ARTICLES

Groups of Perfect Shuffles

Some questions are answered but many remain about the mathematics of card shuffling.

Steve Medvedoff
Kent Morrison
California Polytechnic State University
San Luis Obispo, CA 93407

There are two ways to perfectly shuffle an ordinary deck of cards. First divide the deck in half and then interleaf the cards. The top card either remains on top or becomes the second card. A perfect shuffle is difficult but not impossible to perform. There are magicians who can execute a perfect shuffle and there are even a few who can do eight consecutive perfect shuffles—leaving the top card on top—to bring the deck back to its original position.

In 1983 a fascinating paper appeared dealing with the mathematics of perfect shuffles [**4**]. The work of Persi Diaconis, Ron Graham, and William Kantor completely determines the structure of the permutation groups generated by the two perfect shuffles of a deck containing an even number of cards. Incidentally, Diaconis was a professional magician before he became a mathematician-statistician and is able to perform eight perfect shuffles. Graham is also an amateur juggler. An interesting account of their work by Gina Kolata appeared in *Science* [**7**]. In this paper we will describe their results briefly but we will focus on problems that generalize theirs, problems that remain unsolved for the most part and problems that can be attacked in an experimental way by the tools of undergraduate algebra. We offer the subject of shuffle groups as a promising area in which to do exploratory group theory.

Shuffle groups

The mathematics of card shuffles has a long history and has been of most interest to magicians. There are card tricks based on mathematical principles rather than sleight-of-hand, or a combination of the two. One trick that children pass on to each other is the three-pile trick using 27 cards. The paper of Diaconis, Graham, and Kantor has a long section on the history of the mathematics of shuffles and there are two articles by Martin Gardner ([**5**], [**6**]) in his highly readable style.

What we mean by a **perfect shuffle** is a particular way of permuting the cards in a deck. We generalize the usual shuffle, in which the deck is divided into two piles, by allowing the deck to be divided into several equal piles. Then these piles are interleaved perfectly. For example, consider a deck of 33 cards. First divide the deck into three equal piles, the top, middle, and bottom piles each having eleven cards. Put these piles side by side in the order: top, middle, bottom. Next rearrange the piles in any of the six possible ways. Finally, pick up the cards from left to right, one at a time. The resulting arrangement is a perfect 3-shuffle (or ternary shuffle). There are six distinct 3-shuffles. If the cards in our deck are numbered $1,2,\dots,33$, then after dividing into piles, we envision them like this:

1	12	23
2	13	24
.	.	.
.	.	.
.	.	.
11	22	33

Now re-position the piles like this (one of six possibilities):

12	1	23
13	2	24
.	.	.
.	.	.
.	.	.
22	11	33

Next pick up the cards from left to right. The new order is $12,1,23,13,2,24,\dots,22,11,33$. In this way we have six permutations of the numbers $1,\dots,33$ and we ask: *what subgroup of the symmetric group S_{33} do they generate*? Actually we have already asked this particular question and managed to answer it, but this is the sort of problem we are interested in. By the way, the answer is that they generate *all* of S_{33}, but it takes quite a bit of work to get the answer.

As you can see from the example, we have an infinite number of groups to study. If we want to divide our deck into k piles before shuffling, then the deck size must be a multiple of k, say kn. For positive integers k and n we generate a subgroup of the permutation group S_{kn}. The generators are the perfect k-shuffles, of which there are $k!$. We call this subgroup $G_{k,kn}$, and we would simply like to know what $G_{k,kn}$ looks like for all possible k and n. In our example with 33 cards we know $G_{3,33} = S_{33}$.

The 2-shuffles, or binary shuffles, are the usual shuffles that we attempt in order to mix up a deck of playing cards. It is the corresponding family of groups $G_{2,2n}$ that have been completely determined by Diaconis, Graham, and Kantor. Although we do not normally shuffle cards by dividing a deck into three or more piles, there are uses of k-shuffles in card tricks. The three pile trick using 27 cards involves the group $G_{3,27}$, which happens to be very much smaller than S_{27}.

Here is a brief summary of what is known about the shuffle groups:

(1) The binary shuffle groups $G_{2,2n}$ are all taken care of. There are five infinite families and two exceptional cases [**4**]. We will describe them later.
(2) We have determined G_{k,k^m}, and we will describe it in this paper.
(3) $G_{3,3n}$ is understood for deck sizes up to 63 (that is, for $n \leq 21$), and we have a solid conjecture for all n, a classification into three families.
(4) $G_{4,4n}$ is understood for decks up to 32 cards, and we have a conjecture for all n, a classification into four families.

We determined the structure of $G_{3,3n}$ and $G_{4,4n}$ for small values of n using the computer system for group theory called CAYLEY. The CAYLEY system was invaluable for concrete knowledge of these groups and gave us the data for the conjectured classification for $k = 3$ and 4. It was also a tremendous amount of fun to use. For access to the program and for help in using it, we would like to thank John Cannon, who has developed CAYLEY over the last twenty years, and Charles Sims and the Rutgers University Mathematics Department whose version of CAYLEY we used. CAYLEY is an immense system of hundreds of algorithms, in 250,000 lines of code, that is designed for the computational algebra of groups by generators and relations, permutation groups, finite fields and their polynomial rings, and linear algebra over finite fields. (CAYLEY is available from John Cannon, University of Sydney, Sydney, Australia, for a modest fee in both VAX and CYBER implementations. It is an expert system that works best with an expert's hand but is used, too, for laboratory work in undergraduate algebra courses.) We would also like to thank William Kantor and Martin Gardner for their interest in this work.

