Shuffling with ordered cards

Steve Butler[1]
(joint work with Ron Graham)

[1]Department of Mathematics
University of California Los Angeles
www.math.ucla.edu/~butler

Combinatorics, Groups, Algorithms and Complexity
23 March 2010

Mathematics from cards and shuffling

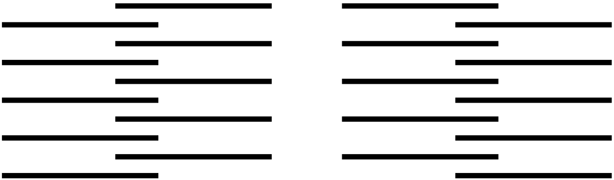
Cards make excellent motivation for mathematical problems (and can even lead to great mathematicians).

- Counting how many different hands are possible in a 52 card deck. (Combinatorics)
- Given what cards have already been played, finding the likelihood of a face card. (Probability)
- How many "shuffles" does it take to randomize a deck of cards. (Random walks on graphs)

    (Of course it depends on who is doing the shuffling!)

Perfect riffle shuffles

A perfect riffle shuffle consists of splitting a deck of cards into two equal stacks and perfectly alternating the cards between the two stacks.

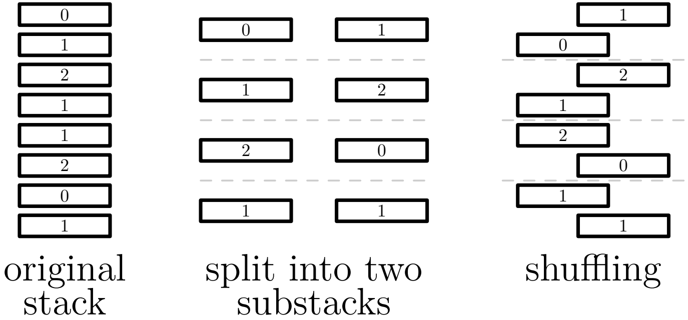


In-shuffle Out-shuffle

These two shuffles are generators for a group of how to get to all possible arrangements of cards $\langle I, O \rangle$.

A new shuffle

We consider a new shuffle of a deck where cards have ordered labels and where not only the position but also the label of the card is important. Again we split the deck into k equally sized stacks but now we use the label to determine which card drops first. (Larger labels want to drop "down". When there is a tie then the order is unimportant.)



Suppose that we have $N = kn$ labeled cards. Suppose the labels are $a_0, a_1, \ldots, a_{n-1}, a_n, a_{n+1}, \ldots, a_{2n-1}, a_{2n}, \ldots, a_{kn-1}$. Construct $k \times n$ matrix filling rows left to right, top to bottom.

$$\begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_n & a_{n+1} & \cdots & a_{2n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \cdot & \cdot & \cdots & a_{kn-1} \end{pmatrix}.$$

Sort each column according to the ordering of the labels,

$$\begin{pmatrix} b_0 & b_k & \cdots & \cdot \\ b_1 & b_{k+1} & \cdots & \cdot \\ \vdots & \vdots & \ddots & \vdots \\ b_{k-1} & b_{2k-1} & \cdots & b_{kn-1} \end{pmatrix}.$$

Concatenate the columns to form the labels for the shuffled cards $b_0, b_1, \ldots, b_{k-1}, b_k, b_{k+1}, \ldots, b_{2k-1}, b_{2k}, \ldots, b_{kn-1}$.

An example, $N = 12$, $k = 3$

Starting with a stack of labeled cards in order 021100122110 then one shuffle gives the following.

$$021100122110 \longrightarrow \begin{pmatrix} 0 & 2 & 1 & 1 \\ 0 & 0 & 1 & 2 \\ 2 & 1 & 1 & 0 \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} 2 & 2 & 1 & 2 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \longrightarrow 200210111210$$

Repeating we have

$$021100122110 \longrightarrow 200210111210 \longrightarrow 211200110210$$
$$\longrightarrow 200210111210$$

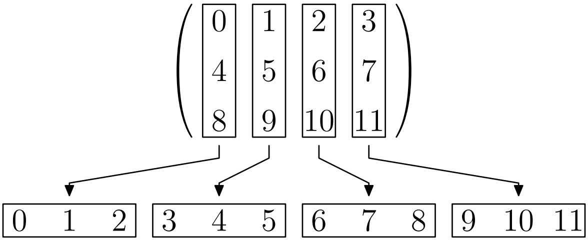
Observation

Starting with a stack of cards then after finitely many shuffles we will enter into a periodic cycle.

