COMBINATORICS AND CARD SHUFFLING

Sami Assaf
University of Southern California

in collaboration with

Persi Diaconis
Stanford University

K. Soundararajan
Stanford University

University of Cape Town
11 May 2012

Question:

How many times must an iterative procedure be carried out?

-riffle shuffles of a deck of cards

-random walk on a finite group

Answer:

It depends.

- what are the important properties?
- how to measure randomness?
- how good is good enough?

Gilbert–Shannon–Reeds model

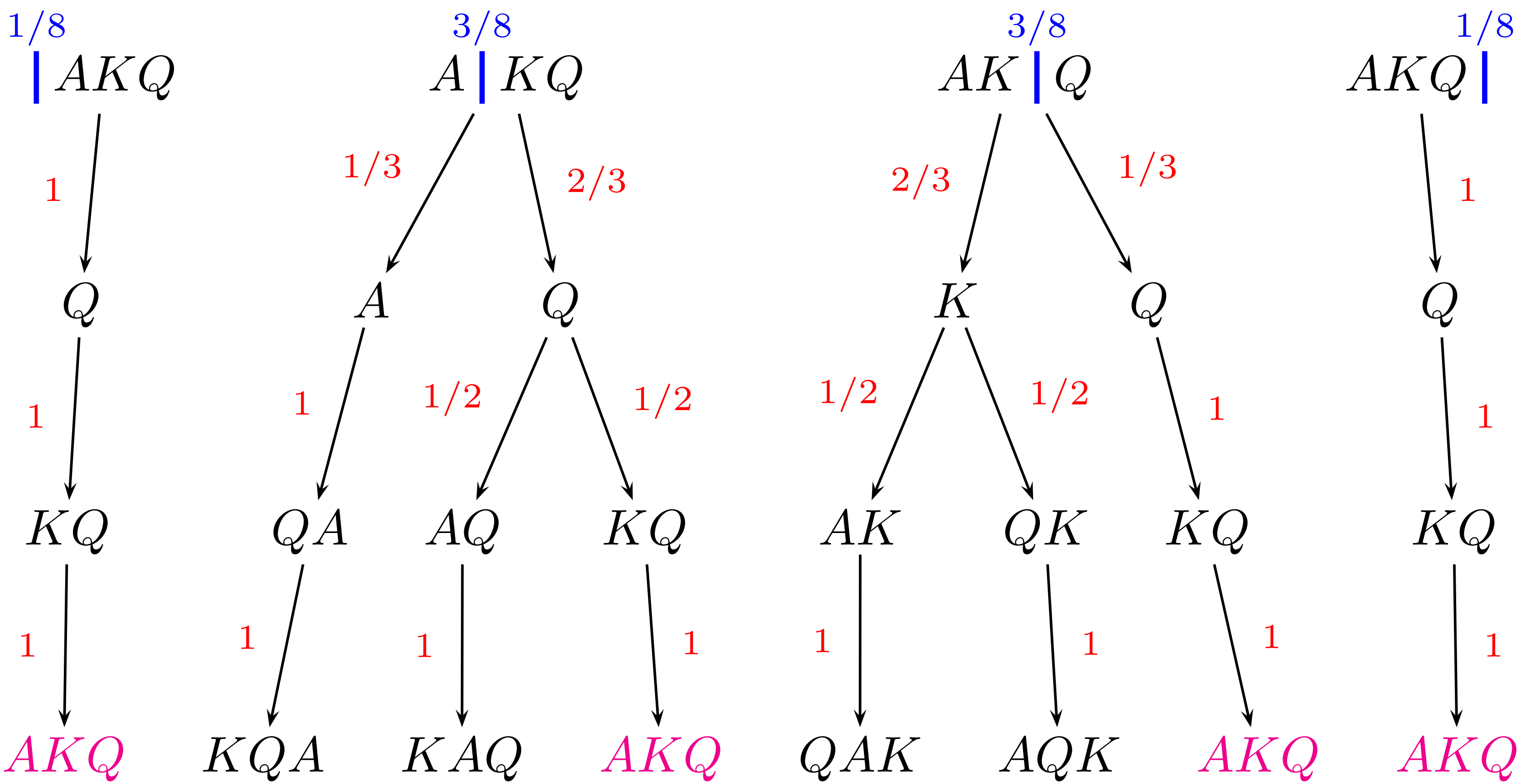
Deck of n cards, e.g. $\{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\} \times \{2, 3, 4, 5, 6, 7, 8, 9, \mathrm{T}, \mathrm{J}, \mathrm{Q}, \mathrm{K}, \mathrm{A}\}$

