# The perfect riffle shuffles 7.1

**Tony Forbes**

Bridge involves four players and a deck of cards. The details of the game need not concern us except for some explanation we will need for later.

(i) The players, who always have names South, West, North and East, sit at the four sides of a square table in that order going clockwise.
(ii) There is a sequence of deals. Each deal proceeds as follows.
  (a) West shuffles the cards.
  (b) East cuts the cards.
  (c) South deals all 52 cards, one at a time, in order West, North, East, South, West, North, East, South, ..., South.
  (d) Competitive activity takes place involving bidding and card play.
  (e) The players change their names for the next deal: (West, North, East, South) → (South, West, North, East).
(iii) Wealth is redistributed according to some agreed scheme.

We are interested in bridge games where each player gets 13 cards of the same suit, a situation which we call a *perfect deal*.

To a mathematician the probability of a perfect deal is utterly and incredibly small. I'm sure there are websites that derive the exact value, or maybe one can work it out for oneself:

$$\frac{52 \cdot 39 \cdot 26 \cdot 13 \cdot (12!)^4}{52!} = \frac{1}{2235197406895366368301560000}. \qquad (1)$$

To a seasoned bridge player, however, the probability is considerably greater, perhaps merely very small or even just small. For a possible approach to calculating it, suppose the following:

$$\begin{aligned}
&\text{fraction of bridge deals where a new deck of cards is used} &&= \nu,\\
&\text{fraction of these where the shuffler does two riffle shuffles} &&= \rho,\\
&\text{fraction of these where both riffle shuffles are perfect} &&= \alpha.
\end{aligned}$$

All new card decks I have seen come neatly partitioned into the four suits, like so:

$$\mathbb{C} = (\diamondsuit A, \diamondsuit 2, \ldots, \diamondsuit K, \clubsuit A, \clubsuit 2, \ldots, \clubsuit K, \heartsuit A, \heartsuit 2, \ldots, \heartsuit K, \spadesuit A, \spadesuit 2, \ldots, \spadesuit K).$$

It turns out that two perfect riffle shuffles of $\mathbb{C}$ followed by a cut produces a perfect deal, and so one can argue that

$$\text{probability of a perfect deal at bridge} \; > \; \alpha\rho\nu.$$

The cut is irrelevant except that it will determine who gets the spades—and this *is* relevant for bridge players because the partnership with the spades will successfully contract for 7♠ and take all 13 tricks, a grand slam, for a score of at least $1360 = 7 \cdot 30 + 1000 + 150$.

I have no idea how to calculate the parameters $\nu$, $\rho$ and $\alpha$ except to assert that if the shuffler is a card sharp worthy of that qualification, then $\alpha$ can be nearly 1. This last observation has consequences. If we assume there exist four bridge enthusiasts that include an expert riffle-shuffler, we can reasonably assume $\alpha > 0.9$. Also $\rho \geq 0.25$ and, since a deck of cards will surely be good for no more than 2000 deals, $\nu \geq 0.0005$. So the group will enjoy a perfect deal with probability exceeding 0.0001, an enormous number compared with (1). And to prove that these things actually do occur in real life see `https://mathsjam.com/assets/talks/2011/RayHill-MathsJam2011PerfectBridgeDeal.pdf`.

Since we will usually be concerned with either numbers or suits but not both at once, we redefine the new deck of cards $\mathbb{C}$ in two different ways:

$$\begin{aligned}
\mathbb{N} &= (1, 2, \ldots, 52),\\
\mathbb{S} &= (\mathtt{d}, \mathtt{d}, \mathtt{d}, \mathtt{d}, \mathtt{d}, \mathtt{d}, \mathtt{d}, \mathtt{d}, \mathtt{d}, \mathtt{d}, \mathtt{d}, \mathtt{d}, \mathtt{d}, \mathtt{c}, \mathtt{c}, \mathtt{c}, \mathtt{c}, \mathtt{c}, \mathtt{c}, \mathtt{c}, \mathtt{c}, \mathtt{c}, \mathtt{c}, \mathtt{c}, \mathtt{c}, \mathtt{c},\\
&\quad\ \mathtt{h}, \mathtt{h}, \mathtt{h}, \mathtt{h}, \mathtt{h}, \mathtt{h}, \mathtt{h}, \mathtt{h}, \mathtt{h}, \mathtt{h}, \mathtt{h}, \mathtt{h}, \mathtt{h}, \mathtt{s}, \mathtt{s}, \mathtt{s}, \mathtt{s}, \mathtt{s}, \mathtt{s}, \mathtt{s}, \mathtt{s}, \mathtt{s}, \mathtt{s}, \mathtt{s}, \mathtt{s}, \mathtt{s}).
\end{aligned}$$

The number form $\mathbb{N}$ is appropriate for whenever we want to subject the cards to arithmetic.

