MATH. SCAND. 98 (2006), 5–11

THE MONGE SHUFFLE FOR TWO-POWER DECKS

ARNE LEDET

Abstract

We consider the so-called Monge shuffle for a deck with 2^k cards, and describe the permutation group generated by the two different Monge shuffles.

Introduction

The *Monge shuffle* – named after Gaspard Monge (1746–1818), who wrote about it in 1773 – is a method for shuffling a deck of cards, in which the cards are taken off the top of the deck (held in one hand) and placed in the other hand alternately on the top and bottom of the packet held there. Thus, if we imagine that the deck has been sorted (from top to bottom) as

♠A, ♠2, ♠3, ♠4, ♠5, ♠6, ♠7, ♠8, ♠9, ♠10, ♠J, ♠Q, ♠K,
◇A, ◇2, ◇3, ◇4, ◇5, ◇6, ◇7, ◇8, ◇9, ◇10, ◇J, ◇Q, ◇K,
♣A, ♣2, ♣3, ♣4, ♣5, ♣6, ♣7, ♣8, ♣9, ♣10, ♣J, ♣Q, ♣K,
♡A, ♡2, ♡3, ♡4, ♡5, ♡6, ♡7, ♡8, ♡9, ♡10, ♡J, ♡Q, ♡K,

a Monge shuffle will put the cards in the following order:

♡K, ♡J, ♡9, ♡7, ♡5, ♡3, ♡A, ♣Q, ♣10, ♣8, ♣6, ♣4, ♣2,
◇K, ◇J, ◇9, ◇7, ◇5, ◇3, ◇A, ♠Q, ♠10, ♠8, ♠6, ♠4, ♠2,
♠A, ♠3, ♠5, ♠7, ♠9, ♠J, ♠K, ◇2, ◇4, ◇6, ◇8, ◇10, ◇Q,
♣A, ♣3, ♣5, ♣7, ♣9, ♣J, ♣K, ♡2, ♡4, ♡6, ♡8, ♡10, ♡Q,

If we simply number the cards $1, \dots, 52$, this permutation can be written in cycle notation as

$$\begin{gathered}(1, 27, 40, 7, 30, 12, 21, 37, 45, 49, 51, 52) \times \\ (2, 26, 14, 20, 17, 35, 44, 5, 29, 41, 47, 50)(3, 28, 13, 33, 43, 48) \times \\ (4, 25, 39, 46)(6, 24, 15, 34, 10, 22, 16, 19, 36, 9, 31, 42) \times \\ (8, 23, 38)(11, 32).\end{gathered}$$

Received July 14, 2004.

Hence, twelve successive Monge shuffles will return the deck to its original order. (This is at best of theoretical interest, though, since actually performing a Monge shuffle on an ordinary deck of cards is rather slow and tedious.) Also, 18 is a fixed point.

REMARK. The Monge shuffle is considered for an even-numbered deck in [6, pp. 245–247], as well as in [1, Ch. XI]. Both accounts include proofs of Proposition 1 below, and in addition Ball gives many references to earlier (mostly nineteenth-century) papers. A brief description can also be found in [3, pp. 321–323]. An alternative way to approach the Monge shuffle, again with a proof of Proposition 1, is given in [5, §4], which also provides a way of determining the cycle structure of the shuffle.

Basic results

A Monge shuffle of an odd-numbered deck leaves the bottom card in place, whereas a Monge shuffle of an even-numbered deck moves the bottom card to the top. In the case of an odd-numbered deck, we can therefore simply ignore the bottom card.

