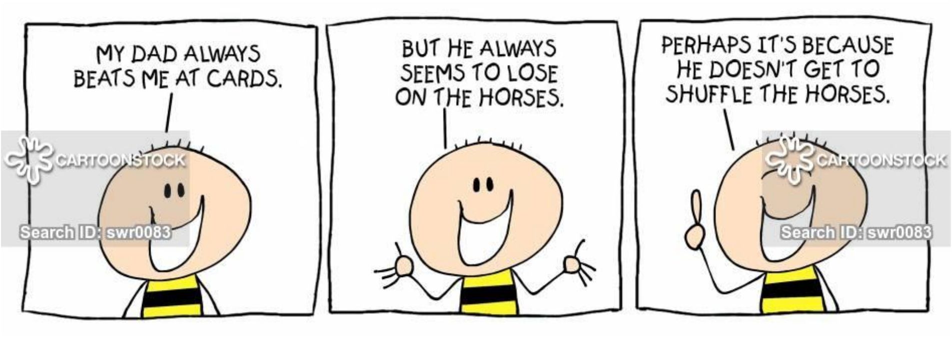
Markov Chain Monte Carlo Methods for Card Shuffling

Rashmeet Kaur Nayyar, Naman Shah

CSE 598: Markov Chain Monte Carlo Methods
Fall 2019

Motivation

- The pattern of cards can become apparent to the players if not shuffled.
- For eg., the cards may not come out of the chute in numerical order, such as, 2-3-4-5.
- This has even led players in casinos to up their bets, and resulted in millions of losses.
- Studying different **techniques for generating random permutations of cards** and **how long it takes to reach randomness** for each technique is therefore important.



Overhand Shuffle

- Most used and easiest practical shuffling method
- Algorithm:
  - Start with all cards in the right hand
  - Repeat till all the cards are in the left hand:
    - Select some k cards from the top of the deck in the right hand
    - Place them on the top of the deck in the left hand

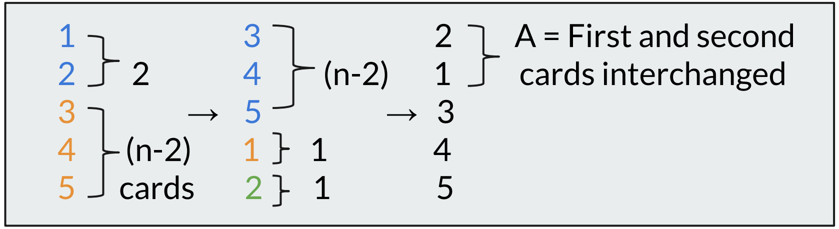
L	R		L	R		L	R		L	R
∅	1		1	3		3	4		4	∅
	2		2	4		1	5		5	
	3	->		5	->	2		->	3	
	4								1	
	5								2	

Upper bound on mixing time: $O(n^2 \log n)$

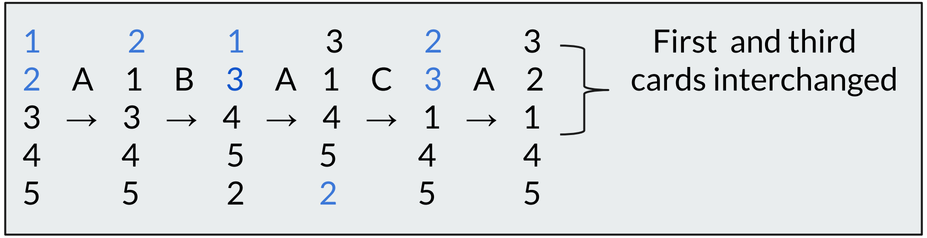
Overhand Shuffle

➔ **Irreducible?**

- perform multiple overhand shuffles using blue, orange, and then green cards

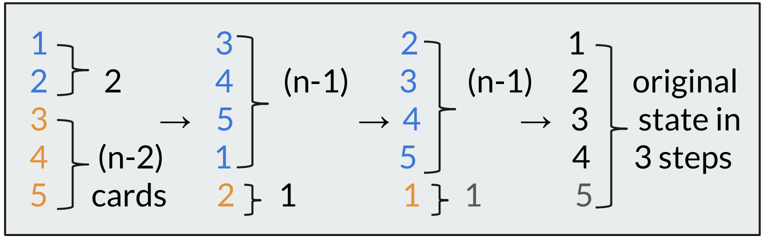


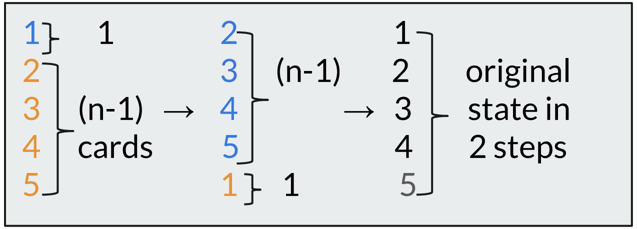
B = put top card at bottom, C = put bottom card at top



Similarly, we can interchange all pairs of cards and achieve all permutations of cards...(although takes a long time)

➔ Aperiodic?