- What periods are possible?
- How long does it take to get to the periodic stack?
- How do we find periodic stacks?
- How do we find fixed stacks?
- How many fixed stacks are there?

Where do the subscripts map?

Returning to the case $N = 12$ and $k = 3$ we have:



This shows, for example, $\{a_2, a_6, a_{10}\} \to \{b_6, b_7, b_8\}$ in some order, depending on the labels.

We would like a rule for defining a map $a_i \to b_j$, i.e., $i \to j$, in some “natural” way.

Shuffling weight function

A shuffling weight function is a map $\varphi : \{0, \ldots, N-1\} \to \mathbb{Z}$ which satisfies the following two conditions for $\ell \in \{0, 1, \ldots, n-1\}$:

(i) $\{\varphi(\ell), \varphi(\ell+n), \ldots, \varphi(\ell+(k-1)n)\} = \{\varphi(k\ell), \varphi(k\ell+1), \ldots, \varphi(k\ell+(k-1))\}$.

(ii) $\varphi(k\ell) < \varphi(k\ell+1) < \cdots < \varphi(k\ell+(k-1))$.

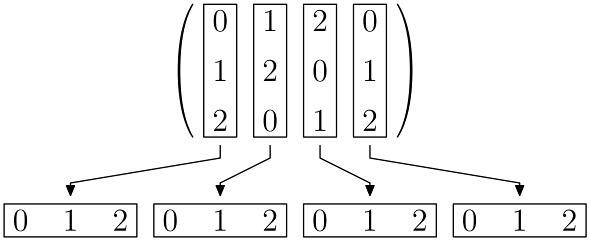
Theorem

A shuffling weight function φ exists for each $N = kn$ and k.

A shuffling weight function for $N = 12$, $k = 3$

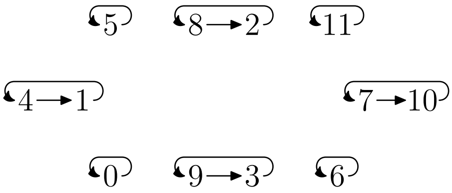
n	0	1	2	3	4	5	6	7	8	9	10	11
$\varphi(n)$	0	1	2	0	1	2	0	1	2	0	1	2

Replacing n by $\varphi(n)$ our previous diagram becomes the following.

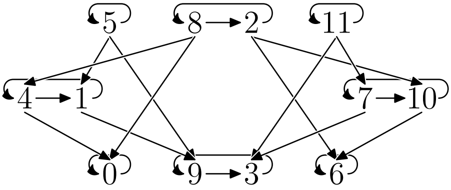


Constructing the shuffling "poset"

We now construct a directed graph by letting $n \to m$ where $\varphi(n) = \varphi(m)$. By defining properties of weight we have in-degree=out-degree= 1 at each vertex (so graph consists of directed cycles). Place into a poset with the cycle containing n at height $\varphi(n)$.



Add to this edges (oriented downwards) between all elements in the same column.



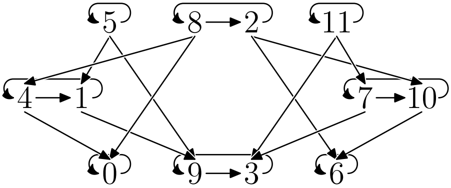
Observation

Shuffling can be done using this poset as follows:

- Place cards according to their position.
- Using vertical directed edges swap cards so no vertical edge has a high card above a low card.
- Using horizontal directed edges move each card to next entry.
- Pick up cards according to their position.

The shuffling poset is useful!

Since we can use the shuffling poset to do the shuffling then this structure gives a lot of information about what happens in the shuffling process.



Observation

The possible periods are divisors of the least common multiple of the cycle lengths in the rows of this poset.

A special case

Suppose that $N = kn = k^t q$ and that $\gcd(k, q) = 1$.

