MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

David Hubač

Permutace s předepsanými délkami cyklů

Katedra didaktiky matematiky

Vedoucí bakalářské práce:	doc. RNDr. Antonín Slavík, Ph.D.
Studijní program:	Matematika se zaměřením na vzdělávání
Studijní obor:	MIUP

Praha 2024

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) 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 .... dne ....

Podpis autora

Děkuji vedoucímu doc. RNDr. Antonínovi Slavíkovi, Ph.D., za to, že mi byl skvělým průvodcem v psaní této práce, za obrovskou míru smyslu pro detail a za spoustu cenných rad.

Název práce: Permutace s předepsanými délkami cyklů

Autor: David Hubač

Katedra: Katedra didaktiky matematiky

Vedoucí bakalářské práce: doc. RNDr. Antonín Slavík, Ph.D., Katedra didaktiky matematiky

Abstrakt: Práce se zabývá zkoumáním a počítáním permutací, jejichž cykly mají předepsané délky. V první části představíme třídu permutací složených pouze z jednocyklů a dvojcyklů a ukážeme některé související úlohy. Druhá část je věnována dalším třídám permutací a postupům, jak zjistit jejich počet. Vedle kombinatorického přístupu využíváme též analytický přístup pracující s tzv. exponenciálními generujícími funkcemi.

Klíčová slova: permutace, nezávislé cykly, telefonní čísla, involuce, exponenciální generující funkce

Title: Permutations with prescribed cycle lengths

Author: David Hubač

Department: Department of Matematics Education

Supervisor: doc. RNDr. Antonín Slavík, Ph.D., Department of Matematics Education

Abstract: The thesis studies and calculates permutations whose cycles have prescribed lengths. The first part introduces a class of permutations whose cycles have lengths one and two, and presents several related problems. In the second part, we examine other classes of permutations as well as methods for calculating their number. In addition to a combinatorial approach, an analytical approach using exponential generating functions is shown.

Keywords: permutation, disjoint cycles, telephone numbers, involution, exponential generating function

Obsah

Úvod **2**

1 Telefonní čísla **4**
1.1 Spojení s teorií grafů 5
1.2 Involutorní zobrazení 5
1.3 Rekurentní rovnice a explicitní vzorec 6

2 Rozmisťování věží **8**
2.1 Burnsideovo lemma 8
2.2 Řešení věžové úlohy 10

3 Permutace s cykly předepsaných délek **15**
3.1 Kombinatorický postup 15
3.2 Exponenciální generující funkce 16
3.3 Analytický postup 18
3.4 Další příklady 21

Úvod

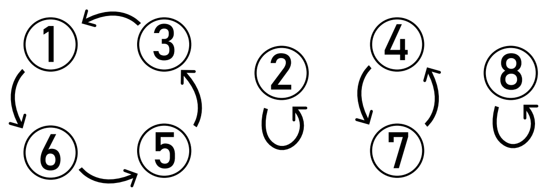
Následující odstavce věnujme připomenutí pojmu *cyklus* ve vztahu k permutacím, pak již budeme moci nastínit, čím se tato bakalářská práce bude zabývat.

Mějme n-prvkovou množinu X. Pokud si její prvky znázorníme jako různé body v rovině, pak jakékoliv zobrazení na množině X je možné popsat n šipkami mezi těmito body tak, že z každého bodu bude vést šipka k jeho obrazu. *Permutace* jsou bijektivní zobrazení na této množině, a tedy pro ně platí, že do každého bodu vede také právě jedna šipka.

Znázorníme si vše na příkladu. Mějme množinu čísel 1 až 8 a na ní permutaci zadanou následující tabulkou:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 2 & 1 & 7 & 3 & 5 & 4 & 8 \end{pmatrix}.$$

Schéma s body a šipkami pak bude vypadat následujícím způsobem:



Díky tomu, že do každého i z každého bodu vede právě jedna šipka, lze ve schématu rozlišit takzvané *cykly*. V našem případě jsou čtyři: dva cykly délky 1, jeden délky 2 a jeden délky 4, či jinak řečeno dva *jednocykly*, jeden *dvojcyklus* a jeden *čtyřcyklus*.

Obecně platí, že schéma každé permutace bude tvořeno jedním či více cykly. Dává tedy smysl zavést alternativní zápis permutací právě přes jejich příslušné cykly. Abychom nemuseli kreslit podobná schémata, zavedeme pohodlnější „vektorový“ zápis cyklů. Ten může vypadat třeba takto:

$$(1, 6, 5, 3)(2)(4, 7)(8).$$

Jedny závorky představují jeden cyklus, každý prvek v závorkách je obrazem svého předchůdce a má za obraz svého následníka (poslední prvek má za následníka první prvek a naopak). Tento zápis není jednoznačný, nezáleží totiž na tom, který prvek napíšeme do závorek na první pozici, ani na pořadí cyklů. Tedy i následující zápis popisuje stejné cykly a stejnou permutaci:

$$(8)(2)(7, 4)(5, 3, 1, 6).$$

V práci několikrát tuto nejednoznačnost obejdeme tím, že si pro zápis určíme přísnější kritéria. Obecně nám to však nevadí – především nás totiž budou u permutací zajímat délky cyklů, které zůstávají neměnné.

Vztah mezi permutacemi a cykly budeme v práci popisovat slovními spojeními „permutaci lze *rozložit* na cykly“, „permutace *je tvořená* cykly“, „permutace *je složená* z cyklů“, „permutace *sestává* z cyklů“ a podobně. Formálně se přitom vždy jedná o *nezávislé* cykly – to znamená, že žádný prvek se nevyskytuje ve více cyklech najednou.

Protože každou permutaci lze zapsat pomocí cyklů a každá množina nezávislých cyklů popisuje nějakou permutaci, dává smysl zkoumat permutace podle vlastností příslušných cyklů. A to je hlavním cílem této bakalářské práce. Shrňme si tedy, co všechno práce pokrývá.

První kapitola představí třídu permutací sestávajících pouze z jednocyklů a dvojcyklů, a to rovnou třemi ekvivalentními pohledy. Jeden pohled nabízí úloha, ve které je úkolem zjistit, kolika způsoby si může n domácností mezi sebou telefonovat. Ukážeme si kombinatorický postup k vyřešení této úlohy. Další pohled zkoumá *involutorní zobrazení*, tedy zobrazení, která jsou samy sobě inverzní. A třetí pohled nabízí interpretaci v jazyce teorie grafů.

Ve druhé kapitole budeme řešit zdánlivě nesouvisející úlohu o věžích na šachovnici. Otázka zní, kolika způsoby lze rozestavět n věží na šachovnici $n \times n$ tak, aby se vzájemně neohrožovaly; přitom však chceme považovat rozmístění lišící se jen o otočení nebo zrcadlové převrácení šachovnice za totožná. Úloha bude vyžadovat zavedení kombinatorického nástroje známého jako *Burnsideovo lemma*. V průběhu řešení narazíme na výše zmíněnou třídu permutací a úlohu vyřešíme za použití výsledku z první kapitoly.

Třetí kapitola je věnována dalším třídám permutací s předepsanými délkami cyklů. Čtenáři budou jistě známé permutace bez pevných bodů – na ty lze totiž nahlížet jako na permutace, v jejichž rozkladu na nezávislé cykly se nenachází jednocykly. Další z úloh je počítání permutací, jejichž cykly jsou pouze lichých délek, pouze sudých délek nebo pouze délek, které jsou násobky vybraného čísla k.

Kombinatorický postup použitý v první kapitole zobecníme, vedle něj však představíme zpravidla obecnější analytický postup, pracující s takzvanými exponenciálními generujícími funkcemi. Poslední sekce třetí kapitoly nabídne přímé porovnání těchto dvou postupů hned na několika úlohách.

Práce je určena čtenářům obeznámeným se základy kombinatoriky a algebry na úrovni bakalářského studia. Ve třetí kapitole navíc budeme používat mocninné řady, derivace a integrály, tedy očekávají se i základní znalosti matematické analýzy. Nyní už přeji příjemné a obohacující čtení.

1. Telefonní čísla

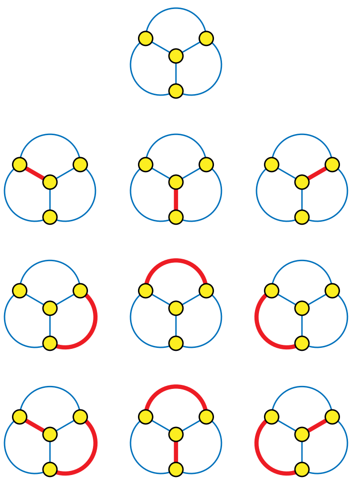
Tato kapitola bude zkoumat zvláštní druh permutací, které se nazývají involutorní, nejdřív se však podíváme na úlohu o takzvaných telefonních číslech. V celé kapitole budeme vycházet především ze stránek [1] a dále v příslušných sekcích ze stránek [2] a [3].

Úloha 1 (O telefonních číslech)**.** *Mějme n (vzájemně rozlišitelných) domácností, v každé je jeden telefon. Jednoho telefonátu se účastní právě dvě různé domácnosti a každá domácnost může telefonovat v daný okamžik nejvýše jednou. Kolik existuje možností, jak mohou být domácnosti telefonicky vzájemně propojeny?*

Definice 2. *Řešení úlohy o telefonních číslech pro n domácností nazveme n-*tým telefonním číslem *a označíme ho T_n.*

Dodefinujeme nulté telefonní číslo $T_0 = 1$, tedy pokud nemáme žádné domácnosti, není žádné telefonní spojení a to pokládáme za jednu validní možnost. Dalších několik čísel lze snadno odvodit: $T_1 = 1$ (jediná možnost pro jednu domácnost je žádné spojení); $T_2 = 2$ (domácnosti jsou nebo nejsou spojeny – dvě možnosti); $T_3 = 4$ (buď žádné spojení, nebo vybereme ke spojení dvě domácnosti, což jsou tři možnosti).

Od T_4 se ale situace začíná komplikovat. Můžeme si pomoci obrázkem a uvidíme, že existuje deset možných schémat, tedy $T_4 = 10$.



Obrázek 1.1: Schéma všech 10 možností propojení 4 domácností (převzato z Wikipedia, `https://en.wikipedia.org/wiki/File:K4_matchings.svg`)

Pro vyšší čísla n je nasnadě využít kombinatorické postupy a hledat rekurentní a explicitní vzorec, abychom mohli pokládat úlohu za vyřešenou. Než se ale dostaneme k vyřešení úlohy, pojďme se zamyslet nad jinými pohledy na telefonní čísla.

1.1 Spojení s teorií grafů

Představme si schéma jedné možnosti telefonního spojení mezi n domácnostmi. Všechny domy jsou vzájemně propojeny a vybraná propojení ukazují, které domy si právě telefonují. Jedná se vlastně o úplný graf s n vrcholy a se specifickým výběrem hran, kterému se říká *párování*.

Definice 3. *Podmnožina hran v obecném grafu se nazývá* párování*, jestliže žádné dvě hrany této množiny nemají společný vrchol.*

Zde vidíme ekvivalenci mezi úlohou o telefonních číslech a hledáním počtu párování na úplném grafu o n vrcholech. Každé párování lze převést na validní výběr telefonátů mezi domácnostmi (z žádného vrcholu nevedou dvě vybrané hrany – žádná domácnost netelefonuje dvakrát najednou) a zároveň každá možnost telefonického spojení je párováním grafu. Graf musí být úplný (tj. obsahující všechny hrany), aby libovolné spojení mezi domácnostmi mohlo být zahrnuto ve výběru hran v grafu.

Problém párování se zkoumá i u neúplných grafů (tedy některé hrany nelze vybrat), známý je například problém hledání největšího párování v bipartitních grafech.

