Math & Magic

Tom Koornwinder and Dick Koornwinder

thkmath@xs4all.nl, dick.koornwinder@gmail.com

https://staff.fnwi.uva.nl/t.h.koornwinder/

Young ORTEC lunch lecture, ORTEC, Zoetermeer, 9 September 2025

Last modified: 11 September 2025

The Koornwinder family is not from the street but . . .

from the lane (in Berkel near Rotterdam).

Vedastus Coornwinder, reverend in Berkel during 1587–1607.

His son David is even in the Louvre:

portrait of David Coornwinder († 1623)

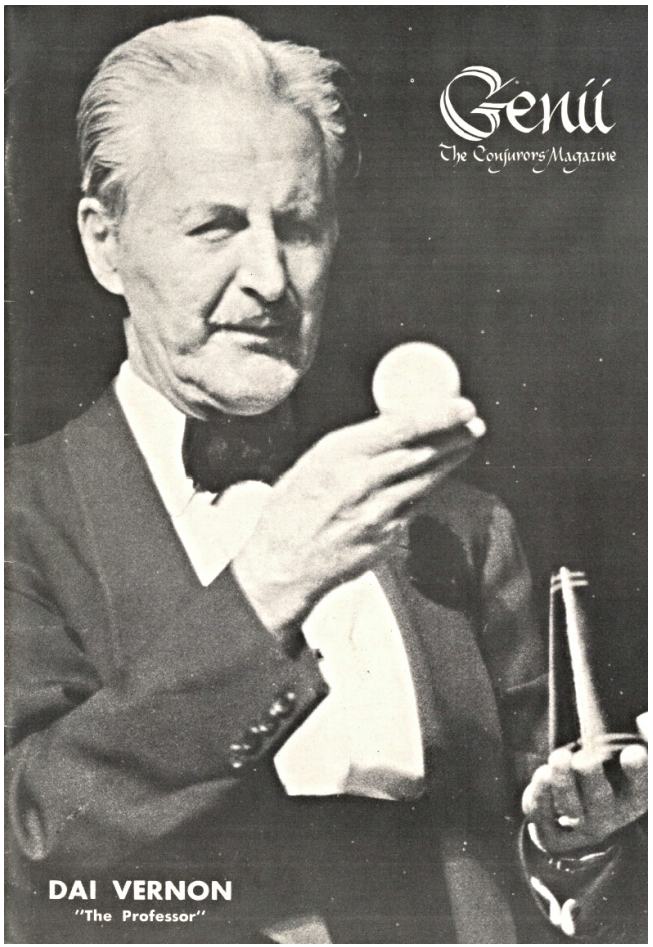
- Descendants of David took important public positions in Berkel and Hazerswoude.
- Later generations were simple farmers or shopkeepers.
- Hendrik Koornwinder started in 1892 in Rotterdam a carpentry and handcart rental shop.

- His sons Arie, Gerrit and Dik continued the carpentry shop.
- Tom is a son of Arie. Dick is a son of Dik.

