Butlletí de la Societat Catalana de Matemàtiques
Vol. 13, núm. 1, 1998. Pàg. 65–79.

Quants cops cal escartejar? Un problema de probabilitats i teoria de grups*

Frederic Utzet

El problema de què ens ocuparem és molt curt d'enunciar: tenim un joc de cartes i volem saber quants cops cal escartejar-les de manera que quedin *ben remenades*. La resolució, però, serà llarga i tindrà molts ingredients: caldrà definir què vol dir que les *cartes quedin ben remenades*, buscar models de les diferents maneres d'escartejar i, un cop ben traduït tot al llenguatge matemàtic, cercar la manera d'atacar el problema. La resolució, que s'ha obtingut en els darrers deu anys, es pot dur a terme utilitzant tècniques molt diverses: a més del càlcul de probabilitats, es poden utilitzar diferents eines algebraiques o d'anàlisi funcional. He escollit presentar la via original d'atac del genial matemàtic americà Persi Diaconis, que utilitza la teoria de representació de grups, ja que m'ha semblat que és la que millor s'adapta a ser explicada —a grans trets, això sí— en una hora, i que a més utilitza resultats coneguts a partir del segon curs de la carrera de matemàtiques.

1 Plantejament del problema. Què vol dir «ben remenades» i altres definicions

Òbviament abans de començar cal precisar el llenguatge. Per concretar les idees (i no escriure massa) ho pensarem amb tres cartes que, en un joc nou, abans de remenar, estaran en l'ordre $a\ b\ c$, on a és la carta de dalt de tot, b la del mig, i c la de baix.

Després d'escartejar-les, direm que les cartes estan «ben remenades» si hi ha la mateixa probabilitat d'obtenir qualsevol de les 3! ordenacions possibles:

$$abc \quad acb \quad bac \quad bca \quad cab \quad cba$$

En altres paraules, cadascuna d'aquestes ordenacions té probabilitat 1/6. (Es diu que tenim una probabilitat uniforme sobre el conjunt de les ordenacions).

Al contrari, si algú després d'escartejar només obtingués les ordenacions

$$abc \quad acb$$

*Aquest text reprodueix, amb alguns complements, la conferència inaugural del curs 96-97 de la Secció de Matemàtiques de la Universitat Autònoma de Barcelona. Agraeixo molt als professors Agustí Reventós i Joan Josep Carmona la seva confiança; malgrat la feina que em va portar, va ser un honor i una satisfacció fer-la.

cadascuna amb probabilitat 1/2, òbviament les cartes estarien mal barrejades, i ens podrien fer moltes trampes en el joc.

Els professionals de les cartes (jugadors, il·lusionistes, tafurs, etc.) sempre han sabut que la gent acostuma a escartejar malament i quan, per exemple, un il·lusionista dóna a un espectador una baralla de cartes i li diu «remeni ben remenat...», i l'espectador barreja dos o tres cops, l'estructura de les cartes quasi no ha canviat, i el mag en treurà partit. Gardner ([12, cap. 6]) explica diversos jocs amb cartes interessants que exploten aquesta idea; val a dir que alguns d'aquests trucs no surten sempre, però sí que funcionen amb una alta probabilitat. A molts espectacles de màgia hi acostuma a haver trucs que depenen de l'atzar (amb cartes o sense): quan surten bé tenen un enorme èxit, ja que ningú s'explica la trampa; quan no van bé, els màgics tenen preparat un altre final, no tan brillant, però que els permet evitar el ridícul. També els jugadors de cartes ho fan servir: per exemple, en un llibre dels anys 30[1] s'explica com utilitzar que les cartes estan mal escartejades per guanyar al bridge (com a incís, observem que des de finals dels anys 60 s'utilitzen màquines d'escartejar als campionats internacionals de bridge; quan s'escarteja a mà, si es fa un contrast estadístic es rebutja la hipòtesi que les cartes han quedat ben barrejades; quan es fa l'escartejat a màquina, el contrast accepta que han quedat ben remenades).

Tornant al nostre problema, quan hom escarteja un joc de cartes no ho fa un cop, sino que utilitza un procediment iteratiu repentint diferents vegades la mateixa tècnica. Anem ara a pensar diferents mètodes d'escartejar:

1. Un mètode determinista

Posem la 1a. carta al 3r. lloc:

$$abc \quad \overset{\text{1a. remenada}}{\longrightarrow} \quad bca \quad \overset{\text{2a. remenada}}{\longrightarrow} \quad cab \quad \longrightarrow \cdots$$

Per a conèixer el resultat de l'escarteig, només cal saber quants cops s'ha escartejat.

