Is Seven Shuffles Enough?

Yi Lee

May 10, 2023

Motivation: A Card Trick

Consider the following trick:

- Start with an ordered deck

Motivation: A Card Trick

Consider the following trick:

- Start with an ordered deck
- Riffle shuffle once

Motivation: A Card Trick

Consider the following trick:

- Start with an ordered deck
- Riffle shuffle once
- Riffle shuffle again

Motivation: A Card Trick

Consider the following trick:

- Start with an ordered deck
- Riffle shuffle once
- Riffle shuffle again
- Pick a card and remember it

Motivation: A Card Trick

Consider the following trick:

- Start with an ordered deck
- Riffle shuffle once
- Riffle shuffle again
- Pick a card and remember it
- Insert it back into the deck

Motivation: A Card Trick

Consider the following trick:

- Start with an ordered deck
- Riffle shuffle once
- Riffle shuffle again
- Pick a card and remember it
- Insert it back into the deck
- Riffle shuffle one last time

Motivation: A Card Trick

Consider the following trick:

- Start with an ordered deck
- Riffle shuffle once
- Riffle shuffle again
- Pick a card and remember it
- Insert it back into the deck
- Riffle shuffle one last time
- Claim: I can find your card

Motivation: A Card Trick

Consider the following trick:

- Start with an ordered deck
- Riffle shuffle once
- Riffle shuffle again
- Pick a card and remember it
- Insert it back into the deck
- Riffle shuffle one last time
- Claim: I can find your card

How?

Motivation: A Card Trick

Consider the following trick:

- Start with an ordered deck 1 rising sequence
- Riffle shuffle once
- Riffle shuffle again
- Pick a card and remember it
- Insert it back into the deck
- Riffle shuffle one last time
- Claim: I can find your card

How?

Motivation: A Card Trick

Consider the following trick:

- Start with an ordered deck 1 rising sequence
- Riffle shuffle once 2 rising sequences
- Riffle shuffle again
- Pick a card and remember it
- Insert it back into the deck
- Riffle shuffle one last time
- Claim: I can find your card

How?

Motivation: A Card Trick

Consider the following trick:

- Start with an ordered deck 1 rising sequence
- Riffle shuffle once 2 rising sequences
- Riffle shuffle again 4 rising sequences
- Pick a card and remember it
- Insert it back into the deck
- Riffle shuffle one last time
- Claim: I can find your card

How?

Motivation: A Card Trick

Consider the following trick:

- Start with an ordered deck 1 rising sequence
- Riffle shuffle once 2 rising sequences
- Riffle shuffle again 4 rising sequences
- Pick a card and remember it
- Insert it back into the deck $4 + 1$ rising sequences
- Riffle shuffle one last time
- Claim: I can find your card

How?

Motivation: A Card Trick

Consider the following trick:

- Start with an ordered deck 1 rising sequence
- Riffle shuffle once 2 rising sequences
- Riffle shuffle again 4 rising sequences
- Pick a card and remember it
- Insert it back into the deck $4 + 1$ rising sequences
- Riffle shuffle one last time $8 + 1$ rising sequences
- Claim: I can find your card

How?

Main Theorem

After shuffling n cards for $\frac{3}{2}\log_2 n + \theta$ times, the distance to uniform is

$$1 - 2\Phi\left(\frac{-2^{-\theta}}{4\sqrt{3}}\right) + O\left(\frac{1}{n^{1/4}}\right)$$

where

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

Main Theorem

After shuffling n cards for $\frac{3}{2}\log_2 n + \theta$ times, the distance to uniform is

$$1 - 2\Phi\left(\frac{-2^{-\theta}}{4\sqrt{3}}\right) + O\left(\frac{1}{n^{1/4}}\right)$$

$$\left[1 - 2\Phi\left(\frac{-1}{4c\sqrt{3}}\right) \xrightarrow{c\to\infty} \frac{1}{2c\sqrt{6\pi}}\right]$$

where

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

Some Data

TABLE 4
Shuffles needed to mix 25, 32, 52, 78, 104, 208 or 312 cards

n	25	32	52	78	104	208	312
$\frac{3}{2}\log_2 n$	6.97	7.50	8.55	9.43	10.05	11.55	12.43