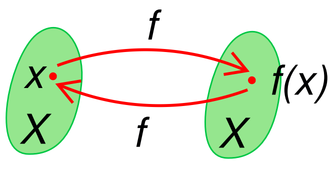
1.2 Involutorní zobrazení

Schémata telefonních spojení s n domácnostmi také odpovídají permutacím na n-prvkové množině. Domácnosti, které ve schématu netelefonují, se v permutaci zobrazují samy na sebe – tvoří jednocyklus, a dvojice domácností navzájem si telefonujících se zobrazují jedna na druhou – tvoří transpozici, dvojcyklus. Tedy libovolné schéma lze převést na permutaci tvořenou pouze jednocykly a dvojcykly. Uvědomme si navíc, že každá domácnost je součástí právě jednoho cyklu, tedy cykly tvoří nezávislý rozklad permutace.

Za použití stejné logiky platí i druhá implikace: máme-li permutaci rozloženou na nezávislé jednocykly a dvojcykly, pak z ní lze zpětně zjistit, které domácnosti spolu telefonují. Získali jsme tedy další ekvivalenci.

Tato třída permutací má charakteristickou vlastnost.

Definice 4. *Zobrazení se nazývá* involutorní*, pokud je samo sobě inverzí.*



Obrázek 1.2: Názorné schéma involutorního zobrazení (převzato z Wikipedia, `https://en.wikipedia.org/wiki/File:Involution.svg`)

Triviálním případem involutorního zobrazení je identita na libovolné množině. V geometrii jsou známými involutorními zobrazeními středová a osová souměrnost či kruhová inverze.

Věta 5. *Množina všech permutací na n-prvkové množině X sestávajících pouze z jednocyklů a dvojcyklů tvoří množinu všech involutorních zobrazení na X.*

Důkaz. Být involutorním zobrazením znamená, že složení dvou takových zobrazení utvoří identitu. Právě toto platí pro naši třídu permutací: zpermutovnání n-prvkové množiny dvakrát po sobě permutací složené pouze z jednocyklů a dvojcyklů prvky v jednocyklu nepřesune a prvky v dvojcyklu přesune tam a zase zpátky. Tedy třída permutací tvoří podmnožinu involutorních zobrazení na dané množině.

Zároveň žádné involutorní zobrazení v této podmnožině nechybí. Aby pro zobrazení vůbec existovala inverze, musí se jednat o bijekci – a bijekce na konečné množině je dle definice permutace. Žádná permutace sestávající z alespoň jednoho nezávislého cyklu délky větší než dva není involutorní, protože na prvky z tohoto cyklu by se zobrazení muselo aplikovat alespoň tolikrát, jak dlouhý cyklus je. Pak až by se všechny prvky tohoto cyklu dostaly zpátky do výchozí pozice. □

Věta nám tedy říká, že právě tato třída permutací je involutorní a žádné jiné permutace tuto vlastnost nemají. Můžeme třídu tedy nazývat *involutorní permutace.*

1.3 Rekurentní rovnice a explicitní vzorec

Pojďme tedy vyřešit úlohu o telefonních číslech, nejdřív pomocí rekurze. Ve schématu s n domácnostmi mohou nastat dvě situace: buď n-tá domácnost netelefonuje, nebo telefonuje s jinou domácností. Platí-li první situace, je počet možností roven $(n-1)$-nímu telefonnímu číslu. Platí-li druhá situace, domácnost má na výběr z $n-1$ možností, s kým si telefonovat, a pro zbylých $n-2$ domácností již víme, že je lze spojit T_{n-2} způsoby. Pro $n \geq 2$ tedy rekurentní vzorec n-tého telefonního čísla vypadá následovně:

$$T_n = T_{n-1} + (n-1) \cdot T_{n-2}. \tag{1.1}$$

Máme nyní nástroj pro výpočet telefonních čísel, není ovšem efektivní pro vysoká čísla n. Například pro $n = 100$ by bylo třeba vypočítat všechny předchozí hodnoty až do T_{99}, což se jeví jako spousta zbytečné práce navíc. Na konstrukci tabulky pro nízké hodnoty n ale rekurze bohatě stačí:

n	0	1	2	3	4	5	6	7	8	9	10
T_n	1	1	2	4	10	26	76	232	764	2620	9496

Nyní se pojďme podívat na explicitní vzorec vyjádřený konečnou sumou, jenž vystačí pro libovolné hodnoty n. Jeho zdůvodnění poskytneme v dalším odstavci.

$$T_n = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} \frac{(2k)!}{2^k k!}. \tag{1.2}$$

Dle kombinatorických pravidel součtu a součinu je vzorec suma podle počtu telefonátů k, kterých může být 0 až $\lfloor n/2 \rfloor$. Kombinační číslo značí výběr $2k$

domácností, které budou telefonovat, a následující zlomek udává počet možností, jak je mezi sebou spárovat. $(2k)!$ pomyslně seřadí všechny telefonující domácnosti a spáruje první s druhou, třetí se čtvrtou atd. Tím ale vznikly duplicity. Nezáleží na pořadí párů ani na pořadí domácností v daném páru, tedy vydělíme sčítanec $k!$ (pro pořadí párů) a 2^k (pro pořadí domácností v párech).

Všimněme si, že $2^k k!$ lze vnímat jako faktoriál čísla $2k$, pokud bychom do příslušného součinu zahrnuli pouze sudá čísla. Pokud tímto výrazem vydělíme $(2k)!$, získáme naopak obdobu faktoriálu složenou pouze z lichých čísel – to je případ v našem vzorci (1.2). Těmto číslům se říká *dvojité faktoriály* (či semifaktoriály), a protože se s nimi ještě budeme setkávat, bude rozumné je formálně definovat.

Definice 6. *Mějme číslo $k \in \mathbb{N}$, pak* dvojité faktoriály *čísel $2k$ a $2k-1$ definujeme po řadě následovně:*

$$(2k)!! := (2k)(2k-2)\dots 4 \cdot 2 = 2^k k!,$$

$$(2k-1)!! := (2k-1)(2k-3)\dots 3 \cdot 1 = \frac{(2k)!}{2^k k!}.$$

Dále dodefinujme $(-1)!! := 1$ a $0!! := 1$.

Zavedení definice pro čísla 0 a -1 nám bude užitečné zde i v dalších místech práce. Dosazením 0 za k do výrazů $2^k k!$ a $\frac{(2k)!}{2^k k!}$ skutečně získáme číslo 1.

Se zavedením dvojitého faktoriálu lze zapsat vzorec (1.2) v kompaktnější podobě:

$$T_n = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} (2k-1)!!.$$

2. Rozmisťování věží

V této kapitole si představíme aplikaci telefonních čísel, a sice na jedné z šachových rozmisťovacích úloh. Tyto úlohy obecně zkoumají, jak lze rozmístit dané šachové figurky na šachovnici tak, aby se navzájem neohrožovaly; případně může být cílem spočítat, kolik takových možností existuje.

My se budeme zabývat věžemi, což jsou figurky, které se pohybují vertikálně a horizontálně o libovolný počet polí. Dvě věže se tedy navzájem ohrožují, pokud sdílí stejný řádek nebo stejný sloupec.

Začneme nejdřív zjednodušenou variantou úlohy:

Úloha 7. *Kolik existuje různých rozmístění n neohrožujících se věží na šachovnici $n \times n$?*

Stačí si uvědomit, že v žádném řádku (ani sloupci) nemůžou být dvě a více věží, tedy musíme do každého řádku umístit jednu věž. Pro nalezení jednoho řešení vlastně hledáme zobrazení, které věži z i-tého řádku přiřadí číslo sloupce od 1 do n takové, že není přiřazeno jiné věži (věž na i-tém řádku bude ve vybraném sloupci sama). Úloha po nás vyžaduje spočítat všechny bijekce na n-prvkové množině, tedy všechny permutace. Těch je $n!$, a to je i řešení úlohy.

Úloha 8 (Věžová úloha)**.** *Kolik existuje různých rozmístění n neohrožujících se věží na šachovnici $n \times n$, pokud rozmístění lišící se otočením či zrcadlovým převrácením považujeme za totožná?*

Nyní se situace začíná komplikovat, k nalezení řešení budeme potřebovat nové názvosloví a zformulování Burnsideova lemmatu. V následující sekci je zahrnut kompletní důkaz Burnsideova lemmatu (včetně dvou pomocných lemmat), který je ale spíše technického rázu, a netrpělivý čtenář jej může bez újmy přeskočit.

2.1 Burnsideovo lemma

V této části vycházíme ze zdroje [4]. Nejprve si ustanovíme značení. Mějme n-prvkovou množinu X, $S(X)$ pak značí množinu všech permutací na této množině. Společně s operací skládání tvoří $S(X)$ grupu. Permutace budeme značit řeckými písmeny π, ρ atd.

Dále budeme pracovat s podgrupou grupy $S(X)$, tu označíme G. Připomeňme, že se jedná o libovolnou množinu permutací, která je uzavřená na skládání, obsahuje identitu a ke každé z vybraných permutací její inverzi.

V následujícím textu považujme množinu X a podgrupu G za pevně vybrané.

Definice 9. *Pro $x \in X$ nazveme $O_x := \{\pi(x) \mid \pi \in G\}$* orbitou *prvku x. Množinu všech orbit označíme $\mathcal{O}$, tedy $\mathcal{O} := \{O_x \mid x \in X\}$.*

Orbita prvku x je vlastně množina všech prvků, kam se může x zobrazit permutacemi z G. Protože identita musí být v každé podgrupě, platí $x \in O_x$.

Věta 10. *Orbity tvoří rozklad množiny X.*

Důkaz. Rozklad množiny znamená, že každý prvek z X náleží právě do jedné podmnožiny – orbity. Víme, že každé x náleží do své vlastní orbity O_x, stačí tedy dokázat, že neexistuje prvek náležící do vícera orbit. Pro spor předpokládejme $y \in X$ takové, že $y \in O_x$ a zároveň $O_x \neq O_y$. Nyní je důležité, že G tvoří grupu. G obsahuje inverze, takže když se z x lze dostat do y (to znamená $y \in O_x$), pak se z y lze dostat do x. A protože G je uzavřená na skládání, z y se lze dostat do každého prvku O_x, a stejně tak z x se lze dostat do každého prvku O_y. Z toho plyne $O_x = O_y$, což je spor.

□

Definice 11. Pevným bodem *zobrazení rozumíme bod, který se zobrazí sám na sebe. Pro $\pi \in S(X)$ označme $P_\pi := \{x \in X \mid \pi(x) = x\}$. Dále pro $x \in X$ označme $St_x := \{\pi \in G \mid \pi(x) = x\}$.*

P_π je množina pevných bodů permutace π. Množině St_x se odborně říká *stabilizátor* prvku x. Jedná se o množinu permutací z G, pro niž je x pevným bodem; právě tyto permutace tedy nehnou s bodem x. Povšimněme si, že identita je vždy prvkem této množiny.

Lemma 12. *Mějme $x \in X$, pak $|O_x| \cdot |St_x| = |G|$.*

Důkaz. Pro $y \in O_x$ označme permutaci $\pi_y \in G$, která převádí x na y. Takových permutací může být více, pak stačí jednu z nich napevno vybrat.

Nabízí se spočítat všechny dvojice (y, ρ) takové, že $y \in O_x$ a $\rho \in St_x$. Stačí však najít vhodné párování těchto dvojic s permutacemi z G, čímž dokážeme, že jejich počet je $|G|$. Párování musí být bijektivní (prosté a na), což znamená, že každá permutace je spárovaná s právě jednou dvojicí (y, ρ) – pak až můžeme tvrdit, že $|O_x| \cdot |St_x| = |G|$.

