $k \le n$.

Dokaz: Naj bo $\mathscr{L}$ seznam vseh podgrup edink indeksa največ $n(n-1)$ v Δ. Nadalje naj bo $N \in \mathscr{L}$ takšna edinka, da velja $\Pi \cap N \le_k \Pi$, $k \le n$, in ima grupa $\underline{\Pi} = \Pi N/N \cong \Pi/(\Pi \cap N)$ komplement K v $\underline{\Delta} = \Delta/N$. Po Izreku 5.2.3 reprezentacija $\chi_K\colon \underline{\Delta} \to S_k$ porodi k-listno povezano g-dopustno regularno krovno projekcijo. Dodajmo, da lahko gledamo samo zveste reprezentacije χ_K. Če je namreč $L = \mathrm{core}_{\underline{\Delta}}(K)$ netrivialna podgrupa, označimo z $q\colon \Delta \to \underline{\Delta}$ kvocientno projekcijo. Potem je $M = q^{-1}(L) \in \mathscr{L}$ takšna edinka, da velja $\Pi \cap M = \Pi \cap N \le_k \Pi$ in ima grupa $\Pi M/M \cong \Pi/(\Pi \cap M) \cong \underline{\Pi}$ komplement v Δ/M, ki ima trivialno sredico. Pripadajoča krovna projekcija je ekvivalentna tisti, ki je porojena iz edinke N. Toda M ima manjši indeks v Δ kot N, zato je bil pripadajoči krov že konstruiran na nekem prejšnjem koraku.

Pokažimo še, da zares dobimo vse krovne projekcije. Po Izreku 5.2.4 je vsaka k-listna povezana g-dopustna regularna krovna projekcija, kjer je $k \le n$, porojena z reprezentacijo $\chi_H\colon \Delta \to S_k$, da velja $N = \mathrm{core}_\Delta(H) \in \mathscr{L}$. Nadalje je po Izreku 5.2.2 ta

Algoritem 5.2: g-dopustne regularne krovne projekcije

Vhodni parametri: univerzalna grupa Δ za avtomorfizem g končnega povezanega grafa X,
poljubno naravno število n

Izhodni parametri: seznam $\mathscr{C}$ permutacijskih napetostnih funkcij grafa X, ki porodijo vse paroma neekvivalentne k-listne povezane g-dopustne regularne krovne projekcije za vse $k \leq n$

$\mathscr{C} \leftarrow \emptyset$;
konstruiraj seznam $\mathscr{L}$ vseh podgrup edink do indeksa $n(n-1)$ v Δ;
for $N \in \mathscr{L}$ *do*
    izračunaj $\underline{\Pi} = \Pi/(\Pi \cap N)$ in $\underline{\Delta} = \Delta/N$;
    if $\underline{\Pi}$ je reda $k \leq n$ in ima komplement K v $\underline{\Delta}$, da je $\mathrm{core}_{\underline{\Delta}}(K) = 1$ *then*
        izračunaj reprezentacijo $\chi_K \colon \underline{\Delta} \to S_k$ in pripadajočo funkcijo ζ;
        if ζ ni ekvivalentna nobeni krovni projekciji v $\mathscr{C}$ *then*
            dodaj ζ v $\mathscr{C}$;
return $\mathscr{C}$;

krovna projekcija ekvivalentna tisti, ki je porojena iz zveste reprezentacije $\chi_K \colon \Delta/N \to S_k$, kjer je $K = H/N$ komplement k $\underline{\Pi} = \Pi N/N \cong \Pi/(\Pi \cap N)$ v $\underline{\Delta} = \Delta/N$. Torej res dobimo vse zahtevane krove. □

5.2.1 *O kompleksnosti*

Oba opisana algoritma Algoritem 5.1 in Algoritem 5.2 sta v praksi predvsem odvisna od učinkovitosti algoritmov za iskanje podgrup (podgrup edink). Žal pa so tehnike, ki so trenutno na voljo za reševanje problema iskanja podgrup, precej omejene. V splošnem lahko pričakujemo, da bo problem iskanja podgrup rešljiv le v primeru, ko sta vhodna parametra n in število generatorjev grupe Δ res majhna. Zaradi tega razloga so metode za reševanje slednjega problema dobile ime „algoritmi za iskanje podgrup (podgrup edink) majhnega indeksa“. Eksperimenti kažejo, da je časovna in prostorska zahtevnost teh algoritmov slabša od eksponentne v parametru n. Zaradi pravkar opisanih dejstev ima v splošnem tako Algoritem 5.1 kot tudi Algoritem 5.2 eksponentno časovno in prostorsko zahtevnost.

5.3 Dopustne rešljive regularne krovne projekcije

V tem razdelku se posvetimo konstrukciji regularnih napetostnih funkcij grafa X, ki porodijo n-listne povezane G-dopustne rešljive regularne krovne projekcije.

Naj bo $\zeta: X \to \Gamma$ končna regularna napetostna funkcija, ki rekonstruira G-dopustno rešljivo regularno krovno projekcijo $\wp$ povezanih grafov. Ker je Γ rešljiva grupa, obstaja zaporedje karakterističnih podgrup $\Gamma = \Gamma_0 > \Gamma_1 > \cdots > \Gamma_n = 1$ z elementarno abelskimi faktorji Γ_{j-1}/Γ_j. Kot je opisano v Razdelku 4.3, takšna vrsta porodi dekompozicijo

$$X \times_\zeta \Gamma \cong X_n \overset{\wp_n}{\to} X_{n-1} \to \ldots \to X_1 \overset{\wp_1}{\to} X_0 = X$$

rešljive regularne krovne projekcije $\wp$ na elementarno abelske regularne krovne projekcije $\wp_j: X_j \to X_{j-1}$, izpeljane iz regularnih napetostnih funkcij $\zeta_j: X_{j-1} \to \Gamma_{j-1}/\Gamma_j$, $1 \le i \le n$. Ker so učinkovite metode za iskanje dopustnih povezanih elementarno abelskih regularnih krovnih projekcij znane, bi zgodbo radi obrnili in rešljive krove poiskali kot kompozicijo elementarno abelskih krovov. To nam zagotavlja naslednja lema.

Lema 5.3.1: Naj bo $r: Y \to X$ G-dopustna rešljiva regularna krovna projekcija povezanih grafov ter $\tilde{G}$ dvig grupe G vzdolž r. Nadalje, naj bo $s: Z \to Y$ $\tilde{G}$-dopustna elementarno abelska regularna krovna projekcija povezanih grafov. Potem je kompozicija $r \circ s: Z \to X$ G-dopustna rešljiva regularna krovna projekcija povezanih grafov.

Dokaz: Ker je projekcija s $\tilde{G}$-dopustna, je tudi $CT(r)$-dopustna. Torej je $r \circ s$ regularna krovna projekcija. Poleg tega je grupa $CT(r \circ s)$ enaka dvigu grupe $CT(r)$ vzdolž projekcije s, zato je izomorfna razširitvi elementarno abelske grupe $CT(s)$ po rešljivi grupi $CT(r)$. Po definiciji rešljive grupe sledi, da je grupa $CT(r \circ s)$ rešljiva. Nazadnje, kompozicija $r \circ s$ je očitno G-dopustna. □

V luči zgornjih opažanj podajmo metodo. Najprej poiščimo množico $\mathscr{S}^{(1)}$ regularnih napetostnih funkcij $\zeta^{(1)}: X \to S$, ki porodijo vse paroma neekvivalentne k-listne povezane G-dopustne elementarno abelske izpeljane krovne projekcije $\wp^{(1)}$, za $k \le n$. Takšno množico lahko poiščemo recimo z metodo opisano na koncu Razdelka 2.5.

Nato za vsako funkcijo $\zeta^{(1)}$ v $\mathscr{S}^{(1)}$ uporabimo isto strategijo na eksplicitno zgrajenem izpeljanem krovu $X \times_{\zeta^{(1)}} S$ ter dvigu $\tilde{G}^{(1)}$ grupe G. Natančneje, najprej poiščemo regularne napetostne funkcije $\bar{\zeta}^{(1)}: X \times_{\zeta^{(1)}} S \to E$, ki porodijo vse paroma neekvivalentne k-listne povezane $\tilde{G}^{(1)}$-dopustne elementarno abelske regularne krovne projekcije

Algoritem 5.3: G-dopustne rešljive regularne krovne projekcije

Vhodni parametri: končen povezan graf X,
grupa $G \leq \mathrm{Aut}(X)$,
naravno število n

Izhodni parametri: seznam $\mathscr{C}$ regularnih napetostnih funkcij grafa X, ki porodijo vse paroma neekvivalentne k-listne povezane G-dopustne rešljive regularne krovne projekcije za $k \leq n$

1: poišči seznam $\mathscr{C}$ regularnih napetostnih funkcij grafa X, ki porodijo vse paroma neekvivalentne k-listne povezane G-dopustne elementarno abelske regularne krovne projekcije za vse $k \leq n$;
2: $i \leftarrow 1$;
3: *while* $i \leq |\mathscr{C}|$ *do*
4: naj bo $\zeta\colon X \to S$ funkcija na i-tem mestu v seznamu $\mathscr{C}$;
5: konstruiraj graf $X \times_\zeta S$ in dvig $\tilde{G}$ grupe G vzdolž projekcije $\wp_\zeta$;
6: poišči seznam $\mathscr{L}$ regularnih napetostnih funkcij grafa $X \times_\zeta S$, ki porodijo vse paroma neekvivalentne k-listne povezane $\tilde{G}$-dopustne elementarno abelske regularne krovne projekcije za vse $k \leq \lfloor n/|S| \rfloor$;
7: *for* $\bar{\zeta} \in \mathscr{L}$ *do*
8: rekonstruiraj kompozicijo $\wp_\zeta \circ \wp_{\bar{\zeta}}$ z regularno napetostno funkcijo ξ;
9: *if* ξ ni ekvivalentna nobeni funkciji v $\mathscr{C}$ *then*
10: dodaj ξ na seznam $\mathscr{C}$;
11: $i \leftarrow i + 1$;
12: *return* $\mathscr{C}$;

$\bar{\wp}^{(1)}$, za $k \leq \lfloor n/|S| \rfloor$. Zatem uporabimo metodo, opisano v Razdelku 4.2, in vsako kompozicijo $\wp^{(1)} \circ \bar{\wp}^{(1)}$ rekonstruiramo z regularno napetostno funkcijo $\zeta^{(2)}\colon X \to S$. Opozorimo, da je lahko funkcija $\zeta^{(2)}$ ekvivalentna kakšni izmed funkciji $\xi^{(1)}$ v $\mathscr{S}^{(1)}$ ali pa celo kakšni funkciji $\xi^{(2)}$, porojeni iz $\xi^{(1)}$. Zato na tem mestu uporabimo metodo za testiranje ekvivalence, opisano v Razdelku 3.2; v primeru, da $\zeta^{(2)}$ ni ekvivalentna nobeni od funkcij $\xi^{(1)}$ oziroma $\xi^{(2)}$, jo dodamo v množico $\mathscr{S}^{(2)}$.

Tako opisan postopek nadaljujemo na množici $\mathscr{S}^{(2)}$. Ker so krovne projekcije lahko največ n-listne, obstaja indeks N, da so vse množice $\mathscr{S}^{(i)}$ prazne za $i > N$. Torej se

postopek po N korakih konča in je

$$\mathscr{S}^{(1)} \cup \mathscr{S}^{(2)} \cup \ldots \cup \mathscr{S}^{(N)}$$

množica regularnih napetostnih funkcij, ki porodijo vse paroma neekvivalentne k-listne povezane G-dopustne rešljive regularne krovne projekcije, za $k \leq n$. Formalna koda je podana v Algoritmu 5.3.

Izrek 5.3.2: Za naravno število n, končen povezan graf X in njegovo podgrupo avtomorfizmov G Algoritem 5.3 generira vse paroma neekvivalentne k-listne povezane G-dopustne krovne projekcije, kjer je $k \leq n$.

6

Razcepne razširitve regularnih dvigov

V tem poglavju nadaljujemo z analizo o strukturi regularnega dviga. Za dano grupo, ki se dvigne vzdolž regularne krovne projekcije, razvijemo učinkovito metodo za testiranje, ali je dvignjena grupa razcepna razširitev. Poudarek je na elementarno abelskih, abelskih in rešljivih regularnih krovnih projekcijah. Zaključimo z eksperimentalnim ovrednotenjem.

6.1 Testiranje razcepnosti razširitve

Naj bo X končen povezan graf in $\zeta\colon X \to \Gamma$ končna povezana regularna napetostna funkcija. Denimo, da se dana podgrupa G avtomorfizmov grafa X dvigne vzdolž izpeljane regularne krovne projekcije $\wp\colon X \times_\zeta \Gamma \to X$. V tem razdelku predstavimo algoritem za testiranje, ali je dvignjena grupa $\tilde{G}$ razcepna razširitev grupe krovnih transformacij $CT(\wp)$ po grupi G.

Najprej opozorimo, da bi se radi izognili tako eksplicitni gradnji izpeljanega krovnega grafa $X \times_\zeta \Gamma$ kot tudi gradnji permutacijskih grup, ki reprezentirata delovanji grup $CT(\wp)$ in $\tilde{G}$ na $X \times_\zeta \Gamma$. Takšne konstrukcije so namreč – kot pokažemo v nadaljevanju – v splošnem časovno in prostorsko precej zahtevne. Razvoj metod, s katerimi se bomo izognili eksplicitnim konstrukcijam, temelji na naslednji reformulaciji standardnega rezultata iz teorije grup v jezik krovnih grafov (primerjaj z [50, Lema 2.76]).

Trditev 6.1.1: Naj bo $\langle S_G \mid R_G \rangle$ prezentacija podgrupe G grupe avtomorfizmov grafa X na množici generatorjev $S_G = \{g_1, g_2, \dots, g_n\}$ in z relatorji $r_j(g_1, g_2, \dots, g_n) \in R_G$, $j = 1, 2, \dots, m$. Predpostavimo, da se grupa G dvigne vzdolž regularne krovne projekcije $\wp\colon \tilde{X} \to X$ povezanih grafov. Potem je dvignjena grupa $\tilde{G}$ razcepna razširitev grupe krovnih transformacij $CT(\wp)$ po grupi G natanko tedaj, ko obstajajo dvigi $\bar{g}_1, \bar{g}_2, \dots, \bar{g}_n$ generatorjev $g_1, g_2, \dots, g_n$, ki zadoščajo relacijam $r_j(\bar{g}_1, \bar{g}_2, \dots, \bar{g}_n) = id_{\tilde{G}}$, $j = 1, 2, \dots, m$.

Dokaz: Predpostavimo najprej, da obstajajo takšni dvigi $\bar{g}_1, \bar{g}_2, \dots, \bar{g}_n$ generatorjev $g_1, g_2, \dots, g_n$, ki zadoščajo relacijam $r_j(\bar{g}_1, \bar{g}_2, \dots, \bar{g}_n) = id_{\tilde{G}}$, $j = 1, 2, \dots, m$, in naj bo $C = \langle \bar{g}_1, \bar{g}_2, \dots, \bar{g}_n \rangle \leq \tilde{G}$. Ker dvigi $\bar{g}_1, \bar{g}_2, \dots, \bar{g}_n$ zadoščajo zgornjim predpostavkam, obstaja homomorfizem $G \to C$ s predpisom $g_i \mapsto \bar{g}_i$, ki je očitno surjektiven. Po drugi strani se C projicira na G s predpisom $\bar{g}_i \mapsto g_i$, zato je $G \to C$ izomorfizem. Ker se C izomorfno projicira na G, mora imeti trivialen presek z jedrom $CT(\wp)$ projekcije $\tilde{G} \to G$. Torej je C komplement podgrupe $CT(\wp)$ v grupi $\tilde{G}$.

Obratno, naj bodo $\bar{g}_1, \bar{g}_2, \ldots, \bar{g}_n$ taki dvigi generatorjev $g_1, g_2, \ldots, g_n$, da je $C = \langle \bar{g}_1, \bar{g}_2, \ldots, \bar{g}_n \rangle \leq \tilde{G}$ komplement podgrupe $CT(\wp)$ v grupi $\tilde{G}$. Potem je $C \cong G$ in vsak avtomorfizem $r_j(\bar{g}_1, \bar{g}_2, \ldots, \bar{g}_n)$ se po predpisu $\bar{g}_i \mapsto g_i$ projicira v $r_j(g_1, g_2, \ldots, g_n) = id_G$. Torej $r_j(\bar{g}_1, \bar{g}_2, \ldots, \bar{g}_n) \in C$ leži v $CT(\wp)$. Ker je C komplement, mora veljati $r_j(\bar{g}_1, \bar{g}_2, \ldots, \bar{g}_n) = id_{\tilde{G}}$. □

V praksi je G končna permutacijska grupa, dana z množico generatorjev $S_G = \{g_1, g_2, \ldots, g_n\}$. Vemo že, da obstajajo metode za izračun njene prezentacije $\langle S_G \mid R_G \rangle$. Nato opazimo, da so v kontekstu krovnih projekcij pogoji $r_j(\bar{g}_1, \bar{g}_2, \ldots, \bar{g}_n) = id_{\tilde{G}}$ ekvivalentni pogojem, da avtomorfizmi $r_j(\bar{g}_1, \bar{g}_2, \ldots, \bar{g}_n)$, ki nujno ležijo v $CT(\wp)$, ohranja neko vozlišče negibno, recimo $(u, 1)$. Ker je namreč grupa $CT(\wp)$ polregularna, je vsak njen element, ki ohranja neko vozlišče negibno, trivialen. Spomnimo še, da so dvigi enolično določeni s sliko enega samega vozlišča. Zato vsaka n-terica napetosti $t_1, t_2 \ldots, t_n \in \Gamma$, skupaj s predpisi $\bar{g}_i(u, 1) = (g_i(u), t_i), 1 \leq i \leq n$, natanko določa dvige $\bar{g}_1, \bar{g}_2, \ldots, \bar{g}_n$. Tedaj lahko vsak pogoj $r_j(\bar{g}_1, \bar{g}_2, \ldots, \bar{g}_n)(u, 1) = (u, 1)$ testiramo tako, da z rekurzivno uporabo zvez (2.6) and (2.7) izračunamo vrednost avtomorfizma $r_j(\bar{g}_1, \bar{g}_2, \ldots, \bar{g}_n)$ v vozlišču $(u, 1)$. Vprašanje obstoja komplementa smo tako prevedli na problem iskanja n-terice napetosti $t_1, t_2 \ldots, t_n$, ki določajo takšne dvige $\bar{g}_1, \bar{g}_2, \ldots, \bar{g}_n$, da velja $r_j(\bar{g}_1, \bar{g}_2, \ldots, \bar{g}_n)(u, 1) = (u, 1)$ za vsak indeks j. V najslabšem primeru moramo tako pregledati celotno množico Γ^n. V posebnih primerih, ki se jim bomo posvetili v nadaljevanju, pa se lahko takšnemu pregledovanju izognemo tako, da obravnavamo napetosti t_i kot neznanke.

Predpostavimo za trenutek, da znamo za vsak indeks j izračunati vrednosti avtomorfizmov $r_j(\bar{g}_1, \bar{g}_2, \ldots, \bar{g}_n)$ v $(u, 1)$, če na vrednosti t_i gledamo kot na neznanke. Ideja je ta, da problem iskanja komplementa prevedemo na ekvivalenten problem reševanja sistema enačb v neznankah $t_1, t_2, \ldots, t_n$, katerega rešitve so v bijektivni korespondenci z vsemi komplementi (in nerešljivost sistema pomeni, da komplement ne obstaja). Iz zvez (2.6) in (2.7) vidimo, da je glavna težava v izražanju avtomorfizmov $g_i^{\#_u} \in \mathrm{Aut}(\Gamma)$ z „zaprto formulo“, kar je v splošnem težko pričakovati. Če pa je Γ abelska grupa, potem lahko njene elemente predstavimo s celoštevilskimi vektorji, njene avtomorfizme pa s celoštevilskimi matrikami.

6.1.1 Abelski regularni krovi

Naj bo Γ abelska grupa, dana s prezentacijo $\Gamma = \langle S_\Gamma \mid R_\Gamma \rangle$ na množici generatorjev $S_\Gamma = \{c_1, c_2, \ldots, c_d\}$ in z relatorji $\lambda_k(c_1, c_2, \ldots, c_d) \in R_\Gamma$, $k = 1, 2, \ldots, s$. Tedaj lahko

vsak element $c \in \Gamma$ reprezentiramo kot stolpični vektor

$$\underline{c} = (\nu_1, \nu_2, \dots, \nu_d)^t \in \mathbb{Z}^{d\times 1}, \quad \text{kjer je} \quad c = \sum_{i=1}^{d} \nu_i c_i.$$

Ta reprezentacija je enolična do jedra (generiranega z relacijami λ_j) naravne kvocientne projekcije $\kappa\colon \mathbb{Z}^{d\times 1} \to \Gamma$ natanko. Nadalje, vsak avtomorfizem $\phi \in \mathrm{Aut}(\Gamma)$ lahko reprezentiramo (zopet ne enolično) kot matriko nad celimi števili $\mathbb{Z}$ tako, da izrazimo vsak $\phi(c_i)$ kot $\phi(c_i) = \sum_{j=1}^{d} \alpha_{ji} c_j$ in definiramo $M_\phi = [\alpha_{ij}] \in \mathbb{Z}^{d\times d}$. Naslednji diagram

$$\begin{array}{ccc} \mathbb{Z}^{d\times 1} & \xrightarrow{M_\phi} & \mathbb{Z}^{d\times 1} \\ \downarrow{\scriptstyle \kappa} & & \downarrow{\scriptstyle \kappa} \\ \Gamma & \xrightarrow{\phi} & \Gamma \end{array}$$

očitno komutira, kar pomeni, da je izračun vrednosti avtomorfizma ϕ v c dan z $\phi(c) = \kappa(M_\phi \cdot \underline{c})$.

Spomnimo, da v abelskem primeru avtomorfizem $g^\# = g^{\#_u}$ ni odvisen od izbire baznega vozlišča. Združimo zvezi (2.6) in (2.7), pa lahko za poljubno vozlišče (v, c) drugo komponento njene slike $\bar{g}_i(v, c)$ izračunamo po formuli

$$\tau_{v,\bar{g}_i}(c) = t_i + g_i^\#(c) + g_i^\#(\zeta(Q)) - \zeta(g_i(Q)), \tag{6.1}$$

kjer je $Q\colon v \to u$ poljuben sprehod. Da si poenostavimo notacijo, bomo matriko, ki reprezentira $g_i^\#$, označevali z $M_i = M_{g_i^\#}$. Potem lahko zgornjo formulo prepišemo v vektorsko obliko

$$T_{v,\bar{g}_i}(\underline{c}) = \underline{t_i} + M_i \cdot \underline{c} + M_i \cdot \underline{\zeta(Q)} - \underline{\zeta(g_i(Q))}, \tag{6.2}$$

kjer je $\tau_{v,\bar{g}_i}(c) = \kappa(T_{v,\bar{g}_i}(\underline{c}))$.