Gcd of all possible steps to reach back to original state is 1.

Top-to-random Shuffle

- Algorithm:
    - Select the topmost card at position 1
    - Select a position i at random from 1 to n
    - Shift all the cards from position 2 to i to the positions 1 to i-1
    - Place the topmost card at this now vacant position i

1	chosen	2	chosen	3		
2	position	3	position	4		
3	→	4	→	2	→	....
4	= 4	1	= 3	1		
5		5		5		

Upper bound on mixing time: O(nlogn)

Top-to-random Shuffle

➔ **Irreducible?**

To transition from a state x to a state y,

1. repeatedly put the top card at the bottom until the the bottom card agrees with the bottom card in state y
2. repeat the same process for next-lowest card and so on until the state matches with y

1		2		3		4		5		1		2
2		3		4		5		1		2		1
3	→	4	→	5	→	1	→	2	→	5	→	5
4		5		1		2		4		4		4
5		1		2		3		3		3		3
State x												State y

➔ **Aperiodic?**

- While randomly selecting the random position to place the topmost card, it can select the position 1 with ½ probability.
- This introduces self loops in the Markov chain, and make the chain aperiodic.

Knuth Shuffle

- simple yet efficient computer based algorithm
- Algorithm:
  - Set i = 1
  - Repeat till i<n:
    - Select an index j at random from i to n
    - Swap the card at location i with the card at location j
    - Set i = i + 1

1	(i=1)	4	(i=2)	4	(i=3)	4	(i=4)	4
2	(j=4)	2	(j=3)	3	(j=5)	3	(j=5)	3
3	→	3	→	2	→	5	→	5
4		1		1		1		2
5		5		5		2		1

We select a card uniformly at random (shown in green) from the cards specified by

Here, we swap the green and blue cards

Knuth Shuffle

- **Irreducible**?
  - In each shuffle, swap card at index i with the card at index i in the target configuration

i=1		i=2		i=3		i=4		
1		2		2		2		2
2		1		1		1		1
3	→	3	→	3	→	5	→	5
4		4		4		4		3
5		5		5		3		4
State x								State y

(blue and green cards are swapped)

- **Aperiodic**?
  - Yes.
  - How?
    - The index j selected uniformly at random can be chosen same as i.
    - This swaps the card at location i with itself, keeping the state unchanged .
    - This creates self loops.

Transposition Shuffle

- general version of Knuth shuffle
- The algorithm works as follows:
  - Select an index i at random. (shown in blue)
  - Select an index j at random. (shown in green)
  - Swap the cards at index i and j with each other.

1		1		5		5		5		
2		4		4		4		1		
3	→	3	→	3	→	1	→	4	→	...
4		2		2		2		2		
5		5		1		3		3		

Upper bound on mixing time: O(nlogn)

Transposition Shuffle

- **Irreducible**?
  - Very similar proof to Knuth shuffle.
  - Let X be the current and Y be the target configuration.
  - Select i s.t X(i) != Y(i).
  - Select j s.t X(j) = Y(i)
  - Swap the cards at index i and j.

- **Aperiodic**?
  - Yes.
  - How?
    - Self loops.
    - If index i selected and index j selected are the same, then the state remains unchanged.

<u>Example:</u>

Start State: 1,2,3,4,5,6
End State: 2,5,1,4,6,3

1,2,3,4,5,6 -> 2,1,3,4,5,6 -> 2,5,3,4,1,6 -> 2,5,1,4,3,6 -> 2,5,1,4,6,3

Thorp Shuffle

- Assumption: number of cards is even
- Algorithm:
  - Cut the deck in half and create two decks left and right of equal sizes.
  - Toss a coin
  - If heads:
    - Drop a card from left deck
    - Drop a card from right deck
  - If tails:
    - Drop a card from right deck
    - Drop a card from left deck

Original deck = [1, 2, 3, 4, 5, 6]
→ Left = [1, 2, 3], Right = [4, 5, 6]
→tossed coin outcome = head
new deck = [1, 4]
Left = [2, 3], Right = [5, 6]
→ tossed coin outcome = tail
new deck = [1, 4, 5, 2]
Left = [3], Right = [6]
→tossed coin outcome = head
new deck = [1, 4, 5, 2, 3, 6]
Left = [ ], Right = [ ]

Upper bound on mixing time: $O(\log_2^3 n)$

Thorp Shuffle

Irreducible? - Yes

Irreducibility of Thorp is difficult to analyze.

