Jon Glapa

On Card Shuffles and Group Theory: “Groups of Perfect Shuffles”

“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.”

Written by Steve Medvedoff and Kent Morrison, the article “Groups of Perfect Shuffles” applies several concepts from group theory to further understand the intriguing concept of shuffle groups. The initial idea of shuffling a deck eight times only to return it to its original position is both mind-boggling and fascinating. Imagine opening a brand new deck of 52 cards (with the cards arranged in both the order of their ascending numeric value and by suit), handing the deck to your friend, watching her shuffle it eight times and then picking up the deck only to find that the order of the cards hasn’t changed. This situation lends itself to a fundamental question of the article: what exactly is a perfect shuffle?

Before delving into the group theory dynamics behind the concept of shuffle groups, one must first understand some key definitions. A perfect shuffle is a “particular way of permuting the cards in a deck” (Medvedoff, p.3). First, consider the standard 52-card deck. A normal perfect shuffle here would be to divide the deck into two equal piles, each with 26 cards, and then shuffling the two piles together by interleaving them perfectly (that is, by combining the two piles back into a single pile of 52 cards that now alternates between a card from the first pile and a card from the second pile).

We can generalize the concept of this standard shuffle by permitting the deck to be initially divided into more than two piles. For example, consider a deck of 21 cards in which the cards are numbered 1 to 21. Let the deck be divided into 3 piles of 7 cards each, forming a left, middle and right pile. There are $3! = 6$ possible permutations of the piles themselves. Select one of these arrangements, then proceed to pick up the top card in the left-most pile, then the top card in the middle pile and finally in the right pile. After doing so, go back to the left-most pile and pick up the second card, proceed to the middle … and so on until all the cards are picked up. In doing so, we are actually seeing that we already have $3!$ possible permutations of the numbers 1, 2, ..., 21. This type of shuffle is called a 3-shuffle. If we view the set of numbers 1, 2, ..., 21 as $S_{21}$, then the question becomes, what subgroup of $S_{21}$ do our permutations of the shuffle groups of a 21-card deck form? As we’ll soon see, the answer is actually all of $S_{21}$.

The article introduces some notation in order to make the explanation of the group theory influence more understandable. We let $k$ be the number of piles we divide the deck into; since the total number of cards in the deck must then be divisible by $k$, we say there are $kn$ cards in the deck. As the article notes, the integers $k$ and $n$ generate a subgroup of $S_{kn}$, and the main focus of the article lies in exploring the structure of this subgroup for various perfect $k$-shuffles and $n$. Therefore, $G_{k, kn}$ is the subgroup formed from perfect $k$-shuffles of $kn$ cards.

It turns out that a lot is already known about the structure of $G$ for $k=2$, 3 or 4. Here is a brief summary of the results extracted from the paper so that we can spend more time on how the results came to be known (p.4).
The binary shuffle groups $G_{2,2n}$ are all taken care of. There are five infinite families and two exceptional cases.

(2) We have determined $G_{k,k^m}$ and we will describe it later in this paper.

(3) $G_{3,3n}$ is understood for deck sizes up to 63, 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.

The group theory mathematics behind the problem of understanding the structures of these groups begins with permutations. We start first with permutations of the piles, which we will call $\beta$. $\beta$ is a permutation, and with the $k$ piles numbered $1,\ldots, k$, $\beta$ is a bijection from the set $\{1,\ldots, k\}$ to itself. Thus, it can permute the elements in a manner such as $\beta(3) = 5$, meaning the third pile moves to the fifth pile’s position. In cycle form, this would mean $(35)$ appears somewhere in the cycle, as in $\beta=(35\ldots)$. $\beta$ lies in $S_k$, the group of permutations of the $k$ piles. For each $\beta$, we have the corresponding shuffle $s_\beta$. This shuffle, $s_\beta$, can be written as the product of two permutations such that $s_\beta=p_\beta s_I$, where $p_\beta$ permutes the piles of the deck and $s_I$ does the actual interleaving (shuffling) of the cards in the manner described above (note: these permutations are written from left-to-right, which is the opposite of the way we wrote permutations in class). $s_I$ can be written as just $s$, and it is called the standard shuffle. From here, we will focus on the fundamental group theory aspects of the article.