Obravnavajmo sedaj vektorje $\underline{t_i}$ kot neznanke. To pomeni, da je vsaka komponenta zase simbolna vrednost, ki predstavlja neko celo število. Ko rekurzivno uporabimo formulo (6.2) za izračunanje vrednosti avtomorfizmov $r_j(\bar{g}_1, \bar{g}_2, \dots, \bar{g}_n)$, je potrebno simbolno računanje. Temu se lahko izognemo na naslednji način. Zložimo vse sim-

bolne vektorje $\underline{t_i}$ v stolpec dn neznank

$$\mathbf{t} = \begin{bmatrix} \underline{t_1} \\ \vdots \\ \underline{t_n} \end{bmatrix} \in \mathbb{Z}^{dn\times 1}$$

in za vsak indeks i definirajmo matriko $E_i = [0, \dots, 0, \mathrm{I}, 0, \dots, 0] \in \mathbb{Z}^{d\times dn}$, ki sestoji iz $n-1$ ničelnih podmatrik $0 \in \mathbb{Z}^{d\times d}$ in ene identične podmatrike $\mathrm{I} \in \mathbb{Z}^{d\times d}$ na i-tem mestu. Očitno je $\underline{t_i} = E_i \cdot \mathbf{t}$. Denimo, da je vektor $\underline{c}$ linearno odvisen od vektorjev $\underline{t_i}$, to je, vektor $\underline{c}$ lahko zapišemo kot $\underline{c} = A\cdot\mathbf{t} + \underline{b}$ za neko matriko $A \in \mathbb{Z}^{d\times dn}$ in neki vektor $\underline{b} \in \mathbb{Z}^{d\times 1}$, ki ne vsebujeta simbolnih vrednosti. Potem je vektor $T_{v,\bar{g}_i}(\underline{c})$ zopet linearno odvisen od vektorjev $\underline{t_i}$. Res. Pišimo $A\cdot\mathbf{t} + \underline{b}$ namesto $\underline{c}$ v formuli (6.2), pa dobimo

$$T_{v,\bar{g}_i}(\underline{c}) = (E_i + M_i \cdot A)\cdot\mathbf{t} + M_i\cdot(\underline{b} + \underline{\zeta(Q)}) - \underline{\zeta(g_i(Q))}, \quad Q\colon v \to u.$$

Torej je $T_{v,\bar{g}_i}(\underline{c})$ spet oblike $A\cdot\mathbf{t} + \underline{b}$, kjer A nadomestimo z matriko $E_i + M_i\cdot A$, $\underline{b}$ pa z vektorjem $M_i\cdot(\underline{b} + \underline{\zeta(Q)}) - \underline{\zeta(g_i(Q))}$. Vrednosti avtomorfizmov $r_j(\bar{g}_1, \bar{g}_2, \dots, \bar{g}_n)$ zato lahko dejansko izračunamo tako, da rekurzivno posodabljamo matriko A in vektor $\underline{b}$. Ker lahko za vektor $\underline{0}$, ki reprezentira element $0 \in \Gamma$, vzamemo kar ničelni vektor, na začetku računanja vrednosti avtomorfizma postavimo A na ničelno matriko in $\underline{b}$ na ničelni vektor.

Iz (6.2) vidimo, da je za sam izračun vrednosti avtomorfizmov $r_j(\bar{g}_1, \bar{g}_2, \dots, \bar{g}_n)$ potrebno še nekaj predračunanja. Če želimo zgraditi matrike M_i za $g_i \in S_G$, moramo poznati slike $g_i^{\#}(c_l)$ generatorjev grupe Γ. Izberimo vpeto drevo T s korenom v baznem vozlišču u in urejeno orientacijo $A^+(X) = \{a_1, a_2, \dots, a_t\}$ grafa X tako, da so $a_1, a_2 \dots, a_r$ loki v kodrevesu $X - T$, $a_{r+1}, a_{r+2}, \dots, a_t$ pa loki v drevesu T. Ker je vsak avtomorfizem $g_i^{\#}$ natanko definiran s predpisom $\zeta(W^{a_k}) \mapsto \zeta(g_i(W^{a_k}))$ na napetostih fundamentalnih obhodov W^{a_k} v vozlišču u, lahko slike $g_i^{\#}(c_l)$ izračunamo tako, da izrazimo generatorje c_l z napetostmi obhodov W^{a_k}. To se prevede na reševanje ustreznih sistemov linearnih enačb nad celimi števili $\mathbb{Z}$. Učinkoviti algoritmi za reševanje takšnih sistemov so že dolgo znani in temeljijo na reduciranju matrike v Hermitovo ali Smithovo normalno obliko (glej [50, Razdelka 9.2.3 in 9.2.4]). Same napetosti $\zeta(W^{a_i})$ in $\zeta(g_i(W^{a_i}))$ pa izračunamo s pregledom grafa v širino (s korenom v u). Hkrati lahko izračunamo tudi napetosti $\zeta(Q)$ in $\zeta(g_i(Q))$, saj lahko za vsak sprehod $Q\colon v \to u$ vzamemo kar pot na vpetem drevesu od v do u. Formalna koda algoritma za izračun vrednosti avtomorfizma je podana v Algoritmu 6.1.

Algoritem 6.1: Izračun vrednosti avtomorfizma v $(u, 0)$

Vhodni parametri: beseda $w(g_1, g_2, \dots, g_n)$,
napetosti $\zeta(Q)$ in $\zeta(g_i(Q))$, kjer je $Q\colon v \to u$ poljuben sprehod za vsako vozlišče v,
matrike $M_i \in \mathbb{Z}^{d\times d}$, ki reprezentirajo avtomorfizme $g_i^{\#}$

Izhodni parametri: matrika A, vektor $\underline{b}$

1: $A \leftarrow d \times dn$ ničelna matrika nad $\mathbb{Z}$;
2: $\underline{b} \leftarrow d \times 1$ ničelni vektor nad $\mathbb{Z}$;
3: $v \leftarrow u$;
4: predpostavimo, da je $w = g_{k_l} \cdots g_{k_1}$;
5: *for* $i \leftarrow 1$ *to* l *do* (*skeniraj besedo w od desne proti levi*)
6: $\quad A \leftarrow E_i + M_i \cdot A$;
7: $\quad \underline{b} \leftarrow M_i(\underline{b} + \underline{\zeta(Q)}) - \underline{\zeta(g_{k_i}(Q))}$;
8: $\quad v \leftarrow g_{k_i}(v)$;
9: *return* A, $\underline{b}$;

Izračunajmo vrednost vsakega avtomorfizem $r_j(\bar{g}_1, \bar{g}_2, \dots, \bar{g}_n)$ v vozlišču $(u, 0)$. Recimo, da velja

$$T_{u,R_j(\bar{g}_1,\bar{g}_2,\dots,\bar{g}_n)}(\underline{0}) = A_j \cdot \mathbf{t} + \underline{b}_j,$$

kjer sta A_j matrika in $\underline{b}_j$ vektor, ki jih vrne Algoritem 6.1. Potem obstaja n-terica $t_1, t_2 \dots, t_n$, ki določa takšne dvige $\bar{g}_1, \bar{g}_2, \dots, \bar{g}_n$, da velja $r_j(\bar{g}_1, \bar{g}_2, \dots, \bar{g}_n)(u, 1) = (u, 1)$ za vsak indeks j, natanko tedaj, ko obstaja vektor $\mathbf{t}$, da vektorji $A_j \cdot \mathbf{t} + \underline{b}_j$ ležijo v jedru $\operatorname{Ker} \kappa$. Z drugimi besedami, celoštevilski linearni sistem

$$\begin{bmatrix} A_1 \\ \vdots \\ A_m \end{bmatrix} \cdot \mathbf{t} = - \begin{bmatrix} \underline{b}_1 \\ \vdots \\ \underline{b}_m \end{bmatrix} \tag{6.3}$$

dm enačb z dn neznankami mora biti rešljiv modulo relacije Λ_j. Uvedimo dodatne

neznanke $\underline{x}_1, \underline{x}_2, \dots, \underline{x}_m \in \mathbb{Z}^{s\times 1}$, pa dobimo celoštevilski linearni sistem

$$\begin{bmatrix} A_1 & \Lambda & 0 & \dots & 0 \\ A_2 & 0 & \Lambda & \dots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ A_m & 0 & \dots & & \Lambda \end{bmatrix} \cdot \begin{bmatrix} \mathbf{t} \\ \underline{x}_1 \\ \underline{x}_2 \\ \vdots \\ \underline{x}_m \end{bmatrix} = - \begin{bmatrix} \underline{b}_1 \\ \underline{b}_2 \\ \vdots \\ \underline{b}_m \end{bmatrix}, \tag{6.4}$$

dm enačb z $dn + sm$ neznankami, kjer je $\Lambda = \begin{bmatrix} \underline{\lambda_1} & \underline{\lambda_2} & \cdots & \underline{\lambda_s} \end{bmatrix} \in \mathbb{Z}^{d\times s}$ in so $\underline{\lambda_k}$ vektorji, ki reprezentirajo relatorje $\lambda_k \in R_\Gamma$.

Problem testiranja razcepnosti dane razširitve smo tako reducirali na ekvivalenten problem rešljivosti sistema linearnih enačb (6.4) nad $\mathbb{Z}$.

Izrek 6.1.2: Pri zgornjih predpostavkah in notaciji je dvignjena grupa $\tilde{G}$ razcepna razširitev grupe krovnih transformacij $CT(\wp)$ po grupi G natanko tedaj, ko ima sistem linearnih enačb (6.4) celoštevilsko rešitev. Nadalje, naj bo $\Omega \subseteq \Gamma^n$ množica vseh rešitev sistema (6.4), ki so reducirane glede na množico relatorjev R_Γ. Potem je Ω v bijektivni korespondenci z vsemi komplementi grupe $CT(\wp)$ v grupi $\tilde{G}$.

Dokaz: Po Trditvi 6.1.1 in zgornji diskusiji je očitno, da je razširitev razcepna natanko tedaj, ko ima sistem linearnih enačb (6.4) celoštevilsko rešitev. Poleg tega je očitno, da vsak komplement grupe $CT(\wp)$ v $\tilde{G}$ ustreza neki rešitvi sistema (6.4) in zato rešitvi v Ω. In še, dve različni rešitvi iz Ω porodita dva različna komplementa. Res. Pa recimo, da sta $(t_1, t_2, \dots, t_n)$ in $(t'_1, t'_2, \dots, t'_n)$ dve različni rešitvi iz Ω, ki porodita isti komplement $\overline{G}$. Potem obstaja indeks i, da velja $t_i \neq t'_i$. To pomeni, da je $\bar{g}_i \neq \bar{g}'_i$. Ker sta $\bar{g}_i$ in $\bar{g}'_i$ oba dviga istega avtomorfizma g_i, mora veljati $\bar{g}'_i = id_c \bar{g}_i$ za nek $id_c \in CT(\wp)$. Po drugi strani pa je $\overline{G}$ komplement, zato velja $\bar{g}'_i = \bar{g}_i$ oziroma $t_i = t'_i$, kar je v protislovju s predpostavko. Torej so vse rešitve v Ω v bijektivni korespondenci z vsemi komplementi. □

6.1.2 *Elementarno abelski regularni krovi*

Naj bo napetostna grupa Γ elementarno abelska grupa $\mathbb{Z}_p^d$, kjer vsak element v $\mathbb{Z}_p^d$ identificiramo s stolpičnim vektorjem v $\mathbb{Z}_p^{d\times 1}$ glede na standardno bazo $e_1, e_2, \dots, e_d$. Posledično lahko namesto reševanja sistema (6.4), rešujemo sistem (6.3) nad $\mathbb{Z}_p$ z Gaussovo eliminacijsko metodo. To nam precej poenostavi računanje, saj se izognemo

problemu nenadzorovane in prevelike rasti celih števil, s katerim se lahko srečamo v abelskem primeru.

Opisani postopek, ki reši problem testiranja razcepnosti v primeru abelskih regularnih krovov, nam neposredno poda algoritem v primeru elementarno abelskih regularnih krovov. Formalna koda je podana v Algoritmu 6.2.

Algoritem 6.2: Testiranje razcepnosti – elementarno abelske regularne napetosti

Vhodni parametri: povezana regularna napetostna funkcija $\zeta\colon X \to \mathbb{Z}_p^d$ na končnem povezanem grafu X,
grupa $G = \langle g_1, g_2, \dots, g_n \mid R_G \rangle$, ki se dvigne

Izhodni parametri: true, če je dvignjena grupa razcepna razširitev, false sicer

1: $\mathbf{A} \leftarrow 0 \times dn$ matrika nad $\mathbb{Z}$;
2: $\mathbf{b} \leftarrow 0 \times 1$ vektor nad $\mathbb{Z}$;
3: izberi poljubno vozlišče u;
4: izračunaj matrike $M_i \in \mathbb{Z}^{d\times d}$, ki reprezentirajo avtomorfizme $g_i^{\#}$, skupaj z napetostmi $\zeta(Q)$ in $\zeta(g_i(Q))$, kjer je $Q\colon v \to u$ sprehod za vsako vozlišče v;
5: *for* $w = w(g_1, g_2, \dots, g_n) \in R_G$ *do*
6: naj bosta matrika $A \in \mathbb{Z}^{d\times dn}$ in vektor $b \in \mathbb{Z}^{d\times 1}$ izhodna parametra, ki ju vrne Algoritem 6.1 pri računanju vrednosti besede w v vozlišču $(u, 0)$;
7: $\mathbf{A} \leftarrow \begin{bmatrix} \mathbf{A} \\ A \end{bmatrix}$; $\mathbf{b} \leftarrow \begin{bmatrix} \mathbf{b} \\ b \end{bmatrix}$;
8: *if* sistem $\mathbf{A} \cdot \mathbf{t} = -\mathbf{b}$ ima rešitev *then*
9: *return* true;
10: *else*
11: *return* false;

Izrek 6.1.3: Naj bo $\zeta\colon X \to \mathbb{Z}_p^d$ povezana regularna napetostna funkcija na končnem povezanem grafu X ranga r in naj se podgrupa $G = \langle g_1, g_2, \dots, g_n \mid R_G \rangle$ avtomorfizmov baznega grafa X dvigne. Potem Algoritem 6.2 testira, ali je dvignjena grupa razcepna razširitev grupe krovnih transformacij po grupi G.

Izrek 6.1.4: Naj bo $\zeta\colon X \to \mathbb{Z}_p^d$ povezana regularna napetostna funkcija na končnem povezanem grafu X ranga r in naj se podgrupa $G = \langle g_1, g_2, \dots, g_n \mid R_G \rangle$ avtomorfizmov

baznega grafa X dvigne. Potem obstaja algoritem, ki reši problem testiranja razcepnosti v $\mathcal{O}(n|V(X)|+nd|E(X)|+d^3r+nd^2r+nd^3L+nd^3|R_G|^2)$ korakih, kjer je $L = \sum_{w\in R_G} |w|$, pri tem pa uporabi $\mathcal{O}(n|V(X)| + nd|E(X)| + nd^2|R_G|)$ prostora.

Dokaz: Napetosti $\zeta(W^{a_k})$, $\zeta(g_i(W^{a_k}))$, $\zeta(Q)$ in $\zeta(g_i(Q))$ v Algoritmu 6.2 izračunamo s pregledom grafa v širino, kjer je cena vsake povezave $\mathcal{O}(d)$; skupaj to vzame $\mathcal{O}(n|V(X)| + nd|E(X)|)$ korakov. Za izračun matrik $M_i \in \mathbb{Z}^{d\times d}$ moramo najprej rešiti d linearnih sistemov enačb:

$$\begin{aligned} x_{1,1}\,\zeta(W^{a_1}) + x_{1,2}\,\zeta(W^{a_2}) + \cdots + x_{1,r}\,\zeta(W^{a_r}) &= e_1 \\ x_{2,1}\,\zeta(W^{a_1}) + x_{2,2}\,\zeta(W^{a_2}) + \cdots + x_{2,r}\,\zeta(W^{a_r}) &= e_2 \\ &\vdots \\ x_{d,1}\,\zeta(W^{a_1}) + x_{d,2}\,\zeta(W^{a_2}) + \cdots + x_{d,r}\,\zeta(W^{a_r}) &= e_d. \end{aligned} \tag{6.5}$$

Reševanje enega sistema z Gaussovim postopkom vzame $\mathcal{O}(d^2r)$ korakov; za reševanje d sistemov torej skupaj $\mathcal{O}(d^3r)$ korakov. Poljubno matriko M_i lahko potem izračunamo v $\mathcal{O}(d^2r)$ korakih; vse matrike M_i, $i = 1, 2, \ldots, n$, pa v $\mathcal{O}(nd^2r)$ korakih. Algoritem 6.1 pri računanju vrednosti poljubne besede w v vozlišču $(u, 0)$ porabi $\mathcal{O}(nd^3|w|)$ korakov; vrednosti vseh relatorjev v $(u, 0)$ lahko torej izračunamo v $\mathcal{O}(nd^3L)$ korakih, kjer je $L = \sum_{w\in R_G} |w|$. Nato moramo rešiti le še linearni sistem $\mathbf{A}\cdot\mathbf{t} = -\mathbf{b}$ za $\mathbf{A} \in \mathbb{Z}_p^{d|R_G|\times dn}$ in $\mathbf{b} \in \mathbb{Z}_p^{dn\times 1}$. Reševanje z Gaussovim postopkom vzame $\mathcal{O}(nd^3|R_G|^2)$ korakov. Problem testiranja razcepnosti lahko torej rešimo v $\mathcal{O}(n|V(X)|+nd|E(X)|+d^3r+nd^2r+nd^3L+nd^3|R_G|^2)$ korakih.

Za predstavitev grafa X s seznamom sosedov potrebujemo $\mathcal{O}(|V(X)|+|E(X)|)$ prostora, za poljuben vektor v $\mathbb{Z}_p^d$ pa $\mathcal{O}(d)$ prostora. Torej lahko napetostno funkcijo ζ predstavimo z $\mathcal{O}(|V(X)|+d|E(X)|)$ prostora, posamezen avtomorfizem g_i pa z $\mathcal{O}(|V(X)|)$; za vse avtomorfizme zato potrebujemo $\mathcal{O}(n|V(X)|)$. Med pregledom grafa v širino potrebujemo $\mathcal{O}(n|V(X)|)$ prostora, da shranimo preslikana vozlišča, in $\mathcal{O}(nd|E(X)|)$ dodatnega prostora, da shranimo vse napetosti preslikanih obhodov. Da shranimo matrike M_i, je potrebnega še $\mathcal{O}(nd^2)$ prostora. Matrika $\mathbf{A} \in \mathbb{Z}_p^{d|R_G|\times dn}$ vzame še $\mathcal{O}(nd^2|R_G|)$ prostora. Skupna prostorska zahtevnost je torej $\mathcal{O}(n|V(X)| + nd|E(X)| + nd^2|R_G|)$. □

6.1.3 *Rešljivi regularni krovi*

Algoritem 6.2 lahko uporabimo za testiranje razcepnosti razširitve dvignjene grupe tudi v primeru, ko je $CT(\wp) \cong \Gamma$ rešljiva grupa. Vemo namreč, da lahko rešljivo regularno

krovno projekcijo dekomponiramo na elementarno abelske regularne krovne projekcije.

Spomnimo, da se grupa G dvigne vzdolž krovne projekcije natanko tedaj, ko se dvigne vzdolž krovne projekcije, ki je ekvivalentna $\wp$. Naj bo N karakteristična podgrupa v Γ in $q\colon \Gamma \to \Gamma/N$ naravna kvocientna preslikava. Potem iz Razdelka 4.3 sledi, da kvocientna preslikava q porodi regularni krovni projekciji $\wp_q$ in $\bar{\wp}_q$, katerih kompozicija $\bar{\wp}_q \circ \wp_q$ je ekvivalentna projekciji $\wp$. Poleg tega se G dvigne vzdolž projekcije $\wp_q$ in njen dvig se dvigne vzdolž projekcije $\bar{\wp}_q$.

Naslednja lema prevede problem testiranja razcepnosti razširitve dviga grupe vzdolž $\wp$ na testiranje razcepnosti razširitev dvigov grup vzdolž $\wp_q$ in $\bar{\wp}_q$ (primerjaj z [55, Izrek 4.2]).

Lema 6.1.5: Pri zgornji notaciji in predpostavkah, da je N karakteristična grupa v Γ in se grupa G dvigne vzdolž projekcije $\wp$, sta naslednji trditi ekvivalentni.

(i) Dvig grupe G vzdolž $\wp$ je razcepna razširitev grupe $CT(\wp)$.

(ii) Dvig grupe G vzdolž $\wp_q$ je razcepna razširitev grupe $CT(\wp_q)$ in dvig nekega njenega komplementa vzdolž $\bar{\wp}_q$ je razcepna razširitev grupe $CT(\bar{\wp}_q)$.

Označimo s H dvig grupe G vzdolž projekcije $\wp_q$. Pozoren bralec bo v Lemi 6.1.5 opazil, da je potrebno, saj v principu, testirati razcepnost razširitev dvigov vseh komplementov v H vzdolž $\bar{\wp}_q$ – med drugim to pomeni, da moramo poiskati vse takšne komplemente. Toda, če je K komplement v H, je vsaka njegova konjugiranka spet komplement. In še, če je dvig komplementa K vzdolž $\bar{\wp}_q$ razcepna razširitev, je tudi vsak dvig njegove konjugiranke vzdolž $\bar{\wp}_q$ razcepna razširitev. Zato je dovolj, da poznamo predstavnike konjugiranostnih razredov komplementov v H.

Vrnimo se k primeru, ko je napetostna grupa Γ rešljiva. Naj bo

$$\Gamma = \Gamma_0 > \Gamma_1 > \cdots > \Gamma_n = 1$$

zaporedje karakterističnih podgrup z elementarno abelskimi faktorji Γ_{j-1}/Γ_j. Takšna vrsta porodi dekompozicijo

$$X \times_\zeta \Gamma \cong X_n \xrightarrow{\wp_n} X_{n-1} \to \ldots \to X_1 \xrightarrow{\wp_1} X_0 = X, \tag{6.6}$$

krovne projekcije $\wp$ na elementarno abelske regularne krovne projekcije $\wp_j\colon X_j \to X_{j-1}$, izpeljane iz regularnih napetostnih funkcij $\zeta_j\colon X_{j-1} \to \Gamma_{j-1}/\Gamma_j$, $1 \leq i \leq n$. Po Lemi 6.1.5 lahko razcepnost razširitve dviga grupe G vzdolž $\wp$ testiramo rekurzivno.

Osnovni korak. Najprej zgradimo vrsto karakterističnih podgrup kot zgoraj. Metoda za izgradnjo takšne vrste je znana (glej [50, Poglavje 8]). Označimo s $q_1\colon \Gamma \to \Gamma/\Gamma_1$ naravno kvocientno preslikavo in zgradimo regularno napetostno funkcijo $\zeta_1\colon X \to \Gamma/\Gamma_1$ kot kompozicijo $\zeta_1 = q_1 \circ \zeta$. Nadalje, označimo z G_1 dvig grupe G vzdolž $\wp_1$ in uporabimo elementarno abelsko verzijo za testiranje, ali je G_1 razcepna razširitev grupe $CT(\wp_1)$ po grupi G (glej Algoritem 6.2). Če je test pozitiven, zgradimo izpeljani krovni graf $X_1 = X \times_{\zeta_1} \Gamma/\Gamma_1$ skupaj s predstavniki konjugiranostnih razredov komplementov v G_1, zatem še regularno napetostno funkcijo $\bar{\zeta}_1\colon X_1 \to \Gamma_1$ (glej Razdelek 4.3) in nadaljujemo rekurzivno vzdolž karakteristične vrste.