All the cards can be brought to the first position

[1,2|3,4] → [3,1|2,4] → [2,3|4,1] → [4,2|3,1] → ....

If the first card is fixed, all the cards can be brought to the second position

[1,2|3,4] → [1,3|2,4] → [1,2|4,3] → [1,4|3,2] → [1,3|4,2] → [1,4|2,3] → [1,2|3,4] → ...

Similarly, all the permutations can be achieved from any state.

Aperiodic? - Yes

[1, 2, 3| 4, 5, 6] → [1, 4, 2| 5, 3, 6] → [1, 5, 4|3, 2, 6] → [1, 3, 5| 2, 4, 6] → [1, 2, 3| 4, 5, 6] (4 steps)

[1, 2, 3| 4, 5, 6] → [4, 1, 5| 2, 6, 3] → [2, 4, 6| 1, 3, 5] → [1, 2, 3| 4, 5, 6] (3 steps)

Thus, the Gcd is 1, and this can be generalized to all the states. Hence, aperiodic.

Riffle Shuffle

- Bayer & Deconis formalized Riffle shuffle using GSR distribution in 1992.
- General and more practical variant of Thorp shuffle.
- The algorithm works as follows:
  - Divide the cards into two decks using binomial distribution.
  - Let p = |left| / |left| + |right|
  - Drop card from left deck with probability p and from right deck with probability 1 - p.

Upper bound on mixing time: $O(\log_2 n)$

Original deck = [1, 2, 3, 4, 5, 6]
→ Left = [1, 2], Right = [3, 4, 5, 6]
(p=⅓), (1-p=⅔)
→ new deck = [3]
Left = [1, 2], Right = [4, 5, 6]
→ new deck = [3, 4]
Left = [1, 2], Right = [5, 6]
→new deck = [3, 4, 1]
Left = [2], Right = [5, 6]
→ new deck = [3, 4, 1]
Left = [2], Right = [5, 6]
→ new deck = [3, 4, 1, 5]
Left = [2], Right = [6]
→new deck = [3, 4, 1, 5, 2]
Left = [], Right = [6]
→new deck = [3, 4, 1, 5, 2, 6]
Left = [], Right = []

Riffle Shuffle

- Irreducibility
  - We can divide and drop cards such that ith index in the resultant state would match ith index in the desired state.
  - Start with i = 0.
  - Perform the above step.
  - Increment i with 1.
- Aperiodic?
  - Yes.
  - How?
    - Self loops.
    - If we drop all the cards from right deck first and then drop all the cards from left deck then we would end up at same state.

Example:

Start State: 1,2,3,4,5,6
End State: 2,5,1,4,6,3

1,|2,3,4,5,6 → 2,1,3,4,5,6 → 2,1,3,4,|5,6 → 2,5,1,3,4,6 → 2,5,|1,3,4,6 → 2,5,1,3,4,6 → 2,5,1,3|,4,6 → 2,5,1,4,3,6 → 2,5,1,4,3,|6 → 2,5,1,4,6,3

Challenges

- Biggest Challenge
  - How do we know if the deck arrangement is random?
- Option:
  - Variational Distance.
- Possible?
  - No. Why?
  - Need to iterate over possible states which are factor of n!
  - For deck of 52 cards: order of 10^87

$$d(\pi, v) = \frac{1}{n} \sum_{u \in \Omega} ||\pi(u) - v(u)||^2$$

Approximate Variational Distance

- Exact variational distance is infeasible to calculate.
- [1] presented an approach to estimate the variational distance for such shufflings.

$$||Q^m - U|| = 1 - 2\Phi\left(\frac{-1}{4c\sqrt{3}}\right) + O_c\left(\frac{1}{n^{1/4}}\right)$$

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

$$O_c\left(\frac{1}{n}\right) = \frac{1}{c^4 n^6} \sum_{i=0}^{n-1} \left(\frac{n}{2} - h - i\right)^4$$

[1] Dave Bayer, Persi Diaconis, et al. 1992. Trailing the dovetail shuffle to its lair. The Annals of Applied Probability 2, 2 (1992), 294–313.

Rising Sequences

- Definition: The maximal subset of an arrangement of the cards consisting successive face values displayed in order
- It is the number of times we need to go through the deck to traverse all the cards in order.

