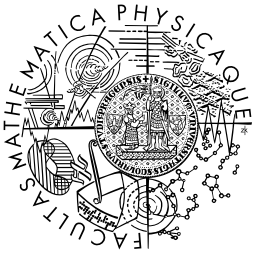

MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Jakub Kašpar

Věncové součiny symetrických grup a počítání Sudoku čtverců

Katedra algebry

Vedoucí bakalářské práce: prof. RNDr. Aleš Drápal, CSc., DSc.
Studijní program: Matematika
Studijní obor: Obecná matematika

Praha 2020

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů. Tato práce nebyla využita k získání jiného nebo stejného titulu.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V Mochově dne 29. 7. 2020 Jakub Kašpar

Rád bych poděkoval vedoucímu práce, prof. Aleši Drápalovi, za všechen čas, který mi věnoval, za milou a trpělivou pomoc a za řadu dobrých rad.

Název práce: Věncové součiny symetrických grup a počítání Sudoku čtverců

Autor: Jakub Kašpar

Katedra: Katedra algebry

Vedoucí bakalářské práce: prof. RNDr. Aleš Drápal, CSc., DSc., Katedra algebry

Abstrakt: Práce systematizuje výpočet esenciálně odlišných Sudoku čtverců pomocí Burnsidova lemmatu. Tento výpočet zásadně staví na popisu tříd konjugace grupy symetrií Sudoku čtverce, který byl v předchozích pracech prováděn pouze pomocí matematického softwaru. V první kapitole shrnuje poznatky o působení grupy na množině a třídách konjugace a rozšiřuje je zejména o popis tříd konjugace věncového součinu, ve druhé kapitole je formálně definována grupa symetrií Sudoku čtverce, ukázáno, že jde o direktní součin vhodných věncových součinů a pomocí výsledků z první kapitoly jsou určeny reprezentanty a velikosti jejích tříd konjugace.

Klíčová slova: věncový součin, symetrická grupa, Burnsidovo lemma, Sudoku čtverec

Title: Wreath products of symmetric groups and enumeration of Sudoku squares

Author: Jakub Kašpar

Department: Department of Algebra

Supervisor: prof. RNDr. Aleš Drápal, CSc., DSc., Department of Algebra

Abstract: The thesis systematizes the enumeration of essentially different Sudoku squares using Burnside's lemma. This enumeration significantly depends on the description of conjugacy classes of symmetry group of Sudoku square, which was in previous works provided only with the strong help of mathematical software. The first chapter of this thesis sums up facts about a group action and about conjugacy classes and proposes the description of conjugacy classes of wreath product, in the second chapter Sudoku square of symmetric group is formally defined and with the help of presented theory are counted representatives and sizes of its conjugacy classes.

Keywords: wreath product, symmetric group, Burnside's lemma, Sudoku square

Obsah

Úvod **2**

1 Věncové součiny symetrických grup **3**
1.1 Působení grupy na množině 3
1.2 Součiny grup 4
1.3 Konjugované prvky a třídy konjugace 5
1.4 Množiny reprezentantů symetrických grup 6
1.5 Množina reprezentantů součinů grup 8

2 Počítání Sudoku čtverců **14**
2.1 Přirozený popis Sudoku čtverce a motivace 14
2.2 Formální definice Sudoku čtverce a jeho symetrií 15
2.3 Esenciálně odlišné Sudoku čtverce a postup jejich enumerace . . . 18
2.4 Struktura a reprezentanty grupy symetrií Sudoku čtverce 19
2.5 Sudoku čtverce se čtvercovými zónami 23

Závěr **29**

Seznam použité literatury **30**

Úvod

Dva vyplněné Sudoku čtverce považujeme za esenciálně odlišné, jestliže, volně řečeno, neexistuje symetrie Sudoku čtverce, která by převáděla jeden na druhý. Původně zamýšleným cílem této bakalářské práce bylo zopakovat a v ideálním případě zobecnit enumeraci těchto esenciálně odlišných Sudoku čtverců, která je popsána v článku [4], její detaily pak na autorově webu [6],[7]. Postup této enumerace je poměrně přímočarý, sestává ze dvou základních výpočtů: nejprve autoři nalezenou všechny třídy konjugace grupy symetrií Sudoku čtverce a následně pro reprezentant každé třídy určí velikost stabilizátoru. Enumerace je pak dokončena snadnou aplikací Burnsidova lemmatu.

Během studia příslušného článku však autora i vedoucího této práce překvapilo, do jaké míry spoléhají jeho autoři na výpočetní techniku: grupu symetrií Sudoku čtverce totiž analyzují téměř výhradně pomocí softwaru GAP, jehož pomocí nacházejí i třídy konjugace. Jediným hlubším poznatkem teorie grup, který sami aktivně používají, je právě Burnsidovo lemma. Téma bakalářské práce bylo proto posunuto od pouhého zopakování enumerace k teoretičtější otázce – tou je nalezení reprezentantů a velikosti tříd konjugace grupy symetrií Sudoku čtverce pouze za pomoci teoretických poznatků, bez spoléhání na výpočetní techniku (GAP byl používán pouze ke kontrole konkrétních výsledků).

První kapitola této práce shrnuje poznatky o působení grupy na množině a o třídách konjugace, probírané v základních kurzech bakalářského studia (vychází především z textu [2]), a rozšiřuje je především o popis tříd konjugace věncových součinů grup. Druhá kapitola následně formálně definuje Sudoku čtverec a grupu jeho symetrií a ukazuje, že tato grupa je izomorfní direktnímu součinu věncových součinů vhodných grup. Hlavním výsledkem celé práce je výpočet množiny reprezentantů a velikostí tříd konjugace této grupy, a to i v případě, že mezi symetrie Sudoku čtverce počítáme i jeho transpozici. Pomocí tohoto výsledku jsou bez použití výpočetní techniky vyřešeny i dva problémy, řešené s vydatnou pomocí softwaru GAP i autory stránky [6].

Popis tříd konjugace věncového součinu grup a z něj plynoucí analýza struktury a tříd konjugace grupy symetrií Sudoku čtverce jsou původním výsledkem, autorovi ani vedoucímu této práce není znám žádný text, který by se touto otázkou zaobíral. To však neznamená, že takový text neexistuje, vzhledem k přístupnosti obou témat je jeho existence nanejvýš pravděpodobná.

1. Věncové součiny symetrických grup

1.1 Působení grupy na množině

Definice 1.1 (Symetrická a permutační grupa)**.** *Nechť X je množina. Grupu všech permutací množiny X nazveme symetrickou grupou na množině X, značíme ji S_X. Její podgrupy nazveme permutačními grupami. Pokud $X = \{1, \ldots, n\}$, značíme $S_X = S_n$.*

Definice 1.2 (Působení grupy na množině)**.** *Nechť G je grupa, X libovolná množina. Homomorfismus $\psi\colon G \to S_X$ označíme jako působení grupy G na množině X. Pro $g \in G$ zapisujeme hodnotu $\psi(g)$ v bodě $x \in X$ pro jednoduchost jako $g(x)$. Pokud $\operatorname{Ker}\psi = 1$, říkáme, že ψ je věrné působení.*

Pozorování 1.3. *Nechť ψ je věrné působení grupy G na množině X. Pak $G \cong \operatorname{Im}\psi$.*

Důkaz. Podle 1. věty o izomorfismu (viz [2, Věta 1.13]) platí

$$G = G/1 = G/\operatorname{Ker}\psi \cong \operatorname{Im}\psi.$$

□

Definice 1.4 (Orbity tranzitivity)**.** *Nechť G je permutační grupa. Definujme relaci tranzitivity $\sim$ na množině X tak, že $x \sim y$, pokud existuje $g \in G$ takové, že $g(x) = y$. Je zřejmé, že $\sim$ je ekvivalence. Jednotlivé bloky ekvivalence $\sim$ na množině X nazýváme orbity tranzitivity (dále pouze orbity).*

Definice 1.5 (Pevný bod, stabilizátor)**.** *Prvek $x \in X$ označíme za pevný bod prvku $g \in G$ permutační grupy G, jestliže $g(x) = x$. Množinu všech pevných bodů prvku $g \in G$ budeme značit $\operatorname{Fix}(g)$ a nazývat stabilizátor g.*

Pak pokud jsou X a G konečné, pak $|X/\!\sim|$, tj. počet orbit, můžeme spočítat pomocí následujícího vztahu:

Věta 1.6 (Burnsidovo lemma)**.** *Nechť konečná permutační grupa G působí na konečné množině X. Pak*

$$|X/\!\sim| = \frac{1}{|G|} \cdot \sum_{g \in G} |\operatorname{Fix}(g)|$$

Důkaz. Popsán např. v [1, Věta 19.4]. □

Slovy řečeno: počet orbit je roven průměrnému počtu pevných bodů jednotlivých prvků G.

1.2 Součiny grup

Definice 1.7 (Direktní součin)**.** *Nechť $G_i = (G_i, \cdot_i, {}^{-1_i}, 1_i)$, $i = 1,\dots,n$, $n \in \mathbb{N}$ je n-tice grup. Pak jejich direktní součin $G_1 \times \cdots \times G_n$ definujeme jako grupu s operacemi definovanými po složkách, tj.:*

$$\begin{aligned}(a_1,\dots,a_n)\cdot(b_1,\dots,b_n) &= (a_1 \cdot_1 b_1,\dots,a_n \cdot_n b_n)\\ (a_1,\dots,a_n)^{-1} &= (a_1^{-1_1},\dots,a_n^{-1_n})\\ 1 &= (1_1,\dots,1_n)\end{aligned}$$

pro všechna $(a_1,\dots,a_n),(b_1,\dots,b_n) \in G_1 \times \cdots \times G_n$.

Pokud $G_1 = \cdots = G_n = G$, píšeme $G \times \cdots \times G = G^n$ a hovoříme o direktní mocnině G.

Ukazovat, že jsou grupové operace skutečně definovány po složkách, může být krajně nepraktické, daleko efektivnější nástroj k ověření, že je grupa direktním součinem, nám poskytuje následující věta:

Věta 1.8. *Nechť G je grupa, H a K její podgrupy a platí následující tři podmínky:*

- $H \cap K = 1$.
- $G = HK$.
- *Pro všechna $h \in H$ a $k \in K$ platí $hk = kh$.*[1]

Pak $G \cong H \times K$.

Důkaz. Popsán v [2, Tvrzení 4.3]. □

Definice 1.9 (Semidirektní součin)**.** *Nechť H a K jsou grupy a ϱ je homomorfismus $K \to \mathrm{Aut}(H)$. Jako semidirektní součin $H \rtimes_\varrho K$ označíme grupu definovanou na $H \times K$ binární operací $(h_1,k_1) \bullet (h_2,k_2) = (h_1\varrho(k_1)(h_2),k_1k_2)$, inverzním prvkem $(h,k)^{-1} = (\varrho(k^{-1})(h^{-1}),k^{-1})$ a jednotkovým prvkem $(1_H,1_K)$ pro $h_1,h_2,h \in H$ a $k_1,k_2,k \in K$.*

Stejně jako v případě direktního součinu není ani z této definice snadné ověřit, že je nějaká grupa izomorfní semidirektnímu součinu svých podgrup. V tomto případě nám situaci usnadní následující věta:

Věta 1.10. *Nechť G je grupa, H a K její podgrupy a platí následující tři podmínky:*

- $H \cap K = 1$.
- $G = HK$.
- $H \trianglelefteq G$.

Pak $G \cong H \rtimes_\varrho K$ pro homomorfismus $\varrho\colon K \to \mathrm{Aut}(H)$ takový, že $\varrho(k)(h) = khk^{-1}$ pro všechna $h \in H$ a $k \in K$.

[1] Tato podmínka je ekvivalentní tomu, že H i K jsou normální podgrupy G.

Důkaz. Popsán v [2, Tvrzení 4.5] □

Definice 1.11 (Věncový součin)**.** *Nechť H a K jsou grupy, $\psi\colon K \to S_n$ je homomorfismus a $f\colon S_n \to \mathrm{Aut}(H^n)$ je homomorfismus takový, že*

$$f(\sigma)(h_1,\ldots,h_n) = (h_{\sigma(1)},\ldots,h_{\sigma(n)}).^2$$

Součin $H^n \rtimes_{f\circ\psi} K$ nazýváme věncovým součinem $H \wr_\psi K$. Jednotlivé prvky $H \wr_\psi K$ tvaru $((h_1,\ldots,h_n),k)$ budeme pro jednoduchost zapisovat jako $(h_1,\ldots,h_n;k)$. Pokud $K = S_n$ a $H = S_m$, budeme pro účely této práce uvažovat vždy $\psi = \mathrm{id}_{S_n}$. Je-li ψ identické zobrazení, píšeme pouze $H \wr K$.

Chceme-li rozhodnout, zda je grupa G izomorfní věncovému součinu svých podgrup H a K, stačí ověřit, že $G \cong H^n \rtimes_\varrho K$ (zpravidla pomocí věty 1.10), a následně ukázat, že ϱ splňuje definici věncového součinu.

1.3 Konjugované prvky a třídy konjugace

Definice 1.12 (Konjugované prvky a třídy konjugace)**.** *Nechť G je grupa. Řekneme, že permutace g a $h \in G$ jsou konjugované v G, pokud existuje $k \in G$ taková, že $k^{-1}gk = h$ (značíme $h = g^k$). Snadno nahlédneme, že relace být konjugován je ekvivalence na G. Třídy této ekvivalence nazýváme třídy konjugace. Pro prvek $g \in G$ budeme třídu konjugace, jejímž je prvkem, značit g^G.*

Věta 1.13. *Nechť G je konečná permutační grupa. Pokud jsou g a h konjugované v G, mají stejný počet cyklů každé délky.*

Důkaz. Protože G je podgrupa symetrické grupy na konečné množině, jistě každé g a $h = kgk^{-1} \in G$ lze rozložit na cykly, tedy

$$g = (a_{11}\ a_{12}\ \ldots\ a_{1k_1}) \cdots (a_{m1}\ a_{m2}\ \ldots\ a_{mk_m})$$

$$h = kgk^{-1} = (k(a_{11})\ k(a_{12})\ \ldots\ k(a_{1k_1})) \cdots (k(a_{m1})\ k(a_{m2})\ \ldots\ k(a_{mk_m})).$$

Vidíme, že g i h mají stejný počet cyklů každé délky. □

Permutace, které mají stejný počet cyklů každé délky, budeme po zbytek této práce nazývat permutacemi *stejného typu*.

