Over het schudden van kaarten

Anke van Zuylen Frans Schalekamp

31 augustus 2000

scriptiecommissie

Prof. dr. H.C. Tijms

dr. A. Ridder

Prof. dr. R. Meester

Voorwoord

Deze scriptie hebben wij geschreven ter afsluiting van de studie econometrie aan de Vrije Universiteit. Natuurlijk is het grootste deel van deze noeste arbeid op ons conto te schrijven, we willen edoch de volgende mensen bedanken voor hun onmisbare bijdrage.

We willen uiteraard professor Tijms bedanken voor het aankaarten van het onderwerp en voor de doorverwijzingen naar deskundigen en boeken van deskundigen, wanneer wij er niet meer uitkwamen. Zijn enthousiasme voor dit onderwerp werkte aanstekelijk. Professor Ditters is één van deze deskundigen. We zijn hem zeer erkentelijk voor de tijd en moeite die hij voor ons heeft genomen. Ook heeft hij ons doorverwezen naar dr. Van der Waall van de UvA. Zonder zijn hulp was het bewijs van onze belangrijkste stelling niet compleet geweest. Dankzij de kritische blik van de overige twee leden van onze scriptiecommissie, professor Meester en dr. Ridder, staan in deze versie van de scriptie minder fouten dan in de eerste. Wij zijn hen zeer erkentelijk hiervoor.

Naast wiskundige problemen kwamen we ook praktische problemen tegen. We willen Liesbeth Douma, de moeder van Frans, bedanken voor het in bruikleen geven van haar laptop op een cruciaal moment en het fungeren als telefonisch raadpleegbare Binas. Wim de Haas en Rietje van Zuylen zijn zelfs zover (naar China) gegaan, hun hele huis ter beschikking te stellen. Het was een zeer prettige werkomgeving voor de laatste loodjes. Henk van Zuylen, de vader van Anke, bedanken we hierbij voor het leveren van de TeX-cd en bijbehorende handleiding.

Het uitleggen van ons scriptie-onderwerp aan geïnteresseerde en minder geïnteresseerde luisteraars op feestjes en dergelijke, heeft ons ook geholpen. In dit verband willen we met name Miep Kruseman, de stiefmoeder van Frans, niet onvermeld laten. Haar enthousiasme voor het quizmaster-probleem, dat overigens de scriptie niet gehaald heeft, compenseerde ruimschoots de keren dat we een minder geïnteresseerd persoon tegenover ons hadden. Ook het enthousiasme van Christiaan Höhner na het lezen van een eerste versie van deze scriptie, heeft ons zeer gestimuleerd.

Tenslotte bedanken we naast reeds hierboven genoemde personen, de volgende mensen voor hun “emotionele support”: Adrie Timmer, de moeder van Anke, in het bijzonder voor haar kaartjes, en Willem en Ellen van Zuylen, voor het noemen van Ankes naam in hun scripties.

Inhoudsopgave

Hoofdstuk 1

Inleiding

Bij een bridgeclub in New York bestond het vermoeden dat enkele van de leden vals speelden. Om dit te onderzoeken, riep de club de hulp in van de wiskundige, en tevens goochelaar, Persi Diaconis. Zijn verrassende conclusie luidde dat er geen sprake was van vals spel, maar dat er te weinig geschud werd! De bridgespelers profiteerden hiervan, doordat de verdeling van de kaarten na het schudden niet willekeurig was: bepaalde volgordes van de kaarten waren waarschijnlijker. Gewapend met deze kennis en door de volgorde van de kaarten na het laatste spel te onthouden, waren de vermeende valsspelers in het voordeel.

De vraag is hoeveel keer een pak kaarten dan wel geschud moet worden, opdat dit soort "vals spel" niet kan voorkomen. Dit lijkt op het eerste gezicht misschien een eenvoudige vraag; schudden kan gemodelleerd worden als een Markovketen en hiermee kan de kansverdeling na elk aantal keer schudden direct bepaald worden. Dit blijkt praktisch onuitvoerbaar, aangezien de toestandsruimte al gauw te groot wordt: bij een pak kaarten (52 kaarten) zijn er 52! ($\sim 10^{68}$) mogelijke ordeningen, die samen de toestandsruimte vormen (zie hoofdstuk 2).

Er is daarom aardig wat literatuur ontstaan omtrent dit onderwerp. De literatuur richt zich voornamelijk op de Amerikaanse manier van schudden, de zogenaamde *riffle shuffle*: het pak kaarten wordt ongeveer in het midden gesneden, de twee stapeltjes worden ieder in één hand genomen en vervolgens "in elkaar geritst". Met name een door Gilbert en Shannon (in de jaren '50), en onafhankelijk door Reeds (1981), ontwikkelde wiskundige beschrijving (de *GSR-shuffle* of *uniforme riffle shuffle*), is veel geanalyseerd. Deze populariteit is vooral te verklaren uit het feit dat deze beschrijving wiskundig "hanteerbaar" is. Wat we hiermee bedoelen zal later duidelijk worden. Opvallend is dat er geen literatuur bestaat die onderzoekt hoe goed deze modellering overeenkomt met de manier waarop werkelijk geschud wordt.

We willen in deze scriptie de vraag onderzoeken, hoe vaak er geschud moet worden, opdat er geen voordeel behaald kan worden door kennis van het schudden. We zullen ons hierbij beperken tot de hierboven genoemde riffle shuffle.

We beginnen met wiskundig vastleggen van het schudproces. We introduceren allereerst het begrip permutatie, om de kaartvolgorde binnen een pak aan te geven, en laten zien dat het schudden een Markovketen vormt. We zullen een instrument, de variation distance, gebruiken om te bepalen in hoeverre een pak goed geschud is.

Vervolgens beperken we ons tot de riffle shuffle. We leggen de kansen van het GSR-model vast in hoofdstuk 3 en we behandelen verschillende methodes uit de literatuur die een antwoord proberen te geven op de vraag hoe vaak geschud moet worden. In de literatuur worden harde conclusies geformuleerd. Zo wordt beweerd dat voor 52 kaarten, 7 keer schudden “genoeg” is. Wij willen deze conclusie niet onderschrijven en zullen bij de behandeling van de literatuur aangeven, waar de auteurs ons inziens hun hand overspelen. Een spelletje van Peter Doyle laat zien dat het soms mogelijk is dat een 7 keer geschud pak kaarten zeer oneerlijke kansen op winst geeft. We zullen wiskundig aantonen waarom dit zo is, en bovendien laten we zien dat dit spel precies het “oneerlijkste” spel is, wanneer er met een riffle shuffle wordt geschud.

We maken verder enkele opmerkingen aangaande de validiteit van de aannames die ten grondslag liggen aan het GSR-model. Door middel van een analyse van de eigenwaarden en de variation distance voor zeer kleine pakken kaarten, proberen we te bepalen in hoeverre (afwijkingen van) de gemaakte aannames van invloed zijn op de conclusies. Om de eigenwaarden te berekenen, hebben wij een methode van Doner en Uppuluri [Doner & Uppuluri, 1970] uitgebreid. En passant, stuitten wij hierbij op een eigenschap van cyclische ondergroepen van de symmetrische groep, die niet algemeen bekend was.

Hoofdstuk 2

Modelleren van het schudden

Samenvatting We leggen wiskundig vast wat schudden is. Hiertoe wordt het begrip permutatie geïntroduceerd en veronderstellen we een kansverdeling op de schudoperaties. Door aan te nemen dat de afzonderlijke schudbeurten onafhankelijk zijn, vormt het schudden een Markovketen. We geven enkele voorwaarden waaraan een goede schudmethode tenminste moet voldoen en definiëren een instrument, de variation distance, om te bepalen in hoeverre een pak goed geschud is.

2.1 Inleiding

Wanneer we ons afvragen hoe vaak we moeten schudden, willen we weten hoeveel keer er geschud moet worden zodanig dat er geen voordeel behaald kan worden met de kennis van hoe er geschud is en hoe de beginvolgorde van de kaarten was, of door de ligging van de kaarten. Een (extreem) voorbeeld: Stel, je wint 1 gulden als je de hartenaas trekt uit een pak van 52 kaarten. Je geeft de spelleider een pak waarvan je weet dat de hartenaas onderop zit. De spelleider schudt het pak één keer met een riffle shuffle. De kans dat de hartenaas weer onderop zit is de kans dat de eerste kaart die de spelleider laat vallen uit de hand komt waarin de hartenaas (onderop) zit. Deze kans zal in de buurt van een half liggen en is in ieder geval veel groter dan $\frac{1}{52}$, de kans dat je de juiste kaart aanwijst wanneer niets bekend is over beginvolgorde en schudmethode.

Het moge duidelijk zijn dat het voordeel dat behaald kan worden afhankelijk is van het spel. In bovenstaand voorbeeld is de verwachte opbrengst wanneer je niets weet gelijk aan $\frac{1}{52} \times 1$ gulden. Wanneer de spelleider het pak met de hartenaas onderop gebruikt èn je wijst de laatste kaart aan is de verwachte opbrengst ongeveer 50 cent. Het voordeel is ongeveer $\frac{1}{2} - \frac{1}{52}$ gulden.

In het meest ideale geval is er geen voordeel te behalen bij welk spel dan ook. De kans op elke volgorde van de kaarten is dan gelijk. We zullen dit allemaal wat preciezer maken, daartoe introduceren we de begrippen *permutatie*, *Markovketen* en *variation distance*.

2.2 Permutaties

De toestand van het pak kaarten, de volgorde waarin de kaarten zitten, kunnen we aanduiden met behulp van het begrip *permutatie*. Een permutatie π van een verzameling $\{1, 2, \ldots, n\}$ (de n kaarten waaruit het pak bestaat labellen we met de cijfers 1 tot en met n) is een bijectieve afbeelding in zichzelf.

Voorbeeld $\pi = (1\ 5\ 2\ 6\ 3\ 4)$ is een permutatie van $\{1, 2, \ldots, 6\}$. De volgorde van de kaarten die we hiermee associëren is: kaart 1, kaart 5, kaart 2, etcetera. In het algemeen geeft een permutatie $\pi = (\pi(1)\ \pi(2)\ \ldots\ \pi(n))$ de kaartvolgorde $\pi(1), \pi(2)$, tot en met $\pi(n)$ weer.

Let op: In sommige literatuur wordt de inverse gebruikt. Bovenstaande permutatie wil dan zeggen dat kaart 1 op plaats 1 zit, kaart 2 op plaats 5, kaart 3 op plaats 2, etcetera.

We zullen het begrip permutatie niet alleen gebruiken als beschrijving van de *kaartvolgorde* (het resultaat van een schudhandeling), maar ook als beschrijving van een bepaalde schudhandeling zelf (de *operatie*). We noteren de schudhandeling dan op dezelfde manier als het resultaat van deze schudhandeling uitgevoerd op een geordend pak (een pak waarin de kaarten op volgorde 1 tot en met n zitten).

Voorbeeld We kunnen de permutatie in bovenstaand voorbeeld ook beschouwen als schudhandeling, toegepast op een geordend pak. Toegepast op een permutatie (toestand) $\sigma = (3\ 2\ 5\ 1\ 6\ 4)$ geeft deze schudhandeling als resultaat de permutatie (toestand) $(3\ 6\ 2\ 4\ 5\ 1)$. We noteren dit als $\sigma\pi$.

Het uitvoeren van een permutatie σ gevolgd door een permutatie π geeft hetzelfde resultaat als het uitvoeren van de permutatie $\sigma\pi$ met $(\sigma\pi)(i) = \sigma(\pi(i))$.

We merken nog op dat permutaties onder deze operatie (het compositieprodukt) een bekende groep uit de algebra vormen, de symmetrische groep $\mathcal{S}_n$ (zie voor details een willekeurige inleiding in de algebra).

Eigenschap 2.1 *Elk element π van $\mathcal{S}_n$ heeft een unieke inverse in $\mathcal{S}_n$.*

Dit volgt direct uit de definitie (een bijectieve afbeelding heeft een unieke inverse).

Voorbeeld De inverse van de permutatie $\pi = (1\ 5\ 2\ 6\ 3\ 4)$ is de permutatie $\pi^{-1} = (1\ 3\ 5\ 6\ 2\ 4)$.

Eigenschap 2.2 *Het aantal elementen in $\mathcal{S}_n$ is $n!$.*

2.3 Markovketen

Definitie 2.3 *Een schudbeurt is een vaste kansverdeling op de verschillende mogelijke operaties.*

Met andere woorden, de beginsituatie (volgorde van de kaarten) heeft geen invloed op het schudden (wel natuurlijk op het resultaat van de schudbeurt). Het totale schudden is dan op te vatten als een reeks onafhankelijke schudbeurten. Dit is niets anders dan (een speciaal geval van) de *Markoveigenschap*. We definiëren een rij stochastische variabelen $(X_s)_{s \in \mathbb{Z}^+}$, waarbij X_s de permutatie (kaartvolgorde) is na schudbeurt s.

Eigenschap 2.4 (Markoveigenschap) $\mathbb{P}(X_{s+1} = \pi \mid X_s = \sigma;\ X_{s-1} = \sigma_{s-1};\ \dots\ ;\ X_0 = \sigma_0) = \mathbb{P}(X_{s+1} = \pi \mid X_s = \sigma)$.

Bovendien zijn de deze overgangskansen stationair; de kansverdeling hangt niet af van het aantal reeds uitgevoerde schudbeurten. $\mathbb{P}(X_{s+1} = \pi \mid X_s = \sigma) = \mathbb{P}(X_1 = \pi \mid X_0 = \sigma)\ \forall s \in \mathbb{Z}^+$.

We kunnen het schudproces derhalve modelleren als een Markovketen met stationaire overgangskansen, met toestandsruimte $I = \mathcal{S}_n$: er kan een (Markov)matrix opgesteld worden met de overgangskansen $p_{\sigma\pi} = \mathbb{P}(X_{s+1} = \pi \mid X_s = \sigma)$.

Voorbeeld We beschouwen een pak met drie kaarten. De toestandsruimte I is $\{(123), (132), (213), (231), (312), (321)\}$. We definiëren een schudbeurt als:

$$
\begin{aligned}
\mathbb{P}\Big((123) \to (123)\Big) &= p_1\\
\mathbb{P}\Big((123) \to (132)\Big) &= p_2\\
\mathbb{P}\Big((123) \to (213)\Big) &= p_3\\
\mathbb{P}\Big((123) \to (231)\Big) &= p_4\\
\mathbb{P}\Big((123) \to (312)\Big) &= p_5\\
\mathbb{P}\Big((123) \to (321)\Big) &= p_6
\end{aligned}
$$

met $p_1 + p_2 + \cdots + p_6 = 1$ ($p_i \geq 0\ \forall i$). De bijbehorende Markovmatrix is dan:

$$
\begin{array}{c}
\\ (123) \\ (132) \\ (213) \\ (231) \\ (312) \\ (321)
\end{array}
\begin{bmatrix}
(123) & (132) & (213) & (231) & (312) & (321) \\
p_1 & p_2 & p_3 & p_4 & p_5 & p_6 \\
p_2 & p_1 & p_5 & p_6 & p_3 & p_4 \\
p_3 & p_4 & p_1 & p_2 & p_6 & p_5 \\
p_5 & p_6 & p_2 & p_1 & p_4 & p_3 \\
p_4 & p_3 & p_6 & p_5 & p_1 & p_2 \\
p_6 & p_5 & p_4 & p_3 & p_2 & p_1
\end{bmatrix}
$$

Lemma 2.5 *De matrix behorend bij een schudproces is dubbelstochastisch.*

Bewijs Per definitie sommeren de rijen van een Markovmatrix tot 1. Ook de kolommen sommeren tot 1. Aangezien elke permutatie een unieke inverse heeft, is er precies één operatie σ die resulteert in π_j wanneer deze uitgevoerd wordt op π_i. Uitgevoerd op een permutatie $\pi_k \neq \pi_i$ resulteert de operatie σ niét in π_j. Elk element komt in iedere kolom dus precies één keer voor. $\square$

Het resultaat van herhaalde schudbeurten kan direct berekend worden door deze matrix met zichzelf (herhaald) te vermenigvuldigen. We noteren met $p^{(s)}_{\sigma\pi} := \mathbb{P}(X_s = \pi \mid X_0 = \sigma)$, en met $P^{(n)}$ de bijbehorende matrix. Een welbekend resultaat is

Eigenschap 2.6 (De vergelijkingen van Chapman-Kolmogorov) *Voor alle $s, t \in \mathbb{Z}^+$ geldt*

$$
p^{(s+t)}_{\sigma\pi} = \sum_{\tau \in I} p^{(s)}_{\sigma\tau} p^{(t)}_{\tau\pi} \qquad (\pi, \sigma \in I).
$$

In matrixnotatie: $P^{(s+t)} = P^{(s)}P^{(t)}$.

Met iteratie en $P = P^{(1)}$ *volgt*

$$P^{(s)} = P^s.$$

In 1955 gooiden de wiskundigen van AT&T Bell Laboratories in Murray Hill, die zich bezig hielden met het schudprobleem, de handdoek in de ring, omdat bij 52 kaarten, er 52! mogelijke permutaties zijn. De Markovmatrix is dan een $52! \times 52!$ ($52! \sim 10^{68}$) matrix. Om een idee te geven hoe groot dit getal is, stellen we ons voor dat we op elk molecuul een element van de matrix schrijven. Dan is ongeveer 1/3 van alle moleculen in dit melkwegstelsel nodig om alle elementen op te kunnen schrijven. Er zijn duidelijk andere benaderingen van dit probleem nodig.

Hoewel het praktisch onmogelijk is de verdeling na elke schudbeurt te berekenen, kunnen we met behulp van de Markovtheorie wel voorwaarden formuleren, waaraan een "goede" schudmethode moet voldoen.

2.4 Convergentie van de Markovketen

De situatie die we hopen te bereiken, is die waarin we "niets weten", oftewel, die waarin elke kaart (met gelijke kans) op elke plek kan zitten. Kortom, in de ideale situatie is elke permutatie even waarschijnlijk; $\mathbb{P}(X_s = \pi) = \frac{1}{n!}\ \forall \pi \in I$. Dit is niets anders dan de *uniforme verdeling* U.

Bij het schudprobleem gaan we ervan uit dat de beginsituatie (deels) bekend is (anders is er geen probleem). Het ideale schudresultaat na s keer schudden is dan dat elke permutatie even waarschijnlijk is, onafhankelijk van de beginsituatie:

$$\mathbb{P}(X_s = \pi \mid X_0 = \sigma) = \frac{1}{n!}\ \forall \pi, \sigma \in I.$$

De enige schudmethode die werkelijk dit resultaat geeft, is die waarbij elke permutatie (operatie) kans $1/n!$ heeft. Bij in de praktijk gebruikte methodes zijn meestal niet alle permutaties bereikbaar na één keer schudden, en is de kans op sommige permutaties groter dan op andere. We zullen het moeten doen met schudmethodes die naar de uniforme verdeling *convergeren.* Zeer slordig gezegd wil dat zeggen, dat de verdeling die het resultaat is van s schudbeurten, de uniforme verdeling steeds beter benadert naarmate s groter wordt.

Uit de Markovtheorie weten we, dat als de Markovketen van het schudproces positief-recurrent en aperiodiek is, voor elke beginsituatie σ $\lim_{s\to\infty} p^s_{\sigma\pi}$ bestaat en een kansverdeling is. We noemen deze de evenwichtsverdeling. Aangezien de Markovmatrix P van een schudproces dubbelstochastisch is, is dit de uniforme verdeling.

We verklaren de gebruikte criteria voor een "goede" schudmethode nader.

Positief-recurrentie. Uit de Markovtheorie is bekend dat een Markovketen met eindige toestandsruimte (zoals bij het schudden) positief-recurrent is als elke twee toestanden communiceren. We zeggen dat twee toestanden π en σ communiceren, wanneer $\exists s \in \mathbb{Z}^+ : \mathbb{P}(X_s = \pi \mid X_0 = \sigma) > 0$ èn $\exists t \in \mathbb{Z}^+ : \mathbb{P}(X_t = \sigma \mid X_0 = \pi) > 0$.

Aperiodiciteit. De periode van een toestand π is de grootste gemene deler van de verzameling van alle aantallen keren schudden waarmee we weer in π kunnen terugkeren:

$$\text{periode}(\pi) := \text{ggd}(\{s \in \mathbb{N} : p^{(s)}_{\pi\pi} > 0\}).$$

Aangezien alle toestanden communiceren, zijn de periodes van alle toestanden gelijk. We noemen een Markovketen aperiodiek wanneer $\forall \pi \in I : \text{periode}(\pi) = 1$.

Een goede schudmethode convergeert dus naar de uniforme verdeling, onafhankelijk van de beginsituatie. Dat niet elke schudmethode aan bovenstaande voorwaarden voldoet, laat het volgende voorbeeld zien van de *perfect shuffle* (die dus helemaal niet zo perfect is als zijn naam doet vermoeden).

Voorbeeld (Perfect shuffle) Een *perfect shuffle* is een riffle shuffle, die "perfect" wordt uitgevoerd: steeds wordt het pak *precies* in het midden gesneden, en vervolgens worden de kaarten uit de twee stapeltjes, precies om-en-om (links-rechts-links-rechts-etcetera) in elkaar geritst. Het lijkt of er niet beter geschud kan worden. Niets is echter minder waar. Deze schudmethode geeft geen goede resultaten, omdat deze volkomen deterministisch is. Na 8 perfect shuffles blijkt een pak van 52 kaarten zelfs tot de oorspronkelijke volgorde te zijn teruggekeerd! We zullen dit aantonen.

De perfect shuffle is herhaald toepassen van de permutatie: $(1\ 27\ 2\ 28\ 3\ 29\ \cdots\ 26\ 52)$. We introduceren een andere manier van beschrijven van permutaties, de cykelnotatie.

Definitie 2.7 *Beschouw een permutatie. Een cykel is een k-tupel $(x_1\ x_2\ \ldots\ x_k)$, met x_i's de gepermuteerde objecten, zodanig dat na het uitvoeren van de permutatie x_i op de plaats van x_{i+1} terecht is gekomen, en x_k op de plaats van x_1.*

Een permutatie kan opgedeeld worden in *partities*, die ieder een *cykel* zijn.

