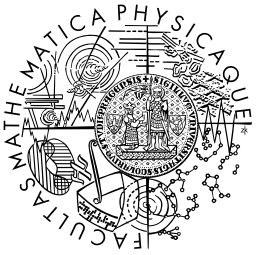


MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁRSKA PRÁCA

Petra Plšková

Algoritmy pre permutačné grupy

Katedra algebry

Vedúci bakalárskej práce: RNDr. Jakub Bulín Ph.D.

Študijný program: Matematika

Študijný obor: Obecná matematika

Praha 2020

Prehlasujem, že som túto bakalársku prácu vypracovala samostatne a výhradne s použitím citovaných prameňov, literatúry a ďalších odborných zdrojov. Táto práca nebola využitá k získaniu iného alebo rovnakého titulu.

Beriem na vedomie, že sa na moju prácu vzťahujú práva a povinnosti vyplývajúce zo zákona č. 121/2000 Sb., autorského zákona v platnom znení, predovšetkým skutočnosť, že Univerzita Karlova má právo na uzavretie licenčnej zmluvy o užití tejto práce ako školského diela podľa §60 odst. 1 autorského zákona.

V ..... dňa ....

Podpis autora

Týmto by som sa chcela poďakovať RNDr. Jakubovi Bulínovi Ph.D. za vedenie mojej bakalárskej práce, cenné rady, odborný dohľad a v neposlednom rade za ochotu a čas. Taktiež ďakujem svojmu priateľovi a rodine za podporu pri písaní tejto práce a počas štúdia.

Názov práce: Algoritmy pre permutačné grupy

Autor: Petra Plšková

Katedra: Katedra algebry

Vedúci bakalárskej práce: RNDr. Jakub Bulín Ph.D., Katedra teoretické informatiky a matematické logiky

Abstrakt: Schreier Simsov algoritmus je základným algoritmom pre permutačné grupy. Jeho úlohou je nájsť bázu a silne generujúcu množinu. Reprezentácia grupy pomocou bázy a silne generujúcej množiny je základom pre veľa ďalších algoritmov. Cieľom tejto práce je poskytnúť čitateľovi detailnejší popis tohto algoritmu. V práci uvedieme jeho pseudokód, vrátane pseudokódov algoritmov riešiacich čiastkové problémy. Časovú a priestorovú zložitosť spočítame vzhľadom k uvedeným pseudokódom. Obdobne popíšeme efektívnu Monte Carlo verziu Schreier Simsovho algoritmu, ktorej časová zložitosť je skoro lineárna. Detailne popíšeme dve vylepšenia algoritmov pre čiastkové problémy, na ktorých je táto verzia založená. Korektnosť deterministickej aj Monte Carlo verzie je podložená teoretickými poznatkami.

Kľúčové slová: permutačná grupa, báza, silne generujúca množina, Schreier Simsov algortimus, Monte Carlo algoritmus

Title: Permutation group algorithms

Author: Petra Plšková

Department: Department of Algebra

Supervisor: RNDr. Jakub Bulín Ph.D., Department of Theoretical Computer Science and Mathematical Logic

Abstract: The Schreier Sims algorithm is a fundamental algorithm for permutation groups. Its purpose is to find a base and a strong generating set. Representation of a group using a base and a strong generating set is the core of many other algorithms. The aim of the thesis is to give the reader a detailed description of the algorithm. We present its pseudocode together with the pseudocode of its subroutines. We analyze the complexity with respect to the given pseudocode. Similarly, we describe an efficient, Monte Carlo version of the Schreier Sims algorithm whose time complexity is nearly linear. We give a detailed description of two improved algorithms for subroutines on which this version is based. We introduce the theoretical framework needed to support the correctness of both the deterministic and the probabilistic version of the algorithm.

Keywords: permutation group, base, strong generating set, Schreier Sims algorithm, Monte Carlo algorithm

Obsah

Úvod

Rozvoj výpočtovej techniky v priebehu minulého storočia motivoval odčlenenie samostatného oboru teórie grúp, takzvanej výpočtovej teórie grúp, ktorá sa zaoberá algoritmami pre grupy. Permutačné grupy sú z výpočtového hľadiska najlepšie preskúmané spomedzi všetkých grúp. Prelom nastal okolo roku 1970, s nástupom metód pre bázu a silne generujúcu množinu permutačnej grupy. V tomto období Sims publikoval svoj algoritmus, tzv. Schreier Simsov algoritmus (Sims, 1970, 1971), ktorý pre ľubovoľnú generujúcu množinu konečnej permutačnej grupy určí bázu danej grupy a príslušnú silne generujúcu množinu. Tento algoritmus sa stal základom pre ďalšie algoritmy skúmajúce permutačné grupy. Schrieier Simsov algoritmus našiel svoje uplatnenie aj v dôkazoch tvrdení, zdanlivo s ním nesúvisiacich. Jedno také uplatnenie súvisí so sporadickými grupami, t.j. konečnými jednoduchými grupami, ktoré nepatria medzi cyklické, alternujúce alebo grupy Lieového typu. Sims v roku 1973 konštrukčne dokázal existenciu a jednoznačnosť Lyonsovej sporadickej grupy (Sims, 1973), rovnakým spôsobom ukázal existenciu a jednoznačnosť tzv. „Baby Monster“ sporadickej grupy (Sims, 1978). Ďalšie uplatnenie sa našlo v teórii grafov. Luks v roku 1981 ukázal, že problém izomorfizmu grafov pre grafy s obmedzeným stupňom vrcholov možno vyriešiť v polynomiálnom čase (Luks, 1982).

Cieľom tejto práce je detailne popísať priebeh Schreier Simsov algoritmu, vrátane časovej a priestorovej náročnosti, a priebeh jeho efektívnej Monte Carlo verzie. V práci predpokladáme, že čitateľ disponuje iba základnými znalosťami teórie grúp, teórie pravdepodobnosti, teórie zložitosti a ovláda základy programovania, odpovedajúc úrovni staršieho študenta bakalárskeho štúdia matematiky. Vo všeobecnosti existuje viacero verzií deterministického Schreier Simsovho algoritmu, v tejto práci uvedieme efektívnejšiu verziu využívajúcu algoritmus Rozklad.

V prvej kapitole definujeme bázu a silne generujúcu množinu pre permutačnú grupu. Zároveň uvedieme niekoľko príkladov pre známe permutačné grupy, špeciálne rozoberieme prípad pre cyklické grupy. Dokážeme tvrdenie o tom, ako vyzerá báza a silne generujúca množina pre cyklickú permutačnú grupu.

V druhej kapitole predstavíme základné pojmy potrebné pre implementáciu Schreier Simsovho algoritmu. Konkrétne definujeme fundamentálne orbity, Schreierov strom, Schreierov vektor a predstavíme algoritmy pre ich konštrukciu a konštrukciu prvku transverzály. V podkapitole 2.3 uvedieme dôkaz Schreierovej lemmy, ktorá je základnou myšlienkou Schreier Simsovho algoritmu. Najvýznamnejším poznatkom tejto kapitoly je algoritmus Rozklad, ktorý zo znalosti báze a silne generujúcej množiny dokáže otestovať či zadaný prvok symetrickej grupy leží v danej permutačnej grupe. Tento algoritmus je analógiou pre Gauss Jordanovú elimináciu, ako je uvedené v oddieli 2.4.1.

V tretej kapitole popíšeme deteministický Schreier Simsov algoritmus, vrátane podrobného pseudokódu, a uvedieme detailnú analýzu jeho časovej a priestorovej zložitosti.

Štvrtá kapitola je venovaná Monte Carlo Schreier Simsovmu algoritmu. Jedná sa o pravdepodobnostný algoritmus, ktorý vychádza z deterministického algoritmu z predchádzajúcej kapitoly. Cieľom tohto Monte Carlo algoritmu je znížiť časovú zložitosť tak, aby bola skoro lineárna. Konkrétne poskytuje dve zlepšenia.

Prvé znižuje hĺbku Schreierových stromov. Druhé zníži počet volaní algoritmu ROZKLAD, ktorý je sám o sebe časovo náročný. Korektnosť oboch vylepšení podrobne obhájime. Cena, ktorú ale zaplatíme za tieto vylepšenia je, že algoritmus nemusí vždy vrátiť správny výsledok.

1. Báza a silne generujúca množina

1.1 Značenie

Najprv zaveďme základné pojmy a značenia používané v tejto práci. Pod pojmom permutačná grupa rozumieme ľubovoľnú podgrupu symetrickej grupy S_n pre $n \in \mathbb{N}$, teda uvažujeme iba konečné permutačné grupy s permutáciami na množine $\{1, ..., n\}$. Jednotkový prvok všeobecnej grupy značíme ako e. Jednotkovým prvkom permutačnej grupy bude identické zobrazenie, značíme ako id. Triviálnu grupu značíme ako 1.

Obraz prvku $\beta \in \{1, ..., n\}$ v permutácii $g \in S_n$ značíme ako β^g. V príkladoch častokrát využívame cyklický zápis permutácií, v algoritmoch je permutácia $g \in S_n$ reprezentovaná ako postupnosť $(1^g, 2^g, ..., n^g)$. Poznamenajme, že skladanie permutácii v tejto práci vykonávame „zľava doprava“ v zmysle, že pre ľubovoľné g,$h \in S_n$ je gh určené predpisom $\beta^{gh} = (\beta^g)^h$ pre každé $\beta \in \{1, ..., n\}$.

Vzťah „H je podgrupou G“ značíme ako $H \leq G$. V tejto práci sa zaoberáme iba pravými rozkladovými triedami grupy H v grupe G a odpovedajúcimi pravými transverzálami. Množinu všetkých pravých rozkladových tried grupy H v grupe G označme ako G/H, nejedná sa ale nutne o faktorgrupu. Počet rozkladových tried pre G/H, t.j. stupeň rozkladu, značíme ako $[G : H]$.

Rád prvku g grupy G značíme ako $ord(g)$. Pokiaľ $X \subseteq G$, tak $\langle X \rangle$ značí podgrupu grupy G generovanú množinou X. Cyklickou grupou nazveme grupu generovanú jedným prvkom. V tejto práci používame logaritmus pri základe 2.

1.2 Báza a silne generujúca množina

Veľká časť algoritmov pre permutačné grupy vyplýva zo znalosti bázy a silne generujúcej množiny pre príslušnú grupu. V tejto podkapitole si uvedené pojmy vysvetlíme. Nasledujúce definície sú z počiatku 4. kapitoly z knihy od Seressa (Seress, 2003, str. 55).

Definícia 1. *Nech $G \leq S_n$ je permutačná grupa a nech $\beta, \beta_1, ..., \beta_i \in \{1,2,...,n\}$, kde i,$n \in \mathbb{N}$.* Stabilizátorom prvku β *nazveme množinu*

$$G_\beta = \{g \in G \mid \beta^g = \beta\}.$$

Stabilizátorom prvkov $\beta_1, ..., \beta_i$ *nazveme*

$$G_{(\beta_1,...,\beta_i)} = \{g \in G \mid \forall j \in \{1, ..., i\} : \ \beta_j^g = \beta_j\}.$$

Stabilizátor ľubovoľne veľa prvkov zrejme tvorí podgrupu G. Existuje index $m \in \mathbb{N}$, $m \leq n$ taký, že $G_{(\beta_1,...,\beta_m)}$ je triviálna grupa. To nás vedie k definícii bázy a príslušného reťazca podgrúp.

Definícia 2. Bázou *permutačnej grupy $G \leq S_n$ nazveme konečnú postupnosť $B = (\beta_1, ..., \beta_m)$ prvkov z $\{1,...,n\}$ takú, že*

$$G_{(\beta_1,...,\beta_m)} = 1.$$

Označme $G^{[i]} := G_{(\beta_1,...,\beta_{i-1})}$. *Pre bázu* B *definujeme nasledujúci* reťazec stabilizátorov,

$$G = G^{[1]} \geq G^{[2]} \geq ... \geq G^{[m]} \geq G^{[m+1]} = 1.$$

Hovoríme, že báza B *je* neredundantná, *pokiaľ* $G^{[i+1]}$ *je vlastnou podgrupou* $G^{[i]}$ *pre všetky* $i \in \{1, ..., m\}$.

Znalosť reťazca stabilizátorov nám umožňuje efektívne skúmať vlastnosti danej permutačnej grupy, či pristupovať k jej prvkom. Najprv je však potrebné vytvoriť vhodnú reprezentáciu pre reťazec stabilizátorov. Požadujeme poznať generujúcu množinu pre každú podgrupu $G^{[i]}$.

Definícia 3. Silne generujúcou množinou *permutačnej grupy* G *vzhľadom k báze* B *nazveme množinu* S *takú, že pre všetky* $i \in \{1, ..., m+1\}$ *platí*

$$\langle S \cap G^{[i]} \rangle = G^{[i]}.$$

Zo znalosti bázy B a príslušnej silne generujúcej množiny S je jednoduché určiť množiny $S^{[i]}$ generujúce $G^{[i]}$. Takáto množina obsahuje práve tie permutácie z S, ktoré stabilizujú prvky β_1,...,β_{i-1}, čo priamo vidno zo zápisu permutácie.

Silne generujúcu množinu budeme tiež skrátene nazývať *SGS* (z angličtiny „strong generating set“). Báza B danej permutačnej grupy a príslušná silne generujúca množina S spolu tvoria základné datové štruktúry pre efektívnu manipuláciu s permutačnou grupou, preto dvojicu (B,S) častokrát nazývame *BSGS*.

V závere kapitoly uvedieme príklady neredundantných báz a odpovedajúcich silne generujúcich množín niektorých známych permutačných grúp a ukážeme špeciálny prípad pre cyklické grupy.

Príklad 1. *Neredundantnou bázou symetrickej grupy* S_n *je práve ľubovoľná postupnosť* $n-1$ *po dvoch rôznych prvkov z množiny* $\{1, ..., n\}$, *napríklad*

$$(1, 2, ..., n-1).$$

Báza menšej veľkosti nemôže existovať, pretože transpozícia dvoch prvkov, ktoré nepatria do báze, stabilizuje všetky prvky bázy. Zároveň pokiaľ by báza obsahovala všetkých n prvkov, tak dostávame spor s neredundantnosťou, keďže stabilizárom ľubovoľných $n-1$ *prvkov je iba identita. Silne genenerujúcou množinou vzhľadom k hore uvedenej báze je*

$$\{(1\ 2), (2\ 3), (3\ 4), ..., (n-1 \quad n)\}.$$

Táto množina generuje celú grupu S_n *a súčasne i-tý až posledný prvok vzhľadom k uvedenému zápisu tejto množiny generuje* $G^{[i]}$, *teda sa skutočne jedná o SGS.*

Príklad 2. *Príkladom neredundantnej bázy alternujúcej grupy* A_n *je*

$$(1, 2, ..., n-2).$$

Opäť platí, že neexistuje neredundantná báza inej veľkosti pre túto grupu. Silne generujúcou množinou vzhľadom k uvedenej báze je

$$\{(1\ 2\ 3), (2\ 3\ 4), (3\ 4\ 5), ..., (n-2 \quad n-1 \quad n)\}.$$

Príklad 3. *Neredundantná báza pre dihedrálnu grupu D_{2n} je vždy tvaru*

$$(i,j)$$

kde $i, j \in \{1, ..., n\}$,$i \neq j$ a $i \not\equiv j + \frac{n}{2}$ $(mod\ n)$, pokiaľ je n párne. Na grupu D_{2n} sa nazerajme ako na grupu symetrií pravidelného n-uholníka. Potom stabilizátorom jedného prvku je grupa obsahujúca iba zrkadlenie podľa osi prechádzajúcej vrcholom príslušnému tomuto prvku a identitu. Toto zrkadlenie stabilizuje maximálne dva prvky. Stabilizovaním ďalšieho, ešte nestabilizovaného, prvku dostaneme triviálnu grupu. Príslušnou silne generujúcou množinou je $\{r, z\}$, kde:

$$r = (1\ 2\ ...\ n)$$

$$z = (i+1 \quad i-1)(i+2 \quad i-2)(i+3 \quad i-3)...$$

1.3 Báza a SGS pre cyklickú grupu

Doposiaľ sme si ukázali príklady permutačných grúp, kde každá neredundantná báza bola rovnakej veľkosti. Vo všeobecnosti však neredundantné bázy môžu byť rôzne veľké, aj napriek tomu, že sú v určitom slova zmysle minimálne. V tejto podkapitole sa zamyslíme nad tým, ako vyzerajú neredundantné bázy a príslušné silne generujúce množiny pre cyklickú permutačnú grupu.

Nech $G = \langle g \rangle \leq S_n$, kde $g \in S_n$. Veľkosť cyklickej grupy G odpovedá rádu generátora g a prvkami grupy G sú práve práve prvky $g^0 = id$, g^1, ..., $g^{ord(g)-1}$. Zároveň platí, že rád permutácie g sa rovná najmenšiemu spoločnému násobku dĺžok jej cyklov v cyklickom zápise. Teda dokážeme jednoducho určiť veľkosť grupy G. Navyše podgrupou cyklickej grupy môže byť opäť len cyklická grupa, generovaná prvkom g^k, pre nejaké $0 \leq k \leq ord(g) - 1$ deliace $|G|$, vzhľadom k Lagrangerovej vete.

Najprv chceme určiť stabilizátor jedného ľubovoľného prvku $\beta \in \{1, ..., n\}$, ktorý grupa G ešte nestabilizuje. Hľadáme $1 < l \leq ord(g) - 1$ také, že $\beta^{g^l} = \beta$. Uvažujme cyklický zápis permutácie g. Na to, aby sa β na danom g^l zobrazovalo samo na seba, musí byť l dĺžkou toho cyklu permutácie g, v ktorom sa β nachádza. Zároveň je l najmenšie nenulové prirodzené číslo také, že g^l stabilizuje β, teda $G_\beta = \langle g^l \rangle$. Uvedomme si ale, že g^l súčasne stabilizuje všetky prvky daného cyklu z cyklického zápisu g a všetky prvky z cyklov dĺžky, ktorá delí l.

