Elmsleyev problem

Šućur, Jurica

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Jurica Šućur

Elmsleyev problem

Završni rad

Osijek, 2018.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Jurica Šućur

Elmsleyev problem

Završni rad

Mentor: doc. dr. sc. Snježana Majstorović

Osijek, 2018.

Sažetak

Ovaj završni rad bavi se ulogom matematike u miješanju igraćih karata, konkretno Elmsleyevim problemom. Taj problem se odnosi na jedno od najtežih načina miješanja karata, popularno savršeno miješanje. Osim njega, detaljno ćemo objasniti i razne druge načine kako promiješati karte. Kod savršenog miješanja, pokušat ćemo odgovoriti na sljedeća pitanja: koliki je najmanji broj istovrsnih miješanja koje dovode karte do početne pozicije? Postoji li niz savršenih miješanja koji kartu s vrha špila dovode na odabranu poziciju u špilu? Za kraj ostavljamo glavno pitanje koje je postavio Elmsley: može li se nizom savršenih miješanja karta s pozicije p prebaciti na poziciju q? U radu ćemo ukratko opisati grupu generiranu savršenim miješanjima, a također ćemo spomenuti i neke od primjena koncepta savršenog miješanja.

Ključne riječi: miješanje igraćih karata, savršeno miješanje, Elmsleyev problem, $\langle \mathbf{I}, \mathbf{O} \rangle$ grupa

Abstract

This bachelor's thesis considers the role of mathematics in shuffling playing cards, specifically with the Elmsley's problem. This problem is concerned with one of the most difficult shuffle methods, the popular *perfect shuffling*. Besides this problem, we will explain in details various types of card shuffling. Concerning perfect shuffle, we will try to give an answer to the following questions: what is the smallest number of perfect shuffles of the same kind required to bring deck of cards in the initial position? Is there a sequence of perfect shuffles which bring top card to the given position in a deck? The last question is the famous Elmsley's problem: is there a sequence of perfect shuffles that bring card at the position p to the position q? In this thesis we will also shortly describe group generated by the sequence of perfect shuffles and mention some applications of the concept of perfect shuffling.

Key words: cards shuffling, perfect shuffle, Elmsley's problem, $\langle \mathbf{I}, \mathbf{O} \rangle$ group

Sadržaj

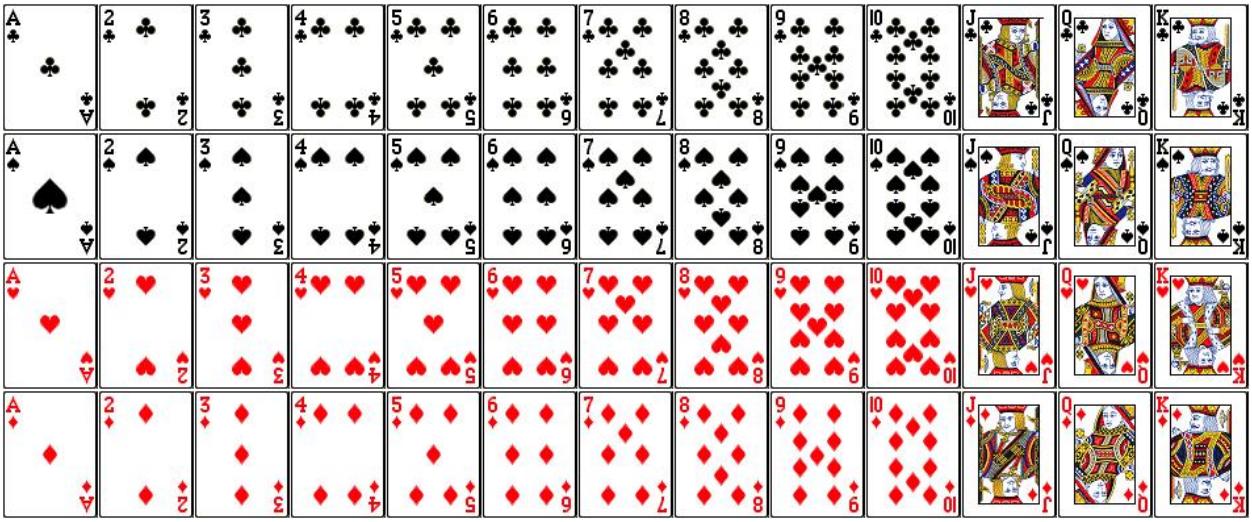
1 Uvod

Kartaška igra ili kartanje je društvena igra u kojoj igrači koriste igraće karte različitih tipova. Neke kartaške igre namijenjene su samo jednom igraču (primjerice *Pasijans* ili na engleskom jeziku *Solitaire*), dok u nekima može sudjelovati više osoba (*Poker*, *Belot*, *Bridž*, *Šnaps*, *Trešeta*,...).

Igraća karta je naziv za komad papira, kartona ili plastike koji služi za igranje kartaških igara. Skup igraćih karata naziva se *špil*. Osim za zabavu, igraće karte mogu služiti i za profesionalno kockanje.

Vjeruje se da su se prvim igraćim kartama služili u istočnoj Aziji (Koreja i Kina), a kasnije su odande, preko Indije i Egipta donesene u Europu. Danas se u različitim dijelovima svijeta koriste različiti špilovi igraćih karata za igre koje su karakteristične za to područje. Svaka igraća karta u špilu je različita, a označene su bojom, simbolima i različitim motivima po kojima se mogu lako složiti.

Jedan od najpoznatijih špilova je englesko-francuski špil koji se kod nas naziva i *standardni špil*, a prikazan je na slici 1.



Slika 1: Standardni špil od 52 karte

Sastoji se od 52 igraće karte u četiri boje: list (pik), romb (karo), djetelina (tref) i srce (herc). Vrijednosti karata su redom: $2, 3, 4, 5, 6, 7, 8, 9, 10$, J (dečko), Q (kraljica), K (kralj) i A (as).

U svakoj kartaškoj igri ključno je miješanje karata. Tim postupkom se osigurava element slučajnosti pri dijeljenju karata igračima. Ipak, postoje razni načini miješanja u kojima djelitelj karata (end. dealer) može utjecati na krajnji ishod igre, odnosno tijekom miješanja može namjestiti karte kako želi, ne bi li njegov tim pobijedio. Da bi se spriječilo varanje, mnoga kartaška pravila zahtijevaju da se špil karata nakon miješanja, a prije dijeljenja, presiječe. Presijecanje je postupak dizanja dijela karata s vrha špila i vraćanje tog dijela ispod drugog dijela špila, pri čemu su karte cijelo vrijeme licem okrenute prema dolje. Običaj je da dealer nakon miješanja daje špil na presijecanje protivniku sa svoje lijeve strane.

