

# SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Kortblandningar, Markovkedjor och Simulering av Doyle's patiens

av

**Fredrik Sköld**

2021 - No K3



# Kortblandningar, Markovkedjor och Simulering av Doyle's patiens

Fredrik Sköld

---

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Daniel Ahlberg

2021



# KORTBLANDNINGAR, MARKOVKEDJOR OCH SIMULERING AV DOYLE'S PATIENS.

FREDRIK SKÖLD

SAMMANFATTNING. The GSR model (Gilbert-, Shannon and Reed) is a mathematical model of the common riffle shuffle method of shuffling playing card. This paper examines the mathematics of the GSR model and card shuffling in general. The main mathematical theory used in this paper is the theory about Markov chains. This paper describes the GSR model and how it can be used to determine when a deck of cards is sufficiently shuffled. In addition, this paper examines the requirements for a card shuffling method for it to converge to the uniform distribution over all possible orderings of the card deck. This paper also shows that the requirement for a sufficiently shuffled card deck may vary depending on the intended use of the card deck, i.e. the game to be played. Therefore, this paper looks at examples of card games when the necessary distance to the uniform distribution varies. To measure the distance to the uniform distribution after a certain amount of GSR shuffles, the Total Variation distance is used. The paper also includes simulations of playing a specific card game, New Age solitaire, using GSR shuffles and other shuffling methods.

## INNEHÅLL

1. Introduktion	3
2. Matematisk modell för att beskriva kortblandningar	5
3. Teori om Markovkedjor och hur Markovkedjor kan användas för att modellera kortblandningar	8
4. Vad krävs för att en kortblandningsprocess ska leda till en välblandad kortlek?	14
5. Riffle shuffle / GSR-blandning - en matematisk modell	19
6. Doyle's patiens, GSR-blandningens svaghet	23
7. Finns det effektivare kortblandningar för att uppnå jämvikt mellan utfallen i Doyle's patiens?	27
8. Simuleringar av kortblandningar och Doyle's patiens - metodbeskrivning	28
9. Simuleringar - finns det bättre sätt att blanda en kortlek	30
10. Diskussion	32
11. Slutsats	33
Referenser	34

## 1. INTRODUKTION

Sannolikhetsteori [11] är en gren om matematik som berör slumpmässiga händelser. Den moderna matematiska sannolikhetsteorin har sina rötter från 1600- och 1700-talet då matematikerna Gerolamo Cardano, Pierre de Fermat och Blaise Pascal var verksamma och började intressera sig av hazardspel och analysera dem matematisk. Sannolikhetsteorin tillämpas idag blandad annat inom fältet statistik, som är en gren inom tillämpad matematik. Inom statistiken används sannolikhetsteorin som teoretisk ramverk för statistisk inferensteori, vilket analyserar slumpmässiga fenomen. Statistikmetodik är en central del i alla kvantitativa forskningsområden som exempelvis Nationalekonomi och Epidemiologi.

Hazardspel och andra typer av konstruerade spel har visat sig fortsatt vara intressant att studera inom sannolikhetsteorin, och vi kommer att belysa några sådana exempel i denna uppsats. Flera av de mest populära hazardspelen använder sig av en kortlek för att generera slumpmässiga utfall i spelen. Dessa utfall avgör sedan vinnare och förlorare utifrån spelets regler. Andra populära hazardspel som att singla slant, eller kasta tärning använder vi oss utav tyngkraften för att generera oförutsägbara utfall, i alla fall för rättvisa mynt och tärningar. Däremot fungerar inte det lika väl för en kortlek. Därför behöver vi på något sätt blanda kortleken för att skapa de oförutsägbara utfallen som söks i hazardspelen. Det finns många olika sätt att blanda en kortlek och i denna uppsatsen kommer vi diskutera några olika kortblandnings metoder, men vi kommer framförallt studera det som på engelska kallas "riffle shuffle". Det var under lång tid en obesvarad fråga hur länge, eller hur många gånger, man behöver blanda en kortlek för att den ska vara tillräckligt blandad. Detta tills [2] Dave Bayer och Perci Diaconis lyckades analysera en matematisk modell som beskriver riffle shuffle, och lyckades avgöra hur välblandad kortleken är efter ett visst antal iterationer. Deras upptäckt fick även massmedial spridning via en tidningsartikel i New York Times [6], och i denna påstår Diaconis att sju blandningar av typen riffle shuffle är tillräckligt för en kortlek med 52 kort. Vi kommer i denna uppsatsen gå in på den matematiska teorin som används för att modellera kortblandningen och beskriva ett mått som kan användas för att bestämma när en kortlek är tillräckligt blandad. Vi kommer även studera vad som är nödvändigt för att en kortblandning ska skapa slumpmässiga utfall. För det finns också blandningsmetoder som inte genererar slumpmässiga utfall, exempel på detta är det som motsägelsefullt kan kallas en perfekt blandning [4]. Därför är det nu lämpligt att definiera vad vi syftar på när vi pratar om en fullständigt blandad kortlek.

**Definition 1.** En kortlek med  $n$  kort är fullständigt blandad om varje möjligt ordning av korten är lika sannolik.

Eftersom en kortlek med  $n$  kort kan ordnas på  $n!$  olika sätt, måste sannolikheten för varje enskild ordningen vara  $\frac{1}{n!}$  för att den ska anses vara fullständigt blandad. Vi kan även säga att kortleken är fullständigt blandad, om sannolikheten att kortleken befinner sig i något av de möjliga ordningarna är likformigt fördelad, efter något blandningsförfarande. Däremot är det inte vanligt förekommande att vi lyckas åstadkomma en fullständig blandning utav en kortlek genom att använda någon blandningsmetod. Det som vanligtvis sker om vi blandar en kortlek är att kortleken kommer vara mer eller mindre välblandad. Med välblandad syftar vi på att vår blandningsfördelning är tillräckligt nära den fullständiga blandningen, och det kan mätas genom att beräkna det totala variationsavståndet mellan fördelningarna, måttet benämns fortsättningsvis som TV-avståndet. Diaconis påstående i artikeln att sju blandningar är tillräckligt för en kortlek med 52 kort, bör därför tolkas som att kortleken är tillräckligt välblandad efter sju riffle shuffles. Påstående bör dock ses som en tumregel, eftersom hur välblandad kortlek vi behöver kan beror på vad kortleken ska användas till. Exempelvis om kortleken ska användas till att spela blackjack där kortens färg inte spelar någon roll, har vi färre möjliga ordningar av kortleken som påverkar utfallet i spelet. Antalet möjliga ordningar av en kortlek som ska användas för att spela blackjack kan beräknas genom multinomialkoefficienten, om vi har en vanlig kortlek med 52 kort, och det finns 13 olika värden på korten, vi beräknar

$$\binom{52}{4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4} = \frac{52!}{4!^{13}},$$

vilket uppenbarligen är mindre än  $52!$ . Detta leder till att det kommer gå snabbare givet någon effektiv blandningsprocess att närma sig den likformiga fördelningen för alla ordningar. Djupare analys av detta är gjord av Conger och Viswanath [3]. Antalet kort i kortleken påverkar också blandningstiden och det är därför Diaconis specificerar att hans påstående gäller en kortlek med 52 kort.

Det finns även kortspel som kräver att vi har en kortlek som är väldigt nära att vara fullständigt blandad för att spelet ska vara rättvist. Ett sådant spel konstruerades av Peter Doyle [9], spelet är en patiens och har två möjliga utfall och kallas även New Age Solitaire. Datorsimuleringar har visat att efter sju riffle shuffles har spelaren ungefär 81 procent chans att vinna spelet. Men om patiensen spelas med en fullständigt blandad kortlek är det jämvikt mellan utfallen i spelet. Utifrån ovannämnd exempel kan vi konstatera att om vi ska påstå att en kortlek är tillräckligt välblandad måste vi ta hänsyn till vad kortleken ska användas till. Relevant matematisk teori för att analysera kortblandningar är teorin kring Markovkedjor, men också mer specifikt hur en kortblandningsprocess kan modelleras som en slumpvandring över en grupp av permutationer. I nästa avsnitt kommer vi beskriva en matematisk modell för att beskriva kortblandningar.



## 2. MATEMATISK MODELL FÖR ATT BESKRIVA KORTBLANDNINGAR

I detta avsnitt använder vi oss av en artikel skriven av Brad Mann [9], för att formulera en matematisk beskrivning av kortblandningar. Det finns flera beskrivningar att utgå ifrån men Mann ger trevlig elementär presentation i sin beskrivning. Vi kan börja med att anta att vi har en kortlek med  $n$  kort som ligger nedåtvänd i en hög. För att underlätta beskrivningen av de olika ordningar av kortleken, kan vi börja med märka korten med heltalen från 1 till  $n$  och se högen som en talföljd  $1, 2, \dots, n$ , där kortet högst upp i högen blir tilldelat heltalet 1 och så vidare. Denna ordning av kortleken kommer vi kalla **den naturliga ordningen** av kortleken. Antalet möjliga ordningar av en kortlek ges av hur många olika **permutationer** vi kan skapa av de  $n$  korten i kortleken, vilket är  $n!$ . Vi kan då använda mängden  $S_n$  för att beteckna mängden av alla möjliga permutationer av talen  $1, 2, \dots, n$ . Vi kan sedan använda elementen i  $S_n$  för att beteckna alla möjliga ordningar av en kortlek, men också alla möjliga omordningar.

Då om vi ska beskriva en kortblandning med en kortlek med fyra kort, då finns alla möjliga permutationer av kortleken i  $S_4$ . Den naturliga ordningen  $(1, 2, \dots, n)$  benämner vi med *id*. Därefter önskar vi skapa en ny ordning av kortleken genom att flytta det sista kortet i ordningen, längst fram i ordningen. Då korten var i ordningen *id* kan vi beskriva det som en permutation som skapar den önskade ordningen enligt tabell 1 nedan.

TABELL 1. Omordning av kortlek

id	1	2	3	4
$id \circ \rho$	4	1	2	3

Där  $\rho$  är permutationen som motsvarar omordningen, och  $id \circ \rho$  är den nya ordningen på kortleken. Vi kan även uttrycka det utan tabell som  $id \circ \rho = [4123]$ , och det kan läsas som att kortet som var i *position*(1)  $\rightarrow$  *position*(2) och *position*(2)  $\rightarrow$  *position*(3) och så vidare. Eftersom permutation  $\rho$  appliceras på den naturliga ordningen som är identitets-elementet i  $S_n$ . Så kommer  $id \circ \rho = \rho$ . Vi kommer fortsättningsvis använda oss sammansättning av permutationer när vi beskriver någon omordning av kortleken, där  $\sigma \circ \rho$  beskriver omordningen  $\rho$  applicerad på ordningen av kortleken  $\sigma$ .

**Definition 2.** En kortblandning för en kortlek med  $n$  kort, är en operation på  $S_n$  där nuvarande ordning  $\sigma$  resulterar i en ny ordning  $\sigma \circ \rho$ . Då är  $\rho \in S_n$  kortblandningen och den väljs enligt någon sannolikhetsfördelning på  $S_n$  som karakteriserar kortblandningen.

**Example 2.1.** Ett enkelt exempel på en kortblandning är om vi tar de översta kortet i en kortlek och sätter in det i någon av de  $n$  möjliga positionerna som finns

i kortleken, och valet av position görs likformig över antalet möjliga positioner. Då om vi har en kortlek med 3 kort kan sannolikhetsfördelning för valet av permutation i  $S_3$  beskrivas enligt följande tabell: 2.1.