Our hero Persi Diaconis

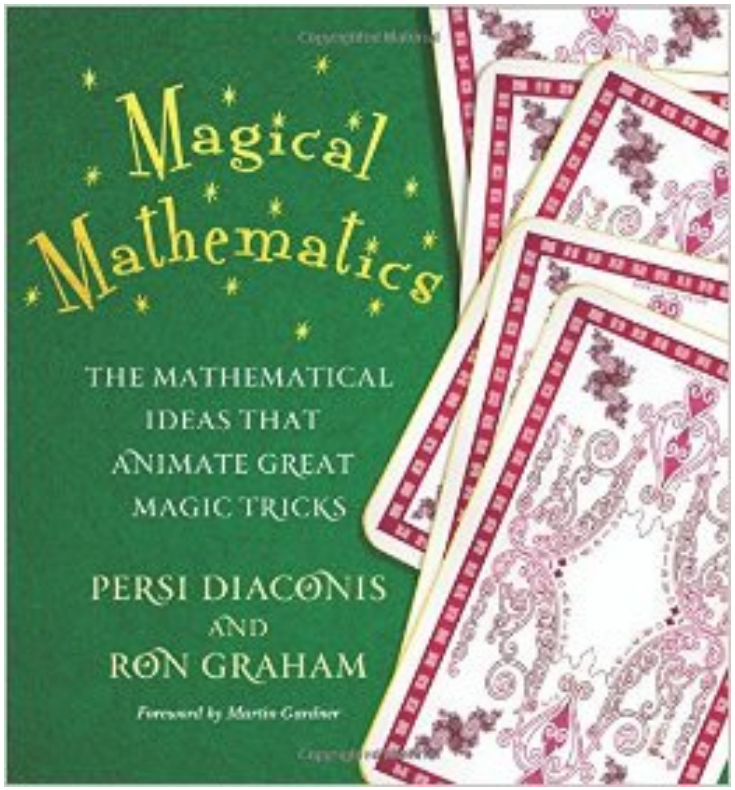
Diaconis left home at 14 to travel with sleight-of-hand legend Dai Vernon.

Persi Diaconis



Dai Vernon, “The Professor”

Later Persi Diaconis became a professor of mathematics at Stanford University.

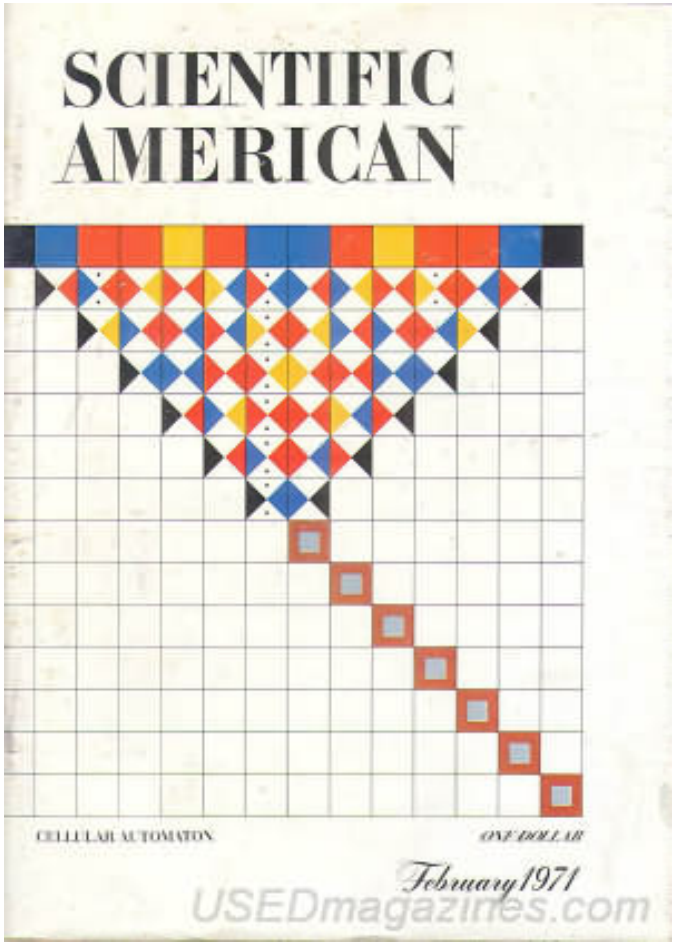


Persi Diaconis & Ron Graham,
Magical Mathematics,
Princeton University Press, 2012

Persi Diaconis and Jason Fulman,
The Mathematics of Shuffling Cards,
American Math. Society, 2023

Another hero: Martin Gardner

Martin Gardner



Mathematical recreations

Plan:

- Gilbreath Principle for Riffle Shuffle
- Faro or Perfect Shuffles
- Down-and-Under Shuffle

Gilbreath Principle (1958)

young Norman Gilbreath

in-the-hands riffle shuffling

Gilbreath Principle (1958)

Definition A set of two piles of cards has *Property P2* if (i) the total number of cards is even, (ii) in both piles red (R) and black (B) cards alternate, and (iii) the upper cards in the two piles have different colour.