2. Un mètode aleatori

Agafem la 1a. carta i la coloquem a l'atzar. El resultat, ara, ja no serà segur, sinó que es poden obtenir les ordenacions abc, bca o bac, cadascuna amb probabilitat 1/3. Així, el resultat de remenar un cop serà la probabilitat següent:

Ordenació	*abc*	*acb*	*bac*	*bca*	*cab*	*cba*
Probabilitat	1/3	0	1/3	1/3	0	0

Quan tornem a escartejar, caldrà fer un diagrama d'arbre com el de la figura 1 per poder calcular les probabilitats.

Després de cada escarteig tindrem una probabilitat sobre el conjunt

$$\{abc, acb, bac, bca, cab, cba\}.$$

Designarem per P la probabilitat corresponent al primer escarteig, per P^{*2} la del segon, i així successivament. Tindrem:

1 E. Cumbelston, *Contract bridge Red Book on Play*, Winston, Philadelphia, 1930 (citat per Diaconis [5]).

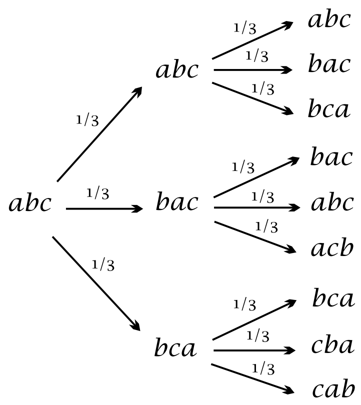

FIGURA 1

Ordenació	*abc*	*acb*	*bac*	*bca*	*cab*	*cba*
P	1/3	0	1/3	1/3	0	0
P^{*2}	2/9	1/9	2/9	2/9	1/9	1/9
P^{*3}	5/27	4/27	5/27	5/27	4/27	4/27
.	.					
.	.					
.	.					

Aquestes probabilitats convergeixen cap a la probabilitat uniforme, que designarem per U:

Ordenació	*abc*	*acb*	*bac*	*bca*	*cab*	*cba*
U	1/6	1/6	1/6	1/6	1/6	1/6

Amb qualsevol sistema *raonable* d'escartejar tindrem que

$$P^{*n} \underset{n\to\infty}{\longrightarrow} U,$$

(en un sentit que definirem més endavant).

La taula de les probabilitats del mètode determinista, per contra, posa de manifest les seves limitacions:

Ordenació	*abc*	*acb*	*bac*	*bca*	*cab*	*cba*
P	0	0	0	1	0	0
P^{*2}	0	0	0	0	1	0
.	.					
.	.					
.	.					

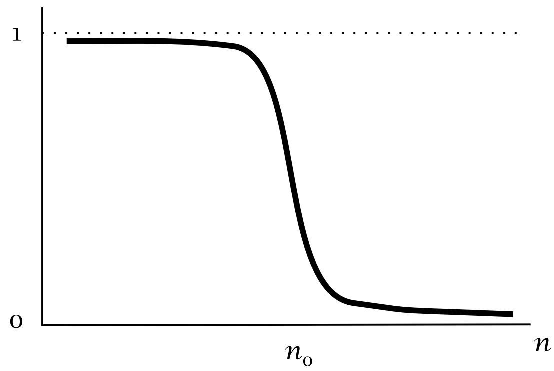

FIGURA 2

i resulta obvi que aquestes probabilitats no poden convergir a la uniforme.

Introduirem a la secció següent uns conceptes que permetran donar rigor a l'estudi. Per començar, definirem una distància $d(P,Q)$ entre dues probabilitats P, Q (que serà un nombre entre 0 i 1), i demostrarem que si el procediment d'escartejar és *raonable* (expressió que definirem), aleshores

$$d(P^{*n}, U) \underset{n\to\infty}{\longrightarrow} 0.$$

Aquest, però, és un resultat **asimptòtic** sense gaire utilitat pràctica, ja que un il·lusionista o un jugador no en tenen prou amb saber que *algun dia* les cartes quedaran ben remenades: volen saber *quants* cops s'ha de remenar. Afinarem l'estudi fins a obtenir la velocitat de convergència de la successió. Però encara més, Persi Diaconis va demostrar que si el procediment d'escartejar és *raonable*, aleshores es produeix el fenomen que reflecteix la figura 2, on $d(n) = d(P^{*n}, U)$.

Així, si $n < n_0$, aleshores $d(n) \simeq 1$ i és com si no haguéssim remenat. Si $n \geq n_0$, aleshores $d(n) \longrightarrow 0$ amb velocitat exponencial. Per tant, a n_0 es presenta un tall realment interessant.