There are two perfect riffle shuffles, which I shall call $R_0$ and $R_1$.

$R_0$: This is the most perfect of the perfect riffle shuffles. It moves all 52 cards and it has a nice definition when it acts on $\mathbb{N}$:

$$x \ \mapsto \ 2x \bmod 53,$$

meaning that the card at position $x$ in the deck goes to position $2x \bmod 53$. To determine which card occupies position $y$ in the shuffled deck, you have to look at the inverse,

$$y \ \mapsto \ \frac{y}{2} \bmod 53.$$

For example, $1 \mapsto 2$ and $(1/2 \bmod 53) = 27 \mapsto (54 \bmod 53) = 1$. The shuffle consists of a single cycle and therefore has order 52:

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

$R_1$: This shuffle is not quite as perfect as $R_0$ because it leaves cards 1 and 52 fixed. It is defined by

$$\begin{aligned} x &\mapsto (2(x-1) \bmod 51) + 1, \quad 1 \le x \le 51, \\ 52 &\mapsto 52, \end{aligned}$$

its inverse is

$$\begin{aligned} y &\mapsto \left(\frac{y-1}{2} \bmod 51\right) + 1, \quad 1 \le y \le 51, \\ 52 &\mapsto 52, \end{aligned}$$

it has order 8, and its cycle representation (omitting fixed points) is

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

More generally we can define $R_k$, $k \in \{0, 1, \ldots, 26\}$. Keep the top $k$ and the bottom $k$ cards fixed, renumber the $52-2k$ middle cards 1, 2, ..., $52-2k$, and perfect riffle shuffle them by $z \mapsto 2z \bmod 53-2k$. However, we shall see later that not much is lost by ignoring $R_2$, $R_3$, ..., $R_{26}$.

We can confirm by straightforward computation that two perfect riffle shuffles of either type ($R_0$ or $R_1$) applied to $\mathbb{C}$ and followed by a cut will create a perfect deal. Writing $k$ for $R_k$, we can express the four options succinctly by

$$[00], \quad [01], \quad [10], \quad [11], \tag{2}$$

which have orders 26, 252, 252, 4, respectively. Assume the dealer is South, the deck is arranged as in $\mathbb{C}$ and the number of cards cut off the top of the deck is a multiple of 4. Then we can determine who gets the spades:

$$[00] : \text{West}, \quad [01] : \text{North}, \quad [10] : \text{East}, \quad [11] : \text{South}.$$

If only a grand slam is important, then just one shuffle will deliver it. Although not a perfect deal, one partnership gets all the spades and hearts between them,

$$[0] : \text{East–West}, \quad [1] : \text{North–South},$$

and 7♠ is made. We can show in detail how $R_0$ and $R_1$ act on $\mathbb{S}$:

$$
\begin{aligned}
[\,] &: \texttt{ddddddddddddddcccccccccccccchhhhhhhhhhhhhhssssssssssssss},\\
\end{aligned}
$$

$$
\begin{aligned}
[\,] &: \texttt{dddddddddddddcccccccccccccchhhhhhhhhhhhhsssssssssssss},\\
[0] &: \texttt{hdhdhdhdhdhdhdhdhdhdhdhdhdscscscscscscscscscscscscsc},\\
[1] &: \texttt{dhdhdhdhdhdhdhdhdhdhdhdhdhcscscscscscscscscscscscscs},\\
[00] &: \texttt{shcdshcdshcdshcdshcdshcdshcdshcdshcdshcdshcdshcdshcd},\\
[01] &: \texttt{hsdchsdchsdchsdchsdchsdchsdchsdchsdchsdchsdchsdchsdc},\\
[10] &: \texttt{cdshcdshcdshcdshcdshcdshcdshcdshcdshcdshcdshcdshcdsh},\\
[11] &: \texttt{dchsdchsdchsdchsdchsdchsdchsdchsdchsdchsdchsdchsdchs},
\end{aligned}
$$

which confirm our assertions made earlier.

We are interested in finding combinations of $R_0$ and $R_1$ that produce perfect deals when acting on $\mathbb{C}$, and for this purpose we define two subgroups of $S_{52}$, the group of all 52! permutations of 52 objects (in our case cards).