Bij 52 kaarten genereert de perfect shuffle de volgende cykels (partities).

(1)
(2 3 5 9 17 33 14 27)
(4 7 13 25 49 46 40 28)
(6 11 21 41 30 8 15 29)
(10 19 37 22 43 34 16 31)
(12 23 45 38 24 47 42 32)
(18 35)
(20 39 26 51 50 48 44 36)
(52).

Het kleinste gemene veelvoud van de lengtes van alle cykels geeft precies de periode geeft van de permutatie. Bij 52 kaarten is de periode 8.

In het algemeen geldt voor $2n$ kaarten bij de perfect shuffle een periode r, waarbij $r \in \mathbb{N}$ de kleinst mogelijke oplossing is van $2^r \equiv 1 \pmod{n-1}$ [Epstein, 1977].

Bewijs De nieuwe positie a_1 van de kaart op positie a_0 wordt gegeven door $a_1 \equiv 2 \times a_0 - 1 \pmod{2n-1}$. Herhaald invullen geeft na s perfect shuffles: $a_s \equiv 2^s a_0 - (\sum_{i=0}^{s-1} 2^i) \pmod{2n-1}$. Omdat $\sum_{i=0}^{s-1} 2^i = 2^s - 1$, volgt nu dat de periode de kleinst mogelijke oplossing is van $2^r \equiv 1 \pmod{n-1}$. □

Hieronder volgt een tabel uit [Epstein, 1977] met de waarden van r voor $2n$ kaarten.

$2n$	r	$2n$	r	$2n$	r
2	1	22	6	42	20
4	2	24	11	44	14
6	4	26	20	46	12
8	3	28	18	48	23
10	6	30	28	50	21
12	10	32	5	52	8
14	12	34	10	54	52
16	4	36	12	56	20
18	8	38	36	58	18
20	18	40	12	60	58

2.5 Variation distance

We weten nu aan welke voorwaarden een schudmethode tenminste moet voldoen, om goede resultaten te kunnen geven. We weten echter nog niet hoe vaak er geschud moet worden (de "snelheid" van convergentie). Hoewel we hebben gezien dat het ondoenlijk is, de totale kansverdeling na s keer schudden te construeren, kan er in sommige gevallen wel iets gezegd worden over de *variation distance*. De variation distance geeft de "afstand" aan tussen twee kansverdelingen Q en R:

Definitie 2.8 *De variation distance tussen twee kansverdelingen Q en R op een discrete toestandsruimte I is gelijk aan*

$$\begin{aligned} \|Q - R\| &= \max_{A \subseteq I}(Q(A) - R(A)) \\ &= \frac{1}{2}\sum_{i \in I} |Q(i) - R(i)| \leq 1. \end{aligned}$$

Dat de laatste twee termen inderdaad gelijk zijn, is als volgt in te zien: We delen de toestandsruimte I op in $A^+ := \{i \in I \mid Q(i) \geq R(i)\}$ en $A^- := I \backslash A^+$. Het is duidelijk dat $Q(A) - R(A)$ zijn maximum aanneemt in $A = A^+$. Nu is $\frac{1}{2}\sum_{i \in I} |Q(i) - R(i)| = \frac{1}{2}\big(Q(A^+) - R(A^+) + R(A^-) - Q(A^-)\big) = Q(A^+) - R(A^+)$. Immers $Q(A^+) - R(A^+) = R(A^-) - Q(A^-)$, want $Q(A^+) + Q(A^-) = R(A^+) + R(A^-) = 1$.

Deze maat is een bruikbaar middel om schudmethodes te vergelijken, aangezien deze een bovengrens geeft op het verschil in winstkans. We zullen uitleggen wat we hiermee bedoelen.

We beschouwen allereerst een *deterministisch spel*. Bij een deterministisch spel bepaalt de ligging van de kaarten volledig of een speler wint of niet. Met andere woorden er is een deelverzameling van de toestandsruimte aan te geven, waarvoor een speler wint.

Voorbeeld Een voorbeeld van een deterministisch spel, is het spel waarbij de speler wint als de onderste kaart de hartenaas is.

Interpretatie 2.9 *(i) Voor elk deterministisch spel geldt*

$$\big|\mathbb{P}_Q(\textit{“speler wint”}) - \mathbb{P}_R(\textit{“speler wint”})\big| \leq \|Q - R\|,$$

met $\mathbb{P}_T$*("speler wint") de kans dat de speler wint bij het spel, gegeven er is geschud met uitkomst verdeeld als* T*.*
Er is een deterministisch spel te definiëren waarvoor geldt $\mathbb{P}_Q$*("speler wint")* $-$ $\mathbb{P}_R$*("speler wint")* $= \|Q - R\|$.

Bewijs Definieer $A \subseteq I$ als die kaartvolgordes waarbij de speler wint.

$$\begin{aligned}
\mathbb{P}_Q(\text{“speler wint”}) - \mathbb{P}_R(\text{“speler wint”}) &= Q(A) - R(A) \\
&\leq \max_{A \subseteq I}(Q(A) - R(A)) \\
&= \|Q - R\|.
\end{aligned}$$

Evenzo vinden we $\mathbb{P}_R(\text{“speler wint”}) - \mathbb{P}_Q(\text{“speler wint”}) \leq \|R - Q\| = \|Q - R\|$, waarmee het resultaat is bewezen.
De gelijkheid geldt wanneer A die deelverzameling is waarop $Q(A) - R(A)$ het maximum aanneemt (dit is A^+ zoals boven). $\square$

Interessanter zijn spelletjes waarbij de speler keuzes kan maken. Een *strategie* is een voorschrift, dat op elk moment dat er een keuze gemaakt moet worden, aangeeft wat er gekozen moet worden. Een *optimale strategie* is een strategie, waarbij de kans dat de speler wint maximaal is.

Voorbeeld Een voorbeeld van een spel met strategie, is het spel waarbij de speler een kaart kiest, en wint als deze kaart de hartenaas is. Wanneer de speler weet, dat de kans dat de hartenaas onderop zit, gelijk is aan een half, dan is de optimale strategie natuurlijk de laatste kaart te kiezen.

We geven nog een voorbeeld van een strategie. In Black Jack kan men zich verzekeren tegen "Black Jack" (aas en tien) bij de dealer als de dealer een aas open heeft liggen. Op het moment dat de speler weet dat er geen tienen meer in het spel zijn, is dit natuurlijk onvoordelig. Een optimale strategie zal voorschrijven niet te verzekeren. Overigens is het spel Black Jack vaak door wiskundigen bestudeerd. Voor optimale strategieën verwijzen wij naar [Epstein, 1977] of op internet http://www.thewizardofodds.com.

Tenslotte merken we op, dat er een optimale strategie bestaat die op elk keuzemoment een *vaste* keuze voorschrijft. Stel namelijk dat dit niet het geval is, dan zou er dus een betere strategie zijn die op een bepaald keuzemoment verschillende keuzes voorschrijft. Dan is ofwel de ene keuze beter dan de andere, en hebben we een betere optimale strategie gevonden (tegenspraak), ofwel de keuzes geven een even grote winstkans. In het laatste geval is elk van deze keuzes optimaal, en is deze strategie niet beter dan dezelfde strategie met in deze situatie een vaste keuze.

Uit het feit dat er een optimale strategie met vaste keuzes bestaat, volgt dat er ook in dit geval aan de ligging van de kaarten gezien kan worden of de speler die met deze strategie speelt, wint of niet. Er bestaat derhalve een deelverzameling van I die precies die toestanden bevat waarbij de speler wint.

Interpretatie 2.9 *(ii) Voor een spel met strategie geldt*

$$\left|\mathbb{P}_Q^{opt}(\text{"speler wint"}) - \mathbb{P}_R^{opt}(\text{"speler wint"})\right| \leq \|Q - R\|,$$

met $\mathbb{P}_T^{opt}$*("speler wint") de kans dat de speler wint bij het spel, gegeven er is geschud met uitkomst verdeeld als* T *en de speler speelt volgens een optimale strategie.*

Bewijs Definieer $A_T^{\text{opt}} \subseteq I$ als die kaartvolgordes waarbij de speler wint, wanneer hij speelt met een vaste strategie, die optimaal is gegeven dat er is geschud met uitkomst verdeeld als T.

$$\begin{aligned}
\mathbb{P}_Q^{\text{opt}}(\text{"speler wint"}) - \mathbb{P}_R^{\text{opt}}(\text{"speler wint"}) &= Q(A_Q^{\text{opt}}) - R(A_R^{\text{opt}}) \\
&\leq Q(A_Q^{\text{opt}}) - R(A_Q^{\text{opt}}) \\
&\leq \|Q - R\|.
\end{aligned}$$

Evenzo vinden we $\mathbb{P}_R^{\text{opt}}(\text{"speler wint"}) - \mathbb{P}_Q^{\text{opt}}(\text{"speler wint"}) \leq \|R - Q\| = \|Q - R\|$, waarmee het resultaat is bewezen.

□

De variation distance is dus een bovengrens op het verschil in waarschijnlijkheid van winnen, als twee schudmethodes vergeleken worden. Wanneer we de vraag stellen, hoe vaak met een bepaalde schudmethode geschud moet worden, willen we kijken in hoeverre de *uniforme verdeling* U benaderd wordt. We noteren de variation distance tussen de kansverdeling na s keer schudden en de uniforme verdeling U als $\|Q^{*s} - U\|$, met Q^{*s} en U $(1 \times n!)$ vectoren.

Q^{*s} is de kansverdeling op de permutaties na s keer schudden waarbij we veronderstellen dat de beginpermutatie π_0 bekend is. Anders gezegd, we beginnen met een startverdeling x_0, een $(1 \times n!)$ vector met één 1 voor element π_0 en verder nullen ($\mathbb{P}(X_0 = \pi_0) = 1$). Dus $Q^{*s} = x_0 P^s$. Aangezien het schudproces is gedefinieerd als een kansverdeling op de *operaties*, maakt het niet uit bij welk element van x_0 een 1 staat. Voor een startverdeling x_0', waarbij meerdere permutaties een positieve kans hebben, geldt: $\|x_0' P^s - U\| \leq \|Q^{*s} - U\|$, wat eenvoudig te bewijzen is met behulp van de driehoeksongelijkheid.

We zullen in de volgende hoofdstukken, tenzij anders vermeld, met “variation distance” de variation distance tusen de kansverdeling resulterend uit een schudproces en de uniforme verdeling aangeven.

We zijn nu voldoende wiskundig bewapend om te bekijken wat in de literatuur gedaan is met het schudprobleem. We zullen beginnen met een wiskundige beschrijving van een riffle shuffle te introduceren, die in de literatuur hoofdzakelijk is geanalyseerd.

Hoofdstuk 3

De GSR- of uniforme riffle shuffle

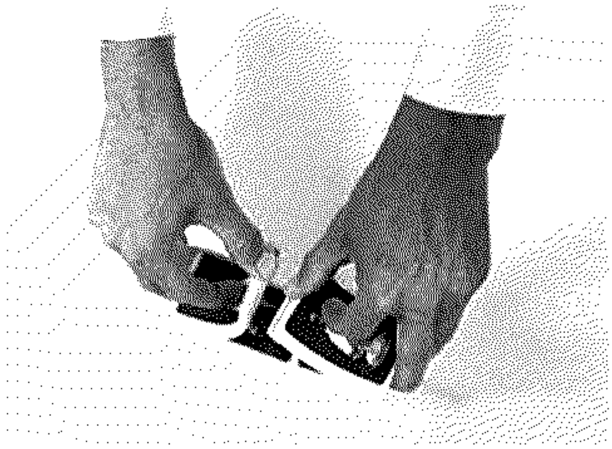
Samenvatting We leggen het in de literatuur veel gebruikte model voor de riffle shuffle, de GSR- of uniforme riffle shuffle vast. Bovendien geven we enkele alternatieve beschrijvingen van dit model. De verdeling na herhaald schudden is af te leiden met behulp van de inverse beschrijving.

3.1 Modelaannames

Bij een riffle shuffle wordt het pak kaarten in tweeën gesplitst, de twee delen worden elk in één hand genomen en vervolgens worden de twee delen "ineengeritst" door afwisselend kaart(en) van de ene en de andere hand te laten vallen.

Een model dat deze shuffle beschrijft is ontwikkeld door Gilbert en Shannon en, onafhankelijk van de andere twee, door Reeds, vandaar de benaming GSR-shuffle. We zullen zien dat de kans op alle mogelijke manieren van splitsen gevolgd door het ineenritsen van de twee delen gelijk is, wat de andere naam voor deze schudmethode, de uniforme shuffle, verklaard. In deze scriptie zullen wij de benaming GSR-shuffle gebruiken voor dit model.

Aanname 3.1 *De kans dat de splitsing K in het pak kaarten na k kaarten valt, wordt binomiaal $(n, \frac{1}{2})$ verdeeld verondersteld. Oftewel, de kans dat kaart $k \in \{0, \ldots, n\}$ de laatste kaart is van het eerste deel is gelijk aan $\mathbb{P}(K = k) = \binom{n}{k}/2^n$. (Lege stapeltjes zijn mogelijk, bij $K = 0$ en $K = n$.)*



Vervolgens worden kaarten uit de linker- en rechterhand weer ineengeritst. De onderlinge volgorde van de kaarten uit één hand blijft hierbij ongewijzigd; nadat het schudden is voltooid resulteert een permutatie waarin kaart 1 tot en met K in hun oorspronkelijke volgorde zitten, maar waarin deze reeks onderbroken kan worden door de reeks van de kaarten $K+1$ tot en met n.

Aanname 3.2 *De kans dat de volgende kaart uit de ene dan wel de andere hand komt, wordt gelijk verondersteld aan het aantal kaarten in desbetreffende hand gedeeld door het aantal kaarten in beide handen samen.*

Voorbeeld Een pak van $n = 6$ kaarten wordt gesplitst na kaart 2. De kans op de permutatie (3 1 4 2 5 6), is, gegeven de splitsing na kaart 2, gelijk aan

$$\mathbb{P}(3\ 1\ 4\ 2\ 5\ 6 \mid K = 2) = \frac{4}{6} \cdot \frac{2}{5} \cdot \frac{3}{4} \cdot \frac{1}{3} \cdot \frac{2}{2} \cdot \frac{1}{1}$$
$$= \frac{n-k}{n} \cdot \frac{k}{n-1} \cdot \frac{n-k-1}{n-2} \cdot \frac{k-1}{n-3} \cdot \frac{n-k-2}{n-4} \cdot \frac{n-k-3}{n-5}.$$

Zoals in bovenstaand voorbeeld gezien kan worden, wordt de noemer van de voorwaardelijke kans op een permutatie, gegeven de splitsing, gevormd door de termen $n(n-1)(n-2)\cdot\cdots\cdot 1$. De teller geeft in een bepaalde volgorde de termen $k(k-1)(k-2)\cdot\cdots\cdot 1$ en $(n-k)(n-k-1)(n-k-2)\cdot\cdots\cdot 1$. Door op deze manier het ineenritsen te beschrijven, is elke manier van ineenritsen van de twee stapeltjes dus even waarschijnlijk, gegeven dat de splitsing na kaart k heeft plaats gevonden. In welke volgorde de kaarten ook vallen, de kans op de resulterende permutatie π is altijd gelijk aan

$$
\begin{aligned}
\mathbb{P}(\pi \mid K = k) &= \frac{k}{n} \cdot \frac{k-1}{n-1} \cdot \dots \cdot \frac{1}{n-k+1} \cdot \frac{n-k}{n-k} \cdot \frac{n-k-1}{n-k-1} \cdot \dots \cdot \frac{1}{1} \\
&= \frac{k!(n-k)!}{n!} = 1/\binom{n}{k}.
\end{aligned}
$$

Het totaal aantal mogelijke permutaties, gegeven een splitsing na kaart k, is natuurlijk ook gelijk aan $\binom{n}{k}$; er moeten immers k plaatsen worden gekozen voor de eerste k kaarten, de overige $n-k$ vullen de overgebleven plaatsen in hun oorspronkelijke volgorde.

De kans op een splitsing $K = k$, gevolgd door het ineenritsen van de stapeltjes op een bepaalde manier, is nu

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

Oftewel, de kansen zijn voor alle mogelijke manieren van splitsen gevolgd door ineenritsen gelijk. (Er zijn $\sum_{k=0}^{n} \binom{n}{k} = 2^n$ manieren van splitsen en ineenritsen mogelijk.)

Dit wil echter niet zeggen dat de kans op elk resultaat (permutatie) gelijk is! Na één enkele keer schudden kan de beginpermutatie (als enige) op meerdere manieren bereikt worden; waar je het pak ook splitst, door de stapeltjes weer op elkaar te leggen krijg je immers altijd de beginpermutatie weer terug. Aangezien het pak op $n+1$ manieren gesplitst kan worden, is de kans op de identiteit gelijk aan $\frac{n+1}{2^n}$. Verder kunnen lang niet alle permutaties bereikt worden na één keer schudden. In hoofdstuk 5 zullen we uitleggen dat de kans groter is dan nul alleen voor die permutaties die bestaan uit slechts één of twee *rising sequences*.

3.2 Een algemenere schudmethode: de α-shuffle

Op een zelfde manier als hierboven de GSR-shuffle is beschreven, zou je ook een shuffle kunnen definiëren waarbij de kaarten in meer dan 2 pakjes worden verdeeld. Neem $\alpha \in \mathbb{Z}^+$. Het pak wordt in α stapeltjes verdeeld, ter grootte $k_1, k_2, \dots, k_\alpha$, met $k_i \geq 0$. (Lege stapeltjes zijn dus toegestaan!). Bij de α-shuffle is de aanname dat de kans dat het pak op deze manier in stapeltjes wordt verdeeld gelijk is aan de multinomiaal coëfficiënt gedeeld door α^n, mits natuurlijk $\sum_i k_i = n$:

$$\mathbb{P}(k_1, k_2, \ldots, k_\alpha) = \binom{n}{k_1, \ldots, k_\alpha} / \alpha^n.$$

Vervolgens worden de stapeltjes ineengeritst, waarbij de onderlinge volgorde van de kaarten binnen één pak weer gelijk blijft. Aanname 3.2 van het GSR-model wordt voor de α-shuffle gegeneraliseerd tot de aanname dat de kans dat de volgende kaart die valt uit pak j valt, gelijk is aan $\frac{l_j}{\sum_i l_i}$ waarbij l_i het nog overgebleven aantal kaarten in stapel i weergeeft. Hierdoor wordt de kans op een bepaalde permutatie π, gegeven dat het pak in de stapeltjes ter grootte $k_1, k_2, \ldots, k_\alpha$ is gesplitst, weer gelijk voor elke π: $\mathbb{P}(\pi \mid k_1, k_2, \ldots, k_\alpha) = \frac{1}{\binom{n}{k_1, \ldots, k_\alpha}}$. Dit resultaat kan ook gevonden worden door te bedenken dat er totaal $\binom{n}{k_1, \ldots, k_\alpha}$ (de multinomiaalcoëfficiënt) manieren mogelijk zijn om de stapeltjes k_1 tot en met k_α in elkaar te schuiven; dit is het aantal manieren om uit n plaatsen k_1 plaatsen te kiezen voor de kaarten uit het eerste stapeltje, k_2 plaatsen voor het tweede stapeltje etcetera.

Zo is ook bij een α-shuffle elke splitsing gevolgd door een bepaalde manier van het weer in elkaar schuiven van de stapeltjes even waarschijnlijk:

$$\mathbb{P}(\pi \mid k_1, k_2, \ldots, k_\alpha) \cdot \mathbb{P}(k_1, k_2, \ldots, k_\alpha) = \frac{1}{\binom{n}{k_1, \ldots, k_\alpha}} \cdot \binom{n}{k_1, \ldots, k_\alpha} / \alpha^n = \frac{1}{\alpha^n}.$$

Voor het uitvoeren van een α-shuffle zijn meerdere handen een vereiste.

3.3 Inverse shuffle

Een zeer bruikbare alternatieve manier om een α-shuffle te beschrijven is de *inverse shuffle* [Bayer & Diaconis, 1992]. In plaats van het pak in α stapeltjes te verdelen en deze stapeltjes weer ineen te ritsen, wordt de inverse handeling uitgevoerd: het pak wordt uit elkaar getrokken in α stapels en de stapels worden op elkaar geplaatst. De stapeltjes mogen leeg zijn.

Een 2-shuffle of riffle shuffle wordt als volgt geïnverteerd: De kaarten worden verdeeld in twee stapeltjes, door op elke kaart met kans $\frac{1}{2}$ een 0 of een 1 te zetten. De kaarten met een 0 vormen, met behoud van hun oorspronkelijke onderlinge volgorde, het eerste stapeltje. De kaarten met een 1 vormen op dezelfde manier het tweede stapeltje. Vervolgens wordt het eerste stapeltje bovenop het tweede geplaatst.

Algemener, wordt bij een inverse α-shuffle een kaart met kans $\frac{1}{\alpha}$ op een kaart een $0, 1, \ldots$ of $\alpha - 1$ geplaatst. De kaarten worden overeenkomstig dit getal in α stapeltjes verdeeld, waarbij de onderlinge volgorde van kaarten met hetzelfde getal weer intact blijft. Tenslotte worden de stapeltjes op elkaar geplaatst volgens het bijbehorende getal.

Op deze manier bestaat er voor elke α-schudhandeling, precies één inverse schudhandeling, namelijk die waarbij 0-en worden geplaatst op precies die kaarten die in de α-schudhandeling in het eerste stapeltje zitten, 1-en op precies die kaarten die in het tweede stapeltje zitten, etcetera.