A shuffling weight function

Let the base k expansion of A be $\ldots A_t A_{t-1} \ldots A_0$. Then

$$\varphi(A) = A_0 + \ldots + A_{t-1}$$

is a shuffling weight function.

The mapping given by the weight function

Let the base k expansion of A be $\ldots A_t A_{t-1} \ldots A_0$. Then

$$A \mapsto kA + A_{t-1} \pmod{N}.$$

Cycle lengths when $\gcd(q, k) = 1$

Theorem

Let $N = k^t q$ with $\gcd(k, q) = 1$, and let $\mathrm{order}_k(s)$ denote the multiplicative order of k modulo s. Then the length of a cycle in the shuffling poset when we divide N into k equal stacks is a divisor of $\mathrm{order}_k(N - q)$. Further, there is a cycle of length $\mathrm{order}_k(N - q)$.

Example

If $N = 12 = 3{\cdot}4$ and $k = 3$ then $\gcd(3, 4) = 1$. So periods are divisors of $\mathrm{order}_3(12 - 4) = \mathrm{order}_3(8) = 2$.

Proof

Suppose we start our cycle at x with base k expansion $\ldots A_{t-1} \ldots A_1 A_0$, then we map t times.

$$\begin{aligned} x &\to kx + A_{t-1} \pmod N \\ &\to k^2x + kA_{t-1} + A_{t-2} \pmod N \\ &\to k^3x + k^2A_{t-1} + kA_{t-2} + A_{t-3} \pmod N \\ &\to \ldots \\ &\to k^t x + \underbrace{\sum_{i=0}^{t-1} k^i A_i}_{=A'} \pmod N. \end{aligned}$$

Proof, continued

Repeating this r times (for a total of rt steps) we have

$$\begin{aligned} x &\rightarrow k^t x + A' \pmod{N} \\ &\rightarrow k^{2t} x + k^t A' + A' \pmod{N} \\ &\rightarrow k^{3t} x + k^{2t} A' + k^t A' + A' \pmod{N} \\ &\rightarrow \cdots \\ &\rightarrow k^{rt} x + \sum_{i=0}^{r-1} k^{it} A' \pmod{N}. \end{aligned}$$

For some r we will be back where we started if

$$k^{rt} x + \sum_{i=0}^{r-1} k^{it} A' \equiv x \quad (\text{mod } N = k^t q)$$

Proof, continued

$$k^{rt}x + \sum_{i=0}^{r-1} k^{it}A' \equiv x \pmod{N = k^t q}$$

Multiply both sides by $k^t - 1$ and simplifying we have

$$(k^{rt} - 1)\big(x(k^t - 1) + A'\big) \equiv 0 \pmod{(k^t - 1)k^t q}.$$

We have $x = A' + mk^t$, substituting we have

$$(k^{rt} - 1)k^t\big(A' + m(k^t - 1)\big) \equiv 0 \pmod{(k^t - 1)k^t q}$$

or

$$(k^{rt} - 1)\big(A' + m(k^t - 1)\big) \equiv 0 \pmod{(k^t - 1)q = N - q}.$$

Proof, concluded

$$(k^{rt}-1)\big(A'+m(k^t-1)\big)\equiv 0 \pmod{N-q}.$$

If $rt = \text{order}_k(N-q)$ then $k^{rt}-1 \equiv 0 \pmod{(k^t-1)q}$ and the above equation is satisfied. So after taking $\text{order}_k(N-q)$ steps all elements are back to where they started so cycle lengths divide $\text{order}_k(N-q)$.

For the special case $x = 1$ ($A' = 1$ and $m = 0$) this reduces to

$$k^{rt} \equiv 1 \pmod{N-q},$$

So cycle containing 1 must be of size $\text{order}_k(N-q)$. □

What happens when $\gcd(q, k) \neq 1$?

????

Example when $N = 24$ and $k = 6$

n	0	1	2	3	4	5	6	7	8	9	10	11
$\varphi(n)$	0	1	4	5	6	7	1	2	5	6	7	8

n	12	13	14	15	16	17	18	19	20	21	22	23
$\varphi(n)$	1	2	3	4	7	8	2	3	4	5	8	9

The resulting shuffling poset has cycles of lengths 1 and 3.