Postoje razni načini kako izmiješati karte. Najlakše je uvježbati takozvano "*rukom preko ruke*" miješanje (eng. *overhand shuffle*). To je tehnika u kojoj mješač prebacuje špil iz, primjerice, lijeve ruke u desnu tako da manji dio karata klizi s vrha špila lijeve ruke u desnu, i to između palca i kažiprsta. Postupak se ponavlja sve dok se sve karte ne prebace u desnu

ruku, a svaki novi dio karata koji dospije u desnu ruku biva položen na vrh ostalog dijela karata. Iako je ovo često korištena tehnika miješanja, ne upotrebljava se u kockarnicama jer takvo miješanje treba ponoviti čak 10000 puta da bi karte bile dobro promiješane! Isto vrijedi i za tzv. *Hindu* miješanje koje se izvodi na sličan način, a prakticira se u Indiji.
Podjela na hrpe (eng. *pile shuffle*) je miješanje koje se izvodi tako da se karte podijele u manje dijelove (na stolu) koji se zatim spoje u novi špil. Ovakvo miješanje je determinističko, ali omogućava dobru razdvojenost karata koje su u početnom špilu bile jedna do druge. *Početničko miješanje* (eng. *Corgi shuffle*) se izvodi tako da se karte raširе po stolu licem okrenute prema dolje, a zatim se dlanom ruke pomiču, odnosno kližu po stolu. Ovim postupkom karte se isprepliću, a dovoljna je jedna minuta takvog miješanja da bi karte bile dobro promiješane. *Monge* miješanje se izvodi tako da se špil smjesti npr. u lijevu ruku, karta s vrha špila se prebaci u desnu ruku, zatim se uzme druga karta s vrha špila i prebaci u desnu ruku na postojeću kartu, treća karta se s vrha špila prebaci ispod novog špila desne ruke, četvrta iznad itd.
Najpoznatije miješanje karata, a koje se često izvodi u kockarnicama jest *uguravanje* jednog dijela špila u drugi (eng. *riffle shuffle*). Izvodi se tako da špil karata podijelimo na dva dijela (ne nužno jednakobrojna). Jedan dio špila stavimo u lijevu ruku, a drugi u desnu tako da je duži rub karata okrenut prema nama. Jedan kraći rub karata zahvatimo srednjim prstom, prstenjakom i malim prstom, a drugi palcem. Pomoću kažiprsta pritišćemo karte s vanjske strane. Zatim približimo dva dijela špila i pomičući palčeve prema gore puštamo karte da padaju na stol, istovremeno iz lijeve i desne ruke. Prilikom padanja karte će se ispreplitati. Da bi se ovom tehnikom karte dobro izmiješale, matematičari su dokazali da postupak uguravanja treba ponoviti sedam puta!
Najteži oblik miješanja uguravanjem je takozvano *savršeno miješanje*, a mogu ga pravilno izvesti samo dobro uvježbani mješači. Pri takvom uguravanju, karte se dijele na dva jednakobrojna dijela, a zatim se dijelovi isprepliću tako da se između svake dvije karte istog dijela špila nalazi točno jedna karta iz drugog dijela. Savršeno miješanje karata se najprije pojavljivalo u knjigama koje su opisivale metode varanja u kartaškim igrama. Prvi opis savršenog miješanja napisao je anonimni Britanac 1726. godine u knjizi "Umjetnost i tajne modernih igara na sreću". Kasnije je savršeno miješanje bilo poznato među mađioničarima pod nazivom *Faro shuffle*, jer je takva metoda miješanja služila za varanje u igri *Faro* [3]. U brojnim trikovima s kartama poznati mađioničari C.T. Jordan, Nelson Downs i mnogi drugi koristili su upravo takvo miješanje jer omogućava premještanje karte na željenu poziciju. Više od 300 godina kockari i mađioničari diljem svijeta proučavali su svojstva savršenog miješanja, a zanimljivo je da se ta metoda može primijeniti u raznim disciplinama, posebice u računalnoj znanosti [6].
U ovom radu bavit ćemo se raznim problemima o savršenom miješanju koji su tijekom povijesti privlačili pažnju mnogih modernih matematičara i mađioničara. Zanimat će nas odgovori na sljedeća pitanja: Koliko savršenih miješanja je potrebno da se sve karte špila vrate u početnu poziciju? Postoje li kombinacije savršenih miješanja koje će kartu s vrha špila dovesti na unaprijed odabranu poziciju? Kako savršenim miješanjem dovesti bilo koju kartu na vrh špila? Posljednjim pitanjem najviše se bavio škotski mađioničar i programer Alex Elmsley davne 1957. godine. Taj problem danas nosi njegovo ime, a može se i generalizirati ukoliko umjesto dovođenja karte na vrh špila želimo dovesti kartu na bilo koju poziciju u špilu.

2 Savršeno miješanje

Kao što smo spomenuli u uvodu, pri savršenom miješanju karte se dijele na dva jednakobrojna dijela, a zatim se dijelovi isprepliću tako da se između svake dvije karte istog dijela špila nalazi točno jedna karta iz drugog dijela. Razlikujemo dva tipa savršenog miješanja. **Out** miješanje (**O**) je savršeno miješanje u kojem karta na vrhu špila nakon miješanja ostaje na vrhu, te **in** miješanje (**I**) kod kojeg karta na vrhu špila nakon miješanja završi na drugom mjestu, odnosno odmah ispod gornje karte. Na slikama 2 i 3 prikazana su **out** i **in** miješanja špila od 10 karata. U početnom špilu karte su označene redom brojevima $0, 1, 2, \ldots, 9$ od vrha prema dnu.

Slika 2: **Out** miješanje

Slika 3: **In** miješanje

2.1 Osnovna svojstva savršenog miješanja

U nastavku rada bavit ćemo se isključivo sa špilom koji sadrži $2n$ karata. Gornju kartu ćemo označavati s 0 i reći da je ta karta na nultoj poziciji, sljedeću s 1 i reći da je na prvoj poziciji,... i tako do donje koju označavamo s $2n-1$.

Propozicija 1 *Neka je u špilu veličine* $2n$ ***out*** *miješanje kartu s* i*-te pozicije prebacilo na poziciju* $\mathbf{O}(i)$*. Tada vrijedi*

$$\mathbf{O}(i) = \begin{cases} 2i \ (\mathrm{mod}\, 2n-1) & za \ \ 0 \leq i < 2n-1, \\ 2n-1 & za \ \ i = 2n-1. \end{cases} \tag{1}$$

Dokaz: Najprije razmotrimo kako **out** miješanje utječe na karte iz gornje polovice špila. Tako ćemo privremeno izbjeći slučaj $\mathbf{O}(i) < i$.
Karta na poziciji i ima i karata iznad sebe pa će nakon **out** miješanja nova pozicija biti za i veća od početne tj. $\mathbf{O}(i) = i + i = 2i = 2i (\mathrm{mod}\, 2n-1)$ za $0 \leq i \leq n-1$. Za karte iz donje polovice špila vrijedi $\mathbf{O}(n) = 1$, $\mathbf{O}(n+1) = 3, \ldots$, $\mathbf{O}(2n-2) = 2n-3$ i, na kraju, $\mathbf{O}(2n-1) = 2n-1$. Preciznije:

$$\mathbf{O}(n+j) = 2j+1, \quad j = 0, 1, \ldots, n-1,$$

odnosno

$$\mathbf{O}(i) = 2(i-n)+1 = 2i-(2n-1), \quad i = n, n+1, \ldots, 2n-1.$$

Ovo možemo pisati kao $\mathbf{O}(i) = 2i (\mathrm{mod}\, 2n-1)$ za $n \leq i < 2n-1$ i $\mathbf{O}(i) = 2n-1$ za $i = 2n-1$. □

Primjerice, za $2n = 10$ karte s početnim poretkom 0,1,2,3,4,5,6,7,8,9 nakon **out** miješanja su u poretku 0,5,1,6,2,7,3,8,4,9 (slika 2).

