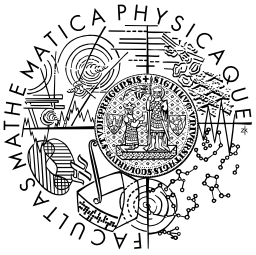


MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Vojtěch Sekera

Permutační grupy a míchání karet

Katedra algebry

Vedoucí bakalářské práce: doc. RNDr. Jan Šťovíček, Ph.D.

Studijní program: Matematika

Studijní obor: Obecná matematika

Praha 2023

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

Za motivaci a podporu během studia a psaní práce vděčím Adéle Brucknerové a Martinu Šochmanovi. Také děkuji vedoucímu práce docentovi RNDr. Janu Štovíčkovi, Ph.D. za trpělivý přístup a rychlé reakce.

Název práce: Permutační grupy a míchání karet

Autor: Vojtěch Sekera

Katedra algebry: Katedra algebry

Vedoucí bakalářské práce: doc. RNDr. Jan Šťovíček, Ph.D., Katedra algebry

Abstrakt: V této bakalářské práci vyřešíme starý problém, pojmenovaný po kouzelníkovi a matematikovi Alexi Elmsleym, spočívající ve vynesení libovolné karty navrch balíčku užitím tzv. „faro shuffle“. Dále odhalíme strukturu tímto míchání generované permutační grupy pro libovolně veliký balíček karet. A ve třetí kapitole faro shuffle zobecníme, načež dojdeme ke slibné domněnce popisující jeho permutační grupu.

Klíčová slova: permutační grupa, míchání karet, faro shuffle

Title: Permutation groups and card shuffling

Author: Vojtěch Sekera

Department of Algebra: Name of the department

Supervisor: doc. RNDr. Jan Šťovíček, Ph.D., Department of Algebra

Abstract: In this thesis we solve an old problem, named after the magician and mathematician Alex Elmsley, of raising a card to the top of the deck using faro shuffles. Furthermore we examine the group structure generated by these shuffles on an arbitrarily large deck of cards. Upon generalizing the faro shuffle in the third chapter, we reach a promising conjecture about these faro shuffle permutation groups.

Keywords: permutation group, card shuffling, faro shuffle

Obsah

Úvod

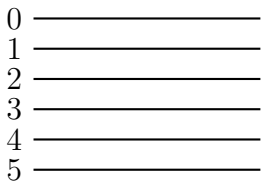
Umění každého kouzelníka s kartami je kontrola nad tím, kde v balíčku se důležité karty nacházejí. Kouzlo často spočívá v tom, že míchání karet připadají divákovi zcela náhodná a nekontrolovatelná. Nejlepším příkladem je tzv. „faro shuffle“, kdy se balíček rozdělí na dvě poloviny, ty se k sobě přiloží kratší hranou téměř rovnoběžně a tlakem a opatrnou manipulací se nechají prolnout v jednu hromádku. V ideálním případě budou karty alternovat. O nesnadnosti tohoto míchání psal kouzelník Alex Elmsley, doporučoval obrousit hrany karet, aby se nezadrhávaly, a radil, jak rychle opravit špatné zamíchání – těžké je už rozdělit balíček přesně napůl. Také díky němu se ustálily názvy „out shuffle“ a „in shuffle“. [Min94]

Cílem této práce je vyzkoumat vlastnosti těchto zamíchání a jimi generovaných grup; jak jimi přemisťovat karty na libovolné pozice za použití co nejmenšího počtu zamíchání, čemu jsou přesně grupy izomorfní a nakonec jak se tyto vlastnosti změní pro zobecněné faro shuffle.

1. První karta

1.1 Definice zamíchání

V celé kapitole značí $2n$ velikost balíčku karet a ty číslujeme od 0 (vrchní karta) po $2n-1$ (spodní karta). Permutace se skládají zleva doprava.



Obrázek 1.1: Balíček šesti karet, $2n = 6$.

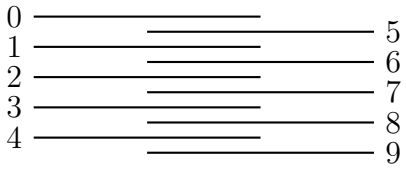
Mějme balíček s $2n$ kartami. Rozdělíme jej na vrchní a spodní polovinu. Nyní bereme karty střídavě zespod těchto balíčků a pokládáme je na výslednou hromádku, dokud balíčky nevyprázdníme. Takovéto zamíchání nazýváme *perfektní*. Pokud jsme první kartu odebrali ze spodního balíčku, jedná se o out shuffle, v opačném případě o in shuffle. Tím způsobem se bezpečně vykoná „faro shuffle".

Definice 1. *Pro balíček o $2n$ kartách definujeme permutace* out shuffle*, resp.* in shuffle *následovně:*

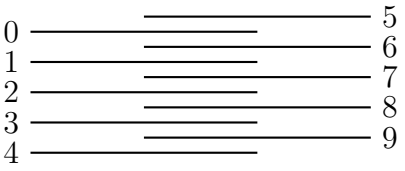
$$O(i) = \begin{cases} 2i \pmod{2n-1}, & 0 \leq i < 2n-1, \\ 2n-1, & i = 2n-1, \end{cases}$$

$$I(i) = 2i + 1 \pmod{2n+1}, \quad 0 \leq i \leq 2n-1.$$

Názýváme je perfektní zamíchání *a pro jimi generovanou grupu $\langle O, I \rangle$ můžeme užívat název* grupa perfektních zamíchání*. Vizte obr. 1.2 a 1.3.*



Obrázek 1.2: Out shuffle



Obrázek 1.3: In shuffle

První matematická otázka by mohla znít: Po kolika zamícháních se balíček vrátí do původního pořadí? Např. v balíčku o deseti kartách stačí šest out shuffle, pro 16 karet jen čtyři out shuffle a pro 26 karet je třeba 20 out shuffle. Číslo neroste nutně s velikostí balíčku, všimněme si, že po k zamícháních se karta $i < 2n-1$ přesune na pozici $2^k i$, hledané číslo je tedy řád 2 (mod $2n-1$). Ten je sice omezen díky Eulerově větě, $2^{\varphi(2n-1)} \equiv 1 \pmod{2n-1}$, což znamená v nejhorším případě $2n-2$. Zda ale toto nastane pro libovolně velké n, je otázka stále otevřená, jmenovitě Artinova domněnka o primitivních kořenech. [Dia06] Pomineme-li vrchní a spodní kartu, permutace odpovídá in shuffle v menším balíčku, tudíž má in shuffle řád jako out shuffle v balíčku o dvě karty větším.

1.2 Elmsleyho problém

Elmsley se věnoval kartám už od dětství, ale také vystudoval matematiku na Cambridge University. Neuniklo by mu, že pokud chce přemístit vrchní kartu na pozici p, stačí p vyjádřit ve dvojkové soustavě a, čteno zleva doprava, za nulu aplikovat out shuffle a za jedničku in shuffle, vše nezávisle na velikosti balíčku. Tedy např. $p = 11 = 1011_2$, zamícháme karty – in shuffle, out, in a in – a původně vrchní karta skončí na pozici 11.

Tvrzení 1. *Permutace vzniklá záměnou nul a jedniček za O a I v binárním zápisu čísla $p < 2n$ přesune vrchní kartu na pozici p.*

Důkaz. Nechť $p = \sum_{i=0}^{k} p_i 2^i$. Jedná se o Hornerovo schéma pro převod do desítkové soustavy:

$$p = 2(2(\ldots 2(2(2 \cdot 0 + p_k) + p_{k-1})) \cdots + p_1) + p_0.$$

□

Přirozeně vyvstala otázka: Jak naopak přesunout kartu p na vrch balíčku? Elmsley v červnu roku 1957 píše do britského kouzelnického časopisu *Pentagram*: „Zatím se mi nepodařilo objevit relativně jednoduchý způsob, jak vynést kartu na vrch balíčku, který by měl jiný počet karet než 2^k. Jediný způsob, který jsem našel, je příliš komplikovaný pro praktické použití.“ Tento problém se proslavil jako Elmsleyho problém a v uplynulých 50 letech se jím zabývali kouzelníci i rekreační matematici. Byly vydávány speciální tabulky, které uváděly nejkratší sekvence pro různé velikosti balíčků. Dokonce se prodávaly počítačové programy, které tuto úlohu řešily. Persi Diaconis a Ron Graham se při sepisování zde citovaného řešení v roce 2006 dozvěděli o Elmsleyově smrti a článek věnovali jeho památce. [DG07]

Demonstrujme řešení: opět se používá dvojková soustava, tentokrát je ale potřeba mezivýpočet. Pro balíček $2n$ karet definujme r tak, že $2^{r-1} < 2n \leq 2^r$. Například pro $2n = 52$ máme $r = 6$ a zvolme třeba $p = 12$. Spočítáme dvě čísla, převedeme je do dvojkové soustavy a doplníme nuly na délku r:

$$b = \lceil p2^r/2n \rceil = \lceil 12 \cdot 64/52 \rceil = 15 = 001111_2,$$
$$x = 2nb - 2^r p = 780 - 768 = 12 = 001100_2.$$

Na ně aplikujeme bitový XOR, $01111_2 \oplus 001100_2 = 000011_2$, a toto číslo (zleva doprava) už udává hledanou sekvenci, neboli $pOOOOII = 0$.

1.2.1 Konstrukce řešení

Tentokrát by bylo nemožné pracovat s moduly, klíčové je převedení problému na přemístění karty 0 na pozici p pomocí inverzních permutací. Jejich předpis se dá odpozorovat nejlépe z obrázků pod definicí permutací, 1.2 a 1.3, a lze ověřit výpočtem OO^{-1} a II^{-1}.

$$O^{-1}(i) = \begin{cases} \lfloor i/2 \rfloor, & \text{je-li } i \text{ sudé,} \\ \lfloor i/2 \rfloor + n, & \text{je-li } i \text{ liché.} \end{cases}$$

$$I^{-1}(i) = \begin{cases} \lfloor i/2 \rfloor + n, & \text{je-li } i \text{ sudé,} \\ \lfloor i/2 \rfloor, & \text{je-li } i \text{ liché.} \end{cases}$$

LEMMA 2. $\lfloor \lfloor x \rfloor / 2 \rfloor = \lfloor x/2 \rfloor$.