TABELL 2. Sannolikhetsfördelning för möjliga permutationer

$\rho$	[123]	[213]	[231]	[132]	[321]	[312]
Sannolikhetsfördelning	1/3	1/3	1/3	0	0	0

Om vi sedan önskar upprepa denna kortblandning flera gånger, då skulle vi kunna kalla det en kortblandningsprocess. En kortblandningsprocess kan även beskrivas som en slumpvandring på gruppen av permutationer  $S_n$ . En slumpvandring kan beskrivas som en stokastiskt eller slumpmässigprocess som beskriver en väg i något matematiskt rum som består av slumpmässiga steg i processen. En grupp inom matematik är en typ av algebraisk struktur som består av en mängd och en binär operation på denna mängd. Definitionen av en grupp kräver att vi har en mängd, i vårt fall  $S_n$  och en binär operation ( $\circ$ ) på mängden som är en funktion  $f$  så att

$$f : S_n \times S_n \rightarrow S_n.$$

Alltså att  $f$  avbildar element i mängden  $S_n$  på samma mängd  $S_n$ , det vill säga att operationen är sluten. Vår binära operation på  $S_n$  kommer att vara sammansättningar av permutationer. Definitionen av en grupp lyder enligt följande:

**Definition 3.** En grupp  $(S_n, \circ)$  är en mängd  $S_n$  tillsammans med en binär operation  $\circ$  på  $S_n$  sådan att:

(G1) Binära operationen  $\circ$  är associativ.

(G2) Det finns ett element  $id \in S_n$  sådant att  $id \circ \rho = \rho \circ id = \rho$ , för alla  $\rho \in S_n$ .

Det kallas även identiteten.

(G3) För varje element  $\rho \in S_n$  finns det ett element  $\sigma \in S_n$  sådant att  $\rho \circ \sigma = \sigma \circ \rho = id$ .

Om det gäller  $\rho \circ \sigma = id$ , kallas element  $\sigma$  inversen till  $\rho$ , och  $\sigma$  är unik. Vilket även kan skrivas som  $\rho^{-1}$ .

Den binära operationen  $\circ$  för permutationsgruppen, är som sagt sammansättning av permutationer, och sammansättning av permutationer är associativt.

Identitets-element för en kortblandning kan beskrivas som en blandning som inte påverkar ordningen av korten. Permutationen för identitets-element är alltså  $id = [1, 2, \dots, n]$ . Ett konkret exempel på en sådan blandning är om vi kuperar en kortleken exakt på mitten två gånger, då kommer vi få tillbaka den ursprungliga ordningen. Vi kan också konstatera att varje element i  $S_n$  kommer besitta en invers. Detta eftersom alla bijektiva funktioner har en invers. Det kan beskrivas som att

om vi genomför någon kortblandning kommer det finnas en blandning som gör den ogjord. Exempelvis i  $S_3$  om vi har att  $\rho = [312]$  då har vi att  $\rho^{-1} = [231]$ , eftersom att  $\rho \circ \rho^{-1} = e$ .

Vi kan också konstatera att varje element i  $S_n$  kommer besitta en unik invers. Så om vi har någon permutation  $\rho$  finns det en unik permutation  $\sigma$  så att  $\rho \circ \sigma = id$ . Vi skulle kunna visa detta genom att anta att vi har en permutation  $\rho$  med två olika inverser  $\sigma_0$  och  $\sigma_1$  till  $\rho$  i  $S_n$ . Då gäller enligt definition 3 att

$$\rho \circ \sigma_0 = id, \text{ och}$$

$$\rho \circ \sigma_1 = id.$$

Om vi då lägger till sammansättningen  $\sigma_0$  till vänster om båda leden i den andra ekvationen får vi

$$(\sigma_0 \circ \rho) \circ \sigma_1 = \sigma_0 \circ id.$$

Och om vi förenklar med att  $\sigma_0 \circ \rho = id$  och  $\sigma_0 \circ id = \sigma_0$  får vi

$$\sigma_1 = \sigma_0.$$

Vilket visar att  $\sigma_1 = \sigma_0$ , och de måste vara samma permutation. Enligt definitionen kan vi då konstatera att  $(S_n, \circ)$  är en grupp. Anledningen till att det är intressant att tolka de olika ordningar av en kortlek som gruppen  $S_n$ , vilket även kallas den symmetriska gruppen, är eftersom vi kommer att kunna visa att slumpvandringar på  $S_n$  har den likformiga fördelningen som stationär fördelning. Men för att visa detta behöver vi först definiera vad vi menar med slumpvandringar och redogöra för teorin kring Markovkedjor.

### 3. TEORI OM MARKOVKEDJOR OCH HUR MARKOVKEDJOR KAN ANVÄNDAS FÖR ATT MODELLERA KORTBLANDNINGAR

En tillämplig modell för att beskriva en kortblandningsprocess av en kortlek är att se det som en slumpvandring över gruppen av permutation, och vi kan använda det teoretiska ramverket för Markovkedjor för att studera denna process. Eftersom Markovkedjor kommer vara den teoretiska grunden för stora delar av denna uppsatsen tar vi oss friheten att grundligt definiera begreppet och hur det förhåller sig till mer specifikt till kortblandningar. I detta avsnitt har jag använt mig av ett kompendium av Jan Enger och Jan Grandell [5], och av David Levin och Yuval Peres [7] bok för att förklara teorin kring Markovkedjor.

En process att blanda en kortlek kan beskrivas som en slumpmässig händelsekedja i tiden, där varje blandninguppreppning är en diskret tidsenhet från tiden 0 till tiden  $t$ . Då vid varje tidpunkt  $t$  beskriver den stokastiska variabeln  $X(t)$  i vårt exempel någon ordningen av kortleken. Men vanligtvis är vi inte endast intresserad av  $X(t)$  vid något specifik tidpunkt, utan hur händelsekedja beter sig över en hel tidsperiod. När vi studera en tidsperiod benämner vi då familjen av stokastiska variabler som  $\{X(t); t \in T\}$ , där  $T$  kan vara ett ändligt eller oändligt tidsintervall.

**Definition 4.** En familj av stokastiska variabler  $\{X(t); t \in T\}$  kallas en stokastisk process.

Vanligtvis svarar parametern  $t$  mot "tid", och mängden  $T$  kallas parameterrummet. För kortblandningar kommer vi betrakta  $T = \{0, 1, \dots\}$ , d.v.s  $T = \mathbf{N}$ , då vi talar om diskret tid i form av antalet blandningar av en kortlek.

En Markovprocess är en specifik typ stokastisk process, kravet för att en stokastisk process ska kallas en Markovprocess är om den betingade sannolikhetsfördelningen för framtida tillstånd i processen endast är beroende av det nuvarande tillståndet. I denna uppsats kommer vi betrakta processer  $\{X_n; n = 0, 1, \dots\}$  i diskret tid, där varje kortblandning kan ses som en tidsenhet för tidpunkterna  $0, 1, 2, \dots$ . Kortleken kommer då befinna sig i någon ordning eller något tillstånd efter varje blandning. Genom blandningarna kommer den att förflytta sig inom ett ändligt tillståndsrum  $S_n = \{i_1, i_2, \dots, i_n\}$ .

**Definition 5.**  $X_n; n \geq 0$  är en Markovkedja med tillståndsrummet  $E$  om

$$P(X_{n+1} = i_{n+1} | X_0 = i_0, X_1 = i_1, \dots, X_n = i_n) = P(X_{n+1} = i_{n+1} | X_n = i_n)$$

för alla  $n$  och tillstånd  $i_0, i_1, \dots, i_{n+1}$  i tillståndsrummet  $E$ .

Definitionen medför att Markovkedjor inte påverkas av tidigare tillstånd, utan att endast det nuvarande tillståndet påverkar framtida tillstånd. För våra syften som är att studera en kortblandning, så överensstämmer definition med vår förståelse

av verkligheten. Vilket är att det är den nuvarande ordningen av kortleken som påverkar framtida ordningar efter en kortblandning. Vi önskar sedan blanda kortleken tillräckligt många gånger så att startordningen av kortleken har liten påverkan på vilken ordning kortleken slutar i efter en blandningsprocess.

**Definition 6.** Övergångssannolikheterna  $p_{ij} = p(i \rightarrow j) = p(X_n = j | X_{n-1} = i)$   $i, j \in E$  d.v.s  $p_{ij}$  är sannolikheten att gå från  $i$  till  $j$  i ett tidssteg.

Övergångssannolikheten  $p_{ij}$  kan ses som en radvektor som innehåller sannolikheterna för att röra sig från tillstånd  $i$  nästa tillstånd  $j \in E$ . Där summan av elementen i vektorn är 1. Om vi använder exempel 2.1 skulle vi kunna uttrycka övergångssannolikheten mellan tillstånden enligt följande. Om vi är i tillstånd  $i = i_0 = [123]$  och de övriga tillstånden är de resterande permutationerna i  $S_3$  och permutationerna är namngivna med  $i_1 = [213]$ ,  $i_2 = [231]$ ,  $i_3 = [132]$ ,  $i_4 = [321]$  och  $i_5 = [312]$  enligt tidigare exempel. Där

$$p_{ij} = p(i \rightarrow j) = \begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 0 \end{pmatrix}.$$

**Definition 7.** Övergångsmatrisen  $P$  menas matrisen  $(p_{ij})_{i,j \in E}$  av övergångssannolikheterna

$$P = \begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1j} \\ p_{21} & p_{22} & \cdots & p_{2j} \\ \vdots & \vdots & \ddots & \vdots \\ p_{i1} & p_{i2} & \cdots & p_{ij} \end{pmatrix}.$$

Där elementen från den  $i$ :te raden och  $j$ :te kolumnen betecknar övergångssannolikheten från tillstånd  $i$  till tillstånd  $j$ . Summan av elementen i en given rad är 1 eftersom sannolikheten att gå till nästa tillstånd måste vara 1. Om vi har ett oändligt tillståndsrum så är även matrisen oändlig. Övergångsmatris som motsvarar en slumpvandringen på  $S_n$  kommer att vara av storlek  $n! \times n!$ .

**Definition 8.** Ett tillstånd  $i$  sägs leda till ett tillstånd  $j$  om det är möjligt att från tillstånd  $i$  att förflytta sig till tillstånd  $j$  i  $n$  tidssteg, vilket kan beskrivas som  $i \rightarrow j$ , med positiv sannolikhet. Om även  $j \rightarrow i$  så sägs de två tillstånden kommunicera och kan betecknas som  $i \leftrightarrow j$ .

Med andra ord i avseende för kortblandningar betyder att om vi kan gå från en ordningen till en annan ordning genom någon kortblandningsprocess, och sedan tillbaka med samma ordning genom samma kortblandningsprocess. Då betyder detta att de ordningar kommunicerar med den givna kortblandningsprocessen.

**Definition 9.** En mängd av tillstånd där alla tillstånden kommunicerar med varandra benämns en irreducibel tillståndsmängd. Om en kedja omfattar hela tillståndsrummet och alla tillstånd kommunicerar kallas det en irreducibel kedja.