Rekurzivni korak. Označimo z G_j dvig grupe G vzdolž projekcije $\wp_1 \circ \wp_2 \circ \cdots \circ \wp_j$, z M_j pa njeno grupo krovnih transformacij $CT(\wp_1 \circ \wp_2 \circ \cdots \circ \wp_j)$. Predpostavimo, da smo na j-tem koraku zgradili izpeljani krovni graf X_j skupaj z regularno napetostno funkcijo $\bar{\zeta}_j\colon X_j \to \Gamma_j$ in množico $\{U_{ij} \mid 1 \leq i \leq k_j\}$ predstavnikov konjugiranostnih razredov komplementov grupe M_j v grupi G_j. Na naslednjem koraku najprej zgradimo regularno napetostno funkcijo

$$\zeta_{j+1}\colon X_j \to \Gamma_j/\Gamma_{j+1}$$

kot kompozicijo $\zeta_{j+1} = q_{j+1} \circ \bar{\zeta}_j$, kjer je $q_{j+1}\colon \Gamma_j \to \Gamma_j/\Gamma_{j+1}$ naravna kvocientna projekcija. Nato za vsako grupo U_{ij} označimo z $\tilde{U}_{ij}$ njen dvig vzdolž $\wp_{j+1}$, z $N_{M_j}(U_{ij})$ njen normalizator v M_j ter z $\tilde{N}_{M_j}(U_{ij})$ dvig normalizatorja vzdolž $\wp_{j+1}$ Naredimo naslednje:

(a) testiramo, ali je grupa $\tilde{U}_{ij}$ razcepna razširitev grupe $CT(\wp_1)$ po grupi U_{ij};

(b) če je test pozitiven, zgradimo izpeljani krovni graf $X_{j+1} = X_j \times_{\zeta_{j+1}} \Gamma_j/\Gamma_{j+1}$ (samo v primeru, če ga nismo zgradili že za kakšen nižji indeks i) skupaj z množico $\mathscr{K}_{ij}$ komplementov grupe $CT(\wp_{j+1})$ v $\tilde{U}_{ij}$ in nato poiščemo množico $\mathscr{C}_{ij} = \{C_{ijk} \mid 1 \leq k \leq s_{ij}\}$ predstavnikov orbit delovanja grupe $\tilde{N}_{M_j}(U_{ij})$ na $\mathscr{K}_{ij}$ s konjugacijo (glej Sliko 6.1).

Če je za vse indekse $i = 1, 2, \ldots, k_j$ test v (a) negativen, potem dvig grupe G vzdolž $\wp$ ni razcepna razširitev in algoritem se ustavi. V nasprotnem primeru pa zgradimo regularno napetostno funkcijo $\bar{\zeta}_{j+1}\colon X_{j+1} \to \Gamma_{j+1}$ in nadaljujemo s procesom. Na tem

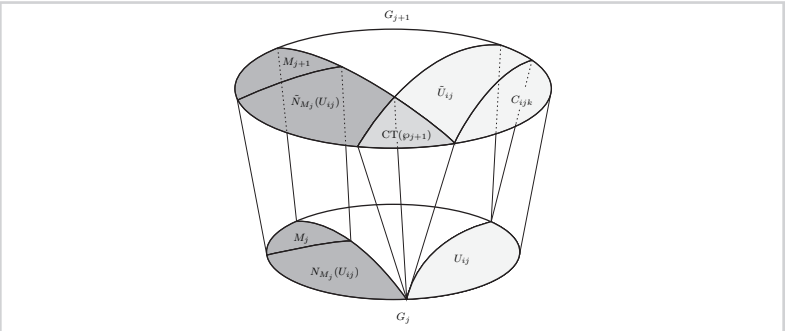
Algoritem 6.3: Testiranje razcepnosti – rešljive regularne napetosti

Vhodni parametri: povezana rešljiva regularna napetostna funkcija $\zeta\colon X \to \Gamma$ na končnem povezanem grafu X,
grupa G, ki se dvigne

Izhodni parametri: true, če je dvignjena grupa razcepna razširitev, false sicer

1: izračunaj karakteristično zaporedje $\Gamma = \Gamma_0 > \Gamma_1 > \cdots > \Gamma_n = 1$ z elementarno abelskimi faktorji Γ_{j-1}/Γ_j;
2: $\zeta \leftarrow$ regularna funkcija $q_1 \circ \zeta\colon X \to \Gamma/\Gamma_1$, kjer $q_1\colon \Gamma \to \Gamma/\Gamma_1$;
3: *if* dvig grupe G vzdolž $\wp_\zeta$ je razcepna razširitev *then*
4: $\tilde{X} \leftarrow X \times_\zeta \Gamma/\Gamma_1$, $M \leftarrow CT(\wp_\zeta)$, $\bar{\zeta} \leftarrow$ regularna funkcija $\tilde{X} \to \Gamma_1$;
5: $\mathscr{U} \leftarrow$ predstavniki konjugiranostnih razredov komplementov grupe $CT(\wp_\zeta)$ v $\tilde{G}$;
6: *for* $j = 1$ *to* $n - 1$ *do*
7: $\zeta \leftarrow$ regularna funkcija $q_{j+1} \circ \bar{\zeta}\colon \tilde{X} \to \Gamma_j/\Gamma_{j+1}$, kjer $q_{j+1}\colon \Gamma_j \to \Gamma_j/\Gamma_{j+1}$;
8: $\mathscr{C} \leftarrow \emptyset$, *razcep* $\leftarrow$ *false*;
9: *for* $U \in \mathscr{U}$ *do*
10: *if* dvig grupe U vzdolž $\wp_\zeta$ je razcepna razširitev *then*
11: *if* $j ==$ $(n-1)$ *then razcep* $\leftarrow$ *true*, break;
12: *if* razcep == false *then* $\tilde{X} \leftarrow \tilde{X} \times_\zeta \Gamma_j/\Gamma_{j+1}$, *razcep* $\leftarrow$ *true*;
13: naj bo $\tilde{U}$ dvig grupe U vzdolž $\wp_\zeta$;
14: $\mathscr{K} \leftarrow$ komplementi grupe $CT(\wp_\zeta)$ v $\tilde{U}$;
15: naj bo $\tilde{N}$ dvig normalizatorja $N_M(U)$ vzdolž $\wp_\zeta$;
16: $\mathscr{K} \leftarrow$ predstavniki orbit delovanja $\tilde{N}$ na $\mathscr{K}$ s konjugacijo;
17: $\mathscr{C} \leftarrow \mathscr{C} \cup \mathscr{K}$;
18: *if razcep* == *false then*
19: break
20: *else*
21: *if* $j ==$ $(n-1)$ *then* break;
22: $M \leftarrow CT(\wp_\zeta)$, $\mathscr{U} \leftarrow \mathscr{C}$, $\bar{\zeta} \leftarrow$ regularna funkcija $\tilde{X} \to \Gamma_{j+1}$;
23: *return* razcep;
24: *else*
25: *return* false;

mestu pripomnimo, da je vsak komplement grupe $CT(\wp_{j+1})$ v $\tilde{U}_{ij}$ tudi komplement grupe M_{j+1} v G_{j+1}. Poleg tega je množica $\mathscr{C}_{1j} \cup \mathscr{C}_{2j} \cup \cdots \cup \mathscr{C}_{kjj}$ kompletna in nereducibilna množica predstavnikov konjugiranostnih razredov komplementov grupe M_{j+1} v G_{j+1} (glej [50, 55] za bolj poglobljeno razlago na to temo). Opozorimo še, da brž ko je na $(n-1)$-vem koraku test v (a) pozitiven za nek indeks i, je dvig grupe G vzdolž $\wp$ razcepna razširitev in algoritem se ustavi. Formalna koda je podana v Algoritmu 6.3.



Slika 6.1
Dvig komplementov.

Izrek 6.1.6: Za povezano rešljivo regularno napetostno funkcijo $\zeta\colon X \to \Gamma$ na končnem povezanem grafu X in podgrupo G avtomorfizmov grafa X, ki se dvigne, Algoritem 6.3 testira, ali je dvignjena grupa razcepna razširitev grupe krovnih transformacij po grupi G.

6.2 Eksperimenti

V tem razdelku ovrednotimo zgornji Algoritem 6.3 za testiranje razcepnosti razširitve dviga vzdolž rešljive regularne krovne projekcije. Njegovo učinkovitost primerjamo z „naivnim algoritmom“, ki sestoji iz naslednjih dveh korakov.

6.2.1 Testno okolje

Oba algoritma smo implementirali v Magmi in jih testirali na operacijskem sistemu Odisej na Fakulteti za matematiko in fiziko, Univerza v Ljubljani (eight 2.93 GHz Quad-Core Intel® Xeon® processors X7350). V vrstici 2 Algoritma 6.4 smo uporabili vgrajeno funkcijo `HasComplement`.

Algoritem 6.4: Testiranje razcepnosti – eksplicitna konstrukcija

Vhodni parametri: povezana rešljiva regularna napetostna funkcija $\zeta\colon X \to \Gamma$ na končnem povezanem grafu X,
grupa G, ki se dvigne

Izhodni parametri: true, če je dvignjena grupa razcepna razširitev, false sicer

1: konstruiraj krovni graf $X \times_\zeta \Gamma$ skupaj z grupo krovnih transformacij $CT(\wp_\zeta)$ in dvignjeno grupo $\tilde{G}$ – kot permutacijski grupi, ki delujeta na $X \times_\zeta \Gamma$;

2: uporabi znano metodo za testiranje razširitve permutacijskih grup (glej [55] in [50, Poglavji 7 in 8]);

6.2.2 *Testna množica podatkov*

Znana orodja za konstruiranje povezanih elementarno abelskih regularnih krovnih projekciji, dopustnih za različne tipe podgrup avtomorfizmov, so bila uporabljena že na številnih majhnih grafih, na primer, na polnih grafih K_4 [56] in K_5 [57], Möbius-Kantorjevem grafu $G(8,3)$ [58], polnem dvodelnem grafu $K_{3,3}$ [56, 59], Petersenovem grafu $G(5,2)$ [60] in na Heawoodovem grafu H [39, 61].

Vendar pa bi želeli imeti bazo podatkov, ki ne bi vsebovala le elementarno abelskih regularnih krovov, ampak tudi rešljive. Zato smo najprej v Magmi implementirali Algoritem 5.3 in generirali regularne napetostne funkcije na:

(i) polnem grafu K_4, ki porodijo povezane $\mathsf{Aut}(K_4)$-dopustne rešljive regularne krovne projekcije do velikosti tisoč vozlišč krovnega grafa,

(ii) polnem grafu K_5, ki porodijo povezane $\mathsf{Aut}(K_5)$-dopustne rešljive regularne krovne projekcije do velikosti tisoč petsto vozlišč krovnega grafa,

(iii) Möbius-Kantorjevem grafu $G(8,3)$, ki porodijo $\mathsf{Aut}(G(8,3))$-dopustne povezane rešljive regularne krovne projekcije do velikosti tisoč petsto vozlišč krovnega grafa,

(iv) polnem dvodelnem grafu $K_{3,3}$, ki porodijo $\mathsf{Aut}(K_{3,3})$-dopustne povezane rešljive regularne krovne projekcije do velikosti dva tisoč vozlišč krovnega grafa,

(v) Petersenovem grafu $G(5,2)$, ki porodijo $\mathsf{Aut}(G(5,2))$-dopustne povezane rešljive regularne krovne projekcije do velikosti tri tisoč vozlišč krovnega grafa,

(vi) Heawoodovem grafu H, ki porodijo $\mathsf{Aut}(H)$-dopustne povezane rešljive regu-

larne krovne projekcije do velikosti deset tisoč vozlišč krovnega grafa.

V primeru, ko je obstajalo več krovnih grafov istega reda, smo v bazo vključili enega izmed njih. Baza podatkov je dosegljiva na zahtevo preko avtorjevega elektronskega naslova.

Opomba 6.2.1: Za iskanje G-dopustnih elementarno abelskih regularnih krovnih projekcij smo v Magmi implementirali metodo, ki je opisana v Razdelku 2.5.1. Problem se prevede na iskanje invariantnih podprostorov matrične grupe. Metoda za iskanje takšnih podprostorov je znana in je že implementiran v Magmi.

6.2.3 Eksperimentalni rezultati

Oba algoritma smo primerjali glede na izvršilni čas (CPU čas). Eksperimentalni časi so zbrani v Tabelah 6.1-6.6. Prvi stolpec predstavlja red napetostnih grup Γ, medtem ko drugi stolpec opisuje tri možne tipe napetostne grupe: rešljiva, a ne abelska; abelska, a ne elementarno abelska; elementarno abelska. Izvršilni časi so podani v tretjem in četrtem stolpcu (za Algoritem 6.3 in Algoritem 6.4, zaporedoma). Zadnji stolpec pove, ali je pripadajoča dvignjena grupa razcepna razširitev. Rezultati obeh algoritmov so prikazani tudi grafično na Sliki 6.2.

Tabela 6.1

Primerjava časov za polni graf K_5

red grupe Γ	tip grupe Γ	Algoritem 6.3	Algoritem 6.4	razcepna razširitev
2	elementarno abelska	0.030	0.010	da
6	rešljiva	0.110	0.050	da
24	rešljiva	0.250	0.270	da
32	elementarno abelska	0.020	0.400	da
48	rešljiva	1.340	0.830	ne
64	elementarno abelska	0.030	1.110	da
96	rešljiva	0.800	2.190	da
125	elementarno abelska	0.020	2.310	ne
128	abelska	3.040	3.460	da
192	rešljiva	2.880	7.390	da
250	abelska	0.120	7.720	ne
256	rešljiva	3.110	11.030	da

Tabela 6.2

Primerjava časov za polni dvodelni graf $K_{3,3}$

red grupe Γ	tip grupe Γ	Algoritem 6.3	Algoritem 6.4	razcepna razširitev
3	elementarno abelska	0.020	0.000	ne
16	elementarno abelska	0.030	0.090	da
27	elementarno abelska	0.020	0.140	ne
32	rešljiva	0.160	0.180	ne
48	abelska	0.170	0.300	ne
64	rešljiva	0.170	0.520	ne
81	elementarno abelska	0.020	0.730	ne
96	rešljiva	0.170	1.010	ne
192	rešljiva	0.020	3.590	ne
243	abelska	0.020	5.360	ne
256	abelska	0.170	5.850	da

Tabela 6.3

Primerjava časov za Möbius-Kantorjev graf

red grupe Γ	tip grupe Γ	Algoritem 6.3	Algoritem 6.4	razcepna razširitev
4	elementarno abelska	0.030	0.080	ne
8	elementarno abelska	0.030	0.180	ne
9	elementarno abelska	0.020	0.190	da
12	abelska	0.030	0.240	ne
16	elementarno abelska	0.030	0.470	ne
24	abelska	0.020	0.740	ne
25	elementarno abelska	0.030	0.620	da
27	elementarno abelska	0.020	0.850	da
32	elementarno abelska	0.030	1.400	ne
36	abelska	0.030	1.160	ne
48	abelska	0.030	2.510	ne
49	elementarno abelska	0.020	1.820	da
64	elementarno abelska	0.030	4.530	ne
72	abelska	0.020	4.130	ne
75	abelska	0.150	3.760	da
81	elementarno abelska	0.030	5.490	da

Kot lahko vidimo iz Tabel 6.1-6.6 in grafov na Sliki 6.2 je očitno, da Algoritem 6.3 prekaša Algoritem 6.4. Izpostavimo, da se razlog skriva v vrstici 2 Algoritma 6.4, ker je

eksplicitna konstrukcija izpeljanega grafa $X \times_\zeta \Gamma$ skupaj z grupama $CT(\wp)$ in $\tilde{G}$ časovno zahtevna. Po drugi strani Algoritem 6.3 nikoli eksplicitno ne konstruira niti krovnega grafa $X_n \cong X \times_\zeta \Gamma$ niti grup $M_n \cong CT(\wp)$ oziroma $G_n \cong \tilde{G}$, ampak konstruira krovne grafe X_j, $j = 1, 2, \ldots, n-1$, v dekompoziciji (6.6) le, če je potrebno. Ti grafi so ponavadi precej manjši.

Tabela 6.4

Primerjava časov za Heawoodov graf

red grupe Γ	tip grupe Γ	Algoritem 6.3	Algoritem 6.4	razcepna razširitev
256	elementarno abelska	0.060	51.400	da
343	elementarno abelska	0.030	60.170	ne
512	rešljiva	64.490	184.730	ne

Tabela 6.5

Primerjava časov za Petersenov graf

red grupe Γ	tip grupe Γ	Algoritem 6.3	Algoritem 6.4	razcepna razširitev
2	elementarno abelska	0.030	0.040	da
4	elementarno abelska	0.030	0.040	da
8	rešljiva	0.160	0.120	ne
36	rešljiva	0.160	0.740	da
64	elementarno abelska	0.030	2.240	da
72	rešljiva	0.200	2.060	ne
125	elementarno abelska	0.020	5.040	ne
128	abelska	3.100	7.300	da
162	rešljiva	0.190	10.620	da
250	abelska	0.120	17.730	ne

Naslednji izrek pove, da je v primeru elementarno abelskih napetostnih razlika med algoritmoma najbolj izražena.

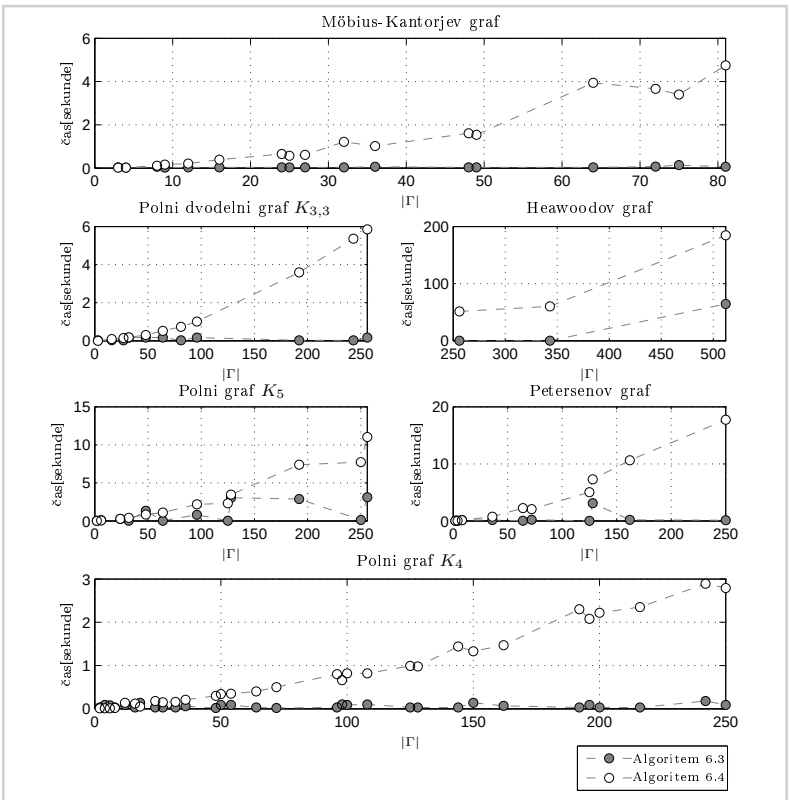
Izrek 6.2.2: Za elementarno abelsko napetostno grupo Algoritem 6.3 nikoli ne konstruira nobenega krovnega grafa X_j, zato njegova zahtevnost tedaj ni odvisna od reda napetostne grupe. Posledično so za fiksni bazni graf izvršilni časi konstantni, medtem ko časi Algoritma 6.4 naraščajo skupaj z redom napetostne grupe.

Tabela 6.6

Primerjava časov za polni graf K_4

red grupe Γ	tip grupe Γ	Algoritem 6.3	Algoritem 6.4	razcepna razširitev
2	elementarno abelska	0.030	0.010	da
4	abelska	0.090	0.010	ne
6	rešljiva	0.080	0.010	da
8	elementarno abelska	0.030	0.020	ne
12	rešljiva	0.090	0.140	ne
16	abelska	0.030	0.120	ne
18	rešljiva	0.140	0.050	da
24	rešljiva	0.030	0.180	ne
27	elementarno abelska	0.030	0.150	da
32	abelska	0.030	0.160	ne
36	rešljiva	0.060	0.210	ne
48	rešljiva	0.020	0.300	ne
50	rešljiva	0.090	0.340	da
54	abelska	0.090	0.350	da
64	abelska	0.030	0.400	ne
72	rešljiva	0.020	0.500	ne
96	rešljiva	0.030	0.800	ne
98	rešljiva	0.100	0.660	da
100	rešljiva	0.090	0.820	ne
108	abelska	0.100	0.820	ne
125	elementarno abelska	0.030	0.990	da
128	abelska	0.030	0.980	ne
144	rešljiva	0.030	1.440	ne
150	rešljiva	0.140	1.330	da
162	rešljiva	0.070	1.470	da
192	rešljiva	0.030	2.300	ne
196	rešljiva	0.090	2.080	ne
200	rešljiva	0.030	2.220	ne
216	abelska	0.030	2.350	ne
242	rešljiva	0.180	2.890	da
250	abelska	0.090	2.790	da

Po drugi strani pa je razlika lahko malo manj izražena le v primeru, ko napetostna grupa ni elementarno abelska in mora Algoritem 6.3 konstruirati vse grafe X_j skupaj z napetostnimi funkcijami in komplementi do indeksa $j = n-1$. To se zgodi na primer, ko je dvignjena grupa razcepna razširitev.



Slika 6.2

Primerjava dveh algoritmov.

Prerezne razcepne razširitve regularnih dvigov

7

Naj bo $\wp\colon \tilde{X} \to X$ regularna krovna projekcija povezanih grafov in Ω neprazna podmnožica vozlišč grafa X. *Prerez* nad Ω je podmnožica vozlišč $\bar{\Omega}$ grafa $\tilde{X}$, ki preseka vsako vlakno nad Ω v natanko enemu vozlišču. Nadalje, naj bo G podgrupa avtomorfizmov grafa X. Množica Ω je *invariantna* glede na delovanje grupe G, če velja $G(\Omega) = \Omega$. Če smo v prejšnjem poglavju študirali, ali v dvigu $\tilde{G}$ grupe G sploh obstaja kakšen komplement grupe $CT(\wp)$, pa se bomo v tem posvetili takšnim komplementom, ki porodijo posebno delovanje na krovnem grafu $\tilde{X}$. Natančneje, ob predpostavki, da velja $G(\Omega) = \Omega$, bomo iskali komplement $\overline{G}$, ki ima invarianten prerez $\bar{\Omega}$ nad Ω glede na njegovo delovanje. Rekli mu bomo *prerezni komplement* nad Ω. Dodajmo, da obstoj prereznega komplementa še ne pomeni, da so vsi komplementi prerezni.

7.1 Osnovno o prereznih razcepnih razširitvah

Naj bo Ω invariantna na delovanje grupe G. Rečemo, da se grupa G dvigne vzdolž $\wp$ kot *prerezna razcepna razširitev* grupe $CT(\wp)$ nad Ω, če se G dvigne vzdolž $\wp$ in grupa $CT(\wp)$ premore kakšen prerezni komplement nad Ω v dvigu $\tilde{G}$. S prereznimi razcepnimi razširitvami se srečamo, na primer, ko imamo opraviti z dvigi stabilizatorjev. Recimo, da se grupa G, ki ohranja vozlišče u, dvigne vzdolž projekcije $\wp$. Potem se G nujno dvigne kot prerezna razcepna razširitev nad $\{u\}$. Namreč, za izbrano vozlišče $\tilde{u}$ v vlaknu $\wp^{-1}(u)$ je njen stabilizator $\tilde{G}_{\tilde{u}}$ prerezni komplement podgrupe $CT_{\wp}$ v dvigu $\tilde{G}$. Poleg tega pa stabilizatorji igrajo pomembno vlogo pri analizi prereznih razcepnih razširitev.