Důsledek 1.14. *Nechť permutační grupa G působí na konečné množině X. Všechny navzájem konjugované permutace mají v tomto působení stejný počet pevných bodů.*

Důkaz. Jsou-li dvě permutace navzájem konjugované, obsahují stejný počet cyklů každé délky, tedy obsahují i stejný počet cyklů délky 1, tedy pevných bodů. □

Definice 1.15 (Množina reprezentantů)**.** *Množinu obsahující právě jeden prvek z každé třídy konjugace na G budeme ve zbytku práce nazývat množinou reprezentantů grupy G. Pro symetrickou grupu S_n budeme množinu reprezentantů značit $\mathcal{R}_n$.*

[2] Je zřejmé, že $f \circ \psi$ je homomorfismus $K \to \mathrm{Aut}(H^n)$.

Přímým dosazením důsledku 1.14 do Burnsidova lemmatu dostáváme následující tvrzení, které pro nás bude ve druhé kapitole mimořádně důležitý.

Důsledek 1.16. *Nechť konečná permutační grupa G působí na konečné množině X. Dále nechť $R \subseteq G$ je množina reprezentantů grupy G a nechť g^G je třída konjugace obsahující prvek g. Pak*

$$|X/\!\sim| = \frac{1}{|G|} \cdot \sum_{g \in R} |g^G| \cdot |\operatorname{Fix}(g)|.$$

Užití tohoto důsledku celý výpočet pomocí Burnsidova lemmatu citelně usnadní – namísto určování velikosti stabilizátoru pro každý prvek G nám totiž stačí najít množinu reprezentantů, pro každý reprezentant spočítat stabilizátor a určit velikost třídy konjugace, kterou zastupuje. V následujících kapitolách tyto množiny reprezentantů pro konkrétní grupy popíšeme.

1.4 Množiny reprezentantů symetrických grup

Pro symetrické grupy platí věta 1.13 jako ekvivalence.

Věta 1.17. *Nechť S_X je symetrická grupa na konečné množině. Permutace g a h jsou konjugované v S_X právě tehdy, když jsou stejného typu.*

Důkaz. Zbývá nám dokázat zpětnou implikaci. Mějme permutace g a h stejného typu, tedy

$$g = (a_{11}\, a_{12}\, \ldots\, a_{1k_1}) \cdots (a_{m1}\, a_{m2}\, \ldots\, a_{mk_m}),$$
$$h = (b_{11}\, b_{12}\, \ldots\, b_{1k_1}) \cdots (b_{m1}\, b_{m2}\, \ldots\, b_{mk_m}).$$

Zvolíme $k \in S_X$ tak, že $k(a_{ij}) = b_{ij}$ (jistě takové k existuje, S_X je množina všech permutací množiny X). Pak $g = khk^{-1}$. □

Pro obecné permutační grupy tato věta neplatí – permutace k, kterou v důkazu volíme, totiž v obecné permutační grupě nemusí ležet.

Definice 1.18 (Číselný rozklad)**.** *Číselným rozkladem čísla $n \in \mathbb{N}$ nazveme konečnou nerostoucí posloupnost přirozených čísel $\lambda = (\lambda_j)_{j=1}^k$ pro nějaké $k \in \mathbb{N}$ takovou, že*

$$n = \lambda_1 + \lambda_2 + \cdots + \lambda_k.$$

Množinu všech číselných rozkladů čísla n budeme značit $\mathcal{P}_n$. Pro $\lambda = (\lambda_j)_{j=1}^k \in \mathcal{P}_n$ a $i \in \{1, \ldots, n\}$ definujeme četnost čísla i v rozkladu λ jako

$$d_i(\lambda) = |\{j \mid \lambda_j = i\}|$$

V dalším textu budeme číselný rozklad λ zapisovat jako $1^{d_1(\lambda)} 2^{d_2(\lambda)} \ldots n^{d_n(\lambda)}$.

Věta 1.19 (Množina reprezentantů symetrické grupy)**.** *Prvky $\mathcal{R}_n$ jsou právě permutace po dvou různých typů s cykly délky $\lambda_1, \ldots, \lambda_k$ pro všechny číselné rozklady $(\lambda_j)_{j=1}^k \in \mathcal{P}_n$.*

Důkaz. Každý prvek $\{1,\dots,n\}$ musí ležet v právě jednom cyklu každé permutace z S_n, tedy součet délek všech cyklů musí být pro každou permutaci právě n. Délky cyklů jsou tedy $\lambda_1,\dots,\lambda_k$ pro nějaký číselný rozklad n. Naopak pro každý číselný rozklad $(\lambda_j)_{j=1}^k$ existuje permutace s cykly délky $\lambda_1,\dots,\lambda_k$, jelikož S_n obsahuje všechny permutace na n prvcích[3]. □

Příklad 1.20 Nalezněte všechny prvky $\mathcal{R}_5$.

Řešení. Nejprve najdeme všechny rozklady z $\mathcal{P}_5$ – těch existuje těchto 7:

$$1^0 2^0 3^0 4^0 5^1, 1^1 2^0 3^0 4^1 5^0, 1^2 2^0 3^1 4^0 5^0, 1^0 2^1 3^1 4^0 5^0, 1^1 2^2 3^0 4^0 5^0, 1^3 2^1 3^0 4^0 5^0, 1^5 2^0 3^0 4^0 5^0.$$

Pro každý z těchto rozkladů nyní nalezneme permutaci s cykly, které mají délky jeho prvků:

- rozkladu $1^0 2^0 3^0 4^0 5^1$ přiřadíme permutaci $(1\,2\,3\,4\,5)$,
- rozkladu $1^1 2^0 3^0 4^1 5^0$ přiřadíme $(1\,2\,3\,4)$,
- rozkladu $1^2 2^0 3^1 4^0 5^0$ přiřadíme $(1\,2\,3)$,
- rozkladu $1^0 2^1 3^1 4^0 5^0$ přiřadíme $(1\,2\,3)\,(4\,5)$,
- rozkladu $1^1 2^2 3^0 4^0 5^0$ přiřadíme $(1\,2)\,(3\,4)$,
- rozkladu $1^3 2^1 3^0 4^0 5^0$ přiřadíme $(1\,2)$,
- rozkladu $1^5 2^0 3^0 4^0 5^0$ přiřadíme identitu.

Tedy $\mathcal{R}_5 = \{(1\,2\,3\,4\,5), (1\,2\,3\,4), (1\,2\,3), (1\,2\,3)\,(4\,5), (1\,2)\,(3\,4), (1\,2), id_{\{1,2,3,4,5\}}\}$. ◀

Definice 1.21 (Centralizátor)**.** *Nechť G je grupa, $g \in G$. Množinu $C_G(g) = \{h \in G \mid hg = gh\}$ nazveme centralizátor prvku g.*

Pozorování 1.22. $C_G(g) = \{h \in G \mid hgh^{-1} = g\}$.

Věta 1.23. *Nechť G je konečná grupa, $g \in G$. Pak*

$$|g^G| = \frac{|G|}{|C_G(g)|}.$$

Důkaz. Důkaz vyložen v [2, Věta 3.10]. □

Věta 1.24 (Velikost třídy konjugace symetrické grupy)**.** *Nechť $g \in S_n$ má cykly délky λ_j pro nějaké $\lambda = (\lambda_j)_{j=1}^k \in \mathcal{P}_n$. Pak*

$$|g^{S_n}| = \frac{n!}{\prod_{j=1}^k \lambda_j \prod_{i=1}^n (d_i(\lambda)!)}.$$

[3] Požadovanou permutací by byla například $(1\,2\,\dots\,\lambda_1)((\lambda_1+1)\,(\lambda_1+2\,\dots\,(\lambda_1+\lambda_2))\cdots((\lambda_1+\lambda_2+\cdots+\lambda_{k-1}+1)\,(\lambda_1+\lambda_2+\cdots+\lambda_{k-1}+2)\,\dots\,(\lambda_1+\lambda_2+\cdots+\lambda_k))$

Důkaz. Podle věty 1.23 a pozorování 1.22 platí

$$|g^G| = \frac{n!}{|C_G(g)|} = \frac{n!}{|\{h \mid hgh^{-1} = g\}|}.$$

Předpokládejme, že $g = (a_{11}\, a_{12}\, \ldots\, a_{1k_1}) \cdots (a_{m1}\, a_{m2}\, \ldots\, a_{mk_m})$. Pak musí platit $hgh^{-1} = (h(a_{11})h(a_{12}) \ldots h(a_{1k_1})) \cdots (h(a_{m1})h(a_{m2}) \ldots h(a_{mk_m}))$. Aby $hgh^{-1} = g$, musí proto permutace h zobrazovat všechny cykly g buď samy na sebe, nebo na jiné cykly stejné délky, pro cyklus délky i máme tedy $d_i(\lambda)!$ možností, kam jej zobrazit, celkem máme $\prod_{i=1}^{n}(d_i(\lambda)!)$ možností. Zobrazujeme-li cyklus délky λ_j, můžeme zvolit jeden z jeho λ_j prvků, který může h zobrazovat na konkrétní prvek obrazu, všechny ostatní jsou již dány jednoznačně. Celkem máme $|C_G(g)| = \prod_{j=1}^{k} \lambda_j \prod_{i=1}^{n}(d_i(\lambda)!)$.

□

Příklad 1.25 Kolik existuje v grupě S_5 permutací složených ze dvou dvojcyklů?

Řešení. Jejich počet je roven $|(1\,2)\,(3\,4)^G|$, což je podle předchozí věty rovno

$$\frac{5!}{2 \cdot 2 \cdot 2! \cdot 1!} = \frac{120}{8} = 15.$$

◀

1.5 Množina reprezentantů součinů grup

Pozorování 1.26 (Konjugované prvky direktního součinu)**.** *Nechť G_1 a G_2 jsou permutační grupy. Pak (g_1,g_2) a $(h_1,h_2) \in G_1 \times G_2$ jsou konjugované v $G_1 \times G_2$ právě tehdy, když g_1 je konjugováno s h_1 a g_2 je konjugováno s h_2.*

Důkaz. $g_1 = k_1 h_1 k_1^{-1}$ a $g_2 = k_2 h_2 k_2^{-1}$ pro vhodné $k_1 \in G_1, k_2 \in G_2$, právě tehdy, když $(g_1,g_2) = (k_1,k_2)(h_1,h_2)(k_1,k_2)^{-1}$. □

Důsledek 1.27 (Množina reprezentantů direktního součinu)**.** *Množinu reprezentantů direktního součinu $G_1 \times G_2$ tvoří právě uspořádané dvojice (r_1,r_2), kde r_1 patří do množiny reprezentantů G_1 a r_2 do množiny reprezentantů G_2.*

Důsledek 1.28. *Nechť $(g_1,g_2) \in G_1 \times G_2$. Pak*

$$|(g_1,g_2)^{G_1 \times G_2}| = |g_1^{G_1}| \cdot |g_2^{G_2}|.$$

Nyní se zaměříme na popis množiny reprezentantů věncového součinu. K tomu budeme potřebovat ještě několik pomocných tvrzení a definic.

Pozorování 1.29. *Pokud jsou (a,b) a (c,d) konjugovány v $H \rtimes_\varrho K$, pak b a d jsou konjugovány v K.*

Důkaz. Pokud jsou (a,b) a (c,d) konjugovány, musí existovat $(u,v) \in H \rtimes_\varrho K$ takové, že

$$(u,v) \bullet (a,b) \bullet (u,v)^{-1} = (c,d).$$

Pak z definice binární operace v semidirektním součinu dostaneme

$$(u\varrho(v)(a\varrho(b)(\varrho(v^{-1})(u^{-1}))), vbv^{-1}) = (c,d).$$

Vidíme, že $d = vbv^{-1}$, a proto b a d jsou konjugovány v K. □

Důsledek 1.30. *Pokud jsou prvky* $(a_1,\dots,a_n;b)$ *a* $(c_1,\dots,c_n;d)$ *konjugovány v grupě* $S_m \wr S_n$*, pak jsou konjugovány i prvky* b *a* d *v* S_n*.*

Definice 1.31 (Zobrazení V)**.** *Definujme zobrazení* $V\colon S_m \wr S_n \to S_{\{1,\dots,m\}\times\{1,\dots,n\}}$ *takové, že pro libovolné* $(a_1,\dots,a_n;b) \in S_m \wr S_n$ *a* $(q,r) \in \{1,\dots,m\} \times \{1,\dots,n\}$ *platí* $V((a_1,\dots,a_n;b))(q,r) = (b(q),a_q(r))$*.*

Pozorování 1.32. *V je věrné působení $S_m \wr S_n$ na množině $\{1,\dots,m\}\times\{1,\dots,n\}$.*

Důkaz. Ukážeme nejprve, že V je působení: z definice věncového součinu

$$(a_1,\dots,a_n;b) \bullet (c_1,\dots,c_n;d) = (a_{d(1)}c_{b(1)},\dots,a_{d(n)}c_{b(n)};bd),$$

tedy

$$V((a_1,\dots,a_n;b) \bullet (c_1,\dots,c_n;d))(q,r) = (bd(q),a_{d(q)}c_q(r)).$$

Zároveň

$$V(a_1,\dots,a_n;b)V(c_1,\dots,c_n;d)(q,r) = V(a_1,\dots,a_n;b)(d(q),c_q(r)) = \\ = (bd(q),a_{d(q)}c_q(r)).$$

Zjistili jsme, že V je homomorfismus $S_m \wr S_n \to S_{\{1,\dots,m\}\times\{1,\dots,n\}}$, tedy působení.

Jediná permutace $(a_1,\dots,a_n;b)$ z $S_m \wr S_n$, pro kterou $V(a_1,\dots,a_n;b)(q,r) = (q,r)$ pro každé $(q.r) \in \{1,\dots,m\} \times \{1,\dots,n\}$, je permutace

$$(id_{\{1,\dots m\}},\dots,id_{\{1,\dots,m\}};id_{\{1,\dots,n\}}),$$

V má proto triviální jádro, jde tedy o věrné působení. □

Důsledek 1.33. $S_m \wr S_n \cong \operatorname{Im} V \leq S_{m\times n}$.