Propozicija 2 *U špilu s* $2n$ *karata, jedno* ***in*** *miješanje premjestit će kartu s* i*-te pozicije na poziciju*

$$\mathbf{I}(i) = 2i+1 \ (\mathrm{mod}\, 2n+1) \ \ 0 \leq i \leq 2n-1. \tag{2}$$

Dokaz: Razmotrimo najprije utjecaj **in** miješanja na karte iz gornje polovice špila. Karta na poziciji i će se nakon **in** miješanja spustiti za $i+1$ mjesta tj. $\mathbf{I}(i) = i + i + 1 = 2i + 1 = 2i + 1 (\bmod 2n+1)$ za $0 \leq i \leq n-1$. Nadalje, vrijedi $\mathbf{I}(n) = 0$, $\mathbf{I}(n+1) = 2$, $\mathbf{I}(n+3) = 4$, ... $\mathbf{I}(2n-2) = 2(n-2)$ i $\mathbf{I}(2n-1) = 2(n-1)$. Pišemo

$$\mathbf{I}(n+j) = 2j, \quad j = 0, 1, \ldots, n-1,$$

odnosno

$$\mathbf{I}(i) = 2(i-n) = 2i + 1 - (2n+1) = 2i + 1 (\bmod 2n+1), \quad i = n, n+1, \ldots, 2n-1.$$

□

U špilu veličine 10, karte s poretkom 0,1,2,3,4,5,6,7,8,9 će nakon jednog **in** miješanja biti u poretku 5,0,6,1,7,2,8,3,9,4 (slika 3).

Primijetimo kako **out** miješanje ostavlja gornju i donju kartu na istim mjestima, dok se preostalih $2n-2$ karata miješaju kao u **in** miješanju. Stoga se svojstva ponovljenih **in** miješanja mogu opisati pomoću svojstava ponovljenih **out** miješanja.

2.2 Vraćanje špila u početno stanje

Za špil s $2n$ karata želimo naći najmanji broj istovrsnih miješanja (**out** ili **in**) koje će karte dovesti do početne pozicije. S obzirom da smo ranije objasnili vezu između **out** i **in** miješanja, bit će dovoljno promotriti samo **out** miješanje. Neka je $k \in \mathbb{N}$. S $\mathbf{O}^k$ označit ćemo k uzastopnih **out** miješanja. Iz formule (1) slijedi da je pozicija pojedine karte nakon k **out** miješanja dana formulom:

$$\mathbf{O}^k(i) = \begin{cases} 2^k i \,(\bmod 2n-1) & \text{za } \ 0 \leq i < 2n-1, \\ 2n-1 & \text{za } \ i = 2n-1. \end{cases} \tag{3}$$

Špil će se vratiti u početnu poziciju nakon k **out** miješanja ako i samo ako vrijedi $\mathbf{O}^k(i) = i \,(\bmod 2n-1)$, za $0 \leq i < 2n-1$. Iz formule (3) vidimo da je to moguće jedino ako je $2^k \equiv 1 \,(\bmod 2n-1)$. Najmanji takav k zovemo *red* od $2 \,(\bmod 2n-1)$. Npr. za 52 karte uzastopne potencije od $2 \,(\bmod 51)$ su 2, 4, 8, 16, 32, 13, 26, 1 itd. Kako je $2^8 = 256 \equiv 1 \,(\bmod 51)$, to znači da će osam uzastopnih **out** miješanja vratiti špil u početnu poziciju. Kod uzastopnih **in** miješanja taj broj je puno veći. Naime, potrebno je 52 takva miješanja da bi se karte vratile u početnu poziciju ($2^{52} \equiv 1 \,(\bmod 53)$, a 2 je *primitivni korijen* modulo 53 pa je 52 najmanja takva potencija).

veličina špila $2n$	2	4	6	8	10	12	14	16	18	20	22	24	26
$ord_2(2n-1)$	1	2	4	3	6	10	12	4	8	18	6	11	20
veličina špila $2n$	28	30	32	34	36	38	40	42	44	46	48	50	52
$ord_2(2n-1)$	18	28	5	10	12	36	12	20	14	12	23	21	8

Tablica 1: Vrijednosti od $ord_2 \,(\bmod 2n-1)$ za špil veličine $2n$, $n \leq 52$.

Željeli bismo naći formulu koja za špil s $2n$ karata daje najmanji broj **out** miješanja koja će vratiti špil u početno stanje. No, iz tablice 1 vidimo da to nije lak posao. Primijetimo da se broj potrebnih **out** miješanja za povratak špila u početno stanje ne povećava ukoliko povećavamo broj karata u špilu. Ranije smo pokazali da je za špil od 52 karte potrebno 8

miješanja, ali za špil od 38 karata taj broj iznosi čak 36! Jedino što odmah možemo zaključiti jest da je za špil s 2^k karata potrebno k **out** miješanja! Pitamo se postoje li jako veliki prirodni brojevi $2n$ takvi da je 2 primitivan korijen modulo $2n-1$. To je poznata hipoteza austrijskog matematičara Emila Artina koja se već dugi niz godina proučava i pokušava riješiti. Poznato je da je Artinova hipoteza točna ukoliko je točna Generalizirana Riemannova hipoteza [4]. Zanimljivo je, ali i pomalo mučno, što vrlo jednostavna pitanja o svojstvima savršenih miješanja mogu dovesti do najznačajnijih hipoteza u modernoj matematici!

3 Elmsleyev problem

Alex Elsmsley (1929 - 2006) je među mađioničarima uglavnom poznat po osmišljavanju raznih trikova s kartama. Mađioničarstvom se počeo baviti već u tinejdžerskim danima, oko 1946. godine. Poznat je po lažnom prebrojavanju karata koje je u literaturi poznato kao *Ghost count*, a kasnije je to prebrojavanje nazvano po njemu: *Elmsleyevo prebrojavanje*. No, Elmsley je bio znanstvenik. Studirao je matematiku i fiziku na sveučilištu u Cambridgeu, a zaposlio se kao programer.
Kod savršenog miješanja najviše su ga zanimala dva problema: može li se savršenim miješanjem karta s vrha špila dovesti na neku drugu, unaprijed zadanu, poziciju i obratno, može li se savršenim miješanjem karta s neke pozicije p dovesti na vrh špila? Prvi problem je uspješno riješio, dok je drugi, danas poznat pod nazivom *Elmsleyev problem*, postavio 1957. godine, te je trebalo oko 50 godina da ga netko uspješno riješi [1, 11]. U ovom odjeljku ćemo pokazati kako se rješavaju ta dva problema.

3.1 Stavljanje karte s vrha na proizvoljnu poziciju

Zahvaljujući Elsmsleyu, ponovljenim postupcima savršenih **in** i **out** miješanja vješti mješači mogu dovesti kartu s vrha špila na bilo koju poziciju u špilu. Za početak, označimo proizvoljnu poziciju s p. Elmsley je taj broj promatrao u binarnom brojevnom sustavu, npr. poziciju 9 označio je s 1001. U takvom zapisu 0 predstavlja **out**, a 1 **in** miješanje, što znači da za premještanje gornje karte na poziciju 9 (na 10. mjesto gledajući od vrha špila) trebamo uzastopce izvesti **in**, **out**, **out**, **in** miješanja.
U nastavku ćemo prikazati detaljan postupak koji opravdava Elmsleyevu proceduru.