Lemma 3.3 *De kans op een α-schudhandeling (dit is dus de kans op een bepaalde manier van splitsen in α stapeltjes, gevolgd door het ineenritsen van deze stapeltjes), is gelijk aan de kans op de bijbehorende inverse schudhandeling, waarbij 0-en worden geplaatst op precies die kaarten die in de α-schudhandeling in het eerste stapeltje zitten, 1-en op precies die kaarten die in het tweede stapeltje zitten, etcetera.*

Bewijs Merk op dat er een multinomiaal $(n, 1/\alpha, 1/\alpha, \ldots, 1/\alpha)$ verdeeld aantal 0-en, 1-en, $\ldots$, $(\alpha - 1)$-en worden gekozen bij de inverse shuffle. Dit komt direct overeen met het kiezen van de groottes van de stapeltjes bij de gewone shuffle. Gegeven $k_0, k_1, \ldots, k_{\alpha-1}$ aantal 0-en, 1-en etcetera, zijn alle mogelijke manieren om de 0-en, 1-en etcetera te plaatsen even waarschijnlijk. Dit komt overeen met de α-shuffle, waarbij gegeven de grootte van de stapeltjes, de kans op alle mogelijke manieren van ineenritsen gelijk is. $\square$

3.4 Herhaald schudden

Stelling 3.4 *De kansverdeling gegenereerd door een α-shuffle gevolgd door een β-shuffle is gelijk aan de kansverdeling na een $\alpha\beta$-shuffle.*

Bewijs We laten zien dat een inverse α-shuffle, gevolgd door een inverse β-shuffle dezelfde kansverdeling geeft als een inverse $\alpha\beta$-shuffle. Op grond van lemma 3.3 (en het feit dat $\alpha\beta = \beta\alpha$) is daarmee de stelling bewezen.

We beschrijven de inverse α-shuffle weer als volgt: Op elke kaart wordt een uniform getrokken getal uit $\{0, \ldots, \alpha - 1\}$ geschreven. De kaarten met een 0 vormen het eerste stapeltje, die met een 1 het tweede, etcetera. Vervolgens worden de stapeltjes op elkaar geplaatst.

Voeren we nu na de inverse α-shuffle een inverse β-shuffle uit, en zetten we het tweede getal vóór het eerste, dan staat er op elke kaart een getal uit $\{0, \ldots, \beta - 1\}$, gevolgd door een getal uit $\{0, \ldots, \alpha - 1\}$. De kaarten met twee keer een 0 komen bovenop in het pak terecht, daaronder volgen de kaarten met 01 tot en met $0(\alpha - 1)$, dan de kaarten met 10 tot met $1(\alpha - 1)$ etcetera tot de laatste kaarten met $(\beta - 1)(\alpha - 1)$.

Wanneer α en β beide 2 zijn, zijn de kaarten na 2 inverse shuffles dus gerangschikt naar het tweecijferige binaire getal wat op de kaarten is geschreven. De kans op ieder getal is gelijk, namelijk $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$. Hetzelfde resultaat kan verkregen worden door op iedere kaart met kans $\frac{1}{4}$ een getal uit $\{0, 1, 2, 3\}$ te schrijven!

Op dezelfde manier volgt dat voor een willekeurige α en β, hetzelfde resultaat als van twee inverse shuffles, verkregen kan worden door voor elke kaart één getal uit $\{0, \ldots, (\alpha - 1)(\beta - 1)\}$ uniform te trekken. $\square$

Gevolg 3.5 *De kansverdeling na s riffle shuffles, is gelijk aan die na het uitvoeren van een 2^s-shuffle.*

Dit belangrijke gevolg zullen we in hoofdstuk 5 gebruiken om de kans op een bepaalde permutatie te bepalen.

Hoofdstuk 4

Koppelen en stoptijden

Samenvatting De GSR-Markovketen kan worden gekoppeld aan een uniform verdeelde keten: op het koppeltijdstip zijn beide ketens niet meer van elkaar te onderscheiden, en is er dus “genoeg” geschud. Hetzelfde idee vinden we bij de stoptijden.

4.1 Koppelen

Een veel gebruikte manier om een bovengrens op de variation distance te krijgen, is het koppelen van Markovketens. Het idee achter koppelen is het volgende. Twee Markovketens $(X_s)_{s\in\mathbb{Z}^+}$ en $(Y_s)_{s\in\mathbb{Z}^+}$ hebben verschillende startverdelingen a, respectievelijk b. De overgangskansen zijn gelijk. Er wordt een simultane verdeling geconstrueerd, zodanig dat de marginale verdeling per keten inderdaad de kansverdeling volgens de overgangskansen is. Op het moment dat beide Markovketens zich in dezelfde toestand bevinden, zijn de ketens niet meer te onderscheiden, aangezien de overgangskansen gelijk zijn. We zeggen dat de ketens dan gekoppeld zijn en noemen dit moment het *koppeltijdstip* T.

Lemma 4.1 *Zij gegeven twee Markovketens, $(X_s)_{s\in\mathbb{Z}^+}$ en $(Y_s)_{s\in\mathbb{Z}^+}$, met gelijke overgangsmatrices P, en startverdelingen a, respectievelijk b.*

$$\|aP^s - bP^s\| \leq \mathbb{P}(T > s)$$

Bewijs

$$\begin{aligned}
\|aP^s - bP^s\| &= \frac{1}{2}\sum_{j\in I} |\mathbb{P}(X_s = j) - \mathbb{P}(Y_s = j)| \\
&= \frac{1}{2}\sum_{j\in I} |\mathbb{P}(X_s = j \mid T > s) - \mathbb{P}(Y_s = j \mid T > s)|\mathbb{P}(T > s) \\
&\quad + \frac{1}{2}\sum_{j\in I} |\mathbb{P}(X_s = j \mid T \le s) - \mathbb{P}(Y_s = j \mid T \le s)|\mathbb{P}(T \le s) \\
&= \frac{1}{2}\sum_{j\in I} |\mathbb{P}(X_s = j \mid T > s) - \mathbb{P}(Y_s = j \mid T > s)|\mathbb{P}(T > s) \qquad (4.1) \\
&\le \frac{1}{2}\sum_{j\in I} \big(\mathbb{P}(X_s = j \mid T > s) + \mathbb{P}(Y_s = j \mid T > s)\big)\mathbb{P}(T > s) \qquad (4.2) \\
&= \mathbb{P}(T > s).
\end{aligned}$$

De gelijkheid in (4.1) volgt uit het feit dat de twee Markovketens gelijke overgangskansen hebben. In (4.2) wordt gebruik gemaakt van de driehoeksongelijkheid. □

Merk op dat voor beide ketens de kansverdeling per schudbeurt gegeven is. Er is echter een ruime keuze aan simultane verdelingen, die hieraan voldoen. Om een zo scherp mogelijke bovengrens te berekenen, zoeken we een simultane verdeling waarvan we $\mathbb{P}(T > s)$ kunnen bepalen, èn waarvan de $\mathbb{P}(T > s)$ relatief klein is (er moet "snel" een koppeling ontstaan). We geven een voorbeeld van een zeer slechte simultane verdeling.

Voorbeeld We kiezen als voorwaardelijke verdeling voor de tweede Markovketen $\mathbb{P}(Y_1 = \pi_1 \mid Y_0 = \pi_0; X_1 = \sigma_1; X_0 = \sigma_0) = \begin{cases} 1 & \text{als } \exists\tau : \pi_1 = \pi_0\tau \text{ èn } \sigma_1 = \sigma_0\tau \\ 0 & \text{anders.} \end{cases}$
Met andere woorden, bij beide ketens wordt elke schudbeurt dezelfde permutatie (operatie) uitgevoerd.

Deze voorwaardelijke verdeling geeft inderdaad een onvoorwaardelijke verdeling, die gelijk is aan de verdeling van de eerste Markovketen. Dit is echter een zeer onbruikbare koppeling om de variaton distance af te schatten, aangezien $\mathbb{P}(T > s) = 1 - \mathbb{P}(X_0 = Y_0)\ \forall s \in \mathbb{Z}^+$. Als de ketens niet in dezelfde toestand beginnen, zullen ze nooit samenkomen.

4.2 Koppelen van de GSR-shuffle

4.2.1 Simultane verdeling

We zoeken een bovengrens voor de variation distance $\|Q^{*s} - U\|$ tussen de verdeling na s GSR-shuffles en de uniforme verdeling. Aangezien de uniforme verdeling de evenwichtsverdeling is van de GSR-keten, geldt dat als de GSR-keten $(Y)_{s\in\mathbb{Z}^+}$ de uniforme verdeling als startverdeling heeft, Y_s uniform verdeeld is voor elke s. We proberen dus een koppeling te construeren tussen een keten met bekende beginpermutatie en een keten met uniforme startverdeling. We zullen dit doen voor de inverse shuffle. Zoals opgemerkt in lemma 3.3, gelden de resultaten die we vinden voor de inverse shuffle ook voor de gewone shuffle.

Achterop elke kaart van het pak, waarvan de beginpermutatie bekend is, wordt met kans $\frac{1}{2}$ een 1 of een 0 gezet. Dezelfde kaart van het andere pak krijgt hetzelfde cijfer. Dus als de hartenaas in het pak waarvan de beginpermutatie bekend is een 1 krijgt, krijgt ook de hartenaas in het andere pak een 1, ongeacht de plaats waar de hartenaas zit. Onafhankelijk van elkaar beschouwd, wordt op beide pakken een inverse shuffle uitgevoerd. Ook in het tweede pak immers, heeft elke kaart kans $\frac{1}{2}$ op een 1 of een 0.

Dit wordt herhaald, waarbij het cijfer van de laatst uitgevoerde inverse shuffle telkens vóór de cijfers van de eerdere shuffles wordt gezet.

Merk nu op dat de kaarten na s inverse shuffles, gesorteerd zijn naar de s-cijferige binaire getallen die achterop de kaarten staan. Kaarten met hetzelfde getal staan nog in hun oorspronkelijke volgorde.

We concluderen dat als alle getallen verschillend zijn, de kaarten van de twee pakken in dezelfde volgorde zitten (gekoppeld zijn).

4.2.2 Verdeling van de koppeltijd

De kans dat alle getallen verschillend zijn kan bepaald worden met het bekende "verjaardagsprobleem".

Het verjaardagsprobleem Het verjaardagsprobleem stelt de vraag wat de kans is dat in een groep van n mensen, meerdere mensen op eenzelfde dag jarig zijn. We gaan uit van een jaar van m dagen, waarbij elke dag even waarschijnlijk is als verjaardag. We bekijken de complementaire kans, de kans dat iedereen op een andere dag jarig is. Er zijn m^n mogelijkheden om voor ieder een verjaardag te kiezen; ieder kan op elke van de m dagen jarig zijn. Wanneer we niet willen dat twee mensen op dezelfde dag jarig zijn, hebben we voor de eerste persoon m dagen om uit te kiezen, voor de tweede zijn er $m-1$ dagen over, etcetera, tot er voor de laatste nog $m-(n+1)$ dagen zijn. De kans dat ieder op een andere dag jarig is, is dus gelijk aan:

$$\frac{m(m-1)(m-2)\dots(m-(n+1))}{m^n} = \frac{m!}{(m-n)!m^n} = \binom{m}{n}\frac{n!}{m^n}.$$

Voor een jaar van $m = 365$ dagen is de kans dat er van $n = 30$ mensen geen twee op dezelfde dag jarig zijn slechts 29%!

Vertalen we bovenstaand probleem naar het verjaardagsprobleem, dan is $m = 2^s$, het aantal mogelijke binaire getallen bestaande uit s cijfers, en n het aantal kaarten. Dus is

$$\mathbb{P}(T > s) = 1 - \binom{2^s}{n}\frac{n!}{2^{sn}}.$$

Hiermee hebben we ook een bovengrens op de variation distance gevonden. Bij $n = 52$ kaarten wordt de variation distance na 7 keer schudden begrens door

$$\|Q^{*7} - U\| \leq \mathbb{P}(T > 7) = 1 - \binom{2^7}{52}\frac{52!}{2^{7\times 52}} \approx 0.999994557.$$

In het volgende hoofdstuk zullen we zien dat de variation distance bij 52 kaarten na 7 keer schudden ongeveer gelijk is aan 0.334; de bovengrens is dus niet bijzonder scherp!

Een ruwe manier om te zeggen hoe vaak geschud moet worden, is het nemen van de verwachting van de koppeltijd T.

$$\begin{aligned}
\mathbb{E}(T) &= \sum_{t=0}^{\infty} t\mathbb{P}(T = t) = \sum_{t=1}^{\infty}\sum_{s=0}^{t-1}\mathbb{P}(T = t) \\
&= \sum_{s=0}^{\infty}\sum_{t=s+1}^{\infty}\mathbb{P}(T = t) = \sum_{s=0}^{\infty}\mathbb{P}(T > s) \\
&= \sum_{s=0}^{\infty}(1 - \binom{2^s}{n}\frac{n!}{2^{sn}}).
\end{aligned}$$

In tabel 4.1 staan de verwachting en variantie van de koppeltijd voor verschillende aantallen kaarten. Wat opvalt is ten eerste dat de verwachting lineair toe

n	6	13	26	52	104	208
$\mathbb{E}(T)$	5.41	7.70	9.71	11.72	13.73	15.73
$\mathbb{V}\text{ar}(T)$	3.04	3.29	3.40	3.45	3.48	3.49

Tabel 4.1: De verwachting en variantie van de koppeltijd voor n kaarten

lijkt te nemen als n verdubbelt. In de volgende paragraaf wordt duidelijk dat het benodigd aantal keer schudden (asymptotisch) inderdaad een logaritmische functie is van n. Het is opmerkelijk dat voor redelijk kleine waarden van n dit reeds het geval lijkt te zijn. Ten tweede neemt de variantie zeer weinig toe als n groter wordt. Hiervoor hebben we geen verklaring.

We merken op dat deze methode zeer weinig zegt: Niet alleen is de verwachting niet het hele antwoord op de vraag hoe vaak er geschud moet worden, de verwachting van de koppeltijd is bovendien niet meer dan een bovengrens van onbekende kwaliteit, op het aantal keer dat er geschud moet worden. Er zijn immers vele mogelijke simultane verdelingen, die verschillende verdelingen van de koppeltijd kunnen geven. Er kunnen simultane verdelingen bestaan die sneller een koppeling teweegbrengen.

4.2.3 Asymptotiek

Met behulp van koppelen, kan er een asymptotische bovengrens gevonden worden op het benodigde aantal keer schudden. We zullen dit laten zien met de koppeling uit de vorige paragraaf.

We gebruiken het volgende lemma, waarvoor we geen bewijs geven [Aldous, 1983].

Lemma 4.2 (Birthday lemma) *Gegeven een reeks onderling onafhankelijke, gelijk verdeelde stochastische variabelen $C_1, C_2, \ldots$ met C_i uniform verdeeld op $\{1, \ldots, m\}$ ("onafhankelijke trekkingen met teruglegging"), en $U_m = \min\{j \mid C_j = C_i \ \exists\, i < j\}$, dan*

$$\frac{U_m}{\sqrt{m}} \xrightarrow{d} V, \quad m \to \infty$$

met V een in v ontaarde verdeling, voor een zekere v, met $0 < v < \infty$.

In de vorige paragraaf hebben we geconcludeerd dat het koppeltijdstip het moment is dat alle getallen op de kaarten verschillend zijn. Deze getallen zijn uniform verdeeld op $\{1,\ldots,2^s\}$. De kansverdeling van de koppeltijd is derhalve $\mathbb{P}(T>s)=\mathbb{P}(U_{2^s}\leq n)=1-\mathbb{P}(U_{2^s}>n)$. Uit het lemma volgt dat

$$\begin{aligned}\lim_{n,s\to\infty}\mathbb{P}(U_{2^s}>n) &= \lim_{n,s\to\infty}\mathbb{P}(U_{2^s}/\sqrt{2^s}>n/\sqrt{2^s})\\ &= \lim_{n,s\to\infty}\mathbb{P}(V>n/\sqrt{2^s}).\end{aligned}$$

Als $\lim_{n,s\to\infty} n/\sqrt{2^s}=0$ dan is zeker $\lim_{n,s\to\infty}\mathbb{P}(U_{2^s}>n)=1$, aangezien $\mathbb{P}(V>0)=1$.

Conclusie: variation distance $\leq \mathbb{P}(T>s)\to 0$ $(n\to\infty)$, als $s>\alpha\log_2 n$ met $\alpha>2$.

Een exacte asymptotische uitdrukking voor het benodigd aantal keer schudden is $\frac{3}{2}\log_2 n$. Het voert te ver om dit hier te bewijzen, we verwijzen voor het bewijs naar bijvoorbeeld [Aldous, 1983].

n	6	13	26	52	104	208
$\frac{3}{2}\log_2 n$	3.88	5.55	7.05	8.55	10.05	11.55

4.3 Stoptijden en sterk uniforme tijden

In [Aldous & Diaconis, 1986] wordt dezelfde methode gebruikt, in andere, algemenere bewoordingen om het resultaat uit de vorige paragraaf af te leiden. Hoewel dit geen nieuwe inzichten oplevert, zullen we in deze paragraaf ook de door Aldous en Diaconis gevolgde benadering weergeven.

Zij definiëren eerst algemener een *stoptijd* T waarop gestopt wordt omdat voldaan is aan de *stopregel* $\hat{T}$. Een stopregel is gedefinieerd als een functie op alle mogelijke (oneindige) reeksen van uitkomsten van schudbeurten. Voor elke reeks uitkomsten van achtereenvolgende schudbeurten geeft een stopregel het tijdstip (de schudbeurt) waarop gestopt kan worden.

Voorbeeld Een stopregel kan zijn, dat gestopt wordt zodra de permutatie waarin het pak zich bevindt na de laatste schudbeurt overeenkomt met de permutatie waarin een andere keten zich bevindt na die schudbeurt. Dan is *de stoptijd gelijk aan de koppeltijd* van de twee ketens!

Een ander (minder zinnig) voorbeeld van een stopregel is, dat gestopt wordt wanneer de hartenaas bovenop in het pak zit.

We geven de formele definities van stopregels en stoptijden, zoals gegeven in

[Aldous & Diaconis, 1986].

Definitie 4.3 *Laat I een eindige groep zijn en I^∞ de verzameling van alle oneindige reeksen $x = (x_1, x_2, \ldots)$ bestaande uit elementen van I. Een stopregel $\hat{T}$ is een functie $\hat{T} : I^\infty \to \mathbb{N} \cup \infty$, zodanig dat als $\hat{T}(x) = j$, dan ook $\hat{T}(x') = j$ voor elke x' met $x'_i = x_i, i \leq j$.*

Definitie 4.4 *Laat P een $(|I| \times |I|)$ overgangsmatrix zijn en (X_s) de bijbehorende Markovketen. Gegeven een stopregel $\hat{T}$ is de stochastische tijd $T = \hat{T}(X_1, X_2, \ldots)$ een stoptijd.*

Wanneer gestopt wordt op het moment dat alle permutaties even waarschijnlijk zijn, noemen we de stoptijd T een *sterk uniforme tijd.*

Definitie 4.5 *Een stoptijd T is sterk uniform wanneer voor elke $s < \infty$ geldt $\mathbb{P}(X_s = x_s \mid T = s) = 1/|I|$, $x_s \in I$ met $|I|$ de cardinaliteit van I.*

Het volgende lemma is afkomstig van Jim Reeds [Aldous & Diaconis, 1986] en geeft een sterk uniforme stoptijd voor de inverse shuffle.

Lemma 4.6 *Beschouw de inverse shuffle. Neem T het eerste tijdstip waarop op elke kaart een ander binair getal staat. Dan is T sterk uniform.*

Bewijs Dit is precies de koppeling als beschreven in de vorige paragraaf. $\square$

Lemma 4.7 *Laat Q weer de verdeling zijn op een eindige groep G. Als T sterk uniform is voor Q, dan*

$$\|Q^{*s} - U\| \leq \mathbb{P}(T > s).$$

Bewijs Het bewijs van dit lemma is precies hetzelfde als het bewijs van lemma 4.1. $\square$

Hoofdstuk 5

De variation distance voor de GSR-shuffle

Samenvatting Het is mogelijk de variation distance exact te bepalen. We merken op dat de kans op een permutatie resulterend uit een GSR-shuffle volledig bepaald is door het aantal "rising sequences" van de permutatie. Hierdoor omzeilen we het probleem van de grote toestandsruimte. We zien dat de variation distance een "cut off"-verschijnsel vertoont, en bestempelen het "cut off"-punt (voorlopig) als genoeg.

5.1 Rising sequences

Een belangrijke eigenschap van de permutaties die het resultaat zijn van een riffle shuffle zijn de zogenaamde *rising sequences*. Een rising sequence is een reeks van opeenvolgende kaarten in het pak. De opeenvolgende kaarten zitten niet noodzakelijk naast elkaar, maar kaart $i+1$ moet wel ná kaart i komen. Formeler:

Definitie 5.1 *Een rising sequence is een maximale reeks kaarten* $i, i+1, \ldots, i+k$*, waarvoor geldt dat* $\pi(i-1) > \pi(i) < \pi(i+1) < \cdots < \pi(i+k) > \pi(i+k+1)$*, waarbij* $\pi(j)$ *de positie van kaart* j *weergeeft.*

De enige permutatie met slechts één rising sequence is de identiteit $(1\ 2\ \ldots\ n)$. Na één keer schudden kan een permutatie verkregen worden met 1 of 2 rising sequences. De kaarten van ieder stapeltje blijven immers in hun oorspronkelijke volgorde.

Voorbeeld Stel dat een pak van 6 kaarten wordt geschud door het in twee stapeltjes van ieder 3 kaarten te verdelen, en vervolgens één kaart van het onderste stapeltje, twee kaarten van het bovenste, twee van het onderste en één van het bovenste stapeltje te laten vallen:

$$1\ 2\ 3\ 4\ 5\ 6 \rightarrow 1\ 2\ 3 \mid 4\ 5\ 6 \rightarrow 1\ 4\ 5\ 2\ 3\ 6$$

Er zijn nu twee rising sequences ontstaan, namelijk [123] en [456]. Dit zijn natuurlijk gewoon het eerste en het tweede stapeltje.

Wanneer twee riffle shuffles na elkaar worden uitgevoerd, kunnen er maximaal $2^2 = 4$ rising sequences ontstaan.