Some Data

TABLE 4
Shuffles needed to mix 25, 32, 52, 78, 104, 208 or 312 cards

n	25	32	52	78	104	208	312
$\frac{3}{2}\log_2 n$	6.97	7.50	8.55	9.43	10.05	11.55	12.43

TABLE 3
Total variation distance for m shuffles of 25, 32, 52, 78, 104, 208 or 312 distinct cards

m	1	2	3	4	5	6	7	8	9	10
25	1.000	1.000	0.999	0.775	0.437	0.231	0.114	0.056	0.028	0.014
32	1.000	1.000	1.000	0.929	0.597	0.322	0.164	0.084	0.042	0.021
52	1.000	1.000	1.000	1.000	0.924	0.614	0.334	0.167	0.085	0.043
78	1.000	1.000	1.000	1.000	1.000	0.893	0.571	0.307	0.153	0.078
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
312	1.000	1.000	1.000	1.000	1.000	1.000	1.000	0.999	0.883	0.565

Literature Overview

- Shuffling Cards and Stopping Time (1986)

Literature Overview

- Shuffling Cards and Stopping Time (1986)
  - Covered mostly in lecture

Literature Overview

- Shuffling Cards and Stopping Time (1986)
  - Covered mostly in lecture
  - $t \leq 2 \log_2 \frac{4n}{3}$

Literature Overview

- Shuffling Cards and Stopping Time (1986)
  - Covered mostly in lecture
  - $t \leq 2\log_2 \frac{4n}{3}$
- Trailing the Dovetail Shuffle to its Lair (1992)

Literature Overview

- Shuffling Cards and Stopping Time (1986)
  - Covered mostly in lecture
  - $t \leq 2 \log_2 \frac{4n}{3}$
- Trailing the Dovetail Shuffle to its Lair (1992)
  - Natural follow-up work

Literature Overview

- Shuffling Cards and Stopping Time (1986)
  - Covered mostly in lecture
  - $t \leq 2\log_2 \frac{4n}{3}$
- Trailing the Dovetail Shuffle to its Lair (1992)
  - Natural follow-up work
  - Main theorem today

Literature Overview

- Shuffling Cards and Stopping Time (1986)
  - Covered mostly in lecture
  - $t \leq 2 \log_2 \frac{4n}{3}$
- Trailing the Dovetail Shuffle to its Lair (1992)
  - Natural follow-up work
  - Main theorem today
- A Rule of Thumb for Riffle Shuffling (2008)

Literature Overview

- Shuffling Cards and Stopping Time (1986)
  - Covered mostly in lecture
  - $t \leq 2 \log_2 \frac{4n}{3}$
- Trailing the Dovetail Shuffle to its Lair (1992)
  - Natural follow-up work
  - Main theorem today
- A Rule of Thumb for Riffle Shuffling (2008)
  - What if there are duplicate cards?

Literature Overview

- Shuffling Cards and Stopping Time (1986)
  - Covered mostly in lecture
  - $t \leq 2 \log_2 \frac{4n}{3}$
- Trailing the Dovetail Shuffle to its Lair (1992)
  - Natural follow-up work
  - Main theorem today
- A Rule of Thumb for Riffle Shuffling (2008)
  - What if there are duplicate cards?
  - Blackjack: Suits don't matter, and $10 = J = Q = K$

Literature Overview

- Shuffling Cards and Stopping Time (1986)
  - Covered mostly in lecture
  - $t \leq 2\log_2 \frac{4n}{3}$
- Trailing the Dovetail Shuffle to its Lair (1992)
  - Natural follow-up work
  - Main theorem today
- A Rule of Thumb for Riffle Shuffling (2008)
  - What if there are duplicate cards?
  - Blackjack: Suits don't matter, and $10 = J = Q = K$
- Analysis of Casino Shelf Shuffling Machines (2013)

Literature Overview

- Shuffling Cards and Stopping Time (1986)
  - Covered mostly in lecture
  - $t \leq 2 \log_2 \frac{4n}{3}$
- Trailing the Dovetail Shuffle to its Lair (1992)
  - Natural follow-up work
  - Main theorem today
- A Rule of Thumb for Riffle Shuffling (2008)
  - What if there are duplicate cards?
  - Blackjack: Suits don't matter, and $10 = J = Q = K$
- Analysis of Casino Shelf Shuffling Machines (2013)
- Shuffling Cards by Spatial Motion (2017)