Pokiaľ chceme stabilizovať viac prvkov, tak g potrebujeme umocniť na najmenší spoločný násobok dĺžok cyklov z cyklického zápisu g, v ktorých sa tieto prvky nachádzajú. Na to, aby sme dostali triviálnu grupu, potrebujeme g umocniť na svoj vlastný rád, teda požaduje, aby $nsn(l_1, ..., l_m) = ord(g)$, kde $l_1, ..., l_m$ sú dĺžky cyklov, v ktorých sa nachádzajú poporadí prvky β_1,...,β_m. Tým sme zabezpečili, že $B = (\beta_1, ..., \beta_m)$ je bázou G. Príslušná silne generujúca množina je $\{g, g^{l_1}, g^{nsn(l_1,l_2)}, ..., g^{nsn(l_1,...,l_{m-1})}\}$. Ostáva zabezpečiť to, aby B bola neredundantná. Ako sme uviedli, g^l súčasne stabilizuje všetky prvky z cyklov dĺžky, ktorá delí l. Teda požadujeme, aby $l_b \nmid l_a$ pre všetky $a,b \in \{1, ..., m\}$, $a < b$. Závery z tejto úvahy sú zhrnuté v nasledujúcom pozorovaní.

Pozorovanie 1. *Daná je permutačná grupa $G = \langle g \rangle \leq S_n$, kde*

$$g = (a_{11}\ a_{12}\ ...\ a_{1l_1})(a_{21}\ a_{22}\ ...\ a_{2l_2})...(a_{k1}\ a_{k2}\ ...\ a_{kl_k})$$

je cyklický zápis permutácie g. Nech $i_1, ..., i_m \in \{1, ..., k\}$ *a* $j_c \in \{1, ..., l_c\}$ *pre každé* $c \in \{1, ..., m\}$, $m \in \mathbb{N}$. *Potom* $B = (a_{i_1 j_1}, a_{i_2 j_2}, ..., a_{i_m j_m})$ *je neredundantná báza grupy G práve vtedy, keď* $nsn(l_{i_1}, l_{i_2}, ..., l_{i_m}) = nsn(l_1, l_2, ..., l_k)$ *a* $l_{i_b} \nmid l_{i_a}$ *pre všetky* $a, b \in \{1, ..., m\}$ *také, že* $a < b$. *Príslušná silne generujúca množina je tvaru*

$$S = \{g, g^{l_{i_1}}, g^{nsn(l_{i_1}, l_{i_2})}, ..., g^{nsn(l_{i_1}, l_{i_2}, ..., l_{i_{m-1}})}\}$$

Dôkaz. Označme $B = (\beta_1, ..., \beta_m) = (a_{i_1 j_1}, a_{i_2 j_2}, ..., a_{i_m j_m})$. Za predpokladu, že $nsn(l_{i_1}, l_{i_2}, ..., l_{i_m}) = nsn(l_1, l_2, ..., l_k)$ a $l_{i_b} \nmid l_{i_a}$ pre všetky $a < b$, platí

$$\begin{aligned}
G^{[1]} &= G = \langle g \rangle, \\
G^{[2]} &= G_{\beta_1} = \langle g^{l_{i_1}} \rangle, \\
G^{[3]} &= G_{(\beta_1, \beta_2)} = \langle g^{nsn(l_{i_1}, l_{i_2})} \rangle, \\
&\vdots \\
G^{[m+1]} &= G_{(\beta_1, ..., \beta_m)} = \langle g^{nsn(l_{i_1}, ..., l_{i_m})} \rangle = \langle g^{nsn(l_1, ..., l_k)} \rangle = \langle g^{ord(g)} \rangle = 1.
\end{aligned}$$

Zrejme $l_{i_1} \geq 2$, teda $G^{[1]} = \langle g \rangle > \langle g^{l_{i_1}} \rangle = G^{[2]}$. Ukážeme, že $G^{[j+1]}$ je vlastná podgrupa $G^{[j]}$ pre $j = 2, ..., m$. Vieme, že l_{i_j} nedelí žiadne z $l_{i_1}, ..., l_{i_{j-1}}$, teda platí nasledujúca ostrá nerovnosť:

$$nsn(l_{i_1}, ..., l_{i_{j-1}}) < nsn(l_{i_1}, ..., l_{i_{j-1}}, l_{i_j})$$

Z uvedenej nerovnosti a z toho, že $ord(g)$ je najmenšie také prirodzené číslo, že platí $g^{ord(g)} = id$, vyplýva, že $G^{[j+1]} > G^{[j]}$ pre všetky $j = 2, ..., m$. Teda B je neredundantná báza.

Opačnú implikáciu dokážeme sporom. Predpokladajme, že B je neredundantná báza. Pokiaľ by platilo $nsn(l_{i_1}, l_{i_2}, ..., l_{i_m}) \neq nsn(l_1, l_2, ..., l_k)$, tak nutne by muselo platiť, že $G_{(\beta_1, \beta_2, ..., \beta_m)} = \langle g^{nsn(l_{i_1}, l_{i_2}, ..., l_{i_m})} \rangle \neq \langle g^{ord(g)} \rangle = 1$, čo je spor s definíciou bázy. Na druhú stranu, pokiaľ by existovali a, b také, že $a < b$ a $l_{i_b} \mid l_{i_a}$, tak $G^{[b+1]} = G_{(\beta_1, ..., \beta_a, ..., \beta_{b-1}, \beta_b)} = \langle g^{nsn(l_{i_1}, ..., l_{i_a}, ..., l_{i_{b-1}}, l_{i_b})} \rangle = \langle g^{nsn(l_{i_1}, ..., l_{i_a}, ..., l_{i_{b-1}})} \rangle = = G_{(\beta_1, ..., \beta_a, ..., \beta_{b-1})} = G^{[b]}$, čo je spor s neredundantnosťou bázy B.

Ako vidno vyššie, množina S je zjednotením množín obsahujúcich generátory pre $G^{[1]}, ..., G^{[m]}$, teda pre všetky $j \in \{1, ..., m\}$ platí $\langle S \cap G^{[j]} \rangle = \langle g^{nsn(l_{i_1}, ..., l_{i_j})} \rangle = = \langle G^{[j]} \rangle$ a zrejme platí aj $\langle S \cap G^{[m+1]} \rangle = \langle \emptyset \rangle = 1$. Dostali sme, že množina S je silne generujúca množina vzhľadom k báze B.

□

Uvedieme príklad, v ktorom vďaka poznatkom vyššie určíme všetky možné neredundantné bázy a ich silne generujúce množiny pre zadanú cyklickú grupu.

Príklad 4. *Daná je cyklická permutačná grupa* $G = \langle g \rangle$, *kde*

$$g = (1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9).$$

Veľkosť tejto grupy je $|G| = ord(g) = nsn(2,3,4) = 12$ *a jej prvkami sú práve* $id = g^0, g, g^2, ..., g^{11}$. *Z hore uvedených poznatkov vieme, že záleží len na tom, v akom cykle sa nachádza prvok, ktorý chceme stabilizovať. Označme prvky* $1, 2$

ako α, prvky $3,4,5$ ako β a prvky $6,7,8,9$ ako γ. Možnosti pre stabilizátor jedného prvku sú $G_\alpha = \langle g^2 \rangle$, $G_\beta = \langle g^3 \rangle$ a $G_\gamma = \langle g^4 \rangle$. Stabilizátory dvojíc prvkov sú:

$$\begin{aligned}
G_{(\alpha,\beta)} &= \langle g^{nsn(2,3)} \rangle = \langle g^6 \rangle < \langle g^2 \rangle = G_\alpha \\
G_{(\alpha,\gamma)} &= \langle g^{nsn(2,4)} \rangle = \langle g^4 \rangle < \langle g^2 \rangle = G_\alpha \\
G_{(\beta,\alpha)} &= \langle g^{nsn(3,2)} \rangle = \langle g^6 \rangle < \langle g^3 \rangle = G_\beta \\
G_{(\beta,\gamma)} &= \langle g^{nsn(3,4)} \rangle = \langle g^{12} \rangle = 1 \\
G_{(\gamma,\alpha)} &= \langle g^{nsn(4,2)} \rangle = \langle g^4 \rangle = G_\gamma \\
G_{(\gamma,\beta)} &= \langle g^{nsn(4,3)} \rangle = \langle g^{12} \rangle = 1
\end{aligned}$$

Našli sme neredundantné bázy tvaru (β,γ) s SGS $\{g,g^3\}$ a (γ,β) s SGS $\{g,g^4\}$. Zároveň žiadna neredundantná báza nebude začínať dvojicou (γ,α).

$$\begin{aligned}
G_{(\alpha,\beta,\gamma)} &= \langle g^{nsn(2,3,4)} \rangle = \langle g^{12} \rangle = 1 \\
G_{(\alpha,\gamma,\beta)} &= \langle g^{nsn(2,4,3)} \rangle = \langle g^{12} \rangle = 1 \\
G_{(\beta,\alpha,\gamma)} &= \langle g^{nsn(3,2,4)} \rangle = \langle g^{12} \rangle = 1
\end{aligned}$$

Tentoraz sme našli neredundantné bázy tvaru (α,β,γ),(α,γ,β) a (β,α,γ). Príslušné SGS sú po poradí $\{g,g^2,g^6\}$, $\{g,g^2,g^4\}$ a $\{g,g^3,g^6\}$. Žiadne iné neredundantné bázy už neexistujú.

2. Základne poznatky pre Schreier Simsov algoritmus

V predchádzajúcej kapitole sme vysvetlili pojem bázy a silne generujúcej množiny. V tejto kapitole definujeme pojmy potrebné pre implementáciu Schrieier Simsovho algoritmu, ktorý má za úlohu nájsť BSGS.

2.1 Fundamentálne orbity

Pre reťazec stabilizátorov

$$G = G^{[1]} \geq G^{[2]} \geq ... \geq G^{[m]} \geq G^{[m+1]} = 1$$

bude našou snahou popísať množiny pravých rozkladových tried $G^{[i]}/G^{[i+1]}$ pre každé $i \in \{1, ..., m\}$. V tejto podkapitole definujeme pojem *fundamentálna orbita* a ukážeme ako súvisí s rozkladovými triedami.

V teórii grúp pod pojmom *pôsobenie grupy* G na množine Ω rozumieme ľubovoľný homomorfizmus $\varphi : G \to S_\Omega$. Zrejme permutačná grupa G pôsobí triviálne na množine $\Omega = \{1,...,n\}$. Definujeme reláciu $\sim$ na Ω nasledovne:

$$\alpha \sim \beta \iff \exists g \in G : \beta = \alpha^g.$$

Relácia $\sim$ je ekvivalenciou, konkrétne je:

- reflexívna ($\alpha = \alpha^{id}$),
- symetrická ($\alpha^g = \beta \iff \beta^{g^{-1}} = \alpha$),
- tranzitívna ($(\alpha^g = \beta \wedge \beta^h = \gamma) \implies \alpha^{gh} = \gamma$).

Jej bloky ekvivalencie budeme nazývať *orbity*. Špeciálne zavedieme pojem *fundamentálna orbita*.

Definícia 4. *(Seress, 2003, str. 56) Nech G je permutačná grupa pôsobiaca na množine $\{1, ..., n\}$ a $B = (\beta_1, ..., \beta_m)$ je jej báza. Množiny*

$$\Delta^{[i]} := \beta_i^{G^{[i]}} = \{\beta_i^g \mid g \in G^{[i]}\}$$

pre $i \in \{1, ..., m\}$ nazveme fundamentálnymi orbitami *grupy G vzhľadom k báze B. Súčasne zavedieme značenie:*

$$\Delta^* := (\Delta^{[1]}, \Delta^{[2]}, ..., \Delta^{[m]}).$$

V nasledujúcom pozorovaní si ukážeme spomenutú súvislosť medzi uvedenými množinami pravých rozkladových tried a fundamentálnymi orbitami. Pozorovanie je ekvivalentné tvrdeniu 2.3.1 z práce Murraya (Murray, 1994).

Pozorovanie 2. *Nech $B = (\beta_1, ..., \beta_m)$ je báza permutačnej grupy G s reťazcom stabilizátorov $G = G^{[1]} \geq G^{[2]} \geq ... \geq G^{[m]} \geq G^{[m+1]} = 1$ a $\beta_i^{G^{[i]}}$ je fundamentálna orbita, $i \in \{1, ..., m\}$. Potom existuje bijekcia medzi $\beta_i^{G^{[i]}}$ a $G^{[i]}/G^{[i+1]}$.*

Dôkaz. Definujme zobrazenie $f : \beta_i^{G^{[i]}} \to G^{[i]}/G^{[i+1]}$ predpisom $f(\alpha) = G^{[i+1]}g$, kde $\alpha = \beta_i^g$ pre nejaké $g \in G^{[i]}$. Zobrazenie f je dobre definované, lebo ak $G^{[i+1]}g \neq G^{[i+1]}h$ pre nejaké $g, h \in G^{[i]}$, tak $\beta_i^g \neq \beta_i^h$. Takisto je zrejme f na $G^{[i]}/G^{[i+1]}$. Zvolme α, γ také, že $\alpha = \beta_i^g \neq \beta_i^h = \gamma$ pre nejaké g,$h \in G^{[i]}$. Potom nutne platí, že $f(\alpha) = G^{[i+1]}g \neq G^{[i+1]}h = f(\gamma)$, pretože $gh^{-1} \notin G^{[i+1]}$, t.j. $\beta_i^{gh^{-1}} \neq \beta_i$. Kebyže $\beta_i^{gh^{-1}} = \beta_i$, tak nutne $\beta_i^g = \beta_i^{gh^{-1}h} = \beta_i^h$, čo je spor s predpokladom. Tým sme ukázali, že zobrazenie f je prosté.

□

Z pozorovania vyššie rovnako vyplýva, že každá pravá rozkladová trieda grupy $G^{[i+1]}$ v grupe $G^{[i]}$ odpovedá množine $\{g \in G^{[i]} \mid \beta_i^g = \alpha\}$ pre nejaké $\alpha \in \beta_i^{G^{[i]}}$.

Podľa Lagrangerovej vety platí $|G| = [G : G_{\beta_1}]|G_{\beta_1}|$. Vzhľadom k pozorovaniu vyššie, m-násobnej aplikácie Lagrangerovej vety a faktu, že $G^{[m+1]} = 1$, dostávame

$$|G| = \prod_{i=1}^{m} [G^{[i]} : G^{[i+1]}] = \prod_{i=1}^{m} |\beta_i^{G^{[i]}}|.$$

Triviálne platí, že $|\beta_i^{G^{[i]}}| \leq n$. Súčasne za predpokladu, že báza B je neredundantná, platí $[G^{[i]} : G^{[i+1]}] \geq 2$. Celkovo

$$2^{|B|} \leq |G| \leq n^{|B|}.$$

Úpravou tohto výrazu dostaneme hornú a dolnú hranicu pre veľkosť neredundantnej bázy B.

Dôsledok 3. *(Seress, 2003, str. 55) Nech $G \leq S_n$ je permutačná grupa a B je jej neredundantná báza. Potom platí:*

$$\left\lceil \frac{\log |G|}{\log n} \right\rceil \leq |B| \leq \lfloor \log |G| \rfloor$$

Príklad 5. *Uvažujme grupu $G = \langle (1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9\ 10\ 11) \rangle$, podľa podkapitoly 1.3 vieme, že má bázy veľkosti 1 a 2. Zároveň:*
$\lceil \log |G| / \log n \rceil = \lceil \log nsn(2,3,6) / \log 11 \rceil = 1$
$\lfloor \log |G| \rfloor = \lfloor \log nsn(2,3,6) \rfloor = 2$

Predchádzajúci príklad je zároveň riešením cvičenia 4.2 z knihy od Seressa (2003, cvičenie 4.2). Fundamentálnu orbitu možno určiť pomerne priamočiaro prehľadávaním do šírky. Následujúci algoritmus bol uvedený v knihe od Holta, Eicka a O'Briena (Holt a kol., 2005, str. 78), kde je uvedený aj dôkaz korektnosti.

Vstup: $\beta_i \in B$, kde B je báza $G \leq S_n$, $S^{[i]} = \{s_{i1},...s_{ik_i}\}$, $s_{i1},...s_{ik_i} \in S_n$, $\langle S^{[i]} \rangle = G^{[i]}$
Výstup: fundamentálna orbita $\Delta^{[i]}$
$\Delta^{[i]} := \{\beta_i\}$;
for $\gamma \in \Delta^{[i]}$ **do**
  for $j = 1,...,k_i$ **do**
    if $\gamma^{s_{ij}} \notin \Delta^{[i]}$ **then**
      $\Delta^{[i]} := \Delta^{[i]} \cup \{\gamma^{s_{ij}}\}$;
    end
  end
end
return $\Delta^{[i]}$;

Algoritmus 1: ORBITA $(\beta_i, S^{[i]})$

Pozorovanie 4. *Algoritmus* ORBITA *je korektný.*

Dôkaz. Označme ako Δ výstup algoritmu ORBITA. Ukážeme, že sa skutočne jedná o fundamentálnu orbitu $\Delta^{[i]}$. Zrejme každé $\gamma^{s_{ij}}$, ktoré sa objaví v Δ, patrí orbite $\Delta^{[i]}$. Naopak pre ľubovoľné $g \in G^{[i]}$ ukážeme, že platí $\beta_i^g \in \Delta$. Vyjadrime g ako

$$g = s_{ij_1} s_{ij_2} ... s_{ij_k},$$

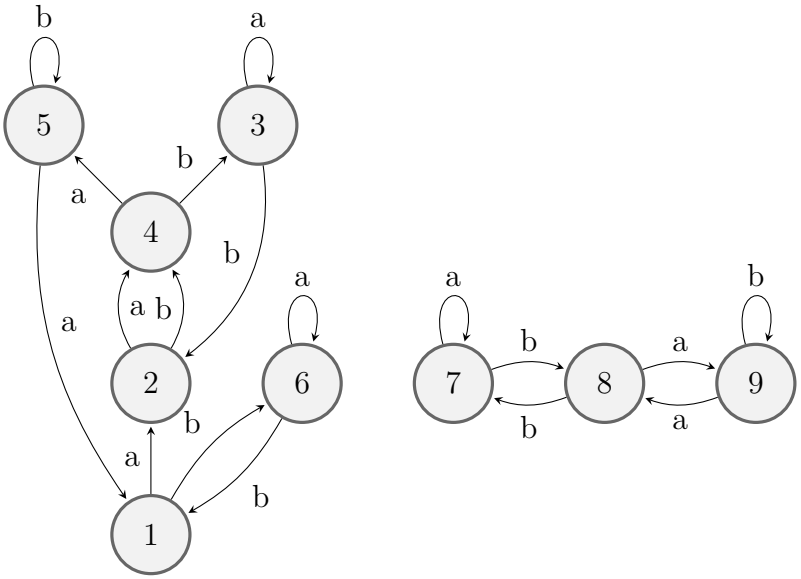
kde $s_{ij_1},...,s_{ij_k} \in S^{[i]} \cup (S^{[i]})^{-1}$. Vďaka konečnosti rádu každého prvku $s \in S^{[i]}$ platí, že $s^{-1} = s^{ord(s)-1}$. Teda bez ujmy na všeobecnosti môžeme predpokladať, že $s_{ij_1},...,s_{ij_k} \in S^{[i]}$. Pokračujeme indukčne podľa k. Pre $k = 0$, t.j. $g = id$, tvrdenie platí, lebo Δ je inicializované na $\{\beta_i\}$. Predpokladajme, že $\gamma = \beta_i^{g'} \in \Delta$ pre $g' = s_{ij_1} s_{ij_2} ... s_{ij_{k-1}}$. Potom aj $\gamma^{s_{ij_k}} = \beta_i^g$ sa objaví v Δ v priebehu cyklu.