One main theorem in this proof relates $G_{k,kn}$ to $A_{kn}$, the group of even permutations of $kn$ elements. It is as follows:

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

(i) $[n]_4 = [0]_4$

(ii) $n$ is even and $[k]_4 = [0]_4$ or $[1]_4$

The theorem above was derived from two preceding proofs relating to the parity of the permutations. The first statement leading to this theorem starts to show some more obvious areas of overlap with the material covered in Math 152:

**LEMMA 1.** If $n$ is odd and $\beta$ is in the group $S_k$ and $\beta$ is an odd permutation, then $p_\beta$ is odd; otherwise, $p_\beta$ is even.

To understand LEMMA 1, consider the $k$ piles of $n$ cards each that the deck has been divided into. If, for example, $\beta=(12)$, then this is essentially trading the places of $n$ pairs of cards from pile 1 to pile 2. Thus, for every transposition in $\beta$, we get $n$ transpositions of $p_\beta$. So, if $n$ is odd and $\beta$ can be written as an odd number of transpositions, we have an odd x odd = odd number of transpositions in $p_\beta$. The second statement leading to this theorem is as follows:

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

The proof for LEMMA 2 is longer, and I won’t discuss its entirety for brevity’s sake. Yet, the proof successfully shows that $s$ can be written as $[n(n-1)/2][k(k-1)/2]$ transpositions.

For almost every value of $k$ or $n$, THEOREM 1 allows us to tell if $G_{k,kn}$ has the same structure as $A_{kn}$ or $S_{kn}$. Yet, this theorem leads to another question. Given that it only holds the vast majority, but not all, of the time, when THEOREM 1 fails to give the structure of $G$, what does $G$ look like?
One interesting area where Theorem 1 fails is when the deck size is a power of $k$, that is, when $kn = k^m$ for some integer $m$. In fact, groups of this sort are actually far smaller than $A_{kn}$ or $S_{kn}$. To experiment on your own, get the ace through nine of three suits, place them numerically ordered in three piles and shuffle the cards by permuting the piles then picking the cards up (do this! You’ll be able to see why the group is relatively small). Medvedoff found that the order of a group of this form is $m(k!)^m$.

Again, consider a deck of 27 cards. After 3 shuffles, the suits will be back together, but, depending on the permutations of the piles, the cards will be moved around (did you try it yourself yet?). The elements of $G_{3, 27}$ that are formed from 3 shuffles actually form a normal subgroup, $N$; more generally, the elements of $G_{k,k^m}$ that are formed from 3 shuffles form a normal subgroup, $N$. We know that these elements form a normal subgroup because we can conjugate any one of these shuffles by another shuffle, $s_3$, to get another element in $N$. Moreover, in $G_{3, 27}$, we can then see $N$ as the product $(S_3) \times (S_3) \times (S_3)$.

Because $N$ is a subgroup, we can develop the quotient group $G_{3,27}/N$, which is isomorphic to the integers modulo $3$. One last definition is necessary to state the final theorem. A group $G$ with a normal subgroup $N$ and quotient $K = G/N$ is a semidirect product of $N$ by $K$ if there is a homomorphism $i: K \rightarrow G$ that identifies $K$ with a subgroup of $G$ such that the composition $K \rightarrow G \rightarrow G/N=K$ is the identity map on $K$ (p.9). Essentially, a semidirect product allows us to construct a group from two subgroups given that one of the subgroups, $N$ in this case, is normal. Thus, we arrive at the second theorem.

Theorem 2: The shuffle group $G_{k,k^m}$ is the semidirect product of $S_k \times \ldots \times S_k$, $m$ factors, by the integers modulo $m$ acting by cyclic permutation of the factors. In particular, the generator of the integers modulo $m$ corresponding to $s_1$ permutes $S_k \times \ldots \times S_k$ by $(\beta_1, \ldots, \beta_m) \rightarrow (\beta_m, \beta_1, \ldots, \beta_{m-1})$. The order of the group is $m(k!)^m$.

The article goes on to explore other areas where Theorem 1 does not hold and also when $k=4$ or higher. There are areas of application of shuffle groups, most prominently in card tricks, as you might guess from the numerous card references in this paper. Yet, shuffle groups also offer an intriguing, hands-on insight into group theory, and there are still numerous aspects of group shuffles to be examined.