Spárujeme dvojici (y, ρ) s permutací $\pi_y \circ \rho$. Protože $\pi_y \in G$ i $\rho \in G$, pak i jejich složení náleží G. Teď je nutné ukázat, že každá dvojice má přidělenou unikátní permutaci (tj. předpis je prostý) a že žádná permutace z G není vynechána (tj. předpis je na).

(1) Mějme $y_1, y_2 \in O_x$ a $\rho_1, \rho_2 \in St_x$. Zpermutovnáním prvku x dostaneme $(\pi_{y_1} \circ \rho_1)(x) = \pi_{y_1}(x) = y_1$ a $(\pi_{y_2} \circ \rho_2)(x) = \pi_{y_2}(x) = y_2$. Pokud $y_1 \neq y_2$, pak tyto permutace musí být různé. Nechť tedy $y_1 = y_2$ a $\rho_1 \neq \rho_2$, pak existuje $z \in X$ takové, že $\rho_1(z) \neq \rho_2(z)$. Protože $\pi_{y_1} = \pi_{y_2}$, pak $\pi_{y_1} \circ \rho_1 \neq \pi_{y_2} \circ \rho_2$. Předpis je prostý.

(2) Mějme permutaci $\sigma \in G$ a hledejme pro ni $y \in O_x$ a $\rho \in St_x$ takové, že bude platit $\sigma = \pi_y \circ \rho$. Zkusme zvolit $\rho = \sigma$, to však je validní pouze v případě, že σ nehne s x. Pomůžeme si tedy složením s inverzní permutací $\pi^{-1}_{\sigma(x)}$, která zobrazuje $\sigma(x)$ zpět na x. Tedy $\rho = \pi^{-1}_{\sigma(x)} \circ \sigma \in St_x$. Z toho plyne i volba $y = \sigma(x)$, protože $\pi_{\sigma(x)} \circ \pi^{-1}_{\sigma(x)} \circ \sigma = \sigma$.

□

Lemma 13. *Mějme $x, y \in X$ takové, že $y \in O_x$, pak $|St_x| = |St_y|$.*

Slovy nám lemma říká, že pro prvky též orbity platí, že počet permutací, které s nimi nehnou, je u nich stejný.

Důkaz. Použijeme podobný postup jako u předchozího lemmatu: hledáme bijektivní zobrazení $F : St_x \to St_y$. Nechť opět π_y je vybraná permutace, která zobrazí x na y, a tudíž π_y^{-1} naopak zobrazí y na x. Pro $\rho \in St_x$ položme $F(\rho) = \pi_y \circ \rho \circ \pi_y^{-1}$; platí, že $F(\rho) \in St_y$.

Pro $\rho_1, \rho_2 \in St_x$ takové, že $F(\rho_1) = F(\rho_2)$, platí rovnost $\pi_y \circ \rho_1 \circ \pi_y^{-1} = \pi_y \circ \rho_2 \circ \pi_y^{-1}$, z čehož přímo vyplývá $\rho_1 = \rho_2$, tedy F je prosté. Pro $\omega \in St_y$ hledáme $\rho \in St_x$ takové, že $\omega = F(\rho)$, tedy $\omega = \pi_y \circ \rho \circ \pi_y^{-1}$. Stačí zvolit $\rho = \pi_y^{-1} \circ \omega \circ \pi_y$ a tím je dokázáno, že F je na.

□

Věta 14 (Burnsideovo lemma)**.** *Pro každou podgrupu G grupy $S(X)$ platí*

$$|\mathcal{O}| = \frac{1}{|G|} \sum_{\pi \in G} |P_\pi|.$$

Slovy počet orbit množiny permutací G je roven průměrnému počtu pevných bodů permutací z G.

Důkaz. Dokazovat budeme ekvivalentní vztah $|\mathcal{O}| \cdot |G| = \sum_{\pi \in G} |P_\pi|$. Dále si pomůžeme trikem: zavedeme množinu $A = \{(\pi, x) \mid \pi \in G, x \in P_\pi\}$ a dvěma způsoby spočítáme její velikost.

(1) Počet dvojic je roven součtu počtů pevných bodů pro všechny permutace z G, z čehož získáme rovnost $|A| = \sum_{\pi \in G} |P_\pi|$.

(2) Počet dvojic lze také získat tak, že pro každé x vezmeme počet permutací, které nehnou s x, a nasčítáme přes všechna x. Tedy získáme rovnost $|A| = \sum_{x \in X} |St_x|$. Nyní využijeme lemmatu 13 a zjednodušíme sumu na iteraci přes orbity: $|A| = \sum_{O \in \mathcal{O}} |O| \cdot |St_{x_O}|$, kde x_O představuje vybraný (libovolný) prvek orbity O. Použití lemmatu 12 upraví rovnici na $|A| = \sum_{O \in \mathcal{O}} |G| = |\mathcal{O}| \cdot |G|$.

Získali jsme tedy rovnost $\sum_{\pi \in G} |P_\pi| = |A| = |\mathcal{O}| \cdot |G|$, čímž je důkaz hotov.

□

2.2 Řešení věžové úlohy

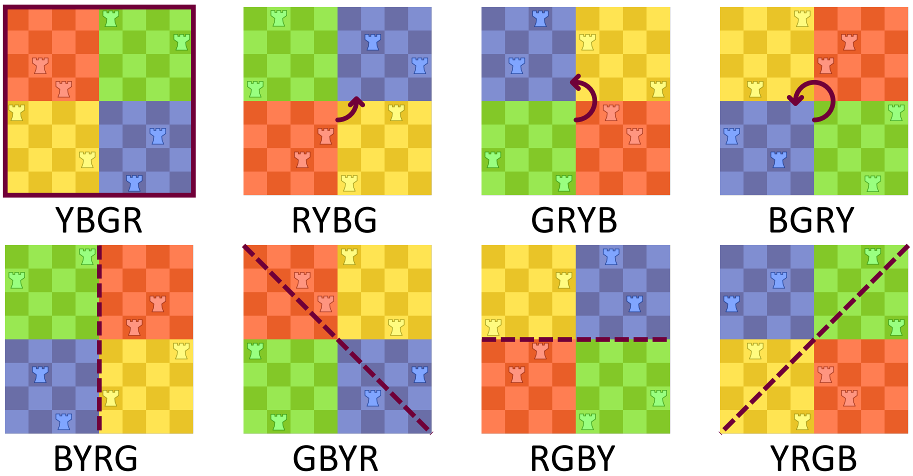
V této podkapitole vyřešíme věžovou úlohu 8 tak, jak je popsáno ve článku [5]. Ve zjednodušené věžové úloze 7 jsme napočítali $n!$ rozmístění. Nyní jich samozřejmě bude méně, protože některá budeme považovat za ekvivalentní. Připomeňme, že tato ekvivalence je definována rotací (o 90, 180 a 270 stupňů), zrcadlovým převrácením (neboli osovou souměrností; vertikální i horizontální) a všemi zobrazeními z nich složenými.

Začneme nalezením množiny všech zobrazení, která zachovávají ekvivalenci. Nechť x značí rotaci o 90 stupňů proti směru hodinových ručiček a nechť y značí vertikální zrcadlové převrácení. Tato dvě zobrazení teď budeme skládat a utvářet nová.

Nabízí se nejdříve skládat pouze rotace a získat tak x^2 a x^3, což jsou rotace o 180 resp. 270 stupňů. x^4 není nic jiného než identita Id, tu musíme též do množiny zahrnout. Pokud nejdříve šachovnici převrátíme (použijeme y) a poté otočíme, získáme další tři zobrazení xy, x^2y a x^3y.

Pojďme si všech 8 zobrazení znázornit na jednom rozmístění věží. Šachovnice je pro názornost obarvená od levého dolního rohu proti směru hodinových ručiček barvami žlutá (Yellow), modrá (Blue), zelená (Green) a červená (Red) – přiřadíme jí zkratku $YBGR$. Obrazy rozmístění budou mít jiné zkratky podle změněného pořadí těchto barev.

$$\begin{array}{ll} Id : YBGR \mapsto YBGR & y : YBGR \mapsto BYRG \\ x : YBGR \mapsto RYBG & xy : YBGR \mapsto GBYR \\ x^2 : YBGR \mapsto GRYB & x^2y : YBGR \mapsto RGBY \\ x^3 : YBGR \mapsto BGRY & x^3y : YBGR \mapsto YRGB \end{array}$$



Obrázek 2.1: Barevné zkratky v obrazech šachovnice

Při prozkoumání obrázku 2.1 si všimněme, že celý druhý řádek (odpovídající zobrazením y, xy, x^2y a x^3y) lze získat pomocí osových souměrností. y a x^2y jsou vertikální a horizontální převrácení, zatímco xy a x^3y jsou souměrnosti podle diagonál. Dále si všimněme, že rotace o 180 stupňů není nic jiného než středová souměrnost.

Celkem tedy máme 8 zobrazení: identitu, tři rotace, dvě převrácení a dvě diagonální souměrnosti. Získali jsme ale všechna navzájem ekvivalentní rozmístění věží? Více obrazů barevné šachovnice neexistuje, protože jsou 4 možnosti, jak obarvit levý dolní roh, a další 2 možnosti, jakým směrem budou další barvy postupovat, celkem tedy 8.

Nalezenou množinu zobrazení označíme $G = \{Id, x, x^2, x^3, y, xy, x^2y, x^3y\}$. G je grupou: je uzavřená na skládání, obsahuje Id a obsahuje inverze svých zobrazení. Z invertibility všech zobrazení vyplývá, že jsou bijektivní, což se nám bude hned hodit.

Nyní můžeme přikročit k řešení našeho problému pomocí Burnsideova lemmatu. Pro dané n označme X množinu všech rozmístění neohrožujících se věží na $n \times n$ šachovnici. Z předchozí úlohy víme, že $|X| = n!$. Dále si uvědomíme, že prvky množiny G lze také chápat jako bijektivní zobrazení na množině X neboli permutace. Z toho vyplývá, že G jakožto podrgupa permutací tvoří rozklad X

na orbity. Jedna orbita je množina rozmístění, které jsou navzájem ekvivalentní a k vyřešení úlohy tedy potřebujeme spočítat počet orbit $|\mathcal{O}|$.

Pro použití Burnsideova lemmatu potřebujeme pro $\pi \in G$ znát počet pevných bodů $|P_\pi|$, tj. počet rozmístění, které π zobrazí samo na sebe. Patrně tato čísla budou stejná pro dvojice x a x^3 (rotace o 90 stupňů), y a x^2y (převrácení), xy a x^3y (diagonální souměrnosti).

Označme $f(n) = |P_{x^2}|$, $g(n) = |P_x| = |P_{x^3}|$, $h(n) = |P_{xy}| = |P_{x^3y}|$ a $i(n) = |P_y| = |P_{x^2y}|$. Pro identitu triviálně platí $|P_{Id}| = n!$. Podle Burnsideova lemmatu získáme rovnost:

$$|\mathcal{O}| = \frac{n! + f(n) + 2g(n) + 2h(n) + 2i(n)}{8}.$$

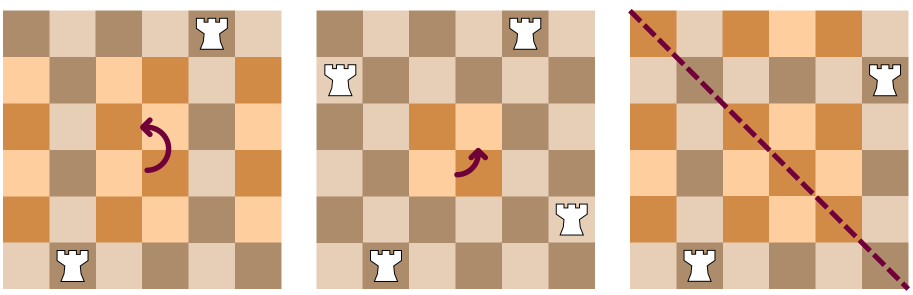
Nejprve pomocí rekurze spočítejme $f(n)$ – počet rozmístění na šachovnici $n \times n$, jež jsou středově souměrná (neměnná vůči středové souměrnosti). Uvažujme nejdříve n sudé, tvaru $n = 2k$.

