Parabola Volume 47, Issue 3 (2011)

Shuffling Along and Cycling Around

David Angell [1]

Many readers will at some time have played games with a pack of cards. In most games one begins by shuffling the cards so as to randomise their order. There are various different ways of shuffling, one of the most popular being the *riffle shuffle*. In this shuffle, the pack is split into two roughly equal parts, one is held in each hand, with the edges adjacent:

The thumbs are used to flip through the two parts so that they are merged together again, cards falling more or less from each hand alternately. If you haven't seen a riffle shuffle before, this description probably didn't help much! Perhaps the picture[2] will give you the idea, or you could ask a friend to demonstrate. If you want to see a video of the riffle shuffle, just go to YouTube [1]. For this article we'll work with a standard pack of 52 cards, and we'll imagine that we can perform a *perfect* riffle shuffle: that is, we begin by dividing the pack into two parts of *exactly* 26 cards each, and then we combine them by interleaving *exactly* one card at a time from each hand. This still leaves two possibilities, depending on which hand releases the first card: the bottom card after the shuffle could be the original bottom card, or it could be the last card from the top half (that is, the original 26th card). The former possibility is known as an *outshuffle*, the latter as an *inshuffle*.

It might seem very difficult to do an absolutely perfect riffle shuffle. (It is – I've tried it!) Amazingly, some people can do it. Even more amazingly, some people can do it eight times in a row! Most amazingly of all, if you perform eight successive perfect

[1] Dr David Angell is a Pure Mathematician and Associate Lecturer in the School of Mathematics and Statistics at the University of New South Wales.

[2] Photo: Todd Klassy, available from Flickr under Creative Commons 2.0 at http://tinyurl.com/pnt6ngz.

outshuffles, *the pack returns to its original order!!* Of course you can check that this is true by doing your riffle shuffles very slowly and carefully, but that takes forever and is extremely boring. So let's do it by mathematics instead.

We need to begin by being very clear on what a shuffle actually is. Imagine that I perform a very simple shuffle by taking the top card of the pack and placing it on the bottom. Then I shuffle again by taking the (new) top card and placing it on the bottom. Even though I have moved different cards, I have just performed *the same shuffle* twice: a shuffle is not a rearrangement of specific cards, but *a way of rearranging cards*. In mathematical terms, it is a function s, where $s(k)$ is the position after the shuffle of the card which was in position k before the shuffle. Note that this has nothing to do with the particular card in any position before or after the shuffle. For example, in the simple shuffle we have just considered (twice), the card in position 1 goes to position 52 while every other card moves up to the previous position. So this shuffle is described by the formula

$$s(k) = \begin{cases} 52 & \text{if } k = 1 \\ k-1 & \text{if } k = 2, 3, \dots, 52. \end{cases}$$

Now how about a riffle shuffle? For an outshuffle we split the pack into two halves, one consisting of the cards in positions $1, 2, \dots, 25, 26$ and the other of those in positions $27, 28, \dots, 51, 52$; then we interleave the two halves. Since the card in position 52 after the shuffle is the same as that in position 52 before the shuffle, we see that the cards in positions $27, 28, \dots, 51, 52$ end up in positions $2, 4, \dots, 50, 52$, while those in positions $1, 2, \dots, 25, 26$ end up in positions $1, 3, \dots, 49, 51$. Thus

$$\begin{array}{cccc} out(1) = 1, & out(2) = 3, \dots, & out(25) = 49, & out(26) = 51 \\ out(27) = 2, & out(28) = 4, \dots, & out(51) = 50, & out(52) = 52 \end{array}$$

With a bit of thought you can see that the shuffle is described by the formula

$$out(k) = \begin{cases} 2k-1 & \text{if } k = 1, 2, \dots, 26 \\ 2k-52 & \text{if } k = 27, 28, \dots, 52. \end{cases}$$

There is an alternative way to write down a shuffle, based on calculating where the card in a given position goes if the pack is repeatedly shuffled in the same way. For example, it is easy from the preceding formulae to see that the destiny of the card originally in position 2 is given by

$$\begin{array}{cccc} out(2) = 3, & out(3) = 5, & out(5) = 9, & out(9) = 17 \\ out(17) = 33, & out(33) = 14, & out(14) = 27, & out(27) = 2 \end{array}$$