□

2.2 Schreierov strom a súvislosť s transverzálou

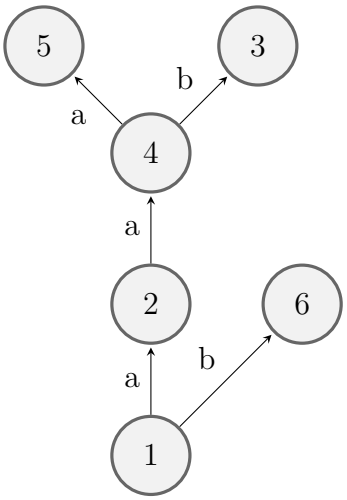
Množina generátorov S permutačnej grupy G pôsobiacej na množine $\{1, ..., n\}$ nám určuje orientovaný graf, tiež uvedený v knihe od Butlera (Butler, 1991, str. 56, 57). Jeho vrcholmi sú prvky množiny $\{1, ..., n\}$. Orientovaná hrana smeruje z vrcholu γ k vrcholu δ a je označená permutáciou $s \in S$, práve vtedy, keď $\gamma^s = \delta$. Komponenty tohto grafu sú práve orbity pôsobenia grupy G. Vďaka tomu, že grupa G je konečná, sú tieto komponenty silne súvislé. Platí, že ak $\gamma^s = \delta$, tak $\delta^{s^j} = \gamma$ pre $j = ord(s) - 1$.

Príklad 6. *Nech permutačnú grupu G generujú permutácie $a = (1\ 2\ 4\ 5)(8\ 9)$, $b = (1\ 6)(2\ 4\ 3)(7\ 8)$. Grupu G reprezentuje nasledujúci graf.*



Dôležitým pre nás bude podgraf tohto grafu, takzvaný Schreierov strom. *Schreierovým stromom* pre β_i vzhľadom k $S^{[i]}$ nazveme orientovaný strom $T^{[i]}$, ktorého každá hrana je orientovaná smerom od koreňa β_i, kde $\langle S^{[i]} \rangle = G^{[i]}$. Vrcholy sú prvky fundamentálnej orbity $\Delta^{[i]}$. Hrana smerujúca z vrcholu γ k vrcholu δ je označená permutáciou $s \in S^{[i]}$, pričom platí $\gamma^s = \delta$. *Hĺbkou* Schreierovho stromu rozumieme dĺžku najdlhšej cesty z koreňu do nejakého listu. Pojem Schreierov strom vo svojej práci používa aj Seress (2003, str. 56), avšak s opačne orientovanými hranami. Kvôli konzistencii so zvyškom literatúry používame danú orientáciu hrán.

Príklad 7. *Uvažujme permutácie a,b ako v predchádzajúcom príklade. Schreierov strom pre $\beta_i = 1$ vzhľadom k $S^{[i]} = \{s_{i1}, s_{i2}\}$, kde $s_{i1} = a, s_{i2} = b$, bude vyzerať nasledovne:*



V počítači možno Schreierov strom reprezentovať pomocou poľa. Vyplýva to z jednoduchého pozorovania, že do každého vrcholu Schreierovho stromu okrem koreňa vedie práve jedna hrana. Do koreňa nevedie žiadna hrana. Jednou možnosťou ako nájsť nejaký Schreierov strom pre β_i vzhľadom k $S^{[i]}$ je využiť algoritmus Orbita na daných vstupoch a pre každý prvok orbity okrem β_i si zapamätať, pre ktoré $s \in S^{[i]}$ bol uložený ako γ^s. Zavádzame nasledujúcu definíciu podľa knihy od Holta a kol. (2005, definícia 4.1).

Definícia 5. Schreierovým vektorom *pre prvok* β_i *vzhľadom k* $S^{[i]}$ *nazveme pole* v_i *dĺžky* n*, pre ktoré platí:*

- $v_i[\beta_i] := -1$
- $v_i[\delta] := j$*, kde vo funkcii* ORBITA *bolo* $\delta \in \beta_i^{G^{[i]}} \setminus \{\beta_i\}$ *vložené ako* $\gamma^{s_{ij}}$
- $v_i[\alpha] := 0$ *pre* $\alpha \notin \beta_i^{G^{[i]}}$

Vzhľadom k tejto definícii rozšírime algoritmus ORBITA tak, aby súčasne našiel aj Schreierov vektor. Algoritmus vo svojej knihe uviedol Holt a kol. (2005, str. 80).

Vstup: $\beta_i \in B$, kde B je báza $G \leq S_n$, $S^{[i]} = \{s_{i1}, ..., s_{ik_i}\}$, $s_{i1}, ..., s_{ik_i} \in S_n$, $\langle S^{[i]} \rangle = G^{[i]}$
Výstup: fundamentálna orbita $\Delta^{[i]}$ a Schreierov vektor v_i

```
for α = 1,...,n do
    v_i[α] := 0;
end
Δ^[i] := {β_i} ;
v_i[β_i] := −1;
for γ ∈ Δ^[i] do
    for j = 1,...,k_i do
        if γ^{s_ij} ∉ Δ^[i] then
            Δ^[i] := Δ^[i] ∪ {γ^{s_ij}};
            v_i[γ^{s_ij}] := j;
        end
    end
end
return Δ^[i], v_i;
```

Algoritmus 2: ORBITASCHREIERVEKTOR$(\beta_i, S^{[i]})$

Príklad 8. *Schreierov vektor pre prvok* $\beta_i = 1$ *vzhľadom k* $S^{[i]} = \{s_{i1}, s_{i2}\}$*, kde* s_{i1}, s_{i2} *sú také, ako v predchádzajúcom príklade, bude:*

$$v_i = [-1,1,2,1,1,2,0,0,0]$$

Okrem toho, že Schreierov strom nám určuje fundamentálnu orbitu pre prvok β_i bázy B, určuje súčasne aj prvky transverzály pre $G^{[i]}/G^{[i+1]}$. Sú nimi práve tie permutácie, ktoré dostaneme zložením permutácií na jednoznačne určenej ceste z koreňu β_i do vrcholu γ, pre každé $\gamma \in \Delta^{[i]}$. Reprezentantom pre $\gamma = \beta_i$ bude identita.

Pravé transverzály pre $G^{[i]}/G^{[i+1]}$ označíme ako $R^{[i]}$, kde $i \in \{1, ..., m\}$. Ich prvkami budú $r_{i\gamma}$, pričom platí $\beta_i^{r_{i\gamma}} = \gamma$ pre každé $\gamma \in \Delta^{[i]}$.

Nasledujúci algoritmus určí prvok $r_{i\gamma}$ transverzály $R^{[i]}$ určenej Schreierovým vektorom v_i pre zadané $\gamma \in \{1, ..., n\}$, pokiaľ existuje. Algoritmus vo svojej knihe uviedol Holt a kol. (2005, str. 80).

Vstup: Schreierov vektor v_i pre prvok β_i bázy grupy $G \leq S_n$,
$\gamma \in \{1, ..., n\}$, $S^{[i]} = \{s_{i1}, ..., s_{ik_i}\}$, $s_{i1}, ..., s_{ik_i} \in S_n$, $\langle S^{[i]} \rangle = G^{[i]}$
Výstup: $r_{i\gamma} \in G^{[i]}/G^{[i+1]}$ alebo neúspech, pokiaľ $\gamma \notin \Delta^{[i]}$

```
if v_i[γ] = 0 then
    return neúspech;
end
u := id;
l := v_i[γ];
while l ≠ −1 do
    u := s_il u;
    γ := γ^(s_il^−1);
    l := v_i[γ];
end
return u;
```

Algoritmus 3: PrvokTransverzaly(γ, v_i, $S^{[i]}$)

Ukladanie Schreierových vektorov v počítači namiesto celých transverzál má jednoduchý dôvod, šetrí pamäť. Priestorová náročnosť jedného Schreierovho vektoru je zrejme $\mathcal{O}(n)$, pričom uloženie transverzály je $\mathcal{O}(n^2)$.

2.3 Schreierová lemma

Doposiaľ sme popísali rozkladové triedy z $G^{[i]}/G^{[i+1]}$. Za pomoci algoritmov OrbitaSchreierVektor a PrvokTransverzaly dokážeme zo znalosti $S^{[i]}$ určiť $\Delta^{[i]}$ a $R^{[i]}$, pre $i = 1, ..., m$. Nasledujúca tzv. *Schreierová lemma* nám umožní zo znalosti $\Delta^{[i]}$ a $R^{[i]}$ určiť generujúcu množinu pre $G^{[i+1]}$. Pre $g \in G$, $H \leq G$ a pravú transverzálu R pre G/H označme $\overline{g} := R \cap Hg$. Dôkaz Schreierovej lemmy je doplnený o ozrejmenie, že každý prvok z T leží v H.

Lemma 5. *(Seress, 2003, lemma 4.2.1) Nech G je grupa generovaná množinou S, H je podgrupa G a R je pravá transverzála pre G/H. Potom množina*

$$T = \{rs(\overline{rs})^{-1} | r \in R, s \in S\}$$

generuje podgrupu H.

Dôkaz. Zrejme každý prvok z T náleží H, pretože $H(rs(\overline{rs})^{-1}) = (Hrs)(\overline{rs})^{-1} = = (H\overline{rs})(\overline{rs})^{-1} = H((\overline{rs})(\overline{rs})^{-1}) = He = H$.

Na druhú stranu zvolme $h \in H$ ľubovoľné. Ukážeme, že $h \in \langle T \rangle$. Podľa predpokladu máme, že $G = \langle S \rangle = \langle S \cup S^{-1} \rangle$, teda $h = s_1 s_2 ... s_k$ pre nejaké $s_1 s_2 ... s_k \in S \cup S^{-1}, k \geq 0$. Definujme:

$$r_1 := 1, \quad h_0 := r_1 s_1 s_2 ... s_k$$

$$r_{j+1} := \overline{r_j s_j}, \quad t_j := r_j s_j (\overline{r_j s_j})^{-1}$$

$$h_j := t_1 t_2 ... t_j r_{j+1} s_{j+1} s_{j+2} ... s_k$$

pre $j = 1, ..., k$. Zrejme $h_0 = h$. Nahradením t_{j+1} a r_{j+2} vo výraze pre h_{j+1} dostávame, že pre všetky $j = 1, ..., k-1$ platí:

$$h_{j+1} = t_1 t_2 ... t_j t_{j+1} r_{j+2} s_{j+2} ... s_k =$$
$$= t_1 t_2 ... t_j (r_{j+1} s_{j+1} (\overline{r_{j+1} s_{j+1}})^{-1})(\overline{r_{j+1} s_{j+1}}) s_{j+2} ... s_k =$$
$$= t_1 t_2 ... t_j r_{j+1} s_{j+1} s_{j+2} ... s_k = h_j$$

To znamená, že takisto platí, že $h = h_k = t_1 t_2 ... t_k r_{k+1}$. Vzhľadom k tomu, že $h \in H$ a $t_1 t_2 ... t_k \in \langle T \rangle \leq H$, musí platiť, že $r_{k+1} \in H \cap R = \{1\}$. Teda $h \in \langle T \rangle$. □

Aplikáciou lemmy na grupu $G^{[i]}$ a jej podgrupu $G^{[i+1]}$ dostávame triviálny dôsledok.

Dôsledok 6. *Nech $G^{[i]} = \langle S^{[i]} \rangle$ je stabilizátorom prvých $i-1$ prvkov báze $B = (\beta_1, ..., \beta_m)$ permutačnej grupy G a $G^{[i+1]} = G^{[i]}_{\beta_i}$. Nech $R^{[i]}$ je pravou transverzálou pre $G^{[i]}/G^{[i+1]}$ a pre každé $\gamma \in \Delta^{[i]} = \beta_i^{G^{[i]}}$ nech $r_{i\gamma}$ značí jednoznačne určený prvok $R^{[i]}$ spĺňajúci $\beta_i^{r_{i\gamma}} = \gamma$. Potom*

$$\{r_{i\gamma}\, s\, (r_{i\gamma^s})^{-1} \mid \gamma \in \Delta^{[i]}, s \in S^{[i]}\}$$

generuje $G^{[i+1]}$.

Prvky $r_{i\gamma}\, s\, (r_{i\gamma^s})^{-1}$ nazveme *Schreierovými generátormi* pre grupu $G^{[i+1]}$. Nech transverzálu $R^{[i]}$ určuje nejaký Schreierov strom. Potom do každého vrcholu $\delta \in \Delta^{[i]} \setminus \{\beta_i\}$ tohto stromu vedie práve jedna hrana označená permutáciou $s \in S^{[i]}$ z vrcholu $\gamma \in \Delta^{[i]}$. To je ekvivalentné tomu, že $r_{i\gamma}\, s = r_{i\gamma^s}$, a teda počet triviálnych Schreierových generátorov je $|\Delta^{[i]}| - 1$.

Pozorovanie 7. *Nech $G = \langle X \rangle \leq S_n$, $S^{[1]} = X$, $S^{[i]}$ je množinou netriviálnych Schreierových generátorov pre $G^{[i]}$, $i \in \mathbb{N}, i \geq 2$. Potom veľkosť množiny $S^{[i]}$ je nanajvýš*

$$1 + |\Delta^{[1]}||\Delta^{[2]}|...|\Delta^{[i]}|(|X| - 1)$$

Dôkaz. Množina $S^{[2]}$ má veľkosť nanajvýš $|S^{[1]}||\Delta^{[1]}| - (|\Delta^{[1]}| - 1) = 1 + |\Delta^{[1]}|(|X| - 1)$ ako vyplýva z diskusie vyššie. Nech tvrdenie platí pre nejaké $i \geq 2$, potom veľkosť $S^{[i+1]}$ je nanajvýš $1 + |\Delta^{[1]}|(|S^{[i]}| - 1) = 1 + |\Delta^{[1]}|(1 + |\Delta^{[2]}|...|\Delta^{[i]}|(|X| - 1) - 1) = 1 + |\Delta^{[1]}||\Delta^{[2]}|...|\Delta^{[i]}||\Delta^{[i+1]}|(|X| - 1)$. □

Príklad 9. *Uvažujme $s_1 = (1\ 2\ 3)(4\ 5), s_2 = (1\ 4\ 5)(2\ 3)$ pre $X = \{s_1, s_2\}$, kde $G = \langle X \rangle \leq S_5$ je permutačná grupa a nech G_1 je stabilizátorom prvku 1. Zrejme $\Delta := 1^{G_1} = \{1,2,3,4,5\}$. Zvolme transverzálu $R = \{r_1, ..., r_5\}$ pre $r_1 = id, r_2 = s_1, r_3 = s_1 s_2, r_4 = s_2, r_5 = s_2 s_1$. Potom existuje práve 6 netriviálnych Schreierových generátorov pre G_1, a to $r_2 s_1 r_3^{-1} = (3\ 2\ 4)$, $r_3 s_1 r_1^{-1} = (3\ 5\ 4\ 2)$, $r_3 s_2 r_2^{-1} = (3\ 4\ 5)$, $r_4 s_2 r_5^{-1} = (5\ 4\ 2)$, $r_5 s_1 r_4^{-1} = (5\ 2\ 3)$, $r_5 s_1 r_1^{-1} = (5\ 3\ 2\ 4)$, pričom $1 + |\Delta|(|X| - 1) = 6$.*

Dôvodom, prečo veľkosť $S^{[i]}$ nemusí dosiahnúť hornej hranice uvedenej v pozorovaní, je, že niektoré netriviálne Schreierové generátory môžu byť zhodné pre rôzne $\gamma \in \Delta^{[i]}$ a $s \in S^{[i]}$. V nasledujúcej podkapitole popíšeme algoritmus, vďaka ktorému dokážeme určiť podstatne menšie množiny $S^{[i]}$.

2.4 Rozkladanie na súčin prvkov transverzály

Vďaka predchádzajúcemu dôsledku dokážeme určiť generujúcu množinu pre $G^{[i+1]}$ zo znalosti $S^{[i]}$. Po generujúcej množine $S^{[i+1]}$ pre $G^{[i+1]}$ požadujeme, aby bola čo najmenšia. Predtým, než vložíme niektorý zo Schrierových generátorov do $S^{[i+1]}$, skontrolujeme, či daný generátor negenerujú už vložené prvky v $S^{[i+1]}$. Inak povedané po každom vložení Schreierovho generátoru do $S^{[i+1]}$ sa grupa $\langle S^{[i+1]} \rangle$ zväčší aspoň dvojnásobne. Tým pádom vložíme maximálne $\log |G^{[i]}|$ Schreierových generátorov.