The fundamentals

Now it is time to go into the mathematics of the problem we have outlined. First we develop the notation. Generally, it is more convenient to number the cards beginning with 1 but sometimes it is better to begin with 0. We also number the piles from 1 to k (sometimes 0 to $k-1$). For each permutation σ in S_k, a permutation of the piles, we have the corresponding shuffle that we denote s_σ. The group $G_{k,kn}$ is generated by the elements s_σ for $\sigma \in S_k$. We use the convention that σ is a bijection of the set $\{1,\dots,k\}$ and that $\sigma(2)=3$ means that the second pile is moved to the third position. In cycle notation we would have $(2\ 3\dots)$ somewhere in the expression for σ. The shuffle s_σ can be written as the product of two operations

$$s_\sigma = p_\sigma s_I,$$

first performing the permutation p_σ followed by the shuffle s_I. Here we define p_σ to be the permutation of the deck that is accomplished by dividing it into piles as if to shuffle, permuting the piles according to σ, and then restacking the piles without interleaving with the leftmost pile on top. The shuffle s_I denotes the one in which the piles are not permuted. Thus p_σ permutes the piles and s_I does the interleaving. Notice that we write our operations left to right. Although it was not apparent before, now we see that p_σ is an element of $G_{k,kn}$. Furthermore, we see that we do not need $k!$ generators. All we need are enough elements of the form p_σ, so that the σ's generate S_k, along with the shuffle s_I. It is convenient to call s_I the **standard shuffle** and to denote it by s. We can generate $G_{k,kn}$ with three generators s, p_σ, p_τ, where σ and τ are generators for S_k. (It is easy to see that you can generate S_k with two generators. For example you may use $(1\ 2)$ and $(2\ 3\dots k)$.) When $k=2$, there are only two generators for $G_{2,2n}$.

It is true that $p_\sigma p_\tau = p_{\sigma\tau}$ since successive permutation of the piles is a permutation of the piles, but $s_\sigma s_\tau$ is not $s_{\sigma\tau}$. If we knew how to write $s_\sigma s_\tau$ in a nice way the whole problem would not be hard.

The first step is to determine the parity of our shuffles so that we know when $G_{k,kn}$ is contained in the alternating group A_{kn}.

LEMMA 1. *If n is odd and $\sigma \in S_k$ is an odd permutation, then p_σ is odd; otherwise p_σ is even.*

Proof. A permutation of two piles has the effect of interchanging n pairs of cards. Thus each transposition of σ results in n transpositions for p_σ.

LEMMA 2. *If either k or n is congruent to either 0 or 1 (mod 4) then s is even; otherwise s is odd.*

Proof. We will show that s can be written as $\dfrac{n(n-1)}{2}\dfrac{k(k-1)}{2}$ transpositions. Visualize the deck after cutting:

$$\begin{array}{ccccc}
1 & n+1 & 2n+1 & \cdots & (k-1)n+1 \\
\cdot & \cdot & \cdot & \cdots & \cdot \\
\cdot & \cdot & \cdot & \cdots & \cdot \\
\cdot & \cdot & \cdot & \cdots & \cdot \\
n & 2n & 3n & \cdots & kn.
\end{array}$$

Card 1 will stay put. Card 2 will have $k-1$ new cards in front of it after shuffling. Card 3 will have $2(k-1)$ new cards in front of it. Thus the cards in the first column will require $(k-1)+2(k-1)+\cdots+(n-1)(k-1)$ transpositions of adjacent cards to put them back on top. This sum is $(n(n-1)/2)(k-1)$. Now analyze the second pile in the same way. The number of adjacent transpositions required is $(n(n-1)/2)(k-2)$. For the rest of the piles we see that

$$\frac{n(n-1)}{2}[(k-1)+(k-2)+\cdots+2+1] = \frac{n(n-1)}{2}\frac{k(k-1)}{2}$$

adjacent transpositions are required to restore the deck to its original order.

Now we can say when the generators of $G_{k,kn}$ are all even permutations. Lemma 1 requires that n be even. Lemma 2 shows that if $n \equiv 0 \pmod 4$ then k can be anything, while if $n \equiv 2 \pmod 4$, k must be congruent to 0 or 1 (mod 4). This proves the following result on parity.

THEOREM 1. *If either of the following conditions holds, then $G_{k,kn}$ is a subgroup of A_{kn}:*

(i) $n \equiv 0$ (*mod* 4)

(ii) *n is even and $k \equiv 0$ or 1 (mod 4).*

Otherwise $G_{k,kn}$ contains an odd permutation.

COROLLARY. *If $n \equiv 0$ (mod 4), then $G_{3,3n}$ is contained in A_{3n}.*

Lemma 2 and Theorem 1 are contained in [9] with different notation. Generically, that is for almost all k and n, we expect the parity theorem determines the structure of $G_{k,kn}$ as either S_{kn} or A_{kn}. The cases in which the group is not either of these are the cases of most interest.

We can determine the orders of two of the shuffles: s and s_{rev}. Here **rev** denotes the permutation "reverse" that reverses the order of the piles. Unfortunately we do not know what the orders of the other shuffles are.