We write this information as a *cycle*

$$(\,2\ \ 3\ \ 5\ \ 9\ \ 17\ \ 33\ \ 14\ \ 27\,)\,,$$

which signifies that an outshuffle moves the card from any position in the list to the following position, where the last one "wraps round" to the beginning. Similarly, an outshuffle takes the card from position 18 to position 35, and that from position 35 back to 18, so these numbers form a cycle

$$(\,18\ \ 35\,)\ .$$

The card in position 1 is not moved by an outshuffle, so it is in a cycle by itself,

$$(\,1\,)\ .$$

Calculating what happens to every card in the pack enables us to write the shuffle as a *product of cycles*. ("Product" is not really the right word, but let's leave that until later.) The complete outshuffle is

$$\begin{aligned} out = {} & (\,1\,)(\,2\ \ 3\ \ 5\ \ 9\ \ 17\ \ 33\ \ 14\ \ 27\,)(\,4\ \ 7\ \ 13\ \ 25\ \ 49\ \ 46\ \ 40\ \ 28\,) \\ & (\,6\ \ 11\ \ 21\ \ 41\ \ 30\ \ 8\ \ 15\ \ 29\,)(\,10\ \ 19\ \ 37\ \ 22\ \ 43\ \ 34\ \ 16\ \ 31\,) \\ & (\,12\ \ 23\ \ 45\ \ 38\ \ 24\ \ 47\ \ 42\ \ 32\,)(\,18\ \ 35\,) \\ & (\,20\ \ 39\ \ 26\ \ 51\ \ 50\ \ 48\ \ 44\ \ 36\,)(\,52\,)\ . \end{aligned}$$

Exercise. Check this calculation; use similar methods to show that the inshuffle is defined by

$$in(k) = \begin{cases} 2k & \text{if } k = 1, 2, \ldots, 26 \\ 2k - 53 & \text{if } k = 27, 28, \ldots, 52 \end{cases}$$

and consists of a single cycle

$$\begin{aligned} in = (\, & 1\ \ 2\ \ 4\ \ 8\ \ 16\ \ 32\ \ 11\ \ 22\ \ 44\ \ 35\ \ 17\ \ 34\ \ 15\ \ 30\ \ 7\ \ 14\ \ 28\ \ 3\ \ 6 \\ & 12\ \ 24\ \ 48\ \ 43\ \ 33\ \ 13\ \ 26\ \ 52\ \ 51\ \ 49\ \ 45\ \ 37\ \ 21\ \ 42\ \ 31\ \ 9\ \ 18 \\ & 36\ \ 19\ \ 38\ \ 23\ \ 46\ \ 39\ \ 25\ \ 50\ \ 47\ \ 41\ \ 29\ \ 5\ \ 10\ \ 20\ \ 40\ \ 27\,)\ . \end{aligned}$$

Now let's consider what happens when we repeat the same shuffle over and over again. Remember that our aim is to prove, with a minimum amount of work, the statement I made earlier: eight successive perfect outshuffles will return the cards to their original arrangement. Once again it's important to get our ideas clear: just what is a repeated shuffle? Remember that a shuffle is a function; a repeated shuffle means applying a function to the result of another (or the same) function: that is, it is a function of a function, sometimes called a *composition* of functions. To remind you of this idea we do a simple example from school work: if

$$f(x) = x^2 \quad \text{and} \quad g(x) = x + 1$$

then

$$f(g(x)) = f(x+1) = (x+1)^2\ ,$$

Where we take x, apply the formula for g, then apply the formula for f to the result. Note that the order is important:

$$g(f(x)) = g(x^2) = x^2 + 1\ ,$$

which is not the same as $f(g(x))$. We shall use the symbol $\circ$ to denote function composition: thus, we have just calculated formulae for $f \circ g$ and $g \circ f$.