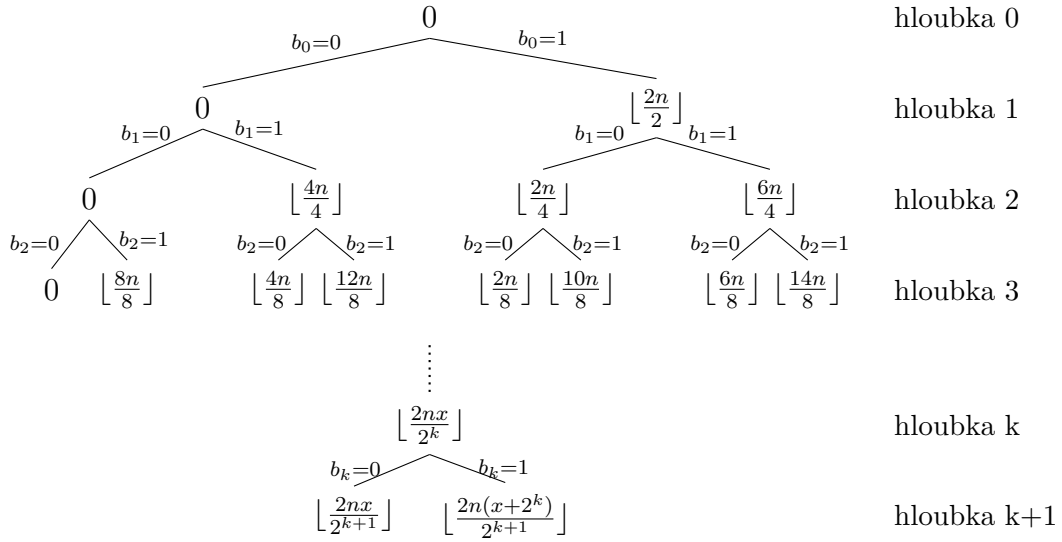
Důkaz. $x = \lfloor x \rfloor + \varepsilon$ pro nějaké $\varepsilon \in [0, 1)$. Dále $\lfloor x \rfloor / 2$ se buďto rovná m nebo $m + 1/2$ pro nějaké $m \in \mathbb{Z}$, tudíž v obou případech máme

$$\frac{\lfloor x \rfloor}{2} \;\le\; \frac{x}{2} = \frac{\lfloor x \rfloor}{2} + \frac{\varepsilon}{2} \;<\; \frac{\lfloor x \rfloor}{2} + \frac{1}{2} \;\le\; m + 1.$$

□

Permutací O^{-1} nebo I^{-1} můžeme díky jejich podobnosti zobrazit $\lfloor x \rfloor$ na $\lfloor \lfloor x \rfloor / 2 \rfloor + bn = \lfloor x/2 + bn \rfloor$ pro $b \in \{0, 1\}$ libovolné, pokud známe paritu $\lfloor x \rfloor$.

Pro naše účely zkonstruujeme binární strom T hloubky r, obr. 1.4, kde $2^{r-1} < 2n \le 2^r$. Hodnotou jeho kořene je číslo 0 a každý vrchol, mající hodnotu x, ústí ve dva potomky: hodnota levého odpovídá obrazu x s volbou $b = 0$ a u pravého obrazu x s volbou $b = 1$. Pro hloubku k značíme dané volby b_k.



Obrázek 1.4: Strom T

Zvolme cestu od kořene dolů až do hloubky r, cesta odpovídá volbám $b_0, b_1, \ldots, b_{r-1}$, a označme $b(k) = \sum_{i=0}^{k-1} b_i 2^i$ a $b = \sum_{i=0}^{r-1} b_i 2^i$. Dále

$$\left\lfloor \frac{2nb}{2^k} \right\rfloor = \left\lfloor \frac{2n}{2^k} \left(\sum_{i<k} b_i 2^i + \sum_{i \ge k} b_i 2^i \right) \right\rfloor = \left\lfloor \frac{2n}{2^k} (b(k) + 2^k M) \right\rfloor = 2nM + \left\lfloor \frac{2nb(k)}{2^k} \right\rfloor \quad (1.1)$$

pro nějaké $M \in \mathbb{Z}$, tudíž parita tohoto výrazu je stejná jako parita $\lfloor 2nb(k)/2^k \rfloor$. Zapíšeme-li ještě $2nb$ ve dvojkové soustavě $2nb = (\ldots, x_1, x_0)$, vidíme, že parita výrazu (1.1) je také rovna x_k. Je-li $\lfloor 2nb(k)/2^k \rfloor$ sudé, odpovídá krok $b_k = 0$ permutaci O^{-1} a $b_k = 1$ permutaci I^{-1}, je-li liché, obráceně.

Nyní je naším úkolem najít cestu do pozice p, neboli takovou, aby $\lfloor 2nb/2^r \rfloor = p$, neboli

$$\begin{aligned} p \leq \frac{2nb}{2^r} &< p+1 \\ \frac{p2^r}{2n} \leq b &< \frac{(p+1)2^r}{2n} \end{aligned} \tag{1.2}$$

Díky výběru r platí $1 \leq 2^r/2n < 2$, a tak existuje jedno až dvě celá čísla b splňující nerovnost. Položme $b = \lceil p2^r/2n \rceil$. Nakonec pomocí parity $\lfloor 2nb(k)/2^k \rfloor$ určíme finální posloupnost permutací. $0 \leq 2nb - 2^r p < 2^r$, a tak $x = 2nb - 2^r p = (x_{r-1}, \ldots, x_1, x_0)$. Toto x koriguje, aby nula odpovídala O^{-1} a jednička I^{-1}, neboť x_k odpovídá paritě hodnoty daného uzlu v hloubce k. Pro $b = (b_{r-1}, \ldots, b_1, b_0)$ posloupnost $b_0 + x_0 \pmod 2, b_1 + x_1 \pmod 2, \ldots, b_{r-1} + x_{r-1} \pmod 2$ udává inverz hledané permutace.

Věta 3. [†] *Mějme balíček velikosti $2n$, pozici p, $0 \leq p < 2n$, a číslo r takové, že $2^{r-1} < 2n \leq 2^r$, dále označme $b = \lceil p2^r/2n \rceil$ a $x = 2nb - 2^r p$. Potom permutace získaná z $(b)_2 \oplus (x)_2$ doplněním nul na r cifer a přepsáním nul na permutaci O a jedniček na permutaci I přemisťuje kartu p na pozici 0.*

Poznámka. Tímto jsme dokázali, že přemístit kartu na vrch balíčku vyžaduje nanejvýš r zamíchání a méně právě v případě, kdy vypočítaná sekvence končí nulami, ty lze umazat, protože out shuffle vrchní kartu nechává na místě. Navíc získáváme nejmenší nutný počet zamíchání pro konkrétní p; pokud případně dvě b splňují (1.2) v důkazu, je nutné porovnat sekvence pro obě možnosti, tedy $b = \lceil p2^r/2n \rceil$ a $b = \lceil p2^r/2n \rceil + 1$. Například při $2n = 26$, $p = 8$ se nabízí $b = 10$ nebo $b = 11$, která vedou k sekvencím $OIII$ a $IOIOI$.

Poznámka. Algoritmus lze upravit k nalezení sekvence zamíchání pro přesun karty z pozice q na p. Postačí strom sestavit s kořenem o hodnotě q, výpočty jsou analogické, $b = \lceil \frac{p2^r - q}{2n} \rceil$ a $x = 2nb + q - 2^r p$.

[†] Oproti zdroji byla opravena chyba v důkazu vedoucí k jinému výsledku, pro příklad v úvodu problému by věta neplatila.

2. Řád grupy zamíchání

Persiho Diaconise nemůžeme považovat jen za uznávaného profesora, který na chvíli zavadil o magii. Začal s ní od brzkého věku: v pěti letech četl svou první knihu o kouzlech a ty rázem předváděl. Ve 13 letech narazil na Alexe Elmsleyho v kouzelnickém obchodě, který mu ukázal, jak osm perfektních zamíchání vrátí balíček do původního uspořádání a jak přemístit vrchní kartu na libovolnou pozici. O rok později byl Diaconis pozván iluzionistou Dai Vernonem do Delwaru, aby s ním konal kouzelnická vystoupení. Nakonec to znamenalo, že Diaconis utekl z domova a strávil deset let života na cestách. [Hof11]

Podobně Ron Graham se věnoval žonglování a s ním spojené matematice, oboje na profesionální úrovni. V roce 1972 byl zvolen prezidentem v *International Jugglers' Association*. [Cai99] Tito dva matematici společně napsali např. *Magical Mathematics: The Mathematical Ideas That Animate Great Magic Tricks* [DG12], kde odhadovali, že méně než sto lidí na světě zvládne provést osm bezchybných perfektních zamíchání za minutu. [CW23]

V této kapitole vyřešíme otázku: Do kolika konfigurací lze balíček perfektními zamícháními dostat? která nás nutí vyzkoumat strukturu grupy $\langle I, O\rangle$ jako takové. Toto řešení objevili Diaconis, Graham a Kantor [DGK83].