Přechod od abstraktního věncového součinu k podgrupě symetrické grupy nám umožňuje pracovat s cyklickým zápisem permutací, čehož nyní využijeme:

Pozorování 1.34. *Nechť* $(a_1,\dots,a_n;b) \in S_m \wr S_n$*,* $b = (q_{11}\dots q_{1k_1})\cdots(q_{l1}\dots q_{lk_l})$*. Označme* $y_i = a_{q_{ik_i}}\dots a_{q_{i1}}$ *pro každé* $i \in \{1,\dots,n\}$*. Pak* $V(a_1,\dots,a_n;b)$ *obsahuje právě cykly tvaru*

$$((q_{i1},r)\,(q_{i2},a_{q_{i1}}(r))\,\dots\,(q_{ik_i},(a_{q_{ik_i-1}}\dots a_{q_{i1}})(r))(q_1,y_i(r))\dots(q_{ik_i},a_{q_{ik_i-1}}\dots \\ \dots a_{q_{i1}}y_i^{w_r-1}(r))),$$

kde $i \in \{1,\dots,l\}, r \in \{1,\dots,m\}$ *a* w_r *je nejmenší přirozené číslo takové, že* $y_i^{w_r}(r) = r$*. Takovýto cyklus má pro dané* r *délku* $w_r \cdot k_i$*.*

Důkaz. Tato struktura cyklů plyne přímo z definice působení V. □

Poznámka 1.35. *Pro* r_1 *a* r_2 *taková, že existuje* $j \in \mathbb{N} : y_i^j(r_1) = r_2$*, se tyto cykly shodují, tj.*

$$((q_{i1},r_1)\,(q_{i2},a_{q_{i1}}(r_1))\,\dots a_{q_{i1}}y_i^{w_r-1}(r_1))) = \\ = ((q_{i1},r_1)\,(q_{i2},a_{q_{i1}}(r_1))\,\dots a_{q_{i1}}y_i^{w_r-1}(r_1))).$$

Definice 1.36 (Nadcyklus)**.** *Ať* $\alpha = V(a_1,\dots,a_n;b)$ *pro nějaké* $(a_1,\dots,a_n;b) \in S_m \wr S_n$ *a permutace* b *obsahuje cyklus* $(q_1\ q_2\ \dots\ q_k)$*. Označme* $P = \{(q_i,r) \mid i \in \{1,\dots,k\}, r \in \{1,\dots,m\}\}$*. Permutaci* $\alpha \restriction_P$ *nazveme nadcyklus (příslušný cyklu* $(q_1\ q_2\ \dots\ q_k)$*) délky* k*.*

Příklad 1.37. Nechť $\gamma \in S_4 \wr S_3$ je tvaru ((1 2 3),id,(1 2 3 4);(1 2)). Pak $V(\gamma)$ je rovno

((1,1) (2,2) (1,2) (2,3) (1,3) (2,1)) ((1,4) (2,4)) ((3,1) (3,2) (3,3) (3,4)).

Nadcyklus příslušný cyklu (1 2) je ((1,1) (2,2) (1,2) (2,3) (1,3) (2,1)) ((1,4) (2,4)), nadcyklus příslušný cyklu (3) je ((3,1) (3,2) (3,3) (3,4)).

Věta 1.38. *Permutace* $V(\alpha)$ *a* $V(\beta)$ *jsou v grupě* $\operatorname{Im} V$ *konjugovány právě tehdy, když existuje bijekce* Φ*, která každému nadcyklu* $V(\alpha)$ *přiřadí nadcyklus* $V(\beta)$ *stejné délky a typu.*

Důkaz. Pokud popsaná bijekce existuje, pak obsahují $V(\alpha) = V(a_1,\dots,a_n;b)$ a $V(\beta) = V(g_1,\dots,g_n;h)$ stejný počet cyklů každé délky a dle věty 1.17 jsou tedy konjugované v symetrické grupě na $m \times n$ prvcích, tj. $V(\beta) = \sigma V(\alpha)\sigma^{-1}$. Ukážeme, že $\sigma \in \operatorname{Im} V$. Zvolme nějaký nadcyklus permutace $V(\alpha)$. Jeho cykly jsou podle pozorování 1.34 právě tvaru

$$((q_{i1},r_{i11})\,(q_{i2},r_{i21})\ \dots\ (q_{ik_i},r_{ik_i1})\ \dots\ \dots\ (q_{i1},r_{i12})\ \dots\ (q_{ik_i},r_{ik_iw_r})) \tag{1.1}$$

pro nějaké w_r jako v pozorování 1.34. Nyní najdeme nadcyklus permutace $V(\beta)$, na který bijekce Φ zobrazí zvolený nadcyklus. Nalezený nadcyklus permutace $V(\beta)$ je stejné délky a typu, jistě tedy bude obsahovat právě cykly tvaru

$$((s_{j1},t_{j11})\,(s_{j2},t_{j21})\ \dots\ (s_{jk_j},t_{jk_j1})\ \dots\ \dots\ (s_{j1},t_{j12})\ \dots\ (s_{jk_j},t_{jk_jw_r})).$$

Uvažujme permutaci $\mu \in S_n$ takovou, že pro $\mu(q_{iu}) = (s_{ju})$, a dále permutace $\nu_i \in S_n$ takové, že $\nu_i(r_{iuv}) = t_{juv}$, $u \in \{1,\dots,k_i\}, v \in \{1,\dots,w_r\}$. Zřejmě $\sigma = V(\nu_1,\dots,\nu_n;\mu) \in \operatorname{Im} V$. Pokud permuace $V(\alpha)$ obsahuje cyklus 1.1, pak permutace $\sigma V(\alpha)\sigma^{-1}$ obsahuje cyklus

$$\begin{aligned}(\sigma(q_{i1},r_{i11})\ \dots\ \sigma(q_{ik_i},r_{k11})\ \dots\ \sigma(q_{i1},r_{i12})\ \dots\ \sigma(q_{ik_i},r_{ik_iw_r})) &= \\ = ((\mu(q_{i1}),\nu_{q_{i1}}(r_{i11})\ \dots\ (\mu(q_{ik_i}),\nu_{q_{ik_i}}(r_{ik_i1}))\ \dots& \\ \dots\ ((\mu(q_{i1}),\nu_{q_{i1}}(r_{i12})\ \dots\ (\mu(q_{ik_i}),\nu_{q_{ik_i}}(r_{ikw_r})) &= \\ = ((s_{j1},t_{j11})\ \dots\ (s_{jk_j},t_{jk_j1})\ \dots\ (s_{j1},t_{j12})\ \dots\ (s_{jk_j},t_{jk_jw_r})).&\end{aligned}$$

Nalezli jsme permutaci σ z $\operatorname{Im} V$ takovou, že $\sigma V(\alpha)\sigma^{-1}$ má všechny cykly shodné jako $V(\beta)$, tedy $\sigma V(\alpha)\sigma^{-1} = V(\beta)$, a tedy $V(\alpha)$ a $V(\beta)$ jsou konjugovány v $\operatorname{Im} V$.

Jsou-li naopak permutace $V(\alpha) = V(a_1,\dots,a_n;b)$ a $V(\beta) = V((c_1,\dots,c_n;d)$ konjugovány v $\operatorname{Im} V$, pak pokud nějaký nadcyklus $V(\alpha)$ obsahuje cyklus

$$((q_1,r_1)(q_2,r_2)\ \dots\ (q_k,r_k)),$$

pak musí nějaký nadcyklus $V(\beta)$ obsahovat cyklus

$$(\sigma(q_1,r_1)\sigma(q_2,r_2)\ \dots\ \sigma(q_k,r_k)).$$

Toto musí platit pro všechny cykly příslušných nadcyklů $V(\alpha)$ a $V(\beta)$, pro každý nadcyklus $V(\alpha)$ proto můžeme najít nadcyklus $V(\beta)$, na který jej Φ zobrazí. □

Důsledek 1.39. *Permutace α a $\beta \in S_m \wr S_n$ jsou konjugovány právě tehdy, když existuje bijekce Φ, která každému nadcyklu $V(\alpha)$ přiřadí nadcyklus $V(\beta)$ stejné délky a typu.*

Definice 1.40 (Množina $\mathcal{R}_{m\wr n}$)**.** *Mějme permutaci $\kappa \in \mathcal{R}_n$ s cykly délek λ_j pro nějaké $\lambda = (\lambda_j)_{j=1}^k$. Pro každé $i \in \{1,\dots,n\}$ označme P_i množinu všech $p \in \{1,\dots,n\}$ takových, že p je nejmenší prvek nějakého cyklu permutace κ o délce i.*[4] *Označme dále K_i množinu všech i-členných kombinací prvků $\mathcal{R}_m$ s opakováním.*

Pak množinu R_κ definujeme jako množinu všech $(a_1,\dots,a_n;\kappa) \in S_m \wr S_n$ takových, že:

- *pro všechny koeficienty $p_1,\dots,p_{d_i(\lambda)} \in P_i$ platí $a_{p_1} = r_1,\dots,a_{p_{d_i(\lambda)}} = r_{d_i(\lambda)}$, kde $\{r_1,\dots,r_{d_i(\lambda)}\}$ je $d_i(\lambda)$-členná kombinace s opakováním procházející celé $K_{d_i(\lambda)}$.*
- *pro všechna p, která nejsou prvky P_i pro žádné $i \in \{1,\dots,n\}$, bude $a_p = \mathrm{id}_{\{1,\dots,n\}}$.*

Nyní definujeme množinu $\mathcal{R}_{m\wr n}$ následovně:

$$\mathcal{R}_{m\wr n} = \bigcup_{\kappa\in\mathcal{R}_n} R_\kappa.$$

Příklad této množiny pro konktrétní m a n může čtenář nalézt v příkladu 2.21. Nyní ukážeme, že $\mathcal{R}_{m\wr n}$ je hledanou množinou reprezentantů. Nejprve dokážeme pomocné pozorování:

Pozorování 1.41. *Nechť $\kappa \in \mathcal{R}_n$ obsahuje cyklus $(q_1\, q_2\, \dots\, q_k)$, jehož nejmenším prvkem je x. Dále nechť $(a_1,\dots,a_n;\kappa) \in \mathcal{R}_{m\wr n}$ a $a_x \in \mathcal{R}_m$ má j cyklů o délkách $l_1,\dots,l_j$. Pak $V(a_1,\dots,a_n;\kappa)$ obsahuje v nadcyklu příslušném $(q_1\, q_2\, \dots\, q_k)$ právě j cyklů délek $k\cdot l_1,\dots,k\cdot l_j$.*

Důkaz. Podle pozorování 1.34 jsou pro jednotlivá $r \in \{1,\dots,m\}$ cykly obsažené v nadcyklu délky $w_r \cdot k$, kde w_r je nejmenší přirozené číslo takové, že

$$(a_{q_k} \circ \dots \circ a_{q_k})^{w_r}(r) = r.$$

Pro všechna $q_i \neq x$ je $a_{q_k} = \mathrm{id}_{\{1,\dots,n\}}$, proto

$$(a_{q_k} \circ \dots \circ a_{q_k})^{w_r} = a_x^{w_r}(r).$$

Tedy w_r je rovno délce cyklu v permutaci a_x, v němž příslušné r leží. □

Věta 1.42 (Množina reprezentantů věncového součinu symetrických grup)**.** *Množina $\mathcal{R}_{m\wr n}$ je množina reprezentantů grupy $S_m \wr S_n$.*

Důkaz. Zvolíme dvě různé permutace $\alpha = (a_1,\dots,a_n;\kappa)$ a $\beta = (b_1,\dots,b_n;\lambda) \in \mathcal{R}_{m\wr n}$. Pokud $\kappa \neq \lambda$, pak κ a λ nejsou konjugovány v S_n a podle pozorování 1.30 nejsou konjugovány ani $V(\alpha)$ a $V(\beta)$, tedy ani α a β. Pokud $\kappa = \lambda$, pak musí existovat $i \in \{1,\dots,n\}$ takové, že $a_i \neq b_i$ (jinak $\alpha = \beta$). Pak ale a_i a b_i mají

[4] Zřejmě $|P_i| = d_i(\lambda)$, P_i jsou pro různá i disjunktní a vždy bude velká část těchto množin prázdná.

jiný počet cyklů nějaké délky, podle pozorování 1.41 mají i $V(\alpha)$ a $V(\beta)$ různý počet cyklů nějaké délky, tedy podle věty 1.38 a jejího důsledku nejsou α a β konjugovány v $S_m \wr S_n$.

Do množiny reprezentantů jsme tedy zahrnuli skutečně nejvýše jeden prvek z každé třídy konjugace. Ukážeme nyní, že z každé třídy konjugace jsme zahrnuli alespoň jeden. Protože κ volíme z $\mathcal{R}_n$, můžeme dostat κ se všemi přípustnými délkami cyklů a tedy permutace z $\mathcal{R}_{m\wr n}$ mají všechny přípustné délky nadcyklů. Cykly každého nadcyklu délky k mají (podle pozorování 1.41) délky $k \cdot l_y$, kde l_y jsou právě délky cyklů permutace $a \in \mathcal{R}_m$ – ta existuje pro všechny přípustné délky cyklů, a tedy všechny permutace z $\mathcal{R}_{m\wr n}$ mají i všechny přípustné typy jednotlivých nadcyklů. □

Definice 1.43. *Nechť $(a_1,\dots,a_n;\kappa) \in \mathcal{R}_{m\wr n}$. Pak pro $\iota \in \{1,\dots,n\}, a \in \mathcal{R}_m$ označíme $e(\iota,a)$ počet permutací $a_j, j \in \{1,\dots,n\}$ takových, že j je nejmenší prvek nějakého cyklu κ délky ι a a_j je stejného typu jako a.*

Pozorování 1.44. *Pokud a má cykly délky $l_1,\dots,l_k$, pak $e(\iota,a)$ je rovno počtu nadcyklů délky ι a cyklů délek $\iota \cdot l_1,\dots,\iota \cdot l_k$ v permutaci $V(a_1,\dots,a_n;\kappa)$.*

Věta 1.45 (Velikost třídy konjugace věncového součinu)**.** *Nechť $\alpha \in \mathcal{R}_{m\wr n}$ je tvaru $\alpha = (a_1,\dots,a_n;\kappa)$, κ má cykly délky λ_j pro nějaké $\lambda = (\lambda_j)_{j=1}^k \in \mathcal{P}_n$. Dále nechť $P = P_1 \cup \dots \cup P_n$, kde $P_1,\dots,P_n$ jsou jako v definici 1.40. Pro permutaci $a_p, p \in P$ označíme délky jejích cyklů jako $l_{p1},\dots,l_{pk_p}$, kde $(l_{pi})_{i=1}^{k_p} = l_p \in \mathcal{P}_m$. Pak*

$$|\alpha^{S_m\wr S_n}| = \frac{(m!)^n n!}{\prod_{j=1}^k \lambda_j \prod_{\iota=1}^n (\prod_{a\in\mathcal{R}_m} (e(\iota,a)!)) \prod_{p\in P} (\prod_{y=1}^{pk_p} l_{py} \prod_{i=1}^m (d_i(l_p)!))}.$$

Důkaz. Jde o přímočaré dosazení do rovnosti z věty 1.23 - čitatel zlomku získáme snadno, neboť $|S_m \wr S_n| = |(S_m)^n \rtimes_\varrho S_n| = (m!)^n n!$, zbývá určit velikost centralizátoru dané permutace. Podle pozorování 1.22 $|C_{S_m\wr S_n}(g)| = |C_{\mathrm{Im}(V)}(V(g))| = |\{h \in \mathrm{Im}(V) \mid hV(g)h^{-1} = g\}|$.