We can do exactly the same kind of things with shuffles: the shuffle $s_1 \circ s_2$ is obtaining by performing the shuffle s_2 first, then performing s_1 on the result. Once again order is important. For example, consider s, the simple shuffle from page 2, and in, the inshuffle. If we do s first and then in, the card in position 1 goes to position

$$in(s(1)) = in(52) = 51 \ ,$$

while if we do them in the opposite order it goes to

$$s(in(1)) = s(2) = 1 \ .$$

Therefore we have

$$in \circ s(1) = 51 \quad \text{and} \quad s \circ in(1) = 1 \ ,$$

and regardless of what happens to other cards, these two shuffles cannot be the same.

This should raise a question about the way we wrote a shuffle as a product of cycles. A cycle is itself a particular kind of function – that is, a particular kind of shuffle: for example, the cycle $c = (\ 31\ \ 41\ \ 5\ )$ is the function defined by

$$\begin{gathered} c(31) = 41 \ , \quad c(41) = 5 \ , \quad c(5) = 31 \ , \\ c(k) = k \quad \text{for all other values of } k. \end{gathered}$$

Therefore our previous expression gives the outshuffle as a *composition of cycles*. (As I mentioned earlier, the term "product", though quite commonly used, is not really the right word.) We calculated the expression for the outshuffle by first considering what happened to the card in position 1, then position 2 and so on. If we had considered the cards in a different order we would probably have written the cycles down in a different order: would this have mattered? In this case it would not, because a very important fact about shuffles is that *disjoint cycles commute*. That is, if c_1 and c_2 are cycles with no elements in common, then $c_1 \circ c_2$ is the same as $c_2 \circ c_1$. To understand why this is true, let's reduce our pack to five cards and consider the cycles

$$c_1 = (\ 1\ \ 3\ \ 5\ ) \quad \text{and} \quad c_2 = (\ 2\ \ 4\ ) \ .$$

If $k = 1, 3$ or 5 then the card in position k is unmoved by c_2, which only moves the card in position 2 to position 4 and vice versa. So

$$c_1(c_2(k)) = c_1(k) \ .$$

But in this case $c_1(k)$ is also $1, 3$ or 5 and is therefore unmoved by c_2, so

$$c_2(c_1(k)) = c_1(k) = c_1(c_2(k)) \ .$$

On the other hand, if $k = 2$ or 4 then k and $c_2(k)$ are both unmoved by c_1 and so

$$c_2(c_1(k)) = c_2(k) = c_1(c_2(k)) \ .$$

This shows that each of our five cards is moved by $c_1 \circ c_2$ in exactly the same way as it is moved by $c_2 \circ c_1$, and so these two shuffles are the same. That is,

$$(\,1\;\;3\;\;5\,)(\,2\;\;4\,) = (\,2\;\;4\,)(\,1\;\;3\;\;5\,)\;.$$

In this special case, the order in which we write the shuffles does not matter.
Exercise. Show that if $c_1 = (\,1\;\;3\;\;5\,)$ and $c_2 = (\,2\;\;3\;\;4\,)$, then the shuffles $c_1 \circ c_2$ and $c_2 \circ c_1$ are *not* the same.

Now we want to know: how many repetitions of a given shuffle does it take to get every card back to its original place? First, again, let's consider a simple shuffle of five cards,

$$c_1 = (\,1\;\;3\;\;5\,)\;.$$

Note that 2 and 4 are not specified here: this means that the cards in these positions are not moved by the shuffle. We could write the same shuffle as

$$(\,1\;\;3\;\;5\,)(\,2\,)(\,4\,)\;,$$

but it's more convenient to leave it as above. It should be easy to see that if we perform c_1 twice in succession we get the cycle

$$c_1^2 = c_1 \circ c_1 = (\,1\;\;5\;\;3\,)\;,$$

and three times gives

$$c_1^3 = c_1 \circ c_1 \circ c_1 = (\,1\,)(\,3\,)(\,5\,)\;,$$

which can also be written

$$c_1^3 = (\,1\,)(\,2\,)(\,3\,)(\,4\,)(\,5\,)\;.$$

That is, c_1^3 leaves every card unmoved. It is what mathematicians call the "identity shuffle", which in ordinary language is no shuffle at all! But it is mathematically convenient to regard a shuffle as being *any* arrangement of cards, including the one which just leaves every card where it was.