Věta 4. *Označme D_n Coxeterovu grupu znaménkových permutačních matic řádu n (bude zadefinována později).*

(a) *Pokud $n = 6$, je $\langle I, O\rangle$ izomorfní semidirektnímu součinu S_5 a $\mathbb{Z}_2^6$,*

(b) *pokud $n = 12$, je $\langle I, O\rangle$ izomorfní semidirektnímu součinu Mathiovy M_{12} a $\mathbb{Z}_2^{11}$ a má řád $95040 \cdot 2^{11}$*

(c) *pokud $2n = 2^k$, je $\langle I, O\rangle$ izomorfní semidirektnímu součinu $\mathbb{Z}_k$ a $\mathbb{Z}_2^k$.*

A v ostatních případech:

(d) *Pokud $n \equiv 0 \pmod 4$, je $\langle I, O\rangle$ izomorfní podgrupě matic D_n takových, že jejich příslušné permutace jsou sudé a součin znamének roven 1, a má řád $n!2^{n-2}$.*

(e) *Pokud $n \equiv 1 \pmod 4$, je $\langle I, O\rangle$ izomorfní podgrupě matic D_n takových, že jejich příslušné permutace jsou sudé, a má řád $n!2^{n-1}$.*

(f) *Pokud $n \equiv 2 \pmod 4$, je $\langle I, O\rangle$ izomorfní D_n řádu $n!2^n$.*

(g) *Pokud $n \equiv 3 \pmod 4$, je $\langle I, O\rangle$ izomorfní podgrupě matic D_n s determinantem rovným 1 a má řád $n!2^{n-1}$.*

Lemma 5. *Řád grupy $\langle I\rangle$ je roven řádu prvku $2 \pmod{2n+1}$ a řád $\langle O\rangle$ roven řádu prvku $2 \pmod{2n-1}$.*

Důkaz. Vizte komentář pod definicí 1. □

Lemma 6. *Řád grupy $\langle I, O\rangle$ je alespoň $2n \times$ řád $2 \pmod{2n-1}$.*

Důkaz. Označme π_k permutaci, která přesune vrchní kartu na pozici k. Potom $O^p\pi_k \neq O^q\pi_l$, pokud $p \neq q$ jsou nanejvýš řád O a $k \neq l$, jelikož $(O^p\pi_k)(0) = k$ a $(O^q\pi_l)(0) = l$. Předpokládejme, že $O^p\pi_k = O^q\pi_k$, potom $O^{p-q} = \mathrm{id}$, spor. □

LEMMA 7. *Nechť $2n = 2^k$. Potom je $\langle I, O\rangle$ izomorfní semidirektnímu součinu $\mathbb{Z}_2^k$ a $\mathbb{Z}_k$, kde generátor grupy $\mathbb{Z}_k$ působí na k-tici $x \in \mathbb{Z}_2^k$ jako cyklický posun $x = (x_{k-1}, \ldots, x_0) \mapsto (x_{k-2}, \ldots, x_0, x_{k-1})$.*

Důkaz. Pozice karet zapíšeme pomocí binárního čísla, $x = (x_{k-1}, \ldots, x_0)$. Potom můžeme O, I zapsat následovně:

$$\begin{aligned} O &: (x_{k-1}, \ldots, x_0) \mapsto (x_{k-2}, \ldots, x_0, x_{k-1}),\\ I &: (x_{k-1}, \ldots, x_0) \mapsto (x_{k-2}, \ldots, x_0, \overline{x}_{k-1}), \qquad \text{kde} \quad \overline{x}_j = 1 - x_j, \end{aligned}$$

což vyplývá z výpočtu

$$\begin{aligned} 2x &= \sum_{i<k-1} 2^{i+1}x_i + 2^k x_{k-1} \equiv \sum_{i<k-1} 2^{i+1}x_i + x_{k-1} \pmod{2n-1},\\ 2x+1 &= \sum_{i<k-1} 2^{i+1}x_i + 2^k x_{k-1} + 1 \equiv \sum_{i<k-1} 2^{i+1}x_i + 1 - x_{k-1} \pmod{2n+1}. \end{aligned}$$

Všimněme si, že $B_j = O^{-j-1}IO^j$ posílá prvek $(x_{k-1}, \ldots, x_j, \ldots, x_0)$ na $(x_{k-1}, \ldots, \overline{x}_j, \ldots, x_0)$, takže je $B = \langle B_0, \ldots, B_{k-1}\rangle$ komutativní a také izomorfní grupě $\mathbb{Z}_2^k$.

Nyní ověříme podmínky pro semidirektní rozklad. Součin $\langle O\rangle B$ obsahuje $I = OB_0$, ze zápisu vidíme $\langle O\rangle B = \langle I, O\rangle$ a průnik B a $\langle O\rangle$ je zřejmě triviální. Pro libovolné B_j platí $O^{-1}B_jO = B_{j+1}$, to znamená normalitu $B \trianglelefteq \langle I, O\rangle$. Celkem $\langle I, O\rangle \cong B \rtimes \langle O\rangle \cong \mathbb{Z}_2^k \rtimes \mathbb{Z}_k$. □

DEFINICE 2. *Pro nezáporná celá čísla $a < b$ definujeme diskrétní interval $[a,b) = \{n \in \mathbb{Z} |\ a \leq n < b\}$. O permutaci $g \in S_{2n}$ řekneme, že je středově souměrná, pokud $g(i) + g(2n-1-i) = 2n-1$ pro každé $i \in [0, n)$. Podgrupu všech středově souměrných permutací značíme C_n. Pro popis takové permutace stačí její chování na prvcích $0 \leq i < n$, označme tedy permutované objekty $0, 1, \ldots, n-1, (n-1)'$, $\ldots, 1', 0' = 2n-1$ a takto značme sdružený pár $\overline{x} = \{x, x'\}$. Bavíme-li se o prvku $\overline{x}$ bez určení x, myslíme tím zápis s volbou menšího x. Potom pro $g \in C_n$ sdružení indukuje permutaci $\overline{g}$, $\overline{g}(\overline{i}) = \overline{g(i)}$, která permutuje sdružené páry mezi sebou.*

POZNÁMKA. Zobrazení $g \mapsto \overline{g}$ je homomorfismus z C_n do S_n a jeho jádro $\langle (0\ 0'), (1\ 1'), \ldots, (n-1, (n-1)')\rangle$ je izomorfní $\mathbb{Z}_2^n$.

Tyty pojmy zavádíme, abychom využili centrální symetrie permutací O a I, neboť pro každé $i \in [0, n)$ platí

$$\begin{aligned} O(i) + O(2n-1-i) &= 2i + 2(2n-1-i) - (2n-1) = 2n-1,\\ I(i) + I(2n-1-i) &= 2i + 1 + 2(2n-1-i) + 1 - (2n+1) = 2n-1, \end{aligned}$$

a tak $\langle I, O\rangle \leq C_n$, potom dále definované grupy usnadní výpočet řádu $\langle I, O\rangle$.

DEFINICE 3. *Pro zobrazení $g \mapsto \overline{g}$ z $G = \langle I, O\rangle$ do S_n značíme jeho homomorfní obraz $\overline{G}$ a jádro homomorfismu K. Dále pro znaménko permutace sgn značíme $\overline{sgn}(g) = sgn(\overline{g})$.*

C_n je ve skutečnosti izomorfní Coxeterově grupě typu $D_n = C_n$, pro naše účely se jedná o grupu permutačních matic s navíc přidaným znaménkem, tedy

$$\left\langle \left\{ (a_{j,k}) \mid a_{\pi(i),i} = \pm 1 \text{ pro } 0 \le i < n \text{ a } \pi \in S_n, \text{ jinak } a_{j,k} = 0 \right\} \right\rangle.$$

Izomorfismus δ je následující: Nechť $\pi \in C_n$, pro $\overline{\pi}$ uvažujme příslušnou permutační matici $(a_{j,k})$ velikosti $n \times n$, ale pokud $\pi(i) \ge n$, $i < n$, nahradíme prvek $a_{\overline{\pi}(i),i}$ za -1.

LEMMA 8. *Mějme* $sgn, \overline{sgn} : S_{2n} \to \{-1, 1\}$. *Potom*

(a) *pokud* $n \equiv 0 \pmod 4$, *pak je* G *obsaženo v jádru sgn i* $\overline{sgn}$,

(b) *pokud* $n \equiv 1 \pmod 4$, *pak je* G *obsaženo v jádru* $\overline{sgn}$,

(c) *pokud* $n \equiv 3 \pmod 4$, *pak je* G *obsaženo v jádru* $sgn \cdot \overline{sgn}$.

Navíc pro $g \in G$ *odpovídá* $sgn(g)$ *součinu znamének matice* $\delta(g)$.

Důkaz. Nejprve dokážeme, že znaménko permutace má stejnou paritu jako počet inverzí, tj. uspořádaných dvojic (x, y) takových, že $x < y$ a $x\pi > y\pi$, pro $\pi \in S_n$. Uvažujme Vandermondův polynom $V(x_1, \dots, x_n) = \prod_{i<j}(x_i - x_j)$. Potom se v $V(x_1\pi, \dots, x_n\pi)$ o znaménko liší právě členy, které jsou inverze π. Takto tedy vyjádříme paritu počtu permutací

$$sgn'(\pi) = \frac{V(x_1\pi, \dots, x_n\pi)}{V(x_1, \dots, x_n)}.$$

Přitom funkce sgn' je multiplikativní, tedy permutaci můžeme rozložit na transpozice, přičemž transpozice se zobrazí na -1. Tím je rovnost dokázána.

$$sgn'(\pi\rho) = \frac{V(x_1\pi\rho, \dots, x_n\pi\rho)}{V(x_1, \dots, x_n)} = \\ = \frac{V(x_1\pi\rho, \dots, x_n\pi\rho)}{V(x_1\pi, \dots, x_n\pi)} \cdot \frac{V(x_1\pi, \dots, x_n\pi)}{V(x_1, \dots, x_n)} = sgn'(\pi) \cdot sgn'(\rho)$$

Lemma postačí dokázat pro O, neboť I má stejnou paritu jako O pro $n' = n+1$. Mějme (x, y), $x < y$. Dle definice platí buď $xO = 2x$, nebo $xO = 2x - (2n-1)$, tedy $xO > yO$ nastane právě tehdy, když $2x > 2y - (2n-1) \ge 0$ a $x < n \le y$, celkem $x \in [0, n)$, $y \in [n, x+n)$. Zvolme $x \in [0, n)$, pro něj máme x možností, jak zvolit y, počet inverzí je tedy $\sum_{x=0}^{n-1} x = n(n-1)\frac{1}{2} = \binom{n}{2}$.

Obdobně postupujeme pro $(\overline{x}, \overline{y})$, $\overline{x} < \overline{y}$. Buďto se $\overline{xO}$ rovná $\overline{2x}$ nebo $\overline{(2n-1-2x)}$. Nerovnost $\overline{xO} > \overline{yO}$ je splněna pouze ve dvou případech, pišme pro jednoduchost $x, y \le n-1$ namísto $\overline{x}, \overline{y}$:

(i) $x, y \ge n/2$, kdy $\overline{xO} = 2n - 1 - 2x > 2n - 1 - 2y = \overline{yO}$, neboli $x < y$,

(ii) $x < n/2 \le y$, kdy $\overline{xO} = 2x > 2n - 1 - 2y = \overline{yO}$, neboli $x + y \ge n$.

