The Mathematics of the Flip and Horseshoe Shuffles

Steve Butler, Persi Diaconis, and Ron Graham

Abstract. We consider new types of perfect shuffles wherein a deck is split in half, one half of the deck is "reversed," and then the cards are interlaced. Flip shuffles are when the reversal comes from turning the half of the deck over so that we also need to account for face-up/face-down configurations, while horseshoe shuffles are when the order of the cards are reversed but all cards still face the same direction. We show that these shuffles are closely related to faro shuffling and determine the order of the associated shuffling groups. An application of this theory is given through a card trick based on applying different shuffles of eight cards.

1. INTRODUCTION. We were led to the problems in this paper by a question from a magician friend, Jeremy Rayner, who sent a picture similar to Figure 1 along with a description of a new form of perfect shuffling [**7**].

Figure 1. A deck in the process of being flip shuffled

Crooked gamblers and skillful magicians have learned to shuffle cards perfectly; cutting off exactly half the deck and riffling the two halves together so they exactly alternate. A more careful description and review of the traditional form of perfect shuffling is in Section 2. Our magician friend wanted to know what happens if one of the halves is turned face-up before shuffling. We will call this a *flip shuffle*. Figure 2 shows what happens for the (out-)flip shuffle with a 10 card deck (labeled $0, 1, \ldots, 9$ from top to bottom), and dashed lines indicate a card has been turned over.

Carefully repeating this 18 times will return the deck of 10 cards to the original order and same face-up/face-down configuration. (One of the more studied questions

http://dx.doi.org/10.4169/amer.math.monthly.123.6.542
MSC: Primary 00A08

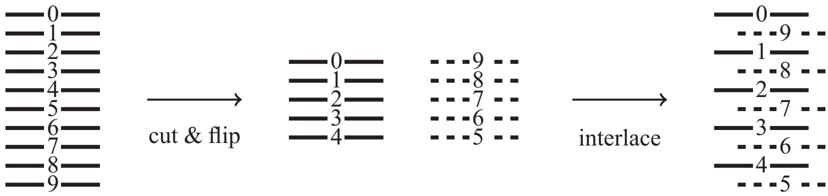


Figure 2. An out-flip shuffle with 10 cards

related to perfect shuffles is the number of times needed to return a deck to the starting order.) Our magician friend had computed by hand[1] how many shuffles were required to recycle decks of small sizes. We reproduce some of this data here (the top row is the deck size, and the bottom row is the number of shuffles needed):

4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36
3	10	4	18	11	18	5	12	12	14	23	8	20	58	6	66	35

.

It is not easy to "see" the pattern in these numbers; for example, they are not monotone (thus larger decks can recycle after fewer shuffles). The order for decks of size 2^k look suspiciously like $k + 1$. Does this pattern continue?

We note that normal perfect shuffles are not easy to perform (even for seasoned professionals), and this additional element of flipping cards over makes it even more difficult. However, it is *easy* to perform inverse shuffles. To carry out the inverse of the (out-)flip shuffle (e.g., as shown in Figure 2), we start with the deck and then deal it alternately between two piles, turning each card over before placing it on its pile. Finally, turn the entire first pile over and place it on the second pile. For the 10 card deck this process is shown in Figure 3 and the interested reader can again verify that it will take 18 of these operations to return the deck to its starting configuration.

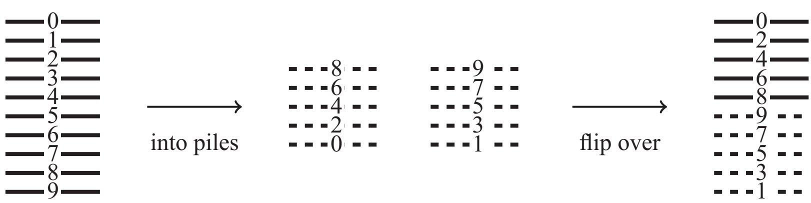


Figure 3. An inverse out-flip shuffle with 10 cards

There is a second type of flip shuffle depending on how we choose to interlace. What we have discussed so far corresponds to the *out*-flip shuffle (since the original top card remains on the *out*side). There is also an *in*-flip shuffle (where the original top card now winds up on the *in*side). The in-flip shuffle for 10 cards is shown in Figure 4. An inverse in-flip shuffle deals into two piles as before but finishes by turning the second pile over and placing it on the first pile. This is shown for 10 cards in Figure 5.

The in-flips behave differently from the out-flips, and the two can be combined in various ways to achieve different effects. This leads to the main question in the field, namely, what can be done by combining these two types of shuffles. The main result of this paper is to completely determine the number of different orderings that can be

[1]Sleight of hand?

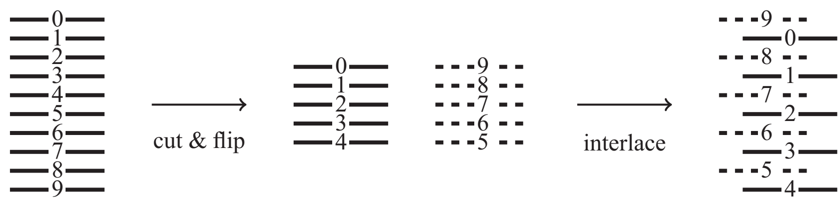


Figure 4. An in-flip shuffle with 10 cards

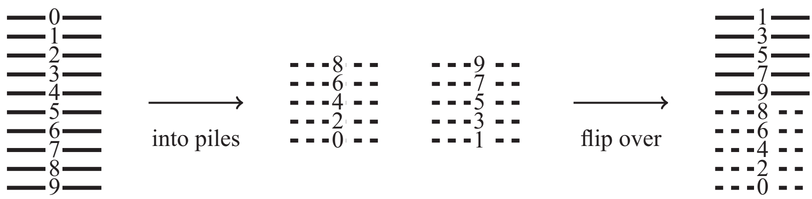


Figure 5. An inverse in-flip shuffle with 10 cards

achieved with these shuffling operations. These results give a nice application of group theory to a somewhat real problem.

