並べ替え操作の計算法

宗政 昭弘
九州大学

1999年8月6日

1　８回で元に戻る out shuffle

トランプのカードを切るときに起こるのがカードの並べ替えである。本講座では、並べ替えを数学的に記述する置換の概念とその計算法について解説する。

５２枚のカードを伏せて一山に積み、下の２６枚を左手に、上の２６枚を右手に持ち、左、右、左、右と交互に一枚ずつ落としていって混ぜ合わせ、一山にする。この操作を８回繰り返すと、カードの順番は初めと全く同じになる。このようなことを実際にカードを操作することなく、紙上、またはコンピュータ上の計算で確かめるために必要となるのが置換の概念とその計算法である。

まず、カードを上述のように並べ替えるという操作を番号を使って表そう。５２枚のカードに通し番号１～５２をつけて、その番号の順に上から積まれているとする。このとき上述のような並べ替えをすると、カードの番号は下の表の下段のようになる。

1	2	3	4	5	6	7	8	9	···	52
1	27	2	28	3	29	4	30	5	···	52

実際にこの操作を正確に実行するには熟練を要するので、例えば１０枚のカード（A, 2, 3, 4, 5, 6, 7, 8, 9, 10）でやってみて

A　6　2　7　3　8　4　9　5　10

となることを確かめてみれば納得が行くだろう。さて、この操作はアウトシャフル（out shuffle）と呼ばれる。これは山の一番上と一番下（外側）のカードがシャフルしたあとも外側に残るので、“out” と呼ぶのだが、逆にインシャフルと（in shuffle）というのもある。それは、５２枚のカードを伏せて一山に積み、下の２６枚を左手に、上の２６枚を右手に持ち、右、左、右、左と交互に一枚ずつ落としていって混ぜ合わる操作のことである。例えば１０枚のカード（A, 2, 3, 4, 5, 6, 7, 8, 9, 10）で in shuffle を実行してみると

6　A　7　2　8　3　9　4　10　5

これだと山の一番上（A）と一番下（10）のカードが外側に残らずに、中に入ってしまう。

さて、今 k 番目のカードが out shuffle によって $O(k)$ 番目に移ったとすると、$O(k)$ $(1 \leqq k \leqq 52)$ の表は以下のとおりである。

k	1	2	3	4	5	$\cdots$	26	27	28	$\cdots$	52
$O(k)$	1	3	5	7	9	$\cdots$	51	2	4	$\cdots$	52

さらに、８回繰り返すと元に戻る、という事実をわかりやすく説明するために、便宜上カードの位置は一番上を０番目ということにして、０から５１までの数字で表すことにする。すると上の表は次のようになる。

k	0	1	2	3	4	$\cdots$	25	26	27	$\cdots$	51
$O(k)$	0	2	4	6	8	$\cdots$	50	1	3	$\cdots$	51

このように書くと、out shuffle で動かない一番下のカードを除けば、実は $O(k)$ が $2k$ を 51 で割った余りに等しいことが容易に見て取れる。一般に、m を正の整数とし、a, b を整数とするとき、$a - b$ が m で割り切れるとき $a \equiv b \pmod{m}$ と書き、 a と b は m を法として合同であるという。もし a を m で割った余りが b ならば、明らかに $a \equiv b \pmod{m}$ が成り立つので、$O(k) \equiv 2k \pmod{51}$ である。

次に、out shuffle を連続して行った場合を考えよう。Out shuffle 一回で k 番目のカードが $O(k)$ 番目に移るのだから、out shuffle 二回では k 番目のカードが $O(O(k))$ 番目に移る。$O(O(k))$ を $O^2(k)$ と書く。同様に $O^n(k)$ というのが定義され、冒頭にある主張は、 $O^8(k) = k$ がすべての k $(0 \leqq k < 51)$ について成り立つということである。合同式の性質

$$a \equiv b \pmod{m} \Longrightarrow ac \equiv bc \pmod{m}$$

を用いると $2O(k) \equiv 2^2 k \pmod{51}$ となる。一方 $O^2(k) \equiv 2O(k) \pmod{51}$ であるから、合同式の次の性質

$$a \equiv b \pmod{m}, \quad b \equiv c \pmod{m} \Longrightarrow a \equiv c \pmod{m}$$

を用いると $O^2(k) \equiv 2^2 k \pmod{51}$ となる。この議論を繰り返すと $O^3(k) \equiv 2^3 k \pmod{51}$, $O^4(k) \equiv 2^4 k \pmod{51}$, ... となり、 $O^8(k) \equiv 2^8 k \pmod{51}$ を得る。すると、 $2^8 = 256 = 51 \times 5 + 1$ だから、$2^8 k = 51 \times (5k) + k$ となり、これは $2^8 k - k$ が 51 で割り切れることを意味している。よって $2^8 k \equiv k \pmod{51}$ であり、したがって $O^8(k) \equiv k \pmod{51}$ を得る。この合同式の両辺はともに 0 から 50 までの数だから、それらの差が 51 で割り切れるためには一致するしかない。つまり $O^8(k) = k$ である。以上により、 out shuffle を８回繰り返すとカードの位置は元に戻ることが証明された。