CUT with binomial probability

$$P(\text{cut } c \text{ cards deep}) = \frac{1}{2^n}\binom{n}{c}$$

DROP proportional to size

$$P(\text{drop from } L) = \frac{\#L}{\#L + \#R}$$



Distribution after a single shuffle

Let $Q_2(\sigma)$ be chance that σ results from a riffle shuffle of the deck.
Let U be the uniform distribution, e.g. $U(\sigma) = \frac{1}{52!}$ for a standard deck.

σ	AKQ	AQK	QAK	KQA	KAQ	QKA
$Q_2(\sigma)$	$1/2$	$1/8$	$1/8$	$1/8$	$1/8$	0
$U(\sigma)$	$1/6$	$1/6$	$1/6$	$1/6$	$1/6$	$1/6$

There are several notions of the distance between Q_2 and U:

$$\|Q_2 - U\|_{TV} = \frac{1}{2}\sum_{\sigma \in \mathcal{S}_n} |Q_2(\sigma) - U(\sigma)| = \frac{1}{2}\left(\frac{1}{3} + 4\frac{1}{24} + \frac{1}{6}\right) = \frac{1}{3}$$

$$\mathrm{SEP} = \max_{\sigma \in \mathcal{S}_n} 1 - \frac{Q_2(\sigma)}{U(\sigma)} = \max\{-2, \tfrac{1}{4}, 1\} = 1$$

Separation bounds total variation: $0 \leq \mathbf{\|Q_2 - U\|_{TV}} \leq \mathrm{SEP}(\mathbf{k}) \leq 1$

Repeated shuffles are defined by convolution powers

$$Q_2^{*k}(\sigma) = \sum_{\tau} Q_2(\tau) Q_2^{*(k-1)}(\sigma\tau^{-1})$$

For Q_2^{*2}, for each of the $n!$ configurations, compute 2^n possibilities.

An a-shuffle is where the deck is cut into a packets with multinomial distribution and cards are dropped proportional to packet size.

CUT with probability

$$\frac{1}{a^n}\binom{n}{c_1, c_2, \ldots, c_a}$$

DROP proportional to size

$$\frac{{}^{\#}H_i}{{}^{\#}H_1 + {}^{\#}H_2 + \ldots + {}^{\#}H_a}$$

Let $Q_a(\sigma)$ be chance that σ results from an a-shuffle of the deck.

Theorem(Bayer–Diaconis) For any a, b, we have $Q_a * Q_b = Q_{ab}$

How many shuffles is enough?

Theorem (Bayer–Diaconis) Let r be the number of rising sequences.

$$\mathbf{Q_a}(\sigma) = \frac{\mathbf{1}}{\mathbf{a^n}}\binom{\mathbf{n}+\mathbf{a}-\mathbf{r}}{\mathbf{n}}$$

Proof: Given a cut, each σ that can result is equally likely, so we just need to count the number of cuts that can result in σ.