So, it takes three repetitions of c_1 to restore the pack to its original arrangement. It should be easy to see that for $c_2 = (\,2\;\;4\,)$ it takes two repetitions to do this, and a little thought will convince you that for

$$s = c_1 \circ c_2 = (\,1\;\;3\;\;5\,)(\,2\;\;4\,)$$

it takes a minimum of six repetitions, and for the seven–card shuffle

$$s = (\,1\;\;2\;\;3\;\;4\,)(\,5\;\;6\,)(\,7\,)$$

it takes a minimum of four.
Question. Before reading further, can you see the pattern?

Given a shuffle s, the minimum number of repetitions of s which are needed to restore the pack to its original sequence is called the *order* of s; if s is a composition of disjoint cycles having lengths $l_1, l_2, \ldots, l_m$, then

$$\mathrm{order}(s) = \mathrm{lcm}(l_1, l_2, \ldots, l_m)\;,$$

the least common multiple of the cycle lengths. In particular, finding the number of outshuffles needed to return a 52–card pack to its original arrangement is now ridiculously easy:

$$\mathrm{order}(\mathit{out}) = \mathrm{lcm}(1, 8, 8, 8, 8, 8, 2, 8, 1) = 8\ .$$

Exercise. How many inshuffles does it take to restore the original arrangement of the pack?

There are a few important questions that should be asked about shuffles and cycles.

- Can *every* shuffle be written as a composition of cycles?
- For a given shuffle, is there *only one way* to write it as a product of cycles?
- With regard to our definition of "order", is it really true that every shuffle, if repeated, will sooner or later restore all the cards to their original locations?

We have more or less taken all these questions for granted in the preceding discussion. In fact, the answer to all three questions is "yes" (with certain qualifications in the second case), and if we wished to investigate the subject thoroughly we should carefully prove this. Rather than do so, however, let's see how the cycle representation of a shuffle makes it quite easy to answer some other questions about the arrangement of cards in a pack.

What is the maximum order of any shuffle of a 52–card pack? In other words, we want to find shuffles which require as many repetitions as possible before the pack resumes its original arrangement. Suppose that the shuffle can be written as a product of cycles which have lengths $l_1, l_2, \ldots, l_m$. Since we are shuffling a 52–card pack we must have

$$l_1 + l_2 + \cdots + l_m = 52\ ,$$

and we wish to find the maximum possible value of $\mathrm{lcm}(l_1, l_2, \ldots, l_m)$, subject to this restriction. This is not an easy calculation. To get the largest possible lcm we would like the cycle lengths to include lots of large independent factors, but unfortunately this is not really possible: the cycle lengths must add up to 52, so if there are lots of them they can't be large, and if they are large there can't be lots of them! For example, letting one of the cycle lengths be a large prime number, say $l_1 = 47$, will be a good start for obtaining a large lcm; but it will leave us nowhere much to go, as the remaining cycle lengths can only add up to 5. We have to compromise by taking a "reasonable lot" of "fairly large" cycle lengths, and it turns out that the best we can do is

$$\mathrm{lcm}(13, 11, 9, 7, 5, 4, 1, 1, 1) = 180180\ .$$

An example of a shuffle with the indicated cycle lengths is

$$\begin{aligned} s = {} & (\,1\ \ 2\ \ \ldots\ \ 13\,)(\,14\ \ 15\ \ \ldots\ \ 24\,)(\,25\ \ 26\ \ \ldots\ \ 33\,) \\ & (\,34\ \ 35\ \ \ldots\ \ 40\,)(\,41\ \ 42\ \ \ldots\ \ 45\,)(\,46\ \ 47\ \ 48\ \ 49\,) \\ & (\,50\,)(\,51\,)(\,52\,)\ . \end{aligned}$$

Notice, by the way, that having a large order does not make s a good shuffle for randomising the pack! In this case the first 13 cards always remain in the first 13 positions, likewise for the next 11 and so on – this is not something that we would be likely to accept as a "random rearrangement".

In s, it might seem wasteful to have the last three elements in cycles of their own. However it turns out that we cannot increase the order by doing anything else with these elements.

Exercise. Check that if we replace the last three cycles in s by a single cycle $(\,50\;\;51\;\;52\,)$, the order of the amended shuffle is still 180180.