Theorem Given is a set of two piles having Property P2. Riffle shuffle them together. From the resulting pile repeatedly take off the top two cards. Each such pair has an R and a B.

Proof The top two cards after the riffle shuffle are:
- either the top two cards of pile 1,
- or the top two cards of pile 2,
- or the top cards of pile 1 and 2.

In all cases an R and a B. The original two piles with two cards taken off as just listed still have Property P2. Riffle shuffling of these two piles yields the original resulting pile with the top two cards taken off. □

Generalized Gilbreath Principle

Definition A set of two piles of cards has *Property Pk* if (i) the total number of cards is a multiple of k, and (ii) numbers $\pmod k$ in the first pile are $j+1, j+2, \ldots$, and in the second pile $j, j-1, j-2, \ldots$.

Theorem Given is a set of two piles having Property Pk. Riffle shuffle them together. From the resulting pile repeatedly take off the top k cards. In each such set the cards are distinct $\pmod k$.

Proof The top k cards after the riffle shuffle are, for some j, the top j cards of the first pile and the top $k-j$ cards of the second pile. They are all distinct $\pmod k$. After these k cards were taken off from the two piles, these still satisfied Property *Pk*. The original resulting pile with the top k cards taken off can be seen as the result of some riffle shuffle of the original two piles with k cards taken off from their tops. □

Application Prepare a deck of cards with successively club, diamond, heart, spade, and so on. Cut several times, deal part of the deck as a second pile, and riffle shuffle the piles. Each next four top cards will have all four suits.

Permutations

Definition

A *permutation* is a one-to-one map σ of $\{1, 2, \ldots, n\}$ onto itself, notated as

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}.$$

Example: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$

Definition (Gilbreath permutation)

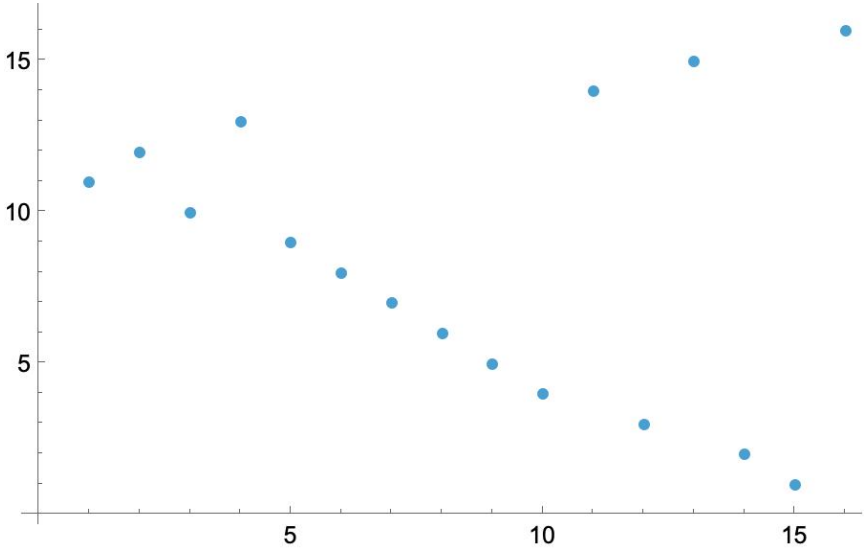
This is a permutation of $\{1, 2, \ldots, n\}$ obtained by applying a riffle shuffle to $j+1, j+2, \ldots, n-1, n$ and $j, j-1, \ldots, 2, 1$.