Om vi har en irreducibel kedja som motsvarar en kortblandning, där alla ordningar av kortleken är tillståndsrummet. Då skulle det innebära att vi från varje permutationen i gruppen  $S_n$  kan nå alla permutationer i  $S_n$  med positiv sannolikhet, genom en blandningsprocess efter något antal steg  $t$  i blandningsprocessen. Denna egenskap kommer visa sig vara en viktig egenskap för kortblandningar för att möjliggöra att kortblandning leder till en välblandad kortlek.

**Definition 10.** Låt  $D_i$  vara mängden av heltal  $n$  sådan att det är möjligt med positiv sannolikhet att gå från tillstånd  $i$  och att återvända till samma tillstånd  $i$  i  $n$  tidsteg. Med perioden  $d_i$  till  $i$  menas att den största gemensamma delaren till talen i  $D_i$ . Om  $d_i = 1$  kallas  $i$  för aperiodiskt tillstånd.

Med detta menas om vi har någon ordning av en kortlek, om vi tillämpar någon kortblandningsprocess och antalet steg som krävs för att återvända till detta tillstånd är slumpmässigt då kommer Markovkedjan som representerar kortblandningen vara aperiodiskt.

**Definition 11.** En fördelning  $\pi = (\pi_1, \pi_2, \dots)$  är en stationär fördelning till en Markovkedja med övergångsmatrisen  $P$  om:

$$\pi P = \pi.$$

Om vi har en kortlekt och använder någon blandningsmetod, som kan representeras med övergångsmatrisen  $P$ , där raderna i matrisen är övergångssannolikheten för tillstånd  $p_{ij}$ . Om vi då har en sannolikhetsfördelning  $\pi$  i vektorform över de olika tillstånd och om vi applicerar blandningsmetoden på  $\pi$  och sannolikhetsfördelningen inte förändras, då måste den  $\pi$  vara en stationära fördelningen.

För kortblandningar betyder detta om vi har en blandningsfördelningen och den inte påverkas om vi skulle göra en till blandning i kedjan, då måste den blandningsfördelningen vara stationär. Det innebär även att fler blandningar inte gör kortleken mer välblandad.

**Definition 12.** En Markovkedja  $X_n; n \geq 0$  sägs vara ergodisk om en gränsfördelning  $P^{(n)}$  existerar och om den är oberoende startfördelningen  $\pi^{(0)}$ , d.v.s om  $\lim_{t \rightarrow \infty} \pi^{(0)} P^{(t)}$  existerar och inte beror av  $\pi^{(0)}$ .

**Sats 13.** *En ändlig, irreducibel, aperiodisk Markovkedja är ergodisk och dess gränsfördelning är den entydiga stationära fördelningen.*

Jag kommer senare ge bevis för en annan formulering av **Sats 13** i form av **Sats 16**.

**Definition 14.** Totala variationsavståndet mellan två sannolikhetsfördelningar  $\mu$  och  $\nu$  över  $X$  definieras som:

$$\|\mu - \nu\|_{TV} = \max_{A \subseteq X} |\mu(A) - \nu(A)|. \quad (1)$$

Totala variationsavståndet användas för att specificera hur välblandad kortlek är givet en blandningsfördelning.

**Sats 15** (Totalt variationsavstånd). *Låt  $\mu$  och  $\nu$  vara två sannolikhetsfördelningar på  $X$ . Då kommer:*

$$\|\mu - \nu\|_{TV} = \frac{1}{2} \sum_{x \in X} |\mu(x) - \nu(x)|.$$

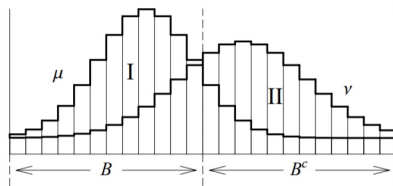
*Bevis.* Låt  $B = \{x : \mu(x) \geq \nu(x)\}$  och låt  $A \subset X$  vara någon händelse. Då följer

$$\mu(A) - \nu(A) \leq \mu(A \cap B) - \nu(A \cap B) \leq \mu(B) - \nu(B). \quad (2)$$

Första olikheten följer eftersom för varje  $x \in A \cap B^c$  uppfyller  $\mu(x) - \nu(x) < 0$ , så skillnaden i sannolikhet kan inte minsta när sådan element tas bort. För andra olikheten noterar vi att om vi inkluderar fler element i  $B$  kan inte skillnaden i sannolikhet minska. Med ett analogt resonemang kan vi även konstatera att

$$\nu(A) - \mu(A) \leq \nu(B^c) - \mu(B^c). \quad (3)$$

Den övre begränsningen i ekvation (2) och (3) faktiskt samma. Dessutom, när  $A = B$  (eller  $B^c$ ), då är  $|\mu(A) - \nu(A)|$  lika med den över begränsningen. Vi kan se detta i Figur 1.



FIGUR 1. Vi har att  $B = \{x : \mu(x) \geq \nu(x)\}$ . Region **I** har area  $\mu(B) - \nu(B)$ . Region **II** har area  $\nu(B^c) - \mu(B^c)$ . Eftersom den totala arean under  $\mu$  och  $\nu$  är 1, och regionerna **I** och **II** måste då ha samma area vilket är  $\|\mu - \nu\|_{TV}$ . [7]

Alltså får vi

$$\|\mu - \nu\|_{TV} = \frac{1}{2} [\mu(B) - \nu(B) + \nu(B^c) - \mu(B^c)] = \frac{1}{2} \sum_{x \in X} |\mu(x) - \nu(x)|.$$

□

Nu när vi har definierat TV-avstånd så kan vi omformulera Sats 13 vilket är ekvivalent med att

$$\max_{x \in X} \|p^t(x, \cdot) - \pi\| \rightarrow 0 \text{ då } t \rightarrow \infty.$$

**Sats 16** (Konvergens). [7] *Antag att  $P$  är irreducibel och aperiodisk med stationära fördelning  $\pi$ . Då gäller det att då  $t \rightarrow \infty$  att*

$$\max_{x \in X} \|P^t(x, \cdot) - \pi\|_{TV} \rightarrow 0.$$

*Bevis.* Eftersom  $P$  är irreducibel och aperiodisk existerar det ett  $r$  så att  $P^r$  har endast strikt positiva element. Låt då  $\Pi$  vara en matris med  $|X|$  rader och varje rad är radvektorn  $\pi$ . För tillräckligt små  $\delta > 0$ , har vi

$$P^r(x, y) \geq \delta\pi(y)$$

för alla  $x, y \in X$ , och låt  $\theta = 1 - \delta$ . Då uppfyller följande ekvation

$$P^r = (1 - \theta)\Pi + \theta Q \tag{4}$$

definitionen en stokastisk matris  $Q$ . Detta går att verifiera genom att kontrollera att  $M\Pi = \Pi$  för alla stokastiska matrisen och att  $\Pi M = \Pi$  för varje matris som uppfyller att  $\pi M = \pi$ . Nu kan vi använda induktion för att visa att

$$P^{rk} = (1 - \theta^k)\Pi + \theta^k Q^k. \tag{5}$$

För  $k \geq 1$ , om  $k = 1$ , håller detta enligt ekvation (4). Vi antar nu att ekvationen (5) håller för när  $k = n$ ,

$$P^{r(n+1)} = P^{rn}P^r = [(1 - \theta^n)\Pi + \theta^n Q^n]P^r.$$

Nu fördelar vi och utvecklar  $P^r$  i andra uttrycket genom att använda ekvation (5) vilket ger

$$P^{r(n+1)} = [1 - \theta^n]\Pi P^r + (1 - \theta)\theta^n Q^n \Pi + \theta^{n+1} Q^n Q.$$

Nu använder vi oss av att  $\Pi P^r = \Pi$  och att  $Q^n \Pi = \Pi$  visar att

$$P^{r(n+1)} = [1 - \theta^{n+1}]\Pi + \theta^{n+1} Q^{n+1}.$$

Det visar att ekvation (5) håller för  $k = n + 1$  om vi antar att ekvationen håller för  $k = n$ , och enligt induktionsprincipen därför gäller det för alla  $k$ .

Om vi nu multiplicerar med  $P^j$  och flyttar om termerna för vi

$$P^{rk+j} - \Pi = \theta^k(Q^k P^j - \Pi). \tag{6}$$

För att avsluta beviset tar vi summa av absolutvärden av elementen i rad  $x_0$  på båda sidor av ekvation (6) och dela med 2. I högerledet är den andra faktorn det största möjliga totala variationsavståndet mellan fördelningarna, vilket är 1. Därigenom får



vi för alla  $x_0$  har vi

$$\|p^{r_k+j}(x_0, \cdot) - \pi\|_{TV} \leq \theta^k.$$

□

Det är högst relevant att standardisera det maximala avståndet (för  $x_0 \in X$ ) mellan  $P^t(x, \cdot)$  och  $\pi$ . För att fastställa när en kortlek är tillräckligt välblandad, det gör vi det genom att bestämma ett visst maximalt avstånd till den stationära fördelningen som ska uppnås. Vi börjar därför med att definiera:

$$d(t) := \max_{x \in X} \|P^t(x, \cdot) - \pi\|_{TV}.$$

Nu kommer vi introducera en viktig parameter som mäter tiden som krävs för att Markovkedja ska vara nära i avstånd till den stationära fördelningen. Blandningstid är definerad av:

$$t_{mix}(\epsilon) := \min\{t : d(t) \leq \epsilon\}$$

och om vi sätter

$$t_{mix} := t_{mix}\left(\frac{1}{4}\right).$$

Värt att kommentera att valet av  $\epsilon$  är godtyckligt val. Dock om det är större än  $\frac{1}{2}$  kommer olikheterna inte att gälla. Valet av  $\epsilon$  bör vara beroende av vad kortleken ska användas till. Vi kommer att gå in på vidare i uppsatsen i senare avsnitt. Men det finns spel som kräver att totala variansavståndet är mycket mindre för att skapa ett rättvist spel.

4. VAD KRÄVS FÖR ATT EN KORTBLANDNINGSPROCESS SKA LEDA TILL EN  
VÄLBLANDAD KORTLEK?

Det finns många olika metoder för att blanda en kortlek, men endast för vissa av dessa metoder kommer de (efter olika lång tid) att komma nära den likformiga fördelningen. Vi kommer i detta avsnitt senare att visa att alla kortblandningar har den likformiga fördelningen som stationär fördelning. Vi kommer också senare i avsnittet klargöra vad som krävs för att en kortblandningsprocess ska inneha den likformiga fördelningen som entydig stationär fördelning. Då skulle vi kunna använda oss av TV-avståndet för att avgöra hur nära vi behöver komma den likformiga fördelningen, för att vi ska anse att kortleken är tillräckligt blandad. Men det finns också blandningar som ger exakt den likformiga fördelningen efter en slumpmässig tid. Vi inleder detta avsnitt med ett vanligt sådant exempel.