Označme $m = \lceil n/2 \rceil$. V prvním případě vybíráme obě čísla z $[m, n)$, dvojic je tedy $\binom{n-m}{2}$. V druhém případě obdobně jako předchozím odstavci vybíráme $x \in [0, m)$ a $y \in [n-x, n)$, to je $\sum_{x=0}^{m-1} x = m(m-1)\frac{1}{2} = \binom{m}{2}$ možností. Celkem

$$\overline{sgn}(O) = \binom{n-m}{2} + \binom{m}{2} = \begin{cases} 2\binom{n/2}{2}, & \text{je-li } n \text{ sudé,} \\ \frac{1}{2}(\frac{n-1}{2}(\frac{n-1}{2} - 1) + \frac{n+1}{2}(\frac{n+1}{2} - 1)) & \\ = \frac{1}{2}\frac{n-1}{2}(\frac{n-3+n+1}{2}) = \frac{1}{4}(n-1)^2, & \text{je-li } n \text{ liché.} \end{cases}$$

Dopočteme konkrétní hodnoty (mod 2) v závislosti na volbě n (mod 4), vizte tabulku 2.1.

n (mod 4)	0		1		2		3	
O	1	1	1	1	-1	1	-1	-1
I	1	1	-1	1	-1	-1	1	1

Tabulka 2.1: Hodnoty sgn a $\overline{sgn}$

Počet záporných znamének v $\delta(g)$ odpovídá počtu $x \in [0, n)$, jejichž obraz při g je alespoň n. Rozebereme případy, počty se shodují s právě zmíněnou tabulkou:

(i) $n = 4k$

$$xO = 2x \geq 4k \qquad xI = 2x + 1 \geq 4k$$
$$4k > x \geq 2k \qquad 4k > x \geq 2k - 1/2$$
$$\text{sudý } \#x \qquad \text{sudý } \#x$$

(ii) $n = 4k + 1$

$$xO = 2x \geq 4k + 1 \qquad xI = 2x + 1 \geq 4k + 1$$
$$4k + 1 > x \geq 2k + 1/2 \qquad 4k + 1 > x \geq 2k$$
$$\text{sudý } \#x \qquad \text{lichý } \#x$$

(iii) $n = 4k + 2$

$$xO = 2x \geq 4k + 2 \qquad xI = 2x + 1 \geq 4k + 2$$
$$4k + 2 > x \geq 2k + 1 \qquad 4k + 2 > x \geq 2k + 1$$
$$\text{lichý } \#x \qquad \text{lichý } \#x$$

(iv) $n = 4k + 3$

$$xO = 2x \geq 4k + 3 \qquad xI = 2x + 1 \geq 4k + 3$$
$$4k + 3 > x \geq 2k + 3/2 \qquad 4k + 3 > x \geq 2k + 1$$
$$\text{lichý } \#x \qquad \text{sudý } \#x$$

Zvolme $\pi, \rho \in C_n$. V maticích $\delta(\pi) = (a_{j,k})$ a $\delta(\rho) = (b_{j,k})$ odpovídají nenulové prvky právě $a_{i\overline{\pi},i}$ a $b_{i\overline{\rho},i}$, takže vynásobení znamének součinu $\delta(\rho) \cdot \delta(\pi)$ odpovídá $\prod_i (b_{i\overline{\pi\rho},i\overline{\pi}} \cdot a_{i\overline{\pi},i}) = (\prod_i b_{i\overline{\rho},i})(\prod_i a_{i\overline{\pi},i})$, součin znamének je multiplikativní, a protože jsme právě vypočítali, že se shoduje se sgn pro O a I, nastává rovnost na celé $\langle I, O \rangle$. □

V důkazu následujících lemmat značíme π^σ konjugaci, $\pi^\sigma = \sigma^{-1}\pi\sigma$.

LEMMA 9. *Nechť $n \geq 3$. Mějme graf, jehož vrcholy tvoří trojcykly z A_n. Mezi vrcholy se nachází hrana právě tehdy, když existuje $i \in [0, n)$, které není pevným bodem ani jedním z nich. Jinak řečeno, i se vyskytuje v zápisu obou permutací. Pokud H je souvislý podgraf takový, že se v zápisech vrcholů objeví všechny $i \in [0, n)$, potom H generuje A_n.*

Důkaz. Mějme dvě permutace spojené hranou. To znamená, že sdílí v zápisu buď jeden, nebo dva prvky z $[0,n)$. Ukážeme, že tato dvojice permutací generuje všechny trojcykly složené z jejich prvků.

(i) $\pi=(abc)$, $\rho=(cde)\in H$.

$$(abd)=\pi^{\rho}, \quad (abe)=\pi^{\rho^2}, \quad (acd)=(\pi^2)^{\rho\pi^2}, \quad (ace)=(\pi^2)^{\rho^2\pi^2},$$
$$(ade)=\rho^{\pi}, \quad (bcd)=\rho^{\pi^2\rho^2}, \quad (bde)=\rho^{\pi^2}, \quad (cbe)=\rho^{\pi^2\rho}.$$

(ii) $\pi=(abc), \rho=(bcd)\in H$. $(abd)=(\pi^2)^{\rho^2}$, $(acd)=\pi^{\rho}$.

Zvolme libovolný trojcyklus $(abc)\in A_n$. Nalezneme sled $\sigma_1,\dots,\sigma_k,\dots,\sigma_{k+l}$ v H takový, že σ_1 obsahuje a, σ_k obsahuje b a σ_{k+l} obsahuje c. Označme $H_i=\langle\sigma_1,\dots,\sigma_i\rangle$. Nechť H_{i-1} obsahuje všechny trojcykly permutující prvky ze zápisů $\sigma_1,\dots,\sigma_{i-1}$, zvolme dva z těchto prvků, x a y, a trojcyklus π, který je obsahuje. Potom dle předchozího rozboru případů $H_i=\langle H_{i-1},\sigma_i\rangle$ obsahuje všechny trojcykly permutující x,y a prvky ze σ_i. Takže dle indukce H_{k+l} obsahuje (abc). Jelikož potom H obsahuje všechny trojcykly, lze složit libovolnou dvojici transpozic $(ab)(cd)=(acb)(bdc)$. □

Definice 4. *G^* značí množinu prvků $g\in G$ takových, že $g([0,n))=[0,n)$. Permutace $z\in S_{2n}$ nechť prohazuje sdružené prvky, tj. $z: x\mapsto x'$ pro každé $x\in[0,n)$. V řeči karet mluvíme o převrácení balíčku.*

Lemma 10. *Pokud $G^*\supseteq A_n$, potom $|K|\geq 2^{n-1}$ a K obsahuje všechny možné sudé permutace.*

Důkaz. Podle tabulky 2.1 je vždy alespoň jedna z permutací $\{\overline{I},\overline{O}\}$ sudá. Zvolme $U\in\{I,O\}$ tak, že $\overline{U}$ je sudá. Podle předpokladu existuje prvek $g\in G^*$ takový, že $\overline{g}=\overline{U}$. Definujeme $k=g^{-1}U$, zřejmě $\overline{k}=\overline{\mathrm{id}}$ a $k\in K\setminus\{z\}$. Dle definic perfektních zamíchání je $0U$ buď 0 nebo 1, stejně tak $0'U=0'$ nebo $1'$, v obou případech k fixuje prvky $0,0'$, ale existují páry které budou prohozeny, protože $U\neq g$. Označme je $(x_1,x_1'),(x_2,x_2'),\dots,(x_m,x_m')$. Nechť $m\geq 3$, zvolme $h=(0\ x_1)(x_2\ x_3)\in G^*$ a platí

$$\begin{aligned} k &= (0)(0')(x_1x_1')(x_2x_2')\cdots(x_mx_m'),\\ k^h &= (x_1)(x_1')(00')(x_2x_2')\cdots(x_mx_m'),\\ kk^h &= (00')(x_1x_1'). \end{aligned}$$

Konjugací poslední uvedené permutace prvky z G^* dostaneme libovolné $(aa')(bb')$, skládáním pak libovolný sudý počet disjunktních transpozic.

$$|K|\geq\sum_{0\leq m\leq n/2}\binom{n}{2m}=\sum_{0\leq m\leq n/2}\left(\binom{n-1}{2m-1}+\binom{n-1}{2m}\right)=2^{n-1},$$

položíme-li $\binom{n-1}{-1}=\binom{n-1}{n}=0$.

Pokud $m<3$, stačí výše použít přímo k. □

Lemmata 9, 10 postačí pro dokázání finální věty pro n liché. Také se neustále budeme vracet do tabulky 2.1.

Lemma 11. *Věta 4 platí pro n liché.*

Důkaz. Začneme sérií výpočtů. Permutace

$$IO^{-1} : x \mapsto x + n \pmod{2n}$$

prohazuje dolní a horní polovinu balíčku karet, což lze nejlépe vypozorovat z obrázků 1.2 a 1.3. Alternativně pišme $x \mapsto (n-1-x)'$, $x \in [0, n)$. Podobně nahlédneme, že $I^{-1}O$ prohazuje prvky v rámci po sobě jdoucích dvojic,

$$I^{-1}O : 2x \leftrightarrow 2x + 1,$$

a díky předpokladu, že n je liché, speciálně $n - 1 \leftrightarrow (n-1)'$. Dále

$$I^{-1}O \cdot IO^{-1} : \begin{cases} 2x \mapsto 2x + 1 + n & \pmod{2n}, \\ 2x + 1 \mapsto 2x + n & \pmod{2n}, \end{cases}$$

$$a = (I^{-1}OIO^{-1})^2 : \begin{cases} 2x \mapsto 2x + 2 & \pmod{2n}, \\ 2x + 1 \mapsto 2x - 1 & \pmod{2n}. \end{cases}$$

A dále

$$\begin{aligned} a &= (0, 2, 4, \ldots, n-1, (n-2)', (n-3)', \ldots, 3', 1')(0', 2', 4', \ldots, 3, 1), \\ b = a^{O^{-1}} &= (0, 1, 2, \ldots, n-1)(0', 1', 2', \ldots, (n-1)'), \\ b^2 &= (0, 2, 4, \ldots, n-1, 1, 3, \ldots, n-2)(0', 2', 4', \ldots, (n-2)'), \\ (b^2)^{I^{-1}O} &= (1, 3, 5, \ldots, n-2, (n-1)', 0, 2, \ldots, n-3)(1', 3', \ldots, (n-3)'), \\ c = b^{-2}(b^2)^{I^{-1}O} &= (0', n-1, 1)(0, (n-1)', 1'), \\ c^{b^{-1}} &= ((n-1)', n-2, 0)(n-1, (n-2)', 0'), \\ d = (c^{b^{-1}})^{I^{-1}O} &= (n-1, n-3, 1)((n-1)', (n-3)', 1'). \end{aligned}$$

Ihned vidíme, že b i d náleží do G^*. Omezíme-li se na $[0, n)$, konjugací prvku d mocninami b dostaneme trojcykly potřebné pro lemma 9, z čehož okamžitě plyne předpoklad lemmatu 10, $G^* \supseteq A_n$, a tak platí spodní odhad $|K| \geq 2^{n-1}$.