Predpokladajme, že pre permutačnú grupu $G \leq S_n$ poznáme nejakú jej bázu $B = (\beta_1, ...\beta_m)$ a príslušné transverzály $R^{[i]}$ pre $G^{[i]}/G^{[i+1]}$. Ukážeme, že každé $g \in G$ možno jednoznačne rozložiť na súčin prvkov transverzál, teda

$$g = r_m r_{m-1} ... r_1$$

kde $r_i := r_{i\gamma_i} \in R^{[i]}$ pre vhodné $\gamma_i \in \Delta^{[i]}$. Existencia a jednoznačnosť tohto rozkladu vyplýva m-násobnou aplikáciou nasledujúcej lemmy. Obdobná lemma je uvedená v práci od Murraya (1994, tvrdenie 2.5.1), postup pre rozklad je inšpirovaný prácou od Seressa (2003, str. 56).

Lemma 8. *Nech $G \leq S_n$ je permutačná grupa, $\beta \in \{1,...,n\}$, G_β je stabilizátor prvku β a R je pravá transverzála pre G/G_β. Potom pre každé $g \in G$ existuje práve jedno $r \in R$ také, že $\beta^r = \beta^g$. Navyše pre toto r platí, že $g = hr$ pre nejaké jednoznačne určené $h \in G_\beta$.*

Dôkaz. Z definície pravej transverzály, pre každé $g \in G$ platí $| R \cap G_\beta g | = 1$. Inak povedané, existujú jednoznačne určené $r \in R$ a $k \in G_\beta$ také, že $r = kg$. Označme $h := k^{-1}$. Dostávame $g = k^{-1}r = hr$. Navyše $\beta^g = \beta^{hr} = (\beta^h)^r = \beta^r$, lebo $h \in G_\beta$.

□

Postup, akým budeme hľadať rozklad pre $g \in G$ je nasledovný. Najprv nájdeme $r_1 \in R^{[1]}$ také, že $\beta_1^{r_1} = \beta_1^g$ a spočítame $g_2 := g r_1^{-1}$, pričom vďaka lemme $g_2 \in G^{[2]}$. V každom ďalšom kroku $i \leq m$ opäť hľadáme $r_i \in R^{[i]}$ také, že $\beta_i^{r_i} = \beta_i^{g_i}$ a spočítame $g_{i+1} := g_i r_i^{-1} \in G^{[i+1]}$. V poslednom kroku dostávame $g_{m+1} = 1$.

Uvedený postup možno zároveň použiť na testovanie toho, či dané $h \in S_n$ leží v grupe G. Pokiaľ by h v grupe G neležalo, môžu nastať dve situácie. Prvou je, že nedokážeme v niektorom kroku $i \leq m$ nájsť vhodné $r_i \in R^{[i]}$. To znamená, že $\beta_i^{h_i}$ pre $h_i = h r_1^{-1} r_2^{-1} ... r_{i-1}^{-1}$ sa nachádza mimo orbitu $\beta_i^{G^{[i]}}$. Druhou možnosťou je, že po m krokoch nám ostal netriviálny zvyšok $h_{m+1} \neq 1$.

Výstup $h \in S_n$ nasledujúceho algoritmu budeme nazývať *zvyšok*, význam výstupu $i \in \{1, ..., m+1\}$ ozrejmíme v nasledujúcej kapitole.

Vstup: $g \in S_n$, $B = (\beta_1,...,\beta_m)$ báza permutačnej grupy $G \leq S_n$,
$S = \cup_{i=1}^{m} S^{[i]}$ silne generujúca množina vzhľadom k B,
$\Delta^* = (\Delta^{[1]},...,\Delta^{[m]})$ fundamentálne orbity grupy G, postupnosť Schreierových vektorov $v = (v_1,..,v_m)$
Výstup: $h \in S_n, i \in \{1,...,m+1\}$
$h := g$;
for $i = 1, ..., m$ **do**
  $\gamma := \beta_i^h$;
  if $\gamma \notin \Delta^{[i]}$ **then**
    return h, i;
  end
  $r_{i\gamma}$:=PrvokTransverzály(γ, v_i, $S^{[i]}$);
  $h := h r_{i\gamma}^{-1}$;
end
return h, $m+1$

Algoritmus 4: Rozklad(g,B,S,v,Δ^*)

Algoritmus rozkladu je uvedený v knihe od Holta (2005, str. 89). Z poznatkov v tejto podkapitole takisto vyplýva, že pokiaľ poznáme prvky pravých transverzál $R^{[1]}$, ..., $R^{[m]}$, dokážeme vypísať všetky prvky grupy G.

2.4.1 Analógia s Gauss Jordanovou elimináciou

Algoritmus rozkladu možno považovať za analógiu Gauss Jordanovej eliminácie. Majme danú maticu $A = (a_{ij})_{m \times n}$ nad poľom T. Gauss Jordanová eliminácia vráti maticu

$$H = R_{i_k}^{-1} \cdot ... \cdot R_{i_1}^{-1} \cdot A$$

Indexy $i_1 < i_2 < ... < i_k$ sú z množiny $\{1, ..., \min\{m, n\}\}$ a určujú pozície pivotov. Matica $R_j^{-1} \in T^{m \times m}$ je pre každé $j = i_1, i_2, ..., i_k$ tvaru:

$$R_j^{-1} = \begin{pmatrix} 1 & 0 & \cdots & 0 & \frac{-a_{1,j}}{a_{j,j}} & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & \frac{-a_{2,j}}{a_{j,j}} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 1 & \frac{-a_{i-1,j}}{a_{j,j}} & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & \frac{1}{a_{j,j}} & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & \frac{-a_{j+1,j}}{a_{j,j}} & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \frac{-a_{m,j}}{a_{j,j}} & 0 & \cdots & 1 \end{pmatrix}$$

Jedná sa o maticu, ktorá je súčinom elementárnych matíc upravujúcich j-tý stĺpec.

Indexy pivotov $(i_1, ..., i_k)$ sú analógiou báze $(\beta_1,...,\beta_k)$ pre permutačnú grupu. Matice $R_{i_1}, R_{i_2},..., R_{i_k}$ sú analógiou prvkov $r_1 \in R^{[1]},...,r_k \in R^{[k]}$. Výraz

$$H = R_{i_k}^{-1} \cdot ... \cdot R_{i_1}^{-1} \cdot A$$

je analógiou pre

$$h = g \cdot r_1^{-1} \cdot r_2^{-1} \cdot ... \cdot r_k^{-1},$$

kde $g \in S_n$ je zadaná permutácia, h je zvyšok algoritmu ROZKLAD na vstupe g.

Za analógiu pre stabilizátory $G^{[j]} = G_{(\beta_1,\ldots,\beta_{j-1})}$ môžeme považovať grupu regulárnych matíc rádu m, ktoré majú v sĺpcoch s indexmi $i_1, i_2, ..., i_{j-1}$ po poradí jednotkové vektory $e_{i_1}, e_{i_2}, ..., e_{i_{j-1}}$. Analógiou pre $G^{[j]}/G^{[j+1]}$ bude grupa regulárnych matíc tvaru $(e_1 \,|\, \cdots \,|\, e_{j-1} \,|\, a \,|\, e_{j+1} |\, \cdots \,|\, e_m)$, kde $a \in T^m$. Do tejto grupy zrejme spadajú aj matice R_j.

3. Schreier Simsov algoritmus

Úlohou Schreier Simsovho algoritmu je nájsť neredundantnú bázu B a príslušnú silne generujúcu množinu S, pokiaľ je daná nejaká množina generátorov X permutačnej grupy G. Myšlienkou je nasledujúce tvrdenie a poznatky z predchádzajúcej kapitoly. Tvrdenie je ekvivalentné tvrdeniu 4.2.3 z knihy od Seressa (2003).

Tvrdenie 9. *Daná je permutačná grupa $G \leq S_n$, $m \in \mathbb{N}$, postupnosť $B = (\beta_1,...,\beta_m)$ prvkov z $\{1,...,n\}$, množina S permutácii z G taká, že $\langle S\rangle = G$. Označme $G^{[1]} = G, G^{[i]} = G_{\beta_1,...,\beta_{i-1}}$ a $S^{[i]} = S \cap G^{[i]}$ pre $i = 1,...,m$ a nech $S^{[m+1]} = \emptyset$. Potom (B,S) je BSGS práve vtedy, keď $\langle S^{[i]}\rangle_{\beta_i} = \langle S^{[i+1]}\rangle$ pre všetky $i = 1,...,m+1$.*

Dôkaz. Nech (B,S) je BSGS, potom pre všetky $i = 1,...,m$ platí $\langle S^{[i+1]}\rangle = G^{[i+1]} = G^{[i]}_{\beta_i} = \langle S^{[i]}\rangle_{\beta_i}$. Na dokázanie opačnej implikácie potrebujeme ukázať, že $G^{[i]} = \langle S \cap G^{[i]}\rangle$ pre každé $i = 1,...,m+1$. Pre $i = 1$ zrejme $G^{[1]} = G = \langle S\rangle = \langle S \cap G^{[1]}\rangle$. Predpokladajme, že $G^{[i]} = \langle S^{[i]}\rangle$, potom platí aj $G^{[i+1]} = G^{[i]}_{\beta_i} = \langle S^{[i]}\rangle_{\beta_i} = \langle S^{[i+1]}\rangle = \langle S \cap G^{[i+1]}\rangle$. Poznamenajme, že tretia rovnosť je z predpokladu implikácie v tvrdení. Navyše $\langle S^{[m+1]}\rangle = \langle\emptyset\rangle = 1 = G^{[m+1]}$. Tým sme dokázali, že ($B$,$S$) je BSGS pre G.

□

3.1 Čiastočná báza a čiastočná silne generujúca množina

Vstupom Schreier Simsovho algoritmu bude takzvaná *čiastočná báza* a *čiastočná silne generujúca množina*. Definujeme ich nasledovne.

Definícia 6. *(Murray, 1994, str. 25) Nech $m \in \mathbb{N}$, $G \leq S_n$ je permutačná grupa a množina X generuje G. Hovoríme, že postupnosť $B = (\beta_1, \beta_2, ..., \beta_m)$ prvkov z $\{1,...,n\}$ je* čiastočná báza *a množina S permutácií z G je* čiastočná silne generujúca množina *grupy G, pokiaľ $X \subseteq S$ a žiaden prvok z S nestabilizuje všetky prvky z B. Dvojicu (B,S) budeme nazývať* čiastočnou *BSGS.*

V tejto kapitole, narozdiel od predchádzajúcich dvoch kapitol, použijeme značenie pre $S^{[i]} := S \cap G^{[i]}$, $\Delta^{[i]} := \beta_i^{\langle S^{[i]}\rangle}$ a $R^{[i]}$ vzhľadom k čiastočnej silne generujúcej množine S a čiastočnej báze B. Množinu $R^{[i]}$ definujeme ako množinu jednoznačne určených prvkov $r_{i\gamma} \in \langle S^{[i]}\rangle$ pre každé $\gamma \in \Delta^{[i]}$, spĺňajúcich $\beta_i^{r_{i\gamma}} = \gamma$. Poznamenajme, že $R^{[i]}$ je iba podmnožinou transverzály pre $\langle S^{[i]}\rangle/\langle S^{[i+1]}\rangle$. Index $i \in \mathbb{N}$ vzhľadom k značeniam vyššie budeme nazývať *úrovňou*.

Poslednú podmienku z definície môžeme tiež prepísať ako:

$$S^{[m+1]} = S \cap G_{(\beta_1,...,\beta_m)} = \emptyset$$

Navyše $\langle S\rangle = G$, keďže $X \subseteq S$ a $S \subseteq G$. Teda čiastočná báza a čiastočná silne generujúca množina spĺňajú predpoklady tvrdenia 9.

Schreier Simsov algoritmus postupným pridávaním prvkov rozšíri čiastočnú bázu a čiastočnú silne generujúcu množinou na bázu a silne generujúcu množinu tak, ako sú definované v kapitole 1. Prvky do čiastočnej bázy sú pridávané na koniec tejto postupnosti. Bázu a silne generujúcu množinu budeme v nasledujúcom texte tiež nazývať *úplnou bázou* a *úplnou silne generujúcou množinou*, z dôvodu lepšieho odlíšenia od predchádzajúcej definície.

Nasledujúci algoritmus priamočiaro nájde čiastočnú bázu B pre čiastočnú silne generujúcu množinu $S := X$, kde X je zadaná generujúca množina pre permutačnú grupu G. Pre nájdenú čiastočná BSGS platí, že $\langle S^{[i+1]} \rangle$ je vlastnou podgrupou $\langle S^{[i]} \rangle$ pre všetky $i = 1, ..., m$, vďaka čomu ju možno rozšíriť na neredundantnú bázu. Zabezpečuje to podmienka $\beta^x \neq \beta$ v algoritme.

Z technických dôvodov zaveďme nasledujúce značenie:

$$S^* := (S^{[1]}, ..., S^{[m]})$$

Rovnako zaveďme procedúru Append($\sim M$,x), ktorá má za úlohu vložiť na koniec postupnosti M prvok x, teda veľkosť M sa zväčší o jedna a posledným prvkom bude x. Znak „$\sim$“ pred množinou M značí prenášanie referenciou. Algoritmus je inšpirovaný časťou algoritmu uvedenom v knihe od Holta a kol. (2005, str. 91).

Vstup: neprázdna množina $X \subseteq S_n$, kde $G = \langle X \rangle$
Výstup: čiastočná báza $B = (\beta_1, ..., \beta_m)$ grupy G, ktorej čiastočná silne generujúca množina je $S := X$, a postupnosť $S^* = (S^{[1]}, ..., S^{[m]})$ reprezentujúca čiastočnú SGS $S = \cup_{i=1}^{m} S^{[i]}$

```
m := 0;
B := ∅;
for x ∈ X do
    if x ∈ G_(β_1,...,β_m) then
        for β = 1, ..., n do
            if β^x ≠ β then
                β_{m+1} := β;
                Append(~ B, β_{m+1});
                m := m + 1;
                S^[m] := X ∩ G_(β_1,...,β_{m-1});
                break;
            end
        end
    end
end
S* := (S^[1], ..., S^[m]);
return B, S*;
```

Algoritmus 5: CiastocnaBSGS(X)

3.2 Schreier Simsov algoritmus

Z tvrdenia 9 vyplýva, že čiastočná BSGS je úplnou BSGS, pokiaľ pre všetky $i = 1, ..., m + 1$ platí:

$$\langle S^{[i]} \rangle_{\beta_i} = \langle S^{[i+1]} \rangle$$

Zrejme vždy platí $\langle S^{[i]} \rangle_{\beta_i} \geq \langle S^{[i+1]} \rangle$, ostáva zabezpečiť aby $\langle S^{[i]} \rangle_{\beta_i} \leq \langle S^{[i+1]} \rangle$. Vďaka Schreierovej lemme vieme, že grupa $\langle S^{[i]} \rangle_{\beta_i}$ je generovaná Schreierovými generátormi. Zvolíme netriviálny Schreierov generátor g. Pomocou algoritmu ROZKLAD otestujeme, či daný Schreierov generátor g patrí grupe $\langle S^{[i+1]} \rangle$, teda či algoritmus vráti triviálny zvyšok. Pokiaľ nie, tak jeho netriviálny zvyšok h vložíme do množiny $S^{[i+1]}$. Vložením zvyšku sa narušia rovnosti medzi $\langle S^{[j]} \rangle_{\beta_j}$ a $\langle S^{[j+1]} \rangle$ pre $j = i+1, i+2, ..., l$, kde l je úroveň, ktorú vrátil algoritmus ROZKLAD.

Pre zvyšok h Schreierovho generátoru g zrejme platí:

$$\langle S^{[i+1]} \cup g \rangle = \langle S^{[i+1]} \cup h \rangle$$

Rovnosť medzi $\langle S^{[i]} \rangle_{\beta_i}$ a $\langle S^{[i+1]} \rangle$ nastane, pokiaľ netriviálne zvyšky všetkých Schreierových generátorov boli vložené do S.

Algoritmus ROZKLAD je možné na grupu $\langle S^{[i+1]} \rangle$ aplikovať, iba ak poznáme úplnú BSGS pre $\langle S^{[i+1]} \rangle$. Z tejto znalosti potom dokážeme spočítať príslušné pravé transverzály $R^{[j]}$ pre $G^{[j]}/G^{[j+1]}$, kde pre $j = i, ..., m$.

Definícia 7. *Nech $B = (\beta_1, ..., \beta_m)$ je čiastočná báza permutačnej grupy $G \leq S_n$, $S \subseteq G$ je čiastočná silne generujúca množiny grupy G vzhľadom k B, kde $i \in \{1, ..., m\}$. Hovoríme, že čiastočná BSGS (B,S) je* pod úrovňou i, *pokiaľ buď $i = m$ alebo pre všetky $j = i+1, ..., m$ platí*

$$\langle S^{[j]} \rangle_{\beta_j} = \langle S^{[j+1]} \rangle.$$

Pojem pod úrovňou zaviedol Seress (2003) vo svojej knihe na strane 59. Táto definícia inak hovorí to, že dvojica $((\beta_{i+1}, ..., \beta_m), \cup_{j=i+1}^{m} S^{[j]})$ je úplnou BSGS pre permutačnú grupu $\langle S^{[i+1]} \rangle$.

V priebehe Schreier Simsovho algoritmu sme stále na tej úrovni, pod ktorou sa nachádza aktuálna BSGS. Triviálne sme vždy pod úrovňou m, začneme teda na nej a postupujeme k nižším úrovniam. Ak sa nachádzame na nejakej úrovni i, otestujeme, či všetky Schreierové generátory ležia v $\langle S^{[i+1]} \rangle$. Pokiaľ áno, postupujeme na úroveň $i-1$, v opačnom prípade vložíme prvý nájdený netriviálny zvyšok do $S^{[i+1]}, ..., S^{[l]}$ a postupne prejdeme na úrovne l, ..., $i+1$, kde l je úroveň, ktorú vrátil algoritmus ROZKLAD. Navyše pokiaľ $l = m+1$, teda keď platí $\beta_j^h = \beta_j$ pre každé $j = i+1, ..., m$, nájdeme nový bázový prvok β_{m+1} taký, že $\beta_{m+1}^h \neq \beta_{m+1}$, a vložíme ho na koniec čiastočnej báze. Uvedená podmienka pre β_{m+1} zabezpečí, že báza na konci algoritmu je neredundantná. Algoritmus skončí, pokiaľ sa dostaneme na úroveň 0, vtedy bude splnená podmienka z tvrdenia 9. To zrejme nastane, keďže pre každú úroveň existuje konečne veľa Schreierových generátorov.