PROPOSITION 1. *The order of s in $G_{k,kn}$ is the order of k (mod $kn-1$), i.e., the smallest power of k congruent to 1 (mod $kn-1$), or equivalently, the order of k in the multiplicative group of units of the ring $\mathbb{Z}_{kn-1}$.*

Proof. Now it is convenient to number the cards from 0 to $kn-1$, because s fixes 0 and $kn-1$ and on the rest it acts by the rule s: $i \to ki \pmod{kn-1}$. Card 1 goes to position k, card 2 goes to position $2k$ and so on. This formula works for $i = 0$ but not for $i = kn-1$. Then the order of s is the smallest positive integer e such that $k^e i \equiv i \pmod{kn-1}$ for all i, but this is equivalent to $k^e \equiv 1 \pmod{kn-1}$.

PROPOSITION 2. *The order of s_{rev} is the order of k (mod $kn+1$).*

Proof. This time number the cards from 1 to kn. After cutting, the cards are arranged in the pattern:

$$\begin{array}{llll}
1 & n+1 & \cdot & \cdot \quad \cdot \\
2 & n+2 & \cdot & \cdot \quad \cdot \\
\cdot & \cdot & \cdot & \cdot \quad \cdot \\
\cdot & \cdot & \cdot & \cdot \quad \cdot \\
\cdot & \cdot & \cdot & \cdot \quad \cdot \\
n & 2n & \cdot & \cdot \quad kn.
\end{array}$$

Now card i in row j and column p satisfies $i = (p-1)n + j$. The shuffle s_{rev} picks up the cards from right to left so that s_{rev} picks up all the cards in the rows above and the cards to the right of the same row before picking up a given card. That means the card in row j and column p will have $k(j-1)$ cards in the rows above it and $k-p$ cards to the right so it will be in position $k(j-1)+k-p+1$. A little arithmetic shows that this is congruent to $ki \pmod{kn+1}$. Thus s_{rev}: $i \to ki \pmod{kn+1}$ and it follows that the order of s_{rev} is as claimed.

This proof is not illuminating because we had to know the answer ahead of time. It is a little easier to see when $k = 2$ and we found that result in [4]. We simply tried out the obvious generalization for a couple of cases with $k = 3$ and 4. Convinced that it was true, we constructed a proof.

As we mentioned before, $G_{2,2n}$ has only two generators. Martin Gardner writes in [5] that Alex Elmsley, a magician, coined the terms "out-shuffle" and "in-shuffle." The out-shuffle is s_I and it leaves the first card on top or on the outside. The in-shuffle is $s_{(12)}$ and it puts the first card in the second position or inside. For $k > 2$, we continue to call s_I the out-shuffle and s_{rev} the in-shuffle, though there are other shuffles that leave the first card outside and that put the first card as deeply as possible inside. Elmsley used the letters O and I to stand for the two shuffles. He noticed in 1957 that a sequence of shuffles denoted by a sequence of O's and I's had the effect of bringing the top card down to the position whose binary expansion was the corresponding sequence of zeros and ones. You must number the cards $0, 1, 2, \ldots$. This happy fact generalizes to k-shuffles. In [**6**] there is a description of the ternary representation for a deck of 27 cards. We have not found a published proof for the general case so we give one here.

PROPOSITION 3. *To bring the top card to position r, label the cards from 0 to $kn-1$, label the piles from 0 to $k-1$, and express r in base k as $r = d_m k^m + \cdots + d_1 k + d_0$, with $0 \le d_i < k$. For each i let τ_i be any permutation that transposes 0 and d_i. Then $s_{\tau_m} \cdots s_{\tau_1} s_{\tau_0}$ maps 0 to r.*

Proof. Let τ be any permutation that transposes 0 and d and is otherwise arbitrary. For card i where $0 \le i \le n-1$, we have $s_\tau(i) = ki + d$. Now the result follows by induction on m. Assuming that $s_{\tau_m} \cdots s_{\tau_1}$ has put the top card into position $i = d_m k^{m-1} + \cdots + d_2 k + d_1$, then $s_{\tau_0}(i) = d_m k^m + \cdots + d_1 k + d_0 = r$. Note that $i \le n-1$ since $r \le kn-1$, and so the rule applies to i.

From this it follows that the group $G_{k,kn}$ acts *transitively* on the set of cards. That means for any two cards i and j there is an element of the group that moves i to j.

Card tricks can be based on the algorithm of Proposition 3. A deck of kn cards is used from which the spectator draws a card. The card is replaced in the deck without letting the magician see it. The magician deals out k piles of n cards face up and asks the spectator to identify the pile containing the card. The magician gathers the cards and repeats the process. After several repetitions, the unknown card appears on the top of the deck. Dealing out the cards and stacking up the pile is the inverse of a shuffle, $(s_\sigma)^{-1}$, where σ is the permutation corresponding to the order in which the piles are picked up. The magician picks up the piles so that the pile with the card and the top pile have their positions interchanged. This procedure inverts the algorithm of Proposition 3 and brings the spectator's card to the top. The cards must be dealt out m times where m is the smallest integer such that $kn \le k^m$. For maximum effect for the same amount of work the magician should use a deck with k^m cards.

Deck size a power of k

An ancient trick going back centuries is the "three-pile trick" using 27 cards. In this version the mystery card appears in the middle—the thirteenth card—after three rounds. A generalization of this trick using m^m cards and an analysis of the trick were given by M. Gergonne in 1813. They are discussed in [**1**] and can be done with any values of k and n. However, the 27 card deck does seem to have a special fascination. It turns out that the shuffle groups G_{k,k^m}, where the deck size is a power of k, are quite special. They are quite small compared to the other shuffle groups because there is a lot of rigidity in the deck for these shuffles.