Sa $\mathbf{O}(i)$ i $\mathbf{I}(i)$ redom označimo poziciju špila nakon **out** i **in** miješanja. Pretpostavit ćemo da se prije primjene bilo kojeg savršenog miješanja karta broj 0 ne nalazi u donjoj polovici špila. Time ćemo izbjeći kompliciranе izraze koji uključuju kongruencije. Nadalje, uzmimo da je špil dovoljno velik tako da možemo pisati

$$\mathbf{O}^k(i) = 2^k i \qquad \text{i} \qquad \mathbf{I}^k(i) = 2^k(i+1) - 1. \tag{4}$$

S obzirom da se bavimo premještanjem karte s vrha špila, imamo $i = 0$ pa su ove formule još jednostavnije. Jasno je da niz **out** i **in** miješanja koji kartu s vrha špila dovodi na poziciju p ne može početi s **out** miješanjem jer ono ne mijenja poziciju te karte. Stoga ćemo pretpostaviti da niz počinje s a uzastopnih **in** miješanja, $a \geq 1$. Slijedi $\mathbf{I}^a(0) = 2^a - 1$. Zatim, za $b \geq 1$ čitajući niz slijeva na desno, imamo

$$\mathbf{I}^a\mathbf{O}^b(0) = 2^{a+b} - 2^b,$$

dodatno, za $c \geq 1$

$$\mathbf{I}^a\mathbf{O}^b\mathbf{I}^c(0) = 2^{a+b+c} - 2^{b+c} + 2^c - 1$$

i tako dalje.

Primijetimo da je broj $\mathbf{I}^a(0) = 2^a - 1$ ujedno i broj karata iznad karte broj 0 nakon a **in** miješanja.

Imamo

$$\begin{aligned}\mathbf{I}^a(0) &= 2^a - 1 \\ &= 2^{a-1} + 2^{a-2} + \cdots + 2 + 1,\end{aligned}$$

$$\begin{aligned}\mathbf{I}^a\mathbf{O}^b(0) &= 2^{a+b} - 2^b \\ &= 2^{a+b} - 1 - (2^b - 1) \\ &= 2^{b+a-1} + 2^{b+a-2} + \cdots + 2^{b+1} + 2^b + 2^{b-1} + \cdots + 2 + 1 - 2^{b-1} - 2^{b-2} - \cdots - 2 - 1 \\ &= 2^{b+a-1} + 2^{b+a-2} + \cdots + 2^{b+1} + 2^b\end{aligned}$$

itd. Ovi izrazi sugeriraju da se broj karata iznad karte broj 0 izrazi binarno:

$$\begin{aligned}\mathbf{I}^a(0) &= (\underbrace{\mathbf{II}\ldots\mathbf{I}}_{a})(0) \\ &= \underbrace{11\ldots1}_{a}{}_{(2)},\end{aligned}$$

odnosno

$$\begin{aligned}\mathbf{I}^a\mathbf{O}^b(0) &= (\underbrace{\mathbf{II}\ldots\mathbf{I}}_{a}\underbrace{\mathbf{OO}\ldots\mathbf{O}}_{b})(0) \\ &= \underbrace{11\ldots1}_{a}\underbrace{00\ldots0}_{b}{}_{(2)}\end{aligned}$$

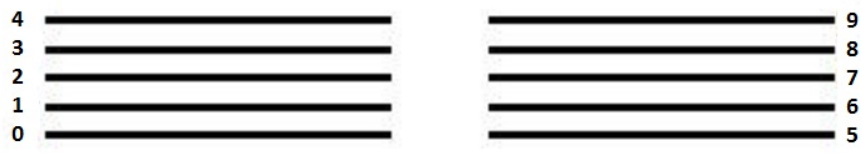
itd. Induktivno dolazimo do pravila kako **out** i **in** miješanjima kartu s vrha špila premjestiti na poziciju p: broj p treba zapisati u binarnom brojevnom sustavu. Jedinice treba zamijeniti s oznakom za **in** miješanje, a nule s oznakom za **out** miješanje. Čitajući niz slijeva na desno, dobivamo niz miješanja koji kartu s vrha špila dovode na poziciju p. Obratno, ako imamo niz **in** i **out** miješanja, pozicija karte koja je inicijalno bila na vrhu špila dobivamo tako da svako **in** miješanje u nizu zamijenimo s jedinicom, a svako **out** miješanje s nulom. Dobiveni broj iz binarnog zapisa prebacimo u dekadski i taj rezultat predstavlja poziciju karte.

3.2 Vraćanje karte na vrh špila

U radu [6] autori Diaconis, Graham i Kantor uvode pojam $\langle \mathbf{I}, \mathbf{O} \rangle$ grupe generirane proizvoljnim **in** i **out** miješanjima. Iz njihovih rezultata slijedi da za bilo koje p i q postoji niz **in** i **out** miješanja koji kartu s pozicije p premješta na poziciju q. Ipak, ovaj postupak ne daje uvid u najkraći način za takvo premještanje. Mi ćemo pokazati metodu koja pronalazi sva savršena miješanja kojima se karta s pozicije p prebacuje na poziciju q koristeći tzv. *inverzna miješanja*. Nizove koje ćemo konstruirati općenito neće biti najkraći.

3.2.1 Inverzna miješanja

Inverzna miješanja $\mathbf{I^{-1}}$ i $\mathbf{O^{-1}}$ redom poništavaju učinak **in** i **out** miješanja. Uz pomoć slike 4 prikazat ćemo kako izgledaju inverzna miješanja.



Slika 4: Deset karata naizmjenično podijeljenih nakon **out** miješanja.

Za izvršiti $\mathbf{O^{-1}}$, karte ćemo dijeliti u dvije hrpe s licem okrenutim prema gore. Zatim desnu hrpu stavimo na lijevu (karta broj 9 sada je na vrhu, a 0 je na dnu). Za izvršiti $\mathbf{I^{-1}}$ radimo isto, ali lijevu hrpu stavljamo na desnu. Oba slučaja završavamo tako da preokrenemo špil licem prema dolje. Navedena miješanja matematički ćemo zapisati kao permutaciju skupa $\{0, 1, 2, \ldots, 2n-1\}$:

$$\mathbf{O}^{-1}(i) = \begin{cases} \lfloor \frac{i}{2} \rfloor, & \text{za } i \text{ paran}, \\ \lfloor \frac{i}{2} \rfloor + n, & \text{za } i \text{ neparan}, \end{cases} \tag{5}$$