Now, let n be even, and number the n-card deck as $1, 2, \dots, n-1, n$, with 1 being the bottom card. The Monge shuffle is then the permutation

$$\begin{array}{rlrl} 1 &\mapsto n, & 2 &\mapsto 1, \\ 3 &\mapsto n-1, & 4 &\mapsto 2, \\ 5 &\mapsto n-2, & 6 &\mapsto 3, \\ &\vdots & &\vdots \\ n-1 &\mapsto \frac{1}{2}n+1, & n &\mapsto \frac{1}{2}n. \end{array}$$

The trick to dealing with the Monge shuffle (see [2, §5]) is to look at the inverse instead: This is the permutation

$$\begin{array}{rlrl} 1 &\mapsto 2, & \frac{1}{2}n+1 &\mapsto n-1, \\ 2 &\mapsto 4, & \frac{1}{2}n+2 &\mapsto n-3, \\ 3 &\mapsto 6, & \frac{1}{2}n+3 &\mapsto n-5, \\ &\vdots & &\vdots \\ \frac{1}{2}n &\mapsto n, & n &\mapsto 1. \end{array}$$

The first column here is just multiplication by 2, whereas the second column is multiplication by -2 modulo $2n+1$.

Consequently, if we identify a and $-a$ in $\mathsf{Z}/(2n+1)$, the inverse Monge shuffle is just multiplication by 2, and we have

PROPOSITION 1. *For an even number n, the order of the n-card Monge shuffle equals the order of* 2 *in* $(\mathsf{Z}/(2n+1))^*/\pm 1$, *i.e., it is the smallest positive k for which* $2^k \equiv \pm 1 \pmod{2n+1}$.

The sign of the n-card Monge shuffle (n even) is $(-1)^{n/2}$.

The following table lists the order of the Monge shuffle for even-numbered decks of up to 104 cards:

n	$\lvert m\rvert$	n	$\lvert m\rvert$	n	$\lvert m\rvert$	n	$\lvert m\rvert$
2	2	28	9	54	18	80	33
4	3	30	30	56	14	82	20
6	6	32	6	58	12	84	78
8	4	34	22	60	55	86	86
10	6	36	9	62	50	88	29
12	10	38	30	64	7	90	90
14	14	40	27	66	18	92	18
16	5	42	8	68	34	94	18
18	18	44	11	70	46	96	48
20	10	46	10	72	14	98	98
22	12	48	24	74	74	100	33
24	21	50	50	76	24	102	10
26	26	52	12	78	26	104	45

The Monge shuffle group

For a given n, there are two (equivalent) n-card Monge shuffles, depending on how the deck is held in the hand – face up or face down. Or, purely as permutations, whether the cards are numbered from top to bottom or from bottom to top.

For an even-numbered deck, one of these is

$$\begin{array}{rlrl} 1 &\mapsto n, & 2 &\mapsto 1, \\ 3 &\mapsto n-1, & 4 &\mapsto 2, \\ 5 &\mapsto n-2, & 6 &\mapsto 3, \\ &\vdots & &\vdots \\ n-1 &\mapsto \frac{1}{2}n+1, & n &\mapsto \frac{1}{2}n, \end{array}$$

as before, whereas the other is

$$\begin{aligned} n &\mapsto 1, & n-1 &\mapsto n, \\ n-2 &\mapsto 2, & n-3 &\mapsto n-1, \\ n-4 &\mapsto 3, & n-5 &\mapsto n-2, \\ &\vdots & &\vdots \\ 2 &\mapsto \tfrac{1}{2}n, & 1 &\mapsto \tfrac{1}{2}n+1. \end{aligned}$$

Let us denote these by m_1 and m_2, respectively. They generate a subgroup M_n of S_n.

Example. Consider this 'Monge shuffle group' for a six-card deck. Here,

$$m_1 = (1,6,3,5,4,2), \quad m_2 = (1,4,2,3,5,6).$$

It follows immediately that M_6 is transitive. Also,

$$m_1 \circ m_2 = (1,2,5,3,4) \quad \text{and} \quad m_1^2 \circ m_2 = (2,4,6,3),$$

from which we conclude that $[S_6 : M_6] \mid 6$. Since there are no subgroups of S_6 of index 3, and since M_6 is not an even subgroup, we must therefore have $M_6 = S_6$ or $M_6 \simeq S_5$.