Aquests fenòmens de tall es donen en diferents situacions i tenen molt interés teòric i aplicat (per exemple, els algorismes per ordenar llistes). A part del problema d'escartejar, on hi ha una solució combinatòria directa (Bayer i Diaconis [3]), s'han trobat tres maneres d'estudiar aquests problemes:

- Mètodes probabilístics: utilitzant temps d'atur forts, deguts a Aldous i Diaconis [1].
- Mètodes algebraics: aplicant representació de grups finits, de Diaconis i Shahshahani [8].
- Anàlisi funcional: utilitzant desigualtats de Sobolev logarítmiques, de Diaconis i Saloff-Coste [7, 8].

Com veieu, a tots aquests resultats hi intervé Persi Diaconis, que és un matemàtic a qui agrada especialment combinar les probabilitats amb altres branques de les matemàtiques, com la teoria de nombres, per exemple. Diaconis té una biografia força curiosa (vegeu [4]): nascut l'any 1945, als 14 anys va deixar l'escola i va marxar de casa per seguir un il·lusionista de carrer. Cap als vint anys, intrigat pels jocs de mans on intervé l'atzar, va voler estudiar una mica de probabilitat, i un amic li va recomanar l'excel·lent llibre de Feller [10]. Com era d'esperar, no va entendre res; però en lloc d'anar plorant a demanar en Feller un camí màgic a la teoria de la probabilitat, Diaconis es va matricular a l'escola per estudiar matemàtiques: tenia 24 anys. Ha fet una carrera científica fulgurant, escrivint llibres i articles d'un gran nivell matemàtic i d'una extraordinària creativitat i originalitat. Als 37 anys li va ser concedit el premi de la Fundació MacArthur, el *premi als genis* (el sou de professor durant 5 anys sense fer cap classe) que s'atorga anualment a una persona entre tots els camps de la ciència i la tècnica. Actualment és professor a la Universitat de Harvard.

2 Probabilitats sobre el grup simètric

Una millor manera de representar la barreja de k cartes seria utilitzar el grup de les permutacions de k elements, S_k (*grup simètric*); d'aquesta manera ens fixarem en *l'acció* d'escartejar, i no tant en el resultat que obtenim. Cada permutació serà una possible barreja; així, amb les tres cartes, l'escarteig de passar la carta de dalt de tot a baix el representarem per

$$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

on l'aplicació $i \mapsto \pi(i)$ indica que la carta en la posició i abans de remenar passa a la posició $\pi(i)$ després de fer-ho. Notem que la segona fila **no** dóna la nova ordenació. Insistim que la permutació es refereix a *l'acció* de remenar, mentre que l'ordenació és el resultat de remenar, que dependrà de l'ordre inicial. A l'inrevés, a qualsevol possible forma de remenar li correspon una (i només una) permutació.

Considerem ara una altra remenada, per exemple la que canvia la primera carta per la tercera, que correspon a la permutació

$$\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

La barreja que consisteix a aplicar primer π i després τ és, precisament, la permutació producte, $\tau \circ \pi$, multiplicades, com és habitual, de dreta a esquerra:

$$\tau \circ \pi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

A partir d'ara escriurem les permutacions sense la fila de dalt; així, posarem només $\pi = (\pi(1)\pi(2)\cdots\pi(k))$.

Amb aquestes notacions, cada forma d'escartejar assignarà una probabilitat als element del grup S_k. Així, l'escartejat que consisteix a posar la primera carta a l'atzar serà ara la probabilitat

Permutació	(123)	(132)	(213)	(231)	(312)	(321)
Probabilitat	1/3	0	1/3	1/3	0	0

Considerem un determinat mètode d'escartejar donat per una probabilitat P sobre S_k. Aplicar-lo dues vegades vol dir primer escollir a l'atzar (segons P) una permutació (posem π), ordenar les cartes d'acord amb aquesta permutació, escollir una segona permutació (posem τ) i tornar a ordenar les cartes; per tant, el resultat final correspon al fet d'haver aplicat una permutació $\tau \circ \pi$ a l'ordenació inicial de les cartes. Tota aquesta operació defineix una probabilitat, que designarem P^{*2}, sobre S_k. Per calcular aquesta probabilitat notem que les dues eleccions son independents, i que amb P^{*2} elegirem una determinada permutació σ a través d'elegir qualsevol permutacions π i τ tals que

$$\sigma = \tau \circ \pi.$$

Llavors,

$$P^{*2}(\sigma) = \sum_{\tau \circ \pi = \sigma} P(\pi) P(\tau) = \sum_{\pi \in S_3} P(\pi) P(\sigma \circ \pi^{-1}).$$

Evidentment aquest procediment és equivalent al diagrama d'arbre que hem utilitzat anteriorment.