Classical stars (★) and bars (|) with n ★'s and $a-1$ | 's of which $r-1$ are fixed. So $n+a-r$ spots and choose n spots for the ★'s. $\square$

★ ★ ★ | ★ ★ ★ ★ | ★ ★

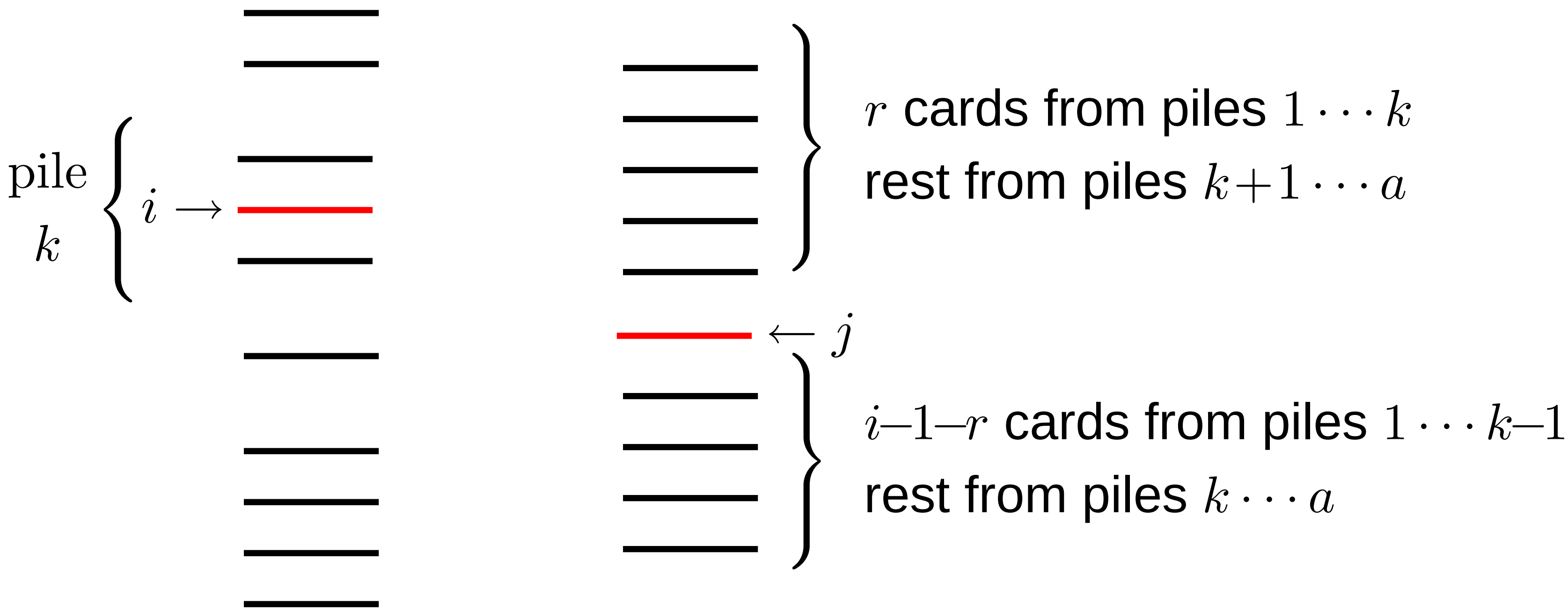
	1	2	3	4	5	6	7	8	9	10	11	12
TV	1.00	1.00	1.00	1.00	.924	.614	.334	.167	.085	.044	.021	.010
SEP	1.00	1.00	1.00	1.00	1.00	1.00	1.00	.996	.931	.732	.479	.278

Following a single card

Theorem (A-D-S) Let $P_a(i,j)$ be the chance that the card at position i moved to position j after an a-shuffle. Then $P_a(i,j)$ is given by

$$\frac{1}{a^n}\sum_{k,r}\binom{j-1}{r}\binom{n-j}{i-r-1}k^r(a-k)^{j-1-r}(k-1)^{i-1-r}(a-k+1)^{(n-j)-(i-r-1)}$$

Proof:



$$\frac{1}{6a^2}\begin{pmatrix} (a+1)(2a+1) & 2(a^2-1) & (a-1)(2a-1) \\ 2(a^2-1) & 2(a^2+2) & 2(a^2-1) \\ (a-1)(2a-1) & 2(a^2-1) & (a+1)(2a+1) \end{pmatrix}$$

Proposition. The matrices $P_a(i,j)$ have the following properties:

1. cross-symmetric: $P_a(i,j) = P_a(n-i+1, n-j+1)$
2. multiplicative: $P_a \cdot P_b = P_{ab}$
3. eigenvalues are $1, 1/a, 1/a^2, \ldots, 1/a^{n-1}$
4. right eigen vectors are independent of a:
   $V_m(i) = (i-1)^{i-1}\binom{m-1}{i-1} + (-1)^{n-i+m}\binom{m-1}{n-i}$ for $1/a^m$

	1	2	3	4	5	6	7	8	9	10	11	12
TV	.873	.752	.577	.367	.200	.103	.052	.026	.013	.007	.003	.002
SEP	1.00	1.00	.993	.875	.605	.353	.190	.098	.050	.025	.013	.006

Random walks on Young subgroups

Let G be a finite group with $Q(g) \geq 0$, $\sum Q(g) = 1$ a probability on G.
Random Walk on G: pick elements with probability Q and multiply

$$1_G \ , \ \ g_1 \ , \ \ g_2 g_1 \ , \ \ g_3 g_2 g_1 \ , \ \ \ldots$$

Let $H \leq G$ be a subgroup of G. Set $X = G/H = \{xH\}$.
The quotient walk is a Markov chain on X with transition matrix

$$\mathbf{K(x,y) = Q(yHx^{-1}) = \sum_{h \in H} Q(yhx^{-1})}$$

In particular, $K^l(x,y) = Q^{*l}(yHx^{-1})$.

riffle shuffles	$\Leftrightarrow$	random walk on $\mathcal{S}_n$
one card tracking	$\Leftrightarrow$	quotient walk on $\mathcal{S}_n / \left(\mathcal{S}_{n-1} \times \mathcal{S}_1\right)$
D_1 1's, D_2 2's, …	$\Leftrightarrow$	quotient walk on $\mathcal{S}_n / \left(\mathcal{S}_{D_1} \times \mathcal{S}_{D_2} \times \cdots\right)$

Proposition (Conger–Viswanath, Assaf–Diaconis–Soundararajan) Consider a deck with D_1 1's, D_2 2's, down to D_m m's. The least likely order after an a-shuffle is the reverse order with m's down to 1's.

$$\text{Proof}: \quad 1 \quad 1 \quad 1 \,|\, 2 \quad 2 \,|\, 2 \quad 2 \quad 2 \quad 2 \,|\, 3 \,|\, 4 \quad 4 \quad 4 \,|\, 5 \quad 5 \,|\, 5 \quad 5 \,|\, 6 \quad 6 \,|\, 6$$

Theorem (Assaf–Diaconis–Soundararajan) For a deck with n cards as above, the probability of getting the reverse deck after an a-shuffle is

$$\mathbf{\frac{1}{a^n} \sum_{0=k_0<k_1<\cdots<k_{m-1}<a} (a-k_{m-1})^{D_m} \prod_{j=1}^{m-1} \left((k_j - k_{j-1})^{D_j} - (k_j - k_{j-1} - 1)^{D_j} \right)}$$

$$\text{Proof}: \quad Q_a(w^*) = \sum_{\substack{A_1+\cdots+A_a=n \\ A \text{ refines } D}} \frac{1}{a^n} \binom{n}{A_1, \ldots, A_a} \frac{1}{\binom{n}{D_1, \ldots, D_m}}$$

In particular, we have a closed formula for $\mathrm{SEP}(a)$ for general decks.