Izrek 7.1.1: Naj bo $\wp : \tilde{X} \to X$ regularna krovna projekcija povezanih grafov in naj obstaja dvig $\tilde{G}$ grupe G avtomorfizmov grafa X. Predpostavimo, da je $\Omega = \cup_{i\in I}\Omega_i$ unija orbit grupe G, in naj bo $\{u_i \in \Omega_i \mid i \in I\}$ množica izbranih baznih vozlišč. Potem so naslednje trditve ekvivalentne.

(i) Grupa $\tilde{G}$ je prerezna razcepna razširitev grupe $CT(\wp)$ nad Ω.

(ii) Obstaja algebraična transverzala $\overline{G}$ grupe $CT(\wp)$ (množica predstavnikov odsekov) v $\tilde{G}$, ki ima invarianten prerez $\bar{\Omega}$ nad Ω.

(iii) Grupa $CT(\wp)$ ima tak komplement $\overline{G}$ v grupi $\tilde{G}$, da je $\overline{G} \cap \widetilde{G_{u_i}}$ stabilizator nekega vozlišča v vlaknu $\wp^{-1}(u_i)$ za $i \in I$.

Dokaz: Predpostavimo, da velja (i). Potem velja (ii), saj je komplement tudi algebraična transverzala.

Predpostavimo, da velja (ii). Najprej pokažimo, da je takšna algebraična transverzala $\overline{G}$ dejansko komplement grupe $CT(\wp)$. Res. Če sta $\bar{g}_1$ in $\bar{g}_2$ v $\overline{G}$, potem sta $\bar{g}_1\bar{g}_2$ in $\overline{g_1g_2}$ oba dviga avtomorfizma g_1g_2, ki preslikata vozlišče $\bar{u} \in \bar{\Omega}$ v vozlišče, ki leži v $\bar{\Omega}$ nad $g_1g_2(u)$. Ker je dvig natanko določen s sliko enega vozlišča, morata biti $\bar{g}_1\bar{g}_2$ in $\overline{g_1g_2}$ enaka. Zato je $\overline{G}$ zaprta za komponiranje. Podobno se pokaže, da je zaprta za inverze. Od tod sledi, da je $\overline{G}$ komplement grupe $CT(\wp)$. Poglejmo si sedaj dvig $\widetilde{G_u}$ stabilizatorja G_u, kjer je u katerokoli izmed vozlišč u_i ($i \in I$). Očitno grupa $\overline{G} \cap \widetilde{G_u} = \{\bar{g} \mid g \in G_u\}$ ohranja vozlišče $\bar{u} \in \bar{\Omega}$. Pravzaprav je ta grupa stabilizator $(\widetilde{G_u})_{\bar{u}}$, zato (iii) velja.

Predpostavimo, da velja (iii). Naj bo torej $\overline{G}$ tak komplement, da je $\overline{G} \cap \widetilde{G_{u_i}}$ stabilizator $(\widetilde{G_{u_i}})_{\bar{u}_i}$ za $i \in I$. Definirajmo prerez nad vsako orbito Ω_i, ki jo porodi delovanje $\overline{G}$ na $\bar{u}_i$. Natančneje, definirajmo funkcijo $t\colon \Omega_i \to V(\bar{X})$ s predpisoma $tu_i = \bar{u}_i$ in $t(gu_i) = \bar{g}(\bar{u}_i)$ za $g \in G$. Ta je dobro definirana, saj zaradi $(\bar{g}_2)^{-1}\bar{g}_1 \in \overline{G} \cap \widetilde{G_{u_i}}$ in posledično $(\bar{g}_2)^{-1}\bar{g}_1(\bar{u}_i) = \bar{u}_i$ nikoli ne pridemo v konflikt. Še več, tako definiran prerez je očitno invariantna na delovanje $\overline{G}$ in (i) velja. □

Predpostavimo sedaj, da $\Omega = G(u)$ sestoji iz ena same orbite. Naj bo $\overline{G}$ prerezni komplement grupe $CT(\wp)$ v $\tilde{G}$ in $\mathrm{Sec}_\Omega(\overline{G})$ množica vseh prerezov nad Ω, ki so invariantni na delovanje $\overline{G}$. Označimo s $Fix(\overline{G} \cap \widetilde{G_u})$ množico negibnih vozlišč delovanja grupe $\overline{G} \cap \widetilde{G_u}$ na vlaknu $\wp^{-1}(u)$. Po Izreku 7.1.1 so prerezi v $\mathrm{Sec}_\Omega(\overline{G})$ porojeni iz $\overline{G}$-orbit vozlišč v $Fix(\overline{G} \cap \widetilde{G_u})$. Takšni prerezi so paroma disjunktni, zato je množica $\mathrm{Sec}_\Omega(\overline{G})$ v bijektivni korespondenci z množico $Fix(\overline{G} \cap \widetilde{G_u})$. Poleg tega jih lahko preštejemo. Naslednji izrek se lahko dokaže na več načinov, na primer, uporabljajoč Izrek 3.6 iz Wielandtove monografije [62]. Tukaj bomo podali neposreden dokaz.

Izrek 7.1.2: [62, Izrek 3.6] Naj se G dvigne kot prerezna razcepna razširitev nad $\Omega = G(u)$ in naj bo $\tilde{u}$ poljubno vozlišče v vlaknu $\wp^{-1}(u)$. Potem ima vsak prerezni komplement $\overline{G}$ toliko invariantnih prerezov kot je moč centralizatorja $|C_{CT(\wp)}(\tilde{G}_{\tilde{u}})|$. Če $\tilde{u}$ leži v $Fix(\overline{G} \cap \widetilde{G_u})$, potem centralizator $C_{CT_\wp}(\tilde{G}_{\tilde{u}})$ deluje tranzitivno (in posledično regularno) na množici $\mathrm{Sec}_\Omega(\overline{G})$.

Dokaz: Naj bo $\overline{G}$ prerezni komplement. Kot smo že omenili zgoraj, je število prerezov v $\mathrm{Sec}_\Omega(\overline{G})$ enako $|Fix(\tilde{G}_{\tilde{u}})|$, kjer je $\tilde{G}_{\tilde{u}} = \overline{G} \cap \widetilde{G_u}$. Naj bo $\tilde{u}' \in Fix(\tilde{G}_{\tilde{u}})$. Potem obstaja enoličen $c \in CT(\wp)$, da velja $\tilde{u}' = c\tilde{u}$. Za vsak $g \in \tilde{G}_{\tilde{u}}$ velja $gc\tilde{u} = c\tilde{u}$

in zato $c^{-1}gc\tilde{u} = \tilde{u}$. Torej je $c^{-1}gc \in \tilde{G}_{\tilde{u}}$ za vsak $g \in \tilde{G}_{\tilde{u}}$, od koder sledi, da c leži v normalizatorju $N_{CT_\wp}(\tilde{G}_{\tilde{u}})$ grupe $\tilde{G}_{\tilde{u}}$ znotraj $CT(\wp)$. Ker je $\tilde{G}_{\tilde{u}}$ komplement grupe $CT(\wp)$, je $N_{CT_\wp}(\tilde{G}_{\tilde{u}})$ pravzaprav centralizator $C_{CT_\wp}(\tilde{G}_{\tilde{u}})$ grupe $\tilde{G}_{\tilde{u}}$ znotraj $CT(\wp)$. Zato $C_{CT_\wp}(\tilde{G}_{\tilde{u}})$ deluje tranzitivno in posledično regularno na množici $Fix(\tilde{G}_{\tilde{u}})$. To pomeni, da je $|\mathrm{Sec}_\Omega(\overline{G})| = |C_{CT_\wp}(\tilde{G}_{\tilde{u}})|$. Nazadnje, $|Fix(\tilde{G}_{\tilde{u}})|$ ni odvisno od izbire vozlišča $\tilde{u} \in \mathrm{fib}_u$, saj so stabilizatorji tranzitivnega delovanja konjugirane podgrupe. □

Za poglobljen študij invariantnih prerezov je pogosto potrebno določiti referenčno vozlišče znotraj vlakna. Po eni strani je zelo verjetno, da mora biti takšno vozlišče izbrano iz množice $Fix(\overline{G} \cap \widetilde{G_u})$, po drugi strani pa je primerno, da je izbor referenčnega vozlišča v vlaknu poljuben. V ta namen moramo obravnavati komplemente do ekvivalence natanko, kar pa je tako ali tako običajen pristop. Misel podkrepimo z naslednjo trditvijo.

Trditev 7.1.3: Predpostavimo, da je $G(\Omega) = \Omega$ in da se G dvigne kot prerezna razcepna razširitev grupe $CT(\wp)$ nad Ω. Naj bo $\overline{G}$ prerezni komplement grupe $CT(\wp)$ z invariantnim prerezom $\bar{\Omega}$ nad Ω in $c \in CT(\wp)$ poljuben. Potem je konjugirana podgrupa $c\,\overline{G}\,c^{-1}$ tudi prerezni komplement grupe $CT(\wp)$ z invariantnim prerezom $c(\bar{\Omega})$ nad Ω.

Zdaj bi radi prešteli število invariantnih prerezov nad orbito v nekem določenem vozlišču, ki so porojene s komplementi iz danega konjugiranostnega razreda. Naj bo $\mathscr{C}$ konjugiranostni razred prereznih komplementov grupe $CT(\wp)$ znotraj $\tilde{G}$ in $\mathrm{Sec}_{\tilde{u}}(\mathscr{C})$ množica prerezov nad orbito $G(u)$ v vozlišču $\tilde{u} \in \wp^{-1}(u)$, ki so invariantne za delovanje kakšnega komplementa v $\mathscr{C}$. Čeprav je ta množica odvisna od izbire $\tilde{u}$, pa njena moč ni. Dejstvo, da $CT(\wp)$ deluje regularno na $\wp^{-1}(u)$ in tranzitivno s konjugacijo na $\mathscr{C}$, nam da naslednji izrek.

Izrek 7.1.4: Predpostavimo, da je $G(\Omega) = \Omega$ in da se G dvigne kot prerezna razcepna razširitev grupe $CT(\wp)$ nad Ω. Naj bo $\overline{G}$ prerezni komplement in u poljubno vozlišče v Ω. Potem število prerezov v $\mathrm{Sec}_{\tilde{u}}(\mathscr{C})$ ni odvisno od izbire vozlišča $\tilde{u}$ v vlaknu $\wp^{-1}(u)$ in velja

$$|\mathrm{Sec}_{\tilde{u}}(\mathscr{C})| = |Fix(\tilde{G}_{\tilde{u}})| \,/\, |C_{CT(\wp)}(\overline{G})| = |C_{CT(\wp)}(\tilde{G}_{\tilde{u}})| \,/\, |C_{CT(\wp)}(\overline{G})|.$$

Dokaz: Konjugacija s $c \in CT(\wp)$ ohranja $\mathscr{C}$ in po Trditvi 7.1.3 preslika množico $\mathrm{Sec}_{\tilde{u}}(\mathscr{C})$ na množico $\mathrm{Sec}_{c(\tilde{u})}(\mathscr{C})$. Ta preslikava je očitno bijekcija, zato $|\mathrm{Sec}_{\tilde{u}}(\mathscr{C})|$ ni

odvisna od izbire vozlišča $\tilde{u}$. Poglejmo si sedaj množico

$$\bigcup_{\tilde{u}\in\wp^{-1}(u)} \mathrm{Sec}_{\tilde{u}}(\mathscr{C})$$

vseh prerezov nad $G(u)$, ki so invariantni na delovanje kakšnega komplementa iz $\mathscr{C}$. Število vseh takšnih prerezov bomo prešteli na dva načina.

Po eni strani je to število enako

$$|\mathrm{Sec}_{\tilde{u}}(\mathscr{C})| \cdot |CT(\wp)|.$$

Po drugi strani najprej spomnimo, da ima vsak komplement $\overline{G} \in \mathscr{C}$ natanko $|Fix(\tilde{G}_{\tilde{u}})|$ invariantnih prerezov. Še več, ker je $c\,\overline{G}\,c^{-1} \cap \widetilde{G_u} = c\,\tilde{G}_{\tilde{u}}\,c^{-1}$ in imajo konjugirane podgrupe isto število negibnih vozlišč, število $|Fix(\tilde{G}_{\tilde{u}})|$ ni odvisno od predstavnika $\overline{G} \in \mathscr{C}$. Torej je število vseh invariantnih prerezov enako $|Fix(\tilde{G}_{\tilde{u}})| \cdot |\mathscr{C}|$. Spomnimo, da je v splošnem kardinalnost konjugiranostnega razreda podgrup enaka indeksu normalizatorja poljubnega predstavnika razreda. Ker je $\mathscr{C}$ konjugiranostni razred prereznih komplementov, že sama grupa $CT(\wp)$ deluje s konjugacijo tranzitivno na $\mathscr{C}$. Torej je indeks pravzaprav enak $[CT(\wp) : C_{CT(\wp)}(\overline{G})]$ (glej, na primer, [50]). Število vseh invariantnih prerezov je zato enako

$$|Fix(\tilde{G}_{\tilde{u}})| \cdot |CT(\wp)| / |C_{CT(\wp)}(\overline{G})|.$$

Združimo skupaj obe štetji ter upoštevajmo Izrek 7.1.2 in rezultat sledi. □

7.2 *Prerezne razcepne razširitve, kombinatorično*

Potrebne in zadostne pogoje, da se grupa G dvigne kot prerezna razcepna razširitev nad Ω, so kombinatorično z regularnimi napetostmi podali Malnič in soavtorji. To je povzeto v naslednjem izreku.

Izrek 7.2.1: ([15, Izrek 9.1, Izrek 9.3]) Pri zgornji notaciji in predpostavki, da je Ω invariantna na delovanje grupe G, se G dvigne kot prerezna razcepna razširitev nad Ω natanko tedaj, ko lahko projekcijo $\wp$ rekonstruiramo z regularno napetostno funkcijo ζ na grafu X, ki zadošča pogoju

$$\zeta(W) = 1 \Rightarrow \zeta(g(W)) = 1 \tag{7.1}$$

za vsak avtomorfizem g v G in vsak sprehod W v X, ki se začne in konča v Ω.

Na tem mestu najprej omenimo, da je ta izrek razširjena verzija starega Biggsovega rezultata (glej [35]), formuliranega v drugačnem jeziku. Poleg tega je Malnič nadalje uporabil ta izrek v [37], kjer je v grobem opisal metodo za testiranje, ali se G dvigne kot prerezna razcepna razširitev nad Ω (toda brez dokaza). Ideja je naslednja: vpeljemo novo vozlišče, ki ga povežemo z vsemi vozlišči v Ω, in nato prevedemo pogoj (7.1) na splošen problem dviga avtomorfizmov. To idejo bomo v nadaljevanju izkoristili v drugo smer – in sicer za konstrukcijo vseh povezanih regularnih krovnih projekcij $\wp\colon \tilde{X} \to X$, vzdolž katerih se G dvigne kot prerezna razcepna razširitev nad Ω (glej Razdelek 7.4). V ta namen vpeljimo naslednjo notacijo.

Stožec $\widehat{X}(\Omega)$ nad X je graf, ki ga dobimo tako, da dodamo novo vozlišče $*$ in ga povežemo z vsakim vozliščem v Ω. Ob predpostavki, da je Ω invariantna na delovanje grupe G, z $\widehat{G}$ označimo podgrupo avtomorfizmov stožca $\widehat{X}$, ki fiksira vozlišče $*$ in deluje na X kot grupa G. Nadalje, razširitev regularne napetostne funkcije $\zeta\colon X \to \Gamma$ na stožec $\widehat{X}(\Omega)$ je regularna napetostna funkcija $\widehat{\zeta}\colon \widehat{X}(\Omega) \to \Gamma$, ki jo dobimo tako, da novim lokom $(u, *)$, $u \in \Omega$, predpišemo poljubne napetosti v Γ, njenim nasprotnim lokom pa ustrezne inverzne napetosti. Obratno, če je ζ regularna napetostna funkcija na $\widehat{X}(\Omega)$, potem njeno restrikcijo na graf X označimo z $\bar{\zeta}$. Potem veljata naslednji lemi.

Lema 7.2.2: Naj bosta $\zeta, \zeta'\colon \widehat{X}(\Omega) \to \Gamma$ ekvivalentni regularni napetostni funkciji na stožcu $\widehat{X}(\Omega)$. Potem sta tudi njuni restrikciji $\bar{\zeta}$ in $\bar{\zeta}'$ na graf X ekvivalentni.

Dokaz: Po definiciji ekvivalence projekcij obstaja izomorfizem $\tilde{g}$ izpeljanih grafov $\widehat{X}(\Omega) \times_\zeta \Gamma$ in $\widehat{X}(\Omega) \times_{\zeta'} \Gamma$, ki zadošča pogoju $\wp_\zeta = \tilde{g} \circ \wp_{\zeta'}$. Ker izomorfizem $\tilde{g}$ očitno preslika vlakno $\wp_\zeta^{-1}(*)$ na vlakno $\wp_{\zeta'}^{-1}(*)$, le-ta porodi izomorfizem izpeljanih grafov $X \times_{\bar{\zeta}} \Gamma$ in $X \times_{\bar{\zeta}'} \Gamma$. Sledi, da sta $\bar{\zeta}$ in $\bar{\zeta}'$ ekvivalentni. □

Lema 7.2.3: Naj bo $\zeta\colon X \to \Gamma$ povezana regularna napetostna funkcija na povezanem grafu X in $\widehat{\zeta}$ poljubna razširitev funkcije ζ na stožec $\widehat{X}(\Omega)$. Potem je regularna napetostna funkcija $\widehat{\zeta}$ tudi povezana. Nadalje, naj bo $\zeta'\colon X \to \Gamma$ regularna napetostna funkcija, ki je ekvivalentna ζ. Potem obstaja razširitev $\widehat{\zeta'}$ funkcije ζ', ki je ekvivalentna funkciji $\widehat{\zeta}$.

Dokaz: Izberimo bazno vozlišče u v Ω in vpeto drevo T v grafu X. Potem povezava $u \sim *$ skupaj z drevesom T definira vpeto drevo T^* v stožcu $\widehat{X}(\Omega)$. Opazimo, da so napetosti $\zeta(W)$ fundamentalnih sklenjenih sprehodov W v vozlišču u grafa X (glede

na drevo T) vsebovane v množici napetosti $\widehat{\zeta}(W^*)$ fundamentalnih sprehodov W^* v u_0 stožca $\widehat{X}(\Omega)$ (glede na drevo T^*), zato je funkcija $\widehat{\zeta}$ povezana.

Naj bo ζ' regularna napetostna funkcija, ki je ekvivalentna ζ. Ker sta po predpostavki ζ in ζ' povezani, sta ekvivalentni natanko tedaj, ko obstaja avtomorfizem α napetostne grupe Γ z lastnostjo $\alpha\zeta(W) = \zeta'(W)$ za vse fundamentalne sklenjene sprehode W v vozlišču u grafa X. Razširimo funkcijo ζ' na naslednji način. Ker lok $(u,*)$ leži na drevesu T^*, mu lahko predpišemo poljubno napetost v Γ. Naj bo W^* fundamentalni sklenjen sprehod v vozlišču u grafa $\widehat{X}(\Omega)$, ki ga določata drevo T^* in lok $(v,*)$, $v \neq u \in \Omega$. Potem lahko loku $(v,*)$ predpišemo takšno napetost v Γ, da velja $\alpha\widehat{\zeta}(W^*) = \widehat{\zeta'}(W^*)$. Tako definirana razširitev $\widehat{\zeta'}$ je očitno ekvivalentna $\widehat{\zeta}$. □

Zdaj imamo pripravljeno vse, da v kombinatoričnem smislu med sabo povežemo regularne krovne projekcije grafa X, vzdolž katerih se G dvigne kot prerezna razcepna razširitev nad Ω, in regularne krovne projekcije stožca $\widehat{X}(\Omega)$, vzdolž katerih se $\widehat{G}$ dvigne.

Izrek 7.2.4: Naj bo $\zeta\colon X \to \Gamma$ regularna napetostna funkcija, ki rekonstruira regularno krovno projekcijo $\wp\colon \tilde{X} \to X$ povezanih grafov, in G podgrupa avtomorfizmov grafa X. Predpostavimo, da je Ω neprazna podmnožica vozlišč grafa X, ki je invariantna na delovanje grupe G. Potem se G dvigne vzdolž projekcije $\wp$ kot prerezna razcepna razširitev nad Ω natanko tedaj, ko obstaja neka razširitev $\widehat{\zeta}\colon \widehat{X}(\Omega) \to \Gamma$ regularne napetostne funkcije ζ, da se $\widehat{G}$ dvigne vzdolž njene izpeljane regularne krovne projekcije $\wp_{\widehat{\zeta}}\colon \widehat{X}(\Omega) \times_{\widehat{\zeta}} \Gamma \to \widehat{X}(\Omega)$.

Dokaz: Predpostavimo, da se G dvigne vzdolž projekcije $\wp$ kot prerezna razcepna razširitev nad Ω. Po Trditvi 7.2.1 obstaja regularna napetostna funkcija ζ' na grafu X, ki prav tako rekonstruira $\wp$ (ζ in ζ' sta ekvivalentni!) in zadošča pogoju (7.1). Zaradi dejstva, da se grupa dvigne vzdolž projekcije natanko tedaj, ko se dvigne vzdolž katerekoli ekvivalentne projekcije, in Leme 7.2.3 je dovolj poiskati razširitev $\widehat{\zeta'}$ funkcije ζ', da se $\widehat{G}$ dvigne vzdolž izpeljane regularne krovne projekcije $\wp_{\widehat{\zeta'}}$. Razširimo ζ' do regularne napetostne funkcije $\widehat{\zeta'}$ na stožcu $\widehat{X}(\Omega)$ tako, da novim lokom $(u,*)$, $u \in \Omega$, pripišemo trivialne napetosti. Pokažimo, da tako definirana $\widehat{\zeta'}$ porodi projekcijo $\wp_{\widehat{\zeta'}}$, vzdolž katere se $\widehat{G}$ dvigne. Res. Naj bo W^* sklenjen sprehod v vozlišču $*$, za katerega velja $\widehat{\zeta'}(W^*) = 1$. Izberimo poljuben avtomorfizem g^* v grupi $\widehat{G}$. Po osnovni lemi o dvigu moramo pokazati, da velja $\widehat{\zeta'}(g^*W^*) = 1$. Pišimo sprehod W^* kot produkt $W^* = W_1^*W_2^* \cdots W_k^*$ sklenjenih sprehodov v vozlišču $*$, kjer je

$W_i^* = P_i W_i Q_i^{-1}$ in je $W_i\colon u_i \to v_i$ sprehod v X z obema krajiščema u_i in v_i v Ω ter sta $P_i\colon * \to u_i$ in $Q_i\colon * \to v_i$ sprehoda dolžine 1, za $i = 1, 2, \dots, k$. Pripomnimo, da velja $\zeta'(W_1)\zeta'(W_2)\cdots\zeta'(W_k) = 1$. Izberimo zdaj vozlišče $u \in \Omega$. Naj bodo $R_i\colon u \to u_i$ and $S_i\colon u \to v_i$ sprehodi, za katere velja $\zeta'(R_i) = \zeta'(S_i) = 1$, za $i = 1, 2, \dots, k$ (takšni sprehodi vedno obstajajo!). Potem je produkt sprehodov $W = \prod_{i=1}^{k} R_i W_i S_i^{-1}$ sklenjen sprehod v vozlišču u in velja $\zeta'(W) = \zeta'(W_1)\zeta'(W_2)\cdots\zeta'(W_k) = 1$. Ker ζ' zadošča pogoju (7.1), velja $\zeta'(gW) = 1$ kot tudi $\zeta'(gR_j) = \zeta'(gS_j) = 1$, za $i = 1, 2, \dots, k$. Torej iz $\zeta'(gW_1)\zeta'(gW_2)\dots\zeta'(gW_k) = 1$ sledi, da je $\widehat{\zeta'}(g^*W^*) = 1$, kar smo želeli pokazati.