We first start by doing a review of what is known for "ordinary" perfect shuffles, also known as faro shuffling in Section 2. We then address what happens for flip shuffling in Section 3. Then in Sections 4 and 5 we will look at horseshoe shuffling, a face-down only version of flip shuffling. In Section 6 we make further connections with other types of shuffling, including a way to combine these different shuffling operations together to create a card trick before finally giving concluding remarks in Section 7.

2. FARO SHUFFLING. The faro shuffle is the classic way of performing perfect shuffles. This is carried out by splitting a deck of $2n$ cards into two equal piles of size n and then perfectly interlacing the two piles. Again there are two possibilities, either the top card remains on the outside (an out-faro shuffle) or it moves to the second position (an in-faro shuffle). The two types are illustrated in Figure 6 for a deck with 10 cards.

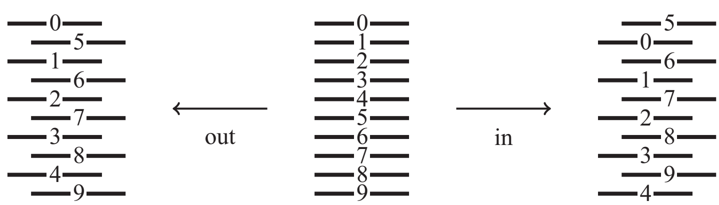


Figure 6. Examples of in- and out-faro shuffles for a deck with 10 cards

Faro shuffles are among the most well known shuffles both for mathematicians and magicians alike. For example, starting with a standard deck of 52 cards then performing eight consecutive out-faro shuffles will return the deck to the starting order. Combining these shuffles it is also possible to move the top card to any position in the deck. To do this, start at the top and label the positions as 0, 1, 2, . . . and write the desired position in binary. Now perform shuffles by reading from left to right where a "1" is an in shuffle and a "0" is an out shuffle. So for example, to move the top card into the position 20 we write 20 in binary, 10100, and perform the appropriate shuffles: in, out, in, out, out. Conversely there is a way to use in- and out-faro shuffles to move a card in any position in the deck to the top (see [**1, 6**]).

A natural question is to determine what orderings of the deck are possible, and what sequence of shuffles leads to a desirable ordering. Thinking of these shuffles as operators on the deck of cards, then this problem becomes determining the "shuffle group," i.e., the group which acts on the deck generated by the in- and out-faro shuffles. This work for faro shuffling was previously carried out (see [**3**]), and the following was determined.

Theorem 1 (Diaconis-Graham-Kantor). *Let* $\mathrm{Faro}(2n)$ *denote the shuffle group generated using in- and out-faro shuffles on a deck of* $2n$ *cards. Then the following holds:*

$$|\,\mathrm{Faro}(2n)| = \begin{cases} 2^9{\cdot}3{\cdot}5 & \text{if } 2n = 12, \\ 2^{17}{\cdot}3^3{\cdot}5{\cdot}11 & \text{if } 2n = 24, \\ k2^k & \text{if } 2n = 2^k, \\ n!2^n & \text{if } n \equiv 2 \pmod 4 \text{ and } 2n \neq 4, 12, \\ n!2^{n-1} & \text{if } n \equiv 1 \pmod 2, \\ n!2^{n-2} & \text{if } n \equiv 0 \pmod 4 \text{ and } 2n \neq 24, 2^k. \end{cases}$$

(Note $|\,\mathrm{Faro}(2n)|$ *is the number of possible arrangements of a deck of* $2n$ *cards which can be obtained by repeated applications of faro shuffles.)*

We note that the groups themselves were determined by Diaconis, Graham, and Kantor. For the exceptional cases of $2n = 12$ and 24, the corresponding groups are $S_5 \rtimes (\mathbb{Z}_2)^6$ and $M_{12} \rtimes (\mathbb{Z}_2)^{11}$, respectively, where S_5 is the symmetric group on 5 elements and M_{12} is the Mathieu group. When $2n = 2^k$, then the group is $(\mathbb{Z}_2)^k \rtimes \mathbb{Z}_k$, and this case is particularly useful for performing magic tricks (more on this later). Finally, all remaining cases correspond to subgroups of index 1, 2, or 4 of the Weyl group B_n (formed by the $2^n n!$ signed permutation matrices of order n).

An important property of faro shuffling we will make use of is "stay stack." This means that two cards which start symmetrically opposite across the center will continue to stay symmetrically opposite after performing an in- or out-faro shuffle. This can be easily checked for $2n = 10$ by examining Figure 6. In general, if we label the positions as $0, 1, 2, \ldots$, then an out-faro shuffle sends a card in position $i < 2n - 1$ to position $2i \pmod{2n-1}$ and it keeps the card in position $2n - 1$ at $2n - 1$. In particular, the top and bottom cards still stay on the top and bottom (i.e., are still symmetrically opposite) and otherwise the cards at positions j and $2n - 1 - j$ map to positions $2j \pmod{2n-1}$ and $2(2n - 1 - j) \equiv -2j \pmod{2n-1}$ which are still symmetrically opposite (i.e., their positions add to $2n - 1$). Finally we note that an in-faro shuffle can be carried out by temporarily adding a top and bottom card, performing an out-faro shuffle, and then removing the top and bottom card. Therefore, since the stay stack result is true for out-faro shuffles, it is also true for in-faro shuffles.

3. FLIP SHUFFLING.

The methods of performing flip and faro shuffling are similar. So the easiest way to begin to understand flip shuffling is to establish a link with faro shuffling. This is the goal of this section.

Theorem 2. *Let* $\mathrm{Flip}(2n)$ *denote the shuffle group generated using in- and out-flip shuffles on a deck of* $2n$ *cards. Then* $\mathrm{Flip}(2n) = \mathrm{Faro}(4n)$.