	1	2	3	4	5	6	7	8	9	10	11	12
B–D	1.00	1.00	1.00	1.00	1.00	1.00	1.00	.995	.928	.729	.478	.278
A♠	1.00	1.00	.993	.875	.605	.353	.190	.098	.050	.025	.013	.006
■■	.962	.925	.849	.708	.508	.317	.179	.095	.049	.025	.013	.006
♣♦♥♠	1.00	1.00	.997	.976	.884	.683	.447	.260	.140	.073	.037	.019
○ + ≋ □ ☆	1.00	1.00	.993	.943	.778	.536	.321	.177	.093	.048	.024	.012
blackjack	1.00	1.00	1.00	1.00	.999	.970	.834	.596	.366	.204	.108	.056

Theorem (Assaf–Diaconis–Soundararajan) Consider a deck of n cards of m-types as above. Suppose that $D_i \geq 3$ for all $1 \leq i \leq m$. Then

$$\mathrm{SEP}(\mathbf{a}) \approx \mathbf{1} - \frac{\mathbf{a}^{\mathbf{m-1}}}{(\mathbf{n+1})\cdots(\mathbf{n+m-1})} \sum_{\mathbf{j=0}}^{\mathbf{m-1}} (-\mathbf{1})^{\mathbf{j}} \binom{\mathbf{m-1}}{\mathbf{j}} \left(\mathbf{1} - \frac{\mathbf{j}}{\mathbf{a}}\right)^{\mathbf{n+m-1}}$$

Proof: Let $m \geq 2$ and a be natural numbers, let $\xi_1, \ldots, \xi_m$ be real numbers in $[0,1]$. Let $r_1, \ldots, r_m$ be natural numbers with $r_i \geq r \geq 2$.

$$\Big| \sum_{\substack{a_1,\ldots,a_m \geq 0 \\ a_1+\ldots+a_m=a}} (a_1+\xi_1)^{r_1} \cdots (a_m+\xi_m)^{r_m} - \frac{r_1! \cdots r_m!}{(r_1+\ldots+r_m+m-1)!}(a+\xi_1+\ldots+\xi_m)^{r_1+\ldots+r_m+m-1} \Big|$$

$$\leq r_1! \cdots r_m! \sum_{j=1}^{m-1} \binom{m-1}{j} \Big(\frac{1}{3(r-1)}\Big)^j \frac{(a+\xi_1+\ldots+\xi_m)^{r_1+\ldots+r_m+m-1-2j}}{(r_1+\ldots+r_m+m-1-2j)!}$$

Heuristically, let $f_k(z) = \sum_{r \geq 0} r^k z^k = A_k(z)/(1-z)^{k+1}$. Then we want the coefficient of z^a in $(1-z)^{m-1} f_{D_1}(z) \cdots f_{D_2}(z)$. Our theorem says

$$(1-z)^{m-1} f_{D_1}(z) \cdots f_{D_2}(z) \approx \frac{D_1! \cdots D_m!}{(n+m-1)!}(1-z)^{m-1} f_{n+m-1}(z)$$

Question:

How many times must a deck of cards be shuffled?

total variation Answer:

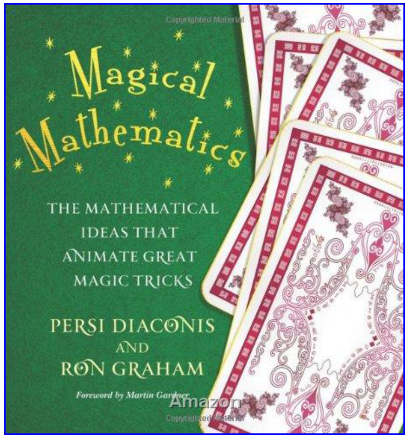
7	if you care about all 52 cards
4	if you care only about the top/bottom card
1	if you care only about the middle card

separation Answer:

12	if you care about all 52 cards
9	if you’re playing Black-Jack
7	if you’re testing for ESP
6	if you care only about the color

References

- D. Bayer and P. Diaconis. Trailing the dovetail shuffle to its lair. *Annals of Applied Probability*, 1992.
- S. Assaf, P. Diaconis and K. Soundararajan. A rule of thumb for riffle shuffles. *Annals of Applied Probability*, 2011.
- P. Diaconis. Mathematical developments from the analysis of riffle shuffling. *Groups, combinatorics & geometry (Durham, 2001)*, 2003.



P. Diaconis and R. Graham

Magical Mathematics: The Mathematical Ideas that Animate Great Magic Tricks

Princeton University Press, 2011