Obratno, naj obstaja razširitev $\widehat{\zeta}$ napetostne funkcije ζ na stožec $\widehat{X}(\Omega)$, da se $\widehat{G}$ dvigne vzdolž njene izpeljane regularne krovne projekcije $\wp_{\widehat{\zeta}}$. Po Trditvi 7.2.1 je dovolj pokazati, da obstaja napetostna funkcija, ki rekonstruira projekcijo $\wp$ in zadošča pogoju (7.1). Naj bo ζ' napetostna funkcija na stožcu $\widehat{X}(\Omega)$, ki ima trivialne napetosti na novih lokih in je ekvivalentna $\widehat{\zeta}$ (takšna napetostna funkcija vedno obstaja). Pokažimo, da njena restrikcija $\bar{\zeta}'$ zadošča želenim pogojem. Ker je ζ tudi restrikcija napetostne funkcije $\widehat{\zeta}$, sta po Lemi 7.2.2 ζ in $\bar{\zeta}'$ ekvivalentni. Torej $\bar{\zeta}'$ rekonstruira projekcijo $\wp$. Nadalje, izberimo poljuben sprehod $W\colon u \to v$ v X, ki ima obe krajišči u in v v Ω, in naj velja $\bar{\zeta}'(W) = 1$. Označimo s $P\colon * \to u$ in $Q\colon * \to v$ sprehoda dolžine 1 v $\widehat{X}(\Omega)$. Potem ima sklenjen sprehod $W^* = PWQ^{-1}$ v vozlišču $*$ napetost $\zeta'(W^*) = 1$. Uporabimo osnovno lemo o dvigu, pa dobimo $\zeta'(g^*W^*) = 1$ za vsak avtomorfizem g^* v $\widehat{G}$. Torej velja $\bar{\zeta}'(gW) = 1$ in izrek je dokazan. □

Kar zadeva testiranje, kdaj se G dvigne vzdolž $\wp$ kot prerezna razcepna razširitev nad Ω, je ena izmed možnosti ta, da uporabimo Izrek 7.2.4. Čeprav nam v tem primeru ni potrebno posebej testirati, ali se G dvigne, bo pozoren bralec opazil, da je potrebno v najslabšem primeru preučiti $|\Gamma|^{|\Omega|-1}$ različnih razširitev regularne napetostne funkcije ζ, ki rekonstruira regularno krovno projekcijo $\wp$. Iz dokaza Leme 7.2.3 namreč sledi naslednje: če obstaja razširitev $\widehat{\zeta}$ funkcije ζ, da se $\widehat{G}$ dvigne vzdolž $\wp_{\widehat{\zeta}}$, potem obstaja tudi razširitev $\widehat{\zeta}'$ funkcije ζ s trivialno napetostjo $\widehat{\zeta}'(u, *) = 1$ na loku $(u, *)$, da se $\widehat{G}$ dvigne vzdolž $\wp_{\widehat{\zeta}'}$. Torej lahko loku $(u, *)$ vedno predpišemo trivialno napetost, za vsakega izmed ostalih $|\Omega| - 1$ lokov $(v, *)$ pa imamo na izbiro $|\Gamma|$ možnih napetosti. Do istega zaključka lahko pridemo tudi na drugačen način. Obstaja namreč bijektivna povezava med vsemi razširitvami funkcije ζ in vsemi prerezi nad Ω. Če je $\widehat{\zeta}$ razširitev, potem množica $\{\widehat{\zeta}(v, *) \mid v \in \Omega\}$ napetosti novih lokov natanko definira prerez $\{(v, \widehat{\zeta}(v, *))\}$ nad Ω in obratno. Ker po Trditvi 7.1.3 velja, da brž ko obstaja invarianten prerez nad

Ω (za nek komplement), obstaja tudi takšen invarianten prerez nad Ω (za konjugiran komplement), ki seka vlakno nad izbranim vozliščem u v vozlišču $(u, 1)$, moramo v najslabšem primeru pregledati $|\Gamma|^{|\Omega|-1}$ prerezov. V naslednjem razdelku bomo videli, da obstajajo učinkovitejše metode.

7.3 Testiranje prerezne razcepnosti razširitve

Naj bo $\zeta\colon X \to \Gamma$ končna povezana regularna napetostna funkcija na končnem povezanem grafu X in G podgrupa v grupi avtomorfizmov grafa X. Nadalje, naj bo Ω neprazna podmnožica vozlišč grafa X, ki je invariantna glede na delovanje grupe G. Denimo, da se grupa G dvigne vzdolž izpeljane regularne krovne projekcije $\wp\colon X \times_\zeta \Gamma \to X$. V tem poglavju bomo predstavili učinkovite metode za testiranje, kdaj je dvignjena grupa $\tilde{G}$ prerezna razcepna razširitev grupe krovnih transformacij $CT(\wp)$ nad Ω.

Zaradi istih razlogov kot v splošnem primeru testiranja, kdaj je dvignjena grupa $\tilde{G}$ razcepna razširitev, se tudi tu želimo izogniti eksplicitni konstrukciji tako izpeljanega grafa $X \times_\zeta \Gamma$ kot tudi grupe $\tilde{G}$. Prvi korak k rešitvi problema predstavlja naslednja trditev, ki jo izpeljemo iz točke (ii) Izreka 7.1.1.

Trditev 7.3.1: Naj bo $\wp\colon \tilde{X} \to X$ regularna krovna projekcija povezanih grafov in $S_G = \{g_1, g_2, \dots, g_n\}$ množica generatorjev podgrupe G avtomorfizmov grafa X. Denimo, da je $G(\Omega) = \Omega$ in da se grupa G dvigne vzdolž projekcije $\wp$. Potem je dvignjena grupa $\tilde{G}$ prerezna razcepna razširitev grupe krovnih transformacij $CT(\wp)$ nad Ω natanko tedaj, ko obstajajo taki dvigi $\bar{g}_1, \bar{g}_2, \dots, \bar{g}_n$ generatorjev $g_1, g_2, \dots, g_n$, zaporedoma, da ima množica $\{\bar{g}_1, \bar{g}_2, \dots, \bar{g}_n\}$ invarianten prerez $\bar{\Omega}$ nad Ω.

Dokaz: Po Izreku 7.1.1 je dovolj poiskati algebraično transverzalo grupe $CT(\wp)$, ki ima invarianten prerez. Pokažimo, da lahko množico $\{\bar{g}_1, \bar{g}_2, \dots, \bar{g}_n\}$ iz trditve razširimo do zahtevane algebraične transverzale grupe $CT(\wp)$. Za vsak $g \in G$ moramo primerno izbrati po en dvig. Pišimo g kot produkt generatorjev $g = g_{i_1} g_{i_2} \cdots g_{i_m}$ in naj bo $\bar{g}_{i_1} \bar{g}_{i_2} \cdots \bar{g}_{i_m}$ izbrani dvig. Na ta način res dobimo transverzalo. Namreč, če je $g = g_{j_1} g_{j_2} \cdots g_{j_k}$, potem oba dviga $\bar{g}_{i_1} \bar{g}_{i_2} \cdots \bar{g}_{i_m}$ in $\bar{g}_{j_1} \bar{g}_{j_2} \cdots \bar{g}_{j_k}$ preslikata vozlišče $\tilde{u} \in \bar{\Omega}$ v isto vozlišče, saj ima množica $\{\bar{g}_1, \bar{g}_2, \dots, \bar{g}_n\}$ invarianten prerez. Torej sta oba dviga enaka. Očitno ima tako dobljena algebraična transverzala invarianten prerez $\bar{\Omega}$. □

V praksi je grupa G običajno dana z množico permutacij, ki generirajo grupo G. Zato predpostavimo, da je G dana z množico generatorjev $S_G = \{g_1, g_2, \dots, g_n\}$. Po pravkar

dokazani trditvi množica $\{\bar{g}_1, \bar{g}_2, \dots, \bar{g}_n\}$, ki ima invarianten prerez $\bar{\Omega}$ nad Ω, generira prerezni komplement $\overline{G}$ grupe $CT(\wp)$.

Izberimo bazno vozlišče u v množici Ω. Vsaka n-terica elementov $t_1, t_2, \dots, t_n$ v napetostni grupi Γ skupaj s predpisi $\bar{g}_i(u,1) = (g_i(u), t_i)$, $i = 1, 2 \dots, n$, natanko določa množico $\{\bar{g}_1, \bar{g}_2, \dots, \bar{g}_n\}$. V luči Trditve 7.3.1 in Trditve 7.1.3 je tako dovolj preveriti, ali obstaja kakšna n-terica, za katero ima množica $\{\bar{g}_1, \bar{g}_2, \dots, \bar{g}_n\}$ takšen invarianten prerez $\bar{\Omega}$, ki seka vlakno $\wp^{-1}(u)$ v vozlišču $(u,1)$.

Kako pa je s testiranjem, kdaj ima dana množica $\{\bar{g}_1, \bar{g}_2, \dots, \bar{g}_n\}$, porojena z elementi $t_1, t_2, \dots, t_n$, invarianten prerez $\bar{\Omega}$, ki seka vlakno $\wp^{-1}(u)$ v vozlišču $(u,1)$? Zaradi poenostavitve predpostavimo, da množica Ω sestoji iz ene same orbite. Tedaj je v resnici potrebno preveriti, ali je orbita vozlišča $(u,1)$ glede na delovanje grupe $\langle \bar{g}_1, \bar{g}_2, \dots, \bar{g}_n \rangle$ prerez. To lahko dosežemo s tem, da modificiramo algoritem za računanje orbite.

Opišimo najprej standardni algoritem za računanje orbite vozlišča u glede na delovanje grupe $G = \langle g_1, g_2, \dots, g_n \rangle$. Naj bo Δ prazna vrsta. Inicializirajmo $\Delta := [u]$. Potem pregledamo elemente v vrste Δ v istem vrstnem redu, kot so bili najdeni, in za vsak generator g_i izračunamo sliko $g_i(v)$. Če slike $g_i(v)$ še ni v Δ, potem jo dodamo na konec vrste. Na koncu so dobljeni elementi v Δ natanko elementi orbite Ω.

Predstavimo poljuben prerez $\bar{\Omega}$ nad Ω s tabelo S, ki jo indeksiramo z elementi množice Ω, se pravi $S[v] = c$, kjer je $(v,c) \in \bar{\Omega}$. Radi bi konstruirali orbito vozlišča $(u,1)$ glede na delovanje grupe $\langle \bar{g}_1, \bar{g}_2, \dots, \bar{g}_n \rangle$ in hkrati med samo konstrukcijo preverjali, ali ustreza pogoju za prerez. Definirajmo dodatno prazno tabelo S dolžine $|\Omega|$ in postavimo $S[u] := 1$. Potem moramo na vsakem koraku v opisanem standardnem algoritmu poleg slike $g_i(v)$ izračunati še $\tau_{v,\bar{g}_i}(S[v])$ – drugo komponento slike $\bar{g}_i(v, S[v])$, ki jo dobimo z uporabo formule (6.1). Če slike $g_i(v)$ še ni v Δ, definiramo še $S[g_i(v)] := \tau_{v,\bar{g}_i}(S[v])$, v nasprotnem pa mora veljati pogoj

$$S[g_i(v)] = \tau_{v,\bar{g}_i}(S[v]). \tag{7.2}$$

Brž ko ta pogoj ni izpolnjen, orbita ne bo prerez, zato tedaj algoritem prekinemo. Formalna koda je podana v Algoritmu 7.1.

Opazimo, da moramo v najslabšem primeru pregledati celotno množico Γ^n. V praksi je ponavadi množica generatorjev majhna, za $n > |\Omega| - 1$ pa moramo v najslabšem primeru pregledati celotno množico $\Gamma^{|\Omega|-1}$.

Opomba 7.3.2: Algoritem 7.1 lahko enostavno razširimo, če Ω sestoji iz več kot ene orbite.

Algoritem 7.1: Testiranje prerezne razcepnosti

Vhodni parametri: povezana regularna napetostna funkcija $\zeta\colon X \to \Gamma$ na končnem povezanem grafu X, kjer je Γ končna grupa, dana s prezentacijo $\langle S_\Gamma | R_\Gamma \rangle$,
grupa $G = \langle g_1, g_2, \dots, g_n \rangle \leq \mathrm{Aut}(X)$, ki se dvigne
elementi $t_1, \dots, t_n$ v Γ, ki določajo podgrupo $\langle \bar{g}_1, \bar{g}_2, \dots, \bar{g}_n \rangle$,
orbita Ω

Izhodni parametri: true, če je $\langle \bar{g}_1, \bar{g}_2, \dots, \bar{g}_n \rangle$ prerezni komplement, false sicer

```
1:  u ← poljubno vozlišče v Ω;
2:  S ← prazna tabela elementov iz Γ dolžine |Ω|;
3:  Δ ← [u];
4:  S[u] ← 1_Γ;
5:  prerez ← true;
6:  for v ∈ Δ do
7:      for i ← 1 to n do
8:          izračunaj sliko τ_{v,ḡ_i}(S[v]);
9:          if g_i(v) ∉ Δ then
10:             Δ ← dodaj g_i(v) v Δ;
11:             S[g_i(v)] ← τ_{v,ḡ_i}(S[v]);
12:         else
13:             if S[g_i(v)] ≠ τ_{v,ḡ_i}(S[v]) then prerez ← false, break;
14: return prerez;
```

Opomba 7.3.3: Primerjaj Algoritem 7.1 s pristopom, ki je opisan na koncu Razdelka 7.2.

Podobno kot v prejšnjem poglavju se lahko tudi tu izognemo takšnemu pregledovanju v primeru, ko je napetostna grupa Γ abelska. Tedaj se problem iskanja prereznega komplementa prevede na ekvivalenten problem reševanja linearnega sistema enačb nad celimi števili.

7.3.1 Abelski regularni krovi

Naj bo Γ abelska grupa, dana s prezentacijo $\Gamma = \langle S_\Gamma \mid R_\Gamma \rangle$ na množici generatorjev $S_\Gamma = \{c_1, c_2, \dots, c_d\}$ in z relatorji $\lambda_k(c_1, c_2, \dots, c_d) \in R_\Gamma$, $k = 1, 2, \dots, s$. Na hitro ponovimo opazke iz Razdelka 6.1.1.

Vsak element $c \in \Gamma$ lahko reprezentiramo kot stolpični vektor $\underline{c} \in \mathbb{Z}^{d\times 1}$ (do relacij λ_j natanko). Poleg tega vsak avtomorfizem $\phi \in \mathrm{Aut}(\Gamma)$ reprezentiramo (zopet ne enolično) kot matriko nad celimi števili $\mathbb{Z}$. Matriko, ki reprezentira $g_i^\#$, označimo z $M_i = M_{g_i^\#}$. Formula za izračun napetosti $\tau_{v_{\tilde{g}_i}}(c)$ se v vektorski obliki glasi

$$T_{v_{\tilde{g}_i}}(\underline{c}) = \underline{t_i} + M_i \cdot \underline{c} + M_i \cdot \underline{\zeta(Q)} - \underline{\zeta(g_i(Q))}.$$

Obravnavajmo sedaj vektorje $\underline{t_i}$ kot neznanke. Simbolnemu računanju se izognemo tako, da zložimo vse vektorje $\underline{t_i}$ v stolpec dn neznank

$$\mathbf{t} = \begin{bmatrix} \underline{t_1} \\ \vdots \\ \underline{t_n} \end{bmatrix} \in \mathbb{Z}^{dn\times 1}$$

in za vsak indeks i definiramo matriko $E_i = [0, \dots, 0, \mathrm{I}, 0, \dots, 0] \in \mathbb{Z}^{d\times dn}$, ki sestoji iz $n-1$ ničelnih podmatrik $0 \in \mathbb{Z}^{d\times d}$ in ene identične podmatrike $\mathrm{I} \in \mathbb{Z}^{d\times d}$ na i-tem mestu. Spomnimo še, da lahko vsak vektor $T_{v_{\tilde{g}_i}}(\underline{c})$ zapišemo kot

$$T_{v_{\tilde{g}_i}}(\underline{c}) = (E_i + M_i \cdot A) \cdot \mathbf{t} + M_i \cdot (\underline{b} + \underline{\zeta(Q)}) - \underline{\zeta(g_i Q)},$$

kjer je $\underline{c} = A \cdot \mathbf{t} + \underline{b}$ za neko matriko $A \in \mathbb{Z}^{d\times dn}$ in nek vektor $\underline{b} \in \mathbb{Z}^{d\times 1}$, ki ne vsebujeta simbolnih vrednosti. Torej je vsak vektor med samim izračunom vrednosti natanko določen s parom $(A, \underline{b})$.

Uporabimo opisano idejo za konstrukcijo orbite v vozlišču $(u, 0)$. Na začetku za vektor $\underline{0}$, ki reprezentira element $0 \in \Gamma$, vzamemo kar ničelni vektor in postavimo $S[u] := (0, \underline{0})$, kjer je 0 ničelna matrika. Vsakič, ko se med pregledovanjem vrste Δ zgodi $g_i(v) \in \Delta$, se pogoj (7.2) prevede v linearni sistem r enačb z rn neznankami. Natančneje, če je $T_{v_{\tilde{g}_i}}(S[v]) = (X, \underline{x})$ in $S[g_i(v)] = (A', \underline{b'})$, potem dobimo sistem $(X - A') \cdot \mathbf{t} = \underline{b'} - \underline{x}$. Opazimo, da se med izvajanjem algoritma pogoj (7.2) izvrši natanko $(|\Omega| n - (|\Omega| - 1))$-krat. Torej nam algoritem vrne sistem $d(|\Omega|(n-1) + 1)$

Algoritem 7.2: Konstrukcija sistema

Vhodni parametri: grupa $G = \langle g_1, g_2, \dots, g_n \rangle \leq \mathrm{Aut}(X)$,
napetosti $\zeta(Q)$ in $\zeta(g_i(Q))$, kjer je $Q\colon v \to u$ poljuben sprehod za vsako vozlišče v,
matrike $M_i \in \mathbb{Z}^{d\times d}$, ki reprezentirajo avtomorfizme $g_i^{\#}$,
orbita Ω

Izhodni parametri: matrika $\mathbf{A}$, vektor $\mathbf{b}$

$u \leftarrow$ poljubno vozlišče v Ω;
$S \leftarrow$ prazna tabela parov $(A \in \mathbb{Z}^{d\times dn}, \underline{b} \in \mathbb{Z}^{d\times 1})$ dolžine $|\Omega|$;
$\mathbf{A} \leftarrow 0 \times dn$ matrika nad $\mathbb{Z}$;
$\mathbf{b} \leftarrow 0 \times 1$ vektor nad $\mathbb{Z}$;
$\Delta \leftarrow [u]$;
$S[u] \leftarrow (0, \underline{0})$, kjer je 0 ničelna matrika v $\mathbb{Z}^{d\times dn}$ in $\underline{0}$ ničelni vektor v $\mathbb{Z}^{d\times 1}$;
for $v \in \Delta$ *do*
    naj bo $S[v] = (A, \underline{b})$;
    for $i \leftarrow 1$ *to* n *do*
        $X \leftarrow E_i + M_i \cdot A$; $\underline{x} \leftarrow M_i \cdot (\underline{b} + \underline{\zeta(Q)}) - \underline{\zeta(g_i(Q))}$;
        if $g_i(v) \notin \Delta$ *then*
            $\Delta \leftarrow$ dodaj $g_i(v)$ v Δ;
            $S[g_i(v)] \leftarrow (X, \underline{x})$;
        else
            naj bo $S[g_i(v)] = (A', \underline{b}')$;
            $\mathbf{A} \leftarrow \begin{bmatrix} \mathbf{A} \\ X - A' \end{bmatrix}$; $\mathbf{b} \leftarrow \begin{bmatrix} \mathbf{b} \\ \underline{b}' - \underline{x} \end{bmatrix}$;
return $\mathbf{A}$, $\mathbf{b}$;

enačb z dn neznankami. Formalna koda za konstrukcijo takšnega sistema je podana v Algoritmu 7.2.

Naj bo

$$\begin{bmatrix} A_1 \\ \vdots \\ A_m \end{bmatrix} \cdot \mathbf{t} = \begin{bmatrix} \underline{b}_1 \\ \vdots \\ \underline{b}_m \end{bmatrix} \tag{7.3}$$

sistem linearnih enačb, ki ga vrne Algoritem 7.2, kjer je $m = |\Omega|(n-1)+1$. Tedaj obstaja n-terica $t_1, t_2, \dots, t_n$, ki določa takšne dvige $\bar{g}_1, \bar{g}_2, \dots, \bar{g}_n$, za katere ima množica $\{\bar{g}_1, \bar{g}_2, \dots, \bar{g}_n\}$ invariantен prerez $\bar{\Omega}$ skozi vozlišče $(u, 1)$ natanko tedaj, ko je sistem (7.3) rešljiv modulo relacije Λ_j. Uvedimo dodatne spremenljivke $\underline{x}_1, \underline{x}_2, \dots, \underline{x}_m \in \mathbb{Z}^{s\times 1}$, pa dobimo linearni sistem nad celimi števil $\mathbb{Z}$

$$\begin{bmatrix} A_1 & \Lambda & 0 & \dots & 0 \\ A_2 & 0 & \Lambda & \dots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ A_m & 0 & \dots & & \Lambda \end{bmatrix} \cdot \begin{bmatrix} \mathbf{t} \\ \underline{x}_1 \\ \underline{x}_2 \\ \vdots \\ \underline{x}_m \end{bmatrix} = \begin{bmatrix} \underline{b}_1 \\ \underline{b}_2 \\ \vdots \\ \underline{b}_m \end{bmatrix}, \tag{7.4}$$

kjer je $\Lambda = \begin{bmatrix} \underline{\lambda_1} & \underline{\lambda_2} & \cdots & \underline{\lambda_s} \end{bmatrix} \in \mathbb{Z}^{d\times s}$ in so $\underline{\lambda_k}$ vektorji, ki reprezentirajo relatorje $\lambda_k \in R_\Gamma$.

Problem testiranja prerezne razcepnosti dane razširitve smo tako prevedli na ekvivalenten problem rešljivosti sistema linearnih enačb (7.4) nad $\mathbb{Z}$. Strnimo zgornje opazke v izrek.