Proof. First we give a bijection between a deck with $4n$ cards with the cards in stay stack and a deck with $2n$ cards where we keep track of whether a card is face-up or face-down. We will use "$\overline{*}$" to denote the card "$*$" has been turned over. We label our $4n$ cards now as $1, \overline{1}, 2, \overline{2}, \ldots, 2n, \overline{2n}$ and assume that the cards i and $\overline{i}$ are symmetrically opposite across the center. The bijection is now to take the deck of $4n$ cards and simply keep the first $2n$ cards. Conversely given $2n$ cards with a face-up/face-down pattern, we form our deck of $4n$ cards by first placing these in the first $2n$ positions and then in the second half placing cards to satisfy stay stack.

Examples of this bijection for $2n = 10$ are as follows:

$$
\begin{array}{ccc}
0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ \bar{9}\ \bar{8}\ \bar{7}\ \bar{6}\ \bar{5}\ \bar{4}\ \bar{3}\ \bar{2}\ \bar{1}\ \bar{0} & \longleftrightarrow & 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9 \\
\bar{9}\ 0\ \bar{8}\ 1\ \bar{7}\ 2\ \bar{6}\ 3\ \bar{5}\ 4\ \bar{4}\ 5\ \bar{3}\ 6\ \bar{2}\ 7\ \bar{1}\ 8\ \bar{0}\ 9 & \longleftrightarrow & \bar{9}\ 0\ \bar{8}\ 1\ \bar{7}\ 2\ \bar{6}\ 3\ \bar{5}\ 4 \\
\bar{4}\ \bar{9}\ 5\ 0\ \bar{3}\ \bar{8}\ 6\ 1\ \bar{2}\ \bar{7}\ 7\ 2\ \bar{1}\ \bar{6}\ 8\ 3\ \bar{0}\ \bar{5}\ 9\ 4 & \longleftrightarrow & \bar{4}\ \bar{9}\ 5\ 0\ \bar{3}\ \bar{8}\ 6\ 1\ \bar{2}\ \bar{7} \\
7\ \bar{4}\ 2\ \bar{9}\ \bar{1}\ 5\ \bar{6}\ 0\ 8\ \bar{3}\ 3\ \bar{8}\ \bar{0}\ 6\ \bar{5}\ 1\ 9\ \bar{2}\ 4\ \bar{7} & \longleftrightarrow & 7\ \bar{4}\ 2\ \bar{9}\ \bar{1}\ 5\ \bar{6}\ 0\ 8\ \bar{3} \\
3\ 7\ \bar{8}\ \bar{4}\ \bar{0}\ 2\ 6\ \bar{9}\ \bar{5}\ \bar{1}\ 1\ 5\ 9\ \bar{6}\ \bar{2}\ 0\ 4\ 8\ \bar{7}\ \bar{3} & \longleftrightarrow & 3\ 7\ \bar{8}\ \bar{4}\ \bar{0}\ 2\ 6\ \bar{9}\ \bar{5}\ \bar{1}.
\end{array}
$$

This bijection commutes with the shuffling operations, i.e., performing a faro shuffle on a deck of $4n$ cards and then applying the bijection will produce the same arrangement as applying the bijection and performing the corresponding flip shuffle. This can be seen in the sequence of above examples where we have performed in-shuffles on both sides.

In general, we observe that when taking the deck with $4n$ cards and cutting it in half, the bottom half exactly corresponds to the action of taking the top half and turning it over (i.e., the order is reversed as well as the face-up/face-down status of each card). When we now interlace these cards, the first $2n$ cards are found by interlacing the first n cards on the top half (which corresponds to the top half of the deck we want to flip shuffle) and the first n cards on the bottom half (which corresponds to the bottom half of the deck we want to flip shuffle). Therefore, the first $2n$ cards are exactly as we would expect. Now using the property of stay stack, the second $2n$ cards are as the bijection requires.

Since the bijection commutes with the shuffling operations, then for any deck arrangement that we can achieve by using faro shuffles on the $4n$ cards there is a unique corresponding arrangement on the deck using flip shuffles with $2n$ cards. In particular, the group actions are isomorphic and so the shuffling groups are the same. ∎

Theorem 2 allows us to understand the number of out-flip shuffles required to recycle $2n$ cards. Namely, the number required to recycle a deck of size $4n$ by using out-faro shuffles is the order of 2 modulo $4n - 1$ (see [**3**]). Thus for $2n = 10$, we have $4n - 1 = 19$ and 2 is a primitive root modulo 19 (e.g., $2^{18} \equiv 1 \pmod{19}$ and no smaller power will do). Thus 18 out-flip shuffles are needed to recycle the deck with 10 cards.

4. HORSESHOE SHUFFLING.

Now we turn to the variation of flip shuffling where we no longer keep track of the face-up/face-down pattern of the cards. This can be carried out as a flip shuffle on a special deck called a "mirror deck" which prints the numbers of the cards on both sides. On a normal deck this is carried out by cutting the deck in half and reversing the order of the bottom half before interlacing. As before, we have two types of horseshoe shuffles, in and out, and they are both shown in Figure 7 for a deck with 10 cards.

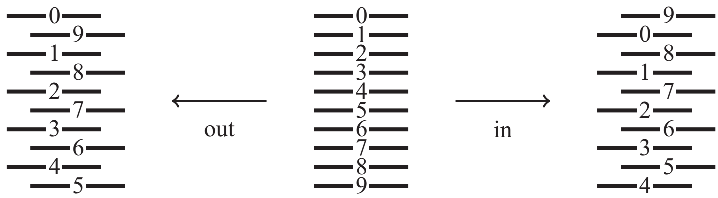


Figure 7. The effect of in- and out-horseshoe shuffles for a deck with 10 cards

The name "horseshoe" comes from being a discrete analog of the horseshoe map introduced by Stephen Smale (see [**8**]), which stretches out the unit square and then folds it back in onto itself.