Current Configuration:

(3, 4, 8, 1, 2, 7, 9, 5, 6, 10)

No. of rising sequences : 4

Cards traversed after 1st pass

(1,2)

Cards traversed after 2nd pass

(1,2,3,4,5,6)

Cards traversed after 3rd pass

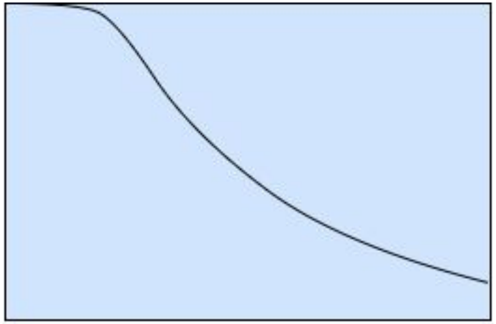
(1,2,3,4,5,6,7)

Cards traversed after 4th pass

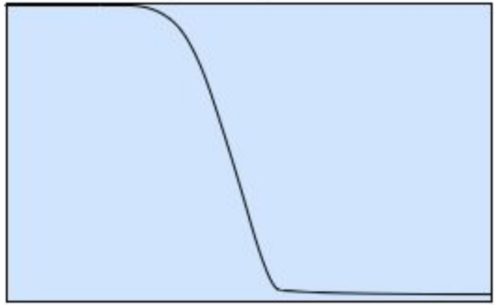
(1,2,3,4,5,6,7,8,9,10)

Cutoff Phenomenon

- When Variational distance encounters a significant drop.
- Cutoff Phenomenon shows fast convergence.
- No significant change after the cutoff.



Steady convergence



Abrupt convergence

Shannon's Entropy

- Entropy is directly proportional to the information required to explain the elements of the set

$$E(s) = -\sum_{i \in s} p_i log_2(p_i)$$

- In card shuffling, let F_{i} be defined as distance between two consecutive cards at index i and i +1 .
- p_{i} is the normalized histogram for of F_{i}.