８回繰り返すと元に戻るのだから、１６回、２４回などでも当然元に戻る。しかし８回より少ない回数しかしないと元には戻っていない。このことは次のようにしてわ

かる。１番の位置（すなわち、上から２番目）のカードの動きに注目すると、

$$1 \to 2 \to 4 \to 8 \to 16 \to 32 \to 13 \to 26 \to 1$$

というふうに動くから、８回目で初めて元の位置に戻る。

2　置換とその位数

前節で述べた out shuffle, in shuffle はもっと一般的な概念である「置換」の例である。N を有限集合とし、N から N への上への一対一対応 $f : N \to N, k \mapsto f(k)$ のことを N 上の置換という。上への一対一対応というのは f の像 $f(k)$ $(k \in N)$ が N の各元をちょうど一回ずつ表していると言っても良い。f, g を N 上の置換とするとき、それらの積 fg は対応 $k \mapsto f(g(k))$ のことであり、それがまた置換になることは容易に確かめられる。積 ff を f^2, fff を f^3 のように略記する。N 上の置換の例として恒等置換 $k \mapsto k$ がある。これを 1_N で表す。f を N 上の置換とするとき f の位数とは、 $f^n = 1_N$ となるような最小の正整数 n のことである。すると、前節で最後に述べたことは $N = \{0, 1, \ldots, 51\}$ 上の置換 O (out shuffle) の位数が８である、ということである。

次に置換の書き方について説明する。ひとつの書き方は前節の表

k	0	1	2	3	4	$\cdots$	25	26	27	$\cdots$	51
$O(k)$	0	2	4	6	8	$\cdots$	50	1	3	$\cdots$	51

であるが、この表の上段はどんな置換に対しても同じなので、置換 O の性質は下段だけでわかるはずであるが、もし上段を省略すると、例えば $O(40)$ が何なのか知るためには初めから 41 番目まで数える必要があり、不便である。そこで cycle notation と呼ばれる次の記法を導入する。

$$(0)(1, 2, 4, 8, 16, 32, 13, 26)(3, 6, 12, 24, 48, 45, 39, 27)$$
$$(5, 10, 20, 40, 29, 7, 14, 28)(9, 18, 36, 21, 42, 33, 15, 30)$$
$$(11, 22, 44, 37, 23, 46, 41, 31)(17, 34)(19, 38, 25, 50, 49, 47, 43, 35)$$

これは、$(k, O(k), O^2(k), \ldots)$ という形のもの（cycle という）で０から５１までの数字が一回ずつ登場している。つまり、k の右側が) でない限り $O(k)$ は k の右側にあり、 k の右側が) のときはそのかっこの最初に現れる数字が $O(k)$ である。たとえば、$O(17) = 34$, $O(34) = 17$ である。つまり、１７番目のカードと３４番目のカードは何度 out shuffle を繰り返しても他のカードと混ざり合うことはなく、それら２枚の位置が入れ替るだけであることがわかった。Cycle notation を使って置換を表すと、その置換の位数がすぐにわかるという利点がある。実際、out shuffle の cycle の長さは 1,2,8 のいずれかである。少し計算してみると容易に想像がつくことだが、一般に置換の位数はその置換の cycle の長さの最小公倍数に等しいことがわかる。

５２枚のカードの in shuffle I は

k	0	1	2	3	4	5	$\cdots$	25	26	27	$\cdots$	51
$I(k)$	1	3	5	7	9	11	$\cdots$	51	0	2	$\cdots$	50

となる。これを cycle notation で書くことは練習問題としておく。In shuffle の位数を求めるには、カードの枚数が $2n$ 枚という一般の場合を扱った方が便利である。そこで $N = \{0, 1, 2, \ldots, 2n-1\}$ 上の out shuffle O と in shuffle I を次のように定義する。

k	0	1	2	3	4	5	$\cdots$	$n-1$	n	$n+1$	$\cdots$	$2n-1$
$O(k)$	0	2	4	6	8	10	$\cdots$	$2n-2$	1	3	$\cdots$	$2n-1$

k	0	1	2	3	4	5	$\cdots$	$n-1$	n	$n+1$	$\cdots$	$2n-1$
$I(k)$	1	3	5	7	9	11	$\cdots$	$2n-1$	0	2	$\cdots$	$2n-2$

Out shuffle と in shuffle は微妙に違うが、今 $2n+2$ 枚のカードの out shuffle を書くと次のようになる。

k	0	1	2	3	4	5	$\cdots$	n	$n+1$	$n+2$	$\cdots$	$2n+1$
$O(k)$	0	2	4	6	8	10	$\cdots$	$2n$	1	3	$\cdots$	$2n+1$

Out shuffle では一番上と一番下のカードは動かないので、上の表で 0 と $2n+1$ を無視して、その間に表れている数字からすべて 1 を引くと、$2n$ 枚のカードの in shuffle の表とちょうど一致する。このことは次のように述べることもできる。５２枚のカード一山を上下からジョーカー１枚ずつではさみ、それら５４枚のカードに out shuffle を行う。上下のジョーカーの位置は変わらないので、それらを取り除くと、５２枚のカードの位置はそれらに in shuffle を行った場合と全く同じになる。

さて、５２枚のカードの out shuffle の置換としての位数は８であることはすでに述べたが、一般にカードの数が $2n$ 枚の場合は位数はいくつになるだろうか。５２枚の場合と同様の議論により、$O(k)$ は $2k$ を $2n-1$ で割った余りに等しいことがわかる。したがって、$O(k) \equiv 2k \pmod{2n-1}$ である。しかし $2^8 \equiv 1 \pmod{2n-1}$ は一般には言えない。8 に代わる値が一般に何になるのかを与える公式はない。そこで仕方がないので、m を正の整数とするとき、$2^n \equiv 1 \pmod{m}$ を満たす最小の正の整数 n のことを 2 の m を法とする位数と呼ぶことにする。位数という言葉は置換に対してすでに定