Literature Overview

- Shuffling Cards and Stopping Time (1986)
  - Covered mostly in lecture
  - $t \leq 2\log_2 \frac{4n}{3}$
- Trailing the Dovetail Shuffle to its Lair (1992)
  - Natural follow-up work
  - Main theorem today
- A Rule of Thumb for Riffle Shuffling (2008)
  - What if there are duplicate cards?
  - Blackjack: Suits don't matter, and $10 = J = Q = K$
- Analysis of Casino Shelf Shuffling Machines (2013)
- Shuffling Cards by Spatial Motion (2017)
  - What if the deck is too big to be riffled?

Literature Overview

- Shuffling Cards and Stopping Time (1986)
  - Covered mostly in lecture
  - $t \leq 2 \log_2 \frac{4n}{3}$
- Trailing the Dovetail Shuffle to its Lair (1992)
  - Natural follow-up work
  - Main theorem today
- A Rule of Thumb for Riffle Shuffling (2008)
  - What if there are duplicate cards?
  - Blackjack: Suits don't matter, and $10 = J = Q = K$
- Analysis of Casino Shelf Shuffling Machines (2013)
- Shuffling Cards by Spatial Motion (2017)
  - What if the deck is too big to be riffled?
  - Analysis of *smooshing* shuffle

Another Way to Riffle Shuffle

a-shuffle: generalization of riffle shuffle

Another Way to Riffle Shuffle

a-shuffle: generalization of riffle shuffle

- Split the deck into a packets using the multinomial distribution

Another Way to Riffle Shuffle

a-shuffle: generalization of riffle shuffle

- Split the deck into a packets using the multinomial distribution
- Iteratively riffle the packets together

Some Facts About a-shuffle

1. There are many equivalent descriptions.

Some Facts About a-shuffle

1. There are many equivalent descriptions.
2. An a-shuffle followed by a b-shuffle is equivalent to a ab-shuffle.

Some Facts About a-shuffle

1. There are many equivalent descriptions.
2. An a-shuffle followed by a b-shuffle is equivalent to a ab-shuffle.
3. If π has r rising sequences, then the probability of obtaining π in an a-shuffle is $\frac{\binom{a+n-r}{n}}{a^n}$.

Approach to Uniformity

Let

- $m = \frac{3}{2} \log_2 n + \theta$ be the number of shuffles,

Approach to Uniformity

Let

- $m = \frac{3}{2}\log_2 n + \theta$ be the number of shuffles,
- $Q^m(r) = \frac{\binom{2^m+n-r}{n}}{2^{mn}}$ be the probability of a permutation with r rising sequences,

Approach to Uniformity

Let

- $m = \frac{3}{2}\log_2 n + \theta$ be the number of shuffles,
- $Q^m(r) = \frac{\binom{2^m+n-r}{n}}{2^{mn}}$ be the probability of a permutation with r rising sequences,
- $A_{n,r} = |\{\, \pi \in \mathrm{Sym}(n) : \pi \text{ has } r \text{ rising sequences} \,\}|$

Approach to Uniformity

Let

- $m = \frac{3}{2}\log_2 n + \theta$ be the number of shuffles,
- $Q^m(r) = \frac{\binom{2^m+n-r}{n}}{2^{mn}}$ be the probability of a permutation with r rising sequences,
- $A_{n,r} = |\{\, \pi \in \mathrm{Sym}(n) : \pi \text{ has } r \text{ rising sequences} \,\}|$

Goal: upper bound the distance

$$\|Q^m - U\| = \sum_{r:Q^m(r)\geq\frac{1}{n!}} A_{n,r}\left(Q^m(r) - \frac{1}{n!}\right)$$

Approach to Uniformity

Let

- $m = \frac{3}{2}\log_2 n + \theta$ be the number of shuffles,
- $Q^m(r) = \frac{\binom{2^m+n-r}{n}}{2^{mn}}$ be the probability of a permutation with r rising sequences,
- $A_{n,r} = |\{\, \pi \in \mathrm{Sym}(n) : \pi \text{ has } r \text{ rising sequences} \,\}|$