Voorbeeld Het geschudde pak uit het vorige voorbeeld wordt nogmaals geschud, waarbij $K = 2$ en er een kaart van het bovenste stapeltje valt, dan één van het onderste stapeltje, de laatste van het bovenste stapeltje en tenslotte de laatsten van het onderste stapeltje.

$$1\ 4\ 5\ 2\ 3\ 6 \ \rightarrow 1\ 4 \mid 5\ 2\ 3\ 6 \ \rightarrow 1\ 5\ 4\ 2\ 3\ 6$$

Het pak bestaat nu uit 3 rising sequences: [123], [4] en [56].

Op bijvoorbeeld de volgende manier ontstaan 4 rising sequences ([1], [23], [4] en [56]):

$$4\ 5\ 2\ 3\ 6 \ \rightarrow 1\ 4 \mid 5\ 2\ 3\ 6 \ \rightarrow 5\ 2\ 1\ 4\ 3\ 6$$

Een kaarttruc Kaarttrucs die gebruik maken van het feit dat het aantal rising sequences in de meeste gevallen verdubbelt met elke keer schudden (tot de capaciteit van het pak is bereikt) zijn begin twintigste eeuw al bedacht door Williams en Jordan. Wij geven een voorbeeld uit [Bayer & Diaconis, 1992]. Een assistent uit het publiek wordt gevraagd een pak kaarten drie keer te schudden. De goochelaar kent de beginvolgorde. De assistent bekijkt de bovenste kaart en stopt hem op een willekeurige plek terug in het pak. De goochelaar gaat het pak kaarten vervolgens door en maakt stapeltjes van opeenvolgende kaarten die hij tegenkomt. Als een kaart niet op een stapeltje past, wordt een nieuw stapeltje gemaakt. De stapeltjes worden nu gevormd door de rising sequences in het geschudde pak. In de meeste gevallen zal het pak uit $2^3 = 8$ rising sequences, of stapeltjes bestaan van gemiddelde lengte $6\frac{1}{2}$ na 3 keer schudden. De kaart die van boven ergens in het midden is gestopt, zal (meestal) dan ook meteen op vallen als een rising sequence van lengte 1.

5.2 De kans op een permutatie

Stelling 5.2 *De kans op een permutatie π na een α-shuffle is volledig bepaald door het aantal rising sequences van π. De kans op een permutatie π van n kaarten met r rising sequences na een α-shuffle is gelijk aan $\binom{n+\alpha-r}{n}/\alpha^n$.*

Bewijs Zoals we boven reeds hebben opgemerkt, worden rising sequences veroorzaakt door het snijden van een pak in α stapeltjes. De kaarten uit één stapeltje maken in ieder geval deel uit van dezelfde rising sequence. Het aantal rising sequences van een permutatie die het resultaat is van een α-shuffle is maximaal gelijk aan α, maar kan ook kleiner zijn dan α, namelijk wanneer van twee stapeltjes k_i en k_{i+1} de kaarten van k_i allemaal vallen vóór de eerste kaart van k_{i+1} valt.

We hebben ook gezien dat wanneer het pak op een bepaalde manier in α stapels is gesplitst, een bepaalde permutatie slechts op één manier bereikt kan worden: door de kaarten precies in de volgorde van de permutatie te laten vallen. Willen we dus een bepaalde permutatie krijgen door een α-shuffle uit te voeren, dan moet het pak zó gesneden zijn dat de laatste kaarten van de rising sequences van de permutatie ook de laatste kaarten van de stapeltjes zijn. Wanneer het aantal rising sequences kleiner is dan α kunnen de overige $\alpha - r$ $(\alpha - 1 - (r-1))$ plaatsen waar het pak wordt gesneden willekeurig gekozen worden. Wellicht ten overvloede merken we op dat er ook gesneden kan worden op een plaats waar al gesneden is; lege stapeltjes zijn immers mogelijk.

Het aantal manieren waarop de $\alpha - r$ plaatsen gekozen kunnen worden, is gelijk aan het aantal manieren waarop we n elementen in $\alpha - r + 1$ groepjes kunnen verdelen; $\binom{n+\alpha-r}{\alpha-r}$. Dit is als volgt in te zien. We stellen ons $n + \alpha - r$ vakjes voor, waarvan er in $\alpha - r$ verticale strepen worden geplaatst. De lege vakjes tussen de verticale strepen vormen $\alpha - r + 1$ groepjes, met in totaal n elementen. We herschrijven

$$\binom{n+\alpha-r}{\alpha-r} = \binom{n+\alpha-r}{n}.$$

Uit het feit dat het totaal aantal mogelijke manieren om een α-shuffle uit te voeren gelijk is aan α^n volgt dat de kans op een permutatie met r rising sequences gelijk is aan

$$\binom{n+\alpha-r}{n}/\alpha^n$$

$\square$

Wanneer we dit resultaat combineren met dat uit de paragraaf 3.4 vinden we dat de kans op een permutatie met r rising sequences na s GSR-shuffles gelijk is aan:

$$\binom{n+2^s-r}{n}/2^{sn}.$$

5.3 De Eulergetallen

Stelling 5.3 *Het aantal permutaties met r rising sequences is gelijk aan het Eulergetal $A_{n,r}$.*

Het Eulergetal $A_{n,r}$ kan recursief gedefinieerd worden door de volgende relatie

$$A_{n+1,r} = (n-r+2)A_{n,r-1} + rA_{n,r},$$

met beginvoorwaarden

$$A_{0,0} = 1, A_{n,0} = 0.$$

Bewijs Bij [Tanny, 1973] wordt het getal $A_{n,r}$ een interpretatie gegeven als het aantal permutaties met precies r *ascending runs*: Wanneer links en rechts van de permutatie verticale strepen worden gezet, en tussen i en $i+1$ wanneer $\pi(i) > \pi(i+1)$, dan zijn de ascending runs de stukken tussen twee verticale strepen.

Dat het aantal permutaties met r ascending runs inderdaad gegeven wordt door bovenstaande recursierelatie is als volgt in te zien. Wanneer een kaart wordt toegevoegd, heeft deze kaart "waarde" $n+1$. Als de permutatie van n kaarten al r ascending runs bevatte, wordt het aantal ascending runs alleen dan niet groter, wanneer de kaart vóór één van de verticale strepen wordt gezet, maar niet voor de eerste, aangezien dit wel zal resulteren in een extra ascending run. Er zijn dan dus r mogelijke plaatsen om kaart $n+1$ in te voegen. Wanneer de permutatie van n kaarten $r-1$ ascending runs bevat, wordt een ascending run toegevoegd wanneer de $(n+1)^{\mathrm{e}}$ kaart op één van de $n+2-r$ overige plaatsen wordt geplaatst.

Dat het aantal ascending runs gelijk is aan het aantal rising sequences wordt duidelijk als we de inverse schrijfwijze voor een permutatie gebruiken. (In paragraaf 2.2 hebben we gezien dat elke permutatie een unieke inverse in $\mathcal{S}_n$ heeft.) In plaats van $\pi(i)$ de oorspronkelijke plaats van de op plaats i staande kaart te laten weergeven, zeggen we dat $\pi^{-1}(i)$ de plaats is die de kaart i in de permutatie inneemt. Zo kan bijvoorbeeld $\pi = (2\ 4\ 1\ 3)$ ook weergegeven worden als $\pi^{-1} = (3\ 1\ 4\ 2)$. De rising sequences bij de eerste weergave, komen precies overeen met de ascending runs in de tweede weergave. Een rising sequence wil immers zeggen dat de opvolgende kaarten op steeds hogere plaatsen terecht zijn gekomen! $\Box$

We geven tenslotte nog een expliciete formule voor $A_{n,r}$:

$$A_{n,r} = \sum_{j=0}^{r}(-1)^j\binom{n+1}{j}(r-j)^n.$$

Het is eenvoudig na te gaan dat deze formule inderdaad een oplossing is van de recursierelatie.

Stelling 5.4 *Het Eulergetal $A_{n,r}$ is gelijk aan het Eulergetal $A_{n,n+1-r}$*

Bewijs We beschouwen bij een permutatie met r rising sequences in plaats van de ascending runs de *descending runs*, waarbij de descending runs gevormd worden door de stukken tussen twee verticale strepen, als strepen worden geplaatst op de $n-1-(r-1)$ posities waar $\pi(i) < \pi(i+1)$ (plus weer één vóór de eerste en één na de laatste positie). Het aantal descending runs is dan gelijk aan $n+1-r$. Omdat een descending run een "van achter naar voor bekeken" ascending run is en het uiteraard niet uitmaakt of we alle permutaties van voor naar achter of van achter naar voor bekijken, volgt $A_{n,r} = A_{n+1-r}$. $\Box$

5.4 Een exacte uitdrukking voor de variation distance

Met de resultaten uit de vorige twee paragrafen kunnen we een exacte uitdrukking geven voor de variation distance na s uniforme riffle shuffles. We gebruiken hierbij het tweede gedeelte van definitie 2.8 van de variation distance.

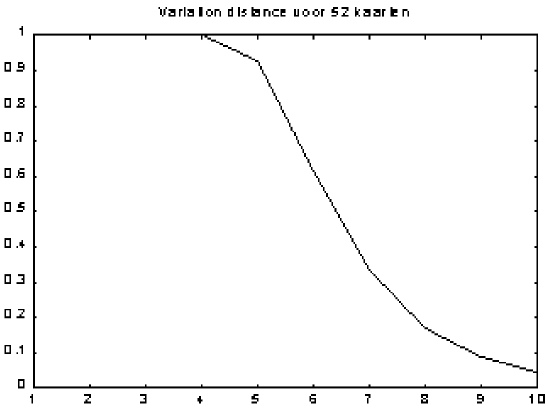
$$\|Q^s - U\| = \frac{1}{2}\sum_{r=1}^{n} A_{n,r}\ |\ \binom{n+2^s-r}{n}/2^{sn} - \frac{1}{n!}|.$$

In tabel 5.1 staat de variation distance voor een half pak kaarten, één, twee en vier pakken, wanneer 1 tot 10 keer geschud wordt.

$n\backslash s$	1	2	3	4	5	6	7	8	9	10
26	1.000	1.000	1.000	0.804	0.469	0.234	0.122	0.062	0.031	0.016
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	0.988	0.772	0.454	0.237	0.119
208	1.000	1.000	1.000	1.000	1.000	1.000	1.000	0.914	0.603	0.329

Tabel 5.1: De variation distance na s shuffles van n kaarten

Het is opmerkelijk dat de variation distance bij de eerste paar schudbeurten weinig afneemt en dichtbij 1 blijft, en vanaf een bepaald aantal keer schudden redelijk snel naar 0 gaat.



5.5 Asymptotiek

Definitie 5.5 *Het "cut off"-punt s_0 is het aantal keer schudden zodanig dat $\|Q^{*((1+\epsilon)s_0)} - U\| \to 0$, en $\|Q^{*((1-\epsilon)s_0)} - U\| \to 1$ voor alle $\epsilon > 0$ en $n \to \infty$.*

Hoewel er geen bewijs voor bekend is, wordt vermoed ([Aldous, 1983], [Aldous & Diaconis, 1986]) dat de variation distance voor elke schudmethode zo'n "cut off"-verschijnsel vertoont.

In [Bayer & Diaconis, 1992] wordt bewezen dat de varation distance resulterend uit de GSR-shuffle, inderdaad een "cut off" vertoont. Zij bewijzen dat wanneer er $s = \log_2(n^{3/2}c)$ maal geschud wordt, de variation distance voor $n \to \infty$, gelijk is aan

$$\|Q^{*s} - U\| = 1 - 2\Phi\big(\frac{-1}{4c\sqrt{3}}\big) + O\big(\frac{1}{n^{1/4}}\big)$$

met $\Phi(x) = \int_{-\infty}^{x} \frac{1}{\sqrt{2\pi}} e^{-t^2/2} dt$, de normale verdeling.

Zij merken vervolgens op dat de funktie $1-2\Phi\big(\frac{-1}{4c\sqrt{3}}\big)$ asymptotisch het volgende gedrag vertoont:

$$\begin{aligned} 1 - 2\Phi\big(\frac{-1}{4c\sqrt{3}}\big) &\sim \frac{1}{2c\sqrt{6\pi}} \qquad \text{voor } c \to \infty, \\ 1 - 2\Phi\big(\frac{-1}{4c\sqrt{3}}\big) &\sim 1 - \frac{4c\sqrt{3}}{\sqrt{2\pi}} \exp\big[-\frac{1}{2}\big(\frac{-1}{4c\sqrt{3}}\big)^2\big] \qquad \text{voor } c \to 0. \end{aligned}$$

Met $c = 2^j$ is j het aantal schudbeurten méér dan $\frac{3}{2}\log_2 n$ dat wordt uitgevoerd. Immers, $s = \log_2(n^{3/2}c) = \frac{3}{2}\log_2 n + \log_2 c$.
We zien dus dat de variation distance exponentieel naar 0 gaat voor j positief (de variation distance neemt voor elke schudbeurt na de $\frac{3}{2}\log_2 n$-de schudbeurt af met een factor 2). Voor j negatief gaat de variation distance zelfs dubbel-exponentieel naar 1.

Bayer en Diaconis bestempelen dit "cut off"-punt als het aantal keer schudden dat genoeg is. Immers, het "cut off"-punt is gedefinieerd als het aantal keer schudden, waarbij de variation distance snel naar 0 gaat wanneer er vaker wordt geschud, en snel naar 1 wanneer er minder vaak wordt geschud. We willen hierbij de kanttekening maken, dat de variation distance in de buurt van het "cut off"-punt voor een gegeven n nog redelijk groot kan zijn. Voor $n = 52$ geeft de asymptotische benadering $\frac{3}{2}\log_2 n$ dat er $\lceil 8.55 \rceil = 9$ keer geschud moet worden. De variation distance is dan 0.085.

In artikelen verwijzend naar [Bayer & Diaconis, 1992] wordt geconcludeerd dat 7 keer schudden volstaat voor $n = 52$, hoewel dit niet expliciet in het artikel staat. Deze conclusie is vermoedelijk gebaseerd op het feit dat de variation distance na 7 keer schudden met elke extra schudbeurt (ongeveer) halveert (zie tabel 5.1). Dit lijkt ons geen geldige redenering: de eigenschap (na het "cut off"-punt neemt de variation distance exponentieel af met een factor 2 (voor $n \to \infty$)) neemt de plaats in van de definitie.

De variation distance is na 7 keer schudden nog vrij groot. Dat dit grote invloed kan hebben, zullen wij in het volgende hoofdstuk illustreren.

Hoofdstuk 6

New Age Solitaire en de variation distance

Samenvatting De fysieke interpretatie van de variation distance wordt voor de GSR-shuffle, expliciet gemaakt met het spel "New Age Solitaire" van Peter Doyle. 7 keer schudden van 52 kaarten is hierbij duidelijk niet voldoende.

6.1 Inleiding

In hoofdstuk 2 hebben wij aangegeven dat aan de variation distance de volgende interpretatie kan worden gegeven: Er is een spel te definieren waarbij de kans op winst volgens de ene verdeling, precies de variation distance groter is dan de kans op winst bij de andere verdeling.

Uit de wiskundige definitie van de variation distance blijkt, dat dan $A^+ = \{i \in I : Q(i) - U(i) \geq 0\}$ precies alle toestanden moet bevatten die winst opleveren. Het spelletje New Age Solitaire van Peter Doyle voldoet hier onder bepaalde voorwaarden aan.

New age solitaire Bij het spelletje New Age Solitaire (Peter Doyle) wordt een pak kaarten als volgt gerangschikt: Als n het aantal kaarten is, met n even, worden kaart 1 tot en met $\frac{1}{2}n$ op volgorde gelegd. Kaart $\frac{1}{2}n + 1$ tot en met kaart n worden in omgekeerde volgorde hier achter geplaatst. Dus kaart n komt na kaart $\frac{1}{2}n$.

Vervolgens wordt het pak kaarten 7 keer geschud met GSR-shuffles. Hierna wordt geprobeerd om twee stapeltjes van de kaarten te maken, stapel A (Yin) waarop kaarten 1 tot en met $\frac{1}{2}n$, en stapel B (Yang) waarop kaarten $\frac{1}{2}n + 1$ tot en met n in oplopende volgorde moeten worden geplaatst. De stapeltjes worden gevuld door één voor één de kaarten van het geschudde pak te halen, en indien de kaart volgt op de laatste kaart van één van de stapeltjes, de kaart op het stapeltje te plaatsen. Anders wordt de kaart weggelegd. Als het hele pak geweest is, wordt de procedure herhaald, met de kaarten die zijn weggelegd. We zeggen nu dat stapeltje A wint als dit stapeltje eerder klaar is dan stapeltje B.

Wanneer de kaarten volledig willekeurig gerangschikt zouden zijn, zou stapeltje A met kans 1/2 winnen. In de literatuur is door simulaties aangetoond dat na 7 keer schudden bij 1 stok kaarten (52 kaarten), wat volgens Bayer en Diaconis "genoeg" zou moeten zijn, de kans op winst ongeveer 81% is. We zullen in dit hoofdstuk laten zien, dat dit zelfs exact berekend kan worden [Schalekamp & Van Zuylen, a]. Onze methode toont precies de zwakke plek van de riffle shuffle. Na tenminste $2\log_2 n - \log_2 12$ keer schudden is de kans op winst gelijk aan de kans op winst volgens de uniforme verdeling plus de variation distance.

6.2 Wanneer wint A?

Als A wint dan wordt dat veroorzaakt door rising sequences met lengte groter dan 1. Bij het maken van stapeltjes A en B, zorgt een rising sequence van lengte 2 of meer er bij A voor, dat er 2 of meer kaarten op stapel A worden gelegd in één beurt, terwijl een rising sequence bij B er door B's omgekeerde beginsituatie voor zorgt, dat er slechts één kaart bijgelegd kan worden. (We spreken van een rising sequence in B bezien vanuit diens beginsituatie, $(n\ (n-1)\ (n-2))$ is een rising sequence, terwijl $((n-2)\ (n-1)\ n)$ een descending sequence wordt genoemd. Op deze manier is ook $(\frac{1}{2}n\ n)$ een rising sequence!)

We kunnen nu twee dingen opmerken:

1. Het aantal rising sequences in A is gelijk aan het aantal beurten dat nodig is om stapeltje A te maken. Zo is voor B het aantal descending sequences gelijk aan het aantal benodigde beurten.
2. Het aantal descending sequences bij een permutatie van n kaarten is gelijk aan $n + 1 - \#$(rising sequences). (Zie het bewijs dat $A_{n,r} = A_{n,n+1-r}$, stelling 5.4.)

Lemma 6.1 *Als er minder dan* $\log_2(\frac{1}{2}n + 1) - 1$ *keer geschud wordt, wint A met kans 1.*

Bewijs Het aantal rising sequences in A na s keer schudden is maximaal 2^s, en het aantal descending sequences in B is minimaal $\frac{1}{2}n+1-2^s$. De kans dat stapel B eerder klaar is dan stapel A wordt pas positief als $\mathbb{P}$(# descending sequences in B $\leq$ # rising sequences in A) > 0. Hieruit volgt dat dan $\frac{1}{2}n - 2^s + 1 \leq 2^s$, en $s \geq \log_2(\frac{1}{2}n + 1) - 1$. $\square$

Stelling 6.2 *Wanneer het aantal rising sequences in het pak kaarten kleiner dan of gelijk aan $\frac{1}{2}n$ is, wint A. Anders wint B.*

Bewijs A wint dan en slechts dan als het aantal rising sequences in A kleiner is dan het aantal descending sequences in B, of als het aantal rising sequences in A gelijk is aan het aantal descending sequences in B èn kaart $\frac{1}{2}n$ vóór kaart n zit (en kaart $\frac{1}{2}n$ en n dus deel uitmaken van één rising sequence).

Als k het aantal rising sequences in A is, en r het totaal aantal rising sequences in het pak, dan zijn er in B in het eerste geval $r - k$ en in het tweede geval $r - k + 1$ rising sequences. Nu wint A als

1. $k < \frac{1}{2}n + 1 - r + k$ als er geen rising sequence is die kaart $\frac{1}{2}n$ en n bevat, en als
2. $k \leq \frac{1}{2}n + 1 - r + k - 1$ als kaart $\frac{1}{2}n$ en n in één rising sequence zitten.

Dit heeft als oplossing $r \in \{1, \ldots, \frac{1}{2}n\}$.

$\square$

De kans dat A wint is dus gelijk aan

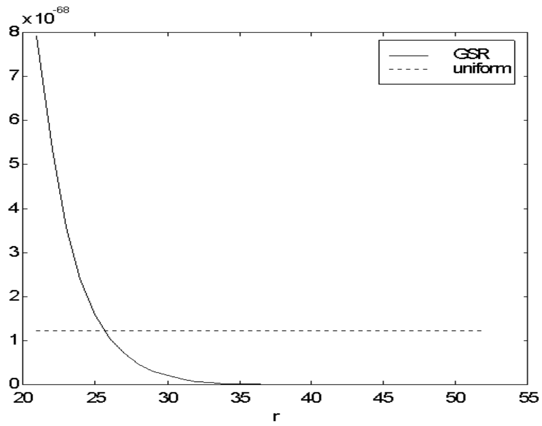
$$\sum_{r=1}^{\frac{1}{2}n} A_{n,r} \binom{n + 2^s - r}{n} / 2^{sn}$$

Waarbij $A_{n,r}$ weer gelijk is aan het Eulergetal.

Na het 7 keer schudden van 1 stok kaarten, is de variation distance gelijk aan 0.334. De hierboven bepaalde kans op winst in New Age Solitaire na 7 keer schudden is 80.7%. Het verschil tussen deze kans en de kans bij een volledig willekeurig gerangschikt pak is dus bijna gelijk aan de variation distance. Dan moet $A^+ = \{i \in I : Q(i) - U(i) \geq 0\}$ bijna gelijk zijn aan (of: iets kleiner zijn dan) de verzameling van alle permutaties met niet meer dan $\frac{1}{2}n$ rising sequences.