Iterant el procés podrem calcular P^{*n}

3 Probabilitats sobre grups finits

Estendrem les idees anteriors a una probabilitat sobre un grup. Sigui G un grup finit; una probabilitat sobre G és una aplicació

$$P : G \longrightarrow [0,1]$$

tal que

$$\sum_{s \in G} P(s) = 1.$$

La probabilitat d'un subconjunt de G es calcula per

$$P(A) = \sum_{s \in A} P(s), \; A \subset G.$$

S'anomena probabilitat **uniforme** sobre G la probabilitat que dóna la mateixa massa a tots els elements de G:

$$U(s) = \frac{1}{\mathrm{Card(G)}}, \quad \forall s \in G.$$

Donades dues probabilitats P i Q sobre G, es defineix el seu producte de convolució per

$$Q * P(s) = \sum_{t \in G} P(t) Q(s\,t^{-1}).$$

També, per a dues probabilitats, la distància de la **variació** es defineix per

$$\begin{aligned} d(P,Q) &= \max_{A \subset G} |P(A) - Q(A)| \\ &= \frac{1}{2} \sum_{s \in G} |P(s) - Q(s)|. \end{aligned}$$

El següent teorema tanca la primera etapa del nostre recorregut:

1 Teorema *(Perron–Frobenius) Si P no està concentrada en una classe lateral d'un subgrup, aleshores*

$$\lim_n d(P^{*n}, U) = 0.$$

Comentaris:

1. I. Csiszar, *Informationstheoretishe Konvergenzbegriffe,* Im Raum der Wahrscheinlichkeits-Verteilingen, Pub. Math. Inst., Hungarian Acad. Sciences VII, 137–158, 1962 (referència citada per Diaconis [5]) explica «el perquè de tot plegat»: A l'anar fent convolucions, l'entropia augmenta; el màxim d'entropia s'assoleix amb la probabilitat uniforme.
2. Un mètode d'escartejar serà *raonable* si la probabilitat corresponent compleix la hipòtesi del teorema. La probabilitat de l'escartejat determinista està concentrada en $\{(312)\}$, que és una classe lateral de S_3.

4 Càlculs explícits per a una passejada aleatòria sobre la circumferència

Veurem ara un exemple on la distància $d(P^{*n}, U)$ pot ser calculada amb una molt bona aproximació. Pensem en Z_p com p punts sobre una circumferència. Imaginem una partícula inicialment en el zero i que cada segon es mou a dreta o esquerra amb probabilitat $1/2$. Equivalentment, tenim una probabilitat P sobre el grup Z_p definida per

$$P(1) = P(p-1) = 1/2.$$

Després de dues passes tindrem una probabilitat P^{*2}, i així successivament.

Per tal d'estudiar el comportament asimptòtic de P^{*n} utilitzarem una tècnica habitual en matemàtiques, que consisteix a canviar els nostres objectes (en aquest cas, probabilitats sobre Z_p) per uns d'equivalents però amb més bones propietats respecte a l'operació o la característica que ens interessa (en aquest cas, la convolució). Concretament, utilitzarem la transformada de Fourier, que en la situació que ens ocupa s'anomena (a matemàtica aplicada) *trasformada discreta de Fourier.*

Donada una probabilitat Q sobre Z_p, o, més generalment, un vector de dimensió p, $Q = (Q(0), \dots, Q(p-1))$, li associem un vector complex

$$\hat{Q} = (\hat{Q}(0), \dots, \hat{Q}(p-1))$$

definit per

$$\hat{Q}(j) = \sum_{k=0}^{p-1} e^{2\pi ijk/p} Q(k),$$

que s'anomena *transformada de Fourier* de Q. Aquest vector $\hat{Q}$ té les següents propietats:

- Fórmula d'inversió de Fourier:

$$Q(j) = \frac{1}{p} \sum_{k=0}^{p-1} e^{-2\pi ijk/p} \hat{Q}(k),$$

és a dir, la transformada de Fourier $\hat{Q}$ determina Q.

- Trivialització de la convolució: la transformada de Fourier canvia el producte de convolució per un producte ordinari.

$$\widehat{Q * R}\,(j) = \hat{Q}(j)\hat{R}(j).$$

En particular,

$$\widehat{Q^{*n}}(j) = \big(\hat{Q}(j)\big)^n.$$

Aquesta darrera propietat ens serà especialment important per a calcular el valor de $d(P^{*n}, U)$, ja que el càlcul directe de P^{*n} és molt enfarfegat, mentre que el de $\big(\hat{Q}\big)^n$ és molt senzill. Utilitzar la transformada de Fourier és com «calçar-se les botes de set llegües».