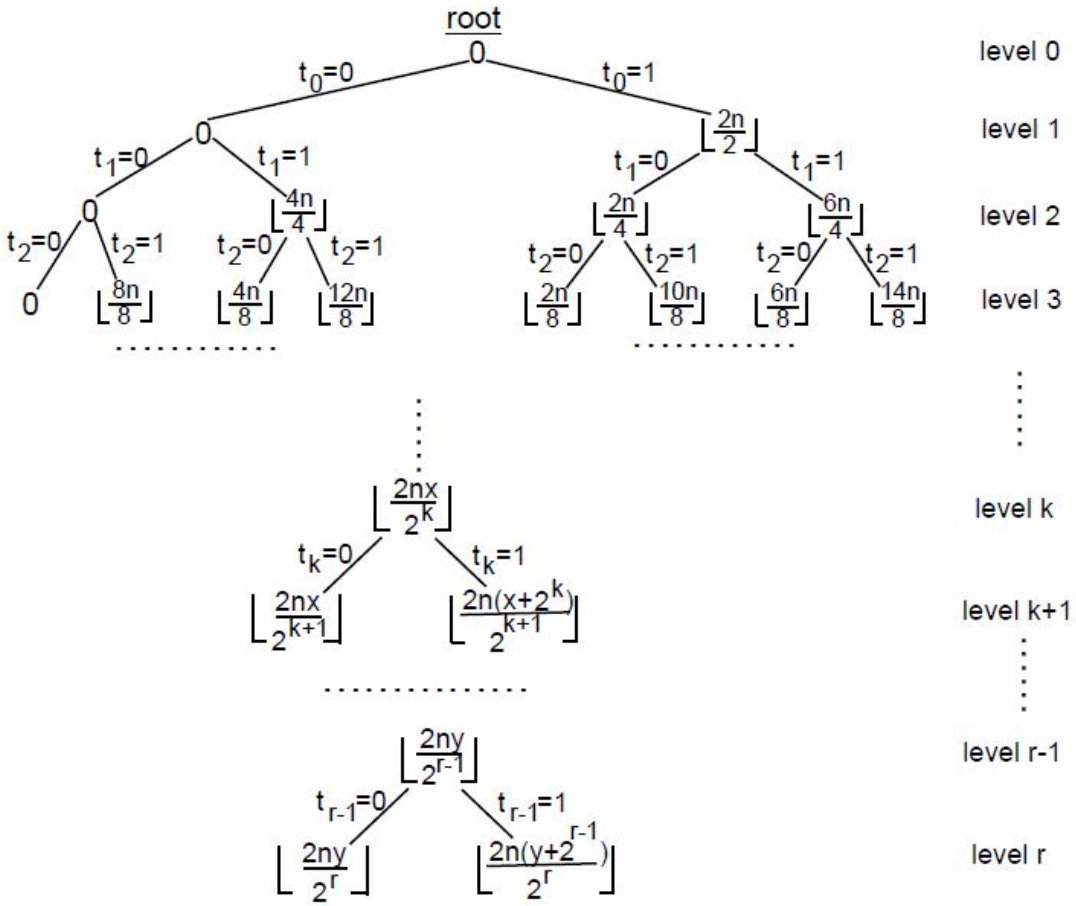
$$\mathbf{I}^{-1}(i) = \begin{cases} \lfloor \frac{i}{2} \rfloor + n, & \text{za } i \text{ paran}, \\ \lfloor \frac{i}{2} \rfloor, & \text{za } i \text{ neparan}. \end{cases} \tag{6}$$

Ako se nakon k **out** miješanja i j **in** miješanja špil vraća u početnu poziciju, tada je $\mathbf{O}^{-1} = \mathbf{O}^{k-1}$ i $\mathbf{I}^{-1} = \mathbf{I}^{j-1}$, što znači da svaki raspored karata u špilu koji možemo postići s **in** i **out** miješanjima, možemo postići i s njima inverznim miješanjima, i obrnuto.
Sada ćemo ukratko objasniti da postoji niz **in** i **out** miješanja koje kartu s pozicije p premješta na poziciju q. Najprije ćemo nizom inverznih miješanja dovesti kartu s pozicije p na vrh špila: podijelimo špil na dvije hrpe, zatim hrpu u kojoj nije karta broj p stavimo na drugu hrpu. Tako će, kada okrenemo karte licem prema dolje, ta karta biti u gornjoj polovici. Ako nastavimo taj postupak, nakon najviše r miješanja ($2^{r-1} < 2n \leq 2^r$) karta s pozicije p će doći na vrh špila. S te pozicije znamo kartu prebaciti na poziciju q primjenom Elmsleyeve binarne procedure koju smo pojasnili u prethodnom potpoglavlju. Takav postupak može dati jako dugačak niz miješanja, no barem smo sigurni da takav niz postoji. Štoviše, pokazat ćemo kako brže i učinkovitije dovesti bilo koju kartu na vrh špila.
Elmsleyev problem dovođenja karte na vrh špila riješit ćemo pronalaženjem što kraćih nizova **in** i **out** miješanja. Kao što smo vidjeli u dijelu 2, **in** i **out** miješanja definirana su

s različitim modulima, a s njima nije lako raditi. Umjesto toga, radit ćemo s inverznim miješanjima, a ona uključuju dijeljenje s 2, računanje *poda* i moguće dodavanje n-a, koje ovisi o parnosti broja i. Pitanje parnosti ćemo za početak zanemariti te ćemo kroz cijeli postupak upotrebljavati jednakost $\lfloor \frac{1}{2} \lfloor x \rfloor \rfloor = \lfloor \frac{x}{2} \rfloor$.

3.2.2 Konstrukcija stabla

Izgradit ćemo binarno stablo $T(2n)$ s $r+1$ razina ($2^{r-1} < 2n \leq 2^r$). Korijen v_0 je na razini 0 i označen je s $\lambda(v_0) = 0$. Općenito, ako je vrh stabla $T(2n)$ na razini i označen s $\lambda(v) = m$, dva "djeteta" od v bit će označena s $\lfloor \frac{m}{2} \rfloor$ i $\lfloor \frac{m}{2} \rfloor + n$. Zapisat ćemo to ovako: $\lfloor \frac{m}{2} + t_i n \rfloor$, gdje je $t_i = 0$ ili $t_i = 1$, za $0 \leq i \leq r$ (vidi sliku 5).



Slika 5: Stablo $T(2n)$

Ako je $t = \sum_{i=0}^{r-1} t_i 2^i$, onda je vrijednost vrha - lista v_t koja odgovara izboru $(t_0, t_1, \ldots, t_{r-1})$ počevši od korijena prema dolje je $\lambda(v_t) = \lfloor \frac{2nt}{2^r} \rfloor$. Općenito, vrijednost vrha v na razini k koja odgovara izboru $(t_0, t_1, \ldots, t_{k-1})$ je $\lambda(v) = \lfloor \frac{2nt(k)}{2^k} \rfloor$, gdje je $t(k) = \sum_{i=0}^{k-1} t_i 2^i$.