6.3 Het crossoverpoint

In de grafiek waarin het aantal rising sequences r is uitgezet tegen de kans op een willekeurige permutatie met r rising sequences na s shuffles, zal de kans tot een bepaald punt, het crossoverpoint, groter zijn dan uniform. In het crossoverpoint snijdt de grafiek de lijn $1/n!$. De volgende grafiek is een voorbeeld hiervan voor $n = 52$ en $s = 7$.



Het crossoverpoint c is die r waarvoor

$$\binom{n+2^s-r}{n}/2^{sn} = \frac{1}{n!}.$$

Het crossoverpoint is niet-dalend bij toenemende waarden van s en gaat uiteindelijk naar $\lfloor \frac{n}{2} \rfloor$. Dit punt wordt bereikt als 2^s ongeveer $n^2/12$ is, of $s \approx 2\log_2 n - \log_2 12$ [Mann, internet].

Lemma 6.3 *Voor $s \geq 2\log_2 n - \log_2 12$ geldt dat de kans dat A wint, gelijk is aan een half plus de variation distance.*

Bewijs De variation distance is natuurlijk gelijk aan

$$\sum_{r=1}^{c} A_{n,r}(\binom{n+2^s-r}{n}/2^{sn} - \frac{1}{n!}),$$

en de kans dat A wint is

$$
\begin{aligned}
\sum_{r=1}^{\frac{1}{2}n} A_{n,r}\binom{n+2^s-r}{n}/2^{sn} &= \|Q^{*s}-U\|+0.5 \\
&\quad - \sum_{r=c+1}^{\frac{1}{2}n} A_{n,r}\left(\frac{1}{n!}-\binom{n+2^s-r}{n}/2^{sn}\right).
\end{aligned}
$$

Voor $s \geq 2\log_2 n - \log_2 12$ geldt $c = \frac{1}{2}n$. $\square$

Voor $n = 52$ kaarten is $2\log_2 n - \log_2 12 \approx 7.8$. Voor $s \geq 8$ is de kans op winst voor A dan ook gelijk aan de variation distance plus een half. Voor $s = 7$ ligt het crossoverpoint op 25, en is de kans A wint gelijk aan:

$$
\begin{aligned}
&\sum_{r=1}^{25} A_{52,r}\binom{52+2^7-r}{52}/2^{7*52} \\
&= \|Q^{*7}-U\|+0.5 - A_{52,26}\left(\frac{1}{52!}-\binom{52+2^7-26}{52}/2^{7*52}\right) \\
&\approx 0.334+0.5-0.027 = 0.807.
\end{aligned}
$$

Hoofdstuk 7

De schudmatrix opnieuw bekeken

Samenvatting Om tot een oordeel te komen over de vraag of de resultaten van het GSR-model in de praktijk te gebruiken zijn, met andere woorden hoe goed het GSR-model de werkelijkheid benadert, kijken we nogmaals naar de Markovketen. Door gebruik te maken van de speciale structuur van de schudmatrix, kunnen eigenwaarden en variation distance berekend worden voor andere schudmodellen.

7.1 Inleiding

We hebben in hoofdstuk 2 reeds geconcludeerd dat de Markovaanpak slechts zeer beperkt bruikbaar is. We hebben vervolgens voor de GSR-shuffle wèl een aantal resultaten kunnen vinden, met behulp van methodes die gebruik maken van specifieke aannames van de GSR-shuffle.

Of het GSR-model wel een goede beschrijving van de werkelijkheid geeft, is echter niet duidelijk. We geven ter illustratie een aantal gegevens uit [Diaconis, 1988]. Hij heeft de resultaten van 103 schudbeurten van hemzelf en 100 schudbeurten van Jim Reeds vastgelegd.

Zoals te zien in de tabellen, snijden Diaconis en Reeds het pak “meer in het midden” dan volgens de binomiale verdeling en zijn de pakketjes van kaarten die tegelijk uit één hand vallen kleiner. We willen onderzoeken in hoeverre dit van invloed is op de gevonden resultaten.

Tabel 7.1: De kans dat het pak op plaats k gesneden wordt

persoon\\k	< 23	23	24	25	26	27	28	29	30	31	> 31
Diaconis	-	.019	.039	.214	.311	.320	.087	.010	-	-	-
Reeds	-	.02	.02	.08	.16	.23	.26	.16	.05	.02	-
binomiaal	.166	.078	.095	.106	.110	.106	.095	.078	.060	.043	.063

Tabel 7.2: De kans op een stapeltje van h kaarten uit één hand

persoon\\h	1	2	3	4	5	6	7	8	9	> 9
Diaconis	.800	.181	.014	.003	.001	-	-	-	-	-
Reeds	.623	.276	.068	.020	.007	.004	.001	.001	.001	.001
GSR-shuffle	.500	.250	.125	.063	.031	.016	.008	.004	.002	.002

Tabel 7.3: De kansverdeling voor de grootte van het eerste stapeltje

	1	2	3	4	5
Diaconis	.37	.37	.17	.10	.01

De methodes die we in de vorige hoofdstukken hebben gebruikt, kunnen niet zonder meer op andere schudmodellen worden toegepast, aangezien ze gebruik maken van de specifieke eigenschappen van de GSR-shuffle.

De berekening van de variation distance in hoofdstuk 5 maakt gebruik van het feit dat de kans op een permutatie volledig bepaald wordt door zijn rising sequences. Wanneer we één van de twee aannames van het GSR-model veranderen, is dit niet langer het geval.

Het koppelen van Markovketens kan in het algemeen bij alle modellen gebruikt worden. De moeilijkheid is echter het vinden van een "handige", goede en geldige simultane verdeling. De simultane verdeling, zoals in hoofdstuk 4, is niet algemeen toepasbaar. We moeten op een andere manier bepalen, hoeveel invloed een afwijking van de voor de GSR-shuffle gemaakte aannames heeft op onze resultaten. We zullen daarom de *eigenwaarden* van de Markovmatrix aan een nader onderzoek onderwerpen.

7.2 Het belang van eigenwaarden

Definitie 7.1 *λ is een eigenwaarde van de matrix P, als geldt: $\exists x \neq (0, \ldots, 0)^T$: $Px = \lambda x$. x wordt de bij λ behorende eigenvector genoemd.*

De eigenwaarden en eigenvectoren bepalen de matrix en matrixprodukten volledig, en, vertaald naar het schudden, is de verdeling na s schudbeurten hiermee derhalve direct te berekenen.

Uit Perron-Frobenius theorie volgt verder dat, wanneer U de evenwichtsverdeling is van Q^{*s}

$$\text{Variation distance} = \|Q^{*s} - U\| \sim c\lambda^s (s \to \infty) \text{ voor een } c > 0$$

met λ de op een na grootste eigenwaarde.

We kunnen met de op een na grootste eigenwaarde dus bepalen "hoe snel" de variation distance asymptotisch naar nul gaat. We kunnen hiermee echter niet zeggen vanaf welke s de variation distance klein wordt.

7.3 Eigenwaarden van de GSR-matrix

De eigenwaarden van de GSR-matrix zijn eenvoudig expliciet te bepalen. Merk op dat een binomiaal coëfficiënt $\binom{x+y}{n}$ is te schrijven als een n-de graads polynoom $\sum_{i=0}^{n} c_i x^i$ voor n en y vast. De kans op een permutatie met r rising sequences bij de GSR-shuffle na s keer schudden, is dan te schrijven als:

$$\binom{2^s + n - r}{n} / 2^{ns} = \sum_{i=0}^{n} c_i (2^s)^i / 2^{ns} = \sum_{i=0}^{n} c_i 2^{s(i-n)} = \sum_{j=0}^{n} c_{n-j} (\frac{1}{2^j})^s.$$

Aangezien elk element van P^s een lineaire combinatie van de eigenwaarden is, is het nu mogelijk te bewijzen dat de eigenwaarden van P worden gegeven door $(\frac{1}{2})^j$ voor $j = 0, 1, \ldots, n$, waarbij de multipliciteit van $(\frac{1}{2})^j$ gelijk aan $(-1)^{n-j} s_1(n, j)$, met $s_1(n, j)$ de Stirling-getallen van de eerste soort.

De eigenwaarden van de matrices van andere schudmodellen zijn helaas niet zo eenvoudig te bepalen. Er bestaan weliswaar computerprogramma's die eigenwaarden en eigenvectoren kunnen berekenen, maar zo'n 6 kaarten (de matrix bevat dan 720×720 is ruim 500 duizend elementen) is het maximum van wat een programma op dit moment aankan. Om voor 7 kaarten de eigenwaarden van de schudmatrix te kunnen berekenen moet de capaciteit vernegenveertigvoudigd worden.

We zullen de Markovmatrix die het resultaat is van een (willekeurig) schudproces daarom nader te bekijken. Door gebruik te maken van de speciale eigenschappen die deze matrix bezit, zullen we de eigenwaarden kunnen bepalen van grotere matrices.

7.4 Het bepalen van de eigenwaarden van een schudmatrix

7.4.1 Centrosymmetrie

Uiteraard kan elke willekeurige volgorde van de permutaties gebruikt worden bij het opstellen van de $n! \times n!$ matrix. Er is echter een voor de hand liggende manier om de permutaties af te tellen, de lexicografische volgorde, waardoor de matrix een extra eigenschap krijgt. De lexicografische volgorde van twee permutaties $\pi = (\pi(1) \ \dots \ \pi(n))$ en $\sigma = (\sigma(1) \ \dots \ \sigma(n))$ is: $\pi < \sigma$ dan en slechts dan als $\exists j : \pi(i) = \sigma(i) \ \forall i < j$ en $\pi(j) < \sigma(j)$.

We hebben een 1-1 correspondentie f_n geconstrueerd tussen de permutaties en $\{1 \ \dots \ n!\}$, zodanig dat de permutaties een nummer krijgen overeenkomstig de lexicografische volgorde. Het nummeren van de permutaties kan handig zijn bij het werken met permutaties. Het idee achter de aftelling is, dat er $n!$ mogelijke permutaties zijn van n elementen. Door het eerste element te verwijderen, ontstaat een permutatie van $n-1$ elementen, waar ten hoogste $(n-1)!$ mogelijkheden voor zijn.

Lemma 7.2 *Er bestaat een 1-1 correspondentie f_n tussen de permutaties en $\{1 \ \dots \ n!\}$, zodanig dat $f_n(\pi) < f_n(\sigma)$ dan en slechts dan als $\pi < \sigma$. Deze wordt gegeven door:*

$$f_n(\pi) = (\pi(1) - 1) \times (n-1)! + f_{n-1}(\pi'),$$

met $f_1((1)) = 1$ en $\pi' = (\pi'(1) \ \dots \ \pi'(n-1))$, waarbij

$$\pi'(i) = \begin{cases} \pi(i+1) & \textit{als } \pi(i+1) < \pi(1) \\ \pi(i+1) - 1 & \textit{als } \pi(i+1) > \pi(1). \end{cases}$$

Bewijs We beginnen het bewijs met op te merken dat $f_n((1\ 2\ \dots\ n)) = 1$, en $f_n((n\ n-1\ \dots\ 1)) = n!$, wat we met behulp van inductie bewijzen. $f_1((1)) = 1 = 1!$, per definitie. Stel nu dat $f_n((n\ n-1\ \dots\ 1)) = n!$, dan $f_{n+1}((n+1\ n\ n-1\ \dots\ 1)) = n \times n! + f_n((n\ n-1\ \dots\ 1)) = n \times n! + n! = (n+1) \times n! = (n+1)!$, waarmee de formule bewezen is. Het is gemakkelijk in te zien dat deze permutatie ook inderdaad het maximum geeft van f_n.

"$\Rightarrow$" Stel $f_n(\pi) < f_n(\sigma)$. Dan $(\pi(1)-1)\times(n-1)! + f_{n-1}(\pi') < (\sigma(1)-1)\times(n-1)! + f_{n-1}(\sigma')$. Aangezien $f_{n-1}(\tau) \leq (n-1)!$ zijn er nu twee gevallen te onderscheiden:
(1) $\pi(1) < \sigma(1)$. Waarmee we bewezen hebben dat $\pi < \sigma$.
(2) $\pi(1) = \sigma(1)$ en $f_{n-1}(\pi') < f_{n-1}(\sigma')$. We kunnen dit herhaald toepassen totdat er geldt $\pi(j) < \sigma(j)$ en $\pi(i) = \sigma(i)\ \forall i < j$. Conclusie: $\pi < \sigma$.

"$\Leftarrow$" Stel $\pi < \sigma$. We kiezen j weer zodanig dat $\pi(i) = \sigma(i)\ \forall i < j$ en $\pi(j) < \sigma(j)$. Het is duidelijk dat $f_n(\pi) - f_{n-j}(\pi^{(j)}) = f_n(\sigma) - f_{n-j}(\sigma^{(j)})$ en $f_{n-j}(\pi^{(j)}) < f_{n-j}(\sigma^{(j)})$. Dus: $f_n(\pi) < f_n(\sigma)$. $\square$

Aangezien f_n is 1-1 relatie is, bestaat ook de inverse f_n^{-1}.

$$\begin{aligned}
f_n^{-1}(x) &= \Big(\Big\lfloor\frac{x-1}{(n-1)!}\Big\rfloor + 1, h\big(f_{n-1}^{-1}(x - \Big\lfloor\frac{x-1}{(n-1)!}\Big\rfloor), \Big\lfloor\frac{x-1}{(n-1)!}\Big\rfloor + 1\big)\Big), \\
f_1^{-1}(1) &= (1), \text{ en} \\
h(i)(\pi, y) &= \begin{cases} \pi(i) & \text{als } \pi(i) < y \\ \pi(i)+1 & \text{als } \pi(i) \geq y. \end{cases}
\end{aligned}$$

Voorbeeld

$$\begin{aligned}
f_6((3\ 2\ 5\ 4\ 1\ 6)) &= 2\times 5! + f_5((2\ \mathbf{4}\ \mathbf{3}\ 1\ \mathbf{5})) \\
&= 240 + 1\times 4! + f_4((\mathbf{3}\ \mathbf{2}\ 1\ \mathbf{4})) \\
&= 264 + 2\times 3! + f_3((2\ 1\ \mathbf{3})) \\
&= 276 + 1\times 2! + f_2((1\ \mathbf{2})) \\
&= 278 + 0\times 1! + f_1((\mathbf{1})) = 278 + 1 = 279.
\end{aligned}$$

Hierbij zijn de getallen die veranderen in π' **vet** gedrukt.

Omgekeerd:

$$\begin{aligned}
f_6^{-1}(279) &= \Big(\Big\lfloor\frac{279-1}{5!}\Big\rfloor + 1, h\Big(f_5^{-1}(279 - \Big\lfloor\frac{279-1}{5!}\Big\rfloor), \Big\lfloor\frac{279-1}{5!}\Big\rfloor\Big)\Big) \\
&= \Big(3, h\Big(\Big(\Big\lfloor\frac{39-1}{4!}\Big\rfloor + 1, h(f_4^{-1}(39 - \Big\lfloor\frac{39-1}{4!}\Big\rfloor), \Big\lfloor\frac{39-1}{4!}\Big\rfloor)), 3\Big)\Big) \\
&= \ldots = \Big(3, h\Big((2, h(3, h(2, h(1, h((1), 1), 2), 2), 3), 2), 3\Big)\Big) \\
&= \Big(3, h\Big(2, h(3, h(2, h((1\ \mathbf{2}), 2), 2), 3), 2), 3\Big)\Big) \\
&= \Big(3, h\Big(2, h(3, h((2\ 1\ \mathbf{3}), 3), 2), 3\Big)\Big)
\end{aligned}$$

$$
\begin{aligned}
&= \Big(3, h\Big(2, h((3\ 2\ 1\ \mathbf{4}), 2), 3\Big)\Big) \\
&= \Big(3, h\Big((2\ \mathbf{4}\ \mathbf{3}\ 1\ \mathbf{5}), 3\Big)\Big) \\
&= \Big(3\ 2\ \mathbf{5}\ \mathbf{4}\ 1\ \mathbf{6}\Big).
\end{aligned}
$$

Eigenschap 7.3 *Als de toestandsruimte op de voor de hand liggende manier wordt afgeteld, is de matrix is centrosymmetrisch (de matrix is invariant onder een 180 graden rotatie:* $p_{ij} = p_{n!+1-i,n!+1-j} \forall i, j$*).*

Bewijs Laat $\pi = (\pi(1), \ldots, \pi(n))$ en $g_n(\pi) = (n+1-\pi(1), n+1-\pi(2), \ldots, n+1-\pi(n))$. We merken op dat als het uitvoeren van permutatie (operatie) σ op π, het resultaat τ $(= \pi\sigma)$ geeft, het uitvoeren van σ op $g_n(\pi)$ het resultaat $g_n(\tau)$ geeft. Dit volgt het feit dat $(g_n(\pi) \circ \sigma)(i) = (g_n(\pi))(\sigma(i)) = n + 1 - \pi(\sigma(i)) = (g_n(\pi\sigma))(i)$.

Dit is makkelijker in te zien, als men bedenkt dat het uitvoeren van de functie g_n niets anders is dan het voorvermenigvuldigen met de permutatie $\nu = (n, n-1, \ldots, 1)$. Het is dan meteen duidelijk dat $(\nu\pi)\sigma = \nu(\pi\sigma)$.

Om de centrosymmetrie te bewijzen, rest het ons te bewijzen dat $f_n(g_n(\pi)) = n! + 1 - f_n(\pi)$.

$$
\begin{aligned}
f_n(g_n(\pi)) &= (g_n(1)(\pi) - 1) \times (n-1)! + f_{n-1}(g'_n(\pi)) \\
&= (n - \pi(1)) \times (n-1)! + f_{n-1}(g_{n-1}(\pi')) && (7.1) \\
&= (n-1)(n-1)! - (\pi(1) - 1) \times (n-1)! + f_{n-1}(g_{n-1}(\pi')) \\
&= \sum_{i=1}^{n-1} i \times i! - f_n(\pi) + 2f_1((1)) && (7.2) \\
&= (n! - 1) - f_n(\pi) + 2 && (7.3) \\
&= n! + 1 - f_n(\pi).
\end{aligned}
$$

De stappen zijn als volgt:
(7.1) dit volgt uit het feit dat $g'_n(\pi) = g_{n-1}(\pi')$,
(7.2) hier is gebruik gemaakt van iteratie,
(7.3) volgt uit het feit dat $\sum_{i=1}^{n-1} i \times i! = n! - 1$, zoals reeds bewezen is bij lemma 7.2 ($f_n((n, n-1, \ldots, 1)) = n!$). □

Voorbeeld Ter verduidelijking geven we de volledige matrix voor $n = 3$.

$$\begin{array}{cc}
 & \begin{matrix} (123) & (132) & (213) & (231) & (312) & (321) \end{matrix} \\
\begin{matrix} (123) \\ (132) \\ (213) \\ (231) \\ (312) \\ (321) \end{matrix} &
\begin{bmatrix}
p_1 & p_2 & p_3 & p_4 & p_5 & p_6 \\
p_2 & p_1 & p_5 & p_6 & p_3 & p_4 \\
p_3 & p_4 & p_1 & p_2 & p_6 & p_5 \\
p_5 & p_6 & p_2 & p_1 & p_4 & p_3 \\
p_4 & p_3 & p_6 & p_5 & p_1 & p_2 \\
p_6 & p_5 & p_4 & p_3 & p_2 & p_1
\end{bmatrix}
\end{array}$$

7.4.2 Opdelen van de matrix in twee delen

Met behulp van eigenschap 7.3 kan het bepalen van de eigenwaarden op een handige manier [Collar, 1962].

Definieer J als de matrix met 1-en op de rechtsboven-linksonder diagonaal en verder 0-en. Merk op dat $JPJ = P$ voor elke centrosymmetrische matrix (immers voorvermenigvuldiging met J zorgt voor omdraaiing van de volgorde van de rijen van P, navermenigvuldiging voor omdraaiing van de volgorde van de kolommen). Bovendien is $J^2 = I$ en $J^{-1} = J$.

Merk op dat elke centrosymmetrische $(2m \times 2m)$ matrix P als volgt geschreven kan worden:

$$P = \begin{bmatrix} A, & C \\ JCJ, & JAJ \end{bmatrix},$$

met A, C en J $(m \times m)$ matrices.

In het vervolg zullen we $C = BJ$ gebruiken ($JCJ = JB$).

Stelling 7.4 (Collar, 1962) *De eigenwaarden van een centrosymmetrische $(2m \times 2m)$ matrix P,*

$$P = \begin{bmatrix} A, & BJ \\ JB, & JAJ \end{bmatrix},$$

zijn gelijk aan de eigenwaarden van de $(m \times m)$ matrices $A + B$ en $A - B$. De matrix van eigenvectoren Σ_P kan uit de eigenvectoren van $A + B$ en $A - B$

bepaald worden:

$$\Sigma_P = \begin{bmatrix} \Sigma_s, & -\Sigma_v \\ J\Sigma_s, & J\Sigma_v \end{bmatrix},$$

met Σ_s de matrix van eigenvectoren behorend bij $A+B$ en Σ_v de matrix van eigenvectoren behorend bij $A-B$.