Počas toho ako vkladáme netriviálny zvyšok do $S^{[i+1]}, ..., S^{[l]}$, potrebujeme prepočítať odpovedajúce orbity a Schreierové vektory. Prvky, ktoré boli súčasťou orbity pred vložením tohto zvyšku, ostanú jej súčasťou naďalej. To isté platí pre odpovedajúce permutácie určené Schreierovým vektorom. Pokiaľ by sme použili algoritmus ORBITASCHREIERVEKTOR tak, ako bol uvedený, spočítal by uvedené prvky nanovo. Nasledujúci algoritmus zabezpečí, aby v priebehu celého Schreier Simsovho algoritmu bol pre ľubovoľnú úroveň i každý prvok orbity $\Delta^{[i]}$ a odpovedajúci prvok Schreierového vektoru v_i spočítaný iba raz.

Vstup: $\beta_i \in B$, kde B je čiastočná báza $G \leq S_n$,
$S^{[i]} = \{s_{i1},...,s_{ik_{i-1}}, s_{ik_i}\}$, $s_{i1},...s_{ik_i} \in S_n$, $\Delta^{[i]}$ a v_i sú orbita a Schreierov vektor pre prvok β_i vzhľadom k $\{s_{i1},...s_{ik_{i-1}}\}$
Výstup: rozšírená orbita $\Delta^{[i]}$ a rozšírený Schreierov vektor v_i pre β_i vzhľadom k $S^{[i]}$

```
Δ' := ∅;
for γ ∈ Δ[i] do
    if γ^{s_{ik_i}} ∉ Δ[i] then
        Δ' := Δ' ∪ {γ^{s_{ik_i}}};
        v_i[γ^{s_{ik_i}}] := k_i;
    end
end
for γ ∈ Δ' do
    for j = 1,...,k_i do
        if γ^{s_ij} ∉ (Δ[i] ∪ Δ') then
            Δ' := Δ' ∪ {γ^{s_ij}};
            v_i[γ^{s_ij}] := j;
        end
    end
end
Δ[i] := Δ[i] ∪ Δ';
return Δ[i],v_i;
```

Algoritmus 6: RozsirOrbitaSchreierVektor($\beta_i, S^{[i]}, \Delta^{[i]}, v_i$)

Schreier Simsov algoritmus implementujeme ako rekurzívnu procedúru SchreierSims, ktorú voláme v hlavnom algoritme Main postupne od poslednej úrovne až po prvú. Po ukončení jedného takého volania dostaneme rozšírenú čiastočnú BSGS, ktorá je pod úrovňou o jeden nižšie ako čiastočná BSGS na vstupe.

Pred uvedením pseudokódu najprv vylepšíme algoritmus tak, aby bol každý Schreierov generátor testovaný iba raz. Zabezpečia to parametre old_Δ^* a T, kde $old\_\Delta^* = (old\_\Delta^{[1]}, ..., old\_\Delta^{[m]})$ predstavuje postupnosť fundamentálnych orbít pre predchádzajúce volanie procedúry SchreierSims a $T \subseteq S^{[i]}$ je množinou tých generátorov z $S^{[i]}$, ktoré neboli súčasťou $S^{[i]}$ v predchádzajúcom volaní. Pokiaľ sa v priebehu volaní rekurzie dostaneme na úroveň i, na ktorej sme už boli, otestujeme len tie Schreierové generátory, ktoré nevznikli z $old\_\Delta^{[i]}$ a $S^{[i]} \setminus T$. Takto dokážeme znížiť časovú zložitosť. K množinám $S^{[i]} = \{s_{i1}, ..., s_{ik_i}\}$ pristupujme ako k postupnostiam, ktoré sú určené indexmi prvkov množín, teda predpokladajme, že môžme na ne aplikovať procedúru Append. Nasledujúce dva pseudokódy sú inšpirované pseudokódom od Butlera (1991, str. 138, 138) a od Holta a kol. (2005, str. 91), spresnené o detaily.

Vstup: $B = (\beta_1,...,\beta_m)$ čiastočná báza, $S = \cup_{i=1}^{k} S^{[i]}$ čiastočná silne generujúca množina, pričom (B,S) je momentálne pod úrovňou i, Δ^* fundamentálne orbity, v Schreirové vektory, old_Δ^*, T definované ako vyššie

for $\gamma \in \Delta^{[i]}$ **do**
  if $\gamma \in old\_\Delta^{[i]}$ **then**
    $generatory := T$;
  end
  else
    $generatory := S^{[i]}$;
  end
  $old\_\Delta^* := \Delta^*$;
  $r_{i\gamma}$:=PrvokTransverzaly(γ,v_i,$S^{[i]}$);
  for $s \in generatory$ **do**
    $r_{i\gamma^s}$:=PrvokTransverzaly(γ^s,v_i,$S^{[i]}$);
    $g := r_{i\gamma} s (r_{i\gamma^s})^{-1}$;
    if $g \neq id$ **then**
      h,l := Rozklad(g, $(\beta_{i+1}, ..., \beta_m)$, $\cup_{j=1}^{m} S^{[j]}$, $(v_{i+1},..,v_m)$, $(\Delta^{[i+1]},...,\Delta^{[m]})$);
      if $h \neq id$ **then**
        if $l = m+1$ **then**
          nájdeme β_{m+1} také, že $\beta_{m+1}^h \neq \beta_{m+1}$;
          Append($\sim B$,β_{m+1});
          $S^{[m+1]} := \emptyset$;
          $\Delta^{[m+1]} := \{\beta_{m+1}\}$;
          for $\alpha = 1,...,n$ **do**
            $v_{m+1}[\alpha] := 0$;
          end
          $v_{m+1}[\beta_{m+1}] := -1$;
          Append($\sim S^*, S^{[m+1]}$);
          Append($\sim \Delta^*, \Delta^{[m+1]}$);
          Append($\sim v, v_{m+1}$);
          $m := m+1$;
        end
        for $j = l,..,i+1$ **do**
          Append($\sim S^{[l]}, h$);
          $\Delta^{[l]}, v_l$:=RozsirOrbitaSchreierVektor(β_l,$S^{[l]}$);
        end
        for $j = l,..,i+1$ **do**
          SchreierSims ($\sim B, \sim S^*, \sim \Delta^*, \sim v, j, old\_\Delta^*, \{h\}$);
        end
      end
    end
  end
end

Algoritmus 7: SchreierSims $(\sim B, \sim S^*, \sim \Delta^*, \sim v, i, old\_\Delta^*, T)$

Vstup: neprázdna množina permutácii X, kde $G = \langle X \rangle \leq S_n$
Výstup: (B,S) BSGS pre G
$B, S^* :=$ CiastocnaBSGS(X);
for $i = 1, ..., m$ **do**
  $\Delta^{[i]}, v_i :=$ OrbitaSchreierVektor $(\beta_i, S^{[i]})$;
end
$\Delta^* := (\Delta^{[1]}, ..., \Delta^{[m]})$;
$v := (v_1, ..., v_m)$;
for $i = m$,...,1 **do**
  SchreierSims$(B, S^*, \Delta^*, v, i, \emptyset, S^{[i]})$;
end
$S := \cup_{i=1}^{m} S^{[i]}$;
return (B, S);

Algoritmus 8: Main(X)

Poznamenajme, že priebehu algoritmu neplatí $S^{[i]} = S \cap G^{[i]}$. Nové generátory pridávame iba do $S^{[j]}$ pre $j = i + 1, ..., l$, kde $l \geq i$, namiesto toho, aby sme ich pridali aj do $S^{[1]}$, ... ,$S^{[i]}$. Dôvodom je, že tieto generátory by následne v grupe $\langle S^{[i]} \rangle$ boli nadbytočné, t.j. ich pridaním by sa grupy $\langle S^{[1]} \rangle$, ... ,$\langle S^{[i]} \rangle$ nezmenili, iba by sa zbytočne navýšil čas potrebný pre výpočet.

3.3 Časová a priestorová zložitosť Schreier Simsovho algoritmu

Časovú a priestorovú zložitosť budeme počítať podobným spôsobom ako je uvedené v knihe od Seressa (2003, str. 60 – 62), avšak vzhľadom k pseudokódom algoritmov vyššie. V tejto podkapitole využijeme vylepšenie z cvičenia 4.4 (Seress, 2003, cvičenie 4.4). Ako bolo už spomenuté, každý Schreierov generátor je testovaný práve raz. Od toho budeme odvíjať aj určovanie časovej zložitosti. Podľa dôsledku 3, báza je veľkosti maximálne $\log |G|$. Pokiaľ $\log |G| \geq n$, veľkosť báze je maximálne n, keďže výstupom je neredundantná báza. V tejto podkapitole budeme používať odhad $|B| \in \mathcal{O}(\log |G|)$. Veľkosť každej orbity je maximálne n, špeciálne pre konkrétne i je veľkosť orbity $\Delta^{[i]}$ maximálne $n - i + 1$. Pre zvolený prvok bázy β_i sa $S^{[i]}$ zväčší maximálne $\log |G^{[i]}|$ krát, keďže vďaka použitiu algoritmu Rozklad a podmienke $h \neq id$ sa grupa $\langle S^{[i]} \rangle$ musí každým pridaním prvku do $S^{[i]}$ aspoň dvojnásobne zväčšiť. Veľkosť ľubovoľnej $S^{[i]}$ je teda maximálne $|X| + \log |G^{[i]}|$.

Úpravou algoritmu Main môžeme tento odhad znížiť na $\log |G^{[i]}|$. Časovú a priestorovú zložitosť následne spočítame vzhľadom k tejto úprave. Stačí ak si predstavíme, že grupa G pôsobí na množine $\{1, ..., n + 1\}$ namiesto $\{1, ..., n\}$ a za nultý prvok báze zvolíme $n + 1$. . Konkrétne definujme $\beta_0 := n + 1$, $S^{[0]} := X$ a spustíme algoritmus SchreierSims pre $B = (\beta_0)$, $S = (S^{[0]})$, $i = 0$ a ostatné odpovedajúce parametre, pričom zrejme orbita $\Delta^{[0]}$ je triviálna. Aj keď dvojica $(n + 1, X)$ síce nespĺňa definíciu čiastočnej BSGS, nám to neprekáža, keďže pre náš účel môže platiť $G = G_{\beta_0}$. Hľadanou silne generujúcou množinou bude opäť $S := \cup_{i=1}^{m} S^{[i]}$. Ďalej uvažujme $|S^{[i]}| \in \mathcal{O}(\log |G|)$. Tým pádom dostávame, že $|S| \leq \sum_{i=1}^{m} |S^{[i]}| \in \mathcal{O}(\log^2 |G|)$.

Algoritmus PrvokTransverzaly pracuje v čase $\mathcal{O}(n^2)$, pretože na spočítanie prvku transverzály zo Schreierovho vektoru zložíme maximálne n permutácii, pričom každé jedno zloženie je v čase $\mathcal{O}(n)$. Algoritmus OrbitaSchreierVektor a RozsirOrbitaSchreierVektor pracujú v čase $|\Delta^{[i]}||S^{[i]}|$ pre dané $1 \leq i \leq m$, čo je $\mathcal{O}(n \log |G|)$. Algoritmus Rozklad pracuje v čase $\mathcal{O}(n^2 \log |G|)$. Ešte poznamenajme, že skladanie permutácií, určenie inverznej permutácie, porovnanie dvoch permutácii, hľadanie prvku nestabilizovaným danou permutáciu a určenie, či nejaký prvok patrí orbite je v čase $\mathcal{O}(n)$, čo je menej ako časová zložitosť predchádzajúcich štyroch algoritmov v tomto odseku.

Počet Schreierových generátorov, vrátane tých na úrovni 0, je maximálne $\sum_{i=0}^{m} |\Delta^{[i]}||S^{[i]}| = 1 \cdot |X| + \sum_{i=1}^{m} |\Delta^{[i]}||S^{[i]}| \in \mathcal{O}(|X| + n \log^2 |G|)$. Pozrime sa bližšie na pseudokód procedúry SchreierSims. Počas toho ako počítame jeden Schreierov generátor, potrebujeme spočítať maximálne dvakrát PrvokTransverzaly, jeden Rozklad a maximálne $\log(|G|)$ krát RozsirOrbitaSchreierVektor. Zvyšok je zanedbateľný. Ako bolo spomenuté v predchádzajúcej podkapitole pomocou algoritmu RozsirOrbitaSchreierVektor je každý prvok orbity $\Delta^{[i]}$ a odpovedajúci prvok Schreierového vektoru v_i na každej úrovni i spočítaný iba raz. Tým pádom v priebehu celého Schreier Simsovho algoritmu spočítame všetky fundamentálne orbity a Schreierové vektory v čase $\mathcal{O}(n \log^2 |G|)$.

Keďže každý Schreierov generátor je spočítaný iba raz, dostávame časovú zložitosť $\mathcal{O}((|X| + n \log^2 |G|)(n^2 + n^2 \log |G|) + n \log^2 |G|)$, čo je

$$\mathcal{O}(|X| n^2 \log |G| + n^3 \log^3 |G|).$$

Čo sa týka priestorovej zložitosti, tak $\sum_{i=0}^{m} |S^{[i]}| \in \mathcal{O}(|X| + \log^2 |G|)$, a keďže sú to permutácie, na ich uloženie potrebujeme $\mathcal{O}(|X| n + n \log^2 |G|)$ pamäte. Ďalej $|B| \in \mathcal{O}(\log |G|)$, $|old\_\Delta^*|$,$|\Delta^*| \in \mathcal{O}(n \log |G|)$, $|v| \in \mathcal{O}(n \log |G|)$, čo odpovedá aj pamäťovej zložitosti. Pre parameter T platí $|T| = |S^{[i]}|$ alebo $|T| = 1$, a teda na jeho uloženie potrebujeme $\mathcal{O}(n \log |G|)$ pamäte. Celkovo dostávame priestorovú zložitosť

$$\mathcal{O}(|X| n + n \log^2 |G|).$$

Poznatky, ktoré sme v tejto podkapitole dokázali, zhrnieme v následujúcom tvrdení.

Tvrdenie 10. *Nech $G = \langle X \rangle \leq S_n$ je permutačná grupa, kde X je generujúca množina pre G, $n \in \mathbb{N}$. Potom existuje deterministický algoritmus, ktorý nájde neredundantnú bázu a príslušnú silne generujúcu množinu v čase $\mathcal{O}(|X| n^2 \log |G| + n^3 \log^3 |G|)$ s priestorovou náročnosťou $\mathcal{O}(|X| n + n \log^2 |G|)$.*

4. Monte Carlo Schreier Simsov algoritmus

Vzhľadom k dôležitosti znalosti báze a silne generujúcej množiny je našou snahou spočítať BSGS v čo najlepšom čase a to aj za cenu toho, že algoritmus nie vždy vráti správny výsledok.

V tejto kapitole predstavíme *pravdepodobnostný Monte Carlo algoritmus*, ktorého časová zložitosť je *skoro lineárna*. Pravdepodobnostný algoritmus je taký, ktorý využíva náhodný generátor čísel počas svojho chodu. Monte Carlo algoritmus je pravdepodobnostný algoritmus, ktorý môže v niektorých prípadoch vrátiť nesprávny výsledok. Pravdepodobnosť, že Monte Carlo algoritmus vráti nesprávny výsledok je ale menej ako polovica. Časová zložitosť algoritmu pre permutačnú grupu $G = \langle X \rangle \leq S_n$ je skoro lineárna, pokiaľ algoritmus prebehne v čase $\mathcal{O}(n|X|\log^k n)$ pre $k > 0$. Algortimus z tejto kapitoly je vylepšením Schreier Simsovho algoritmu uvedeného v predchádzajúcej kapitole.

4.1 Plytké Schreierové stromy

Jedným z faktorov pridávajúcom na časovej zložitosti Schreier Simsovho algoritmu, je hĺbka Schreierovho stromu. Tá môže byť veľkosti až $n-1$, napríklad pre Schreierov strom vzhľadom ku generujúcej množine $\{(1\ 2\ ...\ n)\}$. Avšak pre veľkú časť grúp a ich generujúcich množín bude táto hĺbka značne menšia.

Uvedieme dva algoritmy, ktorých výstupom bude Schreierov strom s obmedzenou hĺbkou, tzv. *plytký Schreierov strom*. Prvým bude deterministický algoritmus z článku od Babaia, Coopermana, Finkelsteina a Seressa (Babai a kol., 1991), uvedený v oddieli 4.1.1, ktorý vráti Schreierov strom hĺbky $\mathcal{O}(\log|G|)$. Druhým bude pravdepodobnostný Monte Carlo algoritmus z článku od Coopermana, Finkelsteina a Sawaragiho (Cooperman a kol., 1990), uvedený v oddieli 4.1.2, ktorý vráti Schreierov strom hĺbky $\mathcal{O}(\log n)$, konkrétne $\mathcal{O}(\log|\beta^G|)$ pre G/G_β. Oba algoritmy sú tiež popísané v knihe od Seressa (2003, podkapitola 4.4). Oba oddiely sú doplnené o pseudokódy potrebných algoritmov. Poznamenajme, že druhý z uvedených algoritmov môžeme využiť iba v prípade, ak máme k dispozícii náhodné prvky grupy G z rovnomerného rozdelenia.

4.1.1 Deterministický algoritmus pre plytké Schreierové stromy

Nasledujúca definícia je z práce od Babaia a kol. (1991, str. 202).

Definícia 8. *Nech* $R = (g_1,g_2,...,g_k)$ *je postupnosť prvkov grupy* $G \leq S_n$. *Potom*

$$C(R) := C(g_1,g_2,...,g_k) = \{g_1^{e_1}g_2^{e_2}...g_k^{e_k} \mid e_1,e_2,...,e_k \in \{0,1\}\}$$

nazveme kockou *pre postupnosť* $(g_1,g_2,...,g_k)$. *Ďalej označme:*

$$C^{-1}(R) := \{g \in G \mid g^{-1} \in C(R)\}$$

Hovoríme, že $C(R)$ *je* nedegenerovaná, *pokiaľ* $|C(R)| = 2^k$.