For our next question we ignore the values ace to king on the cards and concentrate on the suits alone, so that we have 13 identical spades, 13 identical hearts and so on. **Is it possible to arrange the pack so that it looks the same after a single outshuffle?** Remember we are assuming that there are only four "different–looking" cards, so that even though cards have moved after the shuffle, it may not be possible to tell the difference by looking at them.

To answer this question refer back to the expression for out as a product of cycles, and note that the card in position 2 before the shuffle is in position 3 after the shuffle. If the pack is to appear unchanged by the shuffle, the cards in positions 2 and 3 in the given deck must be of the same suit. For similar reasons the card in position 5 must be of the same suit too, and in fact so must all the cards $2, 3, 5, 9, 17, 33, 14, 27$ which occupy a single cycle. So we have to split our four suits of 13 cards into groups of sizes $1, 8, 8, 8, 8, 8, 2, 8, 1$, each consisting of one suit only. It is easy to see that this is impossible.

As we cannot arrange our pack so as to look the same after a single outshuffle, **can we arrange the pack so that it looks the same after two consecutive outshuffles?** We answer this question in the same way as the previous one, first finding the cycle representation of $out \circ out$. In fact, to find the square of a cycle is quite easy. Performing the cycle

$$c = (\,2\;\;3\;\;5\;\;9\;\;17\;\;33\;\;14\;\;27\,)$$

twice moves the card from position 2 to position 3 and then to position 5; the card from position 5 to position 9 and then to position 17; and so on. Therefore the shuffle

$$c^2 = (\,2\;\;3\;\;5\;\;9\;\;17\;\;33\;\;14\;\;27\,) \circ (\,2\;\;3\;\;5\;\;9\;\;17\;\;33\;\;14\;\;27\,)\,,$$

when repeated, moves the card from position 2 to position 5 to position 17 to position 14 and then back to position 2; and that from position 3 to position 9 to position 33 to position 27 and back to position 3. That is, c^2 is a product of two cycles,

$$c^2 = (\,2\;\;5\;\;17\;\;14\,) \circ (\,3\;\;9\;\;33\;\;27\,)\,.$$

Doing the same thing for the rest of the outshuffle gives

$$\begin{aligned} out^2 = (\,1\,) \circ (\,2\;\;5\;\;17\;\;14\,) \circ (\,3\;\;9\;\;33\;\;27\,) \circ (\,4\;\;13\;\;49\;\;40\,) \\ \circ (\,7\;\;25\;\;46\;\;28\,) \circ \cdots \circ (\,18\,) \circ (\,35\,) \circ \cdots \circ (\,52\,)\,. \end{aligned}$$

Thus the pack must be split into groups of sizes $1, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 1, 1, 4, 4, 1$, each group comprised of one suit only, and this is easy: just split each suit of 13 cards into three groups of 4 and a singleton.

Exercise. Give a general rule for the lengths of the cycles making up c^2, if c is a cycle of length l.
Hint. Try working it out for something like $c = (\,3\ \ 14\ \ 15\ \ 9\ \ 26\,)$ first – you will find that the answer is not quite the same as those we have already seen.

To conclude I would like to investigate a fact about shuffles which is not only of interest in itself but has an unexpected and vitally important application. We already know that the order in which we perform successive shuffles makes a difference to the outcome. For example, doing an outshuffle followed by an inshuffle is not the same as doing an inshuffle followed by an outshuffle. If we calculate the entire combined shuffles in terms of cycles, we have

$$\begin{aligned} in \circ out = {} & (\,1\ \ 2\ \ 6\ \ 22\ \ 33\ \ 28\ \ 8\ \ 30\ \ 16\ \ 9\ \ 34\ \ 32\ \ 24\ \ 41\ \ 7\ \ 26\ \ 49\ \ 39\ \ 52 \\ & \ 51\ \ 47\ \ 31\ \ 20\ \ 25\ \ 45\ \ 23\ \ 37\ \ 44\ \ 19\ \ 21\ \ 29\ \ 12\ \ 46\ \ 27\ \ 4\ \ 14\,) \\ & (\,3\ \ 10\ \ 38\ \ 48\ \ 35\ \ 36\ \ 40\,)(\,5\ \ 18\ \ 17\ \ 13\ \ 50\ \ 43\ \ 15\,)(\,11\ \ 42\,) \\ out \circ in = {} & (\,1\ \ 3\ \ 11\ \ 43\ \ 14\ \ 4\ \ 15\ \ 8\ \ 31\ \ 17\ \ 16\ \ 12\ \ 47\ \ 30\ \ 13\ \ 51\ \ 46\ \ 26\ \ 52 \\ & \ 50\ \ 42\ \ 10\ \ 39\ \ 49\ \ 38\ \ 45\ \ 22\ \ 36\ \ 37\ \ 41\ \ 6\ \ 23\ \ 40\ \ 2\ \ 7\ \ 27\,) \\ & (\,5\ \ 19\ \ 24\ \ 44\ \ 18\ \ 20\ \ 28\,)(\,9\ \ 35\ \ 33\ \ 25\ \ 48\ \ 34\ \ 29\,)(\,21\ \ 32\,)\,. \end{aligned}$$