Izrek 7.3.4: Pri zgornjih predpostavkah in notaciji je dvignjena grupa $\tilde{G}$ prerezna razcepna razširitev grupe krovnih transformacij $CT(\wp)$ po grupi G natanko tedaj, ko ima sistem linearnih enačb (7.4) celoštevilsko rešitev.

7.3.2 Elementarno abelski regularni krovi

Naj bo napetostna grupa Γ elementarno abelska grupa $\mathbb{Z}_p^d$, kjer vsak element v $\mathbb{Z}_p^d$ identificiramo s stolpičnim vektorjem v $\mathbb{Z}_p^{d\times 1}$ glede na standardno bazo. Potem namesto sistema (7.4) rešujemo sistem (7.3) nad $\mathbb{Z}_p$ z Gaussovo eliminacijsko metodo. To nam precej poenostavi računanje, poleg tega lahko natančno podamo časovno in prostorsko zahtevnost.

Opisan postopek, ki reši problem testiranja prerezne razcepnosti v primeru abelskih regularnih krovov, nam neposredno poda algoritem v primeru elementarno abelskih regularnih krovov. Formalna koda je podana v Algoritmu 7.3.

Izrek 7.3.5: Naj bo $\zeta: X \to \mathbb{Z}_p^d$ povezana regularna napetostna funkcija na končnem povezanem grafu X in naj se podgrupa $G = \langle g_1, g_2, \dots, g_n \rangle$ avtomorfizmov baznega grafa X dvigne. Potem Algoritem 7.3 testira, ali je dvignjena grupa prerezna razcepna razširitev grupe krovnih transformacij po grupi G nad Ω.

Izrek 7.3.6: Naj se podgrupa $G = \langle g_1, g_2, \dots, g_n \rangle$ avtomorfizmov končnega povezanega grafa X ranga r dvigne vzdolž povezane regularne krovne projekcije, dane z regularno napetostno funkcijo $\zeta\colon X \to \mathbb{Z}_p^d$. Potem obstaja algoritem, ki reši problem testiranja prerezne razcepnosti razširitve dvignjene grupe $\tilde{G}$ nad Ω v $\mathcal{O}(n|V(X)| + nd|E(X)| + d^3r + nd^2r + n^3d^3|\Omega|^2)$, uporabljajoč $\mathcal{O}(|V(X)| + dn|E(X)| + n^2d^2|\Omega|)$ prostora.

Dokaz: Napetosti $\zeta(W^{a_k})$, $\zeta(g_i(W^{a_k}))$, $\zeta(Q)$ in $\zeta(g_i(Q))$ v Algoritmu 7.3 izračunamo s pregledom grafa v širino, kjer je cena vsake povezave $\mathcal{O}(d)$; skupaj to vzame $\mathcal{O}(n|V(X)| + nd|E(X)|)$ korakov. Za izračun matrik $M_i \in \mathbb{Z}^{d\times d}$ moramo najprej rešiti d linearnih sistemov enačb kot v (6.5). Reševanje enega sistema z Gaussovim postopkom vzame $\mathcal{O}(d^2r)$ korakov; za reševanje d sistemov torej skupaj $\mathcal{O}(d^3r)$ korakov. Poljubno matriko M_i lahko potem izračunamo v $\mathcal{O}(d^2r)$ korakih; vse matrike M_i, $i = 1, 2, \dots, n$, pa v $\mathcal{O}(nd^2r)$ korakih. Časovna zahtevnost Algoritma 7.2, ki vrne matriko $\mathbf{A} \in \mathbb{Z}_p^{(d|\Omega|(n-1)+d)\times dn}$ in vektor $\mathbf{b} \in \mathbb{Z}_p^{(d|\Omega|(n-1)+d)\times 1}$, je $\mathcal{O}(n^2d^3|\Omega|)$. Nato moramo rešiti le še linearni sistem $\mathbf{A}\cdot\mathbf{t} = -\mathbf{b}$. Reševanje z Gaussovim postopkom vzame $\mathcal{O}(d^3n^3|\Omega|^2)$ korakov. Problem testiranja prerezne razcepnosti lahko torej rešimo v $\mathcal{O}(n|V(X)| + nd|E(X)| + d^3r + nd^2r + n^3d^3|\Omega|^2)$ korakih.

Za predstavitev grafa X s seznamom sosedov potrebujemo $\mathcal{O}(|V(X)|+|E(X)|)$ prostora, za poljuben vektor v $\mathbb{Z}_p^d$ pa $\mathcal{O}(d)$ prostora. Torej lahko napetostno funkcijo ζ predstavimo z $\mathcal{O}(|V(X)| + d|E(X)|)$ prostora, posamezen avtomorfizem g_i pa z $\mathcal{O}(|V(X)|)$; za vse avtomorfizme zato potrebujemo $\mathcal{O}(n|V(X)|)$. Med pregledom grafa v širino potrebujemo $\mathcal{O}(n|V(X)|)$ prostora, da shranimo preslikana vozlišča, in $\mathcal{O}(nd|E(X)|)$ dodatnega prostora, da shranimo vse preslikane napetosti. Da shranimo matrike M_i, je potrebnega še $\mathcal{O}(nd^2)$ prostora. Matrika $\mathbf{A}$ vzame še $\mathcal{O}(n^2d^2|\Omega|)$ prostora. Skupna prostorska zahtevnost je torej $\mathcal{O}(n|V(X)| + nd|E(X)| + n^2d^2|\Omega|)$. □

7.4 *Konstrukcija vseh prereznih razcepnih razširitev*

Naj bo X povezan graf, G podgrupa njegovih avtomorfizmov in Ω neprazna podmnožica vozlišč grafa X, ki je invariantna na delovanje grupe G. V tem razdelku se bomo posvetili kombinatorični konstrukciji regularnih napetostnih funkcij grafa X, ki porodijo do ekvivalence natanko takšne povezane regularne krovne projekcije, vzdolž katerih se G dvigne kot prerezna razcepna razširitev nad Ω.

Kot smo omenili že na začetku poglavja, osnovna ideja temelji na Izreku 7.2.4. Najprej poiščemo do ekvivalence natanko vse regularne napetosti ζ stožca $\widehat{X}(\Omega)$, ki poro-

Algoritem 7.3: Testiranje prerezne razcepnosti – elementarno abelske regularne napetosti

Vhodni parametri: povezana regularna napetostna funkcija $\zeta\colon X \to \mathbb{Z}_p^d$ na končnem povezanem grafu X,
grupa $G = \langle g_1, g_2, \dots, g_n \rangle \leq \mathrm{Aut}(X)$, ki se dvigne,
orbit Ω

Izhodni parametri: true, če je dvig prerezna razcepna razširitev, false sicer

1: $\mathbf{A} \leftarrow 0 \times dn$ matrika nad $\mathbb{Z}$;
2: $\mathbf{b} \leftarrow 0 \times 1$ vektor nad $\mathbb{Z}$;
3: izberi poljubno vozlišče u;
4: izračunaj matrike $M_i \in \mathbb{Z}^{d\times d}$, ki reprezentirajo avtomorfizme $g_i^{\#}$, skupaj z napetostmi $\zeta(Q)$ in $\zeta(g_i(Q))$, kjer je $Q\colon v \to u$ sprehod za vsako vozlišče v;
5: naj bosta matrika $\mathbf{A}$ in vektor $\mathbf{b}$ izhodna parametra, ki ju vrne Algoritem 7.2 pri konstrukciji sistema;
6: *if* sistem $\mathbf{A} \cdot \mathbf{t} = -\mathbf{b}$ ima rešitev *then*
7: *return* true;
8: *else*
9: *return* false;

dijo takšne povezane regularne krovne projekcije $\wp$, vzdolž katerih se $\widehat{G}$ dvigne. Čeprav je vsaka napetostna funkcija ζ povezana, pa ni nujno, da je povezana vsaka njena restrikcija $\bar{\zeta}$ na graf X. Brž ko je regularna napetostna funkcija $\bar{\zeta}$ povezana, se G dvigne vzdolž njene izpeljane regularne krovne projekcije $\wp_{\bar{\zeta}}$ kot prerezna razcepna razširitev nad Ω. Te opombe so formalno zapisane v naslednjem izreku.

Izrek 7.4.1: Naj bo X povezan graf in Ω neprazna podmnožica vozlišč grafa X, ki je invariantna na delovanje grupe G. Nadalje, naj bo ζ regularna napetostna funkcija na stožcu $\widehat{X}(\Omega)$, ki rekonstruira povezan regularen krov $\wp$ stožca $\widehat{X}(\Omega)$, vzdolž katerega se $\widehat{G}$ dvigne. Če je restrikcija $\bar{\zeta}$ na graf X povezana, potem se G dvigne vzdolž njene izpeljane regularne krovne projekcije $\wp_{\bar{\zeta}}$ kot prerezna razcepna razširitev nad Ω. Še več, vsaka povezana regularna projekcija $\tilde{X} \to X$, vzdolž katere se G dvigne kot prerezna razcepna razširitev nad Ω, je porojena na ta način.

Nenazadnje, če sta ζ in ζ' dve neekvivalentni povezani regularni napetostni funkciji

stožca $\widehat{X}(\Omega)$, se še vedno lahko zgodi, da sta njuni restrikciji $\bar{\zeta}$ in $\bar{\zeta}'$ na graf X povezani, toda ekvivalentni. Torej je potrebno dodatno testiranje.

Zdaj lahko natančno povzamemo naš pristop. Najprej poiščemo vse paroma neekvivalentne povezane regularne napetostne funkcije ζ stožca $\widehat{X}(\Omega)$, ki porodijo $\widehat{G}$-dopustne regularne krovne projekcije. Nato vzamemo njihove restrikcije $\bar{\zeta}$ na graf X in med njimi izločimo tiste, ki so nepovezane. Nazadnje med preostalim povezanimi restrikcijami naredimo nadaljnjo redukcijo, da dobimo vse paroma neekvivalentne povezane regularne napetostne funkcije grafa X, ki porodijo regularne krovne projekcije, vzdolž katerih se G dvigne kot prerezna razcepna razširitev nad Ω.

V bistvu smo prvotni problem prevedli na splošen problem iskanja dopustnih regularnih krovnih projekcij. Torej lahko problem konstrukcije regularni krovnih projekcij, vzdolž katerih se G dvigne kot prerezna razcepna razširitev, rešimo, brž ko znamo rešiti splošen problem dviga avtomorfizmov.

7.4.1 Elementarno abelski regularni krovi grafa K_4

V luči zgornje razprave bomo naš pristop ilustrirali z zgledom. Naj bo $X = K_4$ poln graf z množico vozlišč $V(X) = \{1, 2, 3, 4\}$ in $\Omega = V(X)$. Označimo z $g = (1234)$ avtomorfizem grafa X. Ker v primeru elementarno abelskih regularnih krovov obstajajo učinkovite metode za reševanje problema dviga avtomorfizmov, bomo poiskali vse paroma neekvivalentne povezane elementarno abelske regularne napetostne funkcije grafa X, ki porodijo regularne krovne projekcije, vzdolž katerih se ciklična grupa $G = \langle g \rangle$ dvigne kot prerezna razcepna razširitev nad Ω.

Najprej poiščemo vse paroma neekvivalentne povezane elementarno abelske regularne napetostne funkcije ζ stožca $\widehat{X}(\Omega)$, ki porodijo regularne krovne projekcije, vzdolž katerih se grupa $\widehat{G} = \langle g^* \rangle$ dvigne. V ta namen sledimo metodi, ki so jo razvili Malnič in soavtorji (glej [39]). Izberimo vpeto drevo T^* v stožcu $\widehat{X}(\Omega)$, ki sestoji iz vseh novih povezav $* \sim v$, $v \in V(X)$, in urejeno orientacijo $A^+(X) = \{a_1, a_2, \ldots, a_{10}\}$, kjer so

$$a_1 = (1,2),\ a_2 = (2,3),\ a_3 = (3,4),\ a_4 = (4,1),\ a_5 = (2,4),\ a_6 = (3,1)$$

loki v kodrevesu $\widehat{X}(\Omega) - T^*$, $a_7 = (*,1), a_8 = (*,2), a_9 = (*,3), a_{10} = (*,4)$ pa loki v drevesu T^*. Naj bo $B_{T^*} = \{[W^{a_i}] | 1 \leq i \leq 6\}$ urejena baza vektorskega prostora $H_1(\widehat{X}(\Omega), \mathbb{Z}_p)$, porojena z loki $a_1, a_2, \ldots, a_6$ in $(g^*)^{\#}$ linearna transformacija na $H_1(\widehat{X}(\Omega); \mathbb{Z}_p)$, inducirana z delovanjem avtomorfizma g^* na $H_1(X; \mathbb{Z}_p)$. Označimo

z M_{g^*} še matrično upodobitev transformacije $(g^*)^\#$ glede na bazo B_{T^*}. Po kratkem računanju dobimo transponirano matriko

$$A = M_{g^*}^t = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & 0 \end{bmatrix}.$$

Spomnimo, da je vsak elementarno abelski regularni $\mathbb{Z}_p^d$-krov grafa X nepovezan, če je razsežnost d večja kot je Bettijevo število grafa X. Ker je Bettijevo število grafa X enako tri, je zato dovolj poiskati vse A-invariantne podprostore v $\mathbb{Z}_p^{6\times 1}$ z razsežnostjo $d \leq 3$. Slednji podprostori definirajo regularne napetostne funkcije

$$\zeta\colon \widehat{X}(\Omega) \to \mathbb{Z}_p^{d\times 1}, \quad d = 1, 2, 3,$$

na stožcu $\widehat{X}(\Omega)$, ki porodijo paroma neekvivalentne povezane $\widehat{G}$-dopustne regularne krovne projekcije. Vendar, kot smo že omenili zgoraj, so lahko njihove restrikcije $\bar{\zeta}$ na graf X še vedno nepovezane, kot tudi povezane, toda ekvivalentne.

Da bi testirali, ali restrikcija $\bar{\zeta}$ na graf X ostane povezana, izberimo vpeto drevo T grafa X, ki sestoji iz povezav $1 \sim 2$, $1 \sim 3$ in $1 \sim 4$. Označimo s C_1, C_2 in C_3 sklenjene sprehode v X, določene z vpetim drevesom T in loki a_2, a_3 oziroma a_5. Problem povezanosti restrikcije na graf X se glede na urejeno bazo $B_T = \{C_1, C_2, C_3\}$ vektorskega prostora $H_1(X, \mathbb{Z}_p)$ prevede na pogoj, da napetosti

$$\begin{aligned} \zeta(C_1) &= \zeta(a_1) + \zeta(a_2) + \zeta(a_6), \\ \zeta(C_2) &= \zeta(a_3) + \zeta(a_4) - \zeta(a_6), \\ \zeta(C_3) &= \zeta(a_1) + \zeta(a_4) + \zeta(a_5) \end{aligned}$$

generirajo napetostno grupo $\mathbb{Z}_p^{d\times 1}$. Z drugimi besedami, ali ima matrika

$$\begin{bmatrix} \zeta(C_1)^t \\ \zeta(C_2)^t \\ \zeta(C_3)^t \end{bmatrix}$$

rang d.

Kar zadeva test ekvivalence restrikcij na graf X, naj bosta ζ oziroma ζ' regularni napetostni funkciji stožca $\widehat{X}(\Omega)$, definirani z različnima d-razsežnima podprostoroma v $\mathbb{Z}_p^{6\times 1}$, zaporedoma. Recimo, da sta njuni restrikciji $\bar{\zeta}$ in $\bar{\zeta}'$ na graf X tudi povezani. Potem sta $\bar{\zeta}$ in $\bar{\zeta}'$ ekvivalentni natanko tedaj, ko ima razširjena matrika

$$\left[\begin{array}{c|c} \zeta(C_1)^t & \zeta'(C_1)^t \\ \zeta(C_2)^t & \zeta'(C_2)^t \\ \zeta(C_3)^t & \zeta'(C_3)^t \end{array}\right]$$

rang d.

Poiščimo sedaj A-invariantne podprostore v $\mathbb{Z}_p^{6\times 1}$. Karakterisitčni polinom matrike A je $\kappa_A(x) = (x^4 - 1)(x^2 + 1)$, medtem ko je njen minimalni polinom

$$m_A(x) = x^4 - 1.$$

Opazimo, da je njuna razčlenitev na nerazcepne faktorje nad $\mathbb{Z}_p$ odvisna od kongruenčnega razreda praštevila p po modulu 4. Ker ima minimalni polinom naslednjo razčlenitev

$$m_A(x) = \begin{cases} (x-1)(x+1)(x^2+1), & p \equiv 3 \pmod 4; \\ (x-1)(x+1)(x-i)(x+i), & p \equiv 1 \pmod 4,\ i^2 = -1; \\ (x-1)^4, & p = 2, \end{cases}$$

ločimo naslednje tri primere.

Primer $p \equiv 3 \pmod 4$.

V tem primeru je po Maschkejevem izreku reprezentacija grupe $\langle A \rangle$ popolnoma razcepna. Lastni vrednosti sta 1 in -1, obe z večkratnostjo 1. Pripadajoča lastna podprostora sta $L_A(1) = \langle v_1 \rangle$ in $L_A(-1) = \langle v_2 \rangle$, kjer sta

$$v_1 = (1,1,1,1,0,0)^t \text{ in } v_2 = (1,-1,1,-1,0,0)^t.$$

Vektorski prostor $\mathbb{Z}_p^{6\times 1}$ je prema vsota A-invariantnih podprostorov

$$\mathbb{Z}_p^{6\times 1} = L_A(1) \oplus L_A(-1) \oplus \operatorname{Ker}(A^2 + I).$$

Očitno sta $L_A(1)$ in $L_A(-1)$ edina enorazsežna A-invariantna podprostora. Napetosti pripadajočih baznih homoloških ciklov C_1, C_2, C_3 grafa X so $2, 2, 2$ za tisti krov,

ki je definiran s $L_A(1)$, in $0,0,0$ za tistega, ki je definiran s $L_A(-1)$. Torej le $L_A(1)$ porodi povezan krov grafa X, medtem ko ga $L_A(-1)$ ne.

Ker dvorazsežni A-invariantni podprostor, porojen iz preme vsote $L_A(1) \oplus L_A(-1)$, ne da povezanega krova grafa X, morajo biti vsi ostali dvorazsežni A-invariantni podprostori vsebovani v $\mathsf{Ker}(A^2 + I)$. Ti podprostori so nujno oblike $\langle v, Av\rangle$ za $v \in \mathsf{Ker}(A^2 + I)$. Obstaja natanko $p^2 + 1$ različnih takšnih podprostorov. Izberimo si bazo prostora $\mathsf{Ker}(A^2 + I)$, na primer

$$\begin{aligned} b_1 &= (1,0,-1,0,0,0)^t, \\ b_2 &= (0,1,0,-1,0,0)^t, \\ b_3 &= (0,0,0,0,1,0)^t, \\ b_4 &= (0,0,0,0,0,1)^t, \end{aligned}$$

da preverimo, kateri od teh prostorov porodijo povezane krove grafa X. Poljuben vektor $v \in \mathsf{Ker}(A^2 + I)$ je potem oblike $v = (a,b,-a,-b,c,d)^t$ za $a,b,c,d \in \mathbb{Z}_p$, medtem ko je $Av = (b,-a,-b,a,d,-c)^t$. Označimo z

$$W_{a,b,c,d} = \langle (a,b,-a,-b,c,d)^t, (b,-a,-b,a,d,-c)^t \rangle.$$

Napetosti baznih homoloških ciklov C_1, C_2, C_3 grafa X, definirane s podprostorom $W_{a,b,c,d}$, so

$$\begin{aligned} \zeta(C_1) &= (a+b+d, -a+b-c)^t, \\ \zeta(C_2) &= (-a-b-d, a-b+c)^t, \\ \zeta(C_3) &= (a-b+c, a+b+d)^t. \end{aligned}$$

Iz pogoja za povezanost sledi, da mora biti rang matrike

$$\begin{bmatrix} \zeta(C_1)^t \\ \zeta(C_2)^t \\ \zeta(C_3)^t \end{bmatrix}$$

enak 2. Slednji pogoj se reducira na testiranje, ali sta vektorja $(a+b+d, -a+b-c)^t$ in $(a-b+c, a+b+d)^t$ linearno odvisna v $\mathbb{Z}_p^{2\times 1}$. Naj bo $x = a+b+d$ in $y = a-b+c$. Vektorja $(x,y)^t$ in $(-y,x)^t$ sta linearno odvisna natanko tedaj, ko je $x^2+y^2 \equiv 0 \pmod p$.

Ker je $p \equiv 3 \pmod 4$, je slednji pogoj izpolnjen natanko tedaj, ko velja $x \equiv 0 \pmod p$ in $y \equiv 0 \pmod p$ oziroma $c = -a + b$ in $d = -a - b$. To pomeni, da nepovezan krov grafa X porodijo natanko prostori, generirani z vektorjema

$$v_{a,b} = a(1,0,-1,0,-1,-1)^t + b(0,-1,0,1,-1,1)^t \text{ in } Av_{a,b}.$$

Pokažimo, da v resnici obstaja en sam takšen vektorski podprostor. Opazimo, da je vsak vektor $v_{a,b}$ vsebovan, na primer, v podprostoru $\langle v_{1,0}, Av_{1,0}\rangle$. Zato velja $\langle v_{a,b}, Av_{a,b}\rangle = \langle v_{1,0}, Av_{1,0}\rangle$ za vsak par $a, b \in \mathbb{Z}_p$. Torej je to edini dvorazsežni A-invariantni podprostor, ki porodi nepovezan krov grafa X. Kar zadeva ostale dvorazsežne podprostore, so le-ti oblike $W_{a,b,c,d}$, kjer je $(c,d) \neq (-a+b, -a-b)$. Poleg tega vsi ti podprostori porodijo ekvivalentne krove grafa X. Res. Izberimo si enega izmed teh prostorov, recimo

$$W_{1,1,0,0} = \langle (1,1,-1,-1,0,0)^t, (1,-1,-1,1,0,0)^t \rangle.$$

Naj bosta ζ in ζ' regularni napetostni funkciji, ki sta definirani s podprostoroma $W_{a,b,c,d}$, $(c,d) \neq (-a+b, -a-b)$, oziroma $W_{1,1,0,0}$, zaporedoma. Tedaj je

$$\begin{aligned}\zeta'(C_1) &= (2,0)^t,\\ \zeta'(C_2) &= (-2,0)^t,\\ \zeta'(C_3) &= (0,2)^t.\end{aligned}$$

Opazimo, da je $\zeta(C_1) = -\zeta(C_2)$ in $\zeta'(C_1) = -\zeta'(C_2)$, zato ima razširjena matrika

$$\left[\begin{array}{c|c} \zeta(C_1)^t & \zeta'(C_1)^t \\ \zeta(C_2)^t & \zeta'(C_2)^t \\ \zeta(C_3)^t & \zeta'(C_3)^t \end{array}\right]$$

rang 2 in trditev je dokazana. Kot predstavnika zgornjih dvorazsežnih podprostorov vzamemo $W_{1,1,0,0}$.

Vsak trirazsežni A-invariantni podprostor, ki porodi povezan krov grafa X, je ekvivalenten homološkem krovu grafa X, zato je dovolj poiskati enega takšnega, če obstaja. Hitro se lahko prepričamo, da recimo podprostor $L_A(1) \oplus W_{1,1,0,0}$ ustreza zgornjemu pogoju.