Goal: upper bound the distance

$$\|Q^m - U\| = \sum_{r:Q^m(r)\geq \frac{1}{n!}} A_{n,r}\left(Q^m(r) - \frac{1}{n!}\right)$$

$$= \sum_{r=0}^{r^*} A_{n,r}\left(Q^m(r) - \frac{1}{n!}\right)$$

Bounding the First Term

Let $c = 2^{\theta}$, then

$$\sum_{r=0}^{r^*} A_{n,r} \cdot Q^m(r) \approx \sum_{r=r_0}^{r^*} A_{n,r} \cdot Q^m(r)$$

Bounding the First Term

Let $c = 2^{\theta}$, then

$$\sum_{r=0}^{r^*} A_{n,r} \cdot Q^m(r) \approx \sum_{r=r_0}^{r^*} A_{n,r} \cdot Q^m(r)$$
$$\leq A_{n,r^*} \sum_{r=r_0}^{r^*} Q^m(r)$$

Bounding the First Term

Let $c = 2^{\theta}$, then

$$\begin{aligned}
\sum_{r=0}^{r^*} A_{n,r} \cdot Q^m(r) &\approx \sum_{r=r_0}^{r^*} A_{n,r} \cdot Q^m(r) \\
&\leq A_{n,r^*} \sum_{r=r_0}^{r^*} Q^m(r) \\
&\approx A_{n,r^*} \int_{r_0}^{r^*} Q^m(r)
\end{aligned}$$

Bounding the First Term

Let $c = 2^{\theta}$, then

$$\begin{aligned}\sum_{r=0}^{r^*} A_{n,r} \cdot Q^m(r) &\approx \sum_{r=r_0}^{r^*} A_{n,r} \cdot Q^m(r) \\ &\leq A_{n,r^*} \sum_{r=r_0}^{r^*} Q^m(r) \\ &\approx A_{n,r^*} \int_{r_0}^{r^*} Q^m(r) \\ &\approx \dots\end{aligned}$$

Bounding the First Term

Let $c = 2^\theta$, then

$$\begin{aligned}
\sum_{r=0}^{r^*} A_{n,r} \cdot Q^m(r) &\approx \sum_{r=r_0}^{r^*} A_{n,r} \cdot Q^m(r) \\
&\leq A_{n,r^*} \sum_{r=r_0}^{r^*} Q^m(r) \\
&\approx A_{n,r^*} \int_{r_0}^{r^*} Q^m(r) \\
&\approx \dots \\
&\approx \Phi\left(\frac{1}{4c\sqrt{3}}\right)
\end{aligned}$$

Putting Everything Together

$$\sum_{r=0}^{r^*} A_{n,r}\left(Q^m(r) - \frac{1}{n!}\right) = \Phi\left(\frac{1}{4c\sqrt{3}}\right) - \frac{1}{n!}\sum_{r=0}^{r^*} A_{n,r}$$

Putting Everything Together

$$\begin{aligned}\sum_{r=0}^{r^*} A_{n,r}\left(Q^m(r) - \frac{1}{n!}\right) &= \Phi\left(\frac{1}{4c\sqrt{3}}\right) - \frac{1}{n!}\sum_{r=0}^{r^*} A_{n,r} \\ &\approx \Phi\left(\frac{1}{4c\sqrt{3}}\right) - \Phi\left(-\frac{1}{4c\sqrt{3}}\right)\end{aligned}$$

Putting Everything Together

$$\begin{aligned}
\sum_{r=0}^{r^*} A_{n,r} \left(Q^m(r) - \frac{1}{n!} \right) &= \Phi\left(\frac{1}{4c\sqrt{3}}\right) - \frac{1}{n!} \sum_{r=0}^{r^*} A_{n,r} \\
&\approx \Phi\left(\frac{1}{4c\sqrt{3}}\right) - \Phi\left(-\frac{1}{4c\sqrt{3}}\right) \\
&= 1 - 2\Phi\left(-\frac{1}{4c\sqrt{3}}\right)
\end{aligned}$$