As a senior project at Cal Poly, one of us (Medvedoff) set out to find out anything he could about $G_{k,kn}$ for $k \ge 3$, only having seen [**7**], a brief account of the work of Diaconis, Graham, and Kantor on binary shuffle groups. Soon he noticed that there was something special about $G_{3,9}$ and $G_{3,27}$ and all the groups G_{k,k^m}. The main result in the senior project is the calculation of the order of G_{k,k^m}. It is $m(k!)^m$. After Medvedoff explained the results to his advisor (Morrison), both of us worked on the structure of the group. Without the CAYLEY program or any electronic computer, we found that a deck of cards—a primitive cellulose computer—was essential in understanding the group. In particular, we figured out $G_{3,27}$, whose order is 648, and then abstracted the key features. We strongly advise you to prepare a deck of 27 cards using the ace through nine of three suits. Arrange them from ace to nine in each suit and stack the suits. This is your initial order. Now start shuffling. Divide the deck into suits. Move the suits around and then pick up the cards from left to right. Keep the cards face up and pick up the cards so that the first one picked up is the top card. Doing this you will develop an understanding of $G_{3,27}$ so that you will know what the possible configurations are and how to arrive at them. Then you may finish reading this note.

We label the cards with m-tuples whose entries are the integers $1,2,\ldots,k$ and arrange them 'lexicographically' so that the first card is $(1,1,\ldots,1)$, the second is $(1,1,\ldots,1,2)$, and the last card is $(k,k,\ldots,k)$. After executing the shuffle s_σ the cards are arranged in the following order:

$$\begin{array}{c}
(\sigma^{-1}(1),1,\ldots,1)\\
(\sigma^{-1}(2),1,\ldots,1)\\
\vdots\\
(\sigma^{-1}(k),1,\ldots,1)\\
(\sigma^{-1}(1),1,\ldots,1,2)\\
\vdots\\
(\sigma^{-1}(k),1,\ldots,1,2)\\
\vdots\\
(\sigma^{-1}(k),k,\ldots,k).
\end{array}$$

The card labeled $(i_1,\ldots,i_m)$ is now in position $(i_2,\ldots,i_m,\sigma(i_1))$. The sequence of shuffles $s_{\sigma_1}\cdots s_{\sigma_m}$ puts cards $(i_1,\ldots,i_m)$ into position $(\sigma_1(i_1),\ldots,\sigma_m(i_m))$. The elements of G of the form $s_{\sigma_1}\cdots s_{\sigma_m}$ make up a subgroup N of G that we will show to be normal. With 27 cards, the first digit determines the suit. After any three shuffles the suits are back together, although they may be moved around. To see that N is normal, we conjugate any element of N by any shuffle s_τ. We determine $s_\tau(s_{\sigma_1}s_{\sigma_2}\cdots s_{\sigma_m})s_\tau^{-1}$ by its effect on $(i_1,\ldots,i_m)$. First s_τ sends it to $(i_2,\ldots,i_m,\tau(i_1))$. Then the sequence of m shuffles sends that to $(\sigma_1(i_2),\sigma_2(i_3),\ldots,\sigma_{m-1}(i_m),\sigma_m(\tau(i_1)))$. Then s_τ^{-1} maps to the $(\tau^{-1}(\sigma_m(\tau(i_1))),\sigma_1(i_2),\sigma_2(i_3),\ldots,\sigma_{m-1}(i_m))$. Thus,

$$s_\tau(s_{\sigma_1}\cdots s_{\sigma_m})s_\tau^{-1} = s_{\tau\sigma_m\tau^{-1}}s_{\sigma_1}\cdots s_{\sigma_{m-1}}.$$

Notice that we write $\tau^{-1}\circ\sigma_m\circ\tau$ as $\tau\sigma_m\tau^{-1}$ because our convention is to write operations from left to right. This element is in N because it is a product of m shuffles.

Next, $G/N\cong\mathbb{Z}_m$ because any group element can be written as $s_{\sigma_1}\cdots s_{\sigma_m}s_I^e$, uniquely if $0\le e<m$. This is because s_I cyclically permutes $(i_1,\ldots,i_m)$ by moving the first component to the end, and any sequence of shuffles maps $(i_1,\ldots,i_m)$ to some cyclic permutation of $(\sigma_1(i_1),\ldots,\sigma_m(i_m))$. We identify $\mathbb{Z}_m$ with the subgroup of G consisting of the powers of s_I, which has order m. The subgroup N is the product $(S_k)\times\cdots\times(S_k)$, m times. If we multiply $(s_{\sigma_1}\cdots s_{\sigma_m})(s_{\tau_1}\cdots s_{\tau_m})$, we get $s_{\sigma_1\tau_1}\cdots s_{\sigma_m\tau_m}$ by considering what happens to $(i_1,\ldots,i_m)$.