Poznamenajme, že $C(R)$ je podmnožinou grupy G, ale nie nutne podgrupou. Myšlienka algoritmu pre plytké Schreierové stromy je založená na konštrukcii čo najväčšej postupnosti prvkov permutačnej grupy, ktorých kocka je nedegenerovaná, pokiaľ máme k dispozícii nejakú generujúcu množinu danej grupy. Konštrukciu takejto kocky nám zaručí niekoľkonásobne aplikovanie nasledujúceho pozorovania.

Pozorovanie je opäť z práce od Babaia a kol. (1991, pozorovanie 2.1).

Pozorovanie 11. *Nech* $(g_1,...,g_k, g_{k+1})$ *je postupnosť prvkov grupy* $G \leq S_n$ *a nech* $C_k := C(g_1,...,g_k)$, $C_{k+1} := C(g_1,...,g_k, g_{k+1})$. *Potom* C_{k+1} *je nedegenerovaná práve vtedy, keď* C_k *je nedegenererovaná a* $g_{k+1} \notin C_k^{-1}C_k$.

Dôkaz. Zrejme C_{k+1} je nedegenerovaná práve vtedy, keď C_k je nedegenerovaná a $|C_{k+1}| = 2|C_k|$. Táto rovnosť nastane vtedy, keď $C_k g_{k+1} \cap C_k = \emptyset$. To znamená, že neexistujú $g,h \in C_k$ také, že $gg_{k+1} = h$, t.j. $g_{k+1} = g^{-1}h$. Inak povedané, keď $g_{k+1} \notin C_k^{-1}C_k$.

□

Testovanie, či g_{k+1} patrí $C_k^{-1}C_k$, je náročné. Platí ale nasledovné pre ľubovoľné $\beta \in \{1, ..., n\}$:

$$\beta^{g_{k+1}} \notin \beta^{C_k^{-1}C_k} \implies g_{k+1} \notin C_k^{-1}C_k$$

To nás vedie k zavedeniu pojmu *monotónneho Schreierového stromu*, využívaného v práci od Babaia a kol. (1991), ktorého vrcholy sú práve prvky $\beta^{C_k^{-1}C_k}$.

Definícia 9. *Nech* $R = (g_1, ..., g_k)$ *je postupnosť prvkov grupy* $G \leq S_n$ *a nech* $\beta \in \{1, ..., n\}$. Monotónnym Schreierovým stromom *pre prvok* β *vzhľadom k* R *nazveme zakorenený orientovaný strom, ktorého každá hrana je orientovaná smerom od koreňa* β. *Vrcholmi sú prvky množiny* $\beta^{C^{-1}(R)C(R)} = \{\beta^h \mid h \in C^{-1}(R)C(R)\}$. *Hrany sú označené permutáciami z množiny* $\{g_1,...,g_k, g_1^{-1},...,g_k^{-1}\}$. *Označenia na ceste z koreňa* β *do ľubovoľného vrcholu* γ *tvoria slovo tvaru* $g_k^{e'_k}...g_1^{e'_1}g_1^{e_1}...g_k^{e_k}$, *kde* $e'_i \in \{-1,0\}, e_i \in \{0,1\}$ *pre všetky* $i \in \{1,...,k\}$.

Z definície je zrejme, že každý prvok transverzály pre ľubovoľný monotónny Schreierov strom vzhľadom k R je prvkom množiny $C^{-1}(R)C(R)$.

Pozorovanie 12. *Nech* $G \leq S_n$, $k \in \mathbb{N}$, $g_1,...,g_k \in G$. *Hĺbka monotónneho Schreierovho stromu vzhľadom k* $R = (g_1,...,g_k)$ *je maximálne* $2\log|G|$.

Dôkaz. Monotónny Schreierov strom je hĺbky maximálne $2k$ a súčasne platí $|C(R)| \leq 2^k \leq |G|$, t.j. $k \leq \log|G|$.

□

Obdobne ako v kapitole 2 monotónny Schreierov strom bude reprezentovať *monotónny Schreierov vektor*. Vzhľadom k nasledujúcej definícii označme hodnotu $v_i[\beta_i]$ ako ∞, pričom tým rozumieme pevne zvolené prirodzené číslo, ktoré bude vždy väčšie ako k. Táto definícia sa vzťahuje k algoritmu, ktorý je uvedený za ňou.

Definícia 10. Monotónnym Schreierovým vektorom *pre prvok* β_i *vzhľadom k postupnosti* $R = (g_1, g_2, ..., g_k)$ *prvkov grupy* $G^{[i]}$ *nazveme pole* v_i *dĺžky* n, *pre ktoré platí:*

- $v_i[\beta_i] := \infty$
- $v_i[\delta] := j$, *pokiaľ v algoritme* OrbitaMonotonnySchreierVektor *bolo* $\delta \in \beta_i^{C^{-1}(R)C(R)} \setminus \{\beta_i\}$ *vložené ako* γ^{g_j}
- $v_i[\delta] := -j$, *pokiaľ v algoritme* OrbitaMonotonnySchreierVektor *bolo* $\delta \in \beta_i^{C^{-1}(R)C(R)} \setminus \{\beta_i\}$ *vložené ako* $\gamma^{g_j^{-1}}$
- $v_i[\alpha] := 0$ *pre* $\alpha \notin \beta_i^{C^{-1}(R)C(R)}$

Nasledujúci algoritmus nájde monotónny Schreierov vektor pre β_i vzhľadom k R, postupnosti prvkov z $G^{[i]}$. Algoritmus Index vráti index j, prípadne $-j$, tak, ako je to uvedené v definícii. Časová zložitosť algoritmu OrbitaMonotonnySchreierVektor je $\mathcal{O}(n|R|)$.

Vstup: $R = (g_1,g_2,...,g_k)$ je postupnosť prvkov grupy $G^{[i]} \leq S_n$,
$\beta_i \in \{1,...,n\}$ prvok báze B grupy G
Výstup: množina $\beta_i^{C^{-1}(R)C(R)}$, v_i monotónny Schreierov vektor pre β_i vzhľadom k R

```
Δ := {β_i};
for α = 1,...,n do
    v_i[α] := 0;
end
v_i[β_i] := ∞;
for g ∈ (g_k^{-1}, ..., g_1^{-1}, g_1, ..., g_k) do
    Δ' := Δ;
    for γ ∈ Δ do
        if γ^g ∉ Δ' then
            Δ' := Δ' ∪ {γ^g};
            v_i[γ^g] := Index(g);
        end
    end
    Δ := Δ';
end
return Δ, v_i;
```

Algoritmus 9: OrbitaMonotonnySchreierVektor(R, β_i)

Vráťme sa späť k pozorovaniu 11. Nasledujúci algoritmus pre dané $(g_1, ..., g_k)$, ktorého kocka $C_k := C(g_1, ..., g_k)$ je nedegenerovaná, nájde g_{k+1}, pre ktoré kocka $C_{k+1} := C(g_1, ..., g_k, g_{k+1})$ bude takisto nedegenerovaná. Využijeme, že ak pre dané $\beta \in \{1,...,n\}$ platí $\beta^{g_{k+1}} \notin \beta^{C_k^{-1}C_k}$,potom aj $g_{k+1} \notin C_k^{-1}C_k$. Nech algoritmus Cesta je analógiou algoritmu PrvokTransverzaly z kapitoly 2 pre monotónny Schreierov vektor.

Vstup: $R = (g_1,...,g_k)$ postupnosť prvkov $G^{[i]}$, $s \in G^{[i]}$, $\beta_i \in \{1,...,n\}$, $\Delta = \beta_i^{C(R)^{-1}C(R)}$, v_i monotónny Schreierov vektor pre β_i vzhľadom k R, boolovská premenná $existuje$

Výstup: buď pôvodné parametre $R,\Delta, v_i,existuje$ ako na vstupe, alebo ak existuje $\gamma^s \notin \beta_i^{C(R)^{-1}C(R)}$, vráti $R' = (g_1,...,g_k, g_{k+1})$ také, že $s \in R'$ a $|C(R')| = 2|C(R)|$, monotónny Schreierov vektor v_i pre β_i vzhľadom k R' a $existuje$ s hodnotou $true$

```
for γ ∈ Δ do
    if γ^s ∉ Δ then
        g_{k+1} := Cesta(γ, v_i, R) · s;
        Append(~R, g_{k+1});
        Δ, v_i := OrbitaMonotonnySchreierVektor(R, β_i);
        existuje := true;
        return R, Δ, v_i, existuje;
    end
end
return R, Δ, v_i, existuje;
```

Algoritmus 10: ZdvojnasobKocku$(R, \Delta, v_i, s, \beta_i)$

Algoritmus Zdvojnásob kocku je detailnejším popisom algoritmu uvedenom v práci od Babaia a kol. (1991, str. 203). V závere oddielu sa dostávame ku algoritmu, ktorý vráti monotónny Schreierov vektor pre prvok β_i bázy grupy G vzhľadom k takej postupnosti R prvkov grupy $\langle S^{[i]} \rangle$, že platí

$$\beta_i^{C(R)^{-1}C(R)} = \beta_i^{\langle S^{[i]} \rangle}.$$

Na začiatku algoritmu majme triviálny Schreierov vektor a prázdnu postupnosť R. Kým existuje $s \in S^{[i]}$, pre ktoré platí $\beta_i^{C(R)^{-1}C(R)s} \neq \beta_i^{C(R)^{-1}C(R)}$, pokračujeme ako v algoritme ZdvojnasobKocku pre odpovedajúce parametre. Pokiaľ takýto prvok neexistuje, algoritmus skončí, čo znamená, že bola prehľadaná celá orbita $\beta_i^{\langle S^{[i]} \rangle}$.

Vstup: $\beta_i \in B$, kde B je báza $G \leq S_n$, $S^{[i]} \subseteq G^{[i]}$
Výstup: fundamentálna orbita $\beta_i^{C(R)^{-1}C(R)} = \beta_i^{\langle S^{[i]} \rangle}$, monotónny Schreierov vektor v_i pre β_i vzhľadom k R

```
existuje := true;
R := ∅;
for α = 1,...,n do
    v_i[α] := 0;
end
v_i[β_i] := −1;
Δ := {β_i};
while existuje do
    existuje := false;
    for s ∈ S^[i] do
        R, Δ, v_i, existuje :=
          ZdvojnasobKocku(R, Δ, v_i, s, β_i, existuje);
    end
end
return Δ, v_i;
```

Algoritmus 11: OrbitaPlytkySchreierVektor$(\beta_i, S^{[i]})$

Algoritmus OrbitaPlytkySchreierVektor vyplýva z dôkazu lemmy 2.2 z práce od Babaia a kol. (1991, lemma 2.2), rovnako ako aj nasledujúce tvrdenie.

Tvrdenie 13. *Časová zložitosť algoritmu* OrbitaPlytkySchreierVektor *je* $\mathcal{O}(n \log^2 |G| + n|S^{[i]}|)$.

Dôkaz. Pre každé $\gamma \in \Delta$ a $s \in S^{[i]}$ bude obraz γ^s v rámci celého algoritmu spočítaný nanajvýš raz. Teda celkový čas potrebný na testovanie podmienky $\gamma^s \notin \Delta$ prebehne nanajvýš v čase $|\Delta||S^{[i]}| \in \mathcal{O}(n|S^{[i]}|)$. Vyplýva to z toho, že ak $\gamma^s \in \beta^{C(R)^{-1}C(R)}$, tak aj $\gamma^s \in \beta^{C(R')^{-1}C(R')}$, kde R' vzniklo z R niekoľkonásobným zdvojnásobením kocky. Podmienka $\gamma^s \notin \Delta$ môže byť splnená maximálne $(\log |G|)$-krát, keďže kocka $C(R)$ zdvojnásobuje svoju veľkosť každým pridaním prvku g_{k+1} do nej. Spočítanie prvku g je v čase $\mathcal{O}(n \log |G|)$, pretože najdlhšia možná cesta v monotónnom Schreierovom strome od koreňa β_i je $2 \log |G|$ a skladanie permutácii je v čase $\mathcal{O}(n)$. Ako už bolo spomenuté, časová zložitosť algoritmu OrbitaMonotonnySchreierVektor je $\mathcal{O}(n|R|) \in \mathcal{O}(n \log |G|)$. Celkovo dostávame $\mathcal{O}(n \log^2 |G| + n|S^{[i]}|)$.

□

4.1.2 Pravdepodobnostný algoritmus pre plytké Schreierové stromy

V tomto oddieli predpokladajme, že máme k dispozícii generátor náhodných prvkov Random(G), ktorý z množiny G určí náhodný prvok $g \in G$ z rovnomerného rozloženia. V tejto podkapitole budú hrany Schreierového stromu $T^{[i]}$ označené náhodne vygenerovanými prvkami grupy $G^{[i]}$. Schreierov strom budujeme podobne ako v predchádzajúcom odddiely. Takisto Schreierov vektor nebude

definovaný vzhľadom k algoritmu ORBITA, ako je to uvedené v kapitole 2, ale vzhľadom k nasledujúcemu algoritmu PRORBITAPLYTKYSCHREIERVEKTOR.

Myšlienka pravdepodobnostného algoritmu pre plytké Schreierové stromy je nasledovná. Nech $\Delta \subseteq \beta_i^{\langle S^{[i]} \rangle}$ je množina tých prvkov orbity, ktoré sme doposiaľ našli. Pokiaľ pre náhodný prvok $g \in G^{[i]}$ položíme $\Delta := \Delta \cup \Delta^g$, hĺbka odpovedajúceho Schreierovho stromu sa zväčší nanajvýš o jeden. Pokiaľ teda chceme Schreierov strom hĺbky $\mathcal{O}(\log |\beta_i^{\langle S^{[i]} \rangle}|)$, budeme potrebovať $\mathcal{O}(\log |\beta_i^{\langle S^{[i]} \rangle}|)$ náhodných prvkov. Algoritmus predpokladá znalosť veľkosti orbity $\beta_i^{\langle S^{[i]} \rangle}$.

Vstup: $\beta_i \in B$, kde B je báza $G \leq S_n$, $S^{[i]} \subseteq G^{[i]}, r = |\beta_i^{\langle S^{[i]} \rangle}|$
Výstup: fundamentálna orbita $\beta_i^{\langle S^{[i]} \rangle}$, Schreierov vektor v_i pre β_i vzhľadom množine náhodných prvkov $\{g_1, ..., g_k\}$

```
R := ∅;
k := 0;
for α = 1,...,n do
  | v_i[α] := 0;
end
v_i[β_i] := −1;
Δ := {β_i};
while |Δ| ≠ r do
  | repeat
  |   | g :=RANDOM(G^[i]);
  | until DOSTATOCNEVELKA(|Δ ∪ Δ^g|,|Δ|,p,r);
  | g_{k+1} := g;
  | APPEND(∼ R,g_{k+1});
  | k := k + 1;
  | for j = 1,...,k do
  |   | Δ' := Δ;
  |   | for γ ∈ Δ do
  |   |   | if γ^{g_j} ∉ Δ' then
  |   |   |   | Δ' := Δ' ∪ {γ^{g_j}};
  |   |   |   | v_i[γ^{g_j}] := j;
  |   |   | end
  |   | end
  |   | Δ := Δ';
  | end
end
return Δ, v_i;
```

Algoritmus 12: PRORBITAPLYTKYSCHREIERVEKTOR$(\beta_i, S^{[i]}, r)$

Za predpokladu, že poznáme transverzály $R^{[i]}$, ..., $R^{[m]}$ pre $G^{[i]}/G^{[i+1]}$, ..., $G^{[m]}/G^{[m+1]}$, funkcia RANDOM na vstupe $G^{[i]}$ vráti náhodný prvok g, pre ktorý platí $g = r_m r_{m-1} ... r_i$, kde $r_j \in R^{[j]}$ je z rovnomerného rozdelenia pre každé $j \in \{i+1, ..., m\}$.

Algoritmus DOSTATOCNEVELKA je boolovskou funkciou, ktorá vráti hodnotu *true*, pokiaľ množina $|\Delta \cup \Delta^g|$ je dostačujúcej veľkosti. To, o akú konkrétnu veľkosť sa jedná, vysvetľujú nasledujúce dve lemmy, ktoré boli uvedené v práci od Seressa

(2003, lemma 4.4.4., lemma 4.4.5.), dôkaz prvej lemmy a nesledujúca definícia je z práce od Coopermana a kol. (1990, lemma 3.1).

Definícia 11. *Nech* $G \leq S_n$, $S^{[i]} \subseteq G^{[i]}$, $g \in G^{[i]}$ *náhodný prvok vzhľadom k rovnomernému rozloženiu,* $\Delta^{[i]} = \beta_i^{\langle S^{[i]} \rangle}$ *a* $\Delta \subseteq \Delta^{[i]}$, $\Delta \neq \emptyset$. *Definujme náhodnú veličinu* X_Δ *na* $G^{[i]}$ *predpisom*

$$X_\Delta(g) := |\Delta^g \setminus \Delta|.$$

Strednú hodnotu náhodnej veličiny X_Δ označme ako $E(X_\Delta)$.

Lemma 14. *Nech* G,$S^{[i]}$,g, $\Delta^{[i]}$, Δ *sú ako v definícii vyššie. Potom platí*

$$E(X_\Delta) = \left(\frac{|\Delta^{[i]} \setminus \Delta|}{|\Delta^{[i]}|}\right)|\Delta|$$

Dôkaz. Definujme zobrazenie $\chi_{\Delta,\gamma} : G^{[i]} \mapsto \{0,1\}$ predpisom

$$\chi_{\Delta,\gamma}(g) = \begin{cases} 0, & \text{pokiaľ } \gamma^g \in \Delta, \\ 1 & \text{inak.} \end{cases}$$

Uvažujme pravé rozkladové triedy z množiny $G^{[i]}/G^{[i]}_\gamma$. Zrejme pre každú rozkladovú triedu platí, že jej prvky mapujú γ na to isté $\delta \in \Delta^{[i]}$ a teda aj hodnota funkcie $\chi_{\Delta,\gamma}$ je na prvkoch tej istej rozkladovej triedy rovnaká. Počet rozkladových tried, ktorých prvky nadobúdajú hodnotu 1 danej funkcie, je práve $|\Delta^{[i]}| - |\Delta|$. V pomeru k počtu rozkladových tried je to $(|\Delta^{[i]}| - |\Delta|)/|\Delta^{[i]}|$. Dostávame

$$\sum_{g \in G^{[i]}} \chi_{\Delta,\gamma}(g) = |G^{[i]}| \frac{|\Delta^{[i]}| - |\Delta|}{|\Delta^{[i]}|}.$$

Pre strednú hodnotu náhodnej veličiny X_Δ potom platí

$$E(X_\Delta) = \sum_{g \in G^{[i]}} X_\Delta(g) \frac{1}{|G^{[i]}|} = \sum_{g \in G^{[i]}} \sum_{\gamma \in \Delta^{[i]}} \frac{\chi_{\Delta,\gamma}(g)}{|G^{[i]}|} = \sum_{g \in G^{[i]}} \sum_{\gamma \in \Delta} \frac{\chi_{\Delta,\gamma}(g)}{|G^{[i]}|} =$$

$$= \sum_{\gamma \in \Delta} \Big(\sum_{g \in G^{[i]}} \frac{\chi_{\Delta,\gamma}(g)}{|G^{[i]}|} \Big) = \sum_{\gamma \in \Delta} \frac{|\Delta^{[i]}| - |\Delta|}{|\Delta^{[i]}|} = |\Delta| \frac{|\Delta^{[i]}| - |\Delta|}{|\Delta^{[i]}|}.$$

□

Horný odhad pre strednú hodnotu v dôkaze nasledujúcej lemmy je doplnený o medzikroky.