Bewijs Definieer K als

$$K = \begin{bmatrix} I, & -I \\ J, & J \end{bmatrix},$$

een $(2m \times 2m)$ matrix, I en J $(m \times m)$ matrices. Dan:

$$K^{-1} = \frac{1}{2} \begin{bmatrix} I, & J \\ -I, & J \end{bmatrix}$$

en

$$(7.4)\ K^{-1}PK = \begin{bmatrix} A+B, & 0 \\ 0, & A-B \end{bmatrix}.$$

Noteer met Λ_s de matrix met de eigenwaarden van de matrix $A+B$ op de diagonaal, met Σ_s de bijbehorende matrix van eigenvectoren, en evenzo met Λ_v de matrix met de eigenwaarden van $A-B$, en met Σ_v de bijbehorende matrix van eigenvectoren. Dan

$$\left.\begin{array}{rcl} (A+B)\Sigma_s & = & \Sigma_s\Lambda_s \\ (A-B)\Sigma_v & = & \Sigma_v\Lambda_v \end{array}\right\}.$$

Anders geschreven:

$$\begin{bmatrix} A+B, & 0 \\ 0, & A-B \end{bmatrix} \begin{bmatrix} \Sigma_s, & 0 \\ 0, & \Sigma_v \end{bmatrix} = \begin{bmatrix} \Sigma_s, & 0 \\ 0, & \Sigma_v \end{bmatrix} \begin{bmatrix} \Lambda_s, & 0 \\ 0, & \Lambda_v \end{bmatrix}.$$

Substitutie van 7.4 voor de eerste matrix en voorvermenigvuldiging met K geeft

$$\begin{bmatrix} A, & BJ \\ JB, & JAJ \end{bmatrix} \begin{bmatrix} \Sigma_s, & -\Sigma_v \\ J\Sigma_s, & J\Sigma_v \end{bmatrix} = \begin{bmatrix} \Sigma_s, & -\Sigma_v \\ J\Sigma_s, & J\Sigma_v \end{bmatrix} \begin{bmatrix} \Lambda_s, & 0 \\ 0, & \Lambda_v \end{bmatrix},$$

oftewel

$$P\Sigma_P = \Sigma_P \Lambda_P.$$

De eigenwaarden en eigenvectoren van P zijn derhalve:

$$\begin{aligned} \Lambda_P &= \begin{bmatrix} \Lambda_s, & 0 \\ 0, & \Lambda_v \end{bmatrix}, \\ \Sigma_P &= \begin{bmatrix} \Sigma_s, & -\Sigma_v \\ J\Sigma_s, & J\Sigma_v \end{bmatrix}. \end{aligned}$$

□

Ook voor centrosymmetrische matrices van oneven orde bestaat een dergelijke opdeling (zie voor details [Collar, 1962]).

7.4.3 Partitioneren

Om de eigenwaarden te berekenen van een centrosymmetrische matrix kunnen we op grond van stelling 7.4 volstaan met het berekenen van de eigenwaarden van twee matrices, die de helft kleiner zijn. Stelling 7.4 kan over het algemeen maar één keer worden toegepast, aangezien $A + B$ en $A - B$ niet per definitie weer centrosymmetrisch zijn.

De *schudmatrix* P die wij beschouwen is echter zo bijzonder, dat wij met een aangepaste methode, nog kleinere matrices kunnen krijgen, met dezelfde eigenwaarden als P, die ook nog centrosymmetrisch zijn! Reeds in [Doner & Uppuluri, 1970] worden eigenwaarden van een schudmatrix berekend met behulp van het vormen van partities. De methode die daar gebruikt wordt is een speciaal geval van de onderstaande methode.

We zullen bij het bespreken van de methode gebruik maken van de cykelnotatie van een permutatie, zoals geïntroduceerd in voorbeeld 2.4 over de perfect shuffle. Een permutatie kan opgedeeld worden in *partities*, die ieder een *cykel* zijn. Voor de volledigheid herhalen we de definitie van een cykel.

Definitie 7.5 *Beschouw een permutatie. Een cykel is een k-tupel $(x_1\ x_2\ \ldots\ x_k)$, met x_i's de gepermuteerde objecten, zodanig dat na het uitvoeren van de permutatie x_i op de plaats van x_{i+1} terecht is gekomen, en x_k op de plaats van x_1.*

Voorbeeld De permutatie (1 3 4 2 6 5) heeft de volgende cykels: (1) (kaart 1 gaat naar plaats 1), (2 4 3) (kaart 2 gaat naar plaats 4, kaart 4 gaat naar plaats 3, en kaart 3 gaat naar plaats 2) en (5 6) (kaart 5 en 6 verwisselen van plaats). De laatst genoemde cykel, een cykel van lengte 2, wordt ook wel aangeduid als *transpositie*.

De door ons gebruikte beschrijving van cykels, is de *disjuncte cykeldecompositie* uit de groepentheorie. Deze decompositie in disjuncte cykels is uniek (hoewel de cykels natuurlijk in willekeurige volgorde genoemd kunnen worden en ook het element dat binnen een cykel als eerste genoemd wordt, willekeurig gekozen kan worden (de cykel (2 4 3) is dezelfde als de cykel (3 2 4))).

We geven allereerst een bekend lemma uit de groepentheorie. Wij danken professor Ditters, dat hij ons hierop attent maakte.

Lemma 7.6 *Elke cykel* $(c_1\ c_2\ \ldots\ c_\ell)$ *van een permutatie* π*, wordt in de geconjugeerde van* π*,* $\sigma\pi\sigma^{-1}$*, overgevoerd in de cykel* $(\sigma(c_1)\ \sigma(c_2)\ \ldots\ \sigma(c_\ell))$*.*

Bewijs Neem de verzameling $\Gamma = \{\sigma(c_1), \sigma(c_2), \ldots, \sigma(c_\ell)\}$. Voor $\gamma \in \Gamma$ geldt dat $\sigma\pi\sigma^{-1}\gamma = \sigma\pi\sigma^{-1}\sigma(c_j) = \sigma\pi(c_j) = \sigma(c_{j+1})$ als $j < \ell$ en $\sigma(c_1)$ als $j = \ell$. $\square$

Met behulp van de volgende stelling [Schalekamp & Van Zuylen, b], kunnen we kleinere matrices maken waarvan de eigenwaarden een deelverzameling vormen van de eigenwaarden van de $(n! \times n!)$ schudmatrix P. Het idee is een tweede Markovproces te construeren waarvan de toestandsruimte een factor k kleiner is, door middel van partitioneren. De resulterende Markovmatrix blijkt centrosymmetrisch te zijn, waardoor de eigenwaarden van deze matrix met behulp van de methode van Collar berekend kunnen worden. De matrices waarvan we de eigenwaarden uitrekenen zijn nu $(n!/2k \times n!/2k)$ matrices.

Stelling 7.7 *Gegeven de Markovketen* $(X_s)_{s\in\mathbb{Z}^+}$ *van een schudproces, op de toestandsruimte* $\mathcal{S}_n$*, met* P *de bijbehorende schudmatrix. Beschouw een permutatie* ϑ *met periode (van orde)* k *(*$k = \min_{i>0}\{\vartheta^i = 1\}$*, met 1 de identiteit ofwel het neutrale element,* $(1\ 2\ \ldots\ n)$*).*
De equivalentierelatie $\pi_1 \sim \pi_2 \iff \exists i : \pi_2 = \vartheta^i\pi_1$ *genereert* $\frac{n!}{k}$ *partities* $(P_1, P_2, \ldots, P_{\frac{n!}{k}})$ *van* $\mathcal{S}_n$*.*

We definiëren de keten $(Y_s)_{s\in\mathbb{Z}^+}$ *met als toestandsruimte de partities, als volgt:*

$$Y_s = u \quad als \quad X_s \in P_u \quad \forall s.$$

(i) De keten $(Y_s)_{s\in\mathbb{Z}^+}$ *is een Markovketen.*

(ii) Alle $\frac{n!}{k}$ eigenwaarden van de matrix M_ϑ behorend bij dit Markovproces, zijn ook eigenwaarden van P.

(iii) De matrix M_ϑ is centrosymmetrisch, bij geschikte aftelling van de partities.

Bewijs (i) De kans $\mathbb{P}(\pi \to \sigma)$ is slechts afhankelijk van de operatie η, met $\pi\eta = \sigma$. Dit geeft $\eta = \pi^{-1}\sigma$. We noteren de kans $\mathbb{P}(\pi \to \sigma)$ nu als de kans op de operatie, $\mathbb{P}(\pi^{-1}\sigma)$.

Merk op dat voor een element $\pi_i \in P_i$ geldt:

$$\mathbb{P}(\pi_i \to P_j) = \sum_{\sigma \in P_j} \mathbb{P}(\pi_i^{-1}\sigma) = \sum_{m=0}^{k-1} \mathbb{P}(\pi_i^{-1}\vartheta^m \pi_j),$$

met π_j een willekeurig element van P_j.

Voor de overige elementen $\vartheta^\ell \pi_i$ van P_i geldt:

$$\begin{aligned} \mathbb{P}(\vartheta^\ell \pi_i \to P_j) &= \sum_{m=0}^{k-1} \mathbb{P}(\pi_i^{-1}\vartheta^{-\ell}\vartheta^m \pi_j) \\ &= \sum_{m=0}^{k-1} \mathbb{P}(\pi_i^{-1}\vartheta^{-\ell+m}\pi_j) \\ &= \sum_{m'=0}^{k-1} \mathbb{P}(\pi_i^{-1}\vartheta^{m'}\pi_j) \\ &= \mathbb{P}(\pi_i \to P_j). \end{aligned}$$

We kunnen nu $\mathbb{P}(P_i \to P_j)$ definiëren als $\mathbb{P}(\pi_i \to P_j)$ voor een willekeurig element π_i van P_i. Het is duidelijk dat dit weer een Markovketen is.

(ii) [Doner & Uppuluri, 1970] De matrix behorende bij het Markovproces van de partities noteren we als M_ϑ. Er geldt dat $(M_\vartheta)_{i'j} = \sum_{\pi_g \in P_j} P_{ig}$, voor elke $\pi_i \in P_{i'}$. We nemen hierbij aan dat $P_{ij} = \mathbb{P}(\pi_i \to \pi_j)$.
Stel λ is een eigenwaarde van M_ϑ, met eigenvector x, $M_\vartheta x = \lambda x$. Definieer $y_i = x_j$ als $\pi_i \in P_j$, $j \in \{1, \ldots, \frac{n!}{k}\}$. We tonen elementsgewijs aan dat λ ook een eigenwaarde is van P met eigenvector y.

$$(Py)_i = \sum_{h=1}^{n!} P_{ih} y_h = \sum_{j=1}^{n!/k} \Big(\sum_{\pi_g \in P_j} P_{ig} y_g \Big) = \sum_{j=1}^{n!/k} \Big(\sum_{\pi_g \in P_j} P_{ig} \Big) x_j$$

$$= \sum_{j=1}^{n!/k} (M_\vartheta)_{i'j} x_j = \lambda x_{i'} = \lambda y_i.$$

(iii) We definiëren $\sigma R = \{\sigma\rho \mid \rho \in R\}$ en $R_1 R_2 = \cup_{\rho_1 \in R_1}(\rho_1 R_2)$. Merk op dat als er geldt dat

$$P_{\frac{n!}{k}+1-i} = \nu_\vartheta P_i \quad \forall i,$$

de partitiematrix centrosymmetrisch is. Immers, noem $H_{ij} = \{\eta \mid \pi_i \eta = \pi_j \ \forall\ \pi_i \in P_i,\ \pi_j \in P_j\}$, dan $P_{\frac{n!}{k}+1-i} H_{ij} = \nu_\vartheta P_i H_{ij} = \nu_\vartheta P_j = P_{\frac{n!}{k}+1-j}$.
In het bewijs van eigenschap 7.3 wordt gebruik gemaakt van $\nu = (n, n-1, n-2, \ldots, 2, 1)$.

Noem $\Theta = \{\vartheta, \vartheta^2, \ldots, \vartheta^k\}$. In de groepentheorie wordt dit de *cyclische groep* genoemd met *voortbrenger* ϑ. Uit $\nu_\vartheta P_i = P_{\frac{n!}{k}+1-i}$ volgt dat $\nu_\vartheta \Theta = \Theta \nu_\vartheta$, aangezien $\{\nu_\vartheta \pi_i, \nu_\vartheta \vartheta \pi_i, \ldots, \nu_\vartheta \vartheta^k \pi_1\} = \{\pi_{\frac{n!}{k}+1-i}, \vartheta \pi_{\frac{n!}{k}+1-i}, \ldots, \vartheta^k \pi_{\frac{n!}{k}+1-i}\} = \{\nu_\vartheta \pi_i, \vartheta \nu_\vartheta \pi_i, \ldots, \vartheta^k \nu_\vartheta \pi_i\}$.
Wij herschrijven dit tot $\Theta = \nu_\vartheta \Theta \nu_\vartheta^{-1}$. De verzameling $\mathcal{N}_\Theta = \{\sigma \in \mathcal{S}_n \mid \sigma \Theta \sigma^{-1} = \Theta\}$ heet in de groepentheorie de *normalisator* van Θ binnen $\mathcal{S}_n$. Het is triviaal dat $\Theta \subseteq \mathcal{N}_\Theta$. De vraag is of de normalisator echt groter is dan Θ. Wij danken dr. Van der Waall van de UvA voor zijn onmisbare hulp bij het volgende bewijs.

We geven een constructief bewijs voor het bestaan van $\nu_\vartheta \in \mathcal{N}_\Theta \backslash \Theta$, voor $n \geq 4$. Beschouw de *disjuncte cykeldecompositie* van ϑ. We beschouwen drie gevallen.

(a) Er bestaat een cykel met lengte $\ell > 2$, zeg $(c_1\ c_2\ \ldots\ c_\ell)$. De ν_ϑ die we construeren krijgt nu de volgende cykels: $(c_1\ c_\ell)\ (c_2\ c_{\ell-1})\ \ldots\ (c_{\frac{1}{2}\ell}\ c_{\frac{1}{2}\ell+1})$ voor ℓ even, of $(c_1\ c_\ell)\ (c_2\ c_{\ell-1})\ \ldots\ (c_{\frac{1}{2}(\ell+1)})$ voor ℓ oneven.
Voor de overige cykels $(c'_1\ c'_2\ \ldots\ c'_{\ell'})$ kiezen we ν_ϑ zodanig dat $\nu(c'_i) = c'_j$ met $j \equiv (k-1)(i-1)+1 \pmod{\ell'}$.

De geconstrueerde ν_ϑ is geen macht van ϑ. Immers, ϑ^r heeft in ieder geval als cykel $(c_1\ c_{j_1}\ c_{j_2}\ \ldots)$ met $j_1 \equiv r+1 \pmod{\ell}$, $j_2 \equiv 2r+1 \pmod{\ell}$, etcetera. Deze cykel is alleen dan een cykel van ν_ϑ als dit de transpositie $(c_1\ c_\ell)$ is (de disjuncte cykeldecompositie is immers uniek), oftewel $r+1 \equiv \ell \pmod{\ell}$ en $2r+1 \equiv 1 \pmod{\ell}$. Dit heeft alleen een oplossing voor $\ell = 2$. Dit is in tegenspraak met de aanname $\ell > 2$.

Wij bewijzen tenslotte dat inderdaad voor deze ν_ϑ geldt dat $\nu_\vartheta \Theta \nu_\vartheta^{-1} = \Theta$.
$\nu_\vartheta \vartheta \nu_\vartheta^{-1}$ heeft de cykel $(\nu_\vartheta(c_1)\ \nu_\vartheta(c_2)\ \ldots\ \nu_\vartheta(c_\ell))$ (zie lemma 7.6). Met onze geconstrueerde ν_ϑ is dit $(c_\ell\ c_{\ell-1}\ \ldots\ c_1)$. Dit is uiteraard een cykel van $\vartheta^{\ell-1}$, maar ook van ϑ^{k-1} aangezien ℓ een deler is van k (immers, k is het kleinste

gemene veelvoud van de cykellengtes). Ook de overige cykels komen door de constructie van ν_ϑ overeen met de cykels van ϑ^{k-1}.
We hebben nu bewezen dat $\nu_\vartheta \vartheta \nu_\vartheta^{-1} = \vartheta^{k-1}$. Hieruit volgt dat $\nu_\vartheta \Theta \nu_\vartheta^{-1} = \Theta$, omdat voor de geconjugeerde van ϑ^s geldt

$$\nu_\vartheta \vartheta^s \nu_\vartheta^{-1} = \nu_\vartheta \big(\prod_{i=1}^{s} \nu_\vartheta^{-1} \vartheta^{k-1} \nu_\vartheta \big) \nu_\vartheta^{-1} = \vartheta^{s(k-1)},$$

en $k-1$ en k copriem zijn.

(b) Er bestaan twee cykels met lengte 2, zeg $(c_1\ c_2)\ (c_3\ c_4)$. Kies voor ν_ϑ de permutatie met slechts één cykel van lengte groter dan 1, namelijk $(c_1\ c_2)$. Het is duidelijk dat ν_ϑ geen macht is van ϑ, en dat de geconjugeerde van ϑ^s gelijk is aan ϑ^s.
Overigens kan ook gekozen geworden voor ν_ϑ met cykels $(c_1\ c_3)\ (c_2\ c_4)$.

(c) Er zijn twee cykels van lengte 1, $(c_1)\ (c_2)$. Kies voor ν_ϑ weer de permutatie met slechts één cykel van lengte groter dan 1, namelijk $(c_1\ c_2)$.

Aangezien een permutatie voor $n \geq 4$ in ieder geval in één van bovenstaande drie categorieën valt, hebben we inderdaad het bestaan van een $\nu_\vartheta \in \mathcal{N}_\Theta \backslash \Theta$ bewezen. Het feit dat de normalisator van een cyclische ondergroep van $\mathcal{S}_n$ $(n \geq 4)$ echt groter is dan de cyclische ondergoep zelf, was niet algemeen bekend.

De keuze aan ν_ϑ's is in het algemeen zeer ruim, aangezien bovenstaande gevallen elkaar niet uitsluiten, en er binnen elk geval ook keuzes gemaakt kunnen worden. Het is aardig op te merken, dat het altijd mogelijk is een ν_ϑ te construeren met periode 2.

Tenslotte merken we nog zijdelings op dat voor $n = 3$, voor het geval dat ϑ bestaat uit een 1-cykel en een 2-cykel, de normalisator $\mathcal{N}_\Theta$ gelijk is aan Θ. Sterker nog, $\Theta \cap \pi \Theta \pi^{-1} = \{1\}$ voor $\pi \in \mathcal{S}_3 \backslash \Theta$. Dit is precies de definitie van het *Frobenius complement*. $\mathcal{S}_3$ wordt hierom een *Frobenius groep* genoemd. $\square$

Wij vermoeden dat *alle* eigenwaarden van de oorspronkelijke matrix kunnen worden gevonden met deze methode. Wij hebben hier echter geen bewijs voor kunnen vinden.

Het is niet nodig om alle $n!$ ϑ's af te gaan, om de eigenwaarden van de schudmatrix P te berekenen.

Stelling 7.8 *Voor alle σ, ϑ geldt: de partitiematrix gegenereerd door ϑ, geeft dezelfde eigenwaarden als de partitiematrix gegenereerd door $\tilde{\vartheta} = \sigma \vartheta \sigma^{-1}$.*

Bewijs Merk op dat $\tilde{P}_i = \sigma P_i$, de partities geven behorend bij $\tilde{\vartheta}$. Immers, $\tilde{\vartheta}\tilde{P}_i = \sigma\vartheta\sigma^{-1}\sigma P_i = \sigma\vartheta P_i = \sigma P_i = \tilde{P}_i$.
Laat weer $H_{ij} = \{\eta \mid \pi_i\eta = \pi_j \quad \forall \pi_i \in P_i,\ \pi_j \in P_j\} = \{\pi_i^{-1}\pi_j \quad \forall \pi_i \in P_i,\ \pi_j \in P_j\}$, en evenzo $\tilde{H}_{ij} = \{\tilde{\pi}_i^{-1}\tilde{\pi}_j \quad \forall \tilde{\pi}_i \in \tilde{P}_i,\ \tilde{\pi}_j \in \tilde{P}_j\}$. Er geldt dat $H_{ij} = \tilde{H}_{ij}$, aangezien $\tilde{\pi}_i^{-1}\tilde{\pi}_j = \pi_i^{-1}\sigma^{-1}\sigma\pi_j = \pi_i^{-1}\pi_j$. De matrices gegenereerd door ϑ en $\sigma\vartheta\sigma^{-1}$ zijn derhalve hetzelfde. $\square$

Uit het lemma 7.6 volgt een eigenschap die ϑ en $\tilde{\vartheta}$ gemeen hebben.

Gevolg 7.9 *De cykellengtes van ϑ en $\sigma\vartheta\sigma^{-1}$ zijn gelijk.*

Samenvattend, een algoritme om eigenwaarden van een schudmatrix te berekenen, kan handig gebruik maken van gevolg 7.9 voor de keuze van de verschillende ϑ's. Met behulp van een ν, zoals in het bewijs van stelling 7.7 (iii) kan een centrosymmetrische partitiematrix gemaakt worden. Door de partitiematrices op te delen volgens de methode van Collar, kunnen nu van grotere schudmatrices op een snelle manier de eigenwaarden en eigenvectoren bepaald worden. De multipliciteit van de eigenwaarden kan echter niet op deze manier bepaald worden.

We zullen ter verduidelijking een aantal voorbeelden van partitiematrices geven. Voor de resultaten van deze methode toegepast op een schudmatrix (welke ϑ's geven welke eigenwaarden) verwijzen we naar bijlage A.

7.5 Voorbeelden van de partitiemethode

We geven alle partitiematrices voor $n = 4$.

Aangezien de partitiematrix centrosymmetrisch is (zie bewijs van stelling 7.7), zullen we de matrices A en B geven, zodanig dat

$$P = \begin{bmatrix} A, & BJ \\ JB, & JAJ \end{bmatrix}.$$

De volgorde van de p's is zo gekozen om het gebruik van ϑ en ν duidelijk te maken.