- Fórmula de Plancharel, que estableix la conservació del producte escalar:

$$\sum_j Q(j)R(j) = \frac{1}{p}\sum_k \hat{Q}(k)\hat{R}(k).$$

Tornem a la passejada aleatòria sobre Z_p: recordem que teníem la probabilitat definida per

$$P(1) = P(p-1) = 1/2.$$

Aleshores

$$\hat{P}(j) = \cos\left(\frac{2\pi j}{p}\right),\ j = 0, \ldots, p-1.$$

La probabilitat uniforme sobre Z_p,

$$U(j) = \frac{1}{p},\ \ \forall j \in Z_p,$$

té una transformada de Fourier molt senzilla, ja que la suma de les p arrels p-èsimes de la unitat és zero:

$$\hat{U}(j) = \frac{1}{p}\sum_{k=0}^{p-1} \mathrm{e}^{2\pi i jk/p} = \begin{cases} 1, & j = 0, \\ 0, & j = 1, \ldots, p-1 \end{cases}.$$

Llavors, per a $j = 0$

$$\widehat{P^{*n}}(0) = \Big(\cos\big(\frac{2\pi 0}{p}\big)\Big)^n = 1 \underset{n\to\infty}{\longrightarrow} 1 = \hat{U}(0),$$

i per a $j \neq 0$,

$$\widehat{P^{*n}}(j) = \Big(\cos\big(\frac{2\pi j}{p}\big)\Big)^n \underset{n\to\infty}{\longrightarrow} 0 = \hat{U}(j),$$

d'on és ben evident que

$$\lim_n d(P^{*n}, U) = 0.$$

Però anem a afinar més els càlculs per tal d'establir la velocitat de convergència:

$$\begin{aligned}
d(P^{*n}, U)^2 &= \frac{1}{4}\Big(\sum_{j=0}^{p-1} |P^{*n}(j) - U(j)|\Big)^2 \\
&\leq \frac{1}{4} p \sum_{j=0}^{p-1} \big(P^{*n}(j) - U(j)\big)^2 \qquad \text{(Cauchy – Schwarz)} \\
&= \frac{1}{4} \sum_{j=0}^{p-1} \big(\widehat{P^{*n}}(j) - \hat{U}(j)\big)^2 \qquad \text{(Plancharel)} \\
&\leq \frac{1}{4} \sum_{j=1}^{p-1} \big(\hat{P}(j)\big)^{2n} = \frac{1}{4} \sum_{j=1}^{p-1} \Big(\cos\big(\frac{2\pi j}{p}\big)\Big)^n .
\end{aligned}$$

Ara s'utilitza la desigualtat

$$\cos x \leq e^{-x^2/2}, \; x \in [0, \pi/2],$$

i treballant una mica s'arriba al següent teorema:

2 Teorema *Sigui p imparell, $p \geq 7$. Per a qualsevol $n \geq p^2$,*

$$d(P^{*n}, U) \leq e^{-\alpha n/p^2},$$

i per a qualsevol n,

$$d(P^{*n}, U) \geq \frac{1}{2} e^{-\alpha n/p^2 - \beta n/p^4},$$

on $\alpha = \pi^2/2$ i $\beta = \pi^4/11$.

Amb aquest teorema a la mà, podem afirmar que calen p^2 passos per quedar pròxims a la probabilitat uniforme.

5 El cas general: representacions d'un grup finit

La generalització de l'anàlisi de Fourier utilitza la representació d'un grup finit. Sigui, doncs, G un grup finit. Una **representació** de G és un homomorfisme $\rho : G \to GL(V)$, on V és un espai vectorial de dimensió finita sobre el cos dels nombres complexos i $GL(V)$ és el grup de les aplicacions lineals bijectives de V en V. La dimensió de V s'anomena **dimensió** de la representació.

També és fonamental la noció de representació irreductible, que ens proporciona els elements bàsics amb què es construeixen totes les representacions. Direm que una representació ρ és **irreductible** si no existeix cap subespai W de V no trivial tal que $\rho(s)(W) \subset W$, $\forall s \in G$.

Sigui ara Q una probabilitat (o una funció) sobre G. La **transformada de Fourier** de Q associada a la representació ρ és la matriu

$$\hat{Q}(\rho) = \sum_{s \in G} Q(s)\rho(s).$$

Les propietats fonamentals de la transformada discreta de Fourier són també certes en aquesta situació general:

- *Fórmula d'inversió de Fourier*: la família $\{\hat{Q}(\rho)\}$, on ρ recorre les representacions irreductibles de G, caracteritza Q:

$$Q(s) = \frac{1}{|G|} \sum_{\rho \text{ irred.}} \dim(\rho) \operatorname{Tr}\big(\rho(s^{-1})\hat{Q}(\rho)\big).$$