Triviálně platí $f(2) = 2$. Dále pro indukční krok mějme prázdnou šachovnici $2k \times 2k$. Protože každému řádku náleží právě jedna věž, můžeme první věž umístit na i-tou pozici zleva do posledního řádku a poté středově souměrně věž na i-tou pozici zprava do prvního řádku. Toto lze provést $2k$ způsoby a pro všechny platí, že věže se navzájem nebudou ohrožovat (nemáme prostřední sloupec).

Položením těchto věží jsme zabrali dva středově souměrné řádky a dva středově souměrné sloupce, které si můžeme ze šachovnice odmyslet a zbyde nám šachovnice $(2k-2) \times (2k-2)$ s týmž středem – viz obrázek 2.2 vlevo. Počet možností, jak na tomto zbytku provést rozmístění $2k-2$ neohrožujících se věží, je $f(2k-2)$. Získali jsme tak rekurentní vzorec $f(2k) = 2kf(2k-2)$. Protože $f(2) = 2$, pak $f(4) = 4 \cdot 2$, $f(6) = 6 \cdot 4 \cdot 2$ a obecně $f(2k) = 2k(2k-2)\ldots 4 \cdot 2$ – tak jsme v první kapitole definovali dvojitý faktoriál čísla $2k$ (definice 6). Získáme tak explicitní vzorec

$$f(2k) = 2^k k! = (2k)!!.$$

Pro liché $n = 2k+1$ je na středově souměrném rozmístění pozice jedné věže pevně daná. Protože na šachovnici existuje prostřední řádek, pak věž v něm se musí nacházet v samotném středu šachovnice, jinak by se při zachování středové souměrnosti musely nacházet v tomto řádku dvě věže. Rozmístění zbylých věží pak provádíme na šachovnici $2k \times 2k$, tedy platí $f(2k+1) = f(2k)$.



Obrázek 2.2: Pokládání věže do posledního řádku při zachování souměrnosti v pořadí podle středu, „podle čtvrtin“ a podle diagonály

Nyní podobným způsobem vypočítejme $g(n)$ – počet rozmístění, jež jsou neměnná vůči rotaci o 90 stupňů. Opět nejdřív budeme uvažovat sudé $n = 2k$.

První dvě hodnoty vypadají takto: $g(2) = 0, g(4) = 2$. Mějme opět prázdnou šachovnici $2k \times 2k$ a položme první věž někam do posledního řádku – řekněme, že na i-tou pozici zleva. Pro zachování souměrnosti pak musíme položit věž i do posledního sloupce na i-tou pozici zdola, do prvního řádku na i-tou pozici zprava a do prvního sloupce na i-tou pozici shora, jak je znázorněno na obrázku 2.2 uprostřed. Tyto věže se budou vzájemně ohrožovat právě tehdy, pokud se budou nacházet v rozích. Díky sudosti n nemůže nastat, že by se ohrožovaly protilehlé věže. Počet možností pro výběr pozice věže na posledním řádku je tedy $2k - 2$ a rekurentní vzorec je $g(2k) = (2k - 2)g(2k - 4)$.

Je-li n dělitelné 4, a tedy vyjádřitelné ve tvaru $n = 4k$, pak $g(8) = 6 \cdot 2$ a obecně $g(4k) = (4k - 2)(4k - 6) \dots 6 \cdot 2$. Tuto rekurentní rovnici lze podobně jako u $f(2k)$ vyřešit explicitním vzorcem pomocí dvojitého faktoriálu:

$$g(4k) = 2^k(2k - 1)(2k - 3) \dots 3 \cdot 1 = 2^k(2k - 1)!!.$$

Pokud není sudé n dělitelné 4, pak $n = 4k + 2$ a platí $g(4k + 2) = 0$. Pro lichá n stále platí, že v rozmístěních musí být věž uprostřed šachovnice (stále se totiž jedná o středově souměrná rozmístění) a platí tedy, že $g(2k + 1) = g(2k)$.

Další v pořadí je $h(n)$ – počet rozmístění věží, jež jsou souměrná podle diagonály. Prvních několik hodnot vypadá následovně: $h(1) = 1, h(2) = 2, h(3) = 4$. Představme si opět prázdnou šachovnici $n \times n$ a pokládejme věž do n-tého řádku. Můžeme ji položit do rohu na diagonálu, pak na zbytek šachovnice lze rozmístit věže $h(n-1)$ způsoby. Pokud ji položíme na jedno ze zbylých $n-1$ polí, musíme pro zachování souměrnosti podle diagonály přidat příslušnou věž do n-tého sloupce, viz obrázek 2.2 vpravo. Tyto věže se nikdy ohrožovat nebudou. Po odmyšlení ohrožených polí zbývá pokrýt šachovnici $(n - 2) \times (n - 2)$, což je možné $h(n - 2)$ způsoby. Získali jsme tedy rekurentní vzorec $h(n) = h(n - 1) + (n - 1)h(n - 2)$, který je společně s prvními hodnotami totožný se vzorcem pro telefonní čísla, která jsme prozkoumávali v předchozí kapitole, tedy platí

$$h(n) = T_n.$$

Nakonec $i(n)$ jakožto počet rozmístění věží symetrických podle vertikální nebo horizontální osy je vždy roven nule, protože takové rozmístění pro $n > 1$ vyžaduje dvojice věží ve stejném řádku či sloupci, čímž by se ohrožovaly.

Řešením pro $n > 1$ je tedy:

$$|\mathcal{O}| = \frac{n! + f(n) + 2g(n) + 2T_n}{8},$$

kde

$$f(n) = \begin{cases} (2k)!! & \text{pro } n = 2k \text{ (sudé)}, \\ (2k)!! & \text{pro } n = 2k + 1 \text{ (liché)}, \end{cases}$$

$$g(n) = \begin{cases} 2^k(2k - 1)!! & \text{pro } n = 4k \text{ (dělitelné 4)}, \\ 2^k(2k - 1)!! & \text{pro } n = 4k + 1, \\ 0 & \text{jinak.} \end{cases}$$

Čtenáře jistě zajímá, jaký bude výsledek pro klasickou šachovnici 8×8. Konkrétní hodnoty pro nízká n jsou napsána v následující tabulce.

n	2	3	4	5	6	7	8	9	10
$\lvert\mathcal{O}\rvert$	1	2	7	23	115	694	5282	46066	456454
$n!$	2	6	24	120	720	5040	40320	362880	3628800
$n! : \lvert\mathcal{O}\rvert$	2	3	$\approx$3.43	$\approx$5.22	$\approx$6.26	$\approx$7.26	$\approx$7.63	$\approx$7.88	$\approx$7.95

Ve druhém řádku tabulky je výsledek této úlohy a ve třetím výsledek zjednodušené věžové úlohy 7, oboje pro n v rozsahu 2 až 10. Vyčteme, že na klasické šachovnici existuje celkem $8! = 40320$ rozmístění a z nich lze vybrat nejvýše 5282 reprezentantů takových, aby se vzájemně nelišili o rotaci ani o převrácení.

Ve čtvrtém řádku je vypočítán poměr předešlých dvou řádků, který nám říká, jak velké jsou v průměru třídy ekvivalence pro dané n. Z tabulky je patrné, že pro rostoucí n se tento poměr zezdola blíží k číslu 8. Toto číslo jistě nebude překročeno, protože třídy ekvivalence mohou mít dle definice nejvýše 8 prvků. Dokonce lze snadno nahlédnout, že poměr bude k 8 konvergovat, protože v čitateli řešení $|\mathcal{O}|$ roste $n!$ řádově rychleji než funkce $f(n)$, $g(n)$ i T_n.

Závěrem této kapitoly připomeňme propojení s tématem práce. Při řešení věžové úlohy jsme získali další pohled na telefonní čísla, a sice že n-té telefonní číslo odpovídá počtu rozmístění n navzájem se neohrožujících věží na šachovnici $n \times n$, která jsou souměrná podle diagonály.

3. Permutace s cykly předepsaných délek

V kapitole o telefonních číslech jsme si představili permutace složené pouze z nezávislých jednocyklů a dvojcyklů. Nyní nás budou zajímat permutace, které se skládají z cyklů jinak pevně zvolených délek. Opět se pokusíme zjistit jejich počet nad n-prvkovou množinou.

Množinu přípustných délek označme $C \subset \mathbb{N}$. Počet permutací n-prvkové množiny skládajících se z cyklů délek z C označme $g_C(n)$. Jako triviální případ položme $g_C(0) = 1$. Víme, že pro involutorní permutace byla $C = \{1, 2\}$ a tedy $g_{\{1,2\}}(n) = T_n$.

Následující úlohy již nebudou mít podklad v reálném světě, jak to bylo s telefonními čísly. Jistou interpretaci si tedy aspoň zmiňme zde:

Kolika způsoby lze n osob rozesadit ke kulatým stolům? Chceme, aby počet osob u každého stolu byl z dané množiny C. Nezáleží na tom, kdo sedí u kterého stolu ani na jakém místě – záleží jen na tom, koho má po levé a pravé ruce.

Zřejmě kulaté stoly představují cykly délek z množiny C. Takto tedy lze pohlížet na všechny následující úlohy.

3.1 Kombinatorický postup

Nejdřív se pokusme řešit úlohy podobným postupem, který jsme použili i pro telefonní čísla. Cílem je tedy získat rekurentní rovnici, případně explicitní vzorec vyjádřený sumou. Začneme úlohou velmi podobnou úloze 1 s telefonními čísly.

Úloha 15. *Kolik existuje permutací nad n-prvkovou množinou, které sestávají pouze z nezávislých jednocyklů a trojcyklů?*

V této úloze je $C = \{1, 3\}$, a tedy řešením pro n budeme rozumět číslo $g_{\{1,3\}}(n)$.

Nejprve nalezněme řešení pomocí rekurze. Jeden prvek ani dva prvky trojcyklus neutvoří, takže $g_{\{1,3\}}(1) = 1$ a $g_{\{1,3\}}(2) = 1$. Ze tří prvků lze vytvořit dva trojcykly nebo trojici jednocyklů, takže $g_{\{1,3\}}(3) = 3$. Obecně platí, že n-tý prvek může být součástí trojcyklu, jenž vybereme $(n-1)(n-2)$ způsoby (pomyslně vybíráme prvky na druhé a třetí místo v cyklu), nebo může tvořit jednocyklus. Pro $n > 3$ tedy získáme rekurentní vzorec

$$g_{\{1,3\}}(n) = g_{\{1,3\}}(n-1) + (n-1)(n-2)g_{\{1,3\}}(n-3). \tag{3.1}$$

Všimněme si podobnosti s rekurentním vzorcem (1.1) pro telefonní čísla. I následující explicitní vzorec bude velmi podobný vzorci (1.2):

$$g_{\{1,3\}}(n) = \sum_{k=0}^{\lfloor n/3 \rfloor} \binom{n}{3k} \frac{(3k)!}{3^k k!}. \tag{3.2}$$

Proměnná k v této sumě značí počet trojic prvků tvořících cykly. Podobně jako u vzorce (1.2) pomyslně nejdříve vybereme všechny prvky účastnící se trojcyklu (kombinační číslo), ty seřadíme (čitatel zlomku), ale nezáleží vlastně na pořadí trojic v seřazení ($k!$) ani na tom, který ze tří prvků je v cyklu uveden jako první (3^k).