Nejprve nechť $n \equiv 1 \pmod 4$. Použijeme lemma 8; $\overline{G}$ má všechna znaménka sudá, $\overline{G} = A_n$. Nalezneme sudé $g \in G^*$ takové, že $\overline{g} = \overline{I}$, I je liché podle tabulky. Takže K obsahuje liché gI^{-1}, a tak je největší možné, $|K| = 2^n$. Potom $|G| = n!2^{n-1}$. Podle lemmatu 8 pak pro každé $g \in G$ platí $\det|\delta(g)| = \overline{sgn}(g) = 1$, a tudíž je G izomorfní podgrupě matic Coxeterovy D_n takových, že jejich příslušná permutace je sudá.

Dále nechť $n \equiv 3 \pmod 4$. $\overline{G} \supseteq A_n$ obsahuje lichou permutaci $\overline{O}$, takže nutně $\overline{G} = S_n$. Protože z je liché, není prvkem G (lemma 8), platí $K \subsetneq \mathbb{Z}_2^n$ až na izomorfismus. Dohromady opět $|G| = n!2^{n-1}$. Obdobně jako výše pro $g \in G$, $A = \delta(g)$ platí $\det A = \det|A| \cdot$ (součin znamének A) $= \overline{sgn}(g) \cdot sgn(g) = 1$, a G je izomorfní podgrupě matic Coxeterovy D_n s determinantem rovným 1. □

Pokračujme v důkazu věty pro sudé n, označme $2n = 2^k\nu$. Následující lemmata ukazují, jak operovat s kartami v balíčku po vrstvách. V prvním z nich, lemmatu 12, se naučíme převracet karty v rámci vrstev o 2^r kartách a pak v lemmatu 13 převracíme pořadí samotných vrstev velikosti $2n/2^r$.

Lemma 12. *Nechť $r \in [0,k]$. Mějme nezáporná $\mu < 2^{k-r}\nu = 2n/2^r$ a $s < 2^r$. Potom platí*

$$(2^r\mu + s)O^{-r}I^r = 2^r\mu + (2^r - 1 - s)\ a$$
$$(2^r\mu + s)'O^{-r}I^r = (2^r\mu + (2^r - 1 - s))'.$$

Důkaz. Pro $r = 0$ tvrzení zřejmě platí. Budeme postupovat indukcí. Předpokládejme, že tvrzení platí pro $r - 1 \geq 0$, v indukčním kroku rozlišíme případy pro s sudé a liché. Je-li sudé, $s = 2t$, platí

$$\begin{aligned}(2^r\mu + s)O^{-1}O^{-r+1}I^{r-1}I &= (2^{r-1}\mu + t)O^{-r+1}I^{r-1}I \\ &= (2^{r-1}\mu + (2^{r-1} - 1 - t))I \\ &= 2(2^{r-1}\mu + (2^{r-1} - 1 - t)) + 1 \\ &= 2^r\mu + 2^r - 1 - s.\end{aligned}$$

Obdobně, pokud $s = 2t - 1$,

$$\begin{aligned}(2^r\mu + s)O^{-1}O^{-r+1}I^{r-1}I &= \left(\frac{2^r\mu + s - 1}{2} + n\right)O^{-r+1}I^{r-1}I \\ &= (n + 2^{r-1}\mu + t - 1)O^{-r+1}I^{r-1}I \\ &= (n + 2^{r-1}\mu + 2^{r-1} - t)I \\ &= 2^r\mu + 2^r - 1 - s.\end{aligned}$$

□

Lemma 13. *Nechť $r \in [1,k]$, $0 \leq i < 2^{r-1}$ a $x \in [i(n/2^{r-1}), (i+1)(n/2^{r-1}))$, pak*

$$xI^rO^{-r} = \left(-x - 1 + \frac{n}{2^{r-1}}(2i+1)\right)',$$

$$x'I^rO^{-r} = -x - 1 + \frac{n}{2^{r-1}}(2i+1).$$

Důkaz. Opět postupujeme indukcí. Případ $r = 1$ už známe,

$$xIO^{-1} = x + n = (n - 1 - x)', \quad x \in [0,n).$$

Z předpokladů plyne, že x je vždy menší než n, dále rozdělíme indukční krok $r > 1$ na dvě možnosti: Mějme napřed $x \in [0, n/2)$, pak $xI < n$ a

$$xI = 2x + 1 \in [i(n/2^{r-2}), (i+1)(n/2^{r-2})), \text{ a tak}$$
$$\begin{aligned}xII^{r-1}O^{-r+1}O^{-1} &= \left(-(2x+1) - 1 + \frac{n}{2^{r-2}}(2i+1)\right)'O^{-1} \\ &= \left(-x - 1 + \frac{n}{2^{r-1}}(2i+1)\right)'.\end{aligned}$$

Pro $x \in [n/2, n)$ platí $x'I = 2n - 2x - 2$,

$$i\frac{n}{2^{r-1}} \leq x < (i+1)\frac{n}{2^{r-1}}$$
$$2n - 2 - i\frac{n}{2^{r-2}} \geq x'I = 2n - 2x - 2 > 2n - 2 - (i+1)\frac{n}{2^{r-2}},$$

ale díky tomu, že je $x'I$ sudé, lze posunout spodní hranici, tudíž $x'I \in [(2^{r-1} - i - 1)n/2^{r-2}, (2^{r-1} - i)n/2^{r-2} - 1)$ a můžeme použít indukční předpoklad.

$$\begin{aligned} x'II^{-r+1}O^{r-1}O^{-1} & \\ &= \left(-(2n - 2x - 2) - 1 + \frac{n}{2^{r-2}}(2(2^{r-1} - i - 1) + 1)\right)' O^{-1} \\ &= \left(-n + x + \frac{n}{2^{r-1}}(2^r - 2i - 1) + n\right)' \\ &= 2n - 1 - \left(2n + x - \frac{n}{2^{r-1}}(2i + 1)\right) \\ &= -x - 1 - \frac{n}{2^{r-1}}(2i + 1). \end{aligned}$$

□

Lemma 14. *Permutace $\alpha = (I^k O^{-k} I^{-1} O)^{-2}$ na intervalech $[i2\nu, (i+1)2\nu)$ indukuje permutaci*

$$(i2\nu, i2\nu + 2, i2\nu + 4, \ldots, (i+1)2\nu - 2) \\ ((i+1)2\nu - 1, (i+1)2\nu - 3, \ldots, i2\nu + 3, i2\nu + 1),$$

speciálně pak $(0, 2, 4, \ldots, 2\nu - 2)(2\nu - 1, 2\nu - 3, \ldots, 3, 1)$ na $[0, 2\nu)$.

Důkaz. Počítejme za pomoci předchozího lemmatu, $\nu = n/2^{k-1}$, $r = k$. Označme $A = I^k O^{-k} I^{-1} O$ a zvolme $x \in [i\nu, (i+1)\nu)$.

$$\begin{aligned} x'A &= (-x - 1 + \nu(2i + 1))I^{-1}O \\ &= \begin{cases} \left(\frac{1}{2}(-x - 1 + \nu(2i + 1)) + n\right) O = -x + \nu(2i + 1), & \text{je-li } x \text{ sudé}, \\ \left(\frac{1}{2}(-x - 2 + \nu(2i + 1))\right) O = -x - 2 + \nu(2i + 1), & \text{je-li } x \text{ liché}. \end{cases} \end{aligned}$$

Kromě volby sudého $x = i\nu$ nebo lichého $x = (i+1)\nu$ náleží $x'A$ opět do $[i\nu, (i+1)\nu)$.

$$xAA = \\ = \begin{cases} \Big(\overbrace{-x + \nu(2i + 1)}^{\text{liché}} \Big)' A = -(-x + \nu(2i + 1)) - 2 + \nu(2i + 1) = x - 2, & \text{je-li } x \text{ sudé}, \\ \Big(\overbrace{-x - 2 + \nu(2i + 1)}^{\text{sudé}} \Big)' A = -(-x - 2 + \nu(2i + 1)) + \nu(2i + 1) = x + 2, & x \text{ liché}. \end{cases}$$

Pro sudé $x = i\nu$ máme $x'A = \nu(i+1) \in [(i+1)\nu, (i+2)\nu)$ liché, tedy $xAA = (\nu(i+1))'A = -\nu(i+1) - 2 + \nu(2(i+1)+1) = \nu(i+2) - 2$. A obdobně, je-li $x = \nu(i+1) - 1$ liché, musí $x'A = \nu i - 1 \in [(i-1)\nu, i\nu)$ být sudé a $xAA = -(\nu i - 1) + \nu(2(i-1)+1) = \nu(i-1) + 1$. □

Lemma 15. *$\beta = \alpha^{O^{-1}}$ na intervalech $[i\nu, (i+1)\nu)$ indukuje permutace $(i\nu, \nu + 1, \nu + 2, \ldots, (i+1)\nu)$. Speciálně $(0, 1, \ldots, \nu - 1)$ na $[0, \nu)$.*

Důkaz.

$$\alpha^{O^{-1}} = ((i2\nu)O^{-1}, (i2\nu+2)O^{-1}, \ldots, (i2\nu+2\nu-2)O^{-1})\ldots \\ = (i\nu, i\nu+1, \ldots, i\nu+\nu-1)\ldots.$$

□

Definice 5. *Označíme*

$$\gamma(r) = O^{-r}I^r \quad \textit{(z lemmatu 12)} \\ H(1) = \langle \alpha, \beta, \gamma(1)\rangle \\ H(r) = \langle H(r-1), \gamma(r)\rangle\,.$$

Zkombinování lemmat 12, 14 a 15 získáváme následující vlastnosti.