Permutace $V(g)$ i $hV(g)h^{-1}$ má stejné nadcykly každé délky a typu, pro nadcykly délky ι, kterých $V(g)$ obsahuje $d_\iota(\lambda)$, je proto $\prod_{a\in\mathcal{R}_m} \iota^{e(\iota,a)} \cdot (e(\iota,a))!$ možností, jak je h může zobrazit. Pro všechna přípustná ι proto dostáváme celkem $\prod_{j=1}^k \lambda_j \prod_{\iota=1}^n (\prod_{a\in\mathcal{R}_m} (e(\iota,a)!))$.

Každá permutace $a_p, p \in P$ určuje strukturu cyklů v jednom nadcyklu – má-li a_p $d_i(l_p)$ cyklů délky i, má tento počet cyklů délky $k \cdot i$ i nadcyklus, jehož je p nejmenším prvkem. Permutace h musí cykly této permutace zobrazit na cykly stejné délky, máme tedy $i^{d_i(l_p)} \cdot (d_i(l_p))!$ možností, jak je zobrazit, celkem má h pro dané p právě $(\prod_{y=1}^{pk_p} l_{py} \prod_{i=1}^m (d_i(l_p))!)$ možností, pro všechna p dohromady máme tedy $\prod_{p\in P} (\prod_{y=1}^{pk_p} l_{py} \prod_{i=1}^m (d_i(l_p))!)$. Tímto již máme permutaci h určenou jednoznačně.

□

Příklad 1.46 Určete počet prvků třídy konjugace permutace

$$\gamma = ((1\,2\,3),\mathrm{id},(1\,2)(3\,4),\mathrm{id},(1\,2\,3),\mathrm{id};(1\,2)(3\,4)(5\,6)) \in S_4 \wr S_6.$$

Řešení. Určíme nejprve $e(\iota,a)$ pro všechna ι a a: permutace (1 2) (3 4) (5 6) obsahuje pouze cykly délky 2, tedy $e(\iota,a)$ bude pro $\iota \neq 2$ rovno nule. Na prvním

a pátém místě permutace γ jsou permutace (1 2 3), proto $e(2,(1\,2\,3)) = 2$. Dále $e(2,(1\,2)\,(3\,4) = 1$, pro ostatní $a \in \mathcal{R}_m$ $e(2,a) = 0$. Očividně $P = \{1,3,5\}, l_1 = l_5 = 1^1 2^0 3^1 4^0, l_3 = 1^0 2^2 3^0 4^0, \lambda = 1^0 2^3 3^0 4^0 5^0 6^0$. Po dosazení dostaneme rovnost

$$|\gamma^{S_4 \wr S_6}| = \frac{(4!)^6 6!}{2^3(2! \cdot 1!)(3 \cdot 1)^2(2 \cdot 2)(2! \cdot 1!)} = \frac{137594142720}{1152} = 119439360.$$

◀

2. Počítání Sudoku čtverců

Nyní se přesuneme od obecné teorie grup ke konkrétní úloze a poznatky z předchozí kapitoly aplikujeme na Sudoku čtverce a grupu jejich symetrií. Nejprve přiblížíme, co vůbec je Sudoku čtverec a k čemu potřebujeme řešit jeho symetrie, v dalších kapitolách tyto pojmy vhodně formálně definujeme.

2.1 Přirozený popis Sudoku čtverce a motivace

Za (vyplněný) Sudoku čtverec stupně $m \times n$ je běžné považovat tabulku, která má $(m \cdot n) \times (m \cdot n)$ buňek, rozdělenou do:

- m disjunktních *pásů* tak, že jeden pás tvoří vždy n sousedních řádků,
- n disjunktních *komínků* tak, že jeden komínek tvoří vždy m sousedních sloupců.[1]

Průniky jednotlivých pásů a komínků budou zjevně obdélníkové tabulky s $n \times m$ prvky, které budeme nazývat *zóny*.

Buňky této tabulky jsou vyplněny číslicemi mezi 1 a $m \cdot n$ tak, že každá číslice je umístěna právě jednou v každém řádku, v každém sloupci a v každé zóně, Sudoku čtverec je proto speciálním případem latinského čtverce.

Dále můžeme definovat *hlavolam Sudoku stupně* $m \times n$ jako Sudoku čtverec stupně $m \times n$, v němž některé buňky necháme prázdné. Řekneme nyní, že hlavolam Sudoku je *korektně zadaný*, pokud jej lze doplnit do Sudoku čtverce právě jedním způsobem. Nejběžnější hlavolam Sudoku je stupně 3×3.

První enumerační úloha, která nás nyní může napadnout, je spočítat, kolik Sudoku čtverců daného stupně $m \times n$ existuje. Pro čtverce stupně 3×3 tuto enumeraci popisuje článek [3], jehož autoři za vydatné pomoci výpočetní techniky došli k výsledku 6670903752021072936960, tedy zhruba $6{,}67 \cdot 10^{21}$.

Tento výsledek je jistě zajímavý, vidíme ale, že Sudoku čtverce, které autoři počítali jako různé, se od sebe leckdy liší jen nepatrně – jediný rozdíl může být třeba záměna dvou sloupců v tomtéž komínku.

Pokud však řešíme hlavolam Sudoku, nejsou pro nás některé rozdíly mezi Sudoku čtverci podstatné: dostaneme-li zadané dva hlavolamy, které se liší pouze tím, že jsou v jednom z nich všechny jedničky nahrazeny za dvojky a naopak, na první pohled poznáme, že jde vlastně o tentýž hlavolam, stačí vyřešit pouze jeden a druhý doplnit podle něj. Vidíme, že na konkrétních číslicích příliš nezáleží – podstatné je především to, na kterých $m \cdot n$ pozicích se nacházejí stejné číslice. V kapitole 2.2 proto vyslovíme novou definici Sudoku čtverece, která bude čtverce, mezi nimiž je rozdíl pouze v permutaci číslic, považovat za stejné.

Jedna z nejzajímavějších otázek souvisejících s hlavolamy Sudoku je, kolik buněk v daném Sudoku čtverci můžeme nechat prázdných, aby byl vzniklý hlavolam stále ještě korektně zadán. Toto zjevně nezmění permutace číslic v celém Sudoku čtverci, krom toho ale ani následující permutace buněk:

[1] V anglofonním prostředí bývají pásy nazývány *band* a komínky *stack*, v češtině není autorovi známo žádné ustálené názvosloví.

- permutace pásů daného Sudoku čtverce,
- permutace řádků v jednotlivých pásech,
- permutace komínků daného Sudoku čtverce,
- permutace sloupců v jednotlivých komíncích.

Vidíme, že tyto permutace a jejich složení zachovávají Sudoku čtverec daného stupně Sudoku čtvercem téhož stupně. Až je v části 2.2 formálně popíšeme, budeme je nazývat symetriemi Sudoku čtverce.

S pomocí tohoto pozorování se podařilo dokázat i následující mimořádně zajímavý poznatek, publikovaný v článku [5]:

Věta 2.1. *Neexistuje žádný korektně zadaný hlavolam Sudoku stupně* 3×3*, který by měl vyplněných méně než 17 buněk.*

Důkaz byl proveden hrubou silou – autoři vytvořili velmi efektivní algoritmus, pomocí nějž byli schopni velmi rychle ukázat, že z konkrétního Sudoku čtverce není možné vypustit více než 64 číslic. Pokud by však měli tímto způsobem testovat všech zhruba $6{,}67 \cdot 10^{21}$ Sudoku čtverců stupně 3×3, trval by jim i tak celý výpočet několik bilionů let. Autoři proto s výhodou využili skutečnosti, že ze čtverců, které se liší pouze výše uvedenými symetriemi a záměnou číslic, je možné vypustit stejný počet číslic – namísto všech Sudoku čtverců lze tedy testovat jen ty, které se liší víc, než jen symetriemi a záměnou číslic[2]. Otestovat proto stačilo pouze zhruba $5{,}47 \cdot 10^9$ čtverců, tedy o dvanáct řádů méně[3].

Vidíme, že pro některé účely je mnohem zajímavějším objektem než jeden Sudoku čtverec celá množina Sudoku čtverců taková, že jeden čtverec z ní lze převést na druhý výše uvedenými permutacemi řádků, sloupců a číslic.

Problémem, jehož řešení tato práce popisuje, je enumerace těchto množin Sudoku čtverců.

2.2 Formální definice Sudoku čtverce a jeho symetrií

Pohled na Sudoku čtverec uvedený v předchozích kapitolách je sice intuitivní, nicméně pro další práci s jeho symetriemi není příliš pohodlný. Proto jej nahradíme následující definicí.

Definice 2.2 (Buňka Sudoku čtverce)**.** *Buňku Sudoku čtverce stupně* $m \times n$ *definujeme jako uspořádanou čtveřici hodnot* $(a,i,b,j) \in \{1,\ldots,m\} \times \{1,\ldots,n\} \times \{1,\ldots,n\} \times \{1,\ldots,m\}$*, kde* a *odpovídá číslu pásu, v němž se buňka nachází,* i *číslu řádku v tomto pásu,* b *odpovídá číslu komínku, v němž se buňka nachází, a* j *číslu sloupce v tomto komínku. Řekneme, že tato buňka patří do řádku* (a,i) *a sloupce* (b,j)*.*

[2]Protože Sudoku čtverce stupně 3×3 mají čtvercové zóny, je možné mezi příslušné symetrie zařadit i transpozici Sudoku čtverce, tj. záměnu řádků a sloupců – i ta zachovává Sudoku čtverec stupně 3×3 Sudoku čtverci stupně 3×3.

[3]Sudoku čtverců, které testovali, bylo přesně 5472730538. I tak však celý výpočet zabral téměř rok.

Definice 2.3 (Transverzála Sudoku čtverce)**.** *Transverzálou Sudoku čtverce nazveme množinu buněk* $\mathbf{u}$ *takovou, že pro dvě buňky* $(a_1.i_1,b_1,j_1)$, $(a_2,i_2,b_2,j_2) \in \mathbf{u}$ *platí:*

- $(a_1,i_1) \neq (a_2,i_2)$*, tedy buňky neleží ve stejném řádku,*
- $(b_1,j_1) \neq (b_2,j_2)$*, tedy buňky neleží ve stejném sloupci,*
- $(a_1,b_1) \neq (a_2,b_2)$*, tedy buňky neleží ve stejné zóně.*

Transverzála reprezentuje všechny buňky, v nichž je v Sudoku čtverci vepsaná stejná číslice.

Definice 2.4 (Sudoku čtverec)**.** *Sudoku čtverec stupně* $m \times n$ *je neuspořádaná* $(m \cdot n)$*-tice takových transverzál, která mají prázdný průnik*[4]*.*

Na Sudoku čtverec tedy můžeme nahlížet jako na rozklad množiny buněk do $m \cdot n$ transverzál. Tím, že je Sudoku čtverec neuspořádanou $(m \cdot n)$-ticí, není dáno, která číslice bude ve kterém transverzále[5].

Množinu všech Sudoku čtverců stupně $m \times n$ budeme dále značit $\mathcal{Q}_{m \times n}$.

Příklad 2.5 Zapište formálně následující Sudoku čtverec $\mathbf{S}$ (a s ním i všechny, které se od něj liší pouze záměnou číslic 1–9):

6	8	7	5	2	3	1	9	4
4	3	2	7	1	9	8	6	5
5	9	1	4	8	6	7	2	3
1	5	9	3	7	4	2	8	6
3	6	8	2	9	5	4	7	1
7	2	4	1	6	8	5	3	9
9	4	6	8	5	2	3	1	7
2	7	3	6	4	1	9	5	8
8	1	5	9	3	7	6	4	2

Obrázek 2.1: Příklad Sudoku čtverce stupně 3×3

Řešení. $\mathbf{S} = \{\mathbf{u_1},\mathbf{u_2},\mathbf{u_3},\mathbf{u_4},\mathbf{u_5},\mathbf{u_6},\mathbf{u_7},\mathbf{u_8},\mathbf{u_9}\}$, kde[6]:

- $\mathbf{u_1} = \{(1,1,3,1),(1,2,2,2),(1,3,1,3),(2,1,1,1),(2,2,3,3),(2,3,2,1),(3,1,3,2),(3,2,2,3),(3,3,1,2)\}$,

[4]Díky tomu, že mají prázdný průnik, musí být každá buňka nejvýše v jedné transverzále. Protože v každé transverzále je $m \cdot n$ buněk a transverzál je celkem $m \cdot n$, máme dohromady $m^2 \cdot n^2$ buněk, tedy každá buňka Sudoku čtverce je v právě jedné transverzále.

[5]Jeden Sudoku čtverec v tomto pojetí odpovídá hned $(m \cdot n)!$ vyplněným tabulkám, které se liší jen permutacemi číslic.

[6]$\mathbf{u_i}$ značíme pro přehlednost transverzálu, v níž je na obrázku číslice i.