Zde je tabulka hodnot $g_{\{1,3\}}(n)$ pro nízká n:

n	0	1	2	3	4	5	6	7	8	9	10
$g_{\{1,3\}}(n)$	1	1	1	3	9	21	81	351	1233	5769	31041

Povšimněme si, že $(n-1)(n-2)$ ve vzorci (3.1) je vlastně počet 2-členných variací z $(n-1)$-prvkové množiny (bez opakování). Cyklů délky l, které obsahují jeden daný prvek, je stejný počet jako $(l-1)$-členných variací z $(n-1)$-prvkové množiny.

Definice 16. *Počet l-členných variací z n-prvkové množiny označme symbolem $V(l,n) \coloneqq n(n-1)\dots(n-l+1)$ pro $0 < l \leq n$ a $V(l,n) \coloneqq 0$ pro $l > n$. Dále položme $V(0,n) \coloneqq 1$.*

Využití najdeme v následující úloze, kde již uvažujeme obecnou volbu C. Výsledný vzorec je převzat z knihy [6], s. 280.

Úloha 17. *Kolik existuje permutací nad n prvkovou množinou, které sestávají pouze z nezávislých cyklů délek z dané množiny C?*

Na pravé straně rekurentní rovnice bude suma, v níž každý sčítanec bude odpovídat jedné přípustné délce $c \in C$ cyklu, jenž obsahuje n-tý prvek. Doplnit cyklus délky $c \leq n$ lze $(n-1)(n-2)\dots(n-c+1)$ způsoby a cyklus délky $c > n$ nula způsoby, což oboje odpovídá počtu $(c-1)$-členných variací z $(n-1)$-prvkové množiny. Získáme tedy vzorec:

$$g_C(n) = \sum_{c \in C} V(c-1, n-1) \cdot g_C(n-c). \tag{3.3}$$

Už jsme definovali $g_C(0) = 1$, a tak lze rekurentně vypočítat $g_C(n)$ pro libovolné n.

3.2 Exponenciální generující funkce

Kombinatorické postupy nyní nahradíme matematickou analýzou, konkrétně prací s mocninnými řadami a exponenciálami. Náročnější cesta k sestavení věty se nám následně splatí algoritmickým vyřešením hned několika úloh.

Ve zbytku této kapitoly vycházíme z knihy [7] – ze stran 113–118 je převzata teorie, kterou zde uvádíme ve zjednodušené podobě, a strany 118–122 obsahují příklady, které se posléze pokusíme řešit.

Začneme zavedením hlavního pojmu:

Definice 18. Exponenciální generující funkcí *posloupnosti $\{a_n\}_{n=0}^{\infty}$ rozumíme mocninnou řadu*

$$A(x) \coloneqq \sum_{n=0}^{\infty} a_n \frac{x^n}{n!}.$$

Exponenciální generující funkci posloupnosti $\{g_C(n)\}_{n=0}^{\infty}$ počtu permutací nad n-prvkovou množinou o délkách cyklů z množiny C budeme značit $G_C(x)$.

Cílem této podkapitoly bude dokázat hlavní větu 21, k tomu budeme potřebovat následující lemmata 19 a 20. V další podkapitole větu využijeme k řešení úloh.

Lemma 19. *Pro každou exponenciální generující funkci $A(x)$ a $k \in \mathbb{N}$ platí:*

$$A^k(x) = \left(\sum_{i=0}^{\infty} a_i \frac{x^i}{i!}\right)^k = \sum_{n=0}^{\infty} \left(\sum_{\substack{i_1,\dots,i_k \in \mathbb{N}_0 \\ i_1+\dots+i_k=n}} \frac{a_{i_1}}{i_1!} \cdots \frac{a_{i_k}}{i_k!} \right) x^n.$$

Důkaz. Mocninnou řadu $A(x)$ jsme umocnili na k-tou – představme si tedy součin k těchto mocninných řad. Jakými způsoby lze z tohoto součinu získat x^n? Nechť pro každé $m \in \{1, \dots, k\}$ vybereme z m-té sumy člen obsahující mocninu x^{i_m}, kde $i_m \in \mathbb{N}_0$. Pokud zvolíme i_m tak, aby se posčítala na n, pak součin vybraných členů bude obsahovat mocninu x^n a její koeficient bude součinem koeficientů všech vybraných členů (zlomky na pravé straně rovnice).

Nyní nám stačí najít všechny takové výběry i_m, čímž získáme všechny součiny obsahující x^n. $A^k(x)$ je pak mocninná řada, jež má za n-tý prvek výše uvedený součet.

□

Pro další pozorování označme $g_{C,k}(n)$ počet permutací nad n-prvkovou množinou tvořených právě k cykly, jejichž délky jsou z množiny C. Triviálně platí

$$g_C(n) = \sum_{k=0}^{\infty} g_{C,k}(n).$$

Uvidíme, že se nám vyplatí uvažovat nekonečnou sumu, i když sčítance samozřejmě mohou nabývat nenulových hodnot pouze pro $k \in \{1, 2, \dots, n\}$.

Lemma 20.

$$g_{C,k}(n) = \frac{n!}{k!} \left(\sum_{\substack{i_1,\dots,i_k \in \mathbb{N}_0 \\ i_1+\dots+i_k=n}} \frac{f(i_1)}{i_1!} \cdots \frac{f(i_k)}{i_k!} \right),$$

kde funkce f je definována předpisem

$$f(i) = \begin{cases} (i-1)! & \text{pro } i \in C, \\ 0 & \text{jinak.} \end{cases}$$

Důkaz. Zkusme sestavit permutaci nad n-prvkovou množinou o k cyklech, které mají délky z množiny C. Budeme permutovat n-prvkovou množinu $\{1, \dots, n\}$. Vyberme pro $m \in \{1, \dots, k\}$ čísla i_m tak, aby $i_m \in C$ a $i_1 + \dots + i_k = n$, pak i_m bude značit délku m-tého cyklu permutace. Permutujme čísla $1, \dots, n$ a položme je do seřazených cyklů od prvního do k-tého. To je zdánlivě $n!$ možností, vznikly by nám ale duplicity: jednak nezáleží na pořadí cyklů, jednak nezáleží na vybraném prvním prvku v cyklu. Vydělíme tedy $k!$ (pořadí cyklů) a i_m pro každé i_m (výběr prvního prvku v cyklu).

To v rovnici sedí, protože pokud skutečně pro všechna m platí $i_m \in C$, pak násobíme $\frac{f(i_m)}{i_m!} = \frac{(i_m-1)!}{i_m!} = \frac{1}{i_m}$. Pokud existuje m takové, že $i_m \notin C$, pak z definice f vyjde celý sčítanec nulový.

□

Věta 21. *Pro libovolný výběr $C \subset \mathbb{N}$ platí:*

$$G_C(x) = \sum_{n=0}^{\infty} g_C(n) \frac{x^n}{n!} = \exp\left(\sum_{n \in C} \frac{x^n}{n}\right).$$

Důkaz.

$$G_C(x) = \sum_{n=0}^{\infty} \frac{g_C(n)}{n!} x^n = \sum_{n=0}^{\infty} \sum_{k=0}^{\infty} \frac{g_{C,k}(n)}{n!} x^n = \sum_{k=0}^{\infty} \sum_{n=0}^{\infty} \frac{g_{C,k}(n)}{n!} x^n.$$

Rozepíšeme $g_{C,k}(n)$ podle lemmatu 20:

$$\sum_{k=0}^{\infty} \sum_{n=0}^{\infty} \frac{n!}{k!} \left(\sum_{\substack{i_1,\dots,i_k \in \mathbb{N}_0 \\ i_1+\dots+i_k=n}} \frac{f(i_1)}{i_1!} \cdots \frac{f(i_k)}{i_k!} \right) \frac{x^n}{n!}.$$

Upravíme, $n!$ se pokrátí:

$$\sum_{k=0}^{\infty} \frac{1}{k!} \sum_{n=0}^{\infty} \left(\sum_{\substack{i_1,\dots,i_k \in \mathbb{N}_0 \\ i_1+\dots+i_k=n}} \frac{f(i_1)}{i_1!} \cdots \frac{f(i_k)}{i_k!} \right) x^n.$$

Použijeme lemma 19 a rozepíšeme podle definice f:

$$\sum_{k=0}^{\infty} \frac{1}{k!} \left(\sum_{i=0}^{\infty} f(i) \frac{x^i}{i!} \right)^k = \sum_{k=0}^{\infty} \frac{1}{k!} \left(\sum_{i \in C} (i-1)! \frac{x^i}{i!} \right)^k = \sum_{k=0}^{\infty} \frac{1}{k!} \left(\sum_{i \in C} \frac{x^i}{i} \right)^k.$$

Nakonec si stačí všimnout, že mocninná řada se sečte na exponenciálu:

$$\exp\left(\sum_{i \in C} \frac{x^i}{i}\right).$$

□

Tato věta bude klíčem k vyřešení všech následujících úloh. Postup lze shrnout do dvou kroků: nejdřív je třeba vyjádřit exponenciálu co nejjednodušším způsobem ve tvaru mocninné řady (pomocí prostředků matematické analýzy) a následně porovnáme koeficienty u x^n dvou mocninných řad, z čehož získáme vzorec pro $g_C(n)$.

3.3 Analytický postup

Úloha 22. *Kolik existuje permutací nad n-prvkovou množinou, které sestávají pouze z nezávislých dvojcyklů?*

Ekvivalentně lze říci, že zjišťujeme počet involutorních permutací bez pevných bodů (tzn. neobjevují se jednocykly).

Máme tedy množinu $C = \{2\}$, označme generující funkci $G_2(x)$ a řešení úlohy $g_2(n)$. Dle věty 21 platí $G_2(x) = \exp(x^2/2)$. Pro nalezení rozvoje této exponenciály do mocninné řady si vzpomeňme na vzorec

$$\exp(x) = 1 + x + \frac{x^2}{2} + \frac{x^3}{3!} + \frac{x^4}{4!} + \cdots = \sum_{k=0}^{\infty} \frac{x^k}{k!}, \tag{3.4}$$

kam stačí dosadit $x^2/2$ za x. Získáme rovnost

$$G_2(x) = \exp\left(\frac{x^2}{2}\right) = \sum_{k=0}^{\infty} \frac{x^{2k}}{2^k k!}.$$

Nyní použijeme definici exponenciální generující funkce, čímž obdržíme rovnost

$$\sum_{n=0}^{\infty} g_2(n)\frac{x^n}{n!} = \sum_{k=0}^{\infty} \frac{x^{2k}}{2^k k!}.$$

Zbývá zjistit $g_2(n)$ porovnáním koeficientů u x^n. Pro n liché je koeficient na pravé straně rovnosti 0. Pak i $g_2(2k+1) = 0$, což není žádné překvapení: neexistuje permutace nad lichým počtem prvků, která se má skládat jen z dvojcyklů.

Uvažujme tedy $n = 2k$. Ze vzorce vyplývá, že $g_2(2k) = \frac{(2k)!}{2^k k!}$, což je dle definice 6 dvojitý faktoriál lichých čísel: $g_2(2k) = (2k-1)!!$.

K tomuto výsledku lze snadno dojít i kombinatorickou cestou. Ptáme se, kolika způsoby je možné spárovat $2k$ různých prvků v nějakém uspořádání. Nejmenší prvek lze spárovat $(2k-1)$ způsoby. Vezměme teď nejmenší prvek, který jsme ještě nepoužili – ten lze spárovat $(2k-3)$ způsoby. Takto lze pokračovat, dokud nezbydou poslední dva prvky. Řešením tedy je $(2k-1)(2k-3)\ldots 3\cdot 1 = (2k-1)!!$.