3.2.3 Veza između stabla i savršenog miješanja

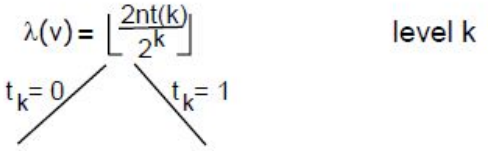
Za $t = \sum_{i=0}^{r-1} t_i 2^i$, ukoliko zapišemo $2nt = \sum_{i\geq 0} s_i 2^i$ u binarnom sustavu, imamo:

$$\left\lfloor \frac{2nt}{2^k} \right\rfloor = \left\lfloor \sum_{i\geq k} s_i 2^{i-k} \right\rfloor = \ldots s_{k+2}s_{k+1}s_k \ (2)$$

S druge strane vrijedi

$$\begin{aligned}\left\lfloor \frac{2nt(k)}{2^k} \right\rfloor &= \left\lfloor \frac{2n}{2^k} \left(\sum_{i=0}^{k-1} t_i 2^i + \sum_{i\geq k} t_i 2^i) \right) \right\rfloor \\ &= \left\lfloor \frac{2n}{2^k}(t(k) + 2^k X) \right\rfloor \\ &= 2nX + \left\lfloor \frac{2nt(k)}{2^k} \right\rfloor\end{aligned}$$

za neki cijeli broj $X \geq 0$. Sada je jasno da je parnost broja$\lfloor \frac{2nt(k)}{2^k} \rfloor$ određena sa s_k i ona odlučuje koje inverzno miješanje iz proizvoljnog vrha stabla trebamo izabrati.



Slika 6: Opća grana

Ako je $\lfloor \frac{2nt(k)}{2^k} \rfloor$ paran broj, tada $t_k = 0$ predstavlja inverzno **out** miješanje, a $t_k = 1$ inverzno **in** miješanje. Ako je $\lfloor \frac{2nt(k)}{2^k} \rfloor$ neparan , $t_k = 0$ predstavlja inverzno **in** miješanje, a $t_k = 1$ inverzno **out** miješanje (pogledati izraze (5), (6) i sliku 6).
Miješanje u vrhu stabla određeno je s $u_k = s_k + t_k \,(\mathrm{mod}\, 2)$ gdje je $u_k = 0 \leftrightarrow \mathbf{O^{-1}}$ i $u_k = 1 \leftrightarrow \mathbf{I^{-1}}$.

3.2.4 Konstrukcija niza inverznih miješanja

Najprije ćemo pronaći niz inverznih miješanja koji će kartu s vrha špila dovesti na poziciju p. U tu svrhu, stavimo

$$\left\lfloor \frac{2nt}{2^r} \right\rfloor = p,$$

a to povlači

$$\frac{2^r p}{2^n} \leq t < \frac{2^r(p+1)}{2n}. \tag{7}$$

S obzirom da vrijedi $2^{r-1} < 2n \leq 2^r$, zaključujemo da za svaki p postoji najmanje jedan, a najviše dva cijela broja koja zadovoljaju nejednakost (7). Točnije, ako proširimo $\frac{p+1}{2n}$ (u bazi 2) kao

$$\frac{p+1}{2n} = .\alpha_1\alpha_2\alpha_3\ldots,$$

tada možemo odabrati t kao $t = \sum_{i=1}^{r} \alpha_i 2^{r-i} = \alpha_1\alpha_2 \dots \alpha_3$ (u bazi 2), odnosno $t = \lfloor \frac{(p+1)2^r}{2n} \rfloor$, $0 < p < 2n-1$. Za $p = 0$ uzmimo $t = 0$, a za $p = 2n-1$ uzmimo $t = 2^r - 1$. Možemo pisati

$$s' = 2nt - 2^r p = s_{r-1}s_{r-2}\dots s_1 s_0\ {}_{(2)}.$$

Sada, pomoću $2nt = \sum_{i\geq 0} s_i 2^i$ određujemo koji se od $\mathbf{O}^{-1}$ ili $\mathbf{I}^{-1}$ provodi u određenom koraku.

S obzirom da gornji opis određuje niz inverznih miješanja za prebacivanje karte s vrha špila na proizvoljnu poziciju, čitajući taj niz s lijeva na desno i mijenjajući inverzna miješanja s običnim **in** i **out** miješanjima, dobivamo niz koji kartu s pozicije p prebacuje na vrh špila.

Primjer 3.1 *Ako u standardnom špilu,* $2n = 52$*, uzmemo* $p = 36$*, tada je* $r = 6$*,* $t = \lfloor \frac{37\cdot 64}{52} \rfloor = 45 = 101101\ {}_{(2)}$*,* $s' = 2340 - 2304 = 36 = 100100\ {}_{(2)}$*. Slijedi da je* $u = 001001$ *pa je* **OOIOOI***, čitajući slijeva na desno, niz savršenih miješanja koji kartu s pozicije* 36 *vraća na vrh špila.*

Ranije smo vidjeli da mogu postojati dvije vrijednosti za t koje zadovoljavaju nejednakost (7). Jedan takav niz miješanja imat će duljinu r, dok će drugi niz biti kraći od r. Ilustrirajmo to na sljedećem primjeru.

Primjer 3.2 *Za* $2n = 52$ *i* $p = 30$ *dobivamo* $r = 6$*, a s obzirom da vrijedi* $\lfloor \frac{52\cdot 37}{64} \rfloor = 30 = \lfloor \frac{52\cdot 38}{64} \rfloor$*, možemo uzeti* $t = 37$ *ili* $t = 38$*. Za* $t = 37 = 100101\ {}_{(2)}$ *imamo* $s' = 1924 - 1920 = 4 = 000100\ {}_{(2)}$ *i* $u = 100001\ {}_{(2)}$*, što predstavlja niz miješanja* **IOOOOI***. Za* $t = 38 = 100110\ {}_{(2)}$ *dobivamo* $s' = 1976 - 1920 = 56 = 111000\ {}_{(2)}$ *i* $u = 011110\ {}_{(2)}$*, što predstavlja niz* **OIIIIO** *koji se može skratiti na* **OIIII** *jer* ***out*** *miješanje ne mijenja položaj karte na vrhu špila. Dakle, postoji niz od 5 miješanja koji kartu s pozicije 30 dovodi na vrh špila.*

Valja još spomenuti da u slučaju $2n = 2^r$ vrijedi $t = p$ pa je $s' = 0$, tj. $s_i = 0$ za svaki i. Stoga je dovoljno izračunati t i binarno ga zapisati.

3.2.5 Algoritam

Napišimo algoritam koji kartu s pozicije p prebacuje na vrh špila.

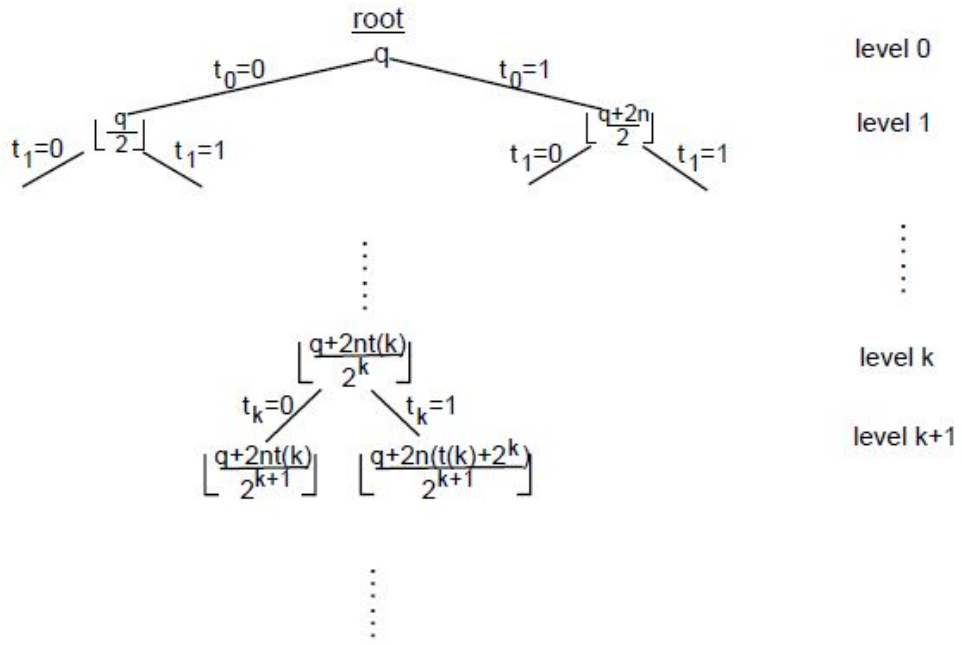
`ULAZ: veličina špila` $2n$, `pozicija karte` p