Primer $p \equiv 1 \pmod 4$.

Po Maschkejevem izreku je reprezentacija grupe $\langle A \rangle$ spet popolnoma razcepna. Matrika A je v tem primeru diagonalna, z diagonalno obliko $\mathrm{diag}_A(1, -1, i, i, -i, -i)$.

Očitno sta enorazsežna lastna podprostora $L_A(1)$ in $L_A(-1)$ enaka kot v prejšnjem primeru, kjer samo podprostor $L_A(1)$ porodi povezan krov grafa X. Za lastni vrednosti i in $-i$, ki zadoščata $i^2 \equiv -1 \pmod p$, sta oba pripadajoča lastna podprostora $L_A(i) = \langle u_i, v_i \rangle$ oziroma $L_A(-i) = \langle u_{-i}, v_{-i} \rangle$ dvorazsežna, kjer je

$$u_i = (1, i, -1, -i, 1, i)^t, \qquad u_{-i} = (1, -i, -1, i, 1, -i)^t,$$
$$v_i = (1, i, -1, -i, 0, 0)^t, \qquad v_{-i} = (1, -i, -1, i, 0, 0)^t.$$

Enorazsežne podprostore v $L_A(i)$ lahko ustrezno parametriziramo kot

$$W_\infty(i) = \langle u_i \rangle,$$
$$W_s(i) = \langle s u_i + v_i \rangle = \langle (s+1, (s+1)i, -(s+1), -(s+1)i, s, si)^t \rangle,\ s \in \mathbb{Z}_p,$$

medtem ko lahko tiste v $L_A(-i)$ parametriziramo kot

$$W_\infty(-i) = \langle u_{-i} \rangle,$$
$$W_s(-i) = \langle s u_{-i} + v_{-i} \rangle = \langle (s+1, -(s+1)i, -(s+1), (s+1)i, s, -si)^t \rangle,\ s \in \mathbb{Z}_p.$$

Pogoji za povezanost, ki jih izračunamo iz prostorov $W_\infty(i)$, $W_s(i)$, $W_\infty(-i)$, $W_s(-i)$, so $i - 2 \not\equiv 0 \pmod p$, $s(i-2) \not\equiv 1 - i \pmod p$, $-i - 2 \not\equiv 0 \pmod p$ oziroma $s(-i-2) \not\equiv 1 + i \pmod p$. Ločimo podprimera $p \neq 5$ in $p = 5$.

Naj bo $p \neq 5$. Potem je $i, -i \neq 2$ in obstaja natanko $2p + 1$ enorazsežnih podprostorov, ki porodijo povezane krove grafa X. Natančneje, množica

$$W_i = \{W_s(i) \mid s \in (\mathbb{Z}_p \backslash \{(1-i)(i-2)^{-1}\}) \cup \{\infty\}\}$$

p podprostorov v $L_A(i)$, množica

$$W_{-i} = \{W_s(-i) \mid s \in (\mathbb{Z}_p \backslash \{(1+i)(-i-2)^{-1}\}) \cup \{\infty\}\}$$

p podprostorov v $L_A(-i)$ in podprostor $L_A(1)$. Vendar vsi podprostori v W_i porodijo ekvivalentne restrikcije na graf X. Naj bosta ζ in ζ' regularni napetostni funkciji,

porojeni iz $W_s(i)$, $s \neq (1-i)(i-2)^{-1}$, oziroma $W_\infty(i)$, zaporedoma. Po kratkem računanju dobimo

$$\begin{aligned} \zeta(C_1) &= (s+1)(1+i)+si, & \zeta'(C_1) &= 1+2i,\\ \zeta(C_2) &= -(s+1)(1+i)-si = -\zeta(C_1), & \zeta'(C_2) &= -1-2i = -\zeta'(C_1),\\ \zeta(C_3) &= (s+1)(1-i)+s = -i\zeta(C_1), & \zeta'(C_3) &= 2-i = -i\zeta'(C_1). \end{aligned}$$

Očitno je rang razširjene matrike

$$\left[\begin{array}{c|c} \zeta(C_1)^t & \zeta'(C_1)^t \\ \zeta(C_2)^t & \zeta'(C_2)^t \\ \zeta(C_3)^t & \zeta'(C_3)^t \end{array}\right]$$

enak 1, zato sta restrikciji $\bar{\zeta}$ in $\bar{\zeta}'$ res ekvivalentni. Podobno lahko pokažemo, da tudi vsi podprostori v W_{-i} porodijo ekvivalentne restrikcije na graf X. Za predstavnika v W_i si izberimo $W_0(i)$, v W_{-i} pa $W_0(-i)$. Pravzaprav so natanko tri paroma neekvivalentne povezane restrikcije grafa X in sicer ena, ki je porojena iz $L_A(1)$, ter dve, ki sta porojeni iz $W_0(i)$ oziroma $W_0(-i)$. Pripadajoči seznam napetosti baznih homoloških ciklov C_1, C_2, C_3 grafa X so: $2, 2, 2$ za tisti krov, ki je porojen iz $L_A(1)$, in $1+i, -1-i, 1-i$ ter $1-i, -1+i, 1+i$ za ostala dva krova. Bralec lahko sam preveri, da so vse tri restrikcije paroma neekvivalentne.

Naj bo $p = 5$. Potem za vsak $s \in \mathbb{Z}_5$ podprostor $W_s(2)$ porodi povezan krov grafa X, medtem ko ga podprostor $W_\infty(2)$ ne. Po drugi strani za vsak $s \neq 3$ dobimo povezan graf X, porojen iz podprostora $W_s(3)$, in en povezan krov grafa X, porojen iz $W_\infty(3)$. Skupaj s krovom grafa X, ki je porojen iz $L_A(1)$, imamo natanko $2p+1 = 11$ povezanih krovov grafa X. Naj ζ označuje regularno napetostno funkcijo, porojeno iz $W_s(2)$. Potem elementaren izračun pokaže, da imajo bazni homološki cikli C_1, C_2, C_3 grafa X napetosti $\zeta(C_1) = 3(s+1)+2s = 3$, $\zeta(C_2) = -3(s+1)-2s = -\zeta(C_1)$ in $\zeta(C_3) = -(s+1)+s = -2\zeta(C_1)$. Očitno podprostori $W_s(2)$, $s \in \mathbb{Z}_5$, porodijo ekvivalentne krove grafa X. Naj bo zdaj ζ regularna napetostna funkcija, porojena iz $W_s(3)$, kjer je $s \neq 3 \in \mathbb{Z}_p$. Nadalje, naj ζ' označuje regularno napetostno funkcijo, porojeno iz $W_\infty(3)$. Potem imamo

$$\begin{aligned} \zeta(C_1) &= 4(s+1)+3s = 2s-1, & \zeta'(C_1) &= 2,\\ \zeta(C_2) &= -4(s+1)-3s = -\zeta(C_1), & \zeta'(C_2) &= -2 = -\zeta'(C_1),\\ \zeta(C_3) &= -2(s+1)+s = -3\zeta(C_1), & \zeta'(C_3) &= -1 = -3\zeta'(C_1). \end{aligned}$$

Očitno je rang razširjene matrike

$$\left[\begin{array}{c|c} \zeta(C_1)^t & \zeta'(C_1)^t \\ \zeta(C_2)^t & \zeta'(C_2)^t \\ \zeta(C_3)^t & \zeta'(C_3)^t \end{array}\right]$$

enak 1, zato sta restrikciji $\bar{\zeta}$ in $\bar{\zeta}'$ ekvivalentni. Za predstavnike krovov grafa X si izberimo tiste, ki so porojeni iz $L_A(1)$, $W_\infty(2)$ in $W_\infty(3)$. Bralec lahko preveri, da slednji porodijo paroma neekvivalentne restrikcije.

Poiščimo sedaj dvorazsežne podprostore. Potrebovali bomo naslednjo lemo.

Lema 7.4.2: Naj bosta U in U' podprostora v $\mathbb{Z}_p^{n\times 1} \cong H_1(\widehat{X}(\Omega), \mathbb{Z}_p)$, ki porodita povezani ekvivalentni restrikciji krova grafa X, ter W in W' podprostora v $\mathbb{Z}_p^{n\times 1}$, ki prav tako porodita povezana ekvivalentna krova grafa X. Predpostavimo, da velja $U \cap W = \{0\} = U' \cap W'$ in da premi vsoti $U \oplus W$ in $U' \oplus W'$ v $\mathbb{Z}_p^{n\times 1}$ porodita povezana krova grafa X. Potem ti vsoti porodita ekvivalentna krova grafa X.

Dokaz: Naj ima graf X rang r in naj bo $\{[C_1], [C_2], \dots, [C_r], [C_{r+1}], \dots, [C_n]\}$ takšna urejena baza prostora $H_1(\widehat{X}(\Omega), \mathbb{Z}_p)$, da je $\{[C_1], [C_2], \dots, [C_r]\}$ urejena baza prostora $H_1(X, \mathbb{Z}_p)$. Naj bodo $M_U \in \mathbb{Z}_p^{n\times d}$, $M'_U \in \mathbb{Z}_p^{n\times d}$, $M_W \in \mathbb{Z}_p^{n\times k}$, $M'_W \in \mathbb{Z}_p^{n\times k}$ matrike, katerih stolpci so bazni vektorji prostorov U, U', W oziroma W', zaporedoma. Označimo z $\bar{M}_U \in \mathbb{Z}_p^{r\times d}$, $\bar{M}_{U'} \in \mathbb{Z}_p^{r\times d}$, $\bar{M}_W \in \mathbb{Z}_p^{r\times k}$ in $\bar{M}_{W'} \in \mathbb{Z}_p^{r\times k}$ še podmatrike, ki so sestavljene iz prvih r vrstic matrik M_U, $M_{U'}$, M_W oziroma $M_{W'}$, zaporedoma. Ker podprostori U, U', W, W' porodijo povezane krove grafa X, imata matriki $\bar{M}_U$ in $\bar{M}_{U'}$ rang d, medtem ko imata matriki $\bar{M}_W$ in $\bar{M}_{W'}$ rang k. Poleg tega ima razširjena matrika

$$\left[\bar{M}_U \;\middle|\; \bar{M}_{U'}\right] \tag{7.5}$$

tudi rang d, saj U in U' porodita ekvivalentna krova. Podobno ima razširjena matrika

$$\left[\bar{M}_W \;\middle|\; \bar{M}_{W'}\right] \tag{7.6}$$

rang k, saj W in W' porodita ekvivalentna krova.

Naj bosta $M_{U\oplus W}$ in $M_{U'\oplus W'}$ matriki, katerih stolpci so bazni vektorji prostorov $U \oplus W$ oziroma $U' \oplus W'$, zaporedoma. Ker velja $U \cap W = \{0\} = U' \cap W'$, dobimo

$$M_{U\oplus W} = \begin{bmatrix} M_U & M_W \end{bmatrix} \in \mathbb{Z}_p^{n\times(d+k)} \text{ in } M_{U'\oplus W'} = \begin{bmatrix} M'_U & M_{W'} \end{bmatrix} \in \mathbb{Z}_p^{n\times(d+k)}.$$

Označimo s $\bar{M}_{U\oplus W} \in \mathbb{Z}_p^{r\times(d+k)}$ in $\bar{M}_{U'\oplus W'} \in \mathbb{Z}_p^{r\times(d+k)}$ podmatriki, ki sta sestavljeni iz prvih r vrstic matrik $M_{U\oplus W}$ in $M_{U'\oplus W'}$, zaporedoma. Potem velja še

$$\bar{M}_{U\oplus W} = \begin{bmatrix} \bar{M}_U & \bar{M}_W \end{bmatrix} \text{ in } \bar{M}_{U'\oplus W'} = \begin{bmatrix} \bar{M}'_U & \bar{M}_{W'} \end{bmatrix}.$$

Ker podprostora $U \oplus W$ in $U' \oplus W'$ porodita povezana krova grafa X, imata obe matriki $\bar{M}_{U\oplus W}$ ter $\bar{M}_{U'\oplus W'}$ rang $d + k$. Toda razširjeni matriki (7.5) in (7.6) imata rang d oziroma k, zato mora imeti tudi razširjena matrika

$$\left[\bar{M}_{U\oplus W} \;\middle|\; \bar{M}_{U'\oplus W'}\right]$$

rang $d + k$. Torej $U \oplus W$ in $U' \oplus W'$ porodita ekvivalentna krova grafa X. □

Najprej opozorimo, da dvorazsežna podprostora $L_A(i)$ in $L_A(-i)$ porodita nepovezana krova grafa X, ker lahko vsakega zapišemo kot premo vsoto dveh enorazsežnih podprostorov, od katerih eden porodi nepovezan krov grafa X. Izmed ostalih dvorazsežnih A-invariantnih podprostorov je po Lemi 7.4.2 dovolj preveriti naslednje preme vsote:

$$L_A(1) \oplus W_0(i), L_A(1) \oplus W_0(-i), W_0(i) \oplus W_0(-i).$$

Bralec lahko preveri, da vsi porodijo povezane in paroma neekvivalentne restrikcije na graf X.

Kar zadeva trirazsežne A-invariantne podprostore, je podobno kot zgoraj dovolj poiskati enega, ki porodi povezan krov grafa X. Ni se težko prepričati, da recimo podprostor $L_A(1) \oplus W_0(i) \oplus W_0(-i)$ zadošča pogoju za povezanost.

Primer $p = 2$.

V tem primeru reprezentacija grupe $\langle A\rangle$ ni popolnoma razcepna. Najprej moramo izračunati jordansko bazo matrike A. Pripadajoča jordanska oblika ima dve elementarni jordanski celici, eno razsežnosti 4 in eno razsežnosti 2. Po kratkem računu dobimo

naslednjo jordansko bazo

$$\begin{aligned} v_1 &= (1,1,1,1,0,0)^t, \\ b_1 &= (0,1,0,1,0,0)^t, \\ b_3 &= (0,0,1,1,0,0)^t, \\ b_4 &= (0,0,0,1,0,0)^t, \\ v_2 &= (0,0,0,0,1,1)^t, \\ b_2 &= (0,0,0,0,1,0)^t, \end{aligned}$$

kjer sta v_1 in v_2 lastna vektorja, štirirazsežni ciklični podprostor je napet na vektorje v_1, b_1, b_3, b_4, medtem ko je dvorazsežni napet na vektorja v_2, b_2.

Obstajajo natanko trije enorazsežni A-invariantni podprostori, vsi vsebovani v dvorazsežnem lastnem podprostoru $L_A(1)$, in sicer $W_\infty(1) = \langle v_1 \rangle$, $W_0(1) = \langle v_2 \rangle$ ter $W_1(1) = \langle (1,1,1,1,1,1)^t \rangle$. Vendar pa le zadnja dva porodita povezana krova grafa X. Poleg tega oba porodita ekvivalentna krova grafa X. Krovu, ki ga dobimo, rečemo *kanonični dvojni* krov.

Vseh dvorazsežnih A-invariantnih podprostorov je sedem. Eden je lastni podprostor $L_A(1) = \langle v_1, v_2 \rangle$, ostalih šest je porojenih iz vektorjev $u \in \mathsf{Ker}(A-I)^2 \setminus L_A(1)$. Takšen dvorazsežen podprostor sestoji iz vektorjev $0, u, Au, u + Au$. Očitno je $Au \neq u$ (ker u ni lastni vektor) in $Au \in \mathsf{Ker}(A-I)^2 \setminus L_A(1)$ (ker $A^2u = Au$ implicira $Au = u$). Zato vektorji v $\mathsf{Ker}(A-I)^2 \setminus L_A(1)$ v istem dvorazsežnem podprostoru nastopajo v parih. Ker množica $\mathsf{Ker}(A-I)^2 \setminus L_A(1)$ vsebuje natanko dvanajst netrivialnih vektorjev, je takšnih podprostorov natanko šest. Le-te lahko predstavimo kot $\langle v_1, b_1 \rangle$, $\langle v_1, u_1 \rangle$, $\langle v_2, b_2 \rangle$, $\langle v_2, u_2 \rangle$, $\langle v_1 + v_2, u_3 \rangle$, $\langle v_1 + v_2, u_4 \rangle$, kjer so

$$\begin{aligned} u_1 &= (0,1,0,1,1,1)^t, \\ u_1 &= (1,1,1,1,1,0)^t, \\ u_3 &= (1,0,1,0,0,1)^t, \\ u_4 &= (1,0,1,0,1,0)^t. \end{aligned}$$

Bralec lahko preveri, da tisti dvorazsežni prostori, ki porodijo povezane restrikcije na graf X, hkrati porodijo ekvivalentne restrikcije. Kot predstavnika vzemimo recimo $\langle v_2, b_2 \rangle$.

Poglejmo si sedaj trirazsežne A-invariantne podprostore. Zopet je dovolj poiskati enega takšnega, ki porodi povezan krov grafa X. Toda bralec se lahko sam prepriča, da v tem primeru ne obstaja takšen podprostor, ki bi porodil povezan krov grafa X. Na koncu omenimo le še, da je vseh trirazsežnih A-invariantnih podprostorov natanko sedem. Trije takšni so vsebovani v $\mathsf{Ker}(A-I)^2$ in sicer $\langle (A-I)^{-1}(v_1)\rangle$, $\langle (A-I)^{-1}(v_2)\rangle$ ter $\langle (A-I)^{-1}(v_1+v_2)\rangle$ (vsak izmed njih vsebuje $L_A(1)$). Pripadajoče baze so $\{v_1, v_2, b_1\}$, $\{v_1, v_2, b_2\}$ oziroma $\{v_1, v_2, u_4\}$. Ostali štirje so ciklični podprostori jordanskih verig dolžine tri (obstaja natanko 16 verig in A deluje polregularno na množici vektorjev v $\mathsf{Ker}(A-I)^3 \setminus \mathsf{Ker}(A-I)^2$ s štirimi orbitami velikosti 4). Pripadajoče baze so $\{v_1, b_1, b_3\}$, $\{v_1, b_1, u_5\}$, $\{v_1, u_6, u_7\}$, $\{v_1, u_6, u_8\}$, kjer so

$$\begin{aligned} u_5 &= (0,0,1,1,1,1)^t, \\ u_6 &= (1,0,1,0,1,1)^t, \\ u_7 &= (1,0,0,1,0,1)^t, \\ u_8 &= (1,0,0,1,1,0)^t. \end{aligned}$$

Opomba 7.4.3: Poglejmo si avtomorfizem $h = (12)$ grafa X. Očitno g in h generirata grupo $\mathsf{Aut}(X)$ avtomorfizmov grafa X. Naj bo $(h^*)^\#$ linearna transformacija prostora $H_1(\widehat{X}(\Omega); \mathbb{Z}_p)$, inducirana z delovanjem avtomorfizma h^* na $H_1(\widehat{X}(\Omega); \mathbb{Z}_p)$. Označimo z $M_{h^*} \in \mathbb{Z}_p^{6,6}$ matrično upodobitev transformacije $(h^*)^\#$ glede na bazo B_{T^*}. Kratek račun nam da

$$M_{h^*}^t = \begin{bmatrix} -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Ni se težko prepričati, da je med podprostori v Tabeli 7.1 le $W_1(1)$ tudi $M_{h^*}^t$-invarianten. Torej je kanonični dvojni krov grafa X edini krov, vzdolž katerega se grupa $\mathsf{Aut}(X)$ dvigne kot prerezna razcepna razširitev nad Ω.

Tabela 7.1

Paroma neekvivalentne regularne napetostne funkcije grafa K_4, ki porodijo povezane elementarno abelske regularne krovne projekcije, vzdolž katerih se ciklična grupa $\langle g \rangle$ avtomorfizmov grafa K_4 dvigne kot prerezna razcepna razširitev nad $\Omega = V(X)$.

Inv. podpr.	$\zeta(a_1)$	$\zeta(a_2)$	$\zeta(a_3)$	$\zeta(a_4)$	$\zeta(a_5)$	$\zeta(a_6)$	Pogoj
$W_1(1)$	$\begin{bmatrix}1\end{bmatrix}$	$\begin{bmatrix}1\end{bmatrix}$	$\begin{bmatrix}1\end{bmatrix}$	$\begin{bmatrix}1\end{bmatrix}$	$\begin{bmatrix}1\end{bmatrix}$	$\begin{bmatrix}1\end{bmatrix}$	$p = 2$
$\langle v_1 \rangle$	$\begin{bmatrix}1\end{bmatrix}$	$\begin{bmatrix}1\end{bmatrix}$	$\begin{bmatrix}1\end{bmatrix}$	$\begin{bmatrix}1\end{bmatrix}$	$\begin{bmatrix}0\end{bmatrix}$	$\begin{bmatrix}0\end{bmatrix}$	$p \neq 2$
$\langle v_i \rangle$	$\begin{bmatrix}1\end{bmatrix}$	$\begin{bmatrix}i\end{bmatrix}$	$\begin{bmatrix}-1\end{bmatrix}$	$\begin{bmatrix}-i\end{bmatrix}$	$\begin{bmatrix}0\end{bmatrix}$	$\begin{bmatrix}0\end{bmatrix}$	$p \equiv 1 \pmod 4$, $i^2 = -1$
$\langle v_{-i} \rangle$	$\begin{bmatrix}1\end{bmatrix}$	$\begin{bmatrix}-i\end{bmatrix}$	$\begin{bmatrix}-1\end{bmatrix}$	$\begin{bmatrix}i\end{bmatrix}$	$\begin{bmatrix}0\end{bmatrix}$	$\begin{bmatrix}0\end{bmatrix}$	$p \equiv 1 \pmod 4$, $i^2 = -1$
$\langle v_2, b_2 \rangle$	$\begin{bmatrix}0\\0\end{bmatrix}$	$\begin{bmatrix}0\\0\end{bmatrix}$	$\begin{bmatrix}0\\0\end{bmatrix}$	$\begin{bmatrix}0\\0\end{bmatrix}$	$\begin{bmatrix}1\\1\end{bmatrix}$	$\begin{bmatrix}1\\0\end{bmatrix}$	$p = 2$
$W_{1,1,0,0}$	$\begin{bmatrix}1\\1\end{bmatrix}$	$\begin{bmatrix}1\\-1\end{bmatrix}$	$\begin{bmatrix}-1\\-1\end{bmatrix}$	$\begin{bmatrix}-1\\1\end{bmatrix}$	$\begin{bmatrix}0\\0\end{bmatrix}$	$\begin{bmatrix}0\\0\end{bmatrix}$	$p \equiv 3 \pmod 4$
$\langle v_1, v_i \rangle$	$\begin{bmatrix}1\\1\end{bmatrix}$	$\begin{bmatrix}1\\i\end{bmatrix}$	$\begin{bmatrix}1\\-1\end{bmatrix}$	$\begin{bmatrix}1\\-i\end{bmatrix}$	$\begin{bmatrix}0\\0\end{bmatrix}$	$\begin{bmatrix}0\\0\end{bmatrix}$	$p \equiv 1 \pmod 4$, $i^2 = -1$
$\langle v_1, v_{-i} \rangle$	$\begin{bmatrix}1\\1\end{bmatrix}$	$\begin{bmatrix}1\\-i\end{bmatrix}$	$\begin{bmatrix}1\\-1\end{bmatrix}$	$\begin{bmatrix}1\\i\end{bmatrix}$	$\begin{bmatrix}0\\0\end{bmatrix}$	$\begin{bmatrix}0\\0\end{bmatrix}$	$p \equiv 1 \pmod 4$, $i^2 = -1$
$\langle v_i, v_{-i} \rangle$	$\begin{bmatrix}1\\1\end{bmatrix}$	$\begin{bmatrix}i\\-i\end{bmatrix}$	$\begin{bmatrix}-1\\-1\end{bmatrix}$	$\begin{bmatrix}-i\\i\end{bmatrix}$	$\begin{bmatrix}0\\0\end{bmatrix}$	$\begin{bmatrix}0\\0\end{bmatrix}$	$p \equiv 1 \pmod 4$, $i^2 = -1$
$\langle v_1, W_{1,1,0,0} \rangle$	$\begin{bmatrix}1\\1\\1\end{bmatrix}$	$\begin{bmatrix}1\\1\\-1\end{bmatrix}$	$\begin{bmatrix}1\\-1\\-1\end{bmatrix}$	$\begin{bmatrix}1\\-1\\1\end{bmatrix}$	$\begin{bmatrix}0\\0\\0\end{bmatrix}$	$\begin{bmatrix}0\\0\\0\end{bmatrix}$	$p \equiv 3 \pmod 4$
$\langle v_1, v_i, v_{-i} \rangle$	$\begin{bmatrix}1\\1\\1\end{bmatrix}$	$\begin{bmatrix}1\\i\\-i\end{bmatrix}$	$\begin{bmatrix}1\\-1\\-1\end{bmatrix}$	$\begin{bmatrix}1\\-i\\i\end{bmatrix}$	$\begin{bmatrix}0\\0\\0\end{bmatrix}$	$\begin{bmatrix}0\\0\\0\end{bmatrix}$	$p \equiv 1 \pmod 4$, $i^2 = -1$

Zaključek

8

Krovne tehnike igrajo pomembno vlogo pri študiju strukturnih lastnosti kombinatoričnih objektov. Posebej so se izkazale za močno orodje pri klasifikaciji oziroma konstrukciji neskončnih družin grafov s predpisanimi simetrijskimi lastnostmi ter generiranju katalogov določenih grafov do razumne velikosti. Kombinatorične tehnike, ki so bile razvite v ta namen, slonijo predvsem na konceptu dviga avtomorfizmov vzdolž krovnih projekcij.