Úloha 23. *Kolik existuje permutací nad n-prvkovou množinou bez pevných bodů?*

Označíme D_n počet řešení dané úlohy a $D(x)$ příslušnou generující funkci. Zde $C = \{2, 3, \ldots\}$, tedy dle věty 21

$$D(x) = \exp\left(\sum_{n=2}^{\infty} \frac{x^n}{n}\right).$$

Pro úpravu exponentu se nám bude hodit známý zápis logaritmu pomocí mocninné řady

$$\ln(1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} x^n, \tag{3.5}$$

do kterého dosadíme $-x$ za x:

$$\ln(1 - x) = -x - \frac{x^2}{2} - \frac{x^3}{3} - \frac{x^4}{4} - \cdots = \sum_{n=1}^{\infty} -\frac{x^n}{n}.$$

Řada v exponentu tedy bude $-\ln(1-x) = \ln\frac{1}{1-x}$, a protože suma začíná až od $n = 2$, pak bude ještě třeba odečíst první člen x. Získáme tedy

$$D(x) = \exp\left(\ln \frac{1}{1-x} - x\right) = \frac{1}{1-x} \exp(-x),$$

což lze dále převést na součin dvou mocninných řad:

$$D(x) = \left(\sum_{j=0}^{\infty} x^j\right)\left(\sum_{k=0}^{\infty} \frac{(-x)^k}{k!}\right).$$

Součinem bude opět mocninná řada. Zpozorujme, že sčítanec s x^n získáme vynásobením k-tého členu druhé sumy s $(n-k)$-tým členem první sumy, kde $0 \leq k \leq n$. Tento sčítanec bude mít koeficient $\frac{(-1)^k}{k!}$, celkový koeficient u x^n pak bude sumou těchto zlomků přes všechna k. A generující funkci $D(x)$ půjde zapsat jako sumu přes všechna n, čímž získáme vzorec

$$D(x) = \sum_{n=0}^{\infty} x^n \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

Nakonec stačí rozepsat $D(x)$ podle definice a vyjádřit D_n:

$$\sum_{n=0}^{\infty} D_n \frac{x^n}{n!} = \sum_{n=0}^{\infty} x^n \sum_{k=0}^{n} \frac{(-1)^k}{k!}$$
$$D_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

Protože $n!$ je počet všech permutací, musí být suma číslo menší než 1. Pokud bychom v sumě provedli limitní přechod do nekonečna $(n \to \infty)$, získáme podle vzorce (3.4) rozklad čísla $\exp(-1) = \frac{1}{e}$. To nám říká, že počet permutací bez pevných bodů je přibližně roven $\frac{n!}{e}$, což je o něco více než jedna třetina počtu všech permutací ($e \doteq 2{,}718$).

Podívejme se nyní znovu na úlohy 1 a 15, které jsme již dokázali vyřešit kombinatoricky, a zkusme dojít ke stejným výsledkům pomocí věty 21.

Úloha 24 (O telefonních číslech). *Kolik existuje permutací nad n-prvkovou množinou, které sestávají pouze z nezávislých jednocyklů a dvojcyklů?*

Počet řešení dané úlohy je T_n (n-té telefonní číslo), příslušnou generující funkci označme $T(x)$. Použitím věty 21 získáme:

$$T(x) = \exp\left(x + \frac{x^2}{2}\right) = \exp(x) \cdot \exp\left(\frac{x^2}{2}\right).$$

Odkážeme se na rozvoje exponenciální funkce z úlohy 22 a získáme součin dvou mocninných řad:

$$\left(\sum_{j=0}^{\infty} \frac{x^j}{j!}\right)\left(\sum_{k=0}^{\infty} \frac{x^{2k}}{2^k k!}\right).$$

Budeme zjišťovat koeficient u x^n tohoto součinu. Jeden sčítanec s x^n získáme vynásobením k-tého členu z druhé řady s $(n-2k)$-tým členem z první řady, kde

$0 \leq k \leq \lfloor n/2 \rfloor$. Koeficient tohoto sčítance je $\frac{1}{(n-2k)!2^k k!}$. Koeficient součtu všech členů s x^n pak bude

$$\sum_{k=0}^{\lfloor n/2 \rfloor} \frac{1}{2^k k!(n-2k)!}$$

a výsledná mocninná řada má tvar

$$T(x) = \sum_{n=0}^{\infty} x^n \sum_{k=0}^{\lfloor n/2 \rfloor} \frac{1}{2^k k!(n-2k)!}.$$

Nyní stačí jen řadu upravit do vhodné podoby, aby se z ní podle definice $T(x)$ dalo vyčíst číslo T_n:

$$T(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!} \sum_{k=0}^{\lfloor n/2 \rfloor} \frac{n!}{(2k)!(n-2k)!} \frac{(2k)!}{2^k k!} = \sum_{n=0}^{\infty} \frac{x^n}{n!} \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} (2k-1)!!,$$

$$T_n = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} (2k-1)!!.$$

Úloha 25. *Kolik existuje permutací nad n-prvkovou množinou, které sestávají pouze z nezávislých jednocyklů a trojcyklů?*

Postup je téměř identický s předchozí úlohou. Nejdříve tedy rozepíšeme exponenciálu na součin dvou mocninných řad podle vzorce (3.4):

$$G_{\{1,3\}}(x) = \exp\left(x + \frac{x^3}{3}\right) = \exp(x) \cdot \exp\left(\frac{x^3}{3}\right) = \left(\sum_{j=0}^{\infty} \frac{x^j}{j!}\right) \left(\sum_{k=0}^{\infty} \frac{x^{3k}}{3^k k!}\right).$$

Poté si všimneme, že sčítanec s x^n lze získat právě vynásobením k-tého členu z druhé řady s $(n-3k)$-tým členem z první řady, kde $0 \leq k \leq \lfloor n/3 \rfloor$. Celkový koeficient u x^n je pak součtem koeficientů členů s x^n přes všechna taková k:

$$G_{\{1,3\}}(x) = \sum_{n=0}^{\infty} x^n \sum_{k=0}^{\lfloor n/3 \rfloor} \frac{1}{3^k k!(n-3k)!}.$$

Upravíme tak, abychom zjistili koeficient u $\frac{x^n}{n!}$, což je $g_{\{1,3\}}(n)$.

$$G_{\{1,3\}}(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!} \sum_{k=0}^{\lfloor n/3 \rfloor} \frac{n!}{(3k)!(n-3k)!} \frac{(3k)!}{3^k k!} = \sum_{n=0}^{\infty} \frac{x^n}{n!} \binom{n}{3k} \sum_{k=0}^{\lfloor n/3 \rfloor} \frac{(3k)!}{3^k k!}$$

$$g_{\{1,3\}}(n) = \binom{n}{3k} \sum_{k=0}^{\lfloor n/3 \rfloor} \frac{(3k)!}{3^k k!}$$

3.4 Další příklady

Úloha 26. *Kolik existuje permutací nad n-prvkovou množinou, které sestávají právě z cyklů sudých délek?*

Analytické řešení. Označíme písmenem S množinu kladných sudých čísel, tedy pracujeme s generující funkcí $G_S(x)$ a řešením úlohy je $g_S(n)$.

Vycházejme opět z věty 21:

$$G_S(x) = \exp\left(\frac{x^2}{2} + \frac{x^4}{4} + \frac{x^6}{6} + \dots\right) = \exp\left(\sum_{k=1}^{\infty} \frac{x^{2k}}{2k}\right).$$

K nalezení součtu nekonečné řady se nám vyplatí použít trik: řadu zderivovat, upravit a pak zpátky zintegrovat.

$$\left(\sum_{k=1}^{\infty} \frac{x^{2k}}{2k}\right)' = \sum_{k=1}^{\infty} x^{2k-1} = x \sum_{k=0}^{\infty} x^{2k} = x \cdot \frac{1}{1-x^2} = \frac{x}{1-x^2}$$

Vyšel nám zlomek, jenž je před integrováním třeba upravit na součet parciálních zlomků:

$$\frac{x}{1-x^2} = \frac{A}{1-x} + \frac{B}{1+x} = \frac{A(1+x) + B(1-x)}{1-x^2}.$$

Z porovnání čitatelů plynou rovnice $0 = A + B$ a $1 = A - B$, z čehož vyčteme řešení $A = \frac{1}{2}$ a $B = -\frac{1}{2}$. Parciální zlomky zintegrujeme a máme

$$-\frac{1}{2}\ln(1-x) - \frac{1}{2}\ln(1+x) = \ln\frac{1}{\sqrt{1-x}} + \ln\frac{1}{\sqrt{1+x}} = \ln\sqrt{\frac{1}{1-x^2}}.$$

Tento výraz je stále v exponentu generující funkce $G_S(x)$. Dosaďme jej tedy:

$$G_S(x) = \exp\left(\ln\sqrt{\frac{1}{1-x^2}}\right) = \sqrt{\frac{1}{1-x^2}} = (1-x^2)^{-1/2}.$$

Generující funkci lze nyní rozepsat do mocninné řady použitím zobecněné binomické věty:

$$\begin{aligned}
(1-x^2)^{-1/2} &= \sum_{k=0}^{\infty} \binom{-1/2}{k} (-1)^k x^{2k} \\
&= \sum_{k=0}^{\infty} \frac{(-1/2)(-3/2)\dots(-1/2-k+1)}{k!} (-1)^k x^{2k} \\
&= \sum_{k=0}^{\infty} \frac{1 \cdot 3 \dots (1+2k-2)}{2^k k!} x^{2k} \\
&= \sum_{k=0}^{\infty} \frac{(2k-1)!!}{2^k k!} x^{2k}.
\end{aligned}$$

Nakonec použijeme definici generující funkce a získáme řešení:

$$G_S(x) = \sum_{n=0}^{\infty} g_S(n) \frac{x^n}{n!} = \sum_{k=0}^{\infty} \frac{(2k-1)!!}{2^k k!} x^{2k},$$

$$g_S(2k) = (2k)! \frac{(2k-1)!!}{2^k k!} = ((2k-1)!!)^2.$$

Liché členy tentokrát na pravé straně rovnosti zcela chybí, tedy

$$g_S(2k+1) = 0.$$

Kombinatorické řešení. Je zřejmé, že sudé cykly lze sestavit pouze ze sudého počtu prvků, tedy rovnou můžeme napsat $g_S(2k+1) = 0$ pro $k \in \mathbb{N}_0$.

Cílem je počítat způsoby, jak utvořit cykly sudých délek z $2k$ prvků pro $k \in \mathbb{N}$. Nejdříve prvky spárujme do dvojcyklů – to činí $(2k-1)!!$ možností, jak jsme zjistili v úloze 22. Dvojcykly uspořádáme vzestupně podle jejich menšího prvku, a menší prvky napíšeme na první pozici cyklů. Tomuto uspořádání budeme říkat *vzestupné.* Tímto způsobem lze uspořádat jakoukoliv permutaci.

Pro znázornění vezměme 8 spárovaných prvků ve vzestupném uspořádání:

$$(1,5)(2,3)(4,8)(6,7).$$

Nyní budeme dvojcykly spojovat. Budeme postupovat zleva doprava, a buď navštívený cyklus „rozšíříme“ (připojíme na jeho konec některý z nenavštívených dvojcyklů), nebo jej „uzavřeme“ a pokročíme k následníkovi. Jeden krok algoritmu vlastně vždy znamená zafixování dvou prvků permutace a posun o dvě pozice doprava.

