Combinatorics of shuffle products
(or how to shuffle a deck of cards)

Matthieu Josuat-Vergès

Laboratoire d'Informatique Gaspard Monge, Université Paris-Est Marne-la-Vallée

Journées du GDR IM
Enumerative problems arise in various contexts:

- discrete probability and statistical physics (compute probabilities in a discrete Markov chain)
- discrete geometry (counting integer points in polytopes)
- algebra and representation theory (count the multiplicity of an irreducible representation in a representation)
- many more examples
Counting problems

▶ **Exact formulas.** Dyck paths, binary trees:

\[
\frac{1}{n+1} \binom{2n}{n}
\]

▶ **Generating functions.** Alternating permutations such as 7162534,

\[
\tan(z) = \frac{\sin(z)}{\cos(z)} = z + 2\frac{z^3}{3!} + 16\frac{z^5}{5!} + 272\frac{z^7}{7!} + \ldots
\]

▶ **Asymptotic formulas.** Integer partitions such as 9 = 4 + 3 + 1 + 1.

\[
p(n) \sim \frac{1}{4n\sqrt{3}} e^{\pi \sqrt{2n/3}} \text{ as } n \to \infty
\]
Bijective problems:
Find bijections between sets with the same cardinality. Prove combinatorial identities by bijections, such as

\[
\sum_{j=0}^{k} \binom{a}{j} \binom{b}{k-j} = \binom{a+b}{k}.
\]

Structural problems: partially ordered sets, group actions on set and related symmetries...
The computational side

- **Experimentation**: software such as SageMath can be used to manipulate combinatorial objects, make new conjectures, give evidence to old conjectures.

- **Proofs**: often the “generic” case of a proof is done by reasoning, leaving a finite number of cases to be checked by computer.

- **Algorithms**: some combinatorial construction have a strong algorithmic flavor.
Shuffle of a deck of cards

Definition
A \textit{shuffle} of a sequence is done by:
1) splitting it in two parts,
2) create a new sequence containing the two parts, keeping their relative order.

Example

\begin{align*}
165482973 & \rightarrow 1654 | 82973 \rightarrow 182697543 \\
\end{align*}

A permutation $\sigma_1 \ldots \sigma_n$ of $1 \ldots n$ is a shuffle of $1 \ldots n$ if there is at most one $i$ such that $i + 1$ is to its left. For example, 41256738.

The number of (nontrivial) shuffles of $1 \ldots n$ is $2^n - n - 1$. 
Perfect shuffles

Here we assume $n$ is even. A perfect shuffle is when you split a deck in two equal parts, and combine the cards in an alternating way. It has two variants:

$$\pi_1 : 12345678 \rightarrow 15263748$$
$$\pi_2 : 12345678 \rightarrow 51627384.$$  

Formally, $\pi_i$ is in the symmetric group $\mathfrak{S}_n$, and a permutation $\sigma$ acts on words by $\sigma \cdot (a_1 \ldots a_n) = a_{\sigma^{-1}(1)} \ldots a_{\sigma^{-1}(n)}$. 
Perfect shuffles

Theorem (Elmsley)

You can move a chosen card $i$ in top position of the deck in $\lfloor \log_2 n \rfloor$ operations, where each operation is $\pi_1$ or $\pi_2$. 

Suppose $n = 2^k$, number the cards from 0 to $n-1$, represent $i$ by its binary expansion $a_1 \ldots a_k$. Then the perfect shuffles are:

$\pi_1$: $a_1 \ldots a_k \rightarrow a_2 \ldots a_k a_1$

$\pi_2$: $a_1 \ldots a_k \rightarrow a_2 \ldots a_k a_1$ ($a_1 = 1 - a_1$).

You can use this to get 0\ldots0 in $k$ steps.
Perfect shuffles

Theorem (Elmsley)

You can move a chosen card $i$ in top position of the deck in $\lfloor \log_2 n \rfloor$ operations, where each operation is $\pi_1$ or $\pi_2$.