V disertaciji so razviti algoritmi, ki podajo odgovore na nekatera naravna vprašanja v zvezi z dvigi avtomorfizmov. Najprej je predstavljen učinkovit algoritem za testiranje, kdaj se avtomorfizem dvigne vzdolž kombinatorično podane krovne projekcije. Problem interpretiramo v jeziku teorije grafov: prevedemo ga na testiranje barvnega izomorfizma permutacijskih grafov in predstavimo algoritme za njegovo reševanje. Posebej obravnavamo regularne napetosti, kjer kot izhodišče uporabimo standardni rezultat iz računske teorije grup.

Dalje, razviti so algoritmi za analizo dvignjene grupe vzdolž regularne krovne projekcije. Opisan je algoritem, ki prek regularnih napetosti poišče prezentacijo dvignjene grupe. Izkoristimo dejstvo, da je dvignjena grupa razširitev grupe krovnih transformacij po grupi, ki jo dvigujemo, in uporabimo splošne metode za iskanje prezentacije razširitve.

Razvit je algoritem za testiranje razcepnosti dvignjene grupe kot razširitve grupe krovnih transformacij. Z uporabo standardnega rezultata iz računske teorije grup se v primeru abelskih oziroma elementarno abelskih regularnih krovov problem prevede na reševanje linearnih sistemov enačb nad celimi števili oziroma nad poljem praštevilske karakteristike. Slednjo idejo nadgradimo v primeru, ko gre za rešljive regularne krove. Dokažemo namreč, da lahko vsako rešljivo regularno krovno projekcijo najprej dekomponiramo na zaporedje elementarno abelskih regularnih projekcij, nato pa rekurzivno uporabimo elementarno abelsko verzijo vzdolž zaporedja.

Razvit je algoritem za testiranje prerezne razcepnosti razširitve dvignjene grupe. Problem se prevede na modifikacijo algoritma za računanje orbite, ki se v primeru abelskih oziroma elementarno abelskih regularnih krovov naprej prevede na reševanje sistema linearnih enačb. Da so algoritmi učinkoviti, so vsi zasnovani tako, da se izognejo eksplicitni konstrukciji tako krovnega grafa kot dvignjene grupe.

Dalje, vpeljane so metode za konstrukcijo krovnih projekcij, vzdolž katerih se dana podgrupa avtomorfizmov dvigne. Najprej so obravnavane permutacijske napetosti, tako za neregulane kot tudi regularne krove. Osnovna ideja temelji na konstrukci-

ji univerzalne grupe in iskanju njenih podgrup, ki porodijo iskane krove. Poleg tega obravnavamo regularne napetosti v primeru rešljivih regularnih krovov. Izkoristimo dejstvo, da lahko vsako rešljivo regularno krovno projekcijo dobimo kot razširitev elementarno abelskih krovnih projekcij, kjer so učinkovite metode že znane. Posebej je podana še metoda za konstrukcijo regularnih krovnih projekcij, vzdolž katerih se dana podgrupa avtomorfizmov dvigne kot prerezna razcepna razširitev. Dokažemo, da se problem prevede na splošni primer konstrukcije vseh dopustnih regularnih krovnih projekcij.

8.1 Razprava in nadaljnje delo

Motivacija za nadaljnje delo se zlasti navezuje na teoretičnih analizo spodnjih mej časovne in prostorske zahtevnosti algoritmov za testiranje, ali se avtomorfizem dvigne. Prav tako bi se bilo zanimivo posvetiti istemu problemu v primeru algoritmov za testiranje, ali je dvignjena grupa (prerezna) razcepna razširitev.

Problem I. Poišči spodnje meje časovne in prostorske zahtevnosti algoritmov za testiranje dviga avtomorfizmov.

Poleg tega bi veljalo algoritem za testiranje prerezne razcepnosti dvignjene grupe nadgraditi v primeru rešljivih regularnih krovov – podobno kot je to narejeno za testiranje razcepnosti razširitve.

Problem II. Razvij algoritem za testiranje, kdaj je dvignjena grupa $\tilde{G}$ prerezna razcepna razširitev rešljive grupe krovnih transformacij $CT(\wp)$ po grupi G.

Ne nazadnje, algoritma za testiranje razcepne oziroma prerezne razcepnosti dvignjene grupe bi kazalo razširiti tako, da bi bila uporabna za testiranje vzdolž poljubne regularne krovne projekcije. V posebnem to pomeni, da je problem potrebno rešiti v primeru, ko grupa krovnih transformacij ne vsebuje elementarno abelske podgrupe edinke.

Problem III. Naj bo Γ končna napetostna grupa, ki ne vsebuje elementarno abelske podgrupe edinke. Dalje, naj bo $\zeta\colon X \to \Gamma$ povezana regularna napetostna funkcija na baznem grafu X in naj se dana podgrupa G avtomorfizmov grafa X dvigne vzdolž izpeljane krovne projekcije $\wp_\zeta\colon X \times_\zeta \Gamma \to X$. Razvij algoritem za testiranje, ali je dvignjena grupa $\tilde{G}$ (prerezna) razcepna razširitev grupe krovnih transformacij $CT(\wp_\zeta)$ po grupi G.

Paket algoritmov v Magmi

A

Čeprav smo se v disertaciji zaradi enostavnosti omejili na enostavne grafe, pa vse implementirane funkcije omogočajo delo s posplošenimi grafi; to so grafi, ki dopuščajo tako večkratne povezave, zanke, kot tudi polpovezave. Formalno je *posplošeni graf* urejena četvorka $X = (D, V; \mathrm{ini}, ^{-1})$, kjer sta D in V disjunktni množici *praporjev* in *vozlišč*,

$$\mathrm{ini} : D \to V, x \to \mathrm{ini}(x)$$

funkcija, ki vsakemu praporju predpiše svojo *začetno* vozlišče, in

$$^{-1} : D \to D, x \to x^{-1}$$

involucija, ki vsak prapor preslika v svoj *nasprotni* prapor. *Končno* vozlišče praporja x je začetno vozlišče praporja x^{-1}. *Povezave* so orbite $\{x, x^{-1}\}$ involucije $^{-1}$. Povezavi e rečemo *polpovezava*, če velja $x^{-1} = x$, *zanka*, če je $x^{-1} \neq x$ ter $\mathrm{ini}(x^{-1}) = \mathrm{ini}(x)$, in *običajna povezava* ali *vez* sicer.

Magma sicer omogoča delo z multigrafi (večkratne povezave in zanke), ni pa implementiranih polpovezav. Zato smo najprej odpravili to pomanjkljivost in podatkovno strukturo `MultiGraph` nadgradili z dodatno informacijo, ki omogoča, da ločimo med zankami in polpovezavami.

A.1 Funkcije za delo s krovnimi grafi

Paket v Magmi vsebuje tako osnovne funkcije kot tudi specializirane funkcije, ki se navezujejo na problem dviga avtomorfizmov. Implementirali smo naslednje funkcije za delo s krovnimi grafi nasploh:

`VoltageSpace`: zgradi (permutacijsko ali regularno) napetostno funkcijo na baznem grafu.

`LocalVoltageGroup`: izračuna lokalno napetostno grupo v danem vozlišču.

`IsLocallyTransitive`: testira, ali je izpeljani krovni graf povezan.

`TReduced`: izračuna reducirano napetostno funkcijo glede na dano vpeto drevo s korenom v danem vozlišču.

`Reduced`: izračuna reducirano napetostno funkcijo s pregledom grafa v širino iz danega vozlišča.

`DerivedCover`: konstruira izpeljani krovni graf.

Izmed algoritmov, ki se nanašajo na študij dviga avtomorfizmov, pa smo implementirali naslednje:

`HasLift`: testira, ali se dani avtomorfizem baznega grafa dvigne vzdolž dane krovne projekcije.

`Lift`: konstruira dvig, v primeru, da obstaja.

`GroupOfCoveringTransformations`: konstruira grupo krovnih transformacij.

`IsSplitExtension` : testira, ali se dana grupa dvigne vzdolž rešljive regularne krovne projekcije kot razcepna razširitev.

`IsStrongSplitExtension` : testira, ali se dana grupa dvigne vzdolž abelske regularne krovne projekcije kot prerezna razcepna razširitev.

A.2 Dostopnost algoritmov

Zadnja verzija opisanih algoritmov za programsko okolje MAGMA je dosegljiva na sletni strani `http://osebje.famnit.upr.si/~rok.pozar`. V okviru nadaljnjega dela nameravamo v paket vključiti tudi algoritme za generiranje dopustnih krovnih projekcij.

LITERATURA

[1] T. Sunada. Crystals that nature might miss creating. *Notices of the AMS*, 38:208–215, 2008.

[2] T. Sunada. Lecture on topological crystallography. *Japan. J. Math.*, 7:1–39, 2012.

[3] C. A. Kelley and J. L. Walker. Ldpc codes from voltage graphs. In *Proceedings of the 2008 IEEE International Symposium on Information Theory*, IEEE Information Theory Society, pages 792–796, 2008.

[4] R. Koetter, W-C W. Li, P. O. Vontobel, and J. L. Walker. Characterizations of pseudo codewords of ldpc codes. *Adv. Math.*, 217:205–229, 2007.

[5] D. Angluin. Local and global properties in networks of processors. In *Proceedings of the 12th ACM Symposium on Theory of Computing*, pages 82–93, 1980.

[6] H. L. Bodlaender. The classification of coverings of processor networks. *Journal of Parallel Distributed Computing*, 6:166–182, 1989.

[7] J. Chen, L. Liu, W. Jia, and S. Chen. An intuitive and effective new representation for interconnection network structures. In *Proceedings of the 8th Annual International Symposium on Algorithms and Computation*, Lecture Notes in Computer Science 1969, pages 350–361, 2000.

[8] J. L. Gross and J. Chen. Algebraic specification of interconnection network relationships by permutation voltage graph mappings. *Math. Systems Theory*, 29(5): 451–470, 1996.

[9] W. Floyd, L. Kay, and M. Shapino. Some elementary properties of sir networks, or, can i get sick because you got vaccinated? *Bull. Math. Biol*, 70(3):713–727, 2008.

[10] W. Floyd, L. Kay, and M. Shapino. A covering-graph approach to epidemics on sis and sis-like networks. *Bull. Math. Biol*, 74(1):175–189, 2012.

[11] J. L. Gross and T. W. Tucker. *Topological Graph Theory*. Wiley - Interscience, New York, 1978.

[12] A. T. White. *Graphs, Groups, and Surfaces*. North-Holland, Amsterdam, 1984.

[13] D. Archdeacon, P. Gvozdjak, and J. Širáň. Constructing and forbidding automorphisms in lifted maps. *Math. Slovaca*, 47:113–129, 1997.

[14] A. Malnič. Group actions, coverings and lifts of automorphisms. *Discrete Math.*, 182:203–218, 1998.

[15] A. Malnič, R. Nedela, and M. Škoviera. Lifting graph automorphisms by voltage assignments. *European J. Combin.*, 21:927–947, 2000.

[16] J. L. Gross and S. R. Alpert. The topological theory of current graphs. *J. Combin. Theory Ser. B*, 17:218–233, 1974.

[17] D. Archdeacon, R. B. Richter, J. Širáň, and M. Škoviera. Branched coverings of maps and lifts of map homomorphisms. *Australas. J. Combin.*, 9:109–121, 1994.

[18] M. D. E. Conder and P. Dobcsányi. Trivalent symmetric graphs on up to 768 vertices. *J. Combin. Math. Combin. Comput.*, 40:41–63, 2002.

[19] M. D. E. Conder, A. Malnič, D. Marušič, and P. Potočnik. Trivalent symmetric graphs on up to 768 vertices. *J. Algebraic Combin.*, 23:255–294, 2006.

[20] D. Ž. Djoković. Automorphisms of graphs and coverings. *J. Combin. Theory Ser. B*, 16:243–247, 1974.

[21] Y. Q. Feng and Y. H. Kwak. Classifying cubic symmetric graphs of order $10p$ or $10p^2$. *Science China Ser. A: Math.*, 49:300–319, 2006.

[22] M. Hofmeister. Isomorphisms and automorphisms of graph coverings. *Discrete Math.*, 98:175–183, 1991.

[23] M. Hofmeister. Graph covering projections arising from finite vector spaces over finite fields. *Discrete Math.*, 143:87–97, 1995.

[24] I. Kovács, A. Malnič, D. Marušič, and Š. Miklavič. One-matching bi-cayley graphs over abelian groups. *European J. Combin.*, 40:602–616, 2009.

[25] J. Kratochvíl, A. Proskurowski, and J. A. Telle. Covering regular graphs. *J. Combin. Theory Ser B*, 71:1–16, 1997.

[26] J. Kratochvíl, A. Proskurowski, and J. A. Telle. Complexity of graph covering problems. *Nordic. J. Comput.*, 5:173–195, 1998.

[27] A. Malnič and D. Marušič. Constructing 4-valent 1/2-transitive graphs with nonsolvable automorphism group. *J. Combin. Theory Ser. B*, 75:46–55, 1999.

[28] P. Potočnik. Edge-colourings of cubic graphs admitting a solvable vertex-transitive group of automorphisms. *J. Combin. Theory Ser. B*, 91:289–300, 2004.

[29] C. Q. Wang and T. S. Chen. Semisymmetric cubic graphs as regular covers of $k_{3,3}$. *Acta Math. Sin. (Engl. Ser.)*, 24:405–416, 2008.

[30] J. Fiala, J. Kratochvíl, and A. Pór. On the computational complexity of partial covers of theta graphs. *Discrete Applied Mathematics*, 156:1143–1149, 2008.

[31] J. Fiala, D. Paulusma, and J. A. Telle. Locally constrained graph homomorphisms and equitable partitions. *European journal of combinatorics*, 29(4):850–880, 2008.

[32] J. Širáň. Coverings of graphs and maps, orthogonality, and eigenvectors. *Australas. J. Combin.*, 14:57–72, 2001.

[33] M. Škoviera. A contribution to the theory of voltage graphs. *Discrete Math.*, 61:281–292, 1986.

[34] S. Rees and L. H. Soicher. An algorithmic approach to fundamental groups and covers of combinatorial cell complexes. *J. Symbolic Comput.*, 29:59–77, 2000.

[35] N. L. Biggs. *Algebraic Graph Theory*. Cambridge Univ. Press, Cambridge, 1974.

[36] Y. Q. Feng, A. Malnič, D. Marušič, and K. Kutnar. On 2-fold covers of graphs. *J. Combin. Theory Ser. B*, 98: 324–341, 2008.

[37] A. Malnič. Action graphs and coverings. *Discrete Math.*, 244:299–322, 2002.

[38] S. F. Du, J. H. Kwak, and M. Y. Xu. Lifting of automorphisms on the elementary abelian regular coverings. *Lin. Alg. Appl.*, 373:101–119, 2003.

[39] A. Malnič, D. Marušič, and P. Potočnik. Elementary abelian covers of graphs. *J. Alg. Combin.*, 20:71–96, 2004.

[40] W. Bosma, J. Cannon, and C. Playoust. The MAGMA algebra system i: The user language. *J. Symbolic Comput.*, 24:235–265, 1997.

[41] A. Malnič and R. Požar. On the split structure of lifted groups. Poslano v objavo.

[42] A. Malnič and R. Požar. On the split liftings with sectional complements. Poslano v objavo.

[43] R. Požar. Sectional split extensions arising from lifts of groups. *Ars Math. Contemp.*, 6:393–408, 2013.

[44] R. Požar. Some computational aspects of solvable regular covers of graphs. Poslano v objavo.

[45] J. D. Dixon and B. Mortimer. *Permutation Groups*, volume GTM 163. Springer-Verlag, New York, 1996.

[46] W. R. Scott. *Group theory*. Dover Publications, New York, 1987.

[47] A. V. Aho, J. E. Hopcroft, and J. D. Ullman. *The Design and Analysis of Computer Algorithms*. Addison-Wesely, Reading (Mass.), 1974.

[48] M. V. Horoševskiĭ. On automorphisms of finite groups. *Math. USSR Sb.*, 22:584–594, 1974.

[49] N. Jacobson. *Lectures in Abstract Algebra, II. Linear Algebra*. Springer, New York, 1953.

[50] D. Holt, B. Eick, and E. A. O'Brien. *Handbook of Computational Group Theory*. Chapman and Hall/CRC, Boca Raton London New York Washington D.C., 2005.

[51] C. M. Hoffmann. *Group-Theoretic Algorithms and Graph Isomorphism*, volume 136 of *Lecture Notes in Computer Science*. Springer, 1982.

[52] M. A. Sridhar. A fast algorithm for testing isomorphism of permutation networks. *IEEE Trans. Computers (TC)*, 38(6):903–909, 1989.

[53] J. Šiagiová. Composition of regular coverings of graphs and voltage assignments. *Australas. J. Combin.*, 28: 131–136, 2003.

[54] D. J. Abadi. Covers in imprimitevely symmetric graphs. University of Western Australia, 1997. "Honours dissertation".

[55] F. Celler, J. Neubüser, and C. R. B. Wright. Some remarks on the computation of complements and normalizers in solvable groups. *Acta Applicandae Mathematicae*, 21:57–76, 1990.

[56] A. Malnič, D. Marušič, and P. Potočnik. On cubic graphs admitting an edge-transitive solvable group. *J. Alg. Combin.*, 20:99–113, 2004.

[57] B. Kuzman. Arc-transitive elementary abelian covers of the complete graph k_5. *Linear Algebra Appl.*, 433: 1909–1921, 2010.

[58] A. Malnič, D. Marušič, Š. Miklavič, and P. Potočnik. Semisymmetric elementary abelian covers of the möbius-kantor graph. *Discrete Math.*, 307:2156–2175, 2007.

[59] Y. Q. Feng and Y. H. Kwak. s-regular cubic graphs as coverings of the complete bipartite graph $k_{3,3}$. *J. Graph Theory*, 45:101–112, 2004.

[60] A. Malnič and P. Potočnik. Invariant subspaces, duality, and covers of the petersen graph. *European J. Combin.*, 27:971–989, 2006.

[61] J. M. Oh. A classification of cubic s-regular graphs of order $14p$. *Discrete Math.*, 309:2721–2726, 2009.

[62] H. Wielandt. *Finite Permutation Groups*. Academic Press, New York, 1964.

STVARNO KAZALO

SEZNAM SIMBOLOV

A^G	normalno zaprtje podmnožice A v grupi G	11
$A^+(X)$	orientacija grafa X	12
G/N	kvocientna ali faktorska grupa po edinki N	11
G_ω	stabilizator elementa w	16
$H_1(X)$	prva homološka grupa grafa X	14
Hx	desni odsek po podgrupi H	11
$H\|G$	množica desnih odsekov po podgrupi H v grupi G	16
$N(u)$	okolica vozlišča u	12
$N \rtimes_\theta K$	poldirektni produkt grupe N po grupi K glede na θ	12
$N_H(G)$	normalizator podgrupe H v grupi G	16
$V(X), E(X), A(X)$	množica vozlišč, povezav in lokov grafa X	12
$X \times_\zeta \Omega$	izpeljani graf	19
$[G, G]$	komutatorska podgrupa v grupi G	11
$[G : H]$	indeks podgrupe H v grupi G	11
$[W]$	homotopski razred sprehoda W	14
$[\,n\,]$	množica naravnih števil $\{1, 2, \ldots, n\}$	15
$\mathsf{Aut}(X)$	grupa avtomorfizmov grafa X	13
$\mathscr{O}(f)$	red velikosti funkcije f	27
$CT(\varphi)$	grupa krovnih transformacij	22
$Fix(G)$	množica negibnih točk delovanja grupe G	85
$\mathrm{Hol}(H)$	holomorf grupe H	12
$\mathsf{Ker}(\phi)$	jedro homomorfizma ϕ	11
Loc_u	lokalna napetostna funkcija v vozlišču u	20

$\mathrm{Sec}_\Omega(\overline{G})$	množica vseh prerezov nad Ω, invariantnih na delovanje $\overline{G}$	85
$\mathrm{Sym}_{\mathrm{L}}(\Omega), \mathrm{Sym}_{\mathrm{R}}(\Omega)$	leva in desna simetrična grupa	14
$\mathbb{Z}$	grupa celih števil	24
$\mathbb{Z}_p$	grupa celoštevilskih ostankov pri deljenju s p	24
$\mathbb{Z}_p^r$	p-elementarno abelska grupa ranga r	24
$\beta(X)$	Bettijevo število ali rang grafa X	14
$\mathrm{core}_G(H)$	sredica podgrupe H v grupi G	17
$\kappa_A(x)$	karakteristični polinom matrike A	26
$\langle S \rangle$	grupa, generirana z množico S	11
ω^G	orbita elementa w	16
$\wp\colon \tilde{X} \to X$	krovna projekcija	17
$\wp^{-1}(u)$	vlakno vozlišča u	17
$\pi(X, u)$	fundamentalna grupa grafa X z vozliščem u	14
$\mathrm{C}_G(H)$	centralizator podgrupe H v grupi G	30
$\mathrm{Im}(\phi)$	slika homomorfizma ϕ	16
ζ	napetostna funkcija	19
$m_A(x)$	minimalni polinom matrike A	26
p	praštevilo	10
$\lvert G \rvert$	moč ali red grupe G	10