Lemma 15. *Nech* G,$S^{[i]}$,g, $\Delta^{[i]}$, Δ *sú ako v definícii vyššie. Potom pre každé* $0 < p < 1/2$ *platí, že*

(a) ak $|\Delta| \leq |\Delta^{[i]}|/2$, *tak*

$$Pr\left(|\Delta \cup \Delta^g| \geq |\Delta|\left(2 - \frac{|\Delta|}{(1-p)|\Delta^{[i]}|}\right)\right) \geq p;$$

(b) ak $|\Delta| \geq |\Delta^{[i]}|/2$*, tak*

$$Pr\left(|\Delta \cup \Delta^g| \geq |\Delta^{[i]}| - \frac{(|\Delta^{[i]}| - |\Delta|)^2}{(1-p)|\Delta^{[i]}|}\right) \geq p;$$

Dôkaz. Nech $X_\Delta(g) := |\Delta^g \setminus \Delta|$ ako v definícii vyššie.

(a) Výraz $|\Delta \cup \Delta^g| \geq |\Delta|(2 - |\Delta|/((1-p)|\Delta^{[i]}|))$ je ekvivalentný výrazu $|\Delta^g \setminus \Delta| \geq c|\Delta|$, pre $c = 1 - |\Delta|/((1-p)|\Delta^{[i]}|)$. Zrejme platí $|\Delta| \geq X_\Delta(g)$ pre každé $g \in G^{[i]}$. Označme $A := \{g \in G^{[i]} \mid X_\Delta(g) \geq c|\Delta|\}$, $q := Pr(X_\Delta(g) \geq c|\Delta|)$. Platí

$$E(X_\Delta) = \sum_{g \in G^{[i]}} X_\Delta(g) \frac{1}{|G^{[i]}|} = \frac{1}{|G^{[i]}|}\left(\sum_{g \in A} X_\Delta(g) + \sum_{g \in G^{[i]} \setminus A} X_\Delta(g)\right) \leq$$

$$\leq \frac{1}{|G^{[i]}|}\left(\sum_{g \in A} |\Delta| + \sum_{g \in G^{[i]} \setminus A} c|\Delta|\right) = \frac{|A|}{|G^{[i]}|}|\Delta| + \frac{|G^{[i]} \setminus A|}{|G^{[i]}|}c|\Delta| =$$

$$= q|\Delta| + (1-q)c|\Delta|.$$

Podľa lemmy 14 platí $E(X_\Delta) = (|\Delta^{[i]} \setminus \Delta|/|\Delta^{[i]}|)|\Delta|$, dosadením daného výrazu a úpravou nerovnosti vyššie dostávame $q \geq p$.

(b) Výraz $|\Delta \cup \Delta^g| \geq |\Delta^{[i]}| - (|\Delta^{[i]}| - |\Delta|)^2/((1-p)|\Delta^{[i]}|))$ je ekvivalentný výrazu $|\Delta^g \setminus \Delta| \geq (1-c)(|\Delta^{[i]}| - |\Delta|)$, pre $c = (|\Delta^{[i]}| - |\Delta|)/((1-p)|\Delta^{[i]}|)$. Označme $q := Pr(X_\Delta(g) \geq (1-c)(|\Delta^{[i]}| - |\Delta|)$. Potom obdobne ako v (a) platí

$$E(X_\Delta) \leq q(|\Delta^{[i]}| - |\Delta|) + (1-q)(1-c)(|\Delta^{[i]}| - |\Delta|).$$

Opäť vzhľadom k lemme 14 dostávame $q \geq p$.

□

Algoritmus DostatocneVelka vráti hodnotu *true* práve vtedy, keď platí

$$|\Delta \cup \Delta^g| \geq \begin{cases} |\Delta|\left(2 - \frac{|\Delta|}{(1-p)|\Delta^{[i]}|}\right), & \text{pokiaľ } |\Delta| \leq |\Delta^{[i]}|/2, \\ |\Delta^{[i]}| - \frac{(|\Delta^{[i]}| - |\Delta|)^2}{(1-p)|\Delta^{[i]}|}, & \text{pokiaľ } |\Delta| \geq |\Delta^{[i]}|/2. \end{cases}$$

Takáto situácia nastane pre každé $g \in G^{[i]}$ z rovnomerného rozdelenia s pravdepodobnosťou aspoň p, ako vyplýva z predchádzajúcej lemmy.

Seress (2003, veta 4.4.6) určil potrebný počet náhodných prvkov grupy $G^{[i]}$, pre ktoré algoritmus PrOrbitaPlytkySchreierVektor vráti úplnú orbitu a príslušný plytký Schreierov vektor s dostatočnou pravdepodobnosťou. Konkrétne pre voľbu $p := 0{,}46$ dokázal, že pokiaľ máme k dispozícii aspoň $8 \log |\Delta^{[i]}| + 16$ náhodných prvkov z rovnomerného rozdelenia, potom s pravdepodobnosťou aspoň $1 - |\Delta^{[i]}|^{-0{,}29}$ algoritmus PrOrbitaPlytkySchreierVektor vráti orbitu a príslušný Schreierov vektor, odpovedajúci stromu hĺbky nanajvýš $2 \log |\Delta^{[i]}| + 4$. Základnou myšlienkou dôkazu je využitie Chernoffovho odhadu, zvyšok dôkazu je technický. Vzhľadom k jeho dĺžke ho v tejto práci neuvedieme.

4.2 Náhodné Schreierové generátory

Ďalším faktorom, ktorý pridáva na časovej zložitosti Schreier Simsovho algoritmu, je použitie algoritmu ROZKLAD pre každý Schreierov generátor. Prepokladajme, že báza a silne generujúca množina je pod úrovňou i. V tejto kapitole ukážeme efektívnejší postup ako otestovať, či

$$\langle S^{[i]} \rangle_{\beta_i} = \langle S^{[i+1]} \rangle.$$

Úvahy v tejto podkapitole sú inšpirované z knihy od Seressa (2003, str.72 – 75). Pre každé $j \in \{i+1, ...,m\}$ označme ako $R^{[j]}$ pravú transverzálu pre $\langle S^{[j]} \rangle / \langle S^{[j+1]} \rangle$, ktorú reprezentuje Schreierov strom $T^{[j]}$. Keďže sme pod úrovňou i, každý prvok z $g \in \langle S^{[i+1]} \rangle$ možno jednoznačne vyjadriť ako súčin $g = r_m r_{m-1} ... r_{i+1}$ pre $r_{i+1} \in R^{[i+1]}$, ..., $r_m \in R^{[m]}$. Ďalej nech $R^{[i]}$ je pravou transverzálou pre $\langle S^{[i]} \rangle / \langle S^{[i]} \rangle_{\beta_i}$, reprezentovanou Schreierovým stromom $T^{[i]}$. Označme ako t súčet hĺbok stromov $T^{[i]}$, $T^{[i+1]}$, ... ,$T^{[m]}$ a nech M značí množinu všetkých permutácii, ktoré označujú nejakú hranu z množiny všetkých hrán uvedených stromov.

Pomocou algoritmu ROZKLAD rozložme každý prvok z $S^{[i]}$ v $R^{[m]} ... R^{[i+1]} R^{[i]}$. Pokiaľ pre niektorý z nich dostaneme netriviálny zvyšok, tak $\langle S^{[i]} \rangle_{\beta_i} \neq \langle S^{[i+1]} \rangle$. V opačnom prípade M generuje $\langle S^{[i]} \rangle$.

Nasledujúce lemma z práce od Babaia (1992, lemma 10.2) je základnou myšlienkou tejto podkapitoly. Dôkaz je doplnený o ozrejmenie vzťahov (4.1) a (4.2).

Lemma 16. *Nech M je generujúcou množinou grupy G a $D \subseteq (M \cup M^{-1} \cup \{e\})^t$. Predpokladajme, že existuje $0 < q \leq 1/(2t+1)$ také, že*

$$|D| \leq (1 - 2qt)|G|.$$

Potom existuje aspoň jedno $m \in M$ také, že

$$|D \setminus Dm| \geq q|D|.$$

Dôkaz. Nech pre spor platí $|D \setminus Dm| < q|D|$ pre každé $m \in M$. Označme $T := M \cup M^{-1} \cup \{e\}$. Množina M generuje G, teda $G = \cup_{k \geq 0} T^k$. Najprv ukážeme, že $G = T^{2t}$.

Pre každé $m \in M$ definujeme zobrazenia $\phi_m : D \setminus Dm^{-1} \to Dm \setminus D$, $\psi_m : D \setminus Dm \to Dm \setminus D$ predpismi $\phi_m(d) = dm$ a $\psi_m(d) = dm$. Zrejme sa jedná o bijekcie na konečných množinách a teda

$$|D \setminus Dm^{-1}| = |Dm \setminus D| = |D \setminus Dm| < q|D|. \tag{4.1}$$

Navyše pre každé m,$n \in T$ platí

$$D \setminus Dmn \subseteq (D \setminus Dn) \cup (D \setminus Dm)n. \tag{4.2}$$

To preto, že ak zvolíme $d \in D \setminus Dmn$, pre ktoré navyše platí $d \notin D \setminus Dn$, tak nutne existuje $d' \in D$ také, že $d = d'n \in Dn$. Súčasne neexistuje $d'' \in D$ pre ktoré by $d' = d''m \in Dm$, inak by $d = d'n = d''mn \in Dmn$, čo je spor. Teda $d \in (D \setminus Dm)n$.

Tým pádom $|D \setminus Dmn| \leq |D \setminus Dn| + |(D \setminus Dm)n| < 2q|D|$, indukčne podľa k potom pre každé $u \in T^k$ dostávame $|D \setminus Du| < kq|D|$. Kým platí $kq \leq 1$, tak

$Du \cap D \neq \emptyset$, teda $u \in D^{-1}D$. Keďže $q \leq 1/(2t+1)$, tak $T^{2t+1} \subseteq D^{-1}D \subseteq T^{2t}$, t.j. $T^{2t} = T^{2t+1} = ... = G$.

Určme počet dvojíc (d,u) takých, že $d \in D, u \in G, du \in D$. Pre pevne zvolené $d \in D$ je počet $u \in G$ takých, že $du \in D$, práve $|D|$. Celkový počet dvojíc je potom $|D|^2$. Na druhú stranu pre pevne zvolené $u \in G = T^{2t}$ je veľkosť $|D \cap Du|$ aspoň $(1-2tq)|D|$, keďže $|D \setminus Du| < 2tq|D|$. Celkový počet dvojíc (d,u) je aspoň $(1-2tq)|D||G|$. Dostávame $|D|^2 \geq (1-2tq)|D||G|$, čo je spor s predpokladom. □

Pokiaľ platí $\langle S^{[i]} \rangle_{\beta_i} \neq \langle S^{[i+1]} \rangle$, tak $|\langle S^{[i]} \rangle_{\beta_i} : \langle S^{[i+1]} \rangle| \geq 2$. To znamená, že $|R^{[m]}...R^{[i+1]}R^{[i]}| \leq |\langle S^{[i]} \rangle_{\beta_i}|/2$ a teda podmienky predchádzajúcej lemmy sú splnené pre parametre $G := \langle S^{[i]} \rangle_{\beta_i}$, M, t ako vyššie, $D := R^{[m]}...R^{[i+1]}R^{[i]}$ a $q = 1/(4t)$.

Inak povedané ak $\langle S^{[i]} \rangle_{\beta_i} \neq \langle S^{[i+1]} \rangle$, tak pre každý náhodný prvok $d \in D$ z rovnomerného rozdelenia platí

$$Pr(\exists g \in M \mid dg \notin D) \geq \frac{1}{4t}. \tag{4.3}$$

Pokiaľ pre $c \in \mathbb{N}$ zvolíme $4ct$ náhodných prvkov $d \in D$ a otestujeme, že pre každé $g \in M$ a každé d platí $dg \in D$, tak

$$Pr(\langle S^{[i]} \rangle_{\beta_i} = \langle S^{[i+1]} \rangle) > 1 - e^{-c}.$$

Ostáva uviesť to, ako otestujeme, či $dg \in D$. Pre každé $d \in D$ existujú jednoznačne určené $h \in \langle S^{[i+1]} \rangle$, $r \in R^{[i]}$ také, že $d = hr$. Navyše $dg = hrg \in D$ práve vtedy keď $hrg(\overline{hrg})^{-1} \in \langle S^{[i+1]} \rangle$, kde $\overline{k} := R^{[i]} \cap \langle S^{[i+1]} \rangle k$ je jednoznačne určený prvok pre každé $k \in G^{[i]}$. Keďže h stabilizuje β_i, tak $\overline{hrg} = \overline{rg}$. Takisto $hrg(\overline{hrg})^{-1} \in \langle S^{[i+1]} \rangle$ práve vtedy, keď $rg(\overline{hrg})^{-1} \in \langle S^{[i+1]} \rangle$. Tým pádom namiesto toho, aby sme testovali pre náhodné $d \in D$, či platí $dg \in D$ pre každé $g \in M$, postačí, aby sme testovali pre náhodné $r \in R^{[i]}$, či platí $rg(\overline{rg})^{-1} \in \langle S^{[i+1]} \rangle$ pre každé $g \in M$. Testovanie pre každé $g \in M$ je ale príliš zdĺhavé.

Jednou možnosťou, ktorá sa ponúka, je testovať $rg(\overline{rg})^{-1} \in \langle S^{[i+1]} \rangle$ pre náhodné $r \in R^{[i]}$ a náhodné $g \in M$. To však nemusí vždy dobre fungovať, dokazuje to nasledujúce riešenie cvičenia 4.5 v knihe od Seressa (2003, cvičenie 4.5). Pred jeho uvedením poznamenajme, že permutačná grupa $G \leq S_n$ je *regulárna*, pokiaľ pre každé $\beta \in \{1,...,n\}$ je $G_\beta = 1$.

Príklad 10. *Nech $H = \{h_1, ..., h_{n-2}\}$ je regulárna permutačná grupa pôsobiaca na $\{1, ..., n-2\}$ a nech $G = \langle h_1, ..., h_{n-2}, (n-1 \quad n) \rangle$. Potom $B = (1, n-1)$ je neredundantná báza, pretože zrejme $G_1 = \langle (n-1 \quad n) \rangle$ a $G_{(1,n-1)} = 1$. Pre každé $\gamma \in 1^{G_1}$ označme $r_\gamma \in R$ jednoznačne určený prvok pravej transverzály R pre G/G_1, pre ktorý platí $r_\gamma(1) = \gamma$. Fundamentálnou orbitu 1^{G_1} je práve $\{1, ..., n-2\}$ a teda každý prvok transverzály R stabilizuje prvok $n-1$. Tým pádom rozklad každého Schreierovho generátora tvaru $r_\gamma \, h \, r_{\gamma^h}^{-1}$, kde $h \in H$, vráti triviálny zvyšok. Označme $x := (n-1 \quad n)$. Naopak rozklad každého Schreierového generátoru tvaru $r_\gamma \, x \, r_{\gamma^x}^{-1}$ v G_1 zrejme vráti netriviálny zvyšok. Zvolme náhodné $r_\gamma \in R$ a $g \in \{h_1, ..., h_{n-2}, (n-1 \quad n)\}$ vzhľadom k rovnomernému rozdeleniu. Potom pravdepodobnosť, že rozklad Schreierovho generátoru $r_\gamma \, g \, r_{\gamma^g}^{-1}$ vráti netriviálny zvyšok, a teda odhalí, že $G_1 \neq 1$, je iba $1/(n-1)$.*

4.2.1 Náhodné subprodukty

Pre pevné $g \in M$ označme ako $P(g, x)$ nasledujúce tvrdenie

$$|\{r \in R^{[i]} \mid rg(\overline{rg})^{-1} \notin \langle S^{[i+1]} \rangle\}| \geq x,$$

kde $x \in \mathbb{N}$. Nech $\neg P$ značí negáciu tvrdenia P.

Pozorovanie 17. $P(g,x) \wedge \neg P(h,y) \implies P(gh, x-y) \wedge P(hg, x-y)$.