- Trivialització de la convolució:

$$\widehat{Q * R}(\rho) = \hat{Q}(\rho)\hat{R}(\rho).$$

- *Fórmula de Plancherel:*

$$\sum_{s\in G} Q(s^{-1})R(s) = \frac{1}{|G|} \sum \dim(\rho) \operatorname{Tr}\big(\hat{Q}(\rho)\hat{R}(\rho)\big).$$

Comentari:
En el cas $G = Z_p$, hi ha p representacions irreductible, $\rho_1, \dots, \rho_p$, i totes tenen dimensió 1,

$$\begin{aligned} \rho_j :\ Z_p &\longrightarrow GL(C) \\ k &\mapsto \rho_j(k) : C \to C \\ &\qquad\qquad z \mapsto z \exp\{2\pi i jk/p\} \end{aligned}$$

d'on resulta la identificació amb la transformada discreta de Fourier que hem utilitzat abans.

A continuació veurem dos exemples on s'aplica tot això:

5.1 Transposicions aleatòries

Tenim k cartes en fila. La mà dreta toca una carta, l'esquerra una altra (poden coincidir) i les intercanviem. Aquesta manera de remenar s'anomena *transposicions aleatòries*. Quantes transposicions aleatòries calen per aproximar-nos a la uniforme? Per estudiar-ho, notem que ara tenim la probabilitat sobre S_k:

$$\begin{aligned} P(id) &= \frac{1}{k}, \\ P(\tau) &= \frac{2}{k^2} \quad (\tau \text{ transposició}). \end{aligned}$$

De forma anàloga al cas de la transformada discreta de Fourier es demostra que

$$d(P^{*n}, U)^2 \le \frac{1}{4} \sum_{\rho \text{ irred.}} \dim(\rho)^2 \operatorname{Tr}\Big(\big(\hat{P}^{*n}(\rho) - U(\rho)\big)^2\Big).$$

L'expresió de l'esquerra és tractable, ja que:

- Sobre la representació trivial, $\tau(\sigma) = 1$, $\forall \sigma \in S_k$, tenim que

  $$\widehat{P^{*n}}(\tau) = \hat{U}(\tau) = 1,$$

  i per a qualsevol representació irreductible no trivial

  $$U(\rho) = 0.$$

- D'altra banda, com que la funció P és constant sobre les classes de conjugació:

$$P(\sigma\pi\sigma^{-1}) = P(\pi), \ \forall\sigma, \pi \in S_k,$$

i pel lema de Schur, per a tota representació irreductible ρ,

$$\widehat{P}(\rho) = C(\rho, P)I,$$

on $C(\rho, P)$ depèn del caràcter i de la dimensió de ρ (i de P).

Treballant amb tots aquests ingredients, es demostra el següent:

3 Teorema *Suposem $k \geq 10$. Sigui*

$$c_n = \frac{n - \frac{1}{2}k\ln k}{k}.$$

Llavors:
(1) Si $c_n > 0$ (és a dir, $n > \frac{1}{2}k\ln k$), es té $d(P^{*n}, U) \leq be^{-2c_n}$.
(2) Si $c_n < 0$, aleshores $d(P^{*n}, U) \geq 2(\frac{1}{e} - e^{e^{-2c_n}})$.

En particular, per a un joc de cartes ordinari, $k = 52$, el punt de tall és

$$\frac{1}{2}k\ln k = 102.7.$$

5.2 La biblioteca desordenada

S'han introduït nombrosos models matemàtics per tal d'estudiar el desordre en una biblioteca generat pels lectors. Analitzarem el següent model: tenim k libres

$$1\ 2\ \cdots\ k$$

Un lector agafa el libre 1. Quan l'està llegint, un segon lector agafa un llibre a l'atzar i mentres l'està llegint, el primer lector torna el seu libre, escollint a l'atzar entre els dos forats que hi ha. Al cap d'una estona els llibres estan ben desordenats. La probabilitat que tenim a S_k és

$$\begin{aligned} P(id) &= \frac{1}{k} \\ P(1\,j) &= \frac{1}{k}, \ j = 2, \ldots, k \end{aligned}$$

on $(1\,j)$ és la transposició que canvia el llibre 1 pel j.

Una anàlisi semblant a la que hem fet abans porta al punt de tall $n_0 = k\ln k$. Per n=100 llibres, s'obté 460.