Lemma 16. *Nechť $r \in [1,k)$. Pro každé $h \in H(r)$ platí $h([0,2^r\nu)) = [0,2^r\nu)$ a $h(x+2^r\nu) = h(x) + 2^r\nu$, jestliže $x, x+2^r\nu \in [0,n)$.*

Lemma 17. *Nechť $\nu > 3$, pak $H(1)$ na $[0,2\nu)$ indukuje $S_{2\nu}$.*

Důkaz. Omezme následující prvky na množinu $[0,2\nu)$,

$$\alpha = (0,2,4,\ldots,2\nu-2)(2\nu-1,\ldots,3,1),$$
$$\beta = (0,1,2,\ldots,\nu-1)(\nu,\nu+1,\ldots,2\nu-1),$$
$$\gamma = \gamma(1) = (0\ 1)(2\ 3)\ldots(\nu-1,\nu)\ldots(2\nu-4,2\nu-3)(2\nu-2,2\nu-1).$$

Dále počítáme, snažíme se izolovat jednotlivý trojcyklus. Protože je ν alespoň 5, mají následující výrazy smysl jako permutace intervalu $[0,2\nu)$; pouze nastane-li rovnost $\nu = 5$, objeví se ve výpočtu nula místo $\nu+5$, výsledek se nezmění.

$$\gamma^{\beta^2} = (2\ 3)(4\ 5)\ldots(\nu-1,0)(1,\nu+2)(\nu+3,\nu+4)\ldots(2\nu-2,2\nu-1)(\nu,\nu+1),$$
$$d = \gamma\gamma^{\beta^2} = (0,\nu+2,\nu)(1,\nu-1,\nu+1),$$
$$d^\beta = (1,\nu+3,\nu+1)(2,0,\nu+2),$$
$$e = d^{d^\beta} = (\nu+2,2,\nu)(\nu+3,\nu-1,1),$$
$$f = e^\alpha = (\nu,4,\nu-2)(\nu+5,\nu+1,2\nu-1),$$
$$e^f = (\nu+2,2,4)(\nu+3,\nu-1,1),$$
$$e^{-1}e^f = (\nu+2,\nu,4).$$

Tento cyklus po konjugaci mocninami α a β obsahuje libovolnou dvojici čísel z $[0,2\nu)$ o 2 vzdálených a třetí prvek ve trojici je opačné parity. Tudíž jsou propojena všechna sudá čísla s lichými a lze použít lemma 9. □

Lemma 18. *Nechť $r \in [1,k)$. Potom jestliže $H(r)$ indukuje $A_{2^r\nu}$ na $[0,2^r\nu)$, tak i $H(r+1)$ indukuje $A_{2^{r+1}\nu}$ na $[0,2^{r+1}\nu)$.*

Důkaz. Předpokládejme, že $H(r)$ indukuje $A_{2^r\nu}$ na $[0, 2^r\nu)$. Omezme všechny permutace na $[0, 2^{r+1}\nu)$. (0 1 2) náleží do $H(r)$, a díky lemmatu 16 náleží do $H(r+1)$ i g:

$$g = (0\ 1\ 2)(2^r\nu, 2^r\nu + 1, 2^r\nu + 2).$$
$$g^{\gamma(r+1)} = (2^{r+1} - 1, 2^{r+1} - 2, 2^{r+1} - 3)(2^r\nu - 1, 2^r\nu - 2, 2^r\nu - 3),$$
$$\text{neboť } 2^r\nu = 2^{r+1}\frac{\nu - 1}{2} + 2^r \xrightarrow{\gamma(r+1)} 2^{r+1}\frac{\nu - 1}{2} + 2^r + 2^{r+1} - 1 - (2^r) = 2^r\nu - 1.$$

$$h = (2^{r+1} - 1, 2^{r+1}, 0) \in H(r),$$
$$g^{\gamma(r+1)h} = (2^{r+1}, 2^{r+1} - 2, 2^{r+1} - 3)(2^r\nu - 1, 2^r\nu - 2, 2^r\nu - 3),$$
$$g^{\gamma(r+1)h}(g^{\gamma(r+1)})^{-1} = (2^{r+1}, 2^{r+1} - 1, 2^{r+1} - 3).$$

Obdobně jako v předchozím důkazu generujeme trojcykly. Konjugace s α a β dovolují libovolné posuny v rámci intervalů $[i2\nu, (i+1)2\nu)$ a ty lze propojit pomocí $\gamma(1), \ldots, \gamma(r+1)$, načež jsou splněny předpoklady pro lemma 9. □

Lemma 19. *Věta 4 platí pro n sudé.*

Důkaz. Jako pro liché n nejprve ukážeme, že $G^* \supseteq A_n$. Pokud je ν alespoň 3, vyplývá to přímo z předchozích dvou lemmat. Nastane-li rovnost $\nu = 3$, není možné použít podobný postup, v důkazu lemmatu 17 nemá $[0, 2\nu)$ dostatek prvků na izolování jednoho trojcyklu a ve skutečnosti jsou $H(1)$ i $H(2)$ příliš malá. Až $H(3)$ je izomorfní A_{24}, což bylo ověřeno v GAPu [22], jako generátory posloužily α, β a $\gamma(3)$.

Nechť $n \neq 6, 12$. Analogicky jako v důkazu lemmatu 11: Opět platí odhad $|K| \geq 2^{n-1}$ z lemmatu 10. Pro $n \equiv 0 \pmod 4$, obsahují G i $\overline{G}$ jen sudé permutace, $\overline{G} = A_n$, a součin znamének příslušných matic je roven 1, $|K| = 2^{n-1}$. Pro $n \equiv 2 \pmod 4$ je podle tabulky 2.1 $\overline{I}$ liché, a tak $\overline{G} = S_n$, $\overline{O}$ je sudé zatímco O liché. Potom $g \in G^*$ splňující $\overline{g} = \overline{O}$ je také sudé ale $gO^{-1} \in K$ liché. $|K| = 2^n$.

Poslední dva speciální případy jsou podrobněji vysvětleny v [DGK83]. Jestliže $n = 6$, je $\overline{G}$ izomorfní S_5 a $|K| = 2^6$. Nejpřekvapivější situace nastane při $n = 12$, kdy je $\overline{G}$ izomorfní Mathiově M_{12}, to díky tomu, že je jediná dvojitě tranzitivní svého řádu, a $|K| = 2^{11}$.

□

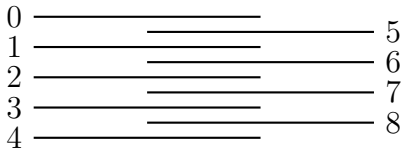
3. Zobecnění

3.1 Lichý počet karet

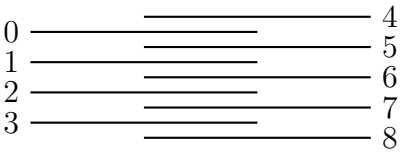
Jak ukazují [DGK83] s [Gol61], pokud definujeme faro shuffle na lichém počtu karet, je situace mnohem jednodušší. Obě zamíchání operují pod $\pmod{2n-1}$, jsou symetrické. To zapříčiní, že výpočet velikosti jimi generované grupy je téměř analogický lemmatu 6. A také díky podobnosti s minulou definicí platí tvrzení 1 beze změny.

Definice 6. *Pro balíček o* $2n-1$ *kartách definujeme permutace* out shuffle*, resp.* in shuffle *následovně:*

$$O(i) = 2i \pmod{2n-1},$$
$$I(i) = 2i+1 \pmod{2n-1}.$$



Obrázek 3.1: Out shuffle



Obrázek 3.2: In shuffle

Věta 20. *Pro balíček velikosti* $2n-1$ *má* $\langle I, O\rangle$ *řád roven* $(2n-1) \times$ *řád* $2 \pmod{2n-1}$.

Důkaz. Zadefinujme permutaci C, která přesune spodní kartu navrch balíčku, $C(i) = i+1 \pmod{2n-1}$. Zřejmě platí $I = OC$, tudíž $\langle O, C\rangle = \langle I, O\rangle$.

Lemma 21. *Nechť* G *je grupa,* $a, b \in G$ *jsou prvky řádů* m, n *a platí* $ba = ab^k$*, kde* $k \not\equiv 0 \pmod{n}$*. Potom má grupa* $\langle a, b\rangle$ *řád nanejvýš* mn *a rovnost nastává, pokud* $a^x = b^y$ *nemá netriviální řešení pro* x, y*.*

Důkaz. Všechny prvky grupy $\langle a, b\rangle$ jsou tvaru $a^i b^j$, neboť $b^j a^i$ lze upravit:

$$b^j a^i = (ab^k a^{-1})^j a^i = ab^{jk} a^{i-1} = a(ab^k a^{-1})^{jk} a^{i-1} = \cdots = a^i b^{jk^i}.$$

Pokud jsou všechny zápisy $a^i b^j$ a $a^x b^y$ navzájem různé, což nastává, právě když $a^{i-x} = b^{y-j}$, má grupa přesně mn prvků. □

Přímo aplikujeme toto lemma na O a C. Řád O je roven řádu $2 \pmod{2n-1}$ jako v úvodu první kapitoly, neboť zápis permutace O je stejný, a řád C je zřejmě $2n-1$ a platí $CO = OC^2 : i \mapsto 2i+2$. Rovnice $O^x = C^y$ nemá netriviální řešení, protože pouze O fixuje první kartu. □

3.2 Zobecněné faro shuffle

Klasické faro shuffle je praktický způsob míchání karet, v této kapitole jej zobecníme tak, že už jeho efektní provedení bohužel nebude možné. Vezměme si 33 karet a rozdělme je do hromádek po 11, zvolme si pořadí těchto hromádek libovolně. Postupně z každé taháme zespodu po jedné kartě a karty skládáme na výslednou hromádku, dokud nedojdou. Tato varianta má tedy dvě složky: napřed se permutují hromádky v rámci balíčku a potom se prolnou dohromady. K závěrům kapitoly dospěli Medvedoff a Morrison [MM87].