As with flip shuffles, inverse horseshoe shuffles are easy to do by dealing two piles on the table. For an inverse out-horseshoe shuffle, deal two piles, turning the top card over and placing it onto the table in a first pile, dealing the second card straight down into a second pile and continuing, over (onto the first pile), down (onto the second pile), over, down, ... Finish by picking up the first pile, and turning it over onto the second pile. This results in the original top card being back on top (see Figure 8). For an inverse in-horseshoe shuffle, deal into two piles but now deal down onto the first pile, over onto the second pile, down, over, down, over, ... Finish by picking up the second pile, and turning it over onto the first pile. This results in the original top card going to the bottom (see Figure 9). These are easy for most performers (and spectators, see our card trick below) to perform.

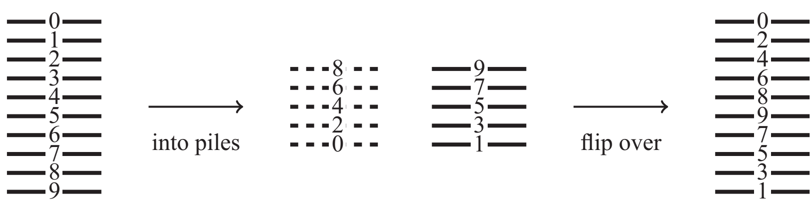


Figure 8. An inverse out-horseshoe shuffle with 10 cards

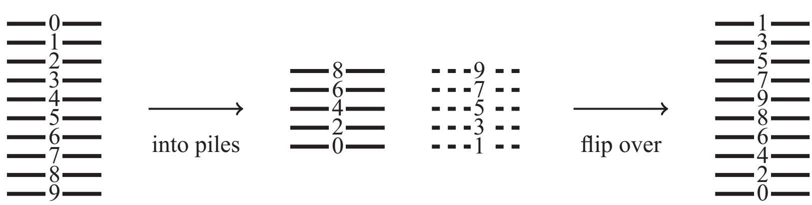


Figure 9. An inverse in-horseshoe shuffle with 10 cards

Since horseshoe shuffling and flip shuffling differ by whether or not we keep track of orientation, we have that the corresponding groups for the horseshoe shuffle are quotients of the groups of those for the flip shuffle. As we will show, the groups are among the simplest and most beautiful in the theory of perfect shuffling.

Theorem 3. *Let* Horse($2n$) *denote the shuffle group generated using in- and out-horseshoe shuffles on a deck of* $2n$ *cards. Then the following holds:*

$$|\operatorname{Horse}(2n)| = \begin{cases} 4{\cdot}5{\cdot}6 & \text{if } 2n = 6, \\ 8{\cdot}9{\cdot}10{\cdot}11{\cdot}12 & \text{if } 2n = 12, \\ (k+1)2^k & \text{if } 2n = 2^k \text{ with } k \geq 2, \\ (2n)! & \text{if } n \equiv 1 \pmod 2 \text{ and } n \neq 3, \\ (2n)!/2 & \text{if } n \equiv 0 \pmod 2 \text{ and } n \neq 6, 2^k. \end{cases}$$

(Note $|\operatorname{Horse}(2n)|$ *is the number of possible arrangements of a deck of* $2n$ *which can be obtained by repeated applications of faro shuffles.)*

The special cases of $2n = 6$ and $2n = 12$ were verified by computer. These two cases are somewhat extraordinary and the corresponding groups are known. When $2n = 6$ then the first *three* cards can be arbitrary which then forces the order of the last three cards, the corresponding group is $PGL(2, 5)$ which is isomorphic to S_5. When $2n = 12$, then the first *five* can be arbitrary which then forces the order of the last seven cards, the corresponding group is again the Mathieu group M_{12} (which is sharply 5-transitive).

We will establish Theorem 3 by working through the remaining general cases. The main thing to observe is that if we can achieve an ordering of the cards using flip shuffles, then we also can achieve the same ordering of the cards using horseshoe shuffles (i.e., the difference between the two being whether or not we keep track of the orientation of the cards).

Lemma 1. *If* $n \equiv 1 \pmod 2$ *and* $n \neq 3$*, then* $\operatorname{Horse}(2n) = S_{2n}$*, the symmetric group of order* $2n$*. In particular,* $|\operatorname{Horse}(2n)| = (2n)!$.

Proof. By Theorem 2 we have that $|\operatorname{Flip}(2n)| = |\operatorname{Faro}(4n)| = (2n)!2^{2n}$. On the other hand, there are only $(2n)!$ ways to order the deck and 2^{2n} face-up/face-down configurations. Hence, the total number of possible orderings under flip shuffling (by considering what combinations can occur) is $(2n)!2^{2n}$. In particular, we must be able to get any ordering using horseshoe shuffles. ∎

Lemma 2. *If* $n \equiv 0 \pmod 2$ *and* $n \neq 6, 2^k$*, then* $\operatorname{Horse}(2n) = A_{2n}$*, the alternating group of order* $2n$*. In particular,* $|\operatorname{Horse}(2n)| = (2n)!/2$.

Proof. By Theorem 2 we have that $|\operatorname{Flip}(2n)| = |\operatorname{Faro}(4n)| = (2n)!2^{2n-2}$. We now take a closer look at what orderings are possible and what face-up/face-down configurations are possible.

For the orderings we will think of our shuffling operations as applying a permutation to $0, 1, \ldots, 2n-1$. We claim that the two different shuffling operations both correspond to even permutations (i.e., can be written as the product of an even number of transpositions). If this is the case, then it will follow that all possible arrangements that we can form correspond to even permutations and in particular there are at most $(2n)!/2$ possible orderings.