**Example 4.1.** [7] Låt oss anta att vi har en kortlek med  $n$  kort som befinner sig i den naturliga ordningen. Vi inleder med att markera kortet i  $position(n)$ , detta eftersom vi kommer behöva veta när detta kort är i  $position(1)$ . Vi börjar nu blanda kortleken genom att ta kortet i  $position(1)$  och sätter in den slumpmässigt i kortleken, med en likformig fördelning över alla positioner 1 till  $n$ . Vi fortsätter sedan denna process tills vi har placerat ett kort under de  $n$ :te kortet, som vi även har markerat. Eftersom för varje enskilt kort har sannolikheten  $\frac{1}{n}$  att placeras i  $position(n)$  kommer de förväntade antalet blandningar innan de sker vara  $n$  blandningar. Nu har vårt  $n$ :te kort rört sig ett steg upp i ordningen av kortleken och är i  $position(n-1)$ . Vi fortsätter processen till vårt markerade kort förflyttar sig ett till steg i ordningen till  $position(n-2)$ . Det förväntas ske efter  $\frac{n}{2}$  blandningar, eftersom det finns två möjliga positioner i under det markerade kortet. Och kortet som vi placerar under det markerade kortet är lika sannolikt att anta  $position(n)$  som  $position(n-1)$ . Om vi fortsätter denna process tills de markerade kortet har förflyttat sig till  $position(1)$ , då kommer alla möjliga ordningar för korten i  $position(2)$  till  $position(n)$  vara lika sannolika. Därefter om vi gör en sista blandning och placerar in de markerade kortet i kortleken, då kommer alla ordningar av kortleken att vara lika sannolika. Alltså kommer vi att få exakt den likformig fördelning över alla möjliga ordningar. Och eftersom vi känner till sannolikheten för att det markerade kortet ska förflytta sig uppåt ett steg, för varje position kan vi beräkna väntevärdet på antalet blandningar vi förväntas behöva göra för att nå den likformiga fördelningen. Vilket ges av att addera sannolikheterna för att det markerade kortet ska förflytta sig ett steg enligt följande beräkning

$$n + \frac{n}{2} + \frac{n}{3} + \cdots + \frac{n}{n} \approx n \log(n),$$

väntevärdet är alltså ungefär  $n \log(n)$ .

Vi kan även tänka oss exempel på en kortblandningsprocess där den likformiga fördelningen inte är den enda stationära fördelningen.

**Example 4.2.** Om vi applicerar det som kan benämnas som perfekt blandning eller Faro shuffle på en kortlek för vi olika stationära fördelningar beroende på starttillståndet av kortleken. Blandningen går ut på att vi delar vår kortlek med  $n$  kort i  $position(\frac{n}{2})$  och det förutsätter att vi har en kortlek med ett jämnt antal kort. Därefter lägger vi korten från de vardera högarna om varandra med ett kort från varje hög i taget. Så i den nya ordningen av korten kommer inget av korten från vardera hög anta en närliggande position med något kort från den tidigare kortleken. Och oavsett hur många kort vi har i kortleken kommer vi efter något antal blandningar vara tillbaka till den ursprungliga ordningen. Nedan kommer jag beskriva en sådan blandningsprocess. Antag att vi har en kortlek med 10 kort i den naturliga ordningen i tillstånd  $i_0$ , vi kommer använda Faro shuffle som kortblandningsprocess. Vi börjar med att dela kortleken efter  $position(\frac{10}{2} = 5)$  sedan ordnar vi korten om varandra från de två delarna. Vi markerar korten från andra delen av kortleken med subscript i ordning  $i_1$ . Därefter upprepas processen enligt samma metod.

$$i_0 = [12345|678910],$$

$$i_1 = [1_62_73_84_95_{10}],$$

$$i_2 = [1_86_42_97_53_{10}],$$

$$i_3 = [1_98_76_54_32_{10}],$$

$$i_4 = [1_59_48_37_26_{10}],$$

$$i_5 = [1_35_79_24_68_{10}],$$

$$i_6 = [12345678910].$$

Om vi skulle uttrycka det som en Markovkedja skulle det vara en reducibel kedja, och eftersom blandningsprocessen är deterministiskt. Där tillstånden som är redovisade kommunicerar med varandra, men inte med andra möjliga tillstånd i gruppen  $S_{10}$ , så kedjan är inte irreducibel. Eftersom Sats 13 inte är uppfyllt kan det finnas flera stationära fördelningen. Vilket stämmer för Markovkedjan med Faro shuffle som övergångsmatris, och den stationära fördelningen som kedjan slutar i beror på starttillståndet. Däremot kommer den likformiga fördelningen vara en stationär fördelning för denna kedja, vi kan dock inte nå den med övergångsfördelning.

Vi kommer nu besvara huvudfrågan i detta avsnitt och det är när en kortblandningsprocess har den likformiga fördelning som en stationär fördelning. Men även när den likformiga fördelningen är kedjans gränsfördelning enligt definition 12, sambandet mellan gränsfördelning och stationära fördelningar är att alla gränsfördelningar

är stationära. Men alla stationära fördelningar är inte gränsfördelningen, som i exempel 4.2, där vi har flera stationära fördelningar. Så om kedjan är irreducibel kommer den likformiga fördelningen vara den enda stationära fördelningen. Är kedjan dessutom aperiodisk konvergerar den mot den likformiga fördelningen enligt Sats 13.

Vi börjar med att visa att den likformiga fördelningen är stationära fördelning för alla kortblandningsprocesser vilket vi modellerar som en slumpvandring över gruppen  $(S_n, \circ)$ , där vår binära operation på gruppen är sammansättning av permutationer.

Vi använder  $\mu$  för att beskriva en sannolikhetsfördelningen på gruppen  $(S_n, \circ)$ , alltså att  $\mu$  beskriver vår kortblandningsmetod och sannolikheten att röra oss från en permutation av kortleken till en annan. Vi kan nu uttrycka det som en Markovkedja där  $S_n$  är vårt tillståndsrum, och kedjan förflyttar sig genom att multiplicera det nuvarande tillståndet till vänster om en slumpmässigt vald permutation enligt  $\mu$ . Då kommer övergångsmatrisen kunna beskrivas som

$$P(g, g \circ h) = \mu(h),$$

där alla  $g, h \in S_n$ . Där  $g \circ h$  är det tillstånd vi rör oss till, vilket också ingår i tillståndsrummet eftersom  $S_n$  är sluten under vår binära operation. Då kan vi använda oss av följande sats.

**Sats 17.** [7] *Låt  $P$  vara övergångsmatrisen för en slumpvandring på en den ändliga gruppen  $S_n$  och låt  $U$  vara den likformiga fördelningen på  $S_n$ . Då är  $U$  en stationär fördelning för  $P$ .*

*Bevis.* Låt  $\mu$  vara övergångsfördelningen för slumpvandringen. Då för alla  $g \in S_n$ ,

$$\sum_{h \in S_n} U(h)P(h, g) = [k = h^{-1} \circ g] = \frac{1}{|S_n|} \sum_{k \in S_n} P(g \circ k^{-1}, g).$$

Vi använder oss av variabelsubstitution för att omindexera till  $k$ . Anledningen till bytet är eftersom vi har definierat övergångsmatrisen att gå från något tillstånd  $h$  till något tillstånd  $g$ , detta sker genom att vi använder oss av någon permutation  $k$  så att  $hk = g$ . Och med ett analogt resonemang till varför varje permutation har en unik invers så kommer endast finnas ett möjligt val av  $k \in S_n$ . Så att  $h \circ k = g$ . Då följer även att  $P(g, kg) = \mu(k)$  för alla  $g \in S_n$  enligt definitionen. Det är också ekvivalent med  $P(k^{-1}g, g) = \mu(k)$ , och vi får

$$\frac{1}{|S_n|} \sum_{k \in S_n} P(g \circ k^{-1}, g) = \frac{1}{|S_n|} \sum_{k \in S_n} \mu(k) = \frac{1}{|S_n|} = U(g).$$

□

Satsen säger alltså om vi har en slumpvandring över gruppen  $(S_n, \circ)$ , då kommer den likformiga fördelningen vara en stationära fördelning. Om vi kombinerar detta

med sats 13, alltså om vi har en aperiodisk och irreducibel kedja så kommer den likformiga fördelningen att vara gränsfördelningen för kedjan. Då kan vi även dra slutsatsen om vi har en aperiodisk och irreducibel kedja och går fler steg i kedjan leder det till att vi närmar oss gränsfördelningen, och att kortleken blir mer välblandad.

Om vi återgår till exempel 2.1 och ställer upp övergångsmatrisen för den blandningsprocessen, och påminner oss om att om vi har tre kort kommer vi ha  $3!$  olika tillstånd i tillståndsrummet  $E = S_3$ . Vi benämner dessa tillstånd enligt följande

$$E_i = \{i_0 = [123], i_1 = [132], i_2 = [213], i_3 = [231], i_4 = [312], i_5 = [321]\}.$$

Vi får då övergångsmatrisen  $P$  baserat på övergångssannolikheten från blandningsprocessen mellan de olika tillstånden

$$P = \begin{pmatrix} \frac{1}{3} & 0 & \frac{1}{3} & \frac{1}{3} & 0 & 0 \\ 0 & \frac{1}{3} & 0 & 0 & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & 0 & 0 & \frac{1}{3} & 0 \\ 0 & 0 & \frac{1}{3} & \frac{1}{3} & 0 & \frac{1}{3} \end{pmatrix}.$$

Vi kan nu verifiera att vi kan nå alla möjliga tillstånd från ett givet tillstånd i  $E_i$ , vilket innebär att kedjan är irreducibel. Om vi observerar första raden i matrisen som motsvara tillstånd  $i_0$ , kan se att vi kan återvända till detta tillstånd på flera sätt. Exempelvis genom att först röra oss från  $i_0 \rightarrow i_2 \rightarrow i_0$ , men vi kan även gå från  $i_0 \rightarrow i_0$ , detta gäller även för alla tillstånd i  $S_3$ . Alltså kan vi se att kedjan är aperiodisk. Vi kan även säkerställa oss om att den likformiga fördelningen är den stationära fördelningen genom att multiplicera  $\pi_i P$ , där  $\pi_i = \frac{1}{3!}$  för alla  $i$ . Då får vi

$$\begin{pmatrix} \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} \end{pmatrix} \begin{pmatrix} \frac{1}{3} & 0 & \frac{1}{3} & \frac{1}{3} & 0 & 0 \\ 0 & \frac{1}{3} & 0 & 0 & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & 0 & 0 & \frac{1}{3} & 0 \\ 0 & 0 & \frac{1}{3} & \frac{1}{3} & 0 & \frac{1}{3} \end{pmatrix} = \begin{pmatrix} \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} \end{pmatrix} = \pi_i.$$

Alltså uppfyller den likformiga fördelningen  $\pi_i$  definition 11 att den är en stationära fördelningen. Vi kan även undersöka vad som händer vid upprepad multiplikation av övergångsmatrisen för att simulera flera blandningar, vi väljer godtyckligt att

genomföra 10 blandningar. Vilket som kan beskrivas som

$$P^{10} = \begin{pmatrix} \frac{1}{3} & 0 & \frac{1}{3} & 0 & \frac{1}{3} & 0 \\ 0 & \frac{1}{3} & 0 & \frac{1}{3} & 0 & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & 0 & \frac{1}{3} & 0 & 0 \\ 0 & 0 & \frac{1}{3} & 0 & \frac{1}{3} & \frac{1}{3} \end{pmatrix}^{10} \approx \begin{pmatrix} \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} \\ \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} \\ \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} \\ \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} \\ \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} \\ \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} \end{pmatrix}.$$

Vi ser då att oberoende vilket tillstånd kedjan startar i om vi applicerar  $P^{10}$  kommer få en likformig sannolikhetsfördelning över alla tillstånd i  $E_i$ . Det antyder att kedjan är ergodisk enligt definition 12. I nästa avsnitt kommer vi använda oss dessa egenskaper för beskriva och förklara den matematiska modellen som beskriver det som kallas riffle shuffle.