Example: $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 \longrightarrow$

$$\left\{ \begin{matrix} 11, 12, 13, 14, 15, 16 \\ 10, 9, 8, 7, 6, 5, 4, 3, 2, 1 \end{matrix} \right\} \longrightarrow$$

$11, 12, 10, 13, 9, 8, 7, 6, 5, 4, 14, 3, 15, 2, 1, 16.$

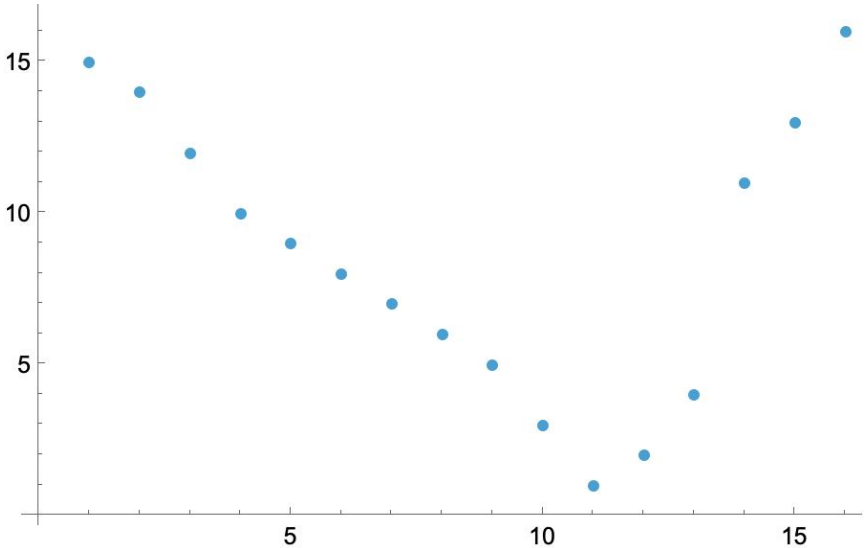
$\sigma: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 \longrightarrow$
$11, 12, 10, 13, 9, 8, 7, 6, 5, 4, 14, 3, 15, 2, 1, 16$



For each k the set $\{\sigma(1), \sigma(2), \ldots, \sigma(k)\}$ consists of k consecutive numbers.

There are 2^{n-1} permutations of this type. (Here $n = 16$.)

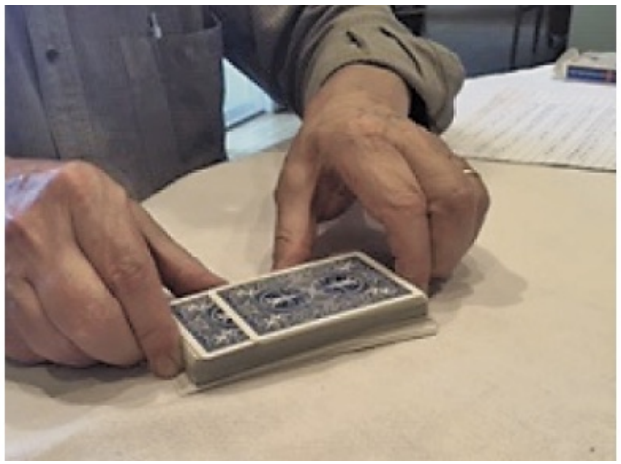
$\sigma^{-1}: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 \longrightarrow$
$15, 14, 12, 10, 9, 8, 7, 6, 5, 3, 1, 2, 4, 11, 13, 16$



Unimodal permutation:
The graph of σ^{-1} first descends to a minimum and then ascends.

Faro or perfect shuffle





Cut a deck of $2n$ cards exactly in half and then riffle the two piles of n cards together so that the cards from the two piles alternate perfectly.

There are two versions:

- An *out-shuffle*, where the original top card is outside (remains the top card)
- An *in-shuffle*, where the original top card goes inside (the top card from the second pile is the new top card).