We will describe the possible arrangements of the 27 card deck whose original order is A to 9 in the suits spades, hearts, clubs. The normal subgroup N is easy to describe, since an element of N leaves all cards in the same suit together. For example, the element $s_{(12)}s_{(23)}s_I$ acts as shown in FIGURE 1. Here, $s_{(12)}$ permutes the suits by interchanging the first—spades—with the second—hearts. Then $s_{(23)}$ permutes the subsuits of the suits, the second subsuit 4,5,6 is

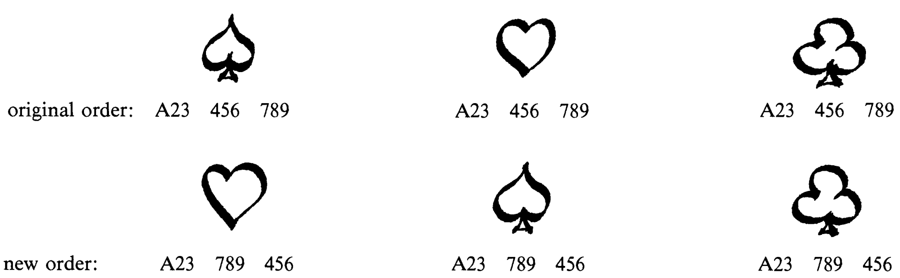

FIGURE 1.

interchanged with the third subsuit 7, 8, 9. This takes place in each of the suits. Finally, the last shuffle s_I leaves the cards in each subsuit alone. The arrangement within each suit is the same. An arbitrary element of the group is something in N followed by s_I^0, s_I or s_I^2. Of course, s_I^0 leaves well enough alone. A single power of s_I leaves the deck with the suits changing every card, while s_I^2 puts three cards of the same suit together. Then s_I^3 puts 9 cards of each suit together, which brings the deck back to N. To determine whether a given arrangement is in $G_{3,27}$ and what it is, first determine the power of s_I that is required. Then shuffle by s_I as many times as needed to reach N. You can recognize the element $s_{\sigma_1}s_{\sigma_2}s_{\sigma_3}$ in N by noting how the suits are permuted by σ_1, the subsuits by σ_2, and the individual cards in the subsuits by σ_3.

Now that we see $G = G_{3,27}$ has a normal subgroup $N = S_3 \times S_3 \times S_3$ and quotient group $K = \mathbb{Z}_3$, we have to put them together to get G. G is not the direct product of N and K, but rather a semidirect product. There are two standard ways to describe semidirect products, both useful. The first is that a group G with normal subgroup N and quotient $K = G/N$ is a **semidirect product** of N by K if there is a homomorphism i: $K \to G$ that identifies K with a subgroup of G and such that the composition $K \to G \to G/N = K$ is the identity map on K. In our example, the quotient G/N can be identified with the cyclic subgroup generated by the standard shuffle s_I. The second definition of a semidirect product begins with groups K and N and builds G. If we have a group homomorphism θ: $K \to \mathrm{Aut}(N)$ where $\mathrm{Aut}(N)$ is the group of automorphisms of N, then we define a group $G = N \times_\theta K$ called the semidirect product of N by K. As a set, G is the Cartesian product $N \times K$. We define the group operation $(n_1, k_1)(n_2, k_2) = (n_1\theta(k_1)(n_2), k_1k_2)$. If the homomorphism θ is not explicitly given, the notation $N \rtimes K$ is also used, emphasizing that N is the normal subgroup. Identify N and K with the subgroups $N \times \{1\}$ and $K \times \{1\}$. Then N will be normal and $\theta(k)$ will correspond to conjugation of $(1, k)$ on $N \times \{1\}$.

Now the action θ of $K = \mathbb{Z}_m$ on $N = S_k \times \cdots \times S_k$ is easy to describe. The generator s_I of $\mathbb{Z}_m$ conjugates an element of N, say $s_{\sigma_1} \cdots s_{\sigma_m}$, by

$$s_I(s_{\sigma_1} \cdots s_{\sigma_m})s_I^{-1} = s_{\sigma_m}s_{\sigma_1} \cdots s_{\sigma_{m-1}}.$$

So we have our theorem.

THEOREM 2. *The shuffle group G_{k,k^m} is the semidirect product of $S_k \times \cdots \times S_k$, m factors, by $\mathbb{Z}_m$ acting by cyclic permutation of the factors. In particular, the generator of $\mathbb{Z}_m$ corresponding to s_I permutes $S_k \times \cdots \times S_k$ by $(\sigma_1, \dots, \sigma_m) \mapsto (\sigma_m, \sigma_1, \dots, \sigma_{m-1})$. The order of the group is $m(k!)^m$.*

Additional comment. This semidirect product is an example of a **wreath product**. The binary shuffle groups are wreath products or very close to wreath products. The symmetry group of Rubik's cube is a wreath product, too. A wreath product is constructed from a group H and a permutation group $P \subset S_m$ by taking the semidirect product of $H \times \cdots \times H$, m factors, with P acting by permuting the factors. Thus we can say G_{k,k^m} is the wreath product of S_k with $\mathbb{Z}_m$.

The binary shuffle groups

To understand $G_{2,2n}$ there is an important symmetry principle called **central symmetry**. Number the cards $1, 2, \dots, n-1, n, n', (n-1)', \dots, 2', 1'$. After shuffling, the order is:

out shuffle: $1, n', 2, (n-1)', \dots, n-1, 2', n, 1'$.
in shuffle: $n', 1, (n-1)', 2, \dots, 2', n-1, 1', n$.