Let

$$\mathcal{R} \;=\; \langle R_0, R_1 \rangle \;=\; \langle [0], [1] \rangle$$

be the group of permutations generated by $R_0$ and $R_1$. For members of $\mathcal{R}$ we use the binary notation suggested above. The identity is [], multiplication corresponds to concatenation and, to be consistent with the left-to-right nature of group multiplication, the object of a group action goes in parentheses on the *left*. Also we tacitly assume that variables appearing within the square brackets take values in {0,1}. Thus, for example, $(x)[abcd] = R_d(R_c(R_b(R_a(x))))$ and $[abcd][efg] = [abcdefg]$. Incidentally, cutting and dealing $(\mathbb{C})[abcd]$ always gives one player a yarborough.[1] Every member of $\mathcal{R}$ can be expressed in the notation just described since

$$
\begin{aligned}
&[0]^{-1} = [000000000000000000000000000000000000000000000000000],\\
&[1]^{-1} = [1111111],
\end{aligned}
$$

which we can write more sensibly with positive exponents: $[0]^{51}$, $[1]^{7}$. Using GAP, we find that $\mathcal{R}$ has order

$$270644318171066643800402165760000000 \;=\; 2^{26}\,26!,$$

not a large number, roughly three times the square root of 52!. The group's centre is $Z(\mathcal{R}) = \langle [0]^{26} \rangle$, which has order 2, and $[0]^{26}$ when acting on $\mathbb{C}$ just turns the deck upside down.

[1]Charles Anderson Worsley Anderson–Pelham, 2nd Earl of Yarborough, offered £1000–£1 against getting a whist hand with no card better than 9; Pr[yarborough] = $32!/19! \cdot 39!/52! \approx 1/1828$. See `https://en.wikipedia.org/wiki/Charles_Anderson-Pelham,_2nd_Earl_of_Yarborough`.

We find that the shuffles $R_2$, $R_3$, ..., $R_{26}$ add nothing new:

$$\langle R_0, R_1, R_2, \ldots, R_{26}\rangle \;=\; \mathcal{R}.$$

Observe that $R_{26}$ does nothing, and $R_{25}$ acting on $\mathbb{N}$ just does the transposition (26,27). This leads to a very good question. Which transpositions are in $\mathcal{R}$? The answer is sufficiently important to justify a theorem.

**Theorem 1** *Suppose $1 \le a < b \le 52$. If $a + b = 53$, then the group $\langle [0], [1], (a, b)\rangle$ is the same as $\langle [0], [1]\rangle$; otherwise $\langle [0], [1], (a, b)\rangle$ is isomorphic to $S_{52}$. Thus $(a, b) \in \mathcal{R}$ if and only if $a + b = 53$.*

**Proof** Use GAP to test each of the 1326 transpositions $(a, b)$. □

One can even find expressions for transpositions of the form $(a, 53 - a)$ just by looking for them:

$$(1,52) : [00110101010]^{23},\ (2,51) : [01010001101]^{23},\ (3,50) : [000000010]^{21},$$
$$(4,49) : [10100011010]^{23},\ (5,48) : [000100000]^{21},\ (6,47) : [000000100]^{21},$$
$$(7,46) : [01000110101]^{23},\ (8,45) : [000101111]^{25},\ (9,44) : [11100101110]^{23},$$
$$(10,43) : [001000000]^{21},\ (11,42) : [101111000]^{25},\ (12,41) : [000001000]^{21},$$
$$(13,40) : [100000000]^{21},\ (14,39) : [00101110111]^{23},\ (15,38) : [0000000111011]^{25},$$
$$(16,37) : [10111001011]^{23},\ (17,36) : [11001011101]^{23},\ (18,35) : [0011111010010]^{25},$$
$$(19,34) : [11011100101]^{23},\ (20,33) : [010000000]^{21},\ (21,32) : [010111100]^{25},$$
$$(22,31) : [01110010111]^{23},\ (23,30) : [0011010111001]^{23},\ (24,29) : [000010000]^{21},$$
$$(25,28) : [000000001]^{21},\ (26,27) : [00011010101]^{23}.$$

The first one says that 253 perfect riffle shuffles suffice to exchange the top and bottom cards whilst leaving the rest of the deck undisturbed. Using GAP we can also prove a theorem concerning pairs of transpositions.