To verify the claim, we start with the cards labeled $0, 1, \ldots, n, n+1, \ldots, 2n-1$; we will describe a sequence of transpositions that will transform this ordering to $0, 2n-1, 1, \ldots, n+1, n-1, n$ (the ordering resulting from an out-horseshoe shuffle). The cards $n-1$ and n are in the correct relative ordering. We now move the card $n+1$ so it comes before $n-1$ which takes two transpositions (i.e., exchange

n and $n+1$ and then exchange $n-1$ and $n+1$). We now move the card $n+2$ so it comes before $n-2$ which takes four transpositions (i.e., we exchange places with $n, n-1, n+1, n-2$). This continues in general so that we will move card $n+i$ so it comes before $n-i$ which will take $2i$ transpositions (i.e., we exchange places with $n, n-1, \ldots, n+(i-1), n-i$). Therefore, the total number of transpositions we have used is

$$0+2+4+\cdots+2(n-1)=n(n+1),$$

which is even and this is an even permutation. For the in-horseshoe shuffle we first place it into the out-horseshoe shuffle and then switch every pair, i.e., apply the transpositions $(0, 2n-1), (1, 2n-2), \ldots, (n-1, n)$. Since, by hypothesis, n is even there are an even number of such pairs showing that the in-horseshoe shuffle will also be an even permutation.

As for the face-up/face-down configuration, let X_i be an indicator that the card in the ith position is face-up (i.e., X_i is 1 if the card is face-up and 0 if the card is face-down). Therefore, the number of cards which are face-up is $\sum X_i$. Applying either shuffle we have that the number of cards which are face-up after one operation is

$$\begin{aligned} X_0+X_1+\cdots+X_{n-1}+(1-X_n)+(1-X_{n+1})+\cdots+(1-X_{2n-1}) \\ \equiv X_0+X_1+\cdots+X_{2n-1}+n \pmod 2. \end{aligned}$$

By hypothesis we have that n is even and therefore the parity of the number of face-up cards never changes with shuffling. Since we start with an even number of face-up cards, we will always have an even number of face-up cards and therefore there are at most 2^{2n-1} possible face-up/face-down configurations.

Combining the two above ideas, we see that there are at most $\frac{(2n)!}{2} \times 2^{2n-1} = (2n)!2^{2n-2}$ possible configurations under flip shuffling, but we already know that we have that many achievable configurations. And therefore each possible combination of ordering (coming from even permutations) and face-up/face-down cards (as long as there is an even number of face-up cards) is possible. In particular, we can achieve any ordering for horseshoe shuffling which corresponds to an even permutation. ■

All that remains now to establish Theorem 3 is the case when the deck size is a power of 2 which we will handle in the next section.

5. HORSESHOE SHUFFLES FOR DECK SIZE A POWER OF TWO. Combining Theorems 1 and 2 we conclude when $2n = 2^k$ that $|\mathrm{Flip}(2n)| = (k+1)2^{k+1}$. Of course this takes more information into account and so we will work to understand what is possible when we ignore the face-up/face-down orientation of the cards. In this section we will determine what happens, and moreover we will show that knowing just the first two cards we can determine the order of the remaining cards.

The first observation is that by using binary to represent the position of a card we can determine where the card will go when we horseshoe shuffle. There are two types of shuffles and on each of the two shuffles we have a top half and a bottom half. If we represent the location using binary as $x_{k-1}x_{k-2}\ldots x_0$ (so the top half is $x_{k-1}=0$ and the bottom half is $x_{k-1}=1$), then the following rules can be verified (note by flipping the bits in the second half we reverse their order):

$$\textit{in}\text{-horseshoe shuffle:}\quad x_{k-1}x_{k-2}\dots x_1x_0 \longrightarrow \begin{cases} x_{k-2}\dots x_0\,1 & \text{if } x_{k-1}=0 \\ \overline{x_{k-2}\dots x_0}\,0 & \text{if } x_{k-1}=1 \end{cases}$$

$$\textit{out}\text{-horseshoe shuffle:}\quad x_{k-1}x_{k-2}\dots x_1x_0 \longrightarrow \begin{cases} x_{k-2}\dots x_0\,0 & \text{if } x_{k-1}=0 \\ \overline{x_{k-2}\dots x_0}\,1 & \text{if } x_{k-1}=1, \end{cases}$$

where we let $\overline{x_i} = 1 - x_i$, i.e., flipping the bit. An illustration of how position is affected as we apply the shuffles is shown in Figure 10 which demonstrates what goes on if we look at the position for the card initially in position 1011 through four shuffles where an *in*-horseshoe shuffle is up and an *out*-horseshoe shuffle is down as we go from left to right.

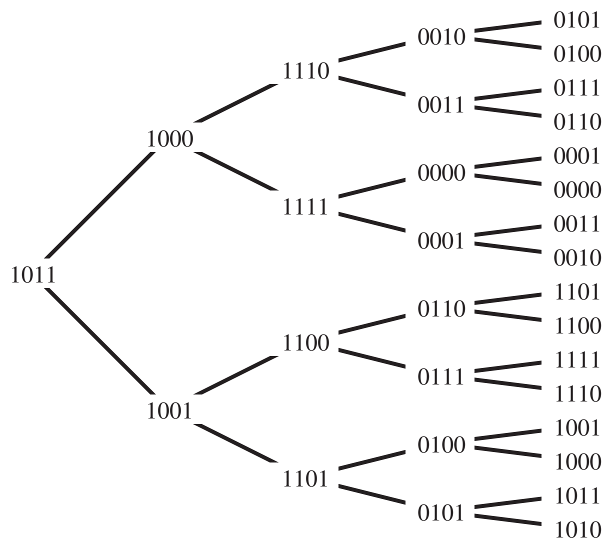


Figure 10. The position of the card initially at 1011 through four shuffles

The diagram shows that by a correct choice of four shuffles we can start in position 1011 and move to *any* desired position. It turns out that this is always the case.