Although these shuffles are not the same, they do have a significant feature in common. Can you see it before reading further?

Perhaps you noticed that both shuffles consist of cycles having the same lengths, namely, one cycle of length 36, two of length 7 and one of length 2. This is related to the important fact that **cycle type is invariant under conjugation**.

What does this mean? Well, the *cycle type* of a shuffle is simply a list of the number of cycles of various lengths, as in the examples we have just seen; *invariant* means that the cycle type of a conjugate of a shuffle is the same as that of the original shuffle. *Conjugate* will take a bit more explanation. First, it should be clear that if a pack of cards is rearranged by any shuffle, then this shuffle can be undone, restoring the original order of the cards. If the given shuffle is denoted by t, the shuffle which undoes t is called the *inverse* of t and is denoted t^{-1}. While inverting a complicated shuffle could be awkward physically – a bit like unscrambling an egg – it is very simple mathematically, especially if the shuffle is given as a composition of disjoint cycles. For example, the inverse of the outshuffle is

$$\begin{aligned} out^{-1} = {} & (\,1\,)(\,27\ \ 14\ \ 33\ \ 17\ \ 9\ \ 5\ \ 3\ \ 2\,)(\,28\ \ 40\ \ 46\ \ 49\ \ 25\ \ 13\ \ 7\ \ 4\,) \\ & (\,29\ \ 15\ \ 8\ \ 30\ \ 41\ \ 21\ \ 11\ \ 6\,)(\,31\ \ 16\ \ 34\ \ 43\ \ 22\ \ 37\ \ 19\ \ 10\,) \\ & (\,32\ \ 42\ \ 47\ \ 24\ \ 38\ \ 45\ \ 23\ \ 12\,)(\,35\ \ 18\,) \\ & (\,36\ \ 44\ \ 48\ \ 50\ \ 51\ \ 26\ \ 39\ \ 20\,)(\,52\,)\,. \end{aligned}$$

Exercise. Give a method of obtaining this from the cycle representation of out, and explain why it works.

We can now explain what is meant by a *conjugate* of a shuffle s: it is a shuffle which can be written as

$$t^{-1} \circ s \circ t\,,$$

where t is any shuffle at all[3]. That is, it is what happens when you perform any shuffle you like, then the given shuffle s, then the inverse of the first shuffle. For example, one of the conjugates of out is

$$\begin{aligned} & in^{-1} \circ out \circ in \\ & \quad = (\,1\ 28\ 29\ 31\ 35\ 43\ 7\ 40\,)(\,2\ 30\ 33\ 39\ 51\ 23\ 20\ 14\,) \\ & \qquad (\,3\ 32\ 37\ 47\ 15\ 4\ 34\ 41\,)(\,5\ 36\ 45\ 11\ 48\ 17\ 8\ 42\,) \\ & \qquad (\,6\ 38\ 49\ 19\ 12\ 50\ 21\ 16\,)(\,9\ 44\,) \\ & \qquad (\,10\ 46\ 13\ 52\ 25\ 24\ 22\ 18\,)(\,26\,)(\,27\,)\,. \end{aligned}$$