- $\mathbf{u_2}$ = {(1,1,2,2),(1,1,1,3),(1,1,3,2),(2,1,3,1),(2,2,2,1),(2,3,1,2),(3,1,2,3), (3,2,1,1),(3,3,3,3)},
- $\mathbf{u_3}$ = {(1,1,2,3),(1,2,1,2),(1,3,1,3),(2,1,2,1),(2,2,1,1),(2,3,3,2),(3,1,3,1), (3,2,1,3),(3,3,2,2)},
- $\mathbf{u_4}$ = {(1,1,3,3),(1,2,1,1),(1,3,2,1),(2,1,2,3),(2,2,3,1),(2,3,1,3),(3,1,1,2), (3,2,2,2),(3,3,3,2)},
- $\mathbf{u_5}$ = {(1,1,2,1),(1,2,3,3),(1,3,1,1),(2,1,2,1),(2,2,2,3),(2,3,3,1),(3,1,2,2), (3,2,3,2),(3,3,1,3)},
- $\mathbf{u_6}$ = {(1,1,1,1),(1,2,3,2),(1,3,2,3),(2,1,3,3),(2,2,1,2),(2,3,2,2),(3,1,1,3), (3,2,2,1),(3,3,3,1)},
- $\mathbf{u_7}$ = {(1,1,1,3),(1,2,2,1),(1,3,3,1),(2,1,2,2),(2,2,3,2),(2,3,1,1),(3,1,3,3), (3,2,1,2),(3,3,2,3)},
- $\mathbf{u_8}$ = {(1,1,1,2),(1,2,3,1),(1,3,2,2),(2,1,3,2),(2,2,1,3),(2,3,2,3),(3,1,2,1), (3,2,3,3),(3,3,1,1)},
- $\mathbf{u_9}$ = {(1,1,3,2),(1,2,2,3),(1,3,1,2),(2,1,1,3),(2,2,2,2),(2,3,3,3),(3,1,1,1), (3,2,3,1),(3,3,2,1)}.

◀

Všechny permutace množiny Sudoku čtverců z kapitoly 2.1 můžeme nyní formálně definovat jako působení vhodné grupy na množině $\mathcal{Q}_{m\times n}$.

Definice 2.6 (Permutace pásů)**.** *Permutaci pásů definujeme jako působení A symetrické grupy S_m na $\mathcal{Q}_{m\times n}$ takové, že pro $\varphi \in S_m, \mathbf{S} \in \mathcal{Q}_{m\times n}$ platí*

$$A(\varphi)(\mathbf{S}) = \{(\varphi(a),i,b,j) \mid (a,i,b,j) \in \mathbf{u}, \mathbf{u} \in \mathbf{S}\}.$$

Definice 2.7 (Permutace řádků)**.** *Permutaci řádků v jednotlivých pásech definujeme jako působení I permutační grupy $(S_n)^m$ na $\mathcal{Q}_{m\times n}$, které pro $(\varphi_1,\ldots,\varphi_m) \in (S_n)^m, \mathbf{S} \in \mathcal{Q}_{m\times n}$ splňuje*

$$I(\varphi_1,\ldots,\varphi_m)(\mathbf{S}) = \{(a,\varphi_a(i),b,j) \mid (a,i,b,j) \in \mathbf{u}, \mathbf{u} \in \mathbf{S}\}.$$

Definice 2.8 (Permutace komínků)**.** *Permutaci komínků definujeme jako působení B permutační grupy S_n na $\mathcal{Q}_{m\times n}$, které pro $\varphi \in S_n, \mathbf{S} \in \mathcal{Q}_{m\times n}$ splňuje*

$$B(\varphi)(\mathbf{S}) = \{(a,i,\varphi(b),j) \mid (a,i,b,j) \in \mathbf{u}, \mathbf{u} \in \mathbf{S}\}.$$

Definice 2.9 (Permutace sloupců)**.** *Permutaci sloupců v jednotlivých komínících definujeme jako působení J permutační grupy $(S_m)^n$ na $\mathcal{Q}_{m\times n}$ takové, že pro $(\varphi_1,\ldots,\varphi_n) \in (S_m)^n, \mathbf{S} \in \mathcal{Q}_{m\times n}$ bude*

$$J(\varphi_1,\ldots,\varphi_n)(\mathbf{S}) = \{(a,i,b,\varphi_b(j)) \mid (a,i,b,j) \in \mathbf{u}, \mathbf{u} \in \mathbf{S}\}.$$

Věta 2.10. *Působení A,B,I a J jsou věrná.*

Důkaz. Stačí ukázat, že mají všechna tato působení triviální jádro:

- $A(\varphi)(\mathbf{S}) = \{(\varphi(a),i,b,j) \,|\, (a,i,b,j) \in \mathbf{u}, \mathbf{u} \in \mathbf{S}\}$, proto pokud pro každý Sudoku čtverec $\mathbf{S}$ platí $A(\varphi)(\mathbf{S}) = \mathbf{S}$, musí platit $\varphi(a) = a$ pro každé $a \in \{1,\ldots,m\}$, jinak by $(\varphi(a),i,b,j)$ nemohlo patřit do téže transverzály $\mathbf{u}$ jako (a,i,b,j), protože v $\mathbf{u}$ leží jen jedna buňka ze sloupce (b,j). Tedy $\varphi = \mathrm{id}_{S_m}$, a tím pádem $\operatorname{Ker} A = \mathrm{id}_{\mathcal{Q}_{m\times n}}$.
- $I(\varphi_1,\ldots,\varphi_m)(\mathbf{S}) = \{(a,\varphi_a(i),b,j) \,|\, (a,i,b,j) \in \mathbf{u}, \mathbf{u} \in \mathbf{S}\}$, proto pokud pro každý Sudoku čtverec $\mathbf{S}$ platí $I(\varphi_1,\ldots,\varphi_m)(\mathbf{S}) = \mathbf{S}$, musí platit $\varphi_k(i) = i$ pro každé $k \in \{1,\ldots,m\}, i \in \{1,\ldots,n\}$, tím pádem $\varphi_k = \mathrm{id}_{S_n}$, proto $\operatorname{Ker} I = \mathrm{id}_{\mathcal{Q}_{m\times n}}$.
- $B(\varphi)(\mathbf{S}) = \{(a,i,\varphi(b),j) \,|\, (a,i,b,j) \in \mathbf{u}, \mathbf{u} \in \mathbf{S}\}$, proto pokud pro každý Sudoku čtverec $\mathbf{S}$ platí $B(\varphi)(\mathbf{S}) = \mathbf{S}$, musí platit $\varphi(b) = b$ pro každé $b \in \{1,\ldots,n\}$, tedy $\varphi = \mathrm{id}_{S_n}$, a tím pádem $\operatorname{Ker} B = \mathrm{id}_{\mathcal{Q}_{m\times n}}$.
- $J(\varphi_1,\ldots,\varphi_n)(\mathbf{S}) = \{(a,i,b,\varphi_b(i)) \,|\, (a,i,b,j) \in \mathbf{u}, \mathbf{u} \in \mathbf{S}\}$, proto pokud pro každý Sudoku čtverec $\mathbf{S}$ platí $J(\varphi_1,\ldots,\varphi_n)(\mathbf{S}) = \mathbf{S}$, musí platit $\varphi_k(i) = i$ pro každé $k \in \{1,\ldots,n\}, i \in \{1,\ldots,m\}$, tím pádem $\varphi_k = \mathrm{id}_{S_m}$, proto $\operatorname{Ker} J = \mathrm{id}_{\mathcal{Q}_{m\times n}}$.

□

Označme nyní $H_A = \operatorname{Im} A$, $H_I = \operatorname{Im} I$, $H_B = \operatorname{Im} B$ a $H_J = \operatorname{Im} J$. Věta 2.10 nám spolu s pozorováním 1.3 dá následující důsledek:

Důsledek 2.11. *H_A, H_I, H_B a H_J jsou permutační grupy na $\mathcal{Q}_{m\times n}$, $H_A \cong S_m, H_I \cong (S_n)^m, H_B \cong S_n$ a $H_J \cong (S_m)^n$.*

Definice 2.12 (Symetrie Sudoku čtverce)**.** *Grupu generovanou grupami H_A, H_I, H_B a H_J označíme G a její prvky budeme nazývat symetrie Sudoku čtverce.*

2.3 Esenciálně odlišné Sudoku čtverce a postup jejich enumerace

Definice 2.13 (Ekvivalentní a esenciálně odlišné Sudoku čtverce)**.** *Na množině Sudoku čtverců $\mathcal{Q}_{m\times n}$ definujme relaci $\sim$ tak, že pro Sudoku čtverce $\mathbf{S}_1, \mathbf{S}_2$ platí $\mathbf{S}_1 \sim \mathbf{S}_2$, pokud existuje $g \in G$ takové, že $g(\mathbf{S}_1) = \mathbf{S}_2$. Zřejmě $\sim$ je ekvivalence. Pokud pro dva Sudoku čtverce platí $\mathbf{S}_1 \sim \mathbf{S}_2$, řekneme, že jsou ekvivalentní, dva bloky ekvivalence $\sim$ na $\mathcal{Q}_{m\times n}$ pak nazveme esenciálně odlišné Sudoku čtverce stupně $m \times n$.*

Otázku, jejíž řešení budu ve zbytku práce popisovat, můžeme tedy položit takto: Kolik existuje esenciálně odlišných Sudoku čtverců daného řádu?

Pozorování 2.14. *$\sim$ je relace tranzitivity na množině $\mathcal{Q}_{m\times n}$ a esenciálně odlišné Sudoku čtverce jsou její orbity.*

Počet esenciálně odlišných Sudoku čtverců je tedy počtem orbit působení grupy G, k jejichž spočtení můžeme využít Burnsidovo lemma (větu 1.6). To nám dává rovnost

$$|\mathcal{Q}_{m\times n}/{\sim}| = \frac{1}{|G|} \cdot \sum_{g\in G} |\operatorname{Fix}(g)|.$$

Může se zdát, že máme vyhráno; než se začneme radovat, musíme si uvědomit, že pro každé $g \in G$ by bylo třeba určit $|\operatorname{Fix}(g)|$, pro což obecně nemáme k dispozici žádný efektivnější nástroj než hrubou sílu – v nejhorším případě testování všech Sudoku čtverců z $\mathcal{Q}_{m\times n}$. Prvků G je navíc poměrně velké množství[7].

Proto namísto přímé aplikace Burnsidova lemmatu aplikujeme důsledek 1.16: najdeme vhodnou množinu reprezentantů $R \subseteq G$ takovou, že v R leží právě jeden prvek z každé třídy konjugace grupy G. Pak získáme:

$$|\mathcal{Q}_{m\times n}/{\sim}| = \frac{1}{|G|} \cdot \sum_{g\in R} |g^G| \cdot |\operatorname{Fix}(g)|.$$

Tento krok představuje zásadní urychlení výpočtu – není třeba počítat stabilizátor pro všechny prvky grupy G, stačí to pouze pro prvky její množiny reprezentantů, kterých je o mnoho řádů méně[8].

Ed Russel a Frazer Jarvis, kteří tento výpočet jako první provedli, nejprve pro danou grupu symetrií pomocí výpočetního softwaru GAP nalezli množinu reprezentantů, načež pro její prvky pomocí vlastního programu spočítali velikost stabilizátoru. V následující kapitole uvidíme, že první část tohoto výpočtu dokážeme pro grupu G provést i bez výpočetní techniky.

2.4 Struktura a reprezentanty grupy symetrií Sudoku čtverce

Ukážeme nejprve, že grupa G je izomorfní vhodnému součinu symetrických grup – z toho již jasně uvidíme, jak vypadá její množina reprezentantů.

Označme nyní R grupu generovanou H_A a H_I (tj. permutacemi řádků a celých pásů) a S grupu generovanou H_B a H_J (tj. permutacemi sloupců a celých komínků).

Věta 2.15. $R \cong S_n \wr S_m$.

Důkaz. Ukážeme nejprve, že $R \cong H_I \rtimes_\varepsilon H_A$ pro nějaké $\varepsilon\colon H_A \to \operatorname{Aut}(H_I)$ – stačí ověřit, zda jsou splněny předpoklady věty 1.10.

Všechna $g \in H_I$ jsou rovna $I(\varphi_1,\ldots,\varphi_n)$ pro nějaké $(\varphi_1,\ldots,\varphi_m) \in (S_n)^m$ a pro libovolný Sudoku čtverec příslušného rozměru s buňkami (a,i,b,j) splňují $g((a,i,b,j)) = (a,\varphi_a(i),b,j)$. Stejně tak všechna $h \in H_A$ jsou rovna $A(\xi)$ pro vhodné $\xi \in S_m$ a buňky Sudoku čtverce zobrazují jako $h((a,i,b,j)) = (\xi(a),i,b,j)$.

- Prvky $k \in H_I \cap H_A$ musejí splňovat $k((a,i,b,j)) = (a,i,b,j)$, ale protože A a I jsou izomorfismy, platí toto pouze pro $k = \mathrm{id}_{\mathcal{Q}_{m\times n}}$ a tedy $H_I \cap H_A = 1$.
- R je generována H_A a H_I, tedy $R = H_A H_I$.
- Pro všechna $g \in H_I$, $h \in H_A$ platí

$$\begin{aligned} h^{-1}gh((a,i,b,j)) = h^{-1}g((\xi(a),i,b,j) = h^{-1}((\xi(a),\varphi_a(i),b,j) = \\ = (\xi^{-1}(\xi(a)),\varphi_{\xi^{-1}(a)}(i),b,j) = (a,\varphi_{\xi^{-1}(a)}(i),b,j) \in H_I \end{aligned}$$

  pro všechny buňky (a,i,b,j), tedy $H_I \trianglelefteq R$.

[7] Z důsledku 2.18 vyplyne, že třeba pro $m \times n = 3 \times 3$ je jich $6^8 = 1679616$.

[8] Jak ukazují Jarvis a Russel v [4], třeba pro $m \times n = 3 \times 3$ bude tříd konjugace pouze 484.

Tedy $R \cong H_I \rtimes_\varepsilon H_A$, proto podle důsledku 2.11 $R \cong (S_n)^m \rtimes_\varrho S_m$ pro nějaké $\varrho\colon S_m \to \mathrm{Aut}(S_n)^m$. Vidíme, že ϱ je působení grupy $H_A \cong S_m$ (tj. permutace komínků) takové, že permutuje souřadnice permutací pásů z grupy $H_I \cong (S_n)^m$, tedy $R \cong S_n \wr S_m$. □

Věta 2.16. *$S \cong S_m \wr S_n$.*

Důkaz. Důkaz bychom provedli zcela analogicky jako důkaz věty 2.15: ukážeme nejprve, že $S \cong H_J \rtimes_\varepsilon H_B$ pro nějaké $\varepsilon\colon H_B \to \mathrm{Aut}(H_J)$ (opět pomocí věty 1.10), a následně opět díky důsledku 2.11 vidíme, že $S \cong H_J \rtimes_\varepsilon H_B \cong S_m \wr S_n$. □

Zbývá ukázat, v jakém vztahu jsou grupy R a S.