- `izračunaj` r `tako da` $2^{r-1} < 2n \leq 2^r$
  - `ako` $0 < p < 2n-1$ `stavi` $t = \lfloor \frac{(p+1)2^r}{2n} \rfloor$
  - `ako` $p = 0$ `stavi` $t = 0$
  - `ako` $p = 2n-1$ `stavi` $t = 2^r - 1$
- `zapiši` t `binarno:` $t = t_{r-1}t_{r-2}\dots t_1 t_0$
- `zapiši` $s' = 2nt - 2^r p$ `binarno:` $s' = s_{r-1}s_{r-2}\dots s_1 s_0$
- `računaj sume` u_i `binarno:` $u_i = t_i + r_i$, $i = 0, 1, \dots, r-1$

`IZLAZ: niz` $u_1, u_2, \dots, u_{r-1}$ `gdje` 0 `u nizu znači OUT, a` 1 `IN.`

3.3 Pomicanje karte s pozicije p na poziciju q

Za početak ćemo prikazati stablo $T_q(2n)$ s označenim vrhovima, slično kao na slici 5, ali s korijenom označenim s q umjesto 0 (slika 7).



Slika 7: Stablo $T_q(2n)$

Sada trebamo pronaći $t = t_{r-1} \dots t_1 t_0$ $_{(2)}$ takav da vrijedi

$$\lfloor \frac{q + 2nt}{2^r} \rfloor = p.$$

Tada je

$$\frac{2^r p - q}{2n} \leq t < \frac{2^r (p+1) - q}{2n}.$$

Znamo otprije da takav t postoji, odnosno da mogu postojati najviše dva takva broja čiji je binarni zapis duljine najviše r, a koji zadovoljavaju prethodnu nejednakost.

Računamo

$$s' = 2nt + q - 2^r p = s_{r-1} s_{r-2} \dots s_1 s_0 \ _{(2)}$$

i binarne sume

$$t_{r-1} + s_{r-1},\ t_{r-2} + s_{r-2},\ \dots,\ t_1 + s_1,\ t_0 + s_0.$$

Dobivene vrijednosti prebacimo u niz **in** i **out** miješanja i gotovi smo!

Primjer 3.3 *Neka je zadano* $2n = 52$, $p = 51$, $q = 1$. *Dakle, želimo kartu na zadnjoj poziciji u špilu prebaciti na drugu poziciju. Dobivamo* $r = 6$ *i* $\frac{64 \cdot 51 - 1}{52} < \frac{64 \cdot 52 - 1}{52}$ *pa je* $t = 63 = 111111$ $_{(2)}$. *Nadalje,* $s' = 3277 - 3264 = 13 = 001101$ $_{(2)}$. *Uzimajući binarni zbroj po komponentama brojeva* t *i* s' *dobivamo niz miješanja* **IIOOIO**. *U ovom slučaju ne smijemo izostaviti* ***out*** *miješanje na zadnjem mjestu niza jer ono ne čuva položaj karata koje nisu na vrhu ili na dnu.*

Napomena 3.1 *Iako su Diaconis i Graham u svome radu [1] tvrdili da njihov algoritam za prebacivanje karte s pozicije q na poziciju p daje najkraći niz savršenih miješanja, programer Rudolf Fleischer je ustanovio da to ipak nije točno, a svoje rezultate predstavio je 2017. godine na konferenciji u Tokiju [2]. Kao protuprimjer uzeo je špil od* 52 *karte, te je kartu s pozicije* 39 *htio prebaciti na vrh špila. Algoritam iz pododjeljka 3.2.5 kao rješenje daje niz* ***OOOIOI****, a najkraći niz je* ***II****. To se lako može provjeriti koristeći simulator koji je kreirao Nate Kiewel [10].*

4 Grupa $\langle \mathbf{I}, \mathbf{O} \rangle$

U pododjeljku 3.2 spomenuli smo grupu $\langle \mathbf{I}, \mathbf{O} \rangle$ generiranu proizvoljnim **in** i **out** miješanjima. Njome su se bavili Diaconis, Graham i Kantor davne 1983. godine u radu [6] pa ćemo izdvojiti neke njihove rezultate.
Oba miješanja, **in** i **out**, čuvaju centralnu simetriju, tj. karte nakon miješanja odlaze na pozicije simetrične s obzirom na sredinu špila. To znači da je $\langle \mathbf{I}, \mathbf{O} \rangle$ podgrupa grupe centralnosimetričnih permutacija, a ova je pak izomorfna Weylovoj grupi B_n svih $n \times n$ permutacijskih matrica čiji su elementi $0, \pm 1$.
Ekvivalentno, to je grupa svih $n!2^n$ simetrija n-dimenzionalnog oktaedra čiji su vrhovi $\pm e_1, \pm e_2, \ldots, \pm e_n$, gdje su $e_1, e_2, \ldots, e_n$ vektori standardne baze u $\mathbb{R}^n$. Parovi $\{e_i, -e_i\}$ odgovaraju parovima karata koje su u centralno simetričnom položaju.
Spomenut ćemo i neke homomorfizme grupe B_n. Za $g \in B_n$ $\operatorname{sgn}(g)$ je predznak od g kao permutacije od $2n$ karata, a $\overline{\operatorname{sgn}}(g)$ je predznak od g kao predznak permutacije od n centralnosimetričnih parova. Nadalje, preslikavanje koje elementu $g \in B_n$ pridružuje $\operatorname{sgn}(g)\overline{\operatorname{sgn}}(g)$ je homomorfizam u $\{\pm 1\}$ čija je jezgra Weylova grupa D_n.