Proposition 1. *For any $0 \le i, j \le 2^k - 1$ we can use k horseshoe shuffles on a deck of size 2^k to move the card in the ith position to the jth position. In particular, every card can be moved to the top in at most k shuffles.*

This can be seen by noting that if we know the leading i digits of a position, then after performing one shuffle (whether an in- or out-shuffle) we know the leading $i-1$ digits. Since we know the initial position (i.e., all k digits of our position), then through performing the kth shuffle we will know the leading digit (i.e., whether we are in the top or bottom half). At each stage there are two possible shuffles that can be applied so there are 2^k possible outcomes. On the other hand, since we can always reverse the process at each step (i.e., we know what the leading digit had to be in the previous location and we know the final digit of the current location which determines what type of shuffle was used) we have that these outcomes are all distinct. Since there are only 2^k outcomes (i.e., positions), then every outcome must occur.

We can now get a lower bound for the number of arrangements.

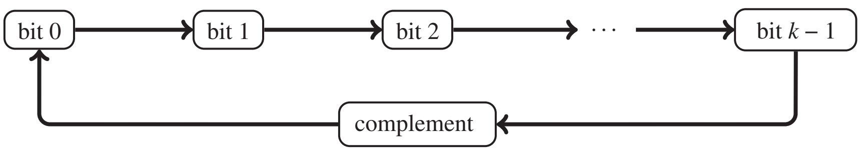
Proposition 2. *There are at least* $(k+1)2^k$ *different arrangements of a deck of size* 2^k *using in- and out-horseshoe shuffles.*

Proof. By the previous proposition, we can place any of the 2^k cards on the top position. Once that card is on top, then repeated out-horseshoe shuffles will leave that card on top. Examining what happens to the card in the second position, we note that it will go into positions as follows:

$$1 \longrightarrow 2 \longrightarrow 2^2 \longrightarrow \cdots \longrightarrow 2^{k-1} \longrightarrow (2^k - 1) \longrightarrow 1.$$

In particular, the cards in these $k+1$ positions will cycle through the second position and so for every card in the first position there are at least $k+1$ cards that can be in the second position, establishing the result. ■

To show that we can only get this many different arrangements, we will first show that the horseshoe shuffles preserve a special ordering; this ordering is also used crucially in the card trick of Section 6. This is based on the following diagram where "bit i" refers to the digit in the binary expansion corresponding with 2^i.



Definition 1. For a deck with cards labeled $0, 1, \ldots, 2^k - 1$ (in binary), a *special ordering* of the cards is one determined by the following procedure. Given an arbitrary first card and an arbitrary starting point in the above diagram carry out the following k times: duplicate the existing card(s) and apply the operation given by the current location on the new card(s); then move to the next location in the diagram.

As an example of this process, if the deck has 16 cards and the first card is eleven (or in binary is 1011) and the starting point is to change bit 2 going (in binary) to 1111, we then change bit 3 for *all* of the numbers we have giving 0011 and 0111, and so on. The entire process proceeds as indicated in Table 1. In particular, this produces the ordering

$$\overset{1011}{11}, \overset{1111}{15}, \overset{0011}{3}, \overset{0111}{7}, \overset{0100}{4}, \overset{0000}{0}, \overset{1100}{12}, \overset{1000}{8}, \overset{1010}{10}, \overset{1110}{14}, \overset{0010}{2}, \overset{0110}{6}, \overset{0101}{5}, \overset{0001}{1}, \overset{1101}{13}, \overset{1001}{9}.$$

To understand what is happening we note that upon splitting the deck in half and reversing the bottom half then the following two things are true.

- Each half deck is built off of the first $k-1$ operations used in determining the special order of the full deck.
- The two half decks differ from each other exactly corresponding to the operation in the diagram that was *not* used (e.g., if we started by flipping bit 2 then the two differ in bit 1). To see this note that if we go around and apply all the operations to a binary string of length k, then we will have what we started with. So in effect the operation that was not used is equivalent to the effect of all other operations combined (i.e., in binary applying an operation twice returns us back to what we started with).

Table 1. An example of determining the ordering

initial	change bit 2	change bit 3	complement	change bit 0
1011	1011	1011	1011	1011
	1111	1111	1111	1111
		0011	0011	0011
		0111	0111	0111
			0100	0100
			0000	0000
			1100	1100
			1000	1000
				1010
				1110
				0010
				0110
				0101
				0001
				1101
				1001

With these two properties we see that when we shuffle the two halves together (either in or out) then the first pair will differ in the missing operation, then the next pair is formed by copying and applying the prior first operation, and so on.

In particular if we started with a special ordering then we will maintain a special ordering after we shuffle. Since we start with the cards in the order $0, 1, \dots, 2^k - 1$, which is special (starting card 0 and initial operation flipping bit 0), then the only possible orderings are these special orderings. But there are at most $(k+1)2^k$ such orderings, i.e., pick the first card and then pick one of $k+1$ operations to apply.

Theorem 4. *There are exactly $(k+1)2^k$ different arrangements of a deck of size 2^k using in- and out-horseshoe shuffles.*

Finally we mention that if we reversed the order of the deck that we would still have the same order of operations used to build up the sequence, e.g., 9, 13, 1, 5, . . . can be built by starting with 9, then changing bit 2, then bit 3, ... We will use this in the next section in an application.

6. OTHER SHUFFLING METHODS. The horseshoe shuffle is closely related to the *milk shuffle* which consists of taking the deck and then "milking" off the top and bottom card and putting them on the table, then continue milking off the top and bottom card and placing on top of the pile on the table until all the cards have been used. So for example if we have a deck with $2n = 10$ cards the result is what is shown in Figure 11.