Věta 2.17. *$G \cong R \times S$.*

Důkaz. Grupa R je generována grupami H_A a H_I, z definice těchto grup proto pro všechna $r \in R$ musejí všechny buňky (a,i,b,j) Sudoku čtverců z množiny $\mathcal{Q}_{m\times n}$ splňovat $r(a,i,b,j) = (\xi(a),\varphi_a(i),b,j)$ pro vhodná $\xi \in S_m, (\varphi_1,\ldots,\varphi_m) \in (S_n)^m$, přičemž jediné $r \in R$, pro které $r(a,i,b,j) = (a,i,b,j)$, je $\mathrm{id}_{\mathcal{Q}_{m\times n}}$.

Analogicky je grupa S generována grupami H_B a H_J, proto z definice těchto grup všechna $s \in S$ musejí pro buňky (a,i,b,j) všech Sudoku čtverců splňovat $s(a,i,b,j) = (a,i,\chi(b),\psi_b(j))$ pro vhodné $\chi \in S_n, (\psi_1,\ldots,\psi_n) \in (S_m)^n$. Zároveň jediné $s \in S$, pro které $s(a,i,b,j) = (a,i,b,j)$, je $\mathrm{id}_{\mathcal{Q}m\times n}$.

Tohoto využijeme k ověření předpokladů věty 1.8:

- $R \cap S = 1$, jelikož pro $k \in R \cap S$ platí $k(a,i,b,j) = (a,i,b,j)$, což platí pouze pro $\mathrm{id}_{\mathcal{Q}m\times n}$.
- Grupa R je generována grupami H_A a H_I, grupa S pak grupami H_B a H_J, grupa G je pak generována všemi čtyřmi grupami H_A, H_B, H_I a H_J, a proto $G = RS$.
- Pro všechny buňky (a,i,b,j) libovolného Sudoku čtverce platí tyto rovnosti:

$$rs(a,b,i,j) = r(a,i,\chi(b),\psi_b(j)) = (\xi(a),\varphi_a(i),\chi(b),\psi_b(j)),$$

$$sr(a,b,i,j) = s(\xi(a),\varphi_a(i),b,j) = (\xi(a),\varphi_a(i),\chi(b),\psi_b(j)).$$

  Vidíme, že vždy $rs(a,b,i,j) = sr(a,i,b,j)$, tedy $sr = rs$.

□

Shrneme-li naše poznatky:

$$G \cong (S_n \wr S_m) \times (S_m \wr S_n).$$

Z tohoto dokážeme (s využitím teorie, kterou jsme shrnuli v sekci 1.5) velmi snadno odvodit, jak budou vypadat reprezentanty tříd konjugace grupy G a jaká bude velikost těchto tříd konjugace.

Důsledek 2.18. $|G| = (n!)^{m+1} \cdot (m!)^{n+1}$

Důkaz. $|G| = |(S_n \wr S_m) \times (S_m \wr S_n)| = |S_n \wr S_m| \cdot |S_m \wr S_n| = |(S_n)^n| \cdot |S_m| \cdot |(S_m)^n| \cdot |S_n| = |S_n|^m \cdot |S_m| \cdot |S_m|^n \cdot |S_n| = |S_n|^{m+1} \cdot |S_m|^{n+1} = (n!)^{m+1} \cdot (m!)^{n+1}$. □

Důsledek 2.19. *Množina $\mathcal{R}_G \subseteq G$ tvaru*

$$\mathcal{R}_G = \{(r,s) | r \in \mathcal{R}_{n\wr m}, s \in \mathcal{R}_{m\wr n}\}$$

je množinou reprezentantů grupy G.

Důkaz. Podle věty 1.27 jsou reprezentanty direktního součinu uspořádanými dvojicemi reprezentantů jednotlivých jeho grup, což jsou v tomto případě (podle věty 1.42) právě prvky množin $\mathcal{R}_{n\wr m}$ a $\mathcal{R}_{m\wr n}$. □

Důsledek 2.20. *Nechť $(r,s) \in \mathcal{R}_G$. Pak*

$$|(r,s)^G| = |r^{S_n\wr S_m}| \cdot |s^{S_m\wr S_n}|.$$

Důkaz. Protože $G \cong (S_n \wr S_m) \times (S_m \wr S_n)$, plyne tvrzení přímo z důsledku 1.28. □

Velikosti tříd konjugace $r^{S_n\wr S_m}$ a $s^{S_m\wr S_n}$ již dokážeme spočítat pomocí věty 1.45. Vidíme, že pro Sudoku čtverec stupně $m \times n$ jsme pro každou třídu konjugace našli permutaci, která ji reprezentuje, a že dokážeme spočíst i velikost příslušné třídy konjugace. Ke zdárné enumeraci již zbývá pro každý nalezený reprezentant určit stabilizátor – tento výpočet se však neobejde bez použití výpočetní techniky a jeho popis a provedení přesahují rozsah této práce.

Frazer Jarvis na svých stránkách [6] uvádí několik provedených enumerací i se seznamem reprezentatnů tříd konjugace a jejich velikostí určených softwarem GAP. V následujícím příkladu je pro Sudoku čtverec stupně 2×3 popíšeme bez použití výpočetní techniky.

Příklad 2.21 Najděte reprezentanty všech tříd konjugace grupy symetrií Sudoku čtverce stupně 2×3:

Řešení. Připomeňme, že $\mathcal{R}_2 = \{\mathrm{id},(1\ 2)\}$ a $\mathcal{R}_3 = \{\mathrm{id},(1\ 2),(1\ 2\ 3)\}$. Nejprve najdeme prvky množiny $\mathcal{R}_{2\wr 3}$: ta je sjednocením množin R_κ pro $\kappa \in \mathcal{R}_3$. Pro $\kappa = \mathrm{id}$ $P_1 = \{1,2,3\}, P_2 = P_3 = \emptyset$, proto $R_{\mathrm{id}} = \{(r_1,r_2,r_3; \mathrm{id})\}$, kde $\{r_1,r_2,r_3\}$ jsou všechny trojčlenné kombinace prvků $\mathcal{R}_2$ s opakováním, tj.

$$R_{\mathrm{id}} = \{(\mathrm{id},\mathrm{id},\mathrm{id}; \mathrm{id}), ((1\ 2), \mathrm{id},\mathrm{id}; \mathrm{id}), ((1\ 2),(1\ 2),\mathrm{id}; \mathrm{id}),((1\ 2),(1\ 2),(1\ 2); \mathrm{id})\}.$$

Pro $\kappa = (1\ 2)$ platí $P_1 = \{3\}, P_2 = \{1\}, P_3 = \emptyset$. Proto

$$R_{(1\ 2)} = \{(\mathrm{id},\mathrm{id},\mathrm{id}; (12)),((12), \mathrm{id}, \mathrm{id}; (12)),(\mathrm{id},\mathrm{id}, (12); (12)),((12),\mathrm{id}, (12); (12))\}.$$

Dále pro $\kappa = (1\ 2\ 3)$ platí $P_1 = P_2 = \emptyset, P_3 = \{1\}$, proto

$$R_{(1\ 2\ 3)} = \{(\mathrm{id},\mathrm{id},\mathrm{id}; (1\ 2\ 3)),((1\ 2),\mathrm{id},\mathrm{id}; (1\ 2\ 3)).\}$$

Tedy

$$\begin{aligned}\mathcal{R}_{2\wr 3} = R_{\mathrm{id}} \cup R_{(1\ 2)} \cup R_{(1\ 2\ 3)} = \{&(\mathrm{id},\mathrm{id},\mathrm{id}; \mathrm{id}), ((1\ 2), \mathrm{id},\mathrm{id}; \mathrm{id}), ((1\ 2),(1\ 2),\mathrm{id}; \mathrm{id}),\\ &((1\ 2),(1\ 2),(1\ 2); \mathrm{id}), (\mathrm{id},\mathrm{id},\mathrm{id}; (1\ 2)),((1\ 2), \mathrm{id}, \mathrm{id}; (1\ 2)),(\mathrm{id},\mathrm{id}, (1\ 2); (1\ 2)),\\ &((1\ 2),\mathrm{id}, (1\ 2); (1\ 2)), (\mathrm{id},\mathrm{id},\mathrm{id}; (1\ 2\ 3)),((1\ 2),\mathrm{id},\mathrm{id}; (1\ 2\ 3))\}.\end{aligned}$$

Analogicky najdeme i všechny prvky množiny $\mathcal{R}_{3\wr 2}$ - ta vypadá následovně:

$\mathcal{R}_{3\wr 2} = \{$(id,id,id; id),(id,(1 2); id),(id,(1 2 3); id),((1 2),(1 2); id),
((1 2),(1 2 3); id),((1 2 3),(1 2 3); id),(id,id; (1 2)),((1 2),id; (1 2)),((1 2 3),id; (1 2))$\}$.

Víme, že grupa symetrií G je izomorfní $(S_3 \wr S_2) \times (S_2 \wr S_3)$, proto podle důsledku 2.19

$$\mathcal{R}_G = \{(r,s) \mid r \in \mathcal{R}_{3\wr 2}, s \in \mathcal{R}_{2\wr 3}\}.$$

Zbývá nám určit velikosti tříd konjugace jednotlivých reprezentantů: podle důsledku 2.20 nám k tomu stačí určit $|r^{S_3 \wr S_2}|$ a $|s^{S_2 \wr S_3}|$ pro všechna $r \in \mathcal{R}_{3\wr 2}$,$s \in \mathcal{R}_{2\wr 3}$. K výpočtu použijeme větu 1.45, budeme dosazovat do vzorce

$$\frac{(m!)^n n!}{\prod_{j=1}^{k} \lambda_j \prod_{\iota=1}^{n} (\prod_{a \in \mathcal{R}_m} (e(\iota,a)!)) \prod_{p \in P} (\prod_{y=1}^{pk_p} l_{py} \prod_{i=1}^{m} (d_i(l_p)!))}.$$

Začněme s prvky $R_{2\wr 3}$:

- pro (id,id,id; id) dostaneme $\frac{(2!)^3 \cdot 3!}{1^3 \cdot 3! \cdot 1^6 \cdot (2!)^3} = \frac{48}{48} = 1$.
- pro ((1 2), id,id; id) dostaneme $\frac{(2!)^3 \cdot 3!}{1^3 \cdot 2! 1! \cdot 2 \cdot 1^4 \cdot (2!)^2 \cdot 1!} = \frac{48}{16} = 3$,
- pro ((1 2),(1 2),id; id) dostaneme $\frac{(2!)^3 \cdot 3!}{1^3 \cdot 1! \cdot 2! \cdot 2^2 \cdot 1^2 \cdot 2! \cdot (1!)^2} = \frac{48}{16} = 3$,
- pro ((1 2),(1 2),(1 2); id) dostaneme $\frac{(2!)^3 \cdot 3!}{1^3 \cdot 3! \cdot 2^3 \cdot (1!)^3} = \frac{48}{48} = 1$,
- pro (id,id,id; (1 2)) dostaneme $\frac{(2!)^3 \cdot 3!}{2 \cdot 1 \cdot 1^4 \cdot (2!)^2} = \frac{48}{8} = 6$,
- pro ((1 2), id, id; (1 2)) dostaneme $\frac{(2!)^3 \cdot 3!}{2 \cdot 1 \cdot 2 \cdot 1^2 \cdot 1! \cdot 2!} = \frac{48}{8} = 6$,
- pro (id,id, (1 2); (1 2)) dostaneme $\frac{(2!)^3 \cdot 3!}{2 \cdot 1 \cdot 1^2 \cdot 2 \cdot 2! \cdot 1!} = \frac{48}{8} = 6$,
- pro ((1 2),id, (1 2); (1 2)) dostaneme $\frac{(2!)^3 \cdot 3!}{2 \cdot 1 \cdot 2 \cdot 2 \cdot (1!)^2} = \frac{48}{8} = 6$,
- pro (id,id,id; (1 2 3)) dostaneme $\frac{(2!)^3 \cdot 3!}{3 \cdot 1 \cdot 1^2 \cdot 2!} = \frac{48}{6} = 8$.
- pro ((1 2),id,id; (1 2 3)) dostaneme $\frac{(2!)^3 \cdot 3!}{3 \cdot 1 \cdot 1^2 \cdot 2 \cdot 1!} = \frac{48}{6} = 8$.

Analogicky určíme velikosti tříd konjugace reprezentantů z $\mathcal{R}_{3\wr 2}$.

- pro (id,id; id) dostaneme $\frac{(3!)^2 \cdot 2!}{1^2 \cdot 2! \cdot 1^6 \cdot (3!)^2} = \frac{72}{72} = 1$,
- pro (id,(1 2); id) dostaneme $\frac{(3!)^2 \cdot 2!}{1^2 \cdot (1!)^2 \cdot 1^4 \cdot 2 \cdot (3!)} = \frac{72}{12} = 6$,
- pro (id,(1 2 3); id) dostaneme $\frac{(3!)^2 \cdot 2!}{1^2 \cdot (1!)^2 \cdot 1^3 \cdot 3 \cdot (3!)} = \frac{72}{18} = 4$,
- pro ((1 2),(1 2); id) dostaneme $\frac{(3!)^2 \cdot 2!}{1^2 \cdot 2! \cdot 2^2 \cdot 1^2} = \frac{72}{8} = 9$,
- pro ((1 2),(1 2 3); id) dostaneme $\frac{(3!)^2 \cdot 2!}{1^2 \cdot (1!)^2 \cdot 2 \cdot 1 \cdot 3 \cdot} = \frac{72}{6} = 12$,
- pro ((1 2 3),(1 2 3); id) dostaneme $\frac{(3!)^2 \cdot 2!}{1^2 \cdot 2! \cdot 3^2} = \frac{72}{18} = 4$,

- pro (id,id; (1 2)) dostaneme $\frac{(3!)^2 \cdot 2!}{2 \cdot 1! \cdot 1^3 \cdot (3!)} = \frac{72}{12} = 6$,
- pro ((1 2),id; (1 2)) dostaneme $\frac{(3!)^2 \cdot 2!}{2 \cdot 1! \cdot 2 \cdot 1 \cdot 1!} = \frac{72}{4} = 18$,
- pro ((1 2 3),id; (1 2)) dostaneme $\frac{(3!)^2 \cdot 2!}{2 \cdot 1! \cdot 3 \cdot 1!} = \frac{72}{6} = 12$.