Checking the conjugates of $m_1 \circ m_2$ under powers of m_1 and m_2 shows that the 5-Sylow subgroup generated by $m_1 \circ m_2$ has only six conjugates in M_6. As S_6 has more than six 5-Sylow subgroups, we conclude that $M_6 \simeq S_5$.

Remark. In [2], another group of Monge shuffles is briefly considered: There, the second Monge shuffle differs from the first by depositing the second card *underneath* the first, rather than on top of it.

If we let r denote the permutation of the deck that reverses the order of the cards, it is clear that $m_2 = r \circ m_1 \circ r$. Also, the two Monge shuffles considered by Diaconis & al. are then m_1 and $r \circ m_1$. Thus, the two 'Monge shuffle groups' coincide if and only if $r \in M_n$. This appears to be the case for 'most' n, although not for all: We prove in the next section that $r \notin M_n$ when $n = 2^k$ for k odd and > 1. Computational evidence (i.e., a half-hundred cases checked by brute force with Maple 7) suggests that these may be the only exceptions.

Powers of two

We will consider the case $n = 2^k$, where the group M_n turns out to be fairly small.

First a trivial observation, also made in [1]:

Lemma. *A Monge shuffle on a 2^k-card deck has order $k+1$.*

This is clear, since of course 2^{k+1} is the smallest power of 2 that is $\equiv \pm 1 \pmod{2^{k+1}+1}$.

We can also note that if $N > 2^k$, then the N-card Monge shuffle has order $> k+1$.

Proposition 2. *Let $n = 2^k$ be a power of 2. Then*

$$M_n \simeq \mathsf{F}_2^{2\lfloor k/2 \rfloor} \rtimes C_{k+1}.$$

(Here, $\lfloor x \rfloor$ denotes the largest integer $\leq x$, and C_d is the cyclic group of order d.)

Proof. Inspired by the case of the Faro shuffle (see [2, Lemma 4]), we number the cards from 0 through $2^k - 1$ and represent them in binary. We then interpret the binary expansion as a vector in F_2^k, i.e., if

$$b = \sum_{i=0}^{k-1} b_i 2^i$$

with $b_i \in \{0, 1\}$, we associate to it the vector

$$\mathbf{b} = (\bar{b}_{k-1}, \dots, \bar{b}_0) \in \mathsf{F}_2^k.$$

The actions of m_1 and m_2 are now given by

$$m_1\colon (b_{k-1}, \dots, b_1, b_0) \mapsto \begin{cases} (1, 1+b_{k-1}, \dots, 1+b_1), & b_0 = 0 \\ (0, b_{k-1}, \dots, b_1), & b_0 = 1 \end{cases}$$

and

$$m_2\colon (b_{k-1}, \dots, b_1, b_0) \mapsto \begin{cases} (1, b_{k-1}, \dots, b_1), & b_0 = 0 \\ (0, 1+b_{k-1}, \dots, 1+b_1), & b_0 = 1 \end{cases}$$

It follows that $m_2^{-1} \circ m_1$ acts as addition by $(1, 1, \dots, 1, 0)$ (on F_2^k).

We note: If f is the function on F_2^k given by addition by $(c_{k-1}, \dots, c_0)$, then $m_1 \circ f \circ m_1^{-1}$ is given by addition by $(c_0, c_0 + c_{k-1}, \dots, c_0 + c_1)$.

Consequently, M_n is the semi-direct product of a subspace of F_2^k and $C_{k+1} = \langle m_1 \rangle$, with the subspace being generated by $m_2^{-1} \circ m_1$ and its conjugates.

For $k = 1$, this means that $M_2 = C_2$.

For $k = 2$, there are three conjugates, and we get $M_4 = V_4 \rtimes C_3 = A_4$.

For $k = 3$, there are two conjugates, and we get $M_8 = V_4 \rtimes C_4$.