## 5. RIFFLE SHUFFLE / GSR-BLANDNING - EN MATEMATISK MODELL

En vanlig metod att blanda en kortlek är det som på engelska benämns "riffle shuffle". I detta avsnitt har vi använt oss av Brad Mann [9] och David Aldous och Percy Diaconis [1] för att beskriva en matematisk modell för riffle shuffle. GSR-blandningen kan beskrivas med ord som att vi först delar kortleken i två högar. Sedan placerar vi högarna mot varandra och böjer upp sidan av högarna som ligger emot varandra och sedan låter vi korten i de två högarna falla om varandra. Därefter för vi ihop de två högarna och vi har fått en ny ordning på kortleken. Blandning



FIGUR 2. Riffle shuffle [8]

innefattar två slumpmässiga händelser, dels när kortleken delas i två delar och dels hur korten blandas om varandra.

En modell för att beskriva riffle shuffle utvecklade Edgar Gilbert och Claude Shannon på Bells lab under 50-talet, och senare fristående av Jim Reed. Modellen benämns även GSR-blandningen efter upphovsmännen. Den matematiska modellen för GSR kan beskrivas enligt följande, antag att vi har en kortlek  $K$  med  $n$  kort, korten i  $K$  markeras enligt talföljden  $\{1, 2, \dots, n\}$  efter den ordningen de ligger i. Vi börjar att välja ett tal  $d$  enligt binomialfördelningen  $d := B(n, p = \frac{1}{2})$ . Därefter använder vi  $d$  för att göra en partition av  $K$ , till två högar,  $A$  och  $B$ . Där hög  $A$  motsvarar talföljderna  $A = \{1, 2, \dots, d\}$  och  $B = \{d+1, d+2, \dots, n\}$ . Sannolikheten att delningspunkten  $d$  sker efter exakt  $d$  kort ges av sannolikhetsfunktionen för binomialfördelningen där  $p = \frac{1}{2}$ ,

$$p_X(d) = P(X = d) = \binom{n}{d} \frac{1}{2} \left(1 - \frac{1}{2}\right)^{n-d} = \binom{n}{d} / 2^n.$$

Därefter betrakta vi alla olika möjligheter att blanda in korten från de två högarna till en ny hög, med restriktionen att korten i varje enskild hög behåller sin inbördesordning. Sedan väljer vi likformig mellan dessa möjligheter. Det kommer att finnas  $\binom{n}{d}$  möjliga sätt, detta eftersom för hög  $A$  behöver vi välja  $d$  positioner bland  $n$  möjliga positioner och korten i hög  $B$  bestäms sedan deterministiskt. Därför

kommer varje partikulär inblandning inneha sannolikheten  $\frac{1}{\binom{n}{d}}$ . Och om vi lägger ihop produkten av en partikulär delningspunkt med en partikulär inblandning får vi

$$\binom{n}{d}/2^n \cdot \frac{1}{\binom{n}{d}} = \frac{1}{2^n}.$$

Vilket innebär att för varje par av möjliga delningspunkter med respektive indelningsdelnings möjligheter är likformigt fördelade. Det kan dock finnas flera par som resulterar i samma permutation vilket vi kommer se i nästa exempel.

**Example 5.1.** Låt oss titta på ett exempel av en GSR blandning, med en kortlek med 3 kort. Anledningen till att vi endast väljer tre kort är eftersom övergångsmatrisen  $P$ , har storleken  $n! \times n!$  Om vi anger de möjliga ordningarna som olika tillstånd i tillståndsrummet  $E$ .

$$E_i = \{i_0 = [123], i_1 = [132], i_2 = [213], i_3 = [231], i_4 = [312], i_5 = [321]\}.$$

Vi kommer att dela vår kortlek så vi har  $d$  kort i den första högen och  $n - d$  i den andra högen enligt binomialfördelning vilket ger oss sannolikhetsutfallet för olika  $d$ ,  $\binom{n}{d} \cdot \frac{1}{2^n}$ , där  $d = 0, 1, 2, 3$ . Vi får då sannolikheten att vi delar kortleken på en given position vilket vi markerar med  $|$ ,  $P(d = 0) = |123 = \frac{1}{8}$ ,  $P(d = 1) = 1|23 = \frac{3}{8}$ ,  $P(d = 2) = 12|3 = \frac{3}{8}$  och  $P(d = 3) = 123| = \frac{1}{8}$ . Om  $d = 0$  eller  $d = 3$  kommer ordningen av kortleken behålla sin ordning, eftersom det inte finns några kort i den andra högen att blanda korten med. Om  $d = 1$  kan vi nå tre olika tillstånd  $i_0$ ,  $i_2$  och  $i_3$ , där sannolikheten för utfall  $i_0 = \frac{1}{3}$  och  $i_2 = \frac{2}{3} \cdot \frac{1}{2} = \frac{1}{3}$  och då måste även sannolikheten för  $i_3 = \frac{1}{3}$ . Om  $d = 2$  kan vi nå följande tre tillstånd  $i_0$ ,  $i_1$  och  $i_4$  och alla dessa möjliga ordningar har alla sannolikheten  $\frac{1}{3}$ . Vi kan nu uttrycka övergångssannolikheten som sannolikhetsvektorn  $p_{i_0j} = \{\frac{1}{2}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, 0\}$ . Om vi genomför samma beräkning av övergångssannolikheterna för de andra tillståndet kan vi skapa övergångsmatrisen

$$T = \begin{pmatrix} \frac{1}{2} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & 0 \\ \frac{1}{8} & \frac{1}{2} & \frac{1}{8} & 0 & \frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & \frac{1}{8} & \frac{1}{2} & \frac{1}{8} & 0 & \frac{1}{8} \\ \frac{1}{8} & 0 & \frac{1}{8} & \frac{1}{2} & \frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & \frac{1}{8} & 0 & \frac{1}{8} & \frac{1}{2} & \frac{1}{8} \\ 0 & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{2} \end{pmatrix}.$$

Så då kan vi fråga oss vad vi får för blandningsfördelning om vi blandar en kortlek med 3 kort med sju GSR blandningar som Diaconis förordade för 52 kort. Om vi



beräknar  $x_t \cdot P^7 = x_{t+7}$ , givet att  $x_t = (1, 0, 0, 0, 0, 0)$  får vi:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{2} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & 0 \\ \frac{1}{8} & \frac{1}{2} & \frac{1}{8} & 0 & \frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & \frac{1}{8} & \frac{1}{2} & \frac{1}{8} & 0 & \frac{1}{8} \\ \frac{1}{8} & 0 & \frac{1}{8} & \frac{1}{2} & \frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & \frac{1}{8} & 0 & \frac{1}{8} & \frac{1}{2} & \frac{1}{8} \\ 0 & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{2} \end{pmatrix}^7 = \begin{pmatrix} \frac{2795}{16384} & \frac{5461}{32768} & \frac{5461}{32768} & \frac{5461}{32768} & \frac{5461}{32768} & \frac{2667}{16384} \end{pmatrix}.$$

Denna ekvation kan då tolkas som att om vi börjar i den naturliga ordningen  $e = \{123\} = i_0$ , efter sju multiplikationer med övergångsmatrisen som representerar en GSR blandning. Då får sannolikheterna för  $p(x_{t+7}|x_t = i_0)$  i vektorform som är sannolikheten över vilket tillstånd vi kommer befinna oss i efter sju GSR-blandningar. Vi kan observera att det är större sannolikhet att vi befinner oss i tillstånd  $i_0$  än tillstånd  $i_5$ , men det verkar inte vara någon relativt stor skillnad mellan sannolikheterna. För att underlätta uppskattning kan vi konvertera bråktalen till decimaltal avrundat till fyra decimaler och får följande sannolikhetsvektor  $p(x_{t+7}|x_t = i_0) = (0.1706, 0.1667, 0.1667, 0.1667, 0.1667, 0.1628)$ . Anledningen till att sannolikheten är större att befinna sig i tillstånd  $i_0$  än  $i_5$ , beror på att övergångssannolikheten från starttillståndet  $i_0$ . Från  $i_0$  kan vi inte nå tillstånd  $i_5$  direkt från  $i_0$ , och det kommer att påverka delningsfördelning för kedjan. Det är därför vi diskuterar hur nära vi är den likformiga fördelningen efter  $t$  kortblandningar, eftersom det kommer finnas skillnader mellan tillstånden som minskar när  $t$  blir stort. Vi kan även nu beräkna TV-avståndet till den likformiga fördelningen genom att använda Sats 3. Om vi kalla delningsfördelningen  $p(x_{t+7}|x_t = i_0) = \mu$ , och låter  $\pi$  vara den likformiga sannolikhetsfördelningen kan vi använda

$$\|\mu - \pi\|_{tv} = \frac{1}{2} \sum_{i \in S_n} |\mu(x) - \nu(x)|.$$

Då efter lite betungande beräkningar eller med hjälp av datorverktyg får vi att

$$\|\mu - \pi\|_{tv} = \frac{\left| \frac{2795}{16384} - \frac{1}{6} \right| + 4 \left| \frac{5461}{32768} - \frac{1}{6} \right| + \left| \frac{2667}{16384} - \frac{1}{6} \right|}{2} = \frac{193}{49152} \approx 0.004.$$

Vilket kan tolkas som att vi är nära den likformiga fördelningen  $\pi$ . Och om vi jämför resultatet med Diaconis påstående om att sju blandningar är tillräckligt för 52 kort, kan vi se att det antagligen tillräckligt med färre blandningar om vi har färre kort i kortleken.

Vi kan även konstatera att övergångsmatrisen för GSR kommer att vara irreducibel och aperiodiskt enligt definitionerna. Eftersom alla tillstånd kommunicerar med varandra, och tiden som krävs för att återvända till ett givet tillstånd kommer vara slumpmässigt. Nu kan vi titta närmare på det generella TV-avståndet för en GSR-blandningsfördelning.

Bayer och Diaconis [2] artikel vägleder oss till en skarp formel för att beräkna TV-avståndet för en kortlek med  $n$  kort och som blandas med  $t$  GSR blandningar. Denna framställning är tagen från [9], där har vi även en variabel  $r$ , där  $r$  motsvarar antalet stigande sekvenser av kort i kortleken. Begreppet  $\langle \frac{n}{r-1} \rangle$  i formelen motsvarar Euler nummer.

$$\sum_{r=1}^n \left\langle \frac{n}{r-1} \right\rangle \left| \frac{2^t + n - r}{2^{nt}} - \frac{1}{n!} \right|.$$

Från tabellen 3 kan vi observera att vi behöver fler GSR-blandningar för att närma oss den likformiga fördelning om vi har fler kort i kortleken. Även tillfället där TV-avståndet är mindre än 1 sker efter fler antal blandningar. Och om vi vill beräkna mixing time som vi har definierat beror det på vårt val av  $\epsilon$ . Om vi skulle sätta  $\epsilon = \frac{1}{4}$ . Då kommer en kortlek med 52 kort vara välblandad efter 8 GSR blandningar. Men eftersom  $\epsilon$  kan sättas godtycklig, så länge  $\epsilon < \frac{1}{2}$  är det möjligt att argumentera att 7 blandningar också är tillräckligt. Men valet av  $\epsilon$  bör anpassas efter vad kortleken ska användas till. Vi nämnde i introduktionen att vi behövde blanda färre gånger om vi spelade spel som blackjack, och i nästa avsnitt kommer vi diskutera ett fall där vi behöver vara mycket närmre den likformiga fördelningen för att skapa ett rättvist spel.