This looks very similar to Figure 7. In particular, if you draw a line connecting the cards in their original order, then you will see that the horseshoe forms the shape "$\cup$" while the milk forms the shape "$\cap$." So these shuffles are essentially the same, and one can be done by first flipping the deck, carrying out the other form of shuffling, and then flipping the deck back over. This suggests there should be two milk shuffles, the second one consists of milking off the top and bottom cards and then before putting them on the pile switching the order, an inconvenient shuffle for performance.

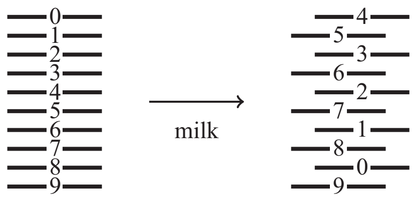


Figure 11. The effect of the milk shuffle for a deck with 10 cards

Going further, this same connection of flipping also applies for the inverse of the milk shuffle, the *Monge shuffle*. This is carried out by taking the deck and placing the top card in the other hand. We then feed the top card of the deck into the other hand one card at a time alternating between being placed on the top or the bottom of the pile. (When the second card is placed under the first this corresponds to the inverse of the milk shuffle, though the second card can also be placed over the first.) This is illustrated in Figure 12 for a deck with $2n = 10$ cards.

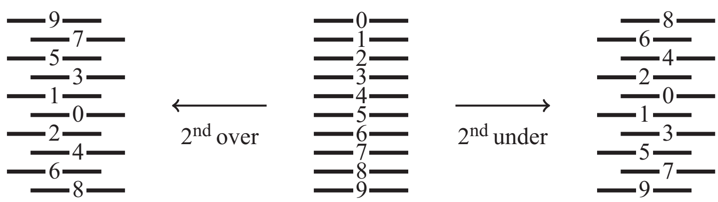


Figure 12. The effect of the two Monge shuffles for a deck with 10 cards

The milk and Monge shuffles have been extensively studied before (see [**2, 3, 4**] and references therein; there are also many online videos which demonstrate how to perform these shuffles).

Returning to the previous section, we note that the special ordering we discussed is preserved when we apply an inverse shuffling operation as well as when we flip the deck. Therefore, for decks of size 2^k, any application of combinations of the (inverse) horseshoe shuffle, milk shuffle, Monge shuffle, or dealing the deck into a pile (i.e., reversing the order; more generally one can deal the cards down 2^i at a time) will still preserve our special ordering. This can be used for a very simple trick which we outline here.

Working from the Outside In. We first describe the effect. We start with a packet of eight cards and tell our audience "In this small pile we have eight cards which we will now use to practice various shuffling techniques." At this point the deck is handed over to audience members where they are then taught about the different shuffles, i.e., the horseshoe,[2] the milk, the Monge, and dealing the cards onto a pile (either one, two, or four at a time). They are allowed and encouraged to do as many shuffles as they want in whatever order they choose.

After much shuffling we now declare "By now we have become somewhat expert as to how to shuffle the deck, but of course we have been shuffling so long that we have no

[2]For most people it is easier to teach and carry out the inverse horseshoe shuffle: deal the cards one at a time alternating between two piles, one being face-up and the other being face-down, and finally turn the face-up cards over onto the face-down pile.

idea of the current ordering of the cards. But as with many problems we can solve what the ordering should be by working from the outside in. So now please deal the cards down either from left to right or from right to left." At this point the cards are dealt (of course the dealing as well as all of the shuffling can occur with the performer having their back turned). "To figure out what cards we have, we need to start somewhere and so will you please turn over the end cards." The end cards are turned over, and the magic begins!

Let us suppose that what we see is the following:

4 ? ? ? ? ? ? 6.

We continue, "Aha! the 4 and the 6, an interesting combination. The 4 is a power of 2 so wants to be with another power of 2 so the next card could be a 1, 2, or an 8 and in this case it is an 8, similarly the number 6 is composite so it wants to be next to one of its prime divisors which are 2 or 3 and in this case it is next to the 2 . . . ." This continues until all the cards have been declared, with various dubious or numerological reasons given as to what should come next, and cards are turned over as the declarations are made with each one being correct. Until finally the ordering is given

4 8 3 7 5 A 2 6.

"And so we see that we can solve this problem by working from the outside in!"

The way this is done is to take the cards and initially order them 8A234567 (either from top to bottom or bottom to top). We will treat 8 as 0 for our computations. Hence, what we have actually done is place the cards in a special order, and in particular an ordering that obeys the rule of the diagram from Section 5. Then as the various shuffles are performed the ordering will change, but each time it will still obey the same diagram. Thus, once the cards are placed down it only remains to determine a starting card (and as noted we can start from either end) and where in the diagram we start from. Taking the end cards, we compute in binary how they differ, since 4 and 6 in binary are respectively 100 and 110 we see they differ in bit 1 (in general if the numbers add to 7 they are complements otherwise the difference tells you which bit to work in). Therefore, we should start with the *next* operation in our diagram which in this case is to flip bit 2 and so 100 (the 4) becomes 000 (which would normally be 0 but we represented by 8). Similarly, on the other side 110 becomes 010 (the 2) giving us our next layer in. Now to get the remaining four, we use the four cards showing and the next operation (in this case complementation) to determine what will come next.

This can be done fairly quickly with a bit of practice in binary, remembering that 8 corresponds with 0. The biggest danger is that someone makes a mistake in shuffling, in which case the ordering will be off. So make sure to carefully walk the audience through each kind of shuffle so that they will not make a mistake; alternatively, you can carry out the shuffles as directed by audience members.

Further embellishments to the performance can be made by using the following.

- Once one of the end cards has been turned over, you can automatically predict one of the cards by the following rule: If $x_0x_1x_2$ is in the first position then $\overline{x_0}x_1\overline{x_2}$ is in the sixth position (this works from either end).

- You can incorporate suits into the performance by starting with the following cards (in the indicated order):

  8S AS 2H 3H 4C 5C 6D 7D.