Suppose $n = 2^k$, number the cards from 0 to $n - 1$, represent $i$ by its binary expansion $a_1 \ldots a_k$. Then the perfect shuffles are:

$$
\pi_1 : a_1 \ldots a_k \to a_2 \ldots a_k a_1
$$

$$
\pi_2 : a_1 \ldots a_k \to a_2 \ldots a_k \overline{a_1}
$$

($\overline{a_1} = 1 - a_1$). You can use this to get 0\ldots0 in $k$ steps.
Perfect shuffles

Diaconis, Graham, Kantor (1983) computed the group generated by the perfect shuffles $\pi_1$ and $\pi_2$.

When $n = 24$, the answer involves one of the sporadic finite simple groups, the Mathieu group $M_{12}$.

They relate perfect shuffle with parallel computing and an $O(\log n)$ fast Fourier transform algorithm.

Let $\omega_n$ denote the order of $\pi_1$ when there are $2n$ cards. This is the order of 2 in the ring of integers modulo $2n − 1$. Very little is known about this sequence, number theory is involved.
Perfect shuffles

There exists other types of perfect shuffles. The *Monge perfect shuffle* is done by reversing one set of cards before mixing the two sets:

$$12345678 \mapsto 18273645$$

Cf. Lachal 2010: computations of the periods of this shuffles (and its variants) via arithmetic.
Riffle shuffle

A riffle shuffle is done by choosing uniformly one shuffle among the $2^n - n - 1$ shuffles of $1, \ldots, n$, and permute the deck of cards accordingly.

Remark
There are effective ways to describe this operation. Begin by splitting the deck of $n$ cards in two sets, according to a binomial distribution: the probability to get sets of size $k$ and $n - k$ is $\binom{n}{k} \frac{1}{2^n}$.

Then choose uniformly a $k$-element subset of $1 \ldots n$ which will give the positions of cards in the first set.

(To avoid trivial shuffles... repeat the operation until you get a nontrivial shuffle !)
Riffle shuffle

Even more, there is a practical way to choose a random subset of size \( k \) among the \( \binom{n}{k} \) choices.

At each step, there are \( i \) (resp. \( j \)) cards remaining cards in the first set (resp. second set). Then the next card you pick is from set 1 with probability \( i/(i+j) \) and from set 2 with probability \( j/(i+j) \).

Start with \((i,j) = (k, n-k)\) and finish when \( i = j = 0 \).
Riffle shuffle

Problem
Take a deck 52 cards, perfectly sorted. How many shuffles do you need to perform to get a randomly sorted deck?

Theorem
*In a “human” situation, 7 is more than enough.*


The formalization of the problem comes from:

It leads to consider a Markov chain on the symmetric group $S_{52}$. 
Riffle shuffle

Given a sequence \((a_1, \ldots, a_n)\), and a permutation \(\sigma \in \mathfrak{S}_n\), the action of \(\sigma\) is

\[
\sigma \cdot (a_1, \ldots, a_n) = (a_{\sigma^{-1}(1)}, \ldots, a_{\sigma^{-1}(n)}).
\]

**Definition**

A descent of a permutation \(\sigma \in \mathfrak{S}_n\) is an index \(1 \leq i \leq n - 1\) such that \(\sigma(i) > \sigma(i + 1)\).

**Lemma**

A shuffle is the action of a permutation \(\sigma \in \mathfrak{S}_n\) with only one descent.

For example, \(147823569 \cdot 165482973 = 182697543\).
Remark
A permutation \(\sigma_1 \ldots \sigma_n\) can be seen in two different ways:
- it is a deck of cards (upon numbering cards from 1 to \(n\)),
- it acts on deck of cards by permuting cards.

The second point of view is natural to compose permutations. But we want to avoid using the huge group \(S_n!\).