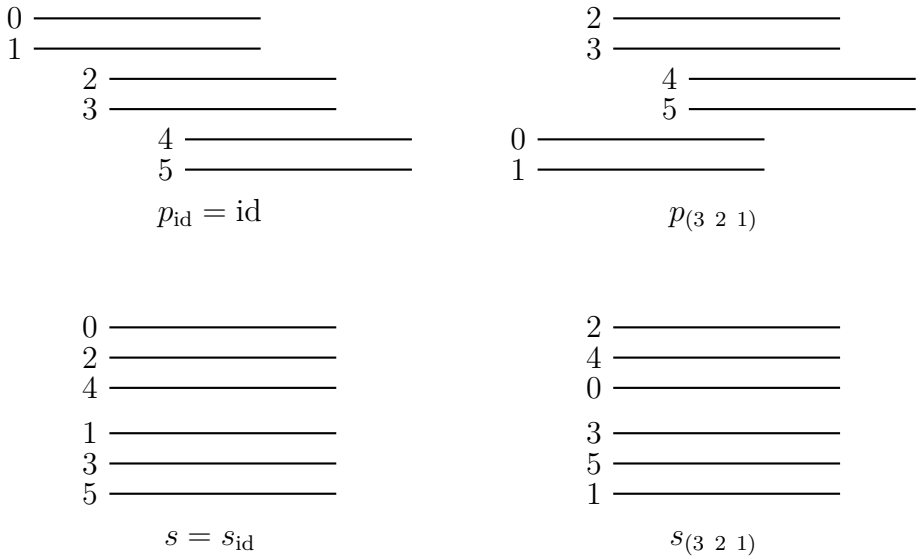
Definice 7. *Mějme balíček kn karet (stále číslujeme 0 až $kn-1$) a $\pi \in S_k$. Symbolem p_π označme permutaci prohazující pořadí hromádek velikosti n podle předpisu π, jinými slovy*

$$p_\pi(i + jn) = i + \pi(j) \cdot n, \quad \textit{pro } i \in [0, n),\ j \in [0, k).$$

Prolnutí hromádek lze zapsat tímto způsobem:

$$s(x) = \begin{cases} kx \pmod{kn-1}, & \textit{pro } x < kn-1, \\ kn-1, & \textit{pokud } x = kn-1. \end{cases}$$
$$s(i + jn) = ki + j$$

Dále značíme $s_\pi = p_\pi s$. Grupu generovanou permutacemi s_π pro $\pi \in S_k$ zapisujeme $G_{k,kn}$.



Obrázek 3.3: Ilustrace definic pro $k = 3$, $n = 2$.

Poznámka. Všimněme si, že pokud zapíšeme čísla karet do k řádků a n sloupců, lze permutaci s interpretovat jako transponování tohoto schématu.

$$\begin{matrix} 0 & 1 \\ 2 & 3 \\ 4 & 5 \end{matrix} \xrightarrow{\ s\ } \begin{matrix} 0 & 2 & 4 \\ 1 & 3 & 5 \end{matrix}$$

Vidíme, že $G_{2,2n}$ odpovídá $\langle I, O\rangle$ z minulé kapitoly. Definice 7 nám neumožňuje jednoduše vyjádřit složení s_π a s_σ. Pro p_π ale máme jednoduchý vztah $p_\pi p_\sigma = p_{\pi\sigma}$ a navíc $p_\pi \in G_{k,kn}$ pro libovolné π, protože $s_\pi = p_\pi s = p_\pi s_{\mathrm{id}}$. Protože ale víme, že S_k lze generovat dvěma prvky (např. $(0\ 1)$ a $(0\ 1\ \ldots k-1)$), lze $G_{k,kn}$ generovat třemi; nechť π, σ generují S_k, potom p_π, p_σ, s stačí pro generování $G_{k,kn}$.

Prvním krokem bude zjistit, zda je $G_{k,kn}$ podgrupou A_{kn}.

Lemma 22. *Permutace p_π je lichá, právě tehdy když n je liché a zároveň π je lichá.*

Důkaz. p_π je rovna složení n disjunktních permutací se stejnou strukturou jako π. □

Lemma 23. *Permutace s je sudá, právě tehdy když je k nebo n kongruentní* 0 *nebo* 1 (mod 4).

Důkaz. Spočteme počet transpozic nutných pro vrácení balíčku nazpět po permutaci s. Budeme po sloupcích na obrázku níže vracet prvky na původní místo transpozicemi sousedících prvků, jde o jakýsi bubble sort. Prvek 0 je na svém místě, 1 se musí posunout o $k-1$ pozic, 2 o $2k-2$, tedy $m < n$ je nutno posunout $m(k-1)$ transpozicemi a první celý sloupec, karty 0 až $n-1$, $t_1 = (n-1)(n/2)(k-1)$ transpozicemi. Obdobně $t_j = (n-1)(n/2)(k-j)$ pro j-tý sloupec.

$$\begin{array}{ccccccc} & 0 & n & \cdots & (k-1)n & & 0\ 1 \ldots\ n-1 \\ & 1 & n+1 & \cdots & \vdots & \xrightarrow{t_1 \text{ transpozic}} & \\ \xrightarrow{s} & \vdots & \vdots & \cdots & & & \\ & n-1 & 2n-1 & \cdots & kn-1 & & \end{array} \begin{array}{ccc} n & \cdots & (k-1)n \\ n+1 & \cdots & \vdots \\ \vdots & \cdots & \\ 2n-1 & \cdots & kn-1 \end{array}$$

$$\xrightarrow{t_2 \text{ transpozic}} \cdots \xrightarrow{t_k \text{ transpozic}} 0\ 1\ \ldots\ kn-1$$

$$\sum t_j = \frac{n(n-1)}{2}\left((k-1)+(k-2)+\cdots+1+0\right) = \frac{n(n-1)}{2}\frac{k(k-1)}{2}.$$

□

Zkombinováním lemmat dostáváme první větu této kapitoly.

Věta 24. *$G_{k,kn}$ je obsažena v A_{kn}, právě tehdy když*

(a) $n \equiv 0 \pmod 4$,

(b) *nebo když je n sudé a k kongruentní* 0 *nebo* 1 (mod 4).

A není složité zobecnit lemma 7.

Definice 8. *Nechť A a G jsou grupy. Pak definujeme věncový součin $A \wr G$ jako semidirektní součin $A^G \rtimes_\phi G$, kde $\phi_g((a_h)_{h\in G}) = (a_{gh})_{h\in G}$ pro $(a_h)_{h\in G} \in A^G$ a $g \in G$.*

Věta 25. *Grupa G_{k,k^m} je izomorfní věncovému součinu $S_k \wr \mathbb{Z}_m$, kde generátor grupy $\mathbb{Z}_m$ působí na m-tici $\tau \in (S_k)^m$ jako cyklický posun $\tau = (\tau_{m-1}, \ldots, \tau_0) \mapsto (\tau_{m-2}, \ldots, \tau_0, \tau_{m-1})$. Řád grupy je roven $m(k!)^m$.*

Důkaz. Zvolme $x \in [0, k^m)$. Máme $x = i + jk^{m-1}$ pro $i \in [0, k^{m-1})$ a $j \in [0, k)$, permutace působí takto $p_\pi(x) = i + \pi(j)k^{m-1}$ a $(p_\pi s)(x) = ki + \pi(j)$. A zapíšeme-li x do soustavy o základu k, neboli $x = (x_{m-1}, \ldots, x_0)$, vypadá působení následovně:

$$(x_{m-1}, \ldots, x_0) \xrightarrow{p_\pi} (\pi(x_{m-1}), \ldots, x_0) \xrightarrow{s} (x_{m-2}, \ldots, x_0, \pi(x_{m-1})).$$

Potom pro $\pi_0, \ldots, \pi_{m-1}, \sigma \in S_k$ máme

$$\begin{aligned}
(x)s_{\pi_{m-1}} \cdots s_{\pi_0} &= (\pi_{m-1}(x_{m-1}), \ldots, \pi_0(x_0)), \\
(x)s_\sigma^{-1} s_{\pi_{m-1}} \cdots s_{\pi_0} &= ((\sigma^{-1}\pi_{m-1})(x_0), \pi_{m-2}(x_{m-1}), \ldots, \pi_0(x_1)), \\
(x)s_\sigma^{-1} s_{\pi_{m-1}} \cdots s_{\pi_0} s_\sigma &= (\pi_{m-2}(x_{m-1}), \ldots, \pi_0(x_1), \pi_{m-1}^\sigma(x_0)).
\end{aligned}$$

Takže množina prvků tvaru $s_{\pi_{m-1}} \cdots s_{\pi_0}$ je uzavřena na skládání a tvoří normální podgrupu, pojmenujme ji $N \trianglelefteq G_{k,kn}$, jež je izomorfní $(S_k)^m$. Z výpočtů výše je N invariantní vůči násobení libovolnou s_π nebo p_π, a tak lze libovolný prvek zapsat jako $s_{\pi_{m-1}} \cdots s_{\pi_0} \cdot s^z$, $z \in \mathbb{Z}$, protože s už působí jen jako cyklický posun. Tudíž $N \langle s \rangle = G_{k,kn}$ a $G_{k,kn}/N$ je izomorfní $\langle s \rangle \cong \mathbb{Z}_m$ a máme semidirektní rozklad, přesněji věncový součin $S_k \wr \mathbb{Z}_m$. □

Nyní si prohlédněme jakým grupám je $G_{k,kn}$ izomorfní, vizte tabulku 3.1 vypočítanou pomocí GAPu [22].

Lze usuzovat, že ve většině případů je $G_{k,kn}$ rovna S_{kn} nebo A_{kn} podle hodnot $k, n \pmod 4$, jak vlastně naznačuje věta 24. Tak i uvádí Medvedoff a Morrison [MM87] jako domněnku; nejspíše pro $k = 3$ mohou nastat pouze tři možnosti S_{3n}, A_{3n}, nebo $S_3 \wr \mathbb{Z}_m$, jediná možnost, kterou se podařilo dokázat (věta 25). Na rozdíl od permutací $2n$ karet zde nelze využít centrální symetrie, i s ní nebyl výpočet naprosto přímočarý. Ukážeme si možný postup důkazu pro $k = 3$ s pevným n. Nejprve je třeba zobecnění tvrzení 1.