For $k > 3$, the conjugates of $(1, 1, \dots, 1, 0)$ are

$$(1, 1, \dots, 1, 0), \quad (0, 1, 1, \dots, 1),$$
$$(1, 1, 0, \dots, 0), \quad (0, 1, 1, 0, \dots, 0), \dots, (0, \dots, 0, 1, 1),$$

and these generate a $(k-1)$-dimensional subspace if k is odd (since the first two are obviously in the span of the remaining $k - 1$), and the entire k-dimensional space if k is even (since the first two are not in the span of the remaining $k - 1$, by a parity argument).

Corollary. (a) *A sequence of $k + 1$ Monge shuffles (in any combination) on a 2^k-card deck is an involution.*

(b) *If k is even, the group M_{2^k} contains all involutions of the form*

$$\mathbf{x} \mapsto \mathbf{x} + \mathbf{a},$$

where $\mathbf{a} \in \mathsf{F}_2^k$. In particular, it contains the permutation that reverses the order of the 2^k cards. This permutation is

$$m_1 \circ (m_2 \circ m_1)^{k/2}.$$

(c) *If $k > 1$ is odd, the group M_{2^k} contains only those involutions of the form*

$$\mathbf{x} \mapsto \mathbf{x} + \mathbf{a}$$

for which the entries in $\mathbf{a}$ add up to 0. In particular, it does not contain the permutation that reverses the order of the 2^k cards.

(d) *M_{2^k} is transitive.*

Proof. (b) The first part is clear. The second follows by writing $m_2 = m_1 \circ (m_1^{-1} \circ m_2) = m_1 \circ (m_2^{-1} \circ m_1)$.

(c) The only thing that needs proving is that $m_1^{(k+1)/2}$ is not given by addition with some $(a_{k-1}, \dots, a_0) \in \mathsf{F}_2^k$. This, however, is clear, since the image of $(0, 0, \dots, 0)$ is $(0, \dots, 0, 1, \dots, 1)$ with $(k + 1)/2$ 1's, whereas the image of $(1, 1, \dots, 1)$ is $(0, \dots, 0, 1, \dots, 1)$ with $(k - 1)/2$ 1's.

Remarks. (1) The most obvious way of 'switching' from one Monge shuffle to the other is to turn the deck over. Thus, if we have 2^k cards, with k even, performing $k + 1$ Monge shuffles, flipping the deck over between any two, will reverse the order of the cards. This is easily confirmed by hand with four or sixteen cards.

(2) It should be clear from the proof of Proposition 2 that all the involutions in M_{2^k} given by addition in F_2^k are products of $k + 1$ Monge shuffles.

(3) If k is even, the 2^{k-1}-card ‘cut’, i.e., the permutation that interchanges the top and bottom halves of a 2^k-card deck, is in M_{2^k}, and can in fact be obtained as

$$m_2 \circ (m_2 \circ m_1)^{k/2}.$$

If $k > 1$ is odd, this cut is not in M_{2^k}.

REFERENCES

1. Ball, W. W. R., *Mathematical Recreations and Essays*, (11. ed., rev. by H. S. M. Coxeter), MacMillan & Co., 1939.
2. Diaconis, P., Graham, R. L., and Kantor, W. M., *The Mathematics of perfect shuffles*, Adv. Appl. Math. 4 (1983), 175–196.
3. Kraitchik, M., *Mathematical Recreations*, 2. ed., Dover, 1953.
4. Monge, G., *Réflexions sur un tour de cartes*, Mem. Math. Phys. Acad. de Sciences Paris (1773), 390–412.
5. Roberts, J. B., *Integral power residues as permutations*, Amer. Math. Monthly 76 (1969), 379–385.
6. Uspensky, J. V., and Heaslet, M. A., *Elementary Number Theory*, McGraw-Hill, 1939.

DEPARTMENT OF MATHEMATICS AND STATISTICS
TEXAS TECH UNIVERSITY
LUBBOCK, TX 79409-1042
USA
E-mail: arne.ledet@ttu.edu