The centrally symmetric pair $\{i, i'\}$ is now in the pair of positions $\{j, j'\}$ for some j. So the cards i and i' that are the same distance from the center remain the same distance from the center. Thus the shuffle group $G_{2,2n}$ is a subgroup of the group $B_n \subset S_{2n}$ consisting of centrally symmetric permutations. B_n is the Weyl group of a simple Lie algebra and has other descriptions. It is the symmetry group of the n-dimensional cube with vertices $\pm e_1, \dots, \pm e_n$. A symmetry must map the pair of vertices $\pm e_i$ to a pair of vertices $\pm e_j$ for some j. Such a linear map on $\mathbb{R}^n$ is represented by a signed permutation matrix: each row and column has only one nonzero entry and that entry is 1 or -1. There is a surjective homomorphism $B_n \twoheadrightarrow S_n$ that forgets the signs in the permutation matrix. With our card deck it means we only keep track of the induced permutation on the set of n symmetric pairs. Therefore, we can consider the parity of the induced permutation in $\underline{S_n}$ as well as the parity of the permutation in S_{2n}. We have group homomorphisms sgn and $\overline{\text{sgn}}$ from B_n to the group $\{\pm 1\}$:

$$\text{sgn}\colon B_n \hookrightarrow S_{2n} \to \{\pm 1\} \quad \overline{\text{sgn}}\colon B_n \twoheadrightarrow S_n \to \{\pm 1\}.$$

We also have the product of these homomorphisms, $\text{sgn}\,\overline{\text{sgn}}\colon B_n \to \{\pm 1\}$, which is a group homomorphism. The binary shuffle groups $G_{2,2n}$ are given by B_n and various kernels of these three homomorphisms. They consist of five families and two special cases.

(0) If $n \equiv 0 \pmod 4$, $n > 12$ and not a power of 2, then $G = \operatorname{Ker}\text{sgn} \cap \operatorname{Ker}\overline{\text{sgn}}$.
(1) If $n \equiv 1 \pmod 4$, then $G = \operatorname{Ker}\overline{\text{sgn}}$.
(2) If $n \equiv 2 \pmod 4$, then $G = B_n$.
(3) If $n \equiv 3 \pmod 4$, then $G = \operatorname{Ker}\text{sgn}\,\overline{\text{sgn}}$.
(4) If $2n = 2^m$ then $G = (\mathbb{Z}_2)^m \times_\theta \mathbb{Z}_m$, where $\mathbb{Z}_m$ acts cyclically on the factors.
(5) The two anomalous cases
  (i) If $n = 6$, then G is the semidirect product $(\mathbb{Z}_2)^6 \rtimes \mathrm{PGL}(2,5)$. See [4] for a description of the action.
  (ii) If $n = 12$, then G is the semidirect product of $(\mathbb{Z}_2)^{11}$ by the Mathieu group M_{12}. The group M_{12} is a subgroup of S_{12} and so it acts naturally on $(\mathbb{Z}_2)^{12}$ by permuting the factors. This action restricts to the subspace of vectors whose components sum to zero. The subspace is 11-dimensional, hence isomorphic to $(\mathbb{Z}_2)^{11}$.

For the ordinary deck of 52 cards, n is 26 and $26 \equiv 2 \pmod 4$. The shuffle group is all of B_{26}. The only restriction on possible configurations is that of central symmetry. We can count the order directly. There are 52 places for the first card, but then the last one must go to a determined location. There are 50 remaining places for the second card, and so on. There are $52 \cdot 50 \cdot 48 \cdots 4 \cdot 2$ arrangements possible. This is $2^{26}(26)!$, a large number, but a small fraction of $(52)!$.

Ternary shuffle group

TABLE 1, compiled with the aid of CAYLEY, points to an obvious conjecture about $G_{3,3n}$. The

$3n$	$G_{3,3n}$	$3n$	$G_{3,3n}$
3	S_3	39	S_{33}
6	S_6	42	S_{42}
9	$(S_3)^2 \rtimes \mathbb{Z}_2$	45	S_{45}
12	A_{12}	48	A_{48}
15	S_{15}	51	S_{51}
18	S_{18}	54	S_{54}
21	S_{21}	57	S_{57}
24	A_{24}	60	A_{60}
27	$(S_3)^3 \rtimes \mathbb{Z}_3$	63	S_{63}
30	S_{30}		
33	S_{33}		
36	A_{36}		

TABLE 1

evidence shows that $G_{3,3n}$ is as large as possible subject to the parity theorem as long as n is not a power of 3.

CONJECTURE. *The classification of* $G_{3,3n}$ *is given by three families*:
(1) *If n is a multiple of* 4, *then* $G_{3,3n} = A_{3n}$.
(2) *If n is not a multiple of* 4 *and not a power of* 3, *then* $G_{3,3n} = S_{3n}$.
(3) *If* $3n = 3^m$, *then* $G_{3,3n} = (S_3)^m \rtimes \mathbb{Z}_3$.

Part (3) has been proved, but we include it for a complete statement.

We have been able to verify the computer results by hand in any of the individual cases, but we have not been able to prove the conjecture. Each case looks a little different but the strategy is the same. We will present a proof that $G_{3,21} = S_{21}$ to illustrate how you can verify the results.

For generators, we use $s = s_I$, p, and q, where p permutes the first and second piles of 7 cards and q cyclically permutes all three piles. Notice that p and q are not shuffles but permutations that we earlier called p_σ. Number the cards from 0 to 20 and recall that s is multiplication by 3 modulo 20 and s fixes 20. The cycle forms of the generators are:

$$s = (1,3,9,7)(2,6,18,14)(4,12,16,8)(5,15)(11,13,19,17)$$

$$p = (7,14)(8,15)(9,16)(10,17)(11,18)(12,19)(13,20)$$

$$q = (0,7,14)(1,8,15)(2,9,16)(3,10,17)(4,11,18)(5,12,19)(6,13,20).$$

Let $G = G_{3,21}$; G is transitive by Proposition 3. Now s and p both fix the top card 0 so they lie in the stabilizer subgroup of 0. The subgroup generated by s and p permutes $1,2,\ldots,20$ and by looking at the cycles of s and p we can see that this subgroup is transitive on $1,2,\ldots,20$. Thus G is **doubly transitive,** meaning that any pair (i_1, i_2) can be mapped to any other pair (j_1, j_2) by some $g \in G$: $g(i_1) = j_1$ and $g(i_2) = j_2$. A doubly transitive group is **primitive**, meaning that there is no way to partition the deck into subsets of equal size $X_1, \ldots, X_r$ (other than the singleton subsets and the whole set) so that the permutations map each X_i to some X_j. (It may help to note that the binary shuffle groups are not primitive because the deck partitions into the central symmetric pairs which have this property.) A classical theorem of Jordan states that a primitive group containing a transposition is the symmetric group and one containing a 3-cycle is at least the alternating group [**11**]. We compute sq and find

$$sq = (0,7,8,11,20,6,4,19,3,16,15,12,2,13,5,1,10,17,18)(9,14).$$

The long cycle has length 19, so that $(sq)^{19} = (9,14)$. Hence G contains a transposition and by Jordan's theorem, $G = S_{21}$.

The strategy that works on these particular groups is to show that G is doubly transitive, hence primitive, and to exhibit a transposition or a 3-cycle, which is found by experimentation. In general, to show that $G_{3,3n}$ is doubly transitive it would suffice to show that the subgroup generated by s and $p_{(2,3)}$ is transitive on $\{1,\ldots,3n-1\}$ as both of them fix 0. Here $p_{(2,3)}$ is the permutation of piles 2 and 3, where the piles are numbered $1,2,3$. For $n \leq 21$, we know that this subgroup, denoted by $\langle s, p_{(2,3)} \rangle$, is transitive on $\{1,\ldots,3n-1\}$, having checked those cases with CAYLEY. In fact, in these cases $\langle s, p_{(2,3)} \rangle$ is either the alternating or the symmetric group, A_{3n-1} or S_{3n-1}, the alternating group occurring when n is a multiple of 4.

There are two ways to proceed to get a full proof of the structure conjecture.
(1) Show $\langle s, p_{(2,3)} \rangle$ is transitive and then show that $G_{3,3n}$ always contains a 3-cycle.
(2) Show $\langle s, p_{(2,3)} \rangle$ is A_{3n-1} or S_{3n-1}. From this it follows that $G_{3,3n}$ is A_{3n} or S_{3n}.

$k = 4$ and beyond

What happens for $k \geq 4$? We believe that, generically, $G_{k,kn}$ is A_{kn} or S_{kn} according to Theorem 1, but not so generically as the case of $G_{3,3n}$ indicates. We found that $G_{4,8}$ is not the expected A_8 and $G_{4,32}$ is not the expected A_{32}. The order of $G_{4,8}$ is 1344, whereas $|A_8| = 20{,}160$, and the group is isomorphic to the semidirect product of $(\mathbb{Z}_2)^3$ by GL(3,2), the group of invertible 3×3 matrices over the field $\mathbb{Z}_2$, which acts linearly on the vector space $(\mathbb{Z}_2)^3$. This is just the affine group of the 3-dimensional vector space V over $\mathbb{Z}_2$ consisting of the maps f: $V \to V$ of the form $f(x) = \varphi(v) + v_0$ for an invertible linear map φ and with $v_0 \in V$. GL(3,2) is also the same as PGL(3,2) or PL(3,2) since the general linear groups and the projective (general) linear groups are the same over fields of characteristic 2. GL(3,2) is a simple group of order 168, the smallest nonabelian simple group larger than A_5 of order 60. Likewise, $G_{4,32}$ is the affine group of the 5-dimensional vector space over $\mathbb{Z}_2$, so $G_{4,32} = (\mathbb{Z}_2)^5 \rtimes \mathrm{GL}(5,2)$. Both of these results come from using CAYLEY and we have only verified $G_{4,8}$ by hand. Our data are summarized in TABLE 2.

$4n$	$G_{4,4n}$
8	$\mathbb{Z}_2^3 \rtimes GL(3,2)$
12	S_{12}
16	$(S_4)^2 \rtimes \mathbb{Z}_2$
20	S_{20}
24	A_{24}
28	S_{28}
32	$\mathbb{Z}_2^5 \rtimes GL(5,2)$

TABLE 2

CONJECTURE. *There are four families classifying* $G_{4,4n}$.
(1) *If n is a power of* 4, *let* $4n = 4^m$. *Then* $G_{4,4n}$ *is* $(S_4)^m \rtimes \mathbb{Z}_m$.
(2) *If n is an odd power of* 2, *let* $4n = 2^{2m+1}$. *Then* $G_{4,4n}$ *is* $(\mathbb{Z}_2)^{2m+1} \rtimes GL(2m+1,2)$.
(3) *If n is even and not a power of* 2, *then* $G_{4,4n} = A_{4n}$.
(4) *If n is odd*, *then* $G_{4,4n} = S_{4n}$.

Part (1) is proved already. Part (2) is an obvious target to attack, but to understand $G_{4,8}$ using pencil, paper, and cards is tedious. The eight cards correspond to the eight points in the 3-dimensional vector spaces $(\mathbb{Z}_2)^3$, the top card being the origin $(0,0,0)$. We express each of the three generators as an affine map so that we know $G_{4,8}$ is a subgroup of the affine group. This is straightforward but does not suggest a way of generalizing to 2^{2m+1} cards. Finally we check that each of the eight translations is in $G_{4,8}$ and that we can fix the top card and map the three basis cards $(0,0,1)$, $(0,1,0)$, and $(1,0,0)$ to any three linearly independent positions. For the last part, working with a deck of eight cards has been convincing and we have to admit we have not written out the details. There must, however, be a better way to do it. You do not want to go on to $G_{4,32}$ and the larger groups in the same way.