Podívejme se, jak může algoritmus probíhat. Zvýrazněné prvky značí konec navštíveného cyklu.

$$\begin{gathered}(1,\mathbf{5})(2,3)(4,8)(6,7)\\(1,5)(2,\mathbf{3})(4,8)(6,7)\\(1,5)(2,3,7,\mathbf{6})(4,8)\\(1,5)(2,3,7,6,4,\mathbf{8})\\(1,5)(2,3,7,6,4,8)\end{gathered}$$

První cyklus se rovnou uzavřel, další se hned dvakrát rozšířil. Poprvé o cyklus $(6,7)$ s prvním prvkem 7, podruhé o cyklus $(4,8)$ s prvním prvkem 4.

Obecně se dá říci, že volba rozšíření je dána výběrem prvku, jenž se nachází napravo od konce navštíveného cyklu. Počet možností je tak nejdřív $2k-2$, pak $2k-4$, a tak dále, až ke 2 a 0. Navíc máme vždy navíc možnost uzavření, tedy možností spojování je $(2k-1)(2k-3)\dots 3\cdot 1 = (2k-1)!!$.

Zřejmě výsledkem bude permutace sestávající z cyklů sudých délek, zatím ale nevíme, zda každá taková permutace půjde vygenerovat právě jedním způsobem.

Všimněme si, že spojování nenarušilo vzestupné uspořádání. Je díky tomu možné jednoznačně uskutečnit zpětný chod z již pospojovaných cyklů: zprava doleva „trháme“ dvojcykly a řadíme je podle vzestupného uspořádání, což je vždy napravo od navštíveného cyklu.

Zpětný chod je možné provést na každé permutaci s cykly sudých délek, protože jediná podmínka je její vzestupné uspořádání. To znamená, že pokud máme vhodně spárované prvky, je právě jeden způsob, jak provést spojování k získání zadané permutace. A párování prvků je při spojování zachováno (spárované prvky zůstanou vedle sebe), tedy lze je přímo ze zadané permutace vyčíst.

Tedy počet hledaných permutací je roven počtu možností, jak utvořit dvojcykly, krát počet možností, jak je pospojovat do větších cyklů. Získáme

$$g_S(2k) = ((2k-1)!!)^2.$$

Úloha 27. *Kolik existuje permutací nad n-prvkovou množinou, které sestávají právě z cyklů lichých délek?*

Analytické řešení. Nechť L je množina všech kladných lichých čísel. Generující funkcí je $G_L(x)$ a řešením úlohy $g_L(n)$. Věta 21 říká

$$G_L(x) = \exp\left(x + \frac{x^3}{3} + \frac{x^5}{5} + \dots\right) = \exp\left(\sum_{k=0}^{\infty} \frac{x^{2k+1}}{2k+1}\right).$$

Stejně jako u předchozí úlohy 26 použijeme trik se zderivováním a zintegrováním exponentu:

$$\left(\sum_{k=0}^{\infty} \frac{x^{2k+1}}{2k+1}\right)' = \sum_{k=0}^{\infty} x^{2k} = \frac{1}{1-x^2}.$$

Před integrací je potřebná úprava na parciální zlomky:

$$\frac{1}{1-x^2} = \frac{A}{1-x} + \frac{B}{1+x} = \frac{A(1+x)+B(1-x)}{1-x^2}.$$

Z čitatelů vyčteme $1 = A + B$ a $0 = A - B$ a získáme řešení $A = B = \frac{1}{2}$. Po zintegrování zlomků získáme

$$-\frac{1}{2}\ln(1-x) + \frac{1}{2}\ln(1+x) = \ln\frac{1}{\sqrt{1-x}} + \ln\sqrt{1+x} = \ln\sqrt{\frac{1+x}{1-x}}.$$

Vyjádříme $G_L(x)$:

$$G_L(x) = \exp\left(\ln\sqrt{\frac{1+x}{1-x}}\right) = \sqrt{\frac{1+x}{1-x}}.$$

Dále se rozšířením $\sqrt{1+x}$ zbavíme odmocniny v čitateli, jmenovatel poté půjde převést na mocninnou řadu pomocí zobecněné binomické věty.

$$G_L(x) = \frac{\sqrt{1+x}}{\sqrt{1-x}} \cdot \frac{\sqrt{1+x}}{\sqrt{1+x}} = \frac{1+x}{\sqrt{1-x^2}} = (1+x)(1-x^2)^{-1/2}$$

Právě tuto mocninou řadu jsme ale hledali i v předchozí úloze 26, takže ji stačí opsat:

$$G_L(x) = (1+x)\sum_{k=0}^{\infty} \frac{(2k-1)!!}{2^k k!} x^{2k}.$$

Mocninná řada s pouze sudými členy je oproti úloze 26 násobena $(1+x)$, takže i liché členy budou nenulové. Při rozepsání definice generující funkce získáme

$$G_L(x) = \sum_{n=0}^{\infty} g_L(n)\frac{x^n}{n!} = (1+x)\sum_{k=0}^{\infty} \frac{(2k-1)!!}{2^k k!} x^{2k}.$$

Nyní je třeba spočítat $g_L(n)$ separátně pro n liché a n sudé:

$$g_L(2k) = (2k)!\frac{(2k-1)!!}{2^k k!} = ((2k-1)!!)^2,$$

$$g_L(2k+1) = (2k+1)!\frac{(2k-1)!!}{2^k k!} = (2k+1)((2k-1)!!)^2. \tag{3.6}$$

Kombinatorické řešení. Všimněme si, že pro n sudé nám vyšlo řešení totožné s předchozí úlohou 26, tedy $g_L(2k) = g_S(2k)$. Jako kombinatorický postup se nám tedy přímo nabízí dokázat tuto rovnost. Toho docílíme nalezením bijekce mezi permutacemi se všemi cykly lichých délek (zkráceně *vzory*) a permutacemi, které mají všechny cykly sudých délek (zkráceně *obrazy*). Vlastnost bijekce se dokáže tím, že ke každému obrazu půjde jednoznačně najít vzor.

Zobrazení samotné bude jednoduché: nalezneme rozklad vzoru na nezávislé cykly a na konec každého druhého cyklu přesuneme poslední prvek cyklu předchozího. Takto ze všech cyklů lichých délek získáme cykly sudých délek. Zatím to ale není korektní postup: různá uspořádání cyklů a prvků v cyklech vedou k různým obrazům též permutace, takže je třeba určit nějaký jednoznačný předpis, jak zapsat permutaci pomocí rozkladu na cykly.

K předchozímu odstavci je třeba učinit dvě pozorování. Zaprvé počet cyklů lichých délek je vždy sudý, skutečně tedy polovina cyklů prvek ztratí a druhá polovina prvek získá. Zadruhé odebráním prvku z jednocyklu se tohoto cyklu zbavíme, tedy obrazy obecně mohou sestávat z méně cyklů než vzory. Tím vzniká problém s hledáním vzoru k obrazu: obecně u cyklu nevíme, zda byl jeho poslední prvek v zobrazení přidělen z jeho předchůdce nebo ze zaniklého jednocyklu.

Zachrání nás následující uspořádání: na první pozici každého cyklu umístíme jeho největší prvek a cykly samotné uspořádáme vzestupně podle hodnoty onoho největšího prvku. Například permutace

$$(4)(5,1,3)(7)(8)(9,2,6)(10)$$

je ve správném tvaru, jakákoliv jiná podoba je špatně.

Všimněme si, že uspořádání je zachováno i pro všechny obrazy, protože pořadí cyklů se nemění a při každém přesunu vkládáme na konec cyklu číslo menší než to, které je na začátku cyklu. Zánik jednocyklů též uspořádání nenaruší, jen změní celkový počet cyklů obrazu. Můžeme tak uvažovat obrazy pouze uspořádaném tvaru.

Zde je obraz naší permutace z příkladu, též v popsaném uspořádání:

$$(5,1,3,4)(8,7)(9,2)(10,6).$$

Nakonec si uvědomme, že máme-li v daném cyklu v obrazu prvek, o kterém víme, že jej zobrazení přesunulo, pak dokážeme říct, kam ve vzoru patří. Pokud má totiž prvek menší hodnotu než první prvek předchůdce daného cyklu, pak ve vzoru náleží na poslední pozici předchůdce. Pokud je naopak daný prvek větší nebo daný cyklus předchůdce nemá, pak prvek ve vzoru tvořil jednocyklus, který umístíme těsně před daný cyklus.

Právě jsme popsali jeden krok algoritmu rekonstrukce vzoru z daného obrazu. Postupujeme od posledního cyklu dopředu, z navštíveného cyklu odebíráme poslední prvek, a pro další krok přeskakujeme cykly, jimž byl přidán prvek. Takto jednoznačně nalezneme k obrazu vzor.

Proveďme rekonstrukci vzoru s obrazem naší demonstrační permutace:

$$(5,1,3,4)(8,7)(9,2)(10,\mathbf{6})$$
$$(5,1,3,4)(8,\mathbf{7})(9,2,6)(10)$$
$$(5,1,3,\mathbf{4})(7)(8)(9,2,6)(10)$$
$$(4)(5,1,3)(7)(8)(9,2,6)(10).$$

Tučně jsou zobrazeny přesouvané prvky. První krok byl přesun 6 na konec předchůdce, protože $6 < 9$, druhý krok přesun 7 do nového jednocyklu, protože $7 > 5$, a nakonec 4 vytvoří jednocyklus na začátku, protože předchůdce už cyklus nemá. Vidíme, že jsme získali zpět původní vzor, se kterým jsme začínali.

Tímto jsme dokázali

$$g_L(2k) = g_S(2k) = ((2k-1)!!)^2.$$

Jsme ale zatím pouze v polovině řešení – je ještě třeba spočítat $g_L(2k+1)$. Protože $g_S(2k+1) = 0$, tak zde nemá smysl hledat bijekci mezi sudými a lichými cykly. Namísto toho se pokusíme využít výsledek $g_L(2k)$.

Použijeme uspořádání popsané v předešlých odstavcích a ptáme se, kam lze v takto uspořádané permutaci nad $(2k+1)$-prvkovou množinou umístit největší prvek, aby všechny cykly byly lichých délek. Tento prvek bude vždy na první pozici cyklu, který dosahuje až k poslední pozici. Aby tento v pořadí poslední cyklus měl lichou délku, musí i největší prvek být na liché pozici – je tedy $k+1$ možností, kam jej položit. Položme tedy prvek na pozici $2i+1$, kde $0 \leq i \leq k$. Zbylé prvky rozdělme na ty, které napíšeme před obsazenou pozici, a ty, které napíšeme za ni. Rozdělení je možné provést $\binom{2k}{2i}$ způsoby. Prvky na pozicích 1 až $2i$ představují permutaci $2i$-prvkové množiny tvořenou pouze lichými cykly. Víme, že počet takových permutací je $g_L(2i) = ((2i-1)!!)^2$. Prvky na pozicích $2i+2$ až $2k+1$ umisťujeme na druhé až poslední místo posledního cyklu délky $2k+1-2i$, to činí $(2k-2i)!$ možností. Sčítáním přes všechna i získáme sumu

$$g_L(2k+1) = \sum_{i=0}^{k} \binom{2k}{2i} ((2i-1)!!)^2 (2k-2i)!.$$

Máme už výsledek, bylo by ale hezké ještě dokázat, že je skutečně totožný se vzorcem (3.6) z analytického postupu. Jako první krok vytkneme ze sumy činitel $(2k-1)!!$:

$$\begin{aligned}
g_L(2k+1) &= \sum_{i=0}^{k} \binom{2k}{2i} (2k-2i)!((2i-1)!!)^2 \\
&= \sum_{i=0}^{k} \frac{(2k)!}{(2k-2i)!(2i)!} (2k-2i)!((2i-1)!!)^2 \\
&= \sum_{i=0}^{k} \frac{(2k)!!(2k-1)!!}{(2i)!} ((2i-1)!!)^2 \\
&= (2k-1)!! \sum_{i=0}^{k} \frac{(2k)!!}{(2i)!!} (2i-1)!!.
\end{aligned}$$