TABELL 3. Totalt variationsavstånd [2] för en kortlek med 25, 52 och 104 kort. Efter  $s$  GSR blandningar.

s	1	2	3	4	5	6	7	8	9	10
25	1.000	1.000	0.999	0.775	0.437	0.231	0.114	0.056	0.028	0.014
52	1.000	1.000	1.000	1.000	0.924	0.614	0.334	0.167	0.085	0.043
104	1.000	1.000	1.000	1.000	1.000	0.893	0.571	0.307	0.153	0.078

Vi kommer i denna uppsats inte att gå djupare in på att härleda denna formel, men vi kommer att använda tabellen som referenspunkt för att jämföra med ett intressant patiens spel, där sannolikheterna att vinna spela ligger väldigt nära eller är samma som TV-avståndet mellan GSR-fördelning och den likformiga fördelningen.

## 6. DOYLE'S PATIENS, GSR-BLANDNINGENS SVAGHET

Vad som är ett tillräckligt TV-avstånd för en kortblandnings fördelning till den likformiga fördelningen beror på vad vi ska använda kortleken till. Peter Doyle [9] har konstruerat en patiens som är ett tydligt exempel på att utgången av spelet påverkas starkt av avståndet för kortleken blandningsfördelning till den likformiga fördelningen. Patiensen kallas även New-Age solitaire.

New-Age solitaire spelas på följande sätt med en vanlig kortlek. Spelet börjar med att en kortlek är placerad i en hög med värdesidan nedåt, och kortleken är ordnad i ordningen  $1, 2, \dots, (26), (52), 51, \dots, 27$  utifrån den naturliga ordningen. Därefter blandar vi kortleken med  $s$  GSR-blandningar. När kortleken är blandad, kommer vi att vända upp ett kort åt gången från toppen av kortleken. Spelet går ut på att vi önskar fylla upp en av två högar, högen Ying ska bestå av korten  $1, 2 \dots 26$  och högen Yang ska bestå av korten  $27, 28, \dots, 52$ . För att förflytta ett uppvänt kort till någon av målhögarna måste det vara kortet som är först i ordningen av högarna. Alltså det första kortet som vi kan placera i vardera hög är korten som motsvarar  $position(1)$  och  $position(27)$ , i den naturliga ordningen. När vi exempelvis har placerat  $position(1)$  i Ying kan vi placera in kort  $position(1 + 1) = position(2)$  och så vidare. Vi fortsätter att vända upp kort ur den blandade högen tills någon av målhögarna har fyllts. De korten som inte har placerats i någon av högarna läggs tillbaka i den blandade kortleken längst ned i ordningen. Den högen som först innehåller 26 kort är vinnaren, och vi kommer betrakta spelet som att vi är vinnare av spelet om Ying högen fylls upp först. Spelet kan även spelas med en kortlek med  $n$  kort, men då måste  $n$  vara ett jämnt heltal. Det som är intressant med denna patiens är att sannolikheten att vinna patiensen har en nära koppling till TV-avståndet mellan GSR-fördelningen och den likformiga fördelningen. Nedan kommer vi presentera en tabell där vi har simulerat utfallet av patienten med Monte Carlo-metod, i tabellen kommer vi att jämföra det med TV-avståndet för GSR som är tagen från tabell 4,  $p(\text{Ying})$  och är baserat på 100000 simuleringar för olika antal GSR-blandningar.

TABELL 4. TV-avstånd i jämförelse Monte Carlo- simuleringar av New age solitaire.

Bladningar GSR	1	2	3	4	5	6	7	8	9	10
TV-avstånd GSR	1.000	1.000	1.000	1.000	0.924	0.614	0.334	0.167	0.085	0.043
$p(\text{Ying})$	1.000	1.000	1.000	1.000	1.000	0.962	0.808	0.667	0.587	0.542
$p(\text{Ying}) - \text{TV-avstånd}$	0.000	0.000	0.000	0.000	0.076	0.348	0.474	0.500	0.502	0.499

Vid granskning av tabellen ser vi att efter fyra blandningar, är både TV-avståndet och  $p(\text{Ying}) \approx 1$ . Därefter börjar TV-avståndet minska, och efter sex blandningar börjar  $p(\text{Ying})$  minska. Efter sju blandningar är  $p(\text{Ying}) \approx 0.81$ . Differensen mellan

TV-avståndet och  $p(\text{Ying})$  är 0.474. Detta är intressant eftersom det sedan enligt tabellen verkar differensen mellan de två raderna konvergera mot 0.5. Det kan tolkas som att TV-avståndet efter sju blandningar är ett bra mått den extra fördelen i sannolikhet att vinna spelet gentemot om det hade varit ett rättvist spel. Och vi kommer endast att få ett rättvist spel om TV-avståndet är nära 0. Det finns även ett lemma som beskriver detta samband upptäckt av Van Zuylen och Schalekamp [10], och följande definition är även omskrivna från deras artikel "The Achilles Heel of the GSR-shuffle".

**Lemma 18.** *Låt  $Q^{*s}$  vara sannolikhetsfördelningen av ordningar efter  $s$  GSR-blandningar och  $U$  vara den likformiga fördelningen. Då för tillräckligt stora  $s$ , (förslagsvis som Mann föreslår  $s > 2 \log_2 n$ ), då har vi*

$$P(\text{vinna Doyles patients efter } s \text{ GSR blandningar}) = \|Q^{*s} - U\| + \frac{1}{2}.$$

Men för att förstå varför detta förhållande gäller behöver definiera två begrepp stigande och avtagande sekvenser av kort i en kortlek efter blandningar. Vi kan börja med en stigande sekvens det definieras enligt följande.

**Definition 19.** En stigande sekvens är en maximal sekvens av kort i ordning  $i, i + 1, \dots, i + j$  så att  $\text{position}(i) < \text{position}(i + 1) < \dots < \text{position}(i + j)$ .

Med maximal implicerar att en stigande sekvens inte går ihop med andra stigande sekvenser. Och avtagande sekvens definieras på samma sätt.

**Definition 20.** En avtagande sekvens är en maximal sekvens av kort i ordning  $i, i - 1, \dots, i - j$  så att  $\text{position}(i) < \text{position}(i - 1) < \dots < \text{position}(i - j)$ .

Så om vi har en kortlek med 10 kort i den naturliga ordningen [12345678910] och gör en GSR blandning och får följande ordning av kortleken [6127389105]. Då i den ursprungliga ordningen har vi en stigande sekvens, och 10 avtagande sekvenser och efter blandningen har vi två stigande sekvenser [678910] och [12345], och 9 avtagande sekvenser, [65], [1], [2], [3], [4], [7], [8], [9], [10]. Och vi har följande lemma för att beskriva sambandet mellan avtagande och stigande sekvenser:

**Lemma 21.** *Låt  $r$  vara antalet stigande sekvenser och  $d$  vara antalet minskande sekvenser i en permutation av längd  $n$ . Då har vi sambandet  $r + d = n + 1$ .*

Antalet stigande sekvenser i en given permutation påverkar sannolikheten för att få den givna permutation givet ett antal GSR blandningar. [2]

**Sats 22.** [10] *Sannolikheten att  $s$  GSR-blandningar på en kortlek i den naturliga ordningen resulterar i permutationen  $\pi$  är*

$$P(\pi | s \text{ GSR-blandningar}) = \frac{\binom{n+2^s-r}{n}}{2^{sn}},$$

där  $r$  är antalet stigande sekvenser i  $\pi$ .

Det är även så att chansen att vinna Doyles patiens är direkt kopplad till antalet stigande sekvenser och är beroende på den unika startordningen av kortleken.

**Lemma 23.** *Låt  $r$  vara antalet stigande sekvenser i en kortlek med  $n$  kort. Då kommer du vinna Doyles patiens om och endast om  $r \leq \frac{n}{2}$ .*

*Bevis.* Om vi betrakta Ying högen som ska fyllas med korten  $1, 2, \dots, \frac{n}{2}$ . Antalet rundor som det tar att fylla denna högen är samma som antalet stigande sekvenser i den delmängden av kortleken, vi kan kalla de  $r_1$ . Analogt gäller även att Yang högen som ska fyllas med korten  $\frac{n}{2} + 1, \frac{n}{2} + 2, \dots, n$  den kommer fyllas efter samma antal rundor som antalet minskande sekvenser i denna delmängd. Vi kan kalla detta  $d_2$ . Så för att Ying högen ska fyllas först måste  $r_1 < d_2$  eller om  $r_1 = d_2$  då måste  $\text{position}(\frac{n}{2}) < \text{position}(n)$ . Alltså att kortet  $\text{position}(\frac{n}{2})$  ligger före kortet i  $\text{position}(n)$ . Vi betecknar sedan antalet stigande sekvenser i Yang högen med  $r_2$ . Då kommer de totala antalet stigande sekvenser i kortleken som vi betecknar med  $r$  vara

$$r = r_1 + r_2 - I_a. \quad (7)$$

Där  $I_A$  är en indikator funktion som definieras enligt följande

$$I_A := \begin{cases} 1 & \text{om } \text{position}(\frac{n}{2}) < \text{position}(n), \\ 0 & \text{om } \text{position}(\frac{n}{2}) > \text{position}(n). \end{cases}$$

Då om vi använder Lemma 21 får vi att  $r_2 = \frac{n}{2} + 1 - d_2$ , och om vi sätter in  $r_2$  i ekvation (7) får vi

$$r = r_1 - d_2 + \frac{n}{2} + 1 - I_a. \quad (8)$$

Så låt oss anta att vi vinner Doyles patiens, då beror antingen på att  $r_1 < d_2$ , vilket vi kan kalla Fall 1. Eller att  $r_1 = d_2$  och att vår indikator funktion antar värde 1, vilket vi kallar Fall 2.

Fall 1 ger oss att om  $r_1 < d_2$  kan vi använda ekvation (8) för att omformulera  $r_1$  och  $d_2$ :

$$\begin{aligned} r_1 &= r + d_2 - \frac{n}{2} - 1 + I_A, \\ d_2 &= r_1 - r + \frac{n}{2} + 1 - I_A. \end{aligned}$$

Om vi sätter in högerleden i olikheten  $r_1 < d_2$  får vi att:

$$r + d_2 - \frac{n}{2} - 1 + I_A < r_1 - r + \frac{n}{2} + 1 - I_A.$$

Om vi subtraherar  $d_2$  och adderar  $r$  i båda leden får vi

$$2r - \frac{n}{2} - 1 + I_A < r_1 - d_2 + \frac{n}{2} + 1 - I_A.$$

Men nu i högerledet har vi  $r$  enligt ekvationen (8), och vi får

$$2r - \frac{n}{2} - 1 + I_A < r.$$

Nu kan vi addera båda leden med  $\frac{n}{2}$  och subtrahera  $r$  i båda led och vi får

$$r - 1 + I_A < \frac{n}{2}.$$

Alltså vinner vi när  $r < \frac{n}{2}$  och  $I_A = 1$  eller om  $r \leq \frac{n}{2}$  om  $I_A = 0$ . Fall 2 beräknas på liknande sätt och ger oss att  $r = \frac{n}{2}$  om  $I_A = 1$ . Om vi kombinerar båda fallen får vi komma vinna om och endast  $r \leq \frac{n}{2}$  och beviset är klart.  $\square$

Vi vet alltså att utfallet av Doyles patiens är beroende på stigande sekvenser i kortleken, vi skulle därför nu kunna konstruera en kortblandningsmetod som garanterar förlust efter en blandning. Om vi tänker en blandningsmetod som motsvarar permutationen  $[n, n-1, \dots, 1]$ . Då skulle vi vända på startordningen i patiensens så att korten som ska placeras i Yang högen ligger i en stigande sekvens och att korten i Ying högen alla ligger i separata minskande sekvenser. Sambandet mellan TV-avstånd och utfall är alltså beroende på den unika startordningen.