We need to identify the permutation \(\sigma\) with the “translation” \(\tau \mapsto \tau \sigma^{-1}\).
The group algebra

It is convenient to work in the *group algebra* \( \mathbb{Z}[\mathfrak{S}_n] \). Its elements are formal sums of permutations with integers coefficients.

**Remark**

An element \( \sum_{\sigma \in \mathfrak{S}_n} a_{\sigma} \sigma \) where \( a_{\sigma} \geq 0 \) naturally gives a probability distribution on \( \mathfrak{S}_n \) by:

\[
P(\sigma) = \frac{a_{\sigma}}{\sum a_{\sigma}}.
\]

Think of \( a_{\sigma} \) as a “non-normalized” probability.

Consider the sum of all shuffles:

\[
E_1 = \sum_{\sigma \in \mathfrak{S}_n} \sigma \quad \sigma \text{ has 1 descent}
\]
The group algebra

Proposition

Consider the expansion

\[ E_1^k = \sum_{\sigma \in \mathfrak{S}_n} A_{k,\sigma} \sigma. \]

then \( A_{k,\sigma} \) is the number of ways to get \( \sigma \) from 1, 2, 3, \ldots, n after \( k \) shuffles.

So \( A_{k,\sigma}/(\sum A_{k,\sigma}) \) is the probability to get \( \sigma \) after \( k \) (uniformly chosen) shuffles applied to 123 \ldots n.

Proof.

By definition, \( A_{k,\sigma} \) is the number of factorizations \( \sigma = \sigma_1 \cdots \sigma_k \) where each \( \sigma_i \) has 1 descent. And \( \sum A_{k,\sigma} \) is the number of \( k \)-tuples of permutations with 1 descent.
The Eulerian algebra

Theorem (Loday, 1994)

The elements

\[ E_k = \sum_{\sigma \in S_n, \text{k descents}} \sigma \quad \text{for} \quad 0 \leq k \leq n - 1, \]

linearly span a n-dimensional subalgebra of \( \mathbb{Z}[S_n] \).

It is called the descent algebra. This means there is an expansion

\[ E_i E_j = \sum_k c_k E_k. \]

So computing \( E_1^k \) can be done in a n-dimensional vector space!
This algebra is named after the *Eulerian numbers*. They are integers $A_{n,k}$ counting the number of permutations in $\mathfrak{S}_n$ with $k$ descents. In particular $A_{n,k}$ is the number of terms in the sum $E_k$.

Generating function: $\sum_{k,n \geq 0} A_{n,k} z^n t^k = \frac{t - 1}{t - e(t-1)z}$. 

1
1 1
1 4 1
1 11 11 1
1 26 66 26 1
: : : :
Theorem

The Eulerian algebra has a basis of orthogonal idempotents, i.e. a linear basis $(P_i)_{1 \leq i \leq n}$ such that $P_i P_j = \delta_{i,j} P_i$.

One of the idempotents is $\frac{1}{n!} \sum_{\sigma \in \mathcal{S}_n} \sigma$. It represents the uniform probability distribution on $\mathcal{S}_n$.

If $E_1 = \sum a_i P_i$ then $E_1^k = \sum a_i^k P_i$. We can get the rate of convergence to the uniform distribution!
Some bijective problems, coming from the Eulerian algebra:

If $\sigma, \tau$ have the same number of descents, find a bijection between:

- factorizations $\sigma = \alpha \beta$ where $\text{des}(\alpha) = i$, $\text{des}(\beta) = j$, and
- factorizations $\tau = \alpha \beta$ where $\text{des}(\alpha) = i$, $\text{des}(\beta) = j$.

(This proves the existence of the algebra.)

For each $\sigma \in S_n$, find a bijection between:

- factorizations $\sigma = \alpha \beta$ where $\text{des}(\alpha) = i$, $\text{des}(\beta) = j$, and
- factorizations $\sigma = \alpha \beta$ where $\text{des}(\alpha) = j$, $\text{des}(\beta) = i$.

(This shows the commutativity.)

Thanks for your attention.