Tvrzení, že nová suma má součet $(2k+1)!!$, dokážeme indukcí. Pro $k = 1$

vyjde suma $2 + 1 = 3 = 3!!$. A nyní indukční krok, známe-li výsledek pro $k - 1$:

$$\begin{aligned}
\sum_{i=0}^{k} \frac{(2k)!!}{(2i)!!}(2i-1)!! &= \sum_{i=0}^{k-1} \left(\frac{(2k)!!}{(2i)!!}(2i-1)!! \right) + (2k-1)!! \\
&= (2k) \sum_{i=0}^{k-1} \left(\frac{(2k-2)!!}{(2i)!!}(2i-1)!! \right) + (2k-1)!! \\
&= (2k)(2k-1)!! + (2k-1)!! \\
&= (2k+1)(2k-1)!! \\
&= (2k+1)!!.
\end{aligned}$$

I kombinatorickou cestou jsme tedy získali výsledek

$$g_L(2k+1) = (2k+1)!!(2k-1)!! = (2k+1)((2k-1)!!)^2.$$

Úloha 28. *Mějme vybrané číslo $k \in \mathbb{N}$. Kolik existuje permutací nad n-prvkovou množinou, které sestávají pouze z cyklů, jejichž délky jsou násobky čísla k?*

Analytické řešení. Exponenciální generující funkci $G_C(x)$ rozepíšeme podle věty 21:

$$G_C(x) = \exp\left(\sum_{n=1}^{\infty} \frac{x^{kn}}{kn} \right) = \exp\left(\frac{x^k}{k} + \frac{x^{2k}}{2k} + \frac{x^{3k}}{3k} + \dots \right).$$

K nalezení součtu mocninné řady v exponentu použijeme vzorec (3.5) pro rozvoj logaritmu:

$$\begin{aligned}
-\ln(1-x) &= x + \frac{x^2}{2} + \frac{x^3}{3} + \dots \\
-\ln(1-x^k) &= x^k + \frac{(x^k)^2}{2} + \frac{(x^k)^3}{3} + \dots = x^k + \frac{x^{2k}}{2} + \frac{x^{3k}}{3} + \dots \\
\frac{-\ln(1-x^k)}{k} &= \frac{x^k}{k} + \frac{x^{2k}}{2k} + \frac{x^{3k}}{3k} + \dots = \sum_{n=1}^{\infty} \frac{x^{kn}}{kn}.
\end{aligned}$$

Nalezený logaritmus dosadíme do exponenciály:

$$G_C(x) = \exp\left(\frac{-\ln(1-x^k)}{k} \right) = \exp\left(\ln(1-x^k)^{-1/k} \right) = (1-x^k)^{-1/k}.$$

Tento výraz lze rozepsat na mocninnou řadu pomocí zobecněné binomické věty:

$$\begin{aligned}
(1-x^k)^{-1/k} &= \sum_{n=0}^{\infty} \binom{-1/k}{n} (-1)^n x^{kn} \\
&= \sum_{n=0}^{\infty} \frac{(-1/k)(-1-1/k)\dots(-n+1-1/k)}{n!} (-1)^n x^{kn} \\
&= \sum_{n=0}^{\infty} \frac{(1/k)(1+1/k)\dots(n-1+1/k)}{n!} x^{kn} \\
&= \sum_{n=0}^{\infty} \frac{(1)(k+1)\dots((n-1)k+1)}{k^n n!} x^{kn} \\
&= \sum_{n=0}^{\infty} \frac{x^{kn}}{(kn)!} \frac{(kn)!(k+1)\dots((n-1)k+1)}{k^n n!}.
\end{aligned}$$

Takto je $G_C(x)$ již ve tvaru, že z ní lze podle její definice přímo vyčíst výsledek:

$$g_C(kn) = \frac{(kn)!(k+1)(2k+1)\ldots((n-2)k+1)((n-1)k+1)}{k^n n!}.$$

Pokud m není násobkem k, pak z generující funkce plyne, že $g_C(m) = 0$, což je zřejmé i z kombinatorického pohledu.

Kombinatorické řešení. Okopírujeme řešení úlohy 26 s jedinou změnou, že prvky budeme seskupovat do cyklů délky k namísto párovat do dvojcyklů. Princip řešení jinak zůstává nenarušen, tedy počet hledaných permutací bude opět roven počtu možností, jak prvky seskupit, krát počet možností, jak je ve vzestupném uspořádání spojovat. Stačí tedy vyjádřit tyto dvě hodnoty.

Mějme nk prvků, ty lze zpermutovat $(kn)!$ způsoby. Pak je stačí rozdělit do n skupin o délkách k, což z nich učiní cykly délek k. Ke stejným cyklům lze ale přijít různými způsoby. Protože nezáleží na pořadí cyklů, vydělíme $n!$, a protože nezáleží na cyklickém posunu v jednotlivých skupinách, vydělíme k pro každý cyklus. Získáme $\frac{(kn)!}{k^n n!}$ možností.

Přejděme nyní ke spojování těchto cyklů – ty uvažujme ve vzestupném uspořádání. V prvním kroku můžeme první cyklus uzavřít, nebo jej rozšířit o jeden z $n-1$ následujících cyklů. Při rozšíření o vybraný cyklus dále záleží na tom, který z k prvků bude na konec navštíveného cyklu zapsán jako první. Tedy pro první krok máme $(n-1)k+1$ možností. Druhý krok bude $(n-2)k+1$ možností, třetí $(n-3)k+1$ možností, až nakonec pro k-tý krok zbývá jediná možnost uzavření. Spojování cyklů lze tedy provést $((n-1)k+1)((n-2)k+1)\ldots(k+1)1$ způsoby a řešením úlohy pro $n \in \mathbb{N}$ je

$$g_C(kn) = \frac{(kn)!}{k^n n!}((n-1)k+1)((n-2)k+1)\ldots(k+1).$$

Úloha 29. *Mějme vybrané číslo $k \in \mathbb{N}$. Kolik existuje permutací nad n-prvkovou množinou, které sestávají pouze z cyklů, jejichž délky nejsou násobky čísla k?*

Analytické řešení. Pomocí věty 18 rozepíšeme příslušnou exponenciální generující funkci:

$$G_C(x) = \exp\left(\sum_{n=1}^{\infty} \frac{x^n}{n} - \sum_{n=0}^{\infty} \frac{x^{kn}}{kn}\right).$$

Zápis obou těchto řad přes logaritmy je zmíněn v předchozí úloze 28, tedy logaritmy rovnou opíšeme a následně upravíme:

$$\begin{aligned}
G_C(x) &= \exp\left(-\ln(1-x) + \frac{\ln(1-x^k)}{k}\right) \\
&= \exp\left(\ln\frac{1}{1-x} + \ln(1-x^k)^{1/k}\right) \\
&= \exp\left(\ln\frac{(1-x^k)^{1/k}}{1-x}\right) \\
&= \frac{(1-x^k)^{1/k}}{1-x}.
\end{aligned}$$

Chceme použít binomickou větu, potřebovali bychom se ale zbavit jmenovatele. Šikovným rozšířením zlomku získáme výhodnější tvar:

$$\frac{(1-x^k)^{1/k}}{1-x} \cdot \frac{1+x+\cdots+x^{k-1}}{1+x+\cdots+x^{k-1}} = \frac{(1-x^k)^{1/k}}{1-x^k}(1+x+\cdots+x^{k-1}).$$

Zlomek pak lze zapsat jako $(1-x^k)^{1/k-1} = (1-x^k)^{(1-k)/k}$, což už umíme upravit přes binomickou větu:

$$\begin{aligned}
(1-x^k)^{(1-k)/k} &= \sum_{n=0}^{\infty} (-1)^n x^{kn} \binom{\frac{1-k}{k}}{n} \\
&= \sum_{n=0}^{\infty} (-1)^n x^{kn} \frac{1}{n!} \cdot \frac{1-k}{k} \cdot \frac{1-2k}{k} \cdots \frac{1-nk}{k} \\
&= \sum_{n=0}^{\infty} x^{kn} \frac{1}{n!} \cdot \frac{k-1}{k} \cdot \frac{2k-1}{k} \cdots \frac{nk-1}{k} \\
&= \sum_{n=0}^{\infty} x^{kn} \frac{k-1}{k} \cdot \frac{2k-1}{2k} \cdots \frac{nk-1}{nk}.
\end{aligned}$$

Generující funkce $G_C(x)$ je tato mocninná řada násobená $(1+x+\cdots+x^{k-1})$. Chceme-li dostat mocninu x^{kn+j}, kde $j \in \{0,1,\ldots,k-1\}$, pak je zřejmé, že z této závorky musíme vzít člen s x^j a z výše uvedené řady vezmeme člen s x^{kn}.

Řešení $g_C(kn+j)$ je však dle definice generující funkce koeficient u $\frac{x^{kn+j}}{(kn+j)!}$, tedy je to koeficient příslušného členu sumy násobený $(kn+j)!$.

$$g_C(kn+j) = (kn+j)! \frac{k-1}{k} \cdot \frac{2k-1}{2k} \cdots \frac{nk-1}{nk} \tag{3.7}$$

Kombinatorické řešení. Zde jej provádět nebudeme, citujme ale alespoň článek [8], v němž je kombinatorické řešení uvedeno v plném rozsahu. Řešení ze článku má však následující tvar, který na první pohled není totožný s naším analytickým řešením (3.7):

$$g_C(kn+j) = \prod_{i=1}^{kn+j} (i - \theta_k(i)),$$

kde

$$\theta_k(i) = \begin{cases} 1 & \text{pokud } k \text{ dělí } i, \\ 0 & \text{jinak.} \end{cases}$$

Tedy laicky řečeno se jedná o $(kn+j)!$, kde každý činitel dělitelný k je nahrazen členem o 1 menším. Právě tak lze ovšem popsat i náš vzorec (3.7), tedy jedná se o dva různé zápisy téhož výsledku.

V této kapitole jsme na několika úlohách ukázali dva rozdílné postupy řešení: analytický, pracující s mocninnými řadami a generujícími funkcemi, a kombinatorický, kreativní a více nevyzpytatelný. Čtenář si může zvolit, který postup je mu bližší.

Literatura

[1] Wikipedia. *Telephone number (mathematics).* Navštíveno 1.9.2023. Dostupné z: `https://en.wikipedia.org/wiki/Telephone_number_(mathematics)`

[2] Wikipedia. *Involution (mathematics).* Navštíveno 1.9.2023. Dostupné z: `https://en.wikipedia.org/wiki/Involution_(mathematics)`

[3] Wikipedia. *Double factorial.* Navštíveno 1.9.2023. Dostupné z: `https://en.wikipedia.org/wiki/Double_factorial`

[4] R. Šámal. *Burnsideovo lemma aneb kterak náhrdelníky spočítati.* Matematický korespondenční seminář, 1998. Dostupné z: `https://prase.cz/library/BurnsideovoLemmaRS/BurnsideovoLemmaRS.pdf`

[5] D. F. Holt. Rooks Inviolate. *The Mathematical Gazette* 58 (1974), 131–134.

[6] J. Arndt. *Matters Computational: Ideas, Algorithms, Source Code.* Berlin: Springer, 2010. ISBN 978-3-642-14764-7.

[7] M. Bóna. *Combinatorics of Permutations.* Boca Raton: CRC Press, 2012. ISBN 978-1-4398-5052-7.

[8] E. A. Bertram a B. Gordon. Counting Special Permutations. *European Journal of Combinatorics* 10 (1989), 221–226.