out-shuffle: $0, 1, 2, \ldots, 2n-1 \longrightarrow$

$$\begin{Bmatrix} 0 & 1 & \ldots & n-1 \\ n & n+1 & \ldots & 2n-1 \end{Bmatrix} \longrightarrow 0, n, 1, n+1, \ldots, n-1, 2n-1$$

in-shuffle: $0, 1, 2, \ldots, 2n-1 \longrightarrow$

$$\begin{Bmatrix} 0 & 1 & \ldots & n-1 \\ n & n+1 & \ldots & 2n-1 \end{Bmatrix} \longrightarrow n, 0, n+1, 1, \ldots, 2n-1, n-1$$

out-shuffle: $0, 1, 2, \ldots, 2n-1 \longrightarrow 0, n, 1, n+1, \ldots, n-1, 2n-1$

$$\pi_0(k) = \begin{cases} 2k, & k = 0, 1, \ldots, n-1, \\ 2(k-n)+1, & k = n, n+1, \ldots, 2n-1. \end{cases}$$

in-shuffle: $0, 1, 2, \ldots, 2n-1 \longrightarrow n, 0, n+1, 1, \ldots, 2n-1, n-1$

$$\pi_1(k) = \begin{cases} 2k+1, & k = 0, 1, \ldots, n-1, \\ 2(k-n), & k = n, n+1, \ldots, 2n-1. \end{cases}$$

So $\pi_\varepsilon(k) = 2k + \varepsilon \quad (k < n, \varepsilon \in \{0, 1\})$.

Then for $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_j \in \{0, 1\}$ we have

$$\pi_{\varepsilon_0}\pi_{\varepsilon_1} \ldots \pi_{\varepsilon_{j-1}}\pi_{\varepsilon_j}(0) = \varepsilon_0 + 2\varepsilon_1 + 2^2\varepsilon_2 + \cdots + 2^j\varepsilon_j, \quad \text{provided} < 2n.$$

Hence, if we want to reach p from 0 with in-shuffles and out-shuffles, then we write p as a binary number $p = \varepsilon_j\varepsilon_{j-1} \ldots \varepsilon_1\varepsilon_0$ and successively apply $\pi_{\varepsilon_j}, \pi_{\varepsilon_{j-1}}, \ldots, \pi_{\varepsilon_1}, \pi_{\varepsilon_0}$.

$$\pi_0(k) = \begin{cases} 2k, & k = 0, 1, \ldots, n-1, \\ 2(k-n)+1, & k = n, n+1, \ldots, 2n-1, \end{cases}$$

$$\pi_1(k) = \begin{cases} 2k+1, & k = 0, 1, \ldots, n-1, \\ 2(k-n), & k = n, n+1, \ldots, 2n-1. \end{cases}$$

$$\pi_0(k) + \pi_0(2n-1-k) = 2n-1,$$
$$\pi_1(k) + \pi_1(2n-1-k) = 2n-1.$$

Theorem

In-shuffles and out-shuffles preserve centrally symmetric pairs of cards.

Number of out-shuffles required to recycle $2n$ cards:

Deck size	2	4	6	8	10	12	14	16	18
Number of shuffles	1	2	4	3	6	10	12	4	8

Deck size	20	22	24	26	28	30	32	34	36
Number of shuffles	18	6	11	20	18	28	5	10	12

Deck size	38	40	42	44	46	48	50	52
Number of shuffles	36	12	20	14	12	23	21	8

Theorem

A deck of $2n$ cards takes its original order after k in-shuffles, where k is the smallest integer such that $2^k = 1 \pmod{2n+1}$.

Corollary

A deck of $2n$ cards takes its original order after k out-shuffles, where k is the smallest integer such that $2^k = 1 \pmod{2n-1}$.

Clearly, if $2n = 2^r$ then r is the smallest value of k such that $2^k = 1 \pmod{2^r - 1}$, so a deck of 2^r cards recycles after r out-shuffles.

If $n = 52$ then $2^8 = 256 = 5 \times 51 + 1 = 1 \pmod{52 - 1}$, while $2^r - 1$ is not a multiple of 51 for $1 \leq r \leq 7$. So a deck of 8 cards recycles after 8 out-shuffles.