**Theorem 2** *For distinct $a, b, c, d \in \{1, 2, \ldots, 52\}$, $(a, b)(c, d) \in \mathcal{R}$ if and only if $a + c = b + d = 53$ or $a + d = b + c = 53$.*

It turns out that there are 650 distinct elements $(a, b)(53 - a, 53 - b)$, and GAP tells us that we can generate $\mathcal{R}$ from $(1, 52)$ and 25 elements of the form $(1, b), (52, 53 - b)$:

$$\mathcal{R} = \langle (1,52), (1,2)(52,51), (1,3)(52,50), (1,4)(52,49), \ldots, (1,26)(52,27)\rangle.$$

**Theorem 3** *The group $\mathcal{R}$ is isomorphic to the wreath product $C_2$ wr $S_{26}$.*

**Proof** Clearly, $C_2$ wr $S_{26}$ has the correct order, $|C_2|^{26}|S_{26}| = 2^{26} \cdot 26!$. Let

$$\mathbb{T} \;=\; (t_1, t_2, \ldots, t_{26}),$$

where $t_i$ is the pair $\{i, 53-i\}$, $t = 1, 2, \ldots, 26$.

In the construction of $C_2$ wr $S_{26}$ we consider $S_{26}$ to be acting on $\mathbb{T}$, while the 26 copies of the cyclic group $C_2$ act on $t_1, t_2, \ldots, t_{26}$ by ordering them one way or the other. A typical element of $C_2$ wr $S_{26}$ is $X = \big((\alpha_1, \alpha_2, \ldots, \alpha_{26}),\ A\big)$ with $\alpha_1, \alpha_2, \ldots, \alpha_{26} \in C_2$ and $A \in S_{26}$. If $Y = \big((\beta_1, \beta_2, \ldots, \beta_{26}),\ B\big)$ is another element, then the product is defined by

$$XY = \big((\alpha_1\beta_{(1)A},\ \alpha_2\beta_{(2)A},\ \ldots,\ \alpha_{26}\beta_{(26)A}),\ AB\big),$$

where $(i)A$ is the $j$ that $A$ sends $i$ to when $A$ acts on $(1, 2, \ldots, 26)$.

To prove the theorem we show that all the components of the wreath product are representable as elements of $\mathcal{R}$.

By Theorem 1, for each $t \in \mathbb{T}$, there exists a sequence of shuffles $U_t = [s_1 s_2 \ldots]$ that flips the elements of $t$; that is, if $t = \{\alpha, 53-\alpha\}$ say, then $U_t$ does the transposition $(\alpha, 53-\alpha)$.

By a straightforward computation, we see that the action of $[0]$ on $\mathbb{T}$ is a single 26-cycle:

$$(t_1, t_2, t_4, t_8, t_{16}, t_{21}, t_{11}, t_{22}, t_9, t_{18}, t_{17}, t_{19}, t_{15},$$
$$t_{23}, t_7, t_{14}, t_{25}, t_3, t_6, t_{12}, t_{24}, t_5, t_{10}, t_{20}, t_{13}, t_{26}).$$

Indeed, recalling that $[0]$ acts on $\mathbb{N}$ by $x \to 2x \bmod 53$, we have

$$t_1 = \{1, 52\} \to \{2, 51\} = t_2 \to \{4, 49\} = t_4 \to \{8, 45\} = t_8 \to \ldots.$$

Furthermore, the sequence

$$V = [0011101111000110]^{21}$$

acting on $\mathbb{N}$ does $(1,2)(51,52)$, and therefore $V$ acting on $\mathbb{T}$ just does the transposition $(t_1, t_2)$. But then $[0]$ and $V$ acting on $\mathbb{T}$ generate the group isomorphic to $S_{26}$ of all 26! permutations of $\mathbb{T}$. $\square$

For a more concrete construction of the wreath product representation, first observe that both $[0]$ and $[1]$ acting on $\mathbb{N}$ have the property that $(i)[k] = j$ iff $(53-i)[k] = 53-j$. Therefore all $R \in \mathcal{R}$ have this property. Consequently, if $(a_1, a_2, \ldots, a_n)$ is a cycle of $(\mathbb{N})R$, $R \in \mathcal{R}$, then either $n$ is even and $a_{n/2+i} = 53 - a_i$, $i = 1, 2, \ldots, n/2$, or there is another cycle $(b_1, b_2, \ldots, b_n)$ with $b_i = 53 - a_i$, $i = 1, 2, \ldots, n$.