Velikost třídy konjugace příslušné reprezentantu $(r,s) \in \mathcal{R}_G$ nyní dostaneme jako $|r^{S_3 \wr S_2}| \cdot |s^{S_2 \wr S_3}|$. Například pro permutaci $g = (((1\,2),\mathrm{id}; (1\,2)),((1\,2),\mathrm{id},\mathrm{id}; (1\,2\,3)))$ proto platí $|g^G| = 18 \cdot 8 = 144$.[9] ◀

2.5 Sudoku čtverce se čtvercovými zónami

V předchozích kapitolách jsme zavedli grupu symetrií Sudoku čtverce G, nalezli reprezentanty všech jejích tříd konjugace a popsali, jak s jejich pomocí spočítat esenciálně odlišné Sudoku čtverce, tedy jak určit počet Sudoku čtverců, které nejsou navzájem transformovatelné pomocí symetrií z G. Po celou dobu jsme pracovali se Sudoku čtverci stupně $m \times n$, pro něž jsme jako symetrie uvažovali permutace sloupců v komínících, celých komínků, řádků v pásech a celých pásů.

Pro Sudoku čtverce stupně $n \times n$ však můžeme grupu G rozšířit o další symetrii – reflexi podle hlavní diagonály, tzv. transpozici Sudoku čtverce. Vidíme, že jejím obrazem je opět Sudoku čtverec stupně $n \times n$ a stejně jako ostatní zobrazení přiblížená v sekci 2.1 nemá vliv kupříkladu na to, kolik můžeme z příslušného Sudoku čtverce vypustit číslic. Na závěr této práce proto přiblížíme, jaké reprezentanty bude mít grupa symetrií, připustíme-li i symetrii Sudoku čtverce odpovídající jeho transpozici – podobně jako ostatní zobrazení popsaná v sekci 2.2 i ji můžeme realizovat jako působení vhodné grupy.

Definice 2.22 (Působení T)**.** *Transpozici Sudoku čtverce reprezentujeme působením T dvouprvkové grupy $\mathbb{Z}_2 = \{0,1\}$, kde 0 je neutrální prvek, na $\mathcal{Q}_{n\times n}$ takovým, že pro čtverec $\mathbf{S} \in \mathcal{Q}_{n\times n}$ platí $T(0) = \mathrm{id}_{\mathcal{Q}_{n\times n}}, T(1)(\mathbf{S}) = \{(b,j,a,i) | (a,i,b,j) \in \mathbf{u}, \mathbf{u} \in \mathbf{S}\}$.*

Dále budeme označovat $\operatorname{Im} T = H_T$.

Pozorování 2.23. *Působení T je věrné.*

Důkaz. $\operatorname{Ker} T = \mathrm{id}_{\mathcal{Q}_{n\times n}}$, $T(1) \neq \mathrm{id}_{\mathcal{Q}_{n\times n}}$ a další prvky $\mathbb{Z}_2$ nemá. □

Důsledek 2.24. *H_T je permutační grupa na $\mathcal{Q}_{n\times n}$, $H_T \cong \mathbb{Z}_2$.*

Definice 2.25 (T-symetrie, T-ekvivalentní, T-esenciálně odlišné Sudoku čtverce)**.** *Grupu generovanou grupami G a H_T nazveme G_T a její prvky budeme nazývat T-symetriemi Sudoku čtverce.*

Na množině Sudoku čtverců $\mathcal{Q}_{n\times n}$ dále definujme relaci $\sim_T$ tak, že pro Sudoku čtverce $\mathbf{S}_1, \mathbf{S}_2$ platí $\mathbf{S}_1 \sim_T \mathbf{S}_2$, pokud existuje $g \in G_T$ takové, že $g(\mathbf{S}_1) = \mathbf{S}_2$. Zřejmě $\sim_T$ je ekvivalence. Pokud pro dva Sudoku čtverce platí $\mathbf{S}_1 \sim_T \mathbf{S}_2$, řekneme, že jsou T-ekvivalentní, dva bloky ekvivalence $\sim_T$ na $\mathcal{Q}_{n\times n}$ pak nazveme T-esenciálně odlišné Sudoku čtverce stupně $n \times n$.

[9] Vidíme tedy, že symetrie Sudoku čtverce 2×3, která zamění 1. a 2. řádek prvního pásu, následně 1. a 2. pás, 1. a 2. sloupec prvního komínku a následně cyklicky 1., 2. a 3. komínek, je konjugována celkem se 143 dalšími symetriemi – namísto výpočtu stabilizátoru pro 144 permutací buněk Sudoku čtverce tedy stačí stabilizátor jen pro tuto jednu.

Vidíme, že tato definice je analogická definicím 2.12 a 2.13. Zcela analogicky jako v předchozích kapitolách se nyní můžeme zabývat otázkou, kolik T-esenciálně odlišných Sudoku čtverců stupně $n \times n$ existuje, a i tuto úlohu můžeme řešit pomocí Burnsidova lemmatu, resp. jeho důsledku 1.16. I v tomto případě tedy potřebujeme najít množinu reprezentantů tříd konjugace G_T.

Věta 2.26. $G_T \cong G \rtimes_\vartheta H_T$

Důkaz. Ověříme předpoklady věty 1.10:

Průnik $G \cap H_T$ obsahuje pouze $\mathrm{id}_{\mathcal{Q}_{n\times n}}$, neboť druhý prvek grupy H_T (tj. transpozice) zjevně v G neleží, G_T je generovaná grupami G a H_T, tedy $G_T = GH_T$. Zbývá ukázat normalitu G_T:

Pro všechna $g \in G, t \in H_T$ platí $t^{-1}gt \in G$, protože pokud $t = T(0)$, pak pro vhodná $\xi,\varphi_a,\chi,\psi_b \in S_n$ platí

$$t^{-1}gt(a,i,b,j) = t^{-1}g(a,i,b,j) = t^{-1}(\xi(a),\varphi_a(i),\chi(b),\psi_b(j)) = \\ = (\xi(a),\varphi_a(i),\chi(b),\psi_b(j)) \in G.$$

Pokud naopak $t = T(1)$, bude pro vhodná $\xi,\varphi_a,\chi,\psi_b \in S_n$ platit

$$t^{-1}gt(a,i,b,j) = t^{-1}g(b,j,a,i) = t^{-1}(\xi(b),\varphi_b(j),\chi(a),\psi_a(i)) = \\ = (\chi(a),\psi_a(i),\xi(b),\varphi_b(j)) \in G.$$

□

Jednotlivé permutace množiny G_T můžeme dále zapisovat ve tvaru $(a_1,a_2;b)$, kde $(a_1,a_2) \in G, b \in H_T$. Permutaci $((\mathrm{id}_{\{1,\dots,n\}},\dots,\mathrm{id}_{\{1,\dots,n\}};\mathrm{id}_{\{1,\dots,n\}}) \in S_n \wr S_n$ budeme pro jednoduchost dále zapisovat jako id, z kontextu bude vždy jasné, myslíme-li identickou permutaci ze symetrické grupy, nebo prvek věncového součinu.

Snadno nahlédneme, na jaké automorfismy zobrazuje ϑ prvky G_T:

$$\vartheta(T(0))(a_1,a_2) = (a_1,a_2)$$

$$\vartheta(T(1))(a_1,a_2) = (a_2,a_1)$$

pro každé $(a_1,a_2) \in G_T$.

Definice 2.27 (Množina $\mathcal{R}_T$)**.** *Nechť K je množina všech dvoučlenných kombinací prvků množiny $\mathcal{R}_n$ s opakováním. Pak definujme množinu $Y \subseteq G_T$ jako*

$$Y = \{(r_1,r_2;T(0)) \in G_T\},$$

kde dvoučlenná kombinace $\{r_1,r_2\} \in K$. Množinu $Z \subseteq G_T$ definujeme dále jako

$$Z = \{(\mathrm{id},r;T(1)) \mid r \in \mathcal{R}_n\}.$$

Množinu $\mathcal{R}_T \subseteq G_T$ nyní definujme jako $Y \cup Z$.

Věta 2.28. *Množina $\mathcal{R}_T$ je množinou reprezentantů grupy G_T.*

Důkaz. Z důkazu pozorování 1.29 víme, jak vypadají konjugované prvky v semidirektním součinu: pokud jsou $(a_1,a_2;s)$ a $(b_1,b_2;t)$ konjugovány v G_T, existuje $(u_1,u_2;x) \in G_T$ takové, že $(u_1,u_2;x) \bullet (a_1,a_2;s) \bullet (u_1,u_2;x)^{-1} = (b_1.b_2;t)$. Rozepsáním rovnosti dostaneme

$$((u_1,u_2)\vartheta(x)((a_1,a_2))\vartheta(s)(\vartheta(x^{-1})(u_1,u_2)^{-1})),xsx^{-1}) = (b_1,b_2;t). \tag{2.1}$$

Všimněme si nyní, že oba prvky H_T jsou involutorní – výše uvedenou rovnost tedy můžeme zapsat také jako

$$((u_1,u_2)\vartheta(x)((a_1,a_2))\vartheta(s)(\vartheta(x)(u_1,u_2)^{-1})),xsx) = (b_1,b_2;t).$$

Protože $xsx = t$, prvky s a t jsou v grupě H_T konjugovány. H_T je dvouprvková grupa a její dva prvky nejsou konjugované, proto $s = t$ a prvky množin Y a Z nemohou být konjugovány.

Ukážeme nejprve, jak vypadají třídy konjugace, které obsahují prvky tvaru $(a_1,a_2,T(0))$. Jelikož $\vartheta(T(0)) = id_G$, dosazením do rovnosti 2.1 dostaneme

$$\begin{aligned}((u_1,u_2)\vartheta(x)((a_1,a_2)\vartheta(s)(\vartheta(x)(u_1,u_2)^{-1})); xsx) = \\ = (((u_1,u_2)\vartheta(x)((a_1,a_2))\vartheta(x)(u_1,u_2)^{-1}); xsx) = (b_1,b_2;t).\end{aligned}$$

Nyní mohou nastat dvě možnosti: pokud $x = T(0)$, můžeme dosadit $\vartheta(x)(a_1,a_2) = (a_1,a_2)$, a proto

$$\begin{aligned}(((u_1,u_2)\vartheta(x)((a_1,a_2)\vartheta(x)(u_1,u_2)^{-1}),xsx) = ((u_1,u_2)(a_1,a_2)(u_1,u_2)^{-1}; xsx) = \\ = (u_1a_1u_1^{-1},u_2a_2u_2^{-1}; s) = (b_1,b_2;t).\end{aligned}$$

Proto (a_1,a_2) je konjugováno s (b_1,b_2) v G. Pokud naopak $x = T(1)$, můžeme dosadit $\vartheta(x)(a_1,a_2) = (a_2,a_1)$, a tedy

$$\begin{aligned}((u_1,u_2)\vartheta(x)((a_1,a_2)\vartheta(x)(u_1,u_2)^{-1}); xsx) = \\ = ((u_1,u_2)\vartheta(x)((a_1,a_2)(u_2^{-1},u_1^{-1})); xsx) = \\ = ((u_1,u_2)\vartheta(x)((a_1u_2^{-1},a_2u_1^{-1})); xsx) = (u_1a_2u_1^{-1},u_2a_1u_2^{-1}; xsx) = (b_1,b_2;t),\end{aligned}$$

tím pádem (a_2,a_1) je konjugováno s (b_1,b_2). Ukázali jsme, že $(a_1,a_2,T(0))$ je konjugováno s $(b_1,b_2,T(0))$ právě tehdy, když (a_1,a_2) je konjugováno buď s (b_1,b_2), nebo s (b_2,b_1). Y obsahuje právě jednu z těchto možností, proto jeho prvky nejsou konjugovány, naopak obsahuje všechny možné dvojice z $\mathcal{R}_{nn}$, proto je množinou obsahující všechny reprezentanty tvaru $(a_1,a_2;T(0))$.

Předpokládejme nyní, že $s = T(1)$. V tom případě pokud $x = T(0)$, pak

$$\begin{aligned}((u_1,u_2)\vartheta(x)((a_1,a_2)\vartheta(s)(\vartheta(x)(u_1,u_2)^{-1})); xsx) = \\ = ((u_1,u_2)\vartheta(x)((a_1,a_2)\vartheta(s)(u_1,u_2)^{-1})); T(1)) = \\ = ((u_1,u_2)\vartheta(x)((a_1,a_2)(u_2^{-1},u_1^{-1})); T(1)) = (u_1a_1u_2^{-1},u_2a_2u_1^{-1}; T(1)) = (b_1,b_2;t).\end{aligned}$$

Pokud naopak $x = T(1)$, dostáváme

$$\begin{aligned}((u_1,u_2)\vartheta(x)((a_1,a_2)\vartheta(s)(\vartheta(x)(u_1,u_2)^{-1})); xsx) = \\ = ((u_1,u_2)\vartheta(x)((a_1,a_2)\vartheta(s)(u_2^{-1},u_1^{-1})); T(1)) = \\ = ((u_1,u_2)\vartheta(x)((a_1,a_2)(u_1^{-1},u_2^{-1})); T(1)) = \\ = (u_1,u_2)(a_2,u_2^{-1},a_1u_1^{-1}); T(1)) = (u_1a_2,u_2^{-1},u_2a_1u_1^{-1}); T(1)) = (b_1,b_2;t).\end{aligned}$$

Poslední rovnosti obou uvedených odvození můžeme přeformulovat jako

$$(u_1,u_2)(a_1,a_2) = (b_1,b_2)(u_2,u_1),$$

$$(u_1,u_2)(a_2,a_1) = (b_1,b_2)(u_2,u_1).$$

Prvky $(a_1,a_2,T(1))$ a $(b_1,b_2,T(1))$ jsou proto konjugovány právě tehdy, pokud existuje $(u_1,u_2) \in G$ splňující některou z těchto dvou rovností. Pro dané (a_1,a_2) jistě můžeme najít (u_1,u_2) tak, že má-li některá z výše uvedených rovností platit, musí $b_1 = \mathrm{id}$. Všechny dvojice (a_1,a_2) jsou tedy konjugovány s (id,b_2) - reprezentanty jsou tedy tvaru $(\mathrm{id},b_2,T(1))$ pro nějaká b_2 – ukážeme, že b_2 může být libovolný reprezentant z $\mathcal{R}_n$.