<u>Example:</u>

Start State: 1,2,3,4,5,6

End State: 2,5,1,4,6,3

i	F
1	1
2	4
3	1
4	1
5	2

p	C
1	3
2	1
4	1

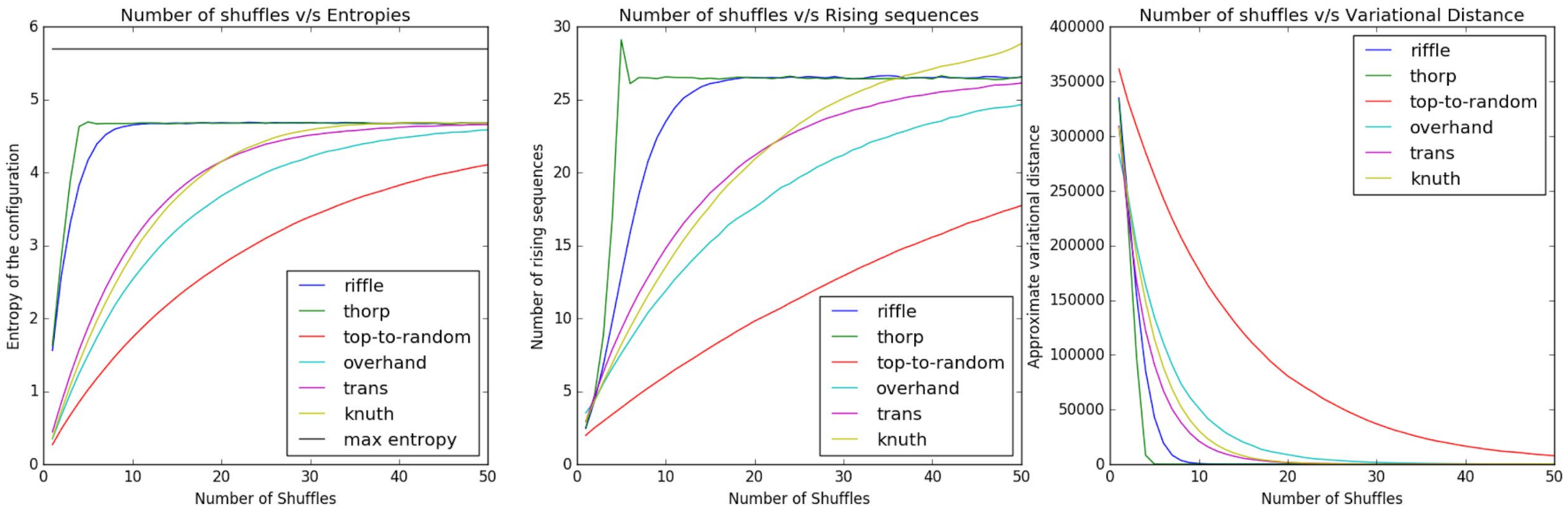
p	C
1	3/5
2	1/5
4	1/5

E(s) = 1.371

Experiments

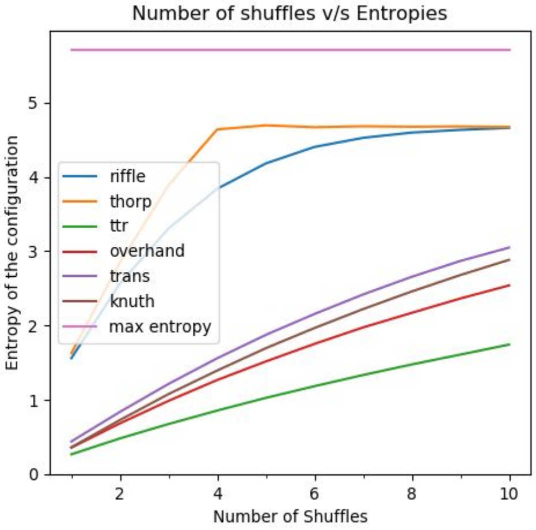
- Implemented Overhand, Top-to-random, Transposition, Knuth, Thorp, and Riffle Shuffles in Python
- Tested the randomness of the deck configuration using
  - Rising sequences,
  - Approximate Variational distance,
  - Shannon’s entropy,
  - Cut-off phenomenon
- An average of 10,000 runs for each shuffling method

Results

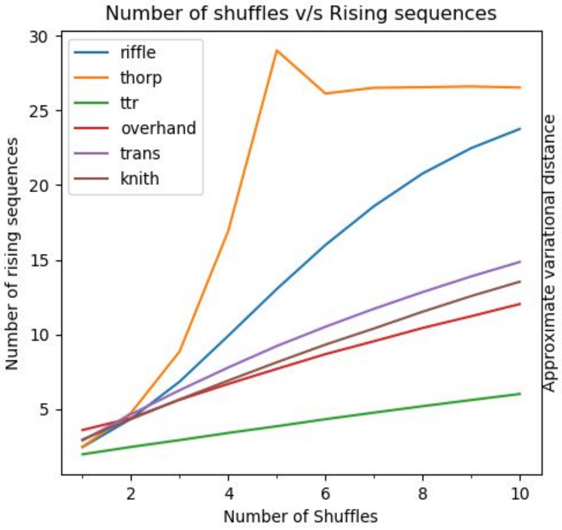


Number of shuffles v/s Entropies
Entropy of the configuration
Number of Shuffles
riffle
thorp
top-to-random
overhand
trans
knuth
max entropy
Number of shuffles v/s Rising sequences
Number of rising sequences
Number of Shuffles
riffle
thorp
top-to-random
overhand
trans
knuth
Number of shuffles v/s Variational Distance
Approximate variational distance
Number of Shuffles
riffle
thorp
top-to-random
overhand
trans
knuth

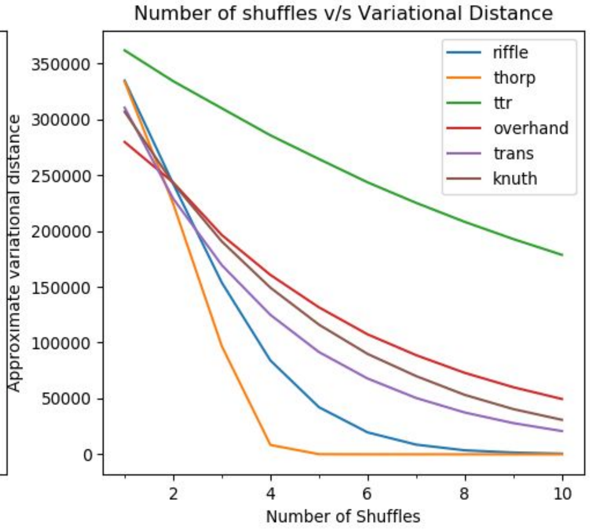
Results



Number of shuffles v/s Entropies
Entropy of the configuration
Number of Shuffles
riffle
thorp
ttr
overhand
trans
knuth
max entropy



Number of shuffles v/s Rising sequences
Number of rising sequences
Number of Shuffles
riffle
thorp
ttr
overhand
trans
knith



Number of shuffles v/s Variational Distance
Approximate variational distance
Number of Shuffles
riffle
thorp
ttr
overhand
trans
knuth

Questions?