Corresponding to $R$ acting on $\mathbb{N}$, we can define a permutation $A$ of $(1, 2, \ldots, 26)$ and a 26-vector $C$ of elements in $\{1, -1\}$ by

$$\begin{array}{lll} (i)A = (i)R, & C_i = 1 & \text{if } (i)R \le 26, \\ (i)A = 53 - (i)R, & C_i = -1 & \text{otherwise.} \end{array}$$

The wreath product representation of $R$ is $(C, A)$. If $(D, B)$ similarly represents $S \in \mathcal{R}$, then the product $RS$ is represented by

$$(C, A)(D, B) \;=\; \big((C_1 D_{(1)A},\ C_2 D_{(2)A},\ \ldots,\ C_{26} D_{(26)A}\big),\ AB\big)\,.$$

One is naturally reminded of Rubik's cube and its 12 edge pieces, each of which can be in one of two orientations. Here the relevant group is $C_2$ wr $S_{12}$. For the details, see [David Singmaster, *Notes on Rubik's 'Magic Cube'*, 5th edition, 1980], pages 58–60.

Also inspired by Rubik's cube, we suggest an interesting challenge of similar fiendishness.

> Unseen by you, someone has shuffled a new deck of cards by a sequence of perfect riffle shuffles chosen at random from $\{R_0, R_1, \ldots, R_{26}\}$. Devise a strategy to restore the deck to its initial state using only $R_0, R_1, \ldots, R_{26}$.

Here is a possible method.

> For $k = 0, 1, \ldots, 25$:
> Repeatedly shuffle the deck using only shuffles $R_k$ and $R_{k+1}$ chosen at random until cards $1 + k$ and $52 - k$ are correct.

And here is an amazing fact. The algorithm just described works! Experiments suggest that the deck will probably get restored after a few thousand shuffles. Although random processes are involved, I have not yet found an instance where I had to abort the procedure because of impatience.

---

To begin our quest for further ways of getting a perfect deal, we define

$$\mathcal{P} \;=\; \{P \in \mathcal{R} :\ \text{for any } x, y \in \mathbb{S},\ x = y \text{ implies } (x)P = (y)P.\}$$

Members of $\mathcal{P}$ map suits to suits when acting on $\mathbb{S}$ or $\mathbb{C}$. We can refer these as *suit permuting sequences*, or maybe just 'elements of $\mathcal{P}$'. Clearly $\mathcal{P}$ is a subgroup of $\mathcal{R}$.

If $P \in \mathcal{P}$, then $P[st] \in \mathcal{R}$ and $P[st]$ acting on $\mathbb{S}$ gives a perfect deal. In case it's not obvious, to prove the converse suppose $R \in \mathcal{R}$ and $(\mathbb{S})R$ gives a perfect deal. When the deck is undealt and uncut it looks like this:

$$\mathbb{D} \;=\; (\alpha, \beta, \gamma, \delta, \alpha, \beta, \gamma, \delta, \ldots, \alpha, \beta, \gamma, \delta),$$

where $(\alpha, \beta, \gamma, \delta)$ is some permutation of $(\mathtt{c}, \mathtt{d}, \mathtt{h}, \mathtt{s})$. Applying the inverse of any of {[00], [01], [10], [11]} results in an arrangement like $\mathbb{S}$ but possibly with the letters permuted. Perhaps it is worth analysing in detail the simplest case, [00]. Acting on $\mathbb{N}$, we have $(y)[0]^{-1} = y/2 \bmod 53$ and therefore $(y)[00]^{-1} = y/4 \bmod 53$. Now we can determine how the residue classes modulo 4 get transformed:

$$\begin{aligned}
y \equiv 0 \pmod 4 &\;\Rightarrow\; (y)[00]^{-1} \in \{1, 2, \dots, 13\},\\
y \equiv 1 \pmod 4 &\;\Rightarrow\; (y)[00]^{-1} \in \{40, 41, \dots, 52\},\\
y \equiv 2 \pmod 4 &\;\Rightarrow\; (y)[00]^{-1} \in \{27, 28, \dots, 39\},\\
y \equiv 3 \pmod 4 &\;\Rightarrow\; (y)[00]^{-1} \in \{14, 15, \dots, 26\}.
\end{aligned}$$

The other three cases, $[01]^{-1}$, $[10]^{-1}$, $[11]^{-1}$, are trickier to deal with by hand, but they are easily proved with the help of a computer.