When we say that cycle type is invariant under conjugation, we mean that the cycle type of any conjugate of a shuffle is the same as that of the original shuffle. In the example we have just seen, $in^{-1} \circ out \circ in$ has six cycles of length 8, one of length 2 and two of length 1, just the same as the outshuffle itself. To prove that s and $t^{-1} \circ s \circ t$ always have the same cycle type, suppose that s contains a cycle

$$(\,a\ \ b\ \ c\ \ \cdots\ \ z\,)\,.$$

Remember that this means

$$s(a) = b\,, \quad s(b) = c\,, \quad \ldots, \quad s(z) = a\,.$$

Now consider the elements

$$t^{-1}(a)\,, \quad t^{-1}(b)\,, \quad t^{-1}(c)\,, \quad \ldots, \quad t^{-1}(z)\,.$$

If we apply $t^{-1} \circ s \circ t$ to each of these we get

$$\begin{aligned} t^{-1}(s(t(t^{-1}(a)))) &= t^{-1}(s(a)) = t^{-1}(b) \\ t^{-1}(s(t(t^{-1}(b)))) &= t^{-1}(s(b)) = t^{-1}(c) \\ &\ \ \vdots \qquad\qquad\quad \vdots \\ t^{-1}(s(t(t^{-1}(z)))) &= t^{-1}(s(z)) = t^{-1}(a)\,; \end{aligned}$$

in other words,

$$(\,t^{-1}(a)\ \ t^{-1}(b)\ \ t^{-1}(c)\ \ \ldots\ \ t^{-1}(z)\,)$$

is one of the cycles which make up $t^{-1} \circ s \circ t$. That is, if s has a cycle of any length whatsoever, $t^{-1} \circ s \circ t$ has a cycle of the same length, and this means that the cycle types are the same.

This proves that cycle type is invariant under conjugation, but so what? Well, conjugates can be used to help with Rubik's cube: see, for example, [2] or [3]. This is not really very surprising, since the problem of solving Rubik's cube is, in effect, the same as undoing a kind of shuffle. A much more dramatic application is described by T.W. Körner [4, page 351], who writes: "Few undergraduates would name [the result

[3] Some sources say $t \circ s \circ t^{-1}$. Explain why this doesn't make any difference.

just proved] as the dullest theorem of the year, but most would consider it a contender. For the mathematicians who struggled with Enigma, it represented the first hint that the plugboard might not be as strong as it seemed."

In this passage, Körner is discussing the British codebreaking effort during World War II. "Enigma" was the name given to the encryption machine used by the Nazi armed forces, and the "plugboard" was a component introduced into later versions of the machine, which made the codes vastly more difficult to break than those implemented by the original Enigma. Although consideration of cycle types and conjugates did not by itself enable the Allies to decipher enemy communications, it did, as Körner states, provide "the first hint" that this might be possible. In the event, the codebreakers at Bletchley Park managed to read many, though not all, of the coded messages they received, and the information they gained was a major factor in the war against the Nazis. It is not too much to suggest that if they had not succeeded, the history of the twentieth century may have turned out very differently.

To me this is one of the eternally fascinating aspects of mathematics. On the one hand we have card–shuffling: a pleasant pastime, of interest to many people, but not something that one could ever describe as vitally important in human history; on the other, a desperate struggle to avert the conquest of Europe, perhaps of other parts of the world too, by a totalitarian regime. And yet the mathematics is the same. People (students especially!) often complain about the abstract nature of mathematics: why waste time proving all these results about nothing in particular? But it is precisely the fact that mathematics is about "nothing in particular" that enables it to be applied in studying all sorts of different things. Abstraction in mathematics is not an "optional extra", but an essential factor in our ability to solve a wide variety of real–world problems through mathematics.

References

[1] How to do – The Riffle Shuffle, http://www.youtube.com/watch?v=N7D6PSJz5aI (Accessed 14 July 2011).

[2] Rubik's Cube: fundamental techniques – conjugates, http://www.ryanheise.com/cube/conjugates.html (Accessed 14 July 2011).

[3] Conjugates and Commutators, http://astro.berkeley.edu/~converse/rubiks.php?id1=basics&id2=concom (Accessed 14 July 2011).

[4] T.W. Körner, *The Pleasures of Counting*, Cambridge University Press, 1996. ★★★★★ strongly recommended!

Searching the web will reveal many more references to these topics. However mathematicians usually refer to "permutations" rather than "shuffles", so this is probably the better search term to use.