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
The basic question

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

**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 $\sigma$ 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.

<table>
<thead>
<tr>
<th>$\sigma$</th>
<th>AKQ</th>
<th>AQK</th>
<th>QAK</th>
<th>KQA</th>
<th>KAQ</th>
<th>QKA</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Q_2(\sigma)$</td>
<td>1/2</td>
<td>1/8</td>
<td>1/8</td>
<td>1/8</td>
<td>1/8</td>
<td>0</td>
</tr>
<tr>
<td>$U(\sigma)$</td>
<td>1/6</td>
<td>1/6</td>
<td>1/6</td>
<td>1/6</td>
<td>1/6</td>
<td>1/6</td>
</tr>
</tbody>
</table>

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

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

$$\text{SEP} = \max_{\sigma \in S_n} 1 - \frac{Q_2(\sigma)}{U(\sigma)} = \max\{-2, \frac{1}{4}, 1\} = 1$$

Separation bounds total variation: $0 \leq \|Q_2 - U\|_{TV} \leq \text{SEP}(k) \leq 1$
Repeated riffle shuffles

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.

\textbf{CUT} with probability

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

\textbf{DROP} proportional to size

\[ \frac{\# H_i}{\# H_1 + \# H_2 + \ldots + \# H_a} \]

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

\textbf{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.

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

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

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. □

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>TV</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
<td>.924</td>
<td>.614</td>
<td>.334</td>
<td>.167</td>
<td>.085</td>
<td>.044</td>
<td>.021</td>
<td>.010</td>
</tr>
<tr>
<td>SEP</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
<td>.996</td>
<td>.931</td>
<td>.732</td>
<td>.479</td>
<td>.278</td>
<td></td>
</tr>
</tbody>
</table>
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:

pile $k$ \( \{ i \rightarrow \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) rest from piles $k+1 \cdots a$ \)

\( j \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( i-1-r \) cards from piles $1 \cdots k-1$ \)

rest from piles $k \cdots a$
An ‘Amazing Matrix’

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 \( a \):
   \[
   V_m(i) = (i - 1)^{i-1} \binom{m-1}{i-1} + (-1)^{n-i+m} \binom{m-1}{n-i} \text{ for } 1/a^m
   \]

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

$$1_G, \ g_1, \ g_2g_1, \ g_3g_2g_1, \ \ldots$$

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

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

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

riffle shuffles $\iff$ random walk on $S_n$

one card tracking $\iff$ quotient walk on $S_n/(S_{n-1} \times S_1)$

$D_1$ 1’s, $D_2$ 2’s, \ldots $\iff$ quotient walk on $S_n/(S_{D_1} \times S_{D_2} \times \cdots)$
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.

Proof: $\begin{array}{cccccccccccc}
1 & 1 & 1 & 2 & 2 & 2 & 2 & 2 & 3 & 4 & 4 & 4 & 5 & 5 & 5 & 6 & 6 & 6
\end{array}$

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

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

Proof: $Q_a(w^*) = \sum_{A_1+\cdots+A_a=n \atop \text{A refines } D} \frac{1}{a^n} \left( \begin{array}{c} n \\ A_1, \ldots, A_a \end{array} \right) \frac{1}{(D_1, \ldots, D_m)}$

In particular, we have a closed formula for $\text{SEP}(a)$ for general decks.
Rule of Thumb

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

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

\[
\text{SEP}(a) \approx 1 - \frac{a^{m-1}}{(n+1) \cdots (n+m-1)} \sum_{j=0}^{m-1} (-1)^j \binom{m-1}{j} (1 - \frac{j}{a})^{n+m-1}
\]
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 $r_i \geq r \geq 2$.

\[
\left| \sum_{a_1, \ldots, a_m \geq 0 \atop a_1 + \ldots + a_m = a} (a_1 + \xi_1)^{r_1} \cdots (a_m + \xi_m)^{r_m} - \frac{r_1! \cdots r_m!}{(r_1 + \ldots + r_m + m - 1)!} (a + \xi_1 + \ldots + \xi_m)^{r_1 + \ldots + r_m + m - 1} \right| \\
\leq r_1! \cdots r_m! \sum_{j=1}^{m-1} \binom{m-1}{j} \left( \frac{1}{3(r-1)} \right)^j \frac{(a + \xi_1 + \ldots + \xi_m)^{r_1 + \ldots + r_m + m - 1 - 2j}}{(r_1 + \ldots + r_m + m - 1 - 2j)!}
\]

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


P. Diaconis and R. Graham
*Magical Mathematics: The Mathematical Ideas that Animate Great Magic Tricks*
Princeton University Press, 2011