Since any $R \in \mathcal{R}$ that gives a perfect deal when acting on $\mathbb{S}$ must have the form $P[st]$ with $P \in \mathcal{P}$, we can concentrate on finding elements of $\mathcal{P}$. Before we reveal the true nature of $\mathcal{P}$, let us see how we can build it up from short sequences of perfect riffle shuffles.

None of the 254 sequences of 1 to 7 perfect riffle shuffles are elements of $\mathcal{P}$. Hence there are no perfect deals for fewer than 10 shuffles acting on $\mathbb{S}$ except those four given by (2).

When we get to 8 shuffles we find precisely 8 suit permuting sequences:

$$P_8 \;=\; \{[abc11111] : \quad a, b, c \in \{0, 1\}\} \;\subseteq\; \mathcal{P}.$$

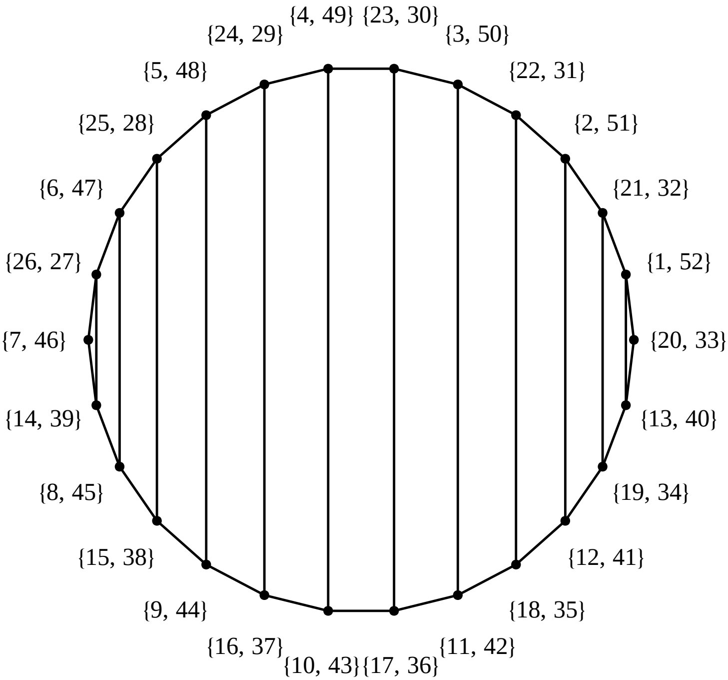
GAP confirms that they generate a group of order 52:

$$\mathcal{P}_8 \;=\; \langle P_8 \rangle \;=\; \langle [00011111], [00111111] \rangle \;\cong\; D_{52},$$

where we (GAP and I) use the notation $D_{2n}$ for the symmetry group of the regular $n$-gon, the *dihedral group* of order $2n$. It might be instructive to construct this group by hand. The results of the shuffle sequences acting on $\mathbb{N}$ are

$$\begin{aligned}
[00011111] : \;& (20, 1, 21, 2, 22, 3, 23, 4, 24, 5, 25, 6, 26,\\
& \qquad 7, 14, 8, 15, 9, 16, 10, 17, 11, 18, 12, 19, 13)\\
& (33, 52, 32, 51, 31, 50, 30, 49, 29, 48, 28, 47, 27,\\
& \qquad 46, 39, 45, 38, 44, 37, 43, 36, 42, 35, 41, 34, 40),\\
[00111111] : \;& (27, 14)(28, 15)(29, 16)(30, 17)(31, 18)(32, 19)(33, 20)(34, 21)\\
& (35, 22)(36, 23)(37, 24)(38, 25)(39, 26)(40, 1)(41, 2)(42, 3)(43, 4)\\
& (44, 5)(45, 6)(46, 7)(47, 8)(48, 9)(49, 10)(50, 11)(51, 12)(52, 13).
\end{aligned}$$

Consider a regular 26-gon $\mathbb{G}$ whose vertices are unordered pairs of corresponding elements of [00011111]'s cycles: {20,33}, {1,52}, {21,32}, ..., {13,40}. Then [00011111] acts on $\mathbb{G}$ by rotating it through $2\pi/26$ and [00111111] reflects the polygon in the line joining {20,33} and {7,46}.