Tvrzení 26. *Pro přesunutí vrchní karty na pozici $x \in [0, kn)$ zapišme x do soustavy o základu k, $x = (x_m, x_{m-1}, \ldots, x_0)$. Označme σ_i libovolnou permutaci z S_k, která zobrazí nulu na x_i. Potom je $s_{\sigma_m} \cdots s_{\sigma_0}$ hledaná permutace.*

Důkaz. Indukcí podle m. Nechť $m = 0$, neboli $x \in [0, k)$. Pak $s_{\sigma_0}(0) \equiv k(0 + xn) \equiv x \pmod{kn - 1}$. Nyní předpokládejme, že permutace $s_{\sigma_m} \cdots s_{\sigma_1}$ přesune nulu na $y = x_m k^{m-1} + \cdots + x_1$. Protože $x < kn$, je y menší než n, a tak $s_{\sigma_0}(y) \equiv k(y + x_0 n) \equiv ky + x_0 \pmod{kn - 1}$. □

Nechť třeba $n = 10$. Spočítáme

$$\begin{aligned}
\alpha &= p_{(1\ 2)} = (10\ 20)(11\ 21)(12\ 22)(13\ 23)(14\ 24)(15\ 25)(16\ 26)(17\ 27)(18\ 28)(19\ 29), \\
\beta &= p_{(0\ 1\ 2)} = (0\ 10\ 20)(1\ 11\ 21)(2\ 12\ 22)(3\ 13\ 23)(4\ 14\ 24)(5\ 15\ 25) \\
&\qquad (6\ 16\ 26)(7\ 17\ 27)(8\ 18\ 28)(9\ 19\ 29). \\
s &= (1\ 3\ 9\ 27\ 23\ 11\ 4\ 12\ 7\ 21\ 5\ 15\ 16\ 19\ 28\ 26\ 20\ 2\ 6\ 18\ 25\ 17\ 22\ 8\ 24\ 14\ 13\ 10).
\end{aligned}$$

n	$G_{3,3n}$	$G_{4,4n}$	$G_{5,5n}$	$G_{6,6n}$
2	S	$(\mathbb{Z}_2)^3 \rtimes \mathrm{PSL}(3,2)$	A	S
3	$S_3 \wr \mathbb{Z}_2$	S	S	S
4	A	$S_4 \wr \mathbb{Z}_2$	A	A
5	S	S	$S_5 \wr \mathbb{Z}_2$	S
6	S	A	A	$S_6 \wr \mathbb{Z}_2$
7	S	S	S	S
8	A	$(\mathbb{Z}_2)^5 \rtimes \mathrm{PSL}(5,2)$	A	A
9	$S_3 \wr \mathbb{Z}_3$	S	S	S
10	S	A	A	S
11	S	S	S	S
12	A	A	A	A
13	S	S	S	S
14	S	A	A	S
15	S	S	S	S
16	A	$S_4 \wr \mathbb{Z}_3$	A	A
17	S	S	S	S
18	S	A	A	S
19	S	S	S	S
20	A	A	A	A

Tabulka 3.1: Hodnoty $G_{k,kn}$. Zapisujeme $S = S_{kn}$, $A = A_{kn}$.

Dokážeme, že $G_{3,30}$ je dvojitě tranzitivní. V zápisu s, v jediném cyklu, chybí pouze 0 a 29. Zřejmě $\langle \alpha, s \rangle$ působí tranzitivně na $\{1, \ldots, 29\}$ a zároveň fixuje nulu. Dále za σ_i ve tvrzení 26 lze použít (0 1 2) a (0 1 2)^2, a tak π_x přesouvající nulu na x náleží do $\langle \beta, s \rangle$. Chceme-li přesunout dvojici (x, y), $x < y$, na (a, b), postačí $(\pi_x)^{-1} \rho \pi_a$, kde $\rho \in \langle \alpha, s \rangle$ zobrazuje $(\pi_x)^{-1}(y)$ na $(\pi_a)^{-1}(b)$.

Definice 9. *Nechť $G \leq S_n$ a $\triangle \subseteq \{0, \ldots, n\}$ je neprázdná množina. Jestliže $g(\triangle) = \triangle$ nebo $g(\triangle) \cap \triangle = \varnothing$ pro každé $g \in G$, nazveme množinu $\triangle$ blokem. Jsou-li jediné bloky grupy triviální bloky, to jest jednoprvkové nebo celá množina, říkáme, že je G primitivní grupa.*

Dvojitá tranzitivita ihned implikuje primitivitu. Zvolme $\triangle \subseteq \{0, \ldots, 29\}$, potom můžeme $i, j \in \triangle$ libovolně zobrazit jedno do $\triangle$ a druhé mimo $\triangle$.

$s^3\alpha = (1\ 17\ 14)(2\ 15\ 18\ 12\ 5\ 29\ 19\ 10\ 9\ 21\ 26\ 6\ 27\ 4\ 11\ 7\ 25\ 8\ 23\ 22\ 24\ 20\ 28)(3\ 13).$

Permutace $s^3\alpha$ má nejdelší cyklus délky 23, takže jejím umocněním na $23 \cdot 3$ získáme transpozici a lze užít následující větu.

Věta 27 (Jordanova). [Isa08] *Nechť je $G \leq S_n$ primitivní grupa a obsahuje cyklus délky p, kde p je prvočíslo menší než $n - 2$. Potom je G rovna A_n nebo S_n.*

Protože $G_{3,30}$ obsahuje transpozici, je rovna celé S_{30}. Obecný postup je tedy dokázat, že $\left\langle p_{(1\ 2)}, s \right\rangle$ je tranzitivní na $\{1, \ldots, kn - 1\}$, a nalézt cyklus délky p a případně lichou permutaci.

Domněnka. (a) Je-li $3n = 3^m$, pak $G_{3,3n} \cong S_3 \wr \mathbb{Z}_m$.

(b) Je-li $n \equiv 0 \pmod 4$, pak $G_{3,3n} = A_{kn}$.

(c) Jinak $G_{3,3n} = S_{kn}$.

Domněnka. Pro $k = 4$ přibude jeden speciální případ.

(a) Je-li $4n = 4^m$, pak $G_{4,4n} \cong S_3 \wr \mathbb{Z}_m$.

(b) Je-li $4n = 2^b$, b liché, pak $G_{4,4n} \cong (\mathbb{Z}_2)^b \rtimes \mathrm{PSL}(b, 2)$.

(c) Je-li n sudé a ne mocnina dvojky, $G_{4,4n} = A_{4n}$.

(d) Je-li n liché, $G_{4,4n} = S_{4n}$.

Medvedoff a Morrison [MM87] píší o Williamu Kantorovi tvrdícím, že se mu podařilo ověřit rovnost $G_{k,kn} = A_{kn}$ nebo S_{kn} v případě $k \geq 4$, kdy k nedělí n. Důkaz ale nebylo možné dohledat. Pomocí GAPu se mi ale podařilo prověřit všechny případy až do $kn \leq 200$.

Domněnka. Nechť $k \geq 5$.

1. Je-li $kn = k^m$, pak $G_{k,kn} \cong S_k \wr \mathbb{Z}_m$.
2. Je-li $n \equiv 0 \pmod 4$, nebo je-li n sudé a $k \equiv 0$ nebo $1 \pmod 4$, pak $G_{k,kn} = A_{kn}$.
3. Jinak $G_{k,kn} = S_{kn}$.

Závěr

Po více než 50 letech byl Elmsleyho problém vyřešen a zde opraven. Zatímco $\langle I, O\rangle$ pro klasické faro je zcela popsána a známa, narážíme zde na Mathiovu grupu a Coxeterovy grupy. Naopak zobecněné faro shuffle přislibuje nanejvýš čtyři různé typy grup, ale jeho otázka doposud nebyla vyřešena, přestože původní článek je sepsán v roce 1987 a dnes lze využít mnohem více výpočetní síly.

Kromě doplnění chybějících důkazů bylo ve druhé kapitole nutno oproti zdroji opravit pár důkazů a tvrzení.

Seznam použité literatury a softwaru

[22] *GAP – Groups, Algorithms, and Programming, Version 4.12.2*. The GAP Group. 2022. URL: https://www.gap-system.org.

[Cai99] David Cain. *RON GRAHAM OBITUARY*. 1999. URL: https://www.juggle.org/ron-graham-obituary/ (cit. 17. 06. 2023).

[CW23] Cornelia A. Van Cott a Katie Wang. *Unshuffling a deck of cards*. 2023. arXiv: 2302.03579 [math.CO].

[DG07] Persi Diaconis a Ron Graham. „The Solutions to Elmsley's Problem". In: *Math Horizons* 14.3 (2007), s. 22–27. DOI: 10.1080/10724117.2007.11974694.

[DG12] Persi Diaconis a Ron Graham. *Magical Mathematics: The Mathematical Ideas That Animate Great Magic Tricks*. Princeton University Press, 2012. ISBN: 9780691151649. URL: http://www.jstor.org/stable/j.ctt7t0gq.

[DGK83] Persi Diaconis, R.L Graham a William M Kantor. „The mathematics of perfect shuffles". In: *Advances in Applied Mathematics* 4.2 (1983), s. 175–196. ISSN: 0196-8858. DOI: https://doi.org/10.1016/0196-8858(83)90009-X. URL: https://www.sciencedirect.com/science/article/pii/019688588390009X.

[Dia06] Persi Diaconis. „Mathematics and Magic Tricks". In: *Annual report of the Clay Mathematics Institute* 36 (2006), s. 5–6. URL: http://www.claymath.org/library/annual_report/ar2006/06report_complete.pdf.

[Gol61] Solomon W. Golomb. „Permutations by Cutting and Shuffling". In: *SIAM Review* 3.4 (1961), s. 293–297. ISSN: 00361445. URL: http://www.jstor.org/stable/2027745 (cit. 04. 07. 2023).

[Hof11] Jascha Hoffman. „Q&A: The mathemagician". In: *Nature* 478.7370 (říj. 2011), s. 457–457. ISSN: 1476-4687. DOI: 10.1038/478457a. URL: https://doi.org/10.1038/478457a.

[Isa08] I. Martin Isaacs. In: *Finite group theory*. American Mathematical Society, 2008, s. 237–245. ISBN: 978-0-8218-4344-4.

[Min94] Stephen Minch. *The Collected Works of Alex Elmsley*. Sv. 2. Tahoma, California: L & L Publishing, 1994, s. 295–301.

[MM87] Steve Medvedoff a Kent Morrison. „Groups of Perfect Shuffles". In: *Mathematics Magazine* 60.1 (1987), s. 3–14. ISSN: 0025570X, 19300980. URL: http://www.jstor.org/stable/2690131.