$\phi(m) := |\{j \in \{1, 2, \ldots, m-1\} \mid (j, m) = 1\}|$ (Euler's totient function)

$2^{\phi(m)} = 1 \pmod{m}$, m odd (Fermat–Euler theorem)

So a deck of $2n$ cards first recyles after k in-shuffles with k a certain divisor of $\phi(2n+1) \leq 2n$, and it first recycles after k out-shuffles with k a certain divisor of $\phi(2n-1) \leq 2n-2$.

If p is an odd prime then $\phi(p) = p - 1$.
By the Artin conjecture there are infinitely many odd primes p such that $2^k \neq 1 \pmod{p}$ for $k < p - 1$.
The Artin conjecture would follow from the generalized Riemann hypthesis.

So magical tricks are related to deep mathematics!

Down-and-under shuffle or Australian shuffle

From a packet of n cards place its top card **down** on the table, its next card **under** on the bottom of the packet, the next down, the next under, and so on, until just one card remains.

$$
\begin{array}{rl}
1, 2, 3, 4, 5, 6, \ldots, n & \\
3, 4, 5, 6, \ldots, n, 2 & 1 \\
5, 6, \ldots, n, 2, 4 & 3, 1 \\
\ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots \\
i_1, i_2 & j_1, j_2, \ldots, 3, 1 \\
i_2 & i_1, j_1, j_2, \ldots, 3, 1
\end{array}
$$

What is the card i_2 that remains?

Theorem

The down-and-under shuffle applied to $\{1, 2, \ldots, n\}$ *gives as the last remaining card* $k = 2(n - 2^r)$*, where* $2^r < n \leq 2^{r+1}$*.*

About the trick

- After a cut of cards $\{1, 2, \ldots, 2n\}$ two cards i, j which are n places apart from each other still satisfy $i - j = \pm n$.
- After repeated cutting take the top card i apart. Then the central card j on place n in the $2n - 1$ remaining cards will be $j = i \pm n$.
- The down-and-under shuffle of $\{1, 2, \ldots, 2n - 1\}$ yields n as the last remaining card iff $n = 2(2n - 1 - 2^r)$, so $n = \frac{2}{3}(2^r + 1)$.
- Then n is integer iff 3 divides $2^r + 1$. This is the case iff r is odd.
- Indeed, $2^r + 1 = (3 - 1)^r + 1 = (-1)^r + 1 \pmod 3$,
- For example:

  $r = 1$, $n = 2$, $2n - 1 = 3$;

  $r = 3$, $n = 6$, $2n - 1 = 11$;

  $r = 5$, $n = 22$, $2n - 1 = 43$.

Proof of Theorem If n is odd then the bottom card becomes the top card after $\frac{1}{2}(n-1)$ steps, so it will go down in the next step, and therefore it can never become the last remaining card.

If n is even then the bottom card becomes the top second card after $\frac{1}{2}n-1$ steps, so it will be the bottom card of a pile of $\frac{1}{2}n$ cards after the $\frac{1}{2}n$-th step.

Then repeat this reasoning: depending on $\frac{1}{2}n$ being odd or even, the bottom card will eventually go down or under, respectively. Only if $n=2^r$ for some positive integer r, the card will end as the last remaining card.

Now let k be the last remaining card. Then k cannot be odd, for then it would have beome the top card after $\frac{1}{2}(k-1)$ steps and next have gone down. So k is even. It came after $\frac{1}{2}k-1$ steps on the top second place, and thus after $\frac{1}{2}k$ steps on the bottom of a pile of $n-\frac{1}{2}k$ cards. Since it will be the last remaining card, $n-\frac{1}{2}k=2^r$, so $k=2(n-2^r)$. Furthermore, $\frac{1}{2}n \leq n-\frac{1}{2}k < n$, so $2^r < n \leq 2^{r+1}$. □

Tom and Dick thank you for your attention.

Credits

The photo of Norman Gilbreath on p.9 is from the journal *The Linking Ring* (1958).
The shuffling photos on pp. 9 and 14 and the table on p.18 are from the book *The Mathematics of Shuffling Cards* by Diaconis & Fulman.

The shuffling photos on p.20 are from the book *Magical Mathematics* by Diaconis & Graham.