Teorem 4.1 *Neka je $\langle \boldsymbol{I}, \boldsymbol{O} \rangle$ permutacijska grupa generirana s* ***in*** *i* ***out*** *miješanjima špila koji sadrži $2n$ karata.*
1.) Ako je $n \equiv 2 \pmod 4$ i $n > 6$ tada je $\langle \boldsymbol{I}, \boldsymbol{O} \rangle$ izomorfna grupi B_n i $|\langle \boldsymbol{I}, \boldsymbol{O} \rangle| = n!2^n$. Ako je $n = 6$, tada je $\langle \boldsymbol{I}, \boldsymbol{O} \rangle$ poludirektni produkt grupe $\mathbb{Z}_2^6$ i projektivne linearne grupe $PGL(2, 5)$.
2.) Ako je $n \equiv 1 \pmod 4$ i $n \geq 5$, tada je $\langle \boldsymbol{I}, \boldsymbol{O} \rangle$ jezgra od $\overline{sgn}$ i $|\langle \boldsymbol{I}, \boldsymbol{O} \rangle| = n!2^{n-1}$.
3.) Ako je $n \equiv 3 \pmod 4$, tada je $\langle \boldsymbol{I}, \boldsymbol{O} \rangle$ izomorfna grupi D_n i $|\langle \boldsymbol{I}, \boldsymbol{O} \rangle| = n!2^{n-1}$.
4.) Ako je $n \equiv 0 \pmod 4, n \geq 12$ i n nije potencija broja 2, tada je $\langle \boldsymbol{I}, \boldsymbol{O} \rangle$ presjek jezgri od sgn i $\overline{sgn}$ i $|\langle \boldsymbol{I}, \boldsymbol{O} \rangle| = n!2^{n-2}$. Ako je $2n = 24$, tada je $\langle \boldsymbol{I}, \boldsymbol{O} \rangle$ poludirektni umnožak grupe $\mathbb{Z}_2^{11}$ i Mathieueve grupe M_{12}.
5.) Ako je $2n = 2^k$, tada je $\langle \boldsymbol{I}, \boldsymbol{O} \rangle$ izomorfna poludirektnom umnošku grupa $\mathbb{Z}_2^k$ i $\mathbb{Z}_k$, gdje se $\mathbb{Z}_k$ ponaša kao ciklički pomak i $|\langle \boldsymbol{I}, \boldsymbol{O} \rangle| = k \cdot 2^k$.

Dokaz ovog teorema nalazi se u [6].

U tablici 2 prikazan je red grupe $\langle \mathbf{I}, \mathbf{O} \rangle$ za špil veličine $2n$, $n \leq 26$. Vrijednosti u talici izračunate su pomoću pojednostavljenog Simsovog algoritma [13] kojeg su razvili Eric Hamilton i Donald Knuth sa sveučilišta u Stanfordu.

$2n$	2	4	6	8	10	12	14	16	18
$\lvert\langle \mathbf{I}, \mathbf{O}\rangle\rvert$	2	$2 \cdot 2^2$	$M/2$	$3 \cdot 2^3$	$M/2$	$M/3!$	$M/2$	$4 \cdot 2^4$	$M/2$
$2n$	20	22	24	26	28	30	32	34	36
$\lvert\langle \mathbf{I}, \mathbf{O}\rangle\rvert$	M	$M/2$	$M/(7! \cdot 2)$	$M/2$	M	$M/2$	$5 \cdot 2^5$	$M/2$	M
$2n$	38	40	42	44	46	48	50	52	
$\lvert\langle \mathbf{I}, \mathbf{O}\rangle\rvert$	$M/2$	$M/4$	$M/2$	M	$M/2$	$M/4$	$M/2$	M	

Tablica 2: Red grupe $\langle \mathbf{I}, \mathbf{O}\rangle$ za špil od $2n$ karata, $n \leq 26$, gdje je $M = 2^n n!$.

5 Neke primjene savršenih miješanja

Osim već spomenutih primjena savršenih miješanja kod mađioničara i mješača karata, postoje i brojne druge primjene. Primjerice, oba tipa savršenog miješanja i njihove kombinacije uvrštene su u računalne algoritme za paralelne procese [14] kao sto su FFT, sortiranje podataka, matrične operacije, obrada slike itd.

Kao prvu primjenu spomenut ćemo transponiranje matrice dimenzije $2^m \times 2^m$. Pretpostavimo da su elementi matrice složeni u niz po retcima. Za matricu 4×4 imamo $a_{00}a_{01}a_{02}a_{03}a_{10}a_{11}a_{12}a_{13}a_{20}a_{21}a_{22}a_{23}a_{30}a_{31}a_{32}a_{33}$. Lako je provjeriti da će nakon m **out** miješanja matrica dimenzije $2^m \times 2^m$ biti transponirana. Tako ćemo, u primjeru za 4×4 imati $a_{00}a_{10}a_{20}a_{30}a_{01}a_{11}a_{21}a_{31}a_{02}a_{12}a_{22}a_{32}a_{03}a_{13}a_{23}a_{33}$.

Spomenimo i to da je potrebno m **in** miješanja da bi se niz od 2^m brojeva zapisao u obrnutom poretku.

Naposljetku ćemo spomenuti vrlo važnu primjenu savršenih miješanja u algoritmu brze Fourierove transformacije. Rose je u svom radu [12] poopćio savršena miješanja te je koristio permutacijske matrice nastale od savršenih miješanja da bi uveo metodu za računanje diskretne Fourierove transformacije (DFT) s primjenom na algoritam brze Fourierove transformacije. Savršena miješanja je doveo u vezu s Kroneckerovim produktom dviju matrica. Glavna ideja korištenja savršenih miješanja u DFT jest da se uz njihovu pomoć DFT matrica reda N može povezati s DFT matricom reda $N/2$.

Literatura

[1] P. Diaconis, R.L. Graham, *The Solutions to Elmsley's Problem*, Math Horizons, 14:22-27, 2007.

[2] R. Fleischer, *Elmsley's Problem Revisited*, Proceedings of the 20th Japan Conference on Discrete and Computational Geometry, Graphs, and Games (JCDCG3 2017), Tokyo, Japan, August 29-September 1, 2017.

[3] J. H. Green, *An Exposure to the Arts and Miseries of Gambling*, James, Cincinnati, 1843.

[4] C. Hooley, *On Artin's Conjecture*, J. Reine Angew. Math. 225: 209–220. 1967.

[5] J. Ellis, H. Fan, J. Shallit, *The Cycles of the Multiway Perfect Shuffle Permutation*, Department of Computer Science, University of Victoria, Victoria, British Columbia, V8W 3P6, Canada, 2002.

[6] P. Diaconis, R. Graham, W. Kantor, *The Mathematics of Perfect Shuffles*, Advances in Applied Mathematics 4: 175-196, 1983.

[7] G. Kolata, (January 9, 1990), *In Shuffling Cards, 7 Is Winning Number*, New York Times.

[8] F. Nikšić, *Brza Fourierova transformacija*, PMF- Matematički odjel, Zagreb, 2007.

[9] S. B. Morris, *The Basic Mathematics of Faro Shuffle*, Pi Mu Epsilon Journal, 6: 85-92, 1975.

[10] N. Kiewel, *Faro Shuffle simulator*, https://natedog.com/cards/faro.html, 2004

[11] S. Ramnath, D. Scully,, *Moving card i to position j with perfect shuffles*, Mathematics Magazine, 69, 362-365, 1996.

[12] D. J. Rose, *Matrix Identities of the Fast Fourier Transform*, Linear Algebra and its application 29, 423-443, 1980.

[13] C. C. Sims, *Computational methods in the study of permutations groups, in "Computational Problems in Abstract Algebra,"*, Proc. Conf., Oxford, 1967 (John Leech, Ed.), 169-183, Pergamon, Oxford, 1970.

[14] H.S. Stone, *Parallel processing with the perfect shuffle*, IEEE Trans. Comput. 2, 153-161, 1971.