Men eftersom det är svårt att hitta en formel eller ekvation som beskriver TV-avståndet mellan en given blandningsfördelning och den likformiga fördelningen. Kommer vi att använda Doyles patiens för att undersöka om det finns varianter på GSR-blandningen som snabbare förändrar sannolikheten att vinna i Doyles patiens. Det kommer dock inte vara ett helt utbytbart mått mot TV-avstånd, men det kommer säga något hur snabbt en blandningsmetod bryter upp befintlig struktur i kortleken i form av stigande och minskande sekvenser i kortleken.

7. FINNS DET EFFEKTIVARE KORTBLANDNINGAR FÖR ATT UPPNÅ JÄMVIKT  
MELLAN UTFALLEN I DOYLE'S PATIENS?

GSR-modellen är en intressant modell att studera eftersom den förhållandevis väl motsvarar blandningsmetoden som på engelska kallas "riffle shuffle". Riffle shuffle är antagligen den vanligaste blandningsmetoden som används när personer ska blanda en kortlek. Det är även den vanligaste blandningsmetodiken som kommer upp vid en internetsökning över hur professionella croupier blandar en kortlek.

En annan blandningsmetod som är återkommande i flera instruktionsvideor om hur en bör kortlek blandas är en blandningsmetod som kallas "box shuffle". Box shuffle är en blandningsmetod som rekommenderas användas tillsammans med riffle shuffle. I regelboken för World Series of Poker år 2013 skulle croupierna tillämpa en blandningsalgoritm som kallades SSBS där S står för riffle shuffle och B för box shuffle. Därför kan det vara intressant att undersöka hur denna blandningsalgoritm påverkar sannolikheten att vinna i Doyle's patiens, då skulle vi kunna säga något hur snabbt den kortblandningsprocessen rör sig mot den likformiga fördelningen.

En box shuffle genomförs genom att dela kortleken i  $n$  ungefär lika stora delar. Så om vi delar en kortlek i  $n$  högar och markerar varje hög med heltalen 1 till  $n$ , och placerar högarna i ordningen  $1, 2, \dots, n$ . Därefter permuterar vi ordningen av högarna till ordningen  $n, n - 1, \dots, 1$ . Då har vi gjort en box shuffle, och korten i de enskilda högarna behåller sin inbördes ordningen. Syftet med blandningen är enligt vissa att korten i botten av kortleken svårt att färdas uppåt i positionsordning med riffle shuffle och då skulle en box shuffle förbättra kortblandningsprocessen. Vilket kan vara relevant för utfallet i Doyle's patiens, eftersom utfallet påverkas av  $I_a$  som vi definierade tidigare. En annan möjlig förklaring till varför denna blandningsprocessen förordas, kan vara att det möjligtvis skulle vara svårare att manipulera kortleken för den som blandar. Vilket inte är ett otänkbar förfarande vid spel om pengar, att den som blandar önskar skapa icke slumpmässiga utfall för sin egen eller någon annans vinning.

Vid simuleringar av box shuffle används multinomialfördelning för att bestämma delningspunkterna för de olika högarna, och vi har valt att dela kortleken i fyra högar.

Men vi har även konstruerat två andra ytterligare blandningsmodeller och genomfört simuleringar med dem. Den första är en variant av GSR som använder sig av en box shuffle för att dela kortleken. Så istället för att dela kortleken enligt binomialfördelningen  $(n, \frac{1}{2})$ , så använder vi multinomialfördelning  $(n, \frac{1}{4}, 4)$ . Där de två högarna som räfflas tillsammans är  $[DC]$  och  $[BA]$ . Den andra modellen använder också samma delningsförfarande, men vi räfflar ihop hög  $D$  och  $C$  för sig till hög  $[DC]$  och  $B$  och  $A$  till hög  $[BA]$  för sig, innan vi sedan räfflar ihop dem

tillsammans tillbaka till en hög. Alla blandningsmetoder är praktiskt möjliga att genomföra utan större svårigheter om man har lite erfarenhet att blanda med vanlig riffle shuffle.

#### 8. SIMULERINGAR AV KORTBLANDNINGAR OCH DOYLE'S PATIENS - METODBESKRIVNING

Programmeringsvertyget som har använts vid simuleringarna är Python 3.8. Vi har i programmet betraktat en kortlek med  $n$  kort, som en lista med element från  $[1, 2, \dots, n]$ . Kortblandningarna i programmet är formulerade som funktioner som tar en lista som input och sedan genomför operationer på listan som motsvar permutationen av kortblandning för skapa en ny ordning av listan. Vi har inte använt oss av några färdiga funktioner för att blanda kortlekarna som används vid simuleringar, utan endast av pseudo-slumpmässiga funktioner för binomial- och multinomialfördelningar för att generera slumpmässiga val i räfflings processen.

GSR-blandningsfunktionen i Python kan beskrivas enligt följande. Funktionen tar en lista som input, därefter genererar den ett heltal enligt binomialfördelningen  $(n, \frac{1}{2})$ . Talet  $d$  som väljs enligt binomialfördelningen används sedan för att avgöra var vi ska dela listan. Det resulterar i att vi har en normalfördelad sannolikhetsfunktion där det är störst sannolikhet att vi delar listan någonstans nära i mitten av listan. När ett tal  $d$  genererats delar vi listan då i två delar så att vi får två listor  $A = [1, 2, \dots, d]$  och  $B = [d, d + 1, \dots, n]$ . De två listorna motsvarar högarna som ska räffla ihop. Sedan använder vi oss av en while-loop som pågår så länge  $i$ , som används som iterator är mindre än längden på listan. För att simulera räfflings processen, använder vi längden av listorna, alltså hur många element som ingår i listorna, så  $|A| := \text{len}(lista1)$  och  $|B| := \text{len}(lista2)$ . Så för att bestämma vilket kort som kommer vara först efter blandningen använder vi samma binomialfördelningsfunktion där  $n = 1$  och sannolikheten för  $p = \frac{|A|}{|A|+|B|}$ . Om utfallet då är 1 kommer vi välja första kortet från  $A$ , annars väljs  $B$ . Om  $A$  väljs lägger vi till elementet som är först i  $A$  till i slutet på ursprungliga lista, och sedan tar vi bort det elementet från sin ursprungliga position. Samma process gäller för  $B$  om  $A$  inte väljs. Detta resulterar i att när loopen har gått ett varv har alla element i listan lagts till i slutet på listan, och tagits bort från deras ursprungliga position, vilket resulterar i att vi har en ny ordningen av listan med samma element av samma längd.

Om vi vill simulera flera blandningar av en kortlek använder vi oss av en funktion som tar input av typen: ett heltal och en lista. Heltalet bestämmer hur många gånger vi önskar applicera blandningen på listan.

Den matematiska modellen för GSR som vi har använt för programmet är inte samma som den vi presenterade i tidigare avsnitt, men är ekvivalent. Den skulle kunna beskrivas matematisk med ord som efter delning av kortleken håller vi de två



högar i vadera hand. Därefter kommer vi släppa ett kort i taget från en av högarna, där sannolikheten av val av hög bestäms efter mängden av kort i vardera hög. Likt de som beskrevs ovan.

Box shuffle är en annan blandningsmodell som vi har programmerat. På samma sätt som GSR använder funktionen en lista som motsvarar kortleken. Men vi kommer att dela kortleken i flera delar än två. För att generera positionerna för uppdelning av listan använder vi oss av multinomialfördelningen  $(n, \frac{1}{r}, r)$ . Där  $n$  är antalet element i listan och  $r$  är antalet uppdelningen. För mina simuleringar har jag valt att  $r := 4$  vilket är ett godtycklig val. Valet baserar sig på vad jag ansåg vara ett rimligt antagande och vad som verkade vara förkommande praxis vid internetsökning om blandningsmodellen. En multinomial fördelning en generalisering av den binomiala fördelning, för om vi skulle sätta  $r = 2$  skulle vi få den binomiala fördelningen eftersom vi endast har två möjliga utfall. Men om vi genomförde den multinomiala fördelningen för  $(52, \frac{1}{4}, 4)$ , kan det ses som sannolikhetsfördelning för 52 upprepade kast av en rättvis fyrsiffrig tärning och utfallet är antalet gånger vardera sida skulle hamnat uppåt. Output från den multinomiala fördelningen kommer vara en lista med med fyra parametrar som avgör var vi kommer dela listan. Så om vi antar att vi har en kortlek med 52 kort i form av en lista  $[1, 2, \dots, n]$  och sedan använder multinomiala fördelningen som ger oss en lista med parametrarna  $[a, b, c, d]$  kommer vi dela (splice) den ursprungliga listan till fyra listor. Där lista1= $[1, 2, \dots, a]$ , lista2= $[a, a+1, \dots, b]$ , lista3= $[b, b+1, \dots, c]$  och lista4= $[c, c+1, \dots, d]$ . Därefter lägger vi ihop listorna för att åstadkomma vår blandning så nya listan kommer motsvara  $lista4 + lista3 + lista2 + lista1$ .

SB är en blandningsalgoritm där vi först gör en GSR-blandning och sedan en box shuffle.

SSBS är en blandningsalgoritm där vi först gör en två GSR-blandningar och sedan en box shuffle och avslutar med en GSR-blandning.

Sedan har jag namngivit en blandningmetod Komboshuffle, där vi använder box shuffle för att dela upp leken i fyra högar  $A, B, C, D$ . Därefter lägger ihop dem till två högar  $DC$  och  $BA$  och sedan räfflar vi ihop de två högarna på samma sätt som för GSR-blandningen.

Vi har även konstruerat ytterligare en blandnings metod som vi kallar Multishuffle. Med Multishuffle delar vi upp kortleken i fyra högar på samma sätt som för Komboshuffle. Men vi sammanfogar D och C med en räfflings process och högarna B och A på samma sätt. Därefter räfflas båda högarna tillsammans.

## 9. SIMULERINGAR - FINNS DET BÄTTRE SÄTT ATT BLANDA EN KORTLEK

I detta avsnitt kommer vi att presentera resultaten av simuleringarna av olika kortblandningar och utfallen av dessa i Doyles patiens efter olika antal blandningar. Doyles patiens som vi tidigare har beskrivit har en nära koppling till TV-avståndet från den likformiga fördelningen. Vi kommer därför använda detta för att skapa en uppskattning över mixing time till den stationära fördelningen, för de olika blandningsprocesserna. Alla blandningsprocesser är aperiodiska och irreducibla, och kommer där inneha den likformiga fördelningen som entydiga stationära fördelning.

TABELL 5. Simuleringar av Doyles patient, olika blandningsmetod. 10 000 observationer.