  We then proceed as before *except* at the last step we have one of the end cards turned over so that we can see and then ask for the *suit* of the other end card. From this information the ordering can be determined as before because if the end card that we see is one of {8S, 3H, 5C, 6D}, then the other end card is one of {AS, 2H, 4C, 7D} and vice versa; in any case, knowing the suit uniquely determines the card. This variation has the nice property of demonstrating that if we know the value of a card (one of 2^3 possibilities) and the suit of another card (one of $3 + 1$ possibilities), then we know which of the $(3 + 1)2^3$ orderings we have.

7. CONCLUDING REMARKS. As we have seen the flip and horseshoe shuffles have nice connections with known shuffles. As a result similar performance techniques can be used for these shuffles. For instance, to move the top card into the ith position (where the positions have been labeled as $0, 1, \ldots$), then we again write i in binary and translate that into in and out shuffles appropriately. This works because as we move the card down to the ith position, it will always remain in the top half as we shuffle and so behaves precisely like what happens with faro shuffling. On the other hand, the problem of moving a card from the ith position to the top position, known as Elmsley's problem (see [**1, 6**]), will need different techniques. For the deck with 10 cards the shortest ways to move the card in the ith position to the top are given in Table 2.

Table 2. How to move the ith card to the top

Position	Shuffling sequence
1	out, in, out, in **or** out, out, in, in
2	in, out, in **or** out, in, in
3	in, out, out, in **or** in, in, in, in
4	in, in
5	out, in
6	out, out, out, in **or** out, in, in, in
7	out, out, in **or** in, in, in
8	in, in, out, in **or** in, out, in, in
9	in

Problem. Determine a general method for a deck of $2n$ cards that moves the card in the ith position to the top using in- and out-horseshoe shuffles.[3]

We also note that we have carried out the analysis for decks with an even number of cards. There are also two types of perfect flip and horseshoe shuffles for decks of odd order. We leave the analysis of this case as an exercise for the interested reader.

[3]Some progress on this problem was done by Émile Nadeau and Stéphanie Schank while undergraduates at UQAM (personal communication). A complete solution is still not known.

One thing that we did not do is give a description of the group for the horseshoe shuffle when the deck has size 2^k. A description of this group has been found by Kent Morrison and we give it here. From Diaconis, Graham, and Kantor [**3**], we have that $\mathrm{Flip}(2^k) = \mathrm{Faro}(2^{k+1})$ is the semidirect product of $k+1$ copies of Z_2 by the cyclic group of order $k+1$ which acts by permuting the factors cyclically. The horseshoe group on 2^k cards is a quotient of this group gotten by dividing out by the order two subgroup generated by $(1, 1, \ldots, 1)$ in the product of the Z_2's. Note the action of the cyclic shift respects the quotient.

The shuffles we have mentioned here are some of many possible shuffles which exhibit interesting mathematical properties. More information about the mathematics behind various shuffles and how it can be used to amaze and entertain friends and colleagues can be found in the recent books of Diaconis and Graham [**2**] as well as Mulcahy [**5**].

ACKNOWLEDGMENT. The authors thank Jeremy Rayner for introducing them to flip shuffles, Kent Morrison for several useful suggestions (including a description of the horseshoe shuffle group for powers of 2), and the referees for their thorough reading and useful suggestions which led to an improved paper.

REFERENCES

1. P. Diaconis, R. Graham, The solutions to Elmsley's problem, *Math Horizons* **14** (2007) 22–27.
2. ———, *Magical Mathematics: The Mathematical Ideas that Animate Great Magic Tricks*. Princeton Univ. Press, Princeton, 2011.
3. P. Diaconis, R. Graham, W. M. Kantor, The mathematics of perfect shuffles, *Adv. Appl. Math.* **4** (1983) 175–196.
4. A. Ledet, The Monge shuffle for two-power decks, *Math. Scand.* **98** (2006) 5–11.
5. C. Mulcahy, *Mathematical Card Magic*. CCR Press, Boca Raton, FL, 2013.
6. S. Ramnath, D. Scully, Moving card i to position j with perfect shuffles, *Math. Mag.* **69** (1996) 361–365.
7. J. Rayner, Flipping perfect shuffles, *Metagrobologist Mag.* (Oct 2014) 54–59.
8. S. Smale, Differentiable dynamical systems, *Bull. AMS* **73** (2967) 747–817.

STEVE BUTLER received his Ph.D. in mathematics from UC San Diego under the direction of Fan Chung Graham in 2008. He was an NSF postdoctoral scholar at UCLA before joining the faculty at Iowa State University in 2011. In preparing for writing this article he took up an intensive training regime in faro shuffling and was able to do eight perfect shuffles in 53 seconds. He is now working on a book about the mathematics of juggling with Joe Buhler, Ron Graham, and Anthony Mays.
Department of Mathematics, Iowa State University, Ames, IA 50011
butler@iastate.edu

PERSI DIACONIS has been shuffling cards since he was five years old. He learned to perfectly shuffle at age 13 and started proving theorems about shuffling at age 20 (he is still at it). He is professor of mathematics and statistics at Stanford University.
Department of Statistics, Stanford University, Stanford, CA 94305
diaconis@math.stanford.edu

RON GRAHAM is the Irwin and Joan Jacobs Professor in the Department of Computer Science and Engineering at the University of California, San Diego, and the Chief Scientist of the California Institute for Telecommunications and Information Technology. He is a former president of the Mathematical Association of America and the American Mathematical Society and has been awarded numerous honors for his extensive groundbreaking work in discrete mathematics. However, he still can't faro shuffle as well as his two coauthors (but he continues to work on it). Most recently he co-wrote Magical Mathematics with Persi Diaconis, which was awarded the 2013 Euler Book Prize.
Department of Computer Science and Engineering, UC San Diego, La Jolla, CA 92093
graham@ucsd.edu