For 9 to 25, the only elements of $\mathcal{P}$ are 152 shuffle sequences of length 16 and 3624 of length 24. All are in $\mathcal{P}_8$. The next elements of $\mathcal{P}$ are the eight 26-shuffle sequences

$$P_{26} \;=\; \{[abc00000000000000000000000] : a, b, c \in \{0, 1\}\}.$$

We now have a slightly bigger group: $\mathcal{P}_{26} = \langle P_{26} \rangle$ has order 104, it includes $\mathcal{P}_8$, it is isomorphic to $C_2 \times D_{52} \cong C_2^2 \times D_{26}$, and it has a 3-generator representation:

$$\mathcal{P}_{26} \;=\; \langle [00011111],\; [00111111],\; [0]^{26} \rangle.$$

Finally (because I am running low on computer power), there are 96704 32-shuffle elements of $\mathcal{P}$ of which only the 52 given in Table 1 are not in

$\mathcal{P}_{26}$. They generate the much larger group

$$\mathcal{P}_{32} = \langle[00011111],\ [0]^{26},\ [00000001011110011110011110011100]\rangle,$$

which includes $\mathcal{P}_{26}$ and has order $15510315217453056000 = 4 \cdot (13!)^2$.

Now let

$$Q = (1,52)(2,51)\dots(13,40).$$

When $Q$ acts on $\mathbb{C}$ it just exchanges the diamonds and spades. Moreover, by Theorem 1, $Q \in \mathcal{R}$. Hence $Q \in \mathcal{P}$, and one can check with GAP that $Q \notin \mathcal{P}_{32}$. Thus we have a subgroup of $\mathcal{P}$ that is bigger than $\mathcal{P}_{32}$:

$$\mathcal{Q} = \langle[00011111],\ [00000001011110011110011110011100],\ Q\rangle.$$

GAP confirms that

$$|\mathcal{Q}| = 31020630434906112000 = 8 \cdot (13!)^2 = 2|\mathcal{P}_{32}|$$

and that $\mathcal{Q}$ is isomorphic to $(C_2 \times C_2) \rtimes ((A_{13} \times A_{13}) \rtimes D_8)$.

**Theorem 4** *We have $\mathcal{P} = \mathcal{Q}$.*

**Proof** A consequence of its definition is that $\mathcal{P}$ is the stabilizer in $\mathcal{R}$ of the structure formed by partitioning the card deck into the suits as a set of four sets of thirteen elements each. Unfortunately I do not know how to calculate it. Fortunately GAP does.

Before we prove the theorem we offer an argument which suggests that a possible element of $\mathcal{P} \setminus \mathcal{Q}$ must be rather weird. By Theorem 3, any permutation of $\mathbb{T} = (\{1,52\},\{2,51\},\dots,\{26,27\})$ together with any combination of transpositions of the elements of $\mathbb{T}$ is achievable with an element of $\mathcal{R}$. Split $\mathbb{T}$ into two ordered sets,

$$\begin{aligned}\mathbb{T}_1 &= (\{1,52\},\{2,51\},\dots,\{13,40\}),\\ \mathbb{T}_2 &= (\{14,39\},\{15,38\},\dots,\{26,27\}).\end{aligned}$$

Suppose $A, B, C, X \in \mathcal{R}$ such that $A$ permutes $\mathbb{T}_1$, $B$ permutes $\mathbb{T}_2$, $C$ either does nothing or exchanges $\mathbb{T}_1 \leftrightarrow \mathbb{T}_2$, and $X$ orders elements of $\mathbb{T}$ one way or the other. By choosing $X$ to line up the suits represented by $(\mathbb{T})ABC$, we can arrange for $ABCX$ to be an element of $\mathcal{P}$. The numbers of choices are 13! for $A$ and $B$, 2 for $C$ and 4 for $X$, altogether $8 \cdot (13!)^2 = |\mathcal{Q}|$.

To confirm that $|\mathcal{P}| = |\mathcal{Q}|$, I must resort to GAP. The sequence of commands

```
# The perfect riffle shuffles [0] and [1] as cycles.
r0 := (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);
r1 := (18,35)(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)(20,39,26,51,50,48,44,36);
# The group R = <[0], [1]>.
gR := Group( r0, r1 );
# The set structure that is to be preserved.
deckS := [ [ 1,2,3,4,5,6,7,8,9,10,11,12,13 ],
           [ 14,15,16,17,18,19,20,21,22,23,24,25,26 ],
           [ 27,28,29,30,31,32,33,34,35,36,37,38,39 ],
           [ 40,41,42,43,44,45,46,47,48,49,50,51,52 ] ];
# Compute the stabilizer in gR of deckS.
gStabS := Stabilizer( gR, deckS, OnSetsDisjointSets );
```