Conjecturing that $G_{9,27}$ might be something along the line of $G_{4,8}$, we checked it with CAYLEY but found that $G_{9,27} = S_{27}$ and was not an affine group over the field $\mathbb{Z}_3$. Some shuffle groups for $k \geq 5$ are in TABLE 3.

k	kn	$G_{k,kn}$
5	10	A_{10}
5	15	S_{15}
5	20	A_{20}
6	12	S_{12}
6	18	S_{18}
7	14	S_{14}
8	16	A_{16}
9	27	S_{27}

TABLE 3

William Kantor reports that he has shown that $G_{k,kn}$ is A_{kn} or S_{kn} when $k \geq 4$ and k does not divide n. We have not seen his argument. This leaves open the case $k = 3$. It also suggests that when k^2 divides the deck size as in $G_{4,8}$ or $G_{9,27}$ you must be more careful.

S. B. Morris, in his 1974 thesis [**8**], and together with R. E. Hartwig in [**9**], consider generalized shuffles of decks of size $kn + m$, $0 \leq m < n$. Shuffle by dividing the deck into k piles, m of them having $n + 1$ cards and the rest having n cards. They consider the out-shuffle or "generalized faro shuffle" and the permutation called the "simple cut" that moves the top card to the bottom of the deck. They determine when the group generated by these two permutations is the symmetric group or the alternating group. They also determine the order of the generalized in-shuffle. (We gave a proof in Proposition 2 for $m = 0$.)

M. Davio and C. Ronse, both of the Philips Research Laboratories in Brussels, have generalized the shuffles using a mixed-radix formalism (mixed-base notation). Their generalizations are in a different direction than ours but could fit into a common generalization of the notion of shuffling. They are interested in shuffles for their application to problems in parallel processing and switching network design. We refer the interested reader to [**3**] and [**10**]. Incidentally, the structure of $G_{2,2^m}$ is of interest in the computational scheme of the Fast Fourier Transform. See [**4**] for a description.

One last question

You probably have noticed the big difference between the binary shuffle groups, $k = 2$, and the groups with $k \geq 3$. We cannot resist mentioning that the groups generated by the out-shuffle s_I and the in-shuffle s_{rev} may be more like the binary shuffle groups which have just those generators. Let $H_{k,kn} \subset G_{k,kn}$ be the subgroup generated by s_I and s_{rev}. Our final question is: *What is the structure of $H_{k,kn}$ for all k and n*? Of course, for $k = 2$ we know the answer since $H_{2,2n} = G_{2,2n}$, but for $k \geq 3$ this is a much more difficult question. For $H_{3,3n}$ we have data from CAYLEY up to 69 cards. There is some tantalizing regularity but not enough. The whole situation is much more complicated than the case $k = 2$ or the case $G_{3,3_n}$. One intriguing result is that $H_{3,24} = H_{2,24}$, which is a semidirect product of $(\mathbb{Z}_2)^{11}$ by the Mathieu group M_{12}. We have also heard indirectly that $H_{d,24} = H_{2,24}$ for any d a proper divisor of 24. The groups $H_{k,kn}$ have central symmetry, the key feature in the binary shuffles, and so it is not surprising they bear so much resemblance.

References

[1] W. W. Rouse Ball, H. S. M. Coxeter, Mathematical Recreations and Essays, 12th ed., University of Toronto Press, Toronto, 1974.

[2] J. J. Cannon, Description of CAYLEY, preprint, Univ. of Sydney.

[3] M. Davio, Kronecker products and shuffle algebra, IEEE Trans. Computers, C-30 (1981) 116–125.

[4] P. Diaconis, R. L. Graham, W. M. Kantor, The mathematics of perfect shuffles, Adv. Appl. Math., 4 (1983) 175–196.

[5] M. Gardner, Mathematical Carnival, Vintage, New York,·1977.
[6] ______, Mathematics, Magic, and Mystery, Dover, New York, 1956.
[7] G. Kolata, Perfect shuffles and their relation to math, Science, 216 (1982) 505–506.
[8] S. B. Morris, Permutations by cutting and shuffling—a generalization to q-dimensions, Thesis, Duke University, 1974.
[9] S. B. Morris, R. E. Hartwig, The generalized faro shuffle, Discrete Math., 15 (1976) 333–346.
[10] C. Ronse, A generalization of the perfect shuffle, Discrete Math., 47 (1983) 293–306.
[11] H. Wielandt, Finite Permutation Groups, trans. R. Bercov, Academic Press, New York, 1964.

"Such a really remarkable discovery. I wanted your opinion on it. About God. You know the formula: m over nought equals infinity, m being any positive number? Well, why not reduce the equation to a simpler form by multiplying both sides by nought? In which case, you have m equals infinity times nought. That is to say that a positive number is the product of zero and infinity. Doesn't that demonstrate the creation of the universe by an infinite power out of nothing? Doesn't it?"...

"'Well,' began Lord Edward, at the other end of the electrified wire, forty miles away, his brother knew, from the tone in which the single word was spoken, that it was no good. The Absolute's tail was still unsalted."

—ALDOUS HUXLEY, *Point Counter Point,*
Chapter XI