Voor $n = 4$ geeft $\vartheta = (2\ 3\ 4\ 1)$ (periode$(\vartheta) = 4$) de volgende partities:

$$P_1 \quad = \quad \{(1\ 2\ 3\ 4), (2\ 3\ 4\ 1), (3\ 4\ 1\ 2), (4\ 1\ 2\ 3)\}$$

$$
\begin{aligned}
P_2 &= \{(1\ 2\ 4\ 3),(2\ 3\ 1\ 4),(3\ 4\ 2\ 1),(4\ 1\ 3\ 2)\} \\
P_3 &= \{(1\ 3\ 2\ 4),(2\ 4\ 3\ 1),(3\ 1\ 4\ 2),(4\ 2\ 1\ 3)\} \\
P_4 &= \{(1\ 3\ 4\ 2),(2\ 4\ 1\ 3),(3\ 1\ 2\ 4),(4\ 2\ 3\ 1)\} \\
P_5 &= \{(1\ 4\ 2\ 3),(2\ 1\ 3\ 4),(3\ 2\ 4\ 1),(4\ 3\ 1\ 2)\} \\
P_6 &= \{(1\ 4\ 3\ 2),(2\ 1\ 4\ 3),(3\ 2\ 1\ 4),(4\ 3\ 2\ 1)\}
\end{aligned}
$$

met ν_ϑ gelijk aan (1 4 3 2). Hieruit volgen deze matrices.

$$
\begin{aligned}
A &= \begin{bmatrix} p_1+p_{10}+p_{17}+p_{19} & p_2+p_9+p_{18}+p_{20} & p_3+p_{12}+p_{14}+p_{21} \\ p_2+p_{12}+p_{23}+p_{13} & p_1+p_{11}+p_{24}+p_{14} & p_5+p_{10}+p_{20}+p_{15} \\ p_3+p_{16}+p_{11}+p_{20} & p_4+p_{15}+p_{12}+p_{19} & p_1+p_{18}+p_8+p_{23} \end{bmatrix} \\
B &= \begin{bmatrix} p_8+p_6+p_{24}+p_{15} & p_7+p_5+p_{23}+p_{16} & p_{11}+p_4+p_{22}+p_{13} \\ p_7+p_4+p_{18}+p_{21} & p_8+p_3+p_{17}+p_{22} & p_9+p_6+p_{16}+p_{19} \\ p_{14}+p_5+p_{22}+p_9 & p_{13}+p_6+p_{21}+p_{10} & p_{17}+p_2+p_{24}+p_7 \end{bmatrix}
\end{aligned}
$$

Dit is de matrix en ϑ die Doner en Uppuluri impliceren in het artikel [Doner & Uppuluri, 1970] (zij kiezen voor elke n $\vartheta = (2\ 3\ 4\ \ldots\ n\ 1)$). Hierin wordt tevens geprobeerd deze matrix te interpreteren als een schudmatrix voor $n-1$ kaarten. De partitiematrix is echter geen schudmatrix, aangezien de kansen per rij niet overeenkomen; een schudbeurt is nu ook afhankelijk van de begintoestand.

Zoals bewezen in stelling 7.8 geven ook alle $\tilde{\vartheta}$ dezelfde partitiematrix. We geven alle alternatieven: $\{\tilde{\vartheta} = \sigma\vartheta\sigma^{-1},\ \forall\, \sigma\} = \{(2\ 3\ 4\ 1),(2\ 4\ 1\ 3),(3\ 1\ 4\ 2),(3\ 4\ 2\ 1),$ $(4\ 1\ 2\ 3),(4\ 3\ 1\ 2)\}$.

We geven de partitiematrix van $\vartheta = (1\ 3\ 4\ 2)$. Hierbij is $\nu_\vartheta = (1\ 2\ 4\ 3)$ gebruikt.

$$
\begin{aligned}
A &= \begin{bmatrix} p_1+p_4+p_5 & p_7+p_{14}+p_{19} & p_9+p_{17}+p_{21} & p_{10}+p_{18}+p_{22} \\ p_7+p_{10}+p_{11} & p_1+p_{16}+p_{21} & p_3+p_{18}+p_{19} & p_4+p_{17}+p_{20} \\ p_{13}+p_{16}+p_{17} & p_3+p_{10}+p_{23} & p_1+p_{12}+p_{20} & p_2+p_{11}+p_{19} \\ p_{19}+p_{22}+p_{23} & p_5+p_{12}+p_{17} & p_2+p_{10}+p_{14} & p_1+p_9+p_{13} \end{bmatrix} \\
B &= \begin{bmatrix} p_3+p_2+p_6 & p_{13}+p_8+p_{20} & p_{15}+p_{11}+p_{23} & p_{16}+p_{12}+p_{24} \\ p_9+p_8+p_{12} & p_{15}+p_2+p_{22} & p_{13}+p_5+p_{24} & p_{14}+p_6+p_{23} \\ p_{15}+p_{14}+p_{18} & p_9+p_4+p_{24} & p_7+p_6+p_{22} & p_8+p_5+p_{21} \\ p_{21}+p_{20}+p_{24} & p_{11}+p_6+p_{18} & p_8+p_4+p_{16} & p_7+p_3+p_{15} \end{bmatrix}
\end{aligned}
$$

We geven weer alle alternatieven: $\{\tilde{\vartheta} = \sigma\vartheta\sigma^{-1},\ \forall\, \sigma\} = \{(1\,3\,4\,2),(1\,4\,2\,3),(2\,3\,1\,4),$ $(2\ 4\ 3\ 1),(3\ 1\ 2\ 4),(3\ 2\ 4\ 1),(4\ 1\ 3\ 2),(4\ 2\ 1\ 3)\}$.

De partitiematrix van $\vartheta = (1\ 2\ 4\ 3)$ met $\nu_\vartheta = (2\ 1\ 3\ 4)$, is

$$
\begin{aligned}
A &= \begin{bmatrix}
p_1+p_2 & p_3+p_5 & p_4+p_6 & p_{13}+p_{19} & p_{14}+p_{20} & p_{17}+p_{23} \\
p_3+p_4 & p_1+p_6 & p_2+p_5 & p_7+p_{20} & p_8+p_{19} & p_{11}+p_{21} \\
p_5+p_6 & p_2+p_4 & p_1+p_3 & p_8+p_{14} & p_7+p_{13} & p_9+p_{15} \\
p_9+p_{10} & p_7+p_{12} & p_8+p_{11} & p_1+p_{22} & p_2+p_{21} & p_5+p_{19} \\
p_{11}+p_{12} & p_8+p_{10} & p_7+p_9 & p_2+p_{16} & p_1+p_{15} & p_3+p_{13} \\
p_{17}+p_{18} & p_{14}+p_{16} & p_{13}+p_{15} & p_4+p_{10} & p_3+p_9 & p_1+p_7
\end{bmatrix} \\
B &= \begin{bmatrix}
p_8+p_7 & p_{11}+p_9 & p_{12}+p_{10} & p_{21}+p_{15} & p_{22}+p_{16} & p_{24}+p_{18} \\
p_{14}+p_{13} & p_{17}+p_{15} & p_{18}+p_{16} & p_{23}+p_9 & p_{24}+p_{10} & p_{22}+p_{12} \\
p_{20}+p_{19} & p_{23}+p_{21} & p_{24}+p_{22} & p_{17}+p_{11} & p_{18}+p_{12} & p_{16}+p_{10} \\
p_{16}+p_{15} & p_{18}+p_{13} & p_{17}+p_{14} & p_{24}+p_3 & p_{23}+p_4 & p_{20}+p_6 \\
p_{22}+p_{21} & p_{24}+p_{19} & p_{23}+p_{20} & p_{18}+p_5 & p_{17}+p_6 & p_{14}+p_4 \\
p_{24}+p_{23} & p_{22}+p_{20} & p_{21}+p_{19} & p_{12}+p_6 & p_{11}+p_5 & p_8+p_2
\end{bmatrix}.
\end{aligned}
$$

De alternatieven: $\{\tilde{\vartheta} = \sigma\vartheta\sigma^{-1},\ \forall\, \sigma\} = \{(1\,2\,4\,3), (1\,3\,4\,2), (1\,4\,3\,2), (2\,1\,3\,4), (3\,2\,1\,4), (4\ 2\ 3\ 1)\}$.

De partitiematrix van $\vartheta = (2\ 1\ 4\ 3)$ met $\nu_\vartheta = (1\ 2\ 4\ 3)$, is

$$
\begin{aligned}
A &= \begin{bmatrix}
p_1+p_8 & p_3+p_{11} & p_4+p_{12} & p_{13}+p_{21} & p_{14}+p_{22} & p_{17}+p_{24} \\
p_3+p_{14} & p_1+p_{17} & p_2+p_{18} & p_7+p_{23} & p_8+p_{24} & p_{11}+p_{22} \\
p_5+p_{20} & p_2+p_{23} & p_1+p_{24} & p_8+p_{17} & p_7+p_{18} & p_9+p_{16} \\
p_9+p_{16} & p_7+p_{18} & p_8+p_{17} & p_1+p_{24} & p_2+p_{23} & p_5+p_{20} \\
p_{11}+p_{22} & p_8+p_{24} & p_7+p_{23} & p_2+p_{18} & p_1+p_{17} & p_3+p_{14} \\
p_{17}+p_{24} & p_{14}+p_{22} & p_{13}+p_{21} & p_4+p_{12} & p_3+p_{11} & p_1+p_8
\end{bmatrix} \\
B &= \begin{bmatrix}
p_7+p_2 & p_9+p_5 & p_{10}+p_6 & p_{15}+p_{19} & p_{16}+p_{20} & p_{18}+p_{23} \\
p_{13}+p_4 & p_{15}+p_6 & p_{16}+p_5 & p_9+p_{20} & p_{10}+p_{19} & p_{12}+p_{21} \\
p_{19}+p_6 & p_{21}+p_4 & p_{22}+p_3 & p_{11}+p_{14} & p_{12}+p_{13} & p_{10}+p_{15} \\
p_{15}+p_{10} & p_{13}+p_{12} & p_{14}+p_{11} & p_3+p_{22} & p_4+p_{21} & p_6+p_{19} \\
p_{21}+p_{12} & p_{19}+p_{10} & p_{20}+p_9 & p_5+p_{16} & p_6+p_{15} & p_4+p_{13} \\
p_{23}+p_{18} & p_{20}+p_{16} & p_{19}+p_{15} & p_6+p_{10} & p_5+p_9 & p_2+p_7
\end{bmatrix}.
\end{aligned}
$$

De alternatieven: $\{\tilde{\vartheta} = \sigma\vartheta\sigma^{-1},\ \forall\ \sigma\} = \{(2\ 1\ 4\ 3), (3\ 4\ 1\ 2), (4\ 3\ 2\ 1)\}$.

Hoofdstuk 8

Andere schudmodellen: een vergelijking

Samenvatting We vergelijken de variation distance en eigenwaarden van het GSR-model met andere schudmodellen, voor zeer kleine pakken kaarten. Op grond hiervan zien we geen reden het GSR-model te verwerpen als onrealistisch.

8.1 De aannames

Het GSR- of uniforme riffle shufflemodel berust zoals uiteengezet in hoofdstuk 3 op de volgende twee aannames: aanname 3.1, de plaats waar het pak gesneden wordt is binomiaal $(n, \frac{1}{2})$ verdeeld en, aanname 3.2, gegeven de plaats waar het pak is gesneden is elke mogelijke permutatie even waarschijnlijk. De vergelijking met de uitkomsten van een experiment van Diaconis en Reeds (inleiding hoofdstuk 7) gaf twijfels over hoe goed het GSR-model de werkelijkheid beschrijft.

Een ander schudmodel dat beschreven staat in [Epstein, 1977] kent kansen toe aan het vallen van één, twee, drie, ... kaarten tegelijk uit één hand. Dit model is intuïtief logischer, en makkelijker aan te passen aan persoonlijk schudgedrag. Hoewel dit model eerder beschreven was dan het GSR-model, zijn er niet dergelijke resultaten bekend als van het GSR-model.

We willen toch bekijken in hoeverre de aannames van het GSR-model van invloed zijn op de resultaten. Daartoe hebben we voor zeer kleine pakken kaarten de eigenwaarden en variation distance bepaald voor verschillende aannames. We hebben de verdeling van de plaats waar het pak gesneden wordt meer in overeenstemming gebracht met de werkelijkheid; een mens snijdt het pak meer in het midden dan de binomiale verdeling beschrijft. Daarnaast hebben we gebruik gemaakt van de "stapeltjes-beschrijving" van Epstein: we hebben kansen toegekend aan het vallen van één, twee of drie kaarten achter elkaar uit één hand. Hiervoor hebben we de kansen gebruikt uit de tabel van Diaconis.

model	*snijden*	*kans gegeven snijden*
GSR	binomiaal$(n, \frac{1}{2})$	uniform
GSR afgeknot	afgeknot binomiaal $(n, \frac{1}{2}, 1)$	uniform
stapeltjes	binomiaal$(n, \frac{1}{2})$	$p_1 = 0.81,\ p_2 = 0.18,\ p_3 = 0.01$
stapeltjes, afgeknot	afgeknot binomiaal $(n, \frac{1}{2}, 1)$	$p_1 = 0.81,\ p_2 = 0.18,\ p_3 = 0.01$
stapeltjes, zeer afgeknot	afgeknot binomiaal $(n, \frac{1}{2}, 2)$	$p_1 = 0.81,\ p_2 = 0.18,\ p_3 = 0.01$

We verduidelijken de in de tabel gebruikte begrippen. De afgeknot binomiale(n, p, c) verdeling is als volgt gedefinieerd: $K \sim$ afgeknot binomiaal(n, p, c), $B \sim$ binomiaal(n, p):

$$\mathbb{P}(K = i) = \begin{cases} \mathbb{P}(B = i) / \sum_{j=c}^{n-c} \mathbb{P}(B = j) & \text{voor } i = c, c+1, \ldots, n-c \\ 0 & \text{anders.} \end{cases}$$

Gegeven de plaats waar het pak gesneden is, valt als eerste een kaart van een bepaalde hand met kans $\frac{\#\text{kaarten in hand}}{n}$. Met p_k worden de kansen op een stapeltje ter grootte k uit één hand vastgelegd. Wanneer de kaarten uit een hand op zijn, vallen de overige kaarten met kans 1. Zijn er twee kaarten in een hand, en de andere hand is niet leeg, dan vallen deze met voorwaardelijke kansen $\tilde{p}_k = p_k/(p_1 + p_2)$ voor $k = 1, 2$.

Voorbeeld De kans op (1 4 5 2 6 3) is, gegeven het pak is gesneden na kaart 3, $\frac{3}{6} \times p_1 \times p_2 \times \tilde{p}_1 \times 1 \times 1$.

8.2 Overhand shuffle

Om de resultaten van de verschillende modellen beter te kunnen vergelijken, zullen we ook de resultaten van een geheel andere schudmethode bekijken: de *overhand shuffle*.

De overhand shuffle is de in Nederland meer gebruikelijke schudmethode, waarbij de kaarten in één hand worden genomen, en deze in kleine pakketjes naar de andere hand worden overgebracht. De kaarten in een pakketje behouden hun onderlinge volgorde, maar de volgorde van de pakketjes wordt omgekeerd.

De gebruikelijke modellering van deze schudmethode is om een kans p toe te kennen aan de eventualiteit dat na een bepaalde kaart een pakketje eindigt. Een voorbeeld moge dit verduidelijken.

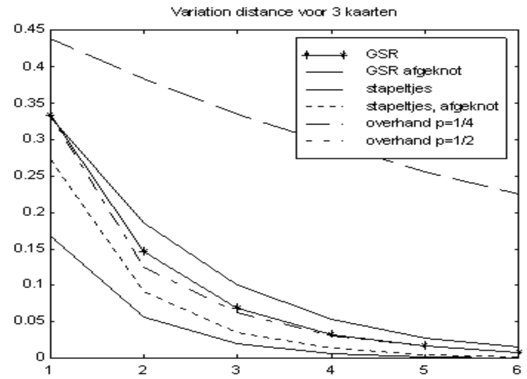
Voorbeeld De kans op de permutatie (5 6 4 2 3 1) is bij de overhand shuffle gelijk aan $p \times q \times p \times p \times q = p^3 q^2$. Immers, de pakketjes zijn [1], $[2, 3]$, [4] en $[5, 6]$.

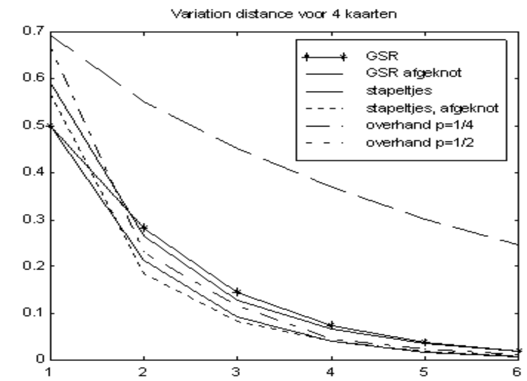
Deze schudmethode is bestudeerd door Pemantle [Pemantle, 1989], die met behulp van een koppeling asymptotische onder- en bovengrenzen op het benodigd aantal keer schudden heeft afgeleid. We zullen deze koppeling niet bespreken, omdat de uitwerking erg specifiek en lang is, en dit niet meer inzicht geeft in het koppelen. De overhand shuffle geeft aanzienlijk slechtere resultaten dan de riffle shuffle: Voor vaste p, moet er tenminste $O(n^2)$ en ten hoogste $O(n^2 \log n)$ keer geschud worden. Omdat de resultaten van de overhand shuffle zo anders zijn dan die van de riffle shuffle, kunnen we hiermee verschillen in de resultaten van verschillende modellen van de riffle shuffle beter interpreteren.

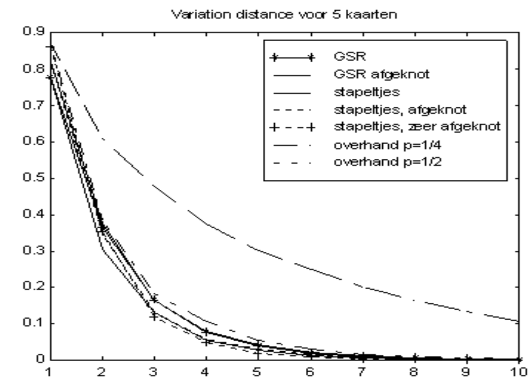
We hebben bij de overhand shuffle voor p de waarden $\frac{1}{4}$ en $\frac{1}{2}$ gebruikt. Voor $p = \frac{1}{2}$ is de kansverdeling uniform op de mogelijke uitkomsten: elke mogelijke permutatie heeft kans $(\frac{1}{2})^{n-1}$. Dit is de verdeling met maximale entropie van alle mogelijke overhand shuffle modellen.

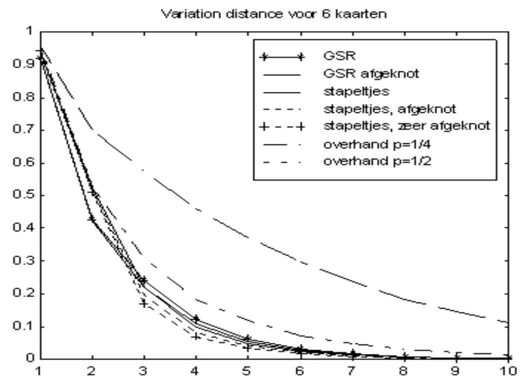
8.3 Resultaten

8.3.1 Variation distance









In alle grafieken wijkt de variation distance voor de andere riffle shuffle modellen, weinig af van die van het GSR-model. We willen ten eerste opmerken dat we heel voorzichtig moeten zijn met het trekken van conclusies, aangezien we slechts resultaten hebben voor zeer weinig kaarten. We kunnen enkel concluderen dat tot 6 kaarten de resultaten van het GSR-model vergelijkbaar zijn met die van meer realistische beschrijvingen.

We maken nog enkele opmerkingen over de verschillende grafieken. Na één keer schudden geven het GSR-model en het afgeknotte GSR-model de beste resultaten. (Het is eenvoudig na te gaan dat deze modellen na één schudbeurt dezelfde variation distance geven). De overige modellen geven slechtere resultaten, het GSR-model heeft immers maximale entropie. Opvallend is echter dat het GSR-model na meerdere schudbeurten niet langer de beste resultaten geeft. Maximum entropie na één schudbeurt garandeert kennelijk niet, dat dit ook de beste resultaten geeft na meerdere schudbeurten.

Als er vaker geschud wordt, geeft het "stapeltjes, zeer afgeknot"-model voor deze waarden van n de beste resultaten. Dit model komt ons inziens het meest overeen met hoe er in werkelijkheid geschud wordt. Dit zou een aanwijzing kunnen zijn, dat het aantal keer schudden dat genoeg is op grond van het GSR-model, ook voldoende zal zijn voor meer realistische modellen.

8.3.2 Eigenwaarden

We geven voor $n = 3$ en $n = 4$ voor de verschillende modellen alle eigenwaarden met multipliciteit. Voor $n = 5$, $n = 6$ en $n = 7$ geven we alleen de drie eigenwaarden met grootste absolute waarde. Voor een volledige lijst van de eigenwaarden voor $n = 5$ en $n = 6$ verwijzen we naar bijlage B. Voor complexe eigenwaarden geldt, dat slechts één per paar gegeven wordt. De gegeven multipliciteit is die van de eigenwaarde plus van de geconjugeerde samen.