yields a group of order $8 \cdot (13!)^2$, the order of $\mathcal{Q}$. □

Another way to create elements of $\mathcal{P}$ is by repetition,

$$[0101000]^{38},$$
$$[00000011]^{40}, [00001011]^{22}, [00100111]^{16}, [01001000]^{23}, [01010011]^{220},$$
$$[01011000]^{22}, [01011001]^{40}, [01011100]^{12}, [01011110]^{13}, [01100111]^{8},$$
$$[01101111]^{7},$$
$$[010001011]^{130}, [010010101]^{112}, [010111011]^{210}, [101001010]^{112},$$
$$[101011101]^{210}, [111011100]^{210},$$
$$[0010000110]^{34}, [0011100011]^{76}, [0110011010]^{76}, [0111010111]^{42},$$
$$[1001110001]^{114}, [1011101001]^{22},$$
$$[00000100111]^{38}, [00001110100]^{260}, [00100011100]^{44}, [01010000101]^{52},$$
$$[01111011010]^{104}, [10000001110]^{390}, [10000011001]^{130}, [10010100101]^{34},$$
$$[10011011101]^{16}, [10101000010]^{52}, [11000001100]^{130}, [11000010001]^{44},$$
$$[11111000101]^{20}, [11111010111]^{20},$$
$$[000010000011]^{95}, [000110000000]^{176}, [000110000100]^{95}, [001100001000]^{95},$$
$$[001100100011]^{30}, [001101000000]^{20}, [001110011000]^{42}, [010000011000]^{95},$$
$$[011000111000]^{23}, [011001100011]^{14}, [011100101000]^{280}, [011110000001]^{23},$$
$$[011110001001]^{110}, [100000010001]^{76}, [100000110000]^{95}, [100011000011]^{170},$$
$$[100100001010]^{76}, [101001101100]^{170}, [101011010111]^{23}, [101011100110]^{152},$$
$$[101111000000]^{23}, [110010000110]^{44}, [110011000001]^{42}, [111000011000]^{23},$$

$$[111001010000]^{280},$$

and here are a few sequences that generate perfect deals:

$$[011111]^{251}, [0111111]^{24}, [0111111]^{50}, [001111110]^{28}, [001111111]^{10},$$
$$[011111110]^{10}, [101111110]^{10}, [0011111100]^{5}, [0111111100]^{253},$$
$$[1011111101]^{14}, [10111111010]^{44}, [101111110100]^{7}.$$

Table 1: Suit permuting sequences of length 32

| | |
|---|---|
| [00000001011110011110011110011100] | [00000011110110111100101111010011] |
| [00010011111010111101001111101011] | [00011001111100011111000111110001] |
| [00011100100000010111100111100111] | [00011110000111100001111000011110] |
| [00011110100111100001111000011110] | [00100001011110011110011110011100] |
| [00100011110110111100101111010011] | [00110011111010111101001111101011] |
| [00111001111100011111000111110001] | [00111100100000010111100111100111] |
| [00111110000111100001111000011110] | [00111110100111100001111000011110] |
| [01000001011110011110011110011100] | [01000011110110111100101111010011] |
| [01010011111010111101001111101011] | [01011001111100011111000111110001] |
| [01011100100000010111100111100111] | [01011110000111100001111000011110] |
| [01011110100111100001111000011110] | [01100001011110011110011110011100] |
| [01100011110110111100101111010011] | [01110011111010111101001111101011] |
| [01111001111100011111000111110001] | [01111100100000010111100111100111] |
| [01111110000111100001111000011110] | [01111110100111100001111000011110] |
| [10000001011110011110011110011100] | [10000011110110111100101111010011] |
| [10010011111010111101001111101011] | [10011001111100011111000111110001] |
| [10011100100000010111100111100111] | [10011110000111100001111000011110] |
| [10011110100111100001111000011110] | [10100001011110011110011110011100] |
| [10100011110110111100101111010011] | [10110011111010111101001111101011] |
| [10111001111100011111000111110001] | [10111100100000010111100111100111] |
| [11000001011110011110011110011100] | [11000011110110111100101111010011] |
| [11010011111010111101001111101011] | [11011001111100011111000111110001] |
| [11011100100000010111100111100111] | [11011110000111100001111000011110] |
| [11011110100111100001111000011110] | [11100001011110011110011110011100] |
| [11100011110110111100101111010011] | [11110011111010111101001111101011] |
| [11111001111100011111000111110001] | [11111100100000010111100111100111] |