6 Finalment, quants cops cal escartejar?

La manera més habitual d'escartejar és l'anomenat escartejat *americà* (els americans l'anomenen *riffle shuffling* degut al soroll [*riffl*] que es produeix en fer-lo), que consisteix separar en dues parts més o menys iguals el joc de cartes i a prendre'n una en cada mà, intercalant després les cartes d'una part amb les de l'altre, *riffl...* (vegeu la Figura 3). És interessant comentar que si l'escartejat es fa perfectament, és a dir, es separen les cartes en dues parts iguals, i s'intercala exactament una de la dreta amb una de l'esquerra, tenim un escartejat determinista; amb 52 cartes, al cap de 8 vegades s'ha retornat a l'ordre inicial (es pot fer un petit programa per a comprobar-ho, o bé es pot buscar l'ordre de la permutació corresponent; vegeu també Gardner [11, cap. 10]). Persi Diaconis explica que els il·lusionistes saben fer aquest escarteig perfecte i ell sabia fer-lo. Fa uns anys, fins i tot, al principi de les conferències feia una demostració de les seves habilitats, però es veu que el públic es quedava tan impressionat que deien: «no pot ser que algú que sap escartejar tan bé sigui capaç de fer bones matemàtiques»; l'ambient es posava tant negatiu que Diaconis va deixar de fer de mag i matemàtic alhora. En resum, l'escartejat americà demana una mica de traça però no massa.

Un model de l'escartejat americà és el següent: considerem un joc amb k cartes, que separarem en dos pilons

$$k \text{ cartes} \quad \begin{cases} \ell & \text{a la mà esquerra,} \\ k-\ell & \text{a la mà dreta,} \end{cases}$$

on el nombre ℓ l'hem elegit de forma aleatòria segons una llei binomial de paràmetres k i $1/2$, és a dir

$$P\{\ell \text{ cartes a l'esquerra}\} = \binom{k}{\ell}\frac{1}{2^k} \quad \ell = 0, \dots, k.$$

Les cartes cauen de l'esquerra o de la dreta proporcionalment al gruix: la primera cau de l'esquerra amb probabilitat ℓ/k i de la dreta amb probabilitat $(k-\ell)/k$.

Després, si tenim a cartes a l'esquerra i b a la dreta, cau carta de l'esquerra amb probabilitat $a/(a+b)$ i de la dreta amb probabilitat $b/(a+b)$.

Un altre model que ens proporciona la mateixa probabilitat sobre S_k és el següent: s'escriu al dors de cada carta un 0 o 1 d'acord amb el resultat d'una tirada de moneda. Totes les cartes amb zero es separen i es posen a sobre de tot.

Diaconis va estar treballant molt amb aquest model, utilitzant distintes tècniques (les bones propietats que tenien les probabilitats anteriors sobre S_k ara no es complien, i l'anàlisi és molt més difícil). Va arribar a desigualtat molt fines, obtingudes amb molt d'esforç i de talent. Finalment, va aconseguir una fórmula per a calcular la distància exacta a la distribució uniforme:

$$d(n) = d(P^{*n}, U) = \frac{1}{2}\sum_{j=1}^{k} A_{k,j}\left|\binom{2^n+k-j}{k}2^{-nk} - \frac{1}{k!}\right|,$$

on $A_{k,j}$ són els nombres d'Euler. Amb aquesta fórmula es poden calcular els valors (per a $k = 52$ cartes) següents :

n	1	2	3	4	5	6	7	8	9	10
$d(n)$	1,000	1,000	1,000	1,000	0,924	0,624	0,312	0,161	0,083	0,041

Notem que la distància és molt propera a 1 fins a 5 remenades i llavors tendeix molt ràpidament a zero, cada vegada decreix per un factor 1/2; per a $n = 10$, ja és