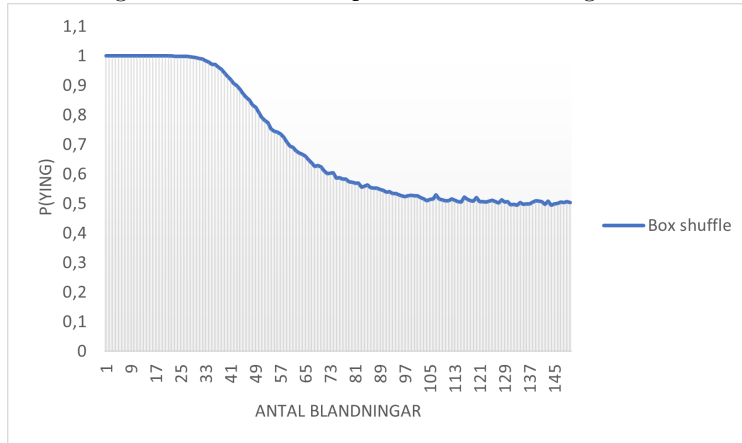
Antalet blandning	1	2	3	4	5	6	7	8	9	10
Box shuffle	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
SB	1.0	1.0	0.9997	0.9319	0.753	0.6327	0.5615	0.5224	0.5184	0.5076
Kombo	1.0	1.0	1.0	0.9999	0.9727	0.8425	0.6871	0.5883	0.5527	0.5199
Multi	1.0	1.0	1.0	0.9151	0.6885	0.572	0.5135	0.5071	0.5001	0.5038
GSR	1.0	1.0	1.0	1.0	1.0	0.9633	0.8097	0.6718	0.5913	0.536
SSBS	1.0	0.9198	0.5736	0.5134	0.5002	0.5063	0.489	0.5029	0.4962	0.4971

I tabellen kan vi se att box shuffle för sig själv inte påverkar möjligheten att vinna patiensens med tio upprepade blandning. Om vi tittar på figur 3, kan vi se att det krävs ungefär 100 blandningar innan vi är relativt nära den likformiga fördelningen mellan utfallen. Därför är blandningsmetoden i såg är inte speciellt effekt för Doyles patiens jämfört med GSR. Vi har ett ungefärligt förhållande att vi behöver göra tio gånger fler box shuffles än GSR-blandningar för att komma nära i jämvikt mellan utfallen. Box shuffle borde däremot påverka indikatorfunktionen i Lemma 23, alltså att det vänder på ordningen om kortet i  $position(\frac{n}{2})$  ligger före kortet i  $position(n)$ .

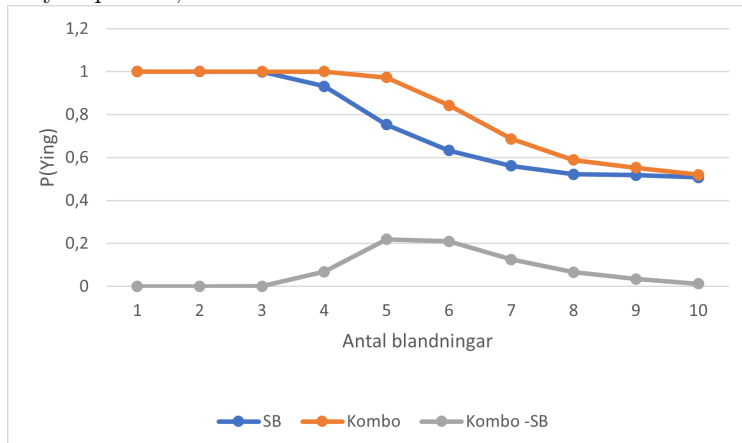
Om vi går vidare att och studerar SB, som består av en GSR- och en box shuffle, kan vi konstatera att den är effektivare än endast en GSR-blandning. Vilket är förväntat eftersom box shuffle har en positiv effekt på blandningsprocessen mot den likformiga fördelningen. Men om vi jämför fyra SB med fem GSR-blandningar ser vi att  $P(\text{ying} | 4 SB) < P(\text{ying} | 5 GSR)$ . Vilket då antyder att kombinationen av de två är effektivare på att bryta upp de stigande sekvenserna i kortleken än de två metoderna för sig om vi antar att en GSR blandning är värd 10 box shuffles. Resultatet håller även vid fler blandningar  $P(\text{ying} | 8 SB) < P(\text{ying} | 10 GSR)$ .

Om vi jämför Kombo med SB, där skillnaden i själva blandningsförfarandet är att i SB så har vi en extra delning av kortleken enligt binomialfördelningen. Vi kan se att bytpunkten inträffar tidigare för SB och differensen på utfall är störst vid  $P(\text{ying} | 5 Kombo) - P(\text{ying} | 5 SB) \approx 0.22$ .

FIGUR 3. Utfall för Box shuffle i Doyles patiens, Monte Carlo-simuleringar med 1 000 utfall per antalet blandningar.



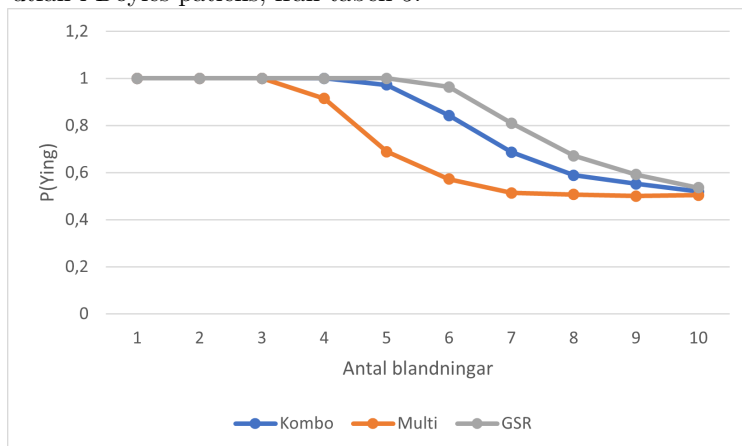
FIGUR 4. Jämförelse mellan SB- och Kombo-blandningar utfall i Doyles patiens, från tabell 5.



Om vi granskar figur 5 kan vi se att differensen mellan då två blandningsmetoderna avtar efter flera blandningar men att skillnaden är störst efter fyra till åtta blandningar.

Om vi går vidare och granskar resultaten för  $p(ying | s \text{ Multi})$ , kan vi se att blandningsmetoden verkar komma nära likformlig fördelning vid 8 till 9 blandningar. Vilket är bättre än de andra blandningsmetoderna vi har studerat. Vilket var väntat eftersom det är den blandningsmetoden flest slumpmässiga händelser som påverkar blandningsfördelning. Därför har den blandningsfördelning också fler möjliga permutationer efter en enskild blandning och har möjlighet att kraftigare påverka antalet stigande och minskande sekvenser än exempelvis GSR.

FIGUR 5. Jämförelse mellan Kombo-, Multi- och GSR-blandningars utfall i Doyles patiens, från tabell 5.



Vidare om vi tittar på resultatet av SBSS som är den mest effektiva metoden för att påverkar utfallet på spelet om vi skulle behandla det som en blandning. Och självfallet måste den vara effektivare än GSR eftersom den innehåller tre GSR-blandningar. Nedan i tabell 6 har jag ställt upp en sådan jämförelse. Vi kan se genom att blanda in en box shuffle i blandningsprocessen ger effekt på utfallet. Men om effekten är tillräcklig för att motivera att introducera en box shuffle, kan vi lämna till diskussionsdelen av uppsatsen.

TABELL 6. Jämförelse mellan SBSS och  $3 \times$  GSR

Antalet bladningar	1	2	3	4	5
3xGSR	1	0.9633	0.5913	0.5176	0.5081
SSBS	1	0.9198	0.5736	0.5134	0.5002

## 10. DISKUSSION

Vi har sett genom simuleringar att det finns varianter av GSR-blandningar som byter upp stigande och minskande sekvenser i kortleken snabbare än en vanlig GSR-blandning. Däremot kommer de blandningarna vara mer tidskrävande för den som blandar kortleken. Exempelvis motsvarar  $P(\text{ying} | 5 \text{ Kombo}) \approx P(\text{ying} | 7 \text{ GSR})$  och jag skulle spekulera att det för de flesta skulle gå snabbare att göra sju GSR-blandningar än fem Multi-blandningar. Därför skulle jag föreslå GSR-blandningsmetoden är antagligen den effektivaste metoden att blanda kortleken om vi önskar bryta den befintliga strukturen i kortleken. Om vi önskar spela ett kortspel med en välblandad kortlek där vårt val av TV-avstånd är nära den likformiga fördelning då är Box shuffle inte nödvändig att applicera. Men påstående

att korten i botten av en kortlek inte färdas uppåt i ordningen kan fortfarande gälla vi har ett lägre krav på hur välblandad kortleken behöver vara alltså färre GSR-blandningar och då är det möjligt att det finns en poäng lägga in en Box shuffle i blandningsmetodiken.

## 11. SLUTSATS

I denna uppsats har vi framförallt grundligt, på matematisk väg gått igenom, varför en kortlek blir mer och mer blandad och vilka villkor som krävs för detta. Vi kan även dra slutsatsen att hur länge vi behöver blanda en kortlek beror på vad den ska användas till. Det finns spel som det konstruerade Doyle's patiens som kräver att vi blandar kortleken nära den likformiga fördelningen för att det ska vara rättvist. De undersökta varianterna av GSR-blandningar var endast marginellt effektivare än en vanlig GSR-blandning. Utöver detta har vi visat genom simuleringar att GSR-blandningen är en effektiv metod att blanda en kortleken och vi kan mäta hur många gånger vi behöver applicera GSR-blandningen givet ett visst val av TV-avstånd till den likformiga fördelning. Men om vi önskar en kortlek som är nära fullständigt blandad behöver vi blanda kortleken mer än tio gånger. Vilket är antagligen fler gånger än de flesta skulle blanda en kortlek.

## REFERENSER

- [1] David Aldous and Persi Diaconis. Shuffling cards and stopping times. *The American Mathematical Monthly*, 93(5):333–348, 1986.
- [2] Dave Bayer, Persi Diaconis, et al. Trailing the dovetail shuffle to its lair. *The Annals of Applied Probability*, 2(2):294–313, 1992.
- [3] M. Conger and D. Viswanath. Shuffling cards for blackjack, bridge, and other card games. *arXiv: Probability*, 2006.
- [4] Persi Diaconis, RL Graham, and William M Kantor. The mathematics of perfect shuffles. *Advances in applied mathematics*, 4(2):175–196, 1983.
- [5] Jan Enger and Jan Grandell. *Markovprocesser och köteori*. Kungl tekniska høgskolan, Institutionen fr matematik, Avd. fr Matematisk . . . , 2003.
- [6] Gina Kolata. In shuffling cards, 7 is winning number. *New York Times*, Jan 1990.
- [7] David A Levin and Yuval Peres. *Markov chains and mixing times*, volume 107. American Mathematical Soc., 2017.
- [8] Sarah Griffiths for MailOnline and Antoine Arraou. How to shuffle cards like a pro shown by a mathematician, Mar 2015.
- [9] Brad Mann. How many times should you shuffle a deck of cards. *Topics in Contemporary Probability and Its Applications*, 15:1–33, 1995.
- [10] Anke Van Zuylen and Frans Schalekamp. The achilles’heel of the gsr shuffle: A note on new age solitaire. *Probability in the Engineering and Informational Sciences*, 18(3):315–328, 2004.
- [11] Wikipedia contributors. Probability theory — Wikipedia, the free encyclopedia, 2020. [Online; accessed 20-November-2020].