Pokud (id,a_2) je konjugováno s (id,b_2), pak existuje $(u_1,u_2) \in G$ takové, že

$$(\mathrm{id},a_2)(u_1,u_2) = (u_2,u_1)(\mathrm{id},b_2).$$

V první složce dostáváme rovnost $u_1 = u_2$, což nám ve druhé složce dá $a_2u_1 = u_1b_2$, tj. $a_2 = u_1b_1u_1^{-1}$, tedy $(\mathrm{id},a_2,T(1))$ je konjugováno s $(\mathrm{id},b_2,T(1))$ právě tehdy, když a_2 je konjugováno s b_2. Nejmenší množinou, v níž ke každému a_2 najdeme b_2, se kterým je konjugováno, je právě $\mathcal{R}_n$. Množina reprezentantů pro prvky $(a_1,a_2,T(1))$ je proto právě $Z = \{(\mathrm{id},r;T(1)) \mid r \in \mathcal{R}_n\}$. □

Věta 2.29. *Nechť $g = (a_1,a_2;s) \in \mathcal{R}_T$.*

1. *Pokud $s = T(0)$ a $a_1 \neq a_2$, pak $|g^{G_T}| = 2|a_1^{S_n \wr S_n}||a_2^{S_n \wr S_n}|$.*
2. *Pokud $s = T(0)$ a $a_1 = a_2$, pak $|g^{G_T}| = |a_1^{S_n \wr S_n}|^2$.*
3. *Pokud $s = T(1)$, pak $|g^{G_T}| = |a_2^{S_n \wr S_n}||S_n \wr S_n| = (n!)^{n+1}|a_2^{S_n \wr S_n}|$.*

Důkaz. Nechť $g \in \mathcal{R}_T$. Nejprve najdeme $C_{G_T}(g)$ – použijeme k tomu pozorování 1.22, které nám říká, že $C_{G_T}(g) = \{h \in G_T \mid hgh^{-1} = g\}$. Ať $h = (b_1,b_2;t)$. Pak rovnost $hgh^{-1} = g$ můžeme zapsat jako $(b_1,b_2;t) \bullet (a_1,a_2;s) \bullet (b_1,b_2;t)^{-1} = (a_1,a_2;s)$. Rozepsáním rovnosti (a využitím toho, že $T(0)$ a $T(1)$ jsou involutorní) dostaneme

$$((b_1,b_2)\vartheta(t)((a_1,a_2))\vartheta(s)(\vartheta(t)(b_1,b_2)^{-1}));tst) = (a_1,a_2;s). \tag{2.2}$$

Pokud $s = T(0)$, můžeme rovnici upravit do tvaru

$$((b_1,b_2)\vartheta(t)((a_1,a_2))(\vartheta(t)(b_1,b_2)^{-1}));T(0)) = (a_1,a_2;T(0)). \tag{2.3}$$

Pokud $t = T(0)$, z této rovnice plyne

$$((b_1,b_2)(a_1,a_2)(b_1,b_2)^{-1}));T(0)) = (b_1a_1b_1^{-1},b_2a_2b_2^{-1};T(0)) = (a_1,a_2;T(0)).$$

Tedy $b_1a_1b_1^{-1} = a_1$ a $b_2a_2b_2^{-1} = a_2$, proto $h = (b_1,b_2;T(0)), b_1 \in C_{S_n \wr S_n}(a_1), b_2 \in C_{S_n \wr S_n}(a_2)$. Pokud naopak $t = T(1)$, z rovnice 2.3 dostáváme

$$((b_1,b_2)\vartheta(T(1))(a_1b_2^{-1},a_2b_1-1);T(0)) = \\ = ((b_1a_2b_1^{-1},b_2a_1b_2^{-1};T(0)) = (a_1,a_2;T(0)).$$

V tom případě by $b_1a_2b_1^{-1} = a_1$ a $b_2a_1b_2 = a_2$. Pokud $a_1 \neq a_2$, pak toto nemůže nastat a b_1,$b_2 \in \emptyset$, neboť dva různé prvky $\mathcal{R}_T$ nejsou konjugovány. Pokud naopak $a_1 = a_2$, pak b_1,$b_2 \in C_{S_n \wr S_n}(a_1)$.

V případě, že $s = T(1)$, víme, že $a_1 = \mathrm{id}$. Z rovnice 2.2 dostáváme

$$((b_1,b_2)\vartheta(t)((\mathrm{id},a_2))\vartheta(T(1))(\vartheta(t)(b_1,b_2)^{-1}));T(1)) = (\mathrm{id},a_2;T(1)).$$

Pokud $t = T(0)$, dostáváme z této rovnice

$$\begin{aligned}((b_1,b_2)((\mathrm{id},a_2))\vartheta(T(1)(b_1,b_2)^{-1}));T(1)) = ((b_1,b_2)((\mathrm{id},a_2))(b_2,b_1)^{-1}));T(1)) = \\ = (b_1b_2^{-1},b_2a_2b_1^{-1};T(1)) = (\mathrm{id},a_2;T(1)).\end{aligned}$$

To, že $b_1b_2^{-1} = \mathrm{id}$, znamená, že $b_1 = b_2$ – tím pádem z rovnosti druhých složek dostáváme $b_1a_2b_1^{-1} = a_2$, tedy $b_1 \in C_{S_n \wr S_n}(a_2)$ Pokud naopak $t = T(1)$, dostáváme rovnici

$$\begin{aligned}&((b_1,b_2)\vartheta(T(1))((\mathrm{id},a_2))\vartheta(T(1))(\vartheta(T(1))(b_1,b_2)^{-1});T(1)) = \\ &= ((b_1,b_2)\vartheta(T(1))((b_1^{-1},a_2b_2^{-1}));T(1)) = (b_1a_2b_2^{-1},b_2b_1^{-1};T(1)) = (\mathrm{id},a_2;T(1)).\end{aligned}$$

Z poslední rovnosti plyne, že $b_1a_2 = b_2$, a tím pádem $b_1a_2b_1^{-1} = a_2$, proto opět $b_1 \in C_{S_n \wr S_n}(a_2)$.

Nyní můžeme rozdělit naše poznatky na jednotlivé případy, rovnosti ze znění věty z nich již snadno plynou:

1. pokud $g = (a_1,a_2;T(0))$ a $a_1 \neq a_2$, pak $C_{G_T}(g) = \{h \in G_T \mid h = (b_1,b_2;T(0)), b_1 \in C_{S_n \wr S_n}(a_1), b_2 \in C_{S_n \wr S_n}(a_2)\}$. Tím pádem $|C_{G_T}(g)| = |C_{S_n \wr S_n}(a_1)| \cdot |C_{S_n \wr S_n}(a_2)|$. Nyní můžeme dosadit do věty 1.23 a dostaneme

$$|g^{G_T}| = \frac{|G_T|}{|C_{G_T}(g)|} = \frac{2|S_n \wr S_n|^2}{|C_{S_n \wr S_n}(a_1)||C_{S_n \wr S_n}(a_2)|} = 2|a_1^{S_n \wr S_n}||a_2^{S_n \wr S_n}|.$$

2. pokud $g = (a_1,a_1;T(0))$, pak $C_{G_T}(g) = \{h \in G_T \mid h = (b_1,b_2;t), b_1,b_2 \in C_{S_n \wr S_n}(a_1), t \in H_T\}$, tím pádem $|C_{G_T}(g)| = 2|C_{S_n \wr S_n}(a_1)|^2$. Dosazením do věty 1.23 dostaneme

$$|g^{G_T}| = \frac{|G_T|}{|C_{G_T}(g)|} = \frac{2|S_n \wr S_n|^2}{2|C_{S_n \wr S_n}(a_1)|^2} = |a_1^{S_n \wr S_n}|^2.$$

3. pokud $g = (\mathrm{id},a_2;T(1))$, $C_{G_T}(g) = \{h \in G_T \mid h = (b_1,b_1;T(0))$ nebo $h = (b_1,b_1a_2;T(1)), b_1 \in C_{S_n \wr S_n}(g), t \in H_T\}$. Celkem $C_{G_T}(g) = 2|C_{S_n \wr S_n}(a_2)|$. Dosazením do věty 1.23 dostaneme

$$|g^{G_T}| = \frac{|G_T|}{|C_{G_T}(g)|} = \frac{2|S_n \wr S_n|^2}{2|C_{S_n \wr S_n}(a_2)|} = |a_2^{S_n \wr S_n}||S_n \wr S_n| = (n!)^{n+1}|a_2^{S_n \wr S_n}|.$$

□

Určili jsme tedy reprezentanty a velikosti tříd konjugace grupy symetrií Sudoku čtverce, do které zahrnujeme i jeho transpozici - pro Sudoku čtverec stupně 3×3 přesně toto počítali autoři článku [4], přehled všech tříd konjugace, které jim vyšly, uvádějí v [7]. Z prostorových důvodů nebudeme opakovat celou jejich enumeraci, spočteme pouze velikost třídy konjugace pro vybrané reprezentanty, které odpovídají třem případům z věty 2.29.

Příklad 2.30 Určete velikost třídy konjugace v grupě symetrií Sudoku čtverce stupně 3×3, reprezentované permutací:

- $g_1 = (((1\,2),(1\,2),(1\,2);\mathrm{id}),((1\,2\,3),\mathrm{id},\mathrm{id};(1\,2\,3));T(0))$,
- $g_2 = (((1\,2),(1\,2),(1\,2);\mathrm{id}),((1\,2),(1\,2),(1\,2);\mathrm{id});T(0))$,
- $g_3 = ((\mathrm{id},\mathrm{id},\mathrm{id};\mathrm{id}),((1\,2),(1\,2),(1\,2);\mathrm{id});T(1))$.

Řešení. Nejprve spočítáme $|((1\,2),(1\,2),(1\,2);\mathrm{id})^{S_3 \wr S_3}|$ a $|((1\,2\,3),\mathrm{id},\mathrm{id};(1\,2\,3))^{S_3 \wr S_3}|$. Použijeme větu 1.45: pro první permutaci $(\lambda_j)_{j=1}^3 = 1,1,1$, $e(1,(1\,2)) = 3$, jinak $e(\iota,a) = 0$, $(l_{py})_{y=1}^3 = 2,1$, $p = 1,2,3$, proto

$$|((1\,2),(1\,2),(1\,2);\mathrm{id})^{S_3 \wr S_3}| = \frac{(3!)^4}{1^3 \cdot 3! \cdot (2 \cdot 1)^3} = \frac{1296}{48} = 27.$$

Pro druhou permutaci $(\lambda_j)_{j=1}^1 = (l_{1y})_{y=1}^1 = 3$, proto

$$|((1\,2\,3),\mathrm{id},\mathrm{id};(1\,2\,3))^{S_3 \wr S_3}| = \frac{(3!)^4}{3 \cdot 1! \cdot 3} = \frac{1296}{9} = 144.$$

Nyní můžeme podle věty 2.29 spočítat požadované velikosti tříd konjugace:

- $|g_1^{G_T}| = 2|((1\,2),(1\,2),(1\,2);\mathrm{id})^{S_3 \wr S_3}||((1\,2\,3),\mathrm{id},\mathrm{id};(1\,2\,3))^{S_3 \wr S_3}| = 2 \cdot 27 \cdot 144 = 7776$.
- $|g_2^{G_T}| = |((1\,2),(1\,2),(1\,2);\mathrm{id})^{S_3 \wr S_3}|^2 = 27^2 = 729$.
- $|g_3^{G_T}| = |((1\,2),(1\,2),(1\,2);\mathrm{id})^{S_3 \wr S_3}| \cdot |S_3 \wr S_3| = 27 \cdot 1296 = 34992$.

Docházíme ke stejnému výsledku jako Frazer Jarvis s Edem Russelem, konkrétně g_1 reprezentuje třídu konjugace označenou v [7] jako č. 185, g_2 třídu konjugace č. 54, g_3 třídu konjugace č. 200. ◀

Závěr

V práci jsme shrnuli známé poznatky z teorie grup, rozšířili je o popis reprezentatnů tříd konjugace věncového součinu a o vztah pro výpočet velikosti každé této třídy. Tyto znalosti následně aplikujeme na grupu symetrií Sudoku čtverce, o níž jsme dokázali, že je direktním součinem vhodných věncových součinů. Poslední část práce se věnuje nalezení reprezentantů tříd konjugace grupy symetrií rozšířené i o transpozici Sudoku čtverce. Téma enumerace esenciálně odlišných Sudoku čtverců však není ani zdaleka vyčerpáno – s ohledem na rozsah práce nebyla (v souladu se zadáním) vůbec provedena vlastní enumerace Sudoku čtverců, tj. výpočet stabilizátoru pro každý námi nalezený reprezentant. Tento výpočet vyžaduje především nalezení dostatečně efektivního algoritmu, který tento výpočet provede ve snesitelném čase, a který v [4] prakticky není popsán[10]. Vytvoření takového algoritmu, použitelného ideálně pro Sudoku čtverce všech možných rozměrů, je druhým velkým krokem k zopakování a zobecnění výpočtů F. Jarvise a E. Russela.

[10]Čtenářům je pouze sděleno, že tento algoritmus funguje podobně jako ten, který byl použit při enumeraci popsané v [3].

Seznam použité literatury

[1] STANOVSKÝ, David. *Základy algebry*. Praha, Matfyzpress, 2010. ISBN 987-80-7378-105-7.

[2] DRÁPAL, Aleš. *Teorie grup*. Praha, Karolinum, 2000. ISBN 80-246-0162-1.

[3] FELGENHAUER, Bertram, JARVIS, Frazer. *Enumerating possible Sudoku grids*. `http://www.afjarvis.staff.shef.ac.uk/sudoku/sudoku.pdf`.

[4] JARVIS, Frazer, RUSSEL, Ed. *Mathematics of Sudoku II*. `http://www.afjarvis.staff.shef.ac.uk/sudoku/russell_jarvis_spec2.pdf`.

[5] McGUIRE, Gary, TUGEMANN, Bastian, CIVARIO, Gilles. *There is no 16-Clue Sudoku: Solving the Sudoku Minimum Number of Clues Problem via Hitting Set Enumeration*. `http://www.math.ie/McGuire_V2.pdf`.

[6] JARVIS, Frazer. *Sudoku enumeration problems*. 2. 2. 2008 [cit. 25. 7. 2020]. `http://www.afjarvis.staff.shef.ac.uk/sudoku/`.

[7] RUSSEL, Ed, JARVIS, Frazer. *There are 5472730538 essentially different Sudoku grids ... and the Sudoku symmetry group*. 7. 9. 2005 [cit. 25. 7. 2020]. `http://www.afjarvis.staff.shef.ac.uk/sudoku/sudgroup.html`.

[8] RUSSEL, Ed, JARVIS, Frazer. *There are 49 essentially different Sudoku 2x3 grids ... and the 2x3 Sudoku symmetry group*. nedatováno [cit. 25. 7. 2020]. `http://www.afjarvis.staff.shef.ac.uk/sudoku/sud23gp.html`.