Dôkaz. Ako vyplýva z textu vyššie, tvrdenie $rg(\overline{rg})^{-1} \notin \langle S^{[i+1]} \rangle$ je ekvivalentné tomu, či $dg \notin D$ pre vhodné, jednoznačne určené $d \in D$. Navyše zrejme $D \setminus Dg = \{d \in D \mid dg \notin D\}$. Inak povedané, chceme ukázať, že

$$(|Dg \setminus D| \geq x) \wedge (|D \setminus Dh| < y) \implies (|D \setminus Dgh| \geq x-y) \wedge (|D \setminus Dhg| \geq x-y).$$

Ukážeme, že platí $(Dg \setminus D)h \subseteq (Dgh \setminus D) \cup (D \setminus Dh)$. Zvolme $d \in D$ také, že $dg \notin D$. Zrejme $dgh \in (Dg \setminus D)h$. Navyše pokiaľ $dgh \in D$, tak nutne $dgh \notin Dh$, pretože $dg \notin D$. Teda $dgh \in (Dgh \setminus D) \cup (D \setminus Dh)$. Platí

$$|(Dg \setminus D)h| \leq |Dg \setminus D| \leq |Dgh \setminus D| + |D \setminus Dh| = |D \setminus Dgh| + |D \setminus Dh|.$$

Dostali sme $|Dg \setminus D| - |D \setminus Dh| \leq |D \setminus Dgh|$, čo dokazuje

$$(|Dg \setminus D| \geq x) \wedge (|D \setminus Dh| < y) \implies |D \setminus Dgh| \geq x-y.$$

Teraz ukážeme, že $D \setminus Dg \subseteq (D \setminus Dgh) \cup (Dh \setminus D)g$. Zvolme $d \in D$ také, že pre každé $d' \in D$ platí $d \neq d'g$, t.j. $d \in D \setminus Dg$. Pokiaľ $d \in Dgh$, tak existuje $d'' \in D$ také, že $d = d''hg$. Súčasne neexistuje $d' \in D$ také, že $d' = d''h$, inak by $d = d''hg = d'g \in Dg$, čo je spor. Teda $d \in (D \setminus Dgh) \cup (Dh \setminus D)g$. Platí

$$|D \setminus Dg| \leq |D \setminus Dgh| + |(Dh \setminus D)g| \leq |D \setminus Dgh| + |D \setminus Dh|.$$

Dostávame

$$(|Dg \setminus D| \geq x) \wedge (|D \setminus Dh| < y) \implies |D \setminus Dhg| \geq x-y.$$

□

Dôkaz pozorovania vyššie je riešením cvičenia 4.8 z knihy od Seressa (2003, cvičenie 4.8). Nasledujúca definícia je z článku od Babaia a kol. (1991, str. 204).

Definícia 12. *Náhodným subproduktom pre postupnosť $(g_1, ..., g_k)$ prvkov grupy G nazveme $g_1^{e_1} ..., g_k^{e_k}$, kde e_i sú nezávislé náhodné veličiny z rovnomerného rozdelenia na množine $\{0,1\}$ pre každé $i \in \{1, ...,k\}$.*

Vraťme sa späť k tomu, ako sa vyhnúť testovaniu platnosti $rg(\overline{rg})^{-1} \in \langle S^{[i+1]} \rangle$ pre každé $g \in M$. Skonštruujeme $w_1 \in M$ a $w_2 \in M$, pre ktoré s dostatočnou pravdepodobnosťou aspoň jeden zo Schreierových generátorov $rw_1(\overline{rw_1})^{-1}$ a $rw_2(\overline{rw_2})^{-1}$ neleží v $\langle S^{[i+1]} \rangle$. Táto konštrukcia bola pôvodne uvedená ako súčasť dôkazu lemmy 3.4 v práci od Babaia a kol. (1991, lemma 3.4).

Náhodne zoraďme prvky množiny M do postupnosti. Označme ako w_1 náhodný subprodukt prvkov tejto postupnosti. Nech k' je náhodné číslo z množiny $\{0, 1, ..., |M| - 1\}$ a $k := \lfloor k'/2 \rfloor$. Nech w_2 je náhodný subprodukt vzhľadom k náhodnému zoradeniu M' do postupnosti, kde M' je náhodná podmnožina M dĺžky k.

Následujúca lemma je z knihy od Seressa (2003, lemma 4.5.4).

Lemma 18. *Nech $x \in \mathbb{N}$, w_1, w_2 ako vyššie a $P(g,x)$ platí pre nejaké $g \in M$. Potom*

$$Pr(P(w_1, x/4) \vee P(w_2, x/4)) \geq 1/4.$$

Dôkaz. Zvolme $g \in M$ také, že $P(g,x)$ platí. Nech S' je ako vyššie, potom $Pr(g \notin M') \geq \binom{|M|-1}{k}\binom{|M|}{k} \geq 1/2$. Nech p značí pravdepodobnosť, že $P(h, x/4)$ platí, kde h je náhodný subprodukt vzhľadom k náhodnému zoradeniu náhodnej podmnožiny $M \setminus \{g\}$ dĺžky k do postupnosti. Keďže w_2 má rovnaké rozdelenie ako h, pokiaľ $g \notin M'$, tak $Pr(P(w_2, x/4)) \mid g \notin M') = p$. A tým pádom

$$Pr(P(w_2, x/4))) \geq Pr(P(w_2, x/4)) \mid g \notin M')\ Pr(g\ \notin\ M') \geq p/2.$$

Nech $w_1 = ug^e v$, kde $e \in \{0,1\}$ a u,v jednoznačne určené. Bez ujmy na všeobecnosti predpokladajme, že dĺžka v nie je väčšia ako dĺžka u. Potom v má rovnaké rozdelenie ako h a teda $Pr(P(v,x/4)) = p$. Podľa pozorovania 17 potom

$$\begin{aligned}
&Pr(P(ug^e, x/2) \mid \neg P(v, x/4)) = \\
&\quad = Pr(P(ug^e, x/2) \mid P(u, x/2) \wedge \neg P(v, x/4))\ Pr(P(u, x/2)) + \\
&\qquad + Pr(P(ug^e, x/2) \mid \neg P(u, x/2) \wedge \neg P(v, x/4))\ Pr(\neg P(u, x/2)) \geq \\
&\quad \geq Pr(e = 0 \mid P(u, x/2) \wedge \neg P(v, x/4))\ Pr(P(u, x/2)) + \\
&\qquad + Pr(e = 1 \mid \neg P(u, x/2) \wedge \neg P(v, x/4))\ Pr(\neg P(u, x/2)) = 1/2,
\end{aligned}$$

pretože náhodná veličina e je nezávislá na u a v. Opäť použitím pozorovania dostávame

$$\begin{aligned}
Pr(P(w_1, x/4)) = Pr(P(ug^e v, x/4)) &\geq \\
&\geq Pr(P(ug^e, x/2) \mid \neg P(v, x/4)) Pr(\neg P(v, x/4)) \geq \\
&\geq (1-p)/2.
\end{aligned}$$

Vďaka tomu, že $\max\{(1-p)/2, p/2\} \geq 1/4$ pre $0 \leq p \leq 1$, je dôkaz hotový. □

Vzhľadom k (4.3) platí $P(g, |D|/4t)$ pre nejaké $g \in M$. Predpoklady predchádzajúcej lemmy sú splnené a platí:

$$Pr(rw_2(\overline{rw_1})^{-1} \notin S^{[i+1]} \vee rw_2(\overline{rw_2})^{-1} \notin S^{[i+1]}) \geq \frac{1}{64t}.$$

Uvedieme pseudokód algoritmu popísaného vyššie. Funkcia NahodnySubprodukt vráti w_1 a w_2 ako v odstavci pred lemmou 18.

Vstup: β_i prvok báze, fundamentálna orbita $\beta_i^{\langle S^{[i]} \rangle}$, Schreierov vektor v_i pre β_i, $S^{[i]} \subseteq G^{[i]}$, $M = \cup_{j=i}^{m} S^{[j]}$ zjednotenie označení hrán Schreierových stromov $T^{[j]}$ pre $j \geq i$, pričom odpovedajúca BSGS je pod úrovňou i
Výstup: Dvojica náhodných Schreierových generátorov $rw_1(\overline{rw_1})^{-1}$ a $rw_2(\overline{rw_2})^{-1}$ vzhľadom k lemme 18
$\gamma :=$ Random($\Delta^{[i]}$);
$r :=$ PrvokTransverzaly($\beta_i, v_i, S^{[i]}$);
$w_1, w_2 :=$ NahodnySubprodukt(M);
return $rw_1(\overline{rw_1})^{-1}$, $rw_2(\overline{rw_2})^{-1}$;

Algoritmus 13: NahodnySchreierGenerator($\beta_i, \Delta^{[i]}, v_i, S^{[i]}, M$)

4.3 Monte Carlo Schreier Simsov algoritmus

V predchádzajúcich dvoch podkapitolách sme popísali potrebné vylepšenia, v tejto podkapitole popíšeme spomínaný skoro lineárny Monte Carlo Schreier Simsov algoritmus.

Pojmy čiastočná báza a čiastočne silne generujúca množina sú definované ako v kapitole 3. V tejto kapitole mierne pozmeníme definíciu pre pojem pod úrovňou.

Definícia 13. *Nech $B = (\beta_1, ..., \beta_m)$ je čiastočná báza permutačnej grupy $G \leq S_n$, $S \subseteq G$ je čiastočná silne generujúca množiny grupy G vzhľadom k B a $i \in \{1, ..., m\}$. Hovoríme, že čiastočná BSGS (B,S) je* pod úrovňou i, *pokiaľ buď $i = m$ alebo pre všetky $j = i + 1, ..., m$ platí*

$$\langle S^{[j]} \rangle_{\beta_j} = \langle S^{[j+1]} \rangle.$$

a súčet hĺbok Schreierových stromov $T^{[i+1]}$, ..., $T^{[m]}$ je nanajvýš $6 \log |\langle S^{[i+1]} \rangle|$.

Pseudokód Monte Carlo Schreier Simsovho algoritmu je uvedený v práci od Babai a kol. (1991, str. 206 – 207). Uvedieme jednoduchší popis tohto algoritmu, obdobne ako v knihe od Seressa (2003, str. 70). Základná myšlienka je v oboch prípadoch rovnaká.

Algoritmus začne na úrovni 0, obdobne ako vo vylepšení uvedenom v podkapitole 3.3. Konkrétne definujme $S^{[0]} := X$ a $\beta_0 := n + 1$, kde $G = \langle X \rangle \leq S_n$.

Pokiaľ sa čiastočná BSGS nachádza pod úrovňou i, tak pomocou deterministického algoritmu OrbitaPlytkySchreierVektor pre plytké Schreierové stromy z podkapitoly 4.1.1 nájdeme strom $T^{[i]}$ hĺbky nanajvýš $2 \log |\langle S^{[i]} \rangle|$. Postupne rozkladáme dvojice náhodných Schreierových generátorov $rw_1(\overline{rw_1})^{-1}$, $rw_2(\overline{rw_2})^{-1}$ nájdených algoritmom NahodnySchreierGenerator zpodkapitoly 4.2 v grupe $\langle S^{[i+1]} \rangle$. Ak náhodný Schreierov generátor má netriviálny zvyšok, vložíme ho do množiny $S^{[i+1]}$ a pokračujeme na úrovni $i + 1$. Obdobne ako v pôvodnom Schreier Simsovom algoritme, pokiaľ daný zvyšok stabilizuje všetky β_{i+1}, ..., β_m, nájdeme nový prvok báze. Pokiaľ posledných $xt \log n$ dvojíc Schreierových generátorov vrátilo po rozklade iba triviálne zvyšky, prehlásime, že $\langle S^{[i]} \rangle_{\beta_i} = \langle S^{[i+1]} \rangle$, kde t je súčet hĺbok Schreierových stromov od úrovne i a nižšie, x je vhodná konštanta. Tým pádom môžeme skonštruovať náhodné prvky v $\langle S^{[i]} \rangle_{\beta_i}$ a prepočítať Schreierov strom $T^{[i]}$ použijúc pravdepodobnostný algoritmus PrOrbitaPlytkySchreierVektor pre plytké Schreierové stromy z podkapitoly 4.1.2. Na označenie hrán tohto stromu použijeme náhodné prvky g_1, ..., g_k, kde $k := \lfloor 2 \log |\Delta^{[i]}| + 4 \rfloor \leq 6 \log |\Delta^{[i]}|$. Ak je táto konštrukcia úspešná, tak $S^{[i]} := S^{[i+1]} \cup \{g_1, ..., g_k\}$ a postúpime na úroveň $i - 1$. Algoritmus končí, keď sa dostaneme na úroveň -1.

Konštanta x pre hore uvedené dvojice náhodných Schreierových generátorov závisí na tom, akú požadujeme maximálnu chybovosť. Pravdepodobnosť, že Monte Carlo Schreier Simsov algoritmus vráti nesprávny výsledok je $1/n^d$, kde d je konštanta predpísaná uživateľom. Algoritmus pracuje v čase $\mathcal{O}(n \log n \log^4 |G| + |X| n \log |G|)$ a vyžaduje $\mathcal{O}(n \log |G| + |X| n)$ pamäte.

Detailna analýza spoľahlivosti algoritmu a časovej a priestorovej zložitosti je uvedená v knihe od Seressa (2003, str. 71, 75).

Záver

V tejto práci sme detailne popísali Schreier Simsov algoritmus vychádzajúc z viacerých zdrojov. Súčasne sme preň uviedli podrobné pseudokódy, vrátane pseudokódov pre čiastkové problémy. Priestorovú a časovú zložitosť sme spočítali vzhľadom k uvedeným pseudokódom. Korektnosť algoritmu vyplýva z teoretických poznatkov, ktoré sme v práci vysvetlili. Rovnako sme popísali aj jeho Monte Carlo verziu. Tá je založená na dvoch vylepšeniach. Prvým je použitie plytkých Schreierových stromov, pre ktoré sme určili deterministický a aj pravdepodobnostný algoritmus spoločne s potrebnými pseudokódmi. Korektnosť týchto algoritmov sme podložili tvrdeniami vyplývajúcimi z teórie pravdepodobnosti a teórie grúp. Určili sme časovú a priestorovú zložitosť a pre pravdepodobnostný algoritmus sme určili aj spoľahlivosť. Druhé zlepšenie sa týkalo použitia náhodných Schreierových generátorov. Určili sme spoľahlivosť takéhoto vylepšenia, ktorú sme opäť podložili teoretickými poznatkami. Na záver sme popísali, ako sú tieto zlepšenia v Monte Carlo Schreier Simsovom algoritme implementované.

Na záver zhrnieme, v čom spočíva prínos tejto práce. Uviedli sme podrobnejšie pseudokódy, ktoré na seba nadväzujú. Okrem pseudokódov prevzatých z literatúry, sme doplnili pseudokódy pre RozsirOrbitaSchreierVektor, OrbitaMonotonnySchreierVektor, OrbitaPlytkySchreierVektor a PrOrbitaPlytkySchreierVektor. Pseudokód algoritmu SchreierSims je kombináciou dvoch pseudokódov, doplnený o detaily. Ďalej sú súčasťou práce riešenia niektorých cvičení uvedených na konci kapitoly 4 v knihe od Seressa (2003, str. 77, 78), obzvlášť tých, ktoré mali napomôcť porozumeniu teórie. Riešením cvičenia 4.2 je príklad 5, riešenie cvičenia 4.4 je súčasťou vylepšenia uvedeného v podkapitole 3.3, riešením cvičenia 4.5 je príklad 10 a riešením cvičenia 4.8 je pozorovanie 17. V Oddieli 1.3 rozoberáme špeciálny prípad báze a silne generujúcej množiny pre cyklické grupy. Sformulovali sme v ňom a dokázali tvrdenie o tom, ako vyzerá neredundantná báza a silne generujúca množina pre cyklické grupy. V príklade 4 sme načrtli spôsob ako nájsť všetky možné neredundantné bázy a ich silne generujúce množiny zo zadaného generátoru cyklickej grupy. V oddieli 2.4.1 uvádzame detailný popis analógie medzi Gauss Jordanovou eliminációu a algoritmom Rozklad. Práca takisto obsahuje niekoľko ilustračných príkladov a dôkazy v tejto práci sú doplnené o chýbajúce kroky.

Zoznam použitej literatúry

Babai, L. (1992). Bounded Round Interactive Proofs in Finite Groups. *SIAM Journal on Discrete Mathematics*, **5**(1), 88–111. ISSN 0895-4801. doi: 10.1137/0405008. URL http://epubs.siam.org/doi/10.1137/0405008.

Babai, L., Cooperman, G., Finkelstein, L. a Ákos Seress (1991). Nearly linear time algorithms for permutation groups with a small base. *Proceedings of the 1991 international symposium on Symbolic and algebraic computation - ISSAC '91*, pages 200–209. doi: 10.1145/120694.120724. URL http://portal.acm.org/citation.cfm?doid=120694.120724.

Butler, G. (1991). *Fundamental algorithms for permutation groups*. Springer-Verlag, New York. ISBN 03-875-4955-2.

Cooperman, G., Finkelstein, L. a Sarawagi, N. (1990). A random base change algorithm for permutation groups. *Proceedings of the international symposium on Symbolic and algebraic computation - ISSAC '90*, pages 161–168. doi: 10.1145/96877.96918. URL http://portal.acm.org/citation.cfm?doid=96877.96918.

Holt, D. F., Eick, B. a O'Brien, E. A. (2005). *Handbook of computational group theory*. Chapman & Hall/CRC, Boca Raton. ISBN 15-848-8372-3.

Luks, E. M. (1982). Isomorphism of graphs of bounded valence can be tested in polynomial time. *Journal of Computer and System Sciences*, **25**(1), 42–65. ISSN 00220000. doi: 10.1016/0022-0000(82)90009-5. URL https://linkinghub.elsevier.com/retrieve/pii/0022000082900095.

Murray, S. H. (1994). The Schreier-Sims algorithm. *Bachelor thesis, Australian National University*. URL http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.6.4493&rep=rep1&type=pdf.

Seress, A. (2003). *Permutation group algorithms*. Cambridge University Press, New York. ISBN 05-216-6103-X.

Sims, C. C. (1970). Computational methods in the study of permutation groups. *Computational Problems in Abstract Algebra*, pages 169–183. doi: 10.1016/B978-0-08-012975-4.50020-5. URL https://linkinghub.elsevier.com/retrieve/pii/B9780080129754500205.

Sims, C. C. (1971). Computation with permutation groups. *Proceedings of the second ACM symposium on Symbolic and algebraic manipulation - SYMSAC '71*, pages 23–28. doi: 10.1145/800204.806264. URL http://portal.acm.org/citation.cfm?doid=800204.806264.

Sims, C. C. (1973). The Existence and Uniqueness of Lyons' Group. *Finite Groups '72, Proceedings of the the Gainesville Conference on Finite Groups*, pages 138–141. doi: 10.1016/S0304-0208(08)71841-3. URL https://linkinghub.elsevier.com/retrieve/pii/S0304020808718413.

Sims, C. C. (1978). How to construct a baby monster. *Finite simple groups II*, pages 339–345.