Tabel 8.1: $n = 3$, riffle en overhand shuffle

GSR		*GSR afgeknot*		*stapeltjes*		*st, afg*		*ovh, $p = 1/2$*		*ovh, $p = 1/4$*	
ew	mult	ew	mult	ew	mult	ew	mult	ew	mult	ew	mult
1	1	1	1	1	1	1	1	1	1	1	1
0.5	3	0.333	3	0.528	2	0.370	2	0.5	1	0.875	1
0.25	2	0	2	0.182	1	-0.091	1	0.25	2	0.438	2
				0.143	2	-0.143	2	-0.25	2	0.313	2

Tabel 8.2: $n = 4$, riffle shuffle

GSR		*GSR afgeknot*		*stapeltjes*			*st, afg*		
ew	mult	ew	mult	ew	imag	mult	ew	imag	mult
1	1	1	1	1		1	1		1
0.5	6	0.429	6	0.531		3	0.464		3
0.25	11	0.143	11	0.387		3	0.299		3
0.125	6	0	6	0.256		2	0.150		2
				0.113	0.028	6	-0.013	0.032	6
				0.064	0.118	6	-0.069	0.135	6
				0.017		2	-0.123		2
				-0.002		1	-0.145		1

Tabel 8.3: $n = 4$, overhand shuffle

ovh, $p = 1/2$		*ovh, $p = 1/4$*	
ew	mult	ew	mult
1	1	1	1
0.5	2	0.833	3
0.427	3	0.793	2
0.25	5	0.363	2
0.073	3	0.355	3
0	3	0.344	3
-0.073	3	0.285	3
-0.25	1	0.25	3
-0.427	3	0.156	1
		0.152	3

Tabel 8.4: $n = 5$, riffle shuffle, grootste eigenwaarden

GSR		*GSR afgeknot*		*stapeltjes*		*st, afg*		*st, zeer afg*	
ew	mult	ew	mult	ew	mult	ew	mult	ew	mult
1	1	1	1	1	1	1	1	1	1
0.5	10	0.467	10	0.531	4	0.500	4	0.439	4
0.25	35	0.2	35	0.321	6	-0.347	1	-0.364	1

Tabel 8.5: $n = 5$, overhand shuffle, grootste eigenwaarden

ovh, $p = 1/2$		*ovh, $p = 1/4$*	
ew	mult	ew	mult
1	1	1	1
-0.553	4	0.801	6
0.535	5	0.765	5

Tabel 8.6: $n = 6$, riffle shuffle, grootste eigenwaarden

GSR		*GSR afgeknot*		*stapeltjes*		*st, afg*		*st, zeer afg*	
ew	mult	ew	mult	ew	mult	ew	mult	ew	mult
1	1	1	1	1	1	1	1	1	1
0.5	15	0.484	15	0.531	5	0.516	5	0.480	5
0.25	85	0.226	85	0.319	10	0.297	10	0.284	5

Tabel 8.7: $n = 6$, overhand shuffle, grootste eigenwaarden

ovh, $p = 1/2$		*ovh, $p = 1/4$*	
ew	mult	ew	mult
1	1	1	1
-0.646	5	0.779	10
0.577	9	0.749	9

Tabel 8.8: $n = 7$, riffle shuffle en overhand shuffle, grootste eigenwaarden

GSR	*GSR afg*	*stapeltjes*	*st, afg*	*st, zeer afg*	*ovh, $p = 1/2$*	*ovh, $p = 1/4$*
1	1	1	1	1	1	1
0.5	0.492	0.531	0.524	0.501	-0.714	0.765
0.25	0.238	0.344	0.334	0.318	0.620	0.741

Met hetzelfde voorbehoud als eerder, merken we enkele dingen op. De één-na-grootste eigenwaarde is voor alle riffle shuffle modellen ongeveer gelijk aan een half. Ook hier is dus geen reden het GSR-model te verwerpen. Verder blijkt de één-na-grootste eigenwaarde voor het afgeknotte $(n, \frac{1}{2}, 1)$ GSR-model in alle door ons bekeken gevallen, gelijk te zijn aan $\frac{1}{2} - \frac{1}{2^n-2}$. Het is aannemelijk dat dit algemeen het geval is, dus voor iedere waarde van n.

Vermoeden 8.1 *De één-na-grootste eigenwaarde voor het afgeknotte $(n, \frac{1}{2}, 1)$ GSR-model is $\frac{1}{2} - \frac{1}{2^n-2}$.*

De kansverdeling van het afgeknotte GSR-model is:

$$\mathbb{P}(\pi_i \to \pi_j) = \begin{cases} \frac{n-1}{2^n-2} & \text{als } i = j \\ \frac{1}{2^n-2} & \text{als } \pi_i^{-1}\pi_j \text{ uit twee rising sequences bestaat} \\ 0 & \text{anders.} \end{cases} .$$

Voor het gewone GSR-model is dit

$$\mathbb{P}(\pi_i \to \pi_j) = \begin{cases} \frac{n+1}{2^n} & \text{als } i = j \\ \frac{1}{2^n} & \text{als } \pi_i^{-1}\pi_j \text{ uit twee rising sequences bestaat} \\ 0 & \text{anders.} \end{cases}.$$

We zien hier dat dezelfde factor $\frac{1}{2^n-2}$ een rolt speelt. Een precieze verklaring kunnen we echter niet geven.

Het effect op de één-na-grootste eigenwaarde van de “stapeltjes”-aanname lijkt ongeveer constant te zijn voor n. Ook hiervoor moeten wij een verklaring schuldig blijven.

Hoofdstuk 9

Samenvatting en conclusie

We hebben in deze scriptie de vraag hoe vaak er geschud moet worden, onderzocht. Hierop kunnen we geen algemeen geldend antwoord geven.

We zeggen dat er genoeg geschud is als er geen voordeel behaald kan worden, door kennis omtrent het schudden en de beginverdeling van de kaarten, of door de ligging van de kaarten. Het moge duidelijk zijn dat dit sterk afhankelijk is van het spel dat gespeeld wordt. We hebben in deze scriptie een antwoord gezocht, dat onafhankelijk is van het spel.

Daartoe hebben we het begrip *variation distance* gebruikt, $\sum_i \frac{1}{2}|P(i) - Q(i)|$ met P en Q kansverdelingen. Wanneer de kaartvolgorde volgens de uniforme verdeling verdeeld is, is er geen voordeel te behalen. We vergelijken daarom met de variation distance de kansverdeling na het schudden met de uniforme verdeling.

Het wiskundig model voor het schudden dat we onderzocht hebben is het *GSR*- of *uniforme riffle shuffle-model*. Een riffle shuffle is de "Amerikaanse" manier van schudden, waarbij het pak in twee delen wordt gesplitst, waarna de delen ineengeritst worden. Bij het GSR-model geldt dat, gegeven de plek waar het pak gesneden wordt, alle mogelijke permutaties even waarschijnlijk zijn. De plek waar het pak gesneden wordt, wordt binomiaal verdeeld verondersteld.

Een bovengrens op de variation distance kan worden bepaald met behulp van een *koppeling*; er kan een kansverdeling geconstrueerd worden, voor het moment dat het pak kaarten niet meer van een uniform verdeeld pak te onderscheiden is (de *koppeltijd*). Deze aanpak is in principe mogelijk voor elk schudmodel. De kwaliteit van deze bovengrens is echter onduidelijk. Het is wel mogelijk *asymptotische* boven- en ondergrenzen te geven voor het benodigde aantal keer schudden, met behulp van koppelen. Tenslotte kan de verwachte koppeltijd dienen als een indicatie voor het benodigde aantal keer schudden, maar ook niet meer dan dat.

Bij het GSR-model, is het mogelijk de variation distance expliciet te bepalen, aangezien de kans op een permutatie slechts afhankelijk is van het aantal *rising sequences* waaruit de permutatie bestaat, en het aantal keer dat er geschud is. De variation distance als functie van het aantal keer schudden, blijkt een "cut off" te vertonen; na eerst dichtbij 1 te blijven, neemt de variation distance een duik richting 0. Bayer en Diaconis bestempelen dit (asymptotische gedefinieerde) punt als "genoeg", hoewel de variation distance in dit punt nog redelijk groot kan zijn. Waarom dit belangrijk kan zijn, wordt geïllustreerd met het spelletje New Age Solitaire; de kans op winst voor dit spel bij een GSR-shuffle is gelijk aan de kans op winst bij een uniforme verdeling plus de variation distance.

We kunnen uit bovenstaande methoden geen voorschrift geven, voor het aantal keer dat er geschud moet worden. Op de verwachte koppeltijd en het "cut off"-punt kan niet gegarandeerd worden dat er geen voordeel behaald kan worden door kennis omtrent het schudden van de kaarten. De variation distance geeft slechts een begrenzing aan hoeveel voordeel er behaald kan worden.

Tenslotte hebben we gekeken hoe goed het GSR-model het schudden in de praktijk benaderd. Een vergelijking van de uitkomsten van het GSR-model met enkele resultaten van fysiek schudden, riep twijfels op over de geldigheid van het GSR-model. We hebben daarom de invloed van afwijkingen van de GSR-aannames voor zeer kleine pakken kaarten onderzocht, met behulp van eigenwaarden en variation distance. Omdat de schudmatrix al gauw te groot wordt, hebben we een methode ontwikkeld om kleinere matrices met dezelfde eigenwaarden te krijgen. Bij het ontwikkelen van deze methode, stuitten we op een "nieuwe" eigenschap van de symmetrische groep.
De eigenwaarden en variation distance van andere riffle shuffle-modellen blijken vergelijkbaar met die van het GSR-model. Hoewel de analyse zeer beperkte zeggingskracht heeft, zien wij op grond hiervan in ieder geval geen reden het GSR-model te verwerpen als onrealistisch.

Bijlage A

Resultaten van de partitiemethode

We geven voor de verschillende ϑ's het aantal eigenwaarden van de $6! \times 6!$ matrix die niet worden gevonden met behulp van de partitiematrix.

$n = 6$	stapeltjes		overhand		
$f(\vartheta)$	# gemist	opmerking	# gemist	opmerking	gecorrigeerd
2	1	c	2	a,c	1
4	0		0		0
8	0		1	a	0
10	1	c	2	a,c	1
28	4	c	6	c	6
34	0		1	a	0
128	1	c	2	a,c	1
130	0		1	a	0
148	0		1	a	0
154	5	b,c	6	a,c	5

De in de tabel gemaakte opmerkingen hebben de volgende betekenis: a : een van twee bijna dezelfde eigenwaarden ontbreekt b : één-na-grootste eigenwaarde ontbreekt c : de twee-na-kleinste eigenwaarde ontbreekt

Opmerking a heeft betrekking op het feit dat de $6! \times 6!$ matrix van de overhand shuffle, twee eigenwaarden heeft die slechts in de achtste decimaal verschillen. Dit kan een afrondingsfout zijn. De laatste kolom geeft dan ook de resultaten van de verschillende ϑ's voor de overhand shuffle, gecorrigeerd voor deze eventuele fout.

De één-na-grootste eigenwaarde, is nodig om te bepalen hoe snel de variation distance asymptotisch naar 0 gaat (zie paragraaf 7.2). Het is frappant dat deze alleen ontbreekt bij het riffle shuffle-model voor $f(\vartheta) = 154$. Dit is precies de ϑ van de partitiematrix voor $n = 6$ die in [Doner & Uppuluri, 1970] wordt voorgesteld om de eigenwaarden te bepalen. Voor de verschillende waarden van n die wij hebben geprobeerd, blijkt de methode van Doner en Uppuluri niet de één-na-grootste eigenwaarde te geven.

Overigens is voor $n > 4$ de partitiematrix van Doner en Uppuluri, niet de kleinste. Immers, de periode van een permutatie is het kleinste gemene veelvoud van de cykellengtes. Voor $n = 5$ bijvoorbeeld kan een ϑ geconstrueerd worden met een 2- en een 3-cykel. Deze heeft periode 6, tegenover periode 5 van de $\vartheta = (2\ 3\ 4\ 5\ 1)$ van Doner en Uppuluri. De kleinere partitiematrices blijken wel de één-na-grootste eigenwaarde te geven.

Verder was het opvallend hoe vaak de twee-na-kleinste eigenwaarde voor beide schudmethoden ontbrak.

Bijlage B

Eigenwaarden

Tabel B.1: $n = 5$

gsr		gsr afgeknot		stapeltjes			st+afg		
ew	mult	ew	mult	ew	imag	mult	ew	imag	mult
1	1	1	1	1		1	1		1
0,5	10	0,467	10	0,531		4	0,500		4
0,25	35	0,2	35	0,321		6	0,276		6
0,125	50	0,067	50	0,246	0,051	10	0,196	0,054	10
0,0625	24	0	24	0,243	0,052	10	0,193	0,056	10
				0,227		4	0,175		4
				0,151	0,070	12	0,095	0,075	12
				0,141		5	0,084		5
				0,120	0,038	8	0,062	0,041	8
				0,072		4	0,010		4
				0,052	0,164	12	-0,011	0,175	12
				0,034	0,014	10	-0,030	0,015	10
				0,027	0,127	8	-0,038	0,135	8
				0,011		6	-0,055		6
				-0,056	0,093	10	-0,126	0,099	10
				-0,065		5	-0,136		5
				-0,132		4	-0,208		4
				-0,263		1	-0,347		1

Tabel B.1: Vervolg $n = 5$

st+z afg			ovh $p = 1/2$		ovh $p = 1/4$	
ew	imag	mult	ew	mult	ew	mult
1		1	1	1	1	1
0,439		4	0,535	5	0,801	6
0,257		5	0,418	6	0,765	5
0,244	0,048	10	0,289	4	0,695	1
0,126		4	0,277	5	0,692	5
0,105	0,225	12	0,25	5	0,681	6
0,079		5	0,226	4	0,330	4
0,061		6	0,178	6	0,317	5
0,056		4	0,149	4	0,295	5
0,008	0,056	12	0,125	11	0,290	5
0,006	0,057	8	0,098	5	0,281	4
0,003	0,134	10	0,086	4	0,275	6
-0,018		4	0,0625	6	0,261	5
-0,019	0,069	10	0	6	0,254	4
-0,055		6	-0,013	4	0,232	6
-0,102		4	-0,033	6	0,223	4
-0,169		4	-0,0625	10	0,215	5
-0,236		5	-0,125	6	0,213	4
-0,294		5	-0,134	4	0,203	6
-0,364		1	-0,160	5	0,199	4
			-0,25	5	0,160	5
			-0,299	4	0,140	5
			-0,553	4	0,121	6
					0,107	5
					0,031	4
					0,016	4

Tabel B.2: $n = 6$

gsr		gsr afgeknot		stapeltjes			st+afg		
ew	mult	ew	mult	ew	imag	mult	ew	imag	mult
1	1	1	1	1		1	1		1
0,5	15	0,484	15	0,531		5	0,516		5
0,25	85	0,226	85	0,319		10	0,297		10
0,125	225	0,097	225	0,285		5	0,262		5
0,0625	274	0,032	274	0,246		16	0,221		16
0,03125	120	0	120	0,239		5	0,215		5
				0,238	0,045	18	0,214	0,047	18
				0,227		10	0,202		10
				0,220		10	0,195		10
				0,186	0,083	32	0,160	0,086	32
				0,171		10	0,144		10

Tabel B.2: Vervolg $n = 6$

gsr		gsr afgeknot		stapeltjes			st+afg		
ew	mult	ew	mult	ew	imag	mult	ew	imag	mult
				0,165		16	0,138		16
				0,159	0,072	10	0,131	0,075	10
				0,156	0,054	10	0,129	0,056	10
				0,155		10	0,128		10
				0,155	0,047	18	0,128	0,049	18
				0,125	0,013	18	0,096	0,013	18
				0,120	0,109	20	0,092	0,113	20
				0,117		5	0,088		5
				0,107		10	0,078		10
				0,099		16	0,070		16
				0,087		9	0,057		9
				0,074		5	0,044		5
				0,072	0,091	18	0,042	0,094	18
				0,057	0,083	20	0,027	0,086	20
				0,053	0,180	20	0,023	0,186	20
				0,052	0,074	18	0,021	0,077	18
				0,052	0,069	20	0,021	0,071	20
				0,052		16	0,021		16
				0,042	0,107	32	0,011	0,110	32
				0,042	0,067	32	0,011	0,069	32
				0,016	0,090	10	-0,015	0,093	10
				0,003		9	-0,030		9
				-0,008	0,090	32	-0,041	0,093	32
				-0,010	0,089	20	-0,042	0,091	20
				-0,011	0,165	10	-0,044	0,170	10
				-0,016		10	-0,049		10
				-0,017	0,085	10	-0,050	0,087	10
				-0,026		5	-0,059		5
				-0,042		10	-0,076		10
				-0,044		16	-0,078		16
				-0,049		5	-0,083		5
				-0,058	0,063	18	-0,092	0,065	18
				-0,060		9	-0,095		9
				-0,064		16	-0,098		16
				-0,064		10	-0,098		10
				-0,069	0,022	32	-0,103	0,022	32
				-0,071		5	-0,106		5
				-0,071	0,163	18	-0,106	0,168	18
				-0,072		5	-0,106		5
				-0,105		10	-0,141		10
				-0,130		1	-0,166		1
				-0,140		9	-0,177		9
				-0,156		5	-0,194		5

Tabel B.2: Vervolg $n = 6$

st+z afg			ovh $p = 1/2$		ovh $p = 1/4$	
ew	imag	mult	ew	mult	ew	mult
1		1	1	1	1	1
0,480		5	0,577	9	0,779	10
0,284		5	0,417	10	0,749	9
0,270		9	0,344	5	0,652	5
0,248		5	0,338	9	0,640	16
0,222		10	0,279	5	0,637	5
0,211		16	0,259	10	0,630	16
0,207		5	0,257	9	0,630	10
0,181	0,080	18	0,254	9	0,611	9
0,179		10	0,233	16	0,606	9
0,166		10	0,197	5	0,603	5
0,134	0,070	18	0,186	9	0,594	10
0,114		16	0,185	16	0,566	5
0,103		10	0,177	16	0,563	10
0,098		5	0,160	10	0,290	10
0,091		10	0,156	10	0,289	5
0,086		5	0,147	5	0,284	9
0,080	0,077	32	0,145	5	0,282	9
0,077	0,087	10	0,136	10	0,267	5
0,072	0,175	32	0,132	9	0,260	16
0,062	0,045	20	0,107	16	0,259	5
0,062	0,091	18	0,103	16	0,252	10
0,053		9	0,102	9	0,245	16
0,043	0,011	20	0,102	10	0,241	5
0,040	0,176	10	0,099	10	0,229	16
0,035	0,170	20	0,095	10	0,227	9
0,029		9	0,094	5	0,223	16
0,017	0,200	20	0,082	16	0,223	9
0,011	0,035	32	0,081	5	0,214	5
0,001		9	0,073	10	0,214	10
-0,009		16	0,072	9	0,212	10
-0,011	0,053	10	0,068	16	0,209	10
-0,012		10	0,066	10	0,201	9
-0,025	0,105	32	0,051	10	0,201	16
-0,030	0,085	20	0,034	9	0,200	5
-0,039	0,048	18	0,033	16	0,198	5
-0,053	0,119	20	0,032	5	0,194	16
-0,065	0,154	10	0,031	5	0,192	5
-0,067		5	0,025	10	0,184	9
-0,068	0,099	32	0,022	16	0,179	5
-0,070		16	0,018	9	0,178	10

Tabel B.2: Vervolg $n = 6$

st+z afg			ovh $p = 1/2$		ovh $p = 1/4$	
ew	imag	mult	ew	mult	ew	mult
-0,079		10	0,013	9	0,172	9
-0,090	0,054	18	0,012	10	0,172	16
-0,097	0,019	10	0,004	16	0,172	10
-0,098		9	0,000	5	0,171	10
-0,118		10	-0,010	10	0,166	10
-0,141	0,239	18	-0,020	5	0,162	9
-0,157	0,057	32	-0,031	16	0,161	9
-0,159		5	-0,031	9	0,158	16
-0,186		5	-0,040	10	0,156	9
-0,206		1	-0,040	9	0,155	5
-0,216		9	-0,041	16	0,155	10
-0,225		5	-0,048	10	0,153	10
			-0,052	5	0,152	5
			-0,064	16	0,131	4
			-0,067	9	0,131	1
			-0,075	9	0,128	16
			-0,095	10	0,127	16
			-0,104	5	0,126	9
			-0,106	16	0,124	16
			-0,116	9	0,118	10
			-0,119	5	0,118	5
			-0,127	10	0,116	9
			-0,133	9	0,115	10
			-0,156	5	0,104	9
			-0,159	10	0,097	16
			-0,165	16	0,042	16
			-0,188	6	0,036	9
			-0,193	10	0,030	10
			-0,232	16	0,029	5
			-0,323	10	0,024	9
			-0,331	9	0,016	10
			-0,379	5	0,011	5
			-0,646	5	0,010	16
					-0,057	1
					-0,072	10
					-0,101	5

Bibliografie

[1] David Aldous. Random walks on finite groups and rapidly mixing Markov chains. In *Seminar on probability, XVII*, pages 243–297. Springer, Berlin, 1983.

[2] David Aldous and Persi Diaconis. Shuffling cards and stopping times. *Amer. Math. Monthly*, 93(5):333–348, 1986.

[3] David Aldous and Persi Diaconis. Strong uniform times and finite random walks. *Adv. in Appl. Math.*, 8(1):69–97, 1987.

[4] Dave Bayer and Persi Diaconis. Trailing the dovetail shuffle to its lair. *Ann. Appl. Probab.*, 2(2):294–313, 1992.

[5] A. R. Collar. On centrosymmetric and centroskew matrices. *Quart. J. Mech. Appl. Math.*, 15:265–281, 1962.

[6] Persi Diaconis. *Group representations in probability and statistics*. Institute of Mathematical Statistics, Hayward, CA, 1988.

[7] Persi Diaconis, James Allen Fill, and Jim Pitman. Analysis of top to random shuffles. *Combin. Probab. Comput.*, 1(2):135–155, 1992.

[8] Persi Diaconis, Michael McGrath, and Jim Pitman. Riffle shuffles, cycles, and descents. *Combinatorica*, 15(1):11–29, 1995.

[9] J. R. Doner and V. R. R. Uppuluri. A Markov chain structure for riff shuffling. *SIAM J. Appl. Math.*, 18:191–209, 1970.

[10] Richard A. Epstein. *The theory of gambling and statistical logic*. Academic Press [Harcourt Brace Jovanovich Publishers], New York, revised edition, 1977.

[11] Brad Mann. How many times should you shuffle a deck of cards? *www.dartmouth.edu/˜chance/teaching_aids/books_articles/Mann.pdf*.

[12] Robin Pemantle. Randomization time for the overhand shuffle. *J. Theoret. Probab.*, 2(1):37–49, 1989.

[13] J. W. Pitman. On coupling of Markov chains. *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete*, 35(4):315–322, 1976.

[14] Frans Schalekamp. Simulation of the matching problem of Montmort. *Probab. Engrg. Inform. Sci.*, 12(3):325–328, 1998.

[15] Frans Schalekamp and Anke Van Zuylen. New age solitaire and the variation distance. *Probab. Engrg. Inform. Sci.*, aangeboden ter publicatie.

[16] Frans Schalekamp and Anke Van Zuylen. On the computation of eigenvalues of shuffling matrices by partitioning. *SIAM J. Appl. Math.*, aangeboden ter publicatie.

[17] S. Tanny. A probabilistic interpretation of Eulerian numbers. *Duke Math. J.*, 40:717–722, 1973.