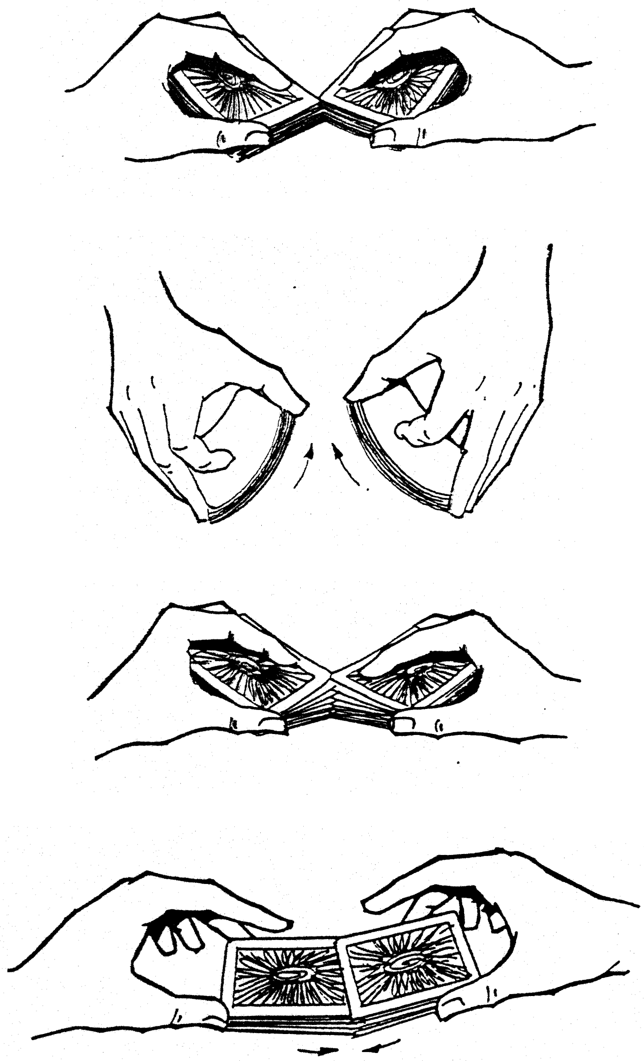

Figura 3

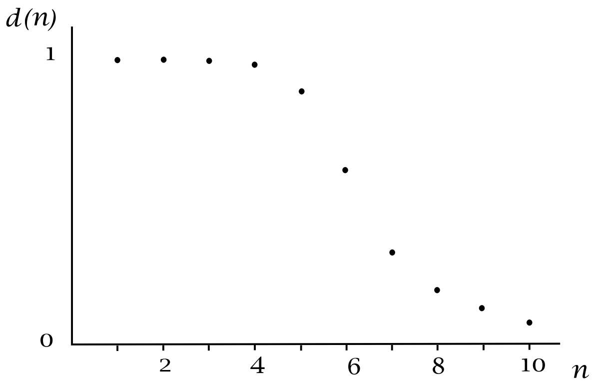

FIGURA 4

pràcticament 0. D'aquí la conclusió que *amb 52 cartes, n'hi ha prou amb 7 remenades.* (Vegeu la figura 4)

Una demostració completa d'aquesta fórmula, llarga però utilitzant només combinatòria, es pot consultar a l'excel·lent article de Mann [13] (que porta el mateix títol que el present treball i que, dissortadament, jo no coneixia en el moment de fer la conferència).

Diaconis també va demostrar el resultat general:

4 TEOREMA *Sigui* $n = \frac{3}{2}\log_2 k + \theta$. *Aleshores*

$$d(P^{*n}, U) = 1 - 2F(-2^{-\theta}/4\sqrt{3}) + O(1/k^{1/4}),$$

on F és la funció de distribució d'una llei normal estàndard.

Referències

[1] ALDOUS, D., DIACONIS, P. «Suffling cards and stopping times», *Amer. Math. Mon.*, **93**, 155–177, 1986.

[2] ALDOUS, D., DIACONIS, P. «Strong Uniform Times and Finite Random Walks», *Adv. Appl. Math.*, **8**, 69–97, 1987.

[3] BAYER, D., DIACONIS, P. «Trailing the Dovetail Shuffle to its Lair», *Ann. App. Prob.*, **2**, 294–313, 1992.

[4] DEGROOT, M. «A conversation with Persi Diaconis», *Statistical Sciences*, **1** 319–334, 1186

[5] DIACONIS, P. *Group Representations in Probability and Statistics*, Hayward, California, IMS, 1988.

[6] DIACONIS, P. «The cutoff phenomenon in finite Markov chains», *Proc. Natl. Acad. Sc. USA*, **93**, 1659–1664, 1996.

[7] DIACONIS, P., SALOFF-COSTE, L. «Comparation theorems for reversible Markov chains», *Ann. Appl. Prob.*, **3**, 696–730, 1993.

[8] DIACONIS, P., SALOFF-COSTE, L., «Logarithmic Sobolev inequalities and finite Markov chains», *Ann. Appl. Prob.*, **6**, 695–750, 1996.

[9] DIACONIS, P., SHAHSHAHANI, M. «Generating Random Permutation with random Transposition», *Z. Wahrsch. Verw. Geb.*, **57**, 159–179, 1981.

[10] FELLER, W. *Una introducción a la teoria de probabilidades y sus aplicaciones*, vol. 1, Limusa, México, 1973.

[11] GARDNER, M., *Carnaval matemático*, Alianza Editorial, Madrid, 1980.

[12] GARDNER, M., *Festival mágico-matemático*, Alianza Editorial, Madrid, 1984.

[13] MANN, B. «How many times should you shuffle a deck of cards», *Topics in Contemporary Probability and its Applications*, 261–289, J. Snell edit., CRC Press, Boca Raton. 1995.

DEPARTAMENT DE MATEMÀTIQUES
UNIVERSITAT AUTÒNOMA DE BARCELONA
08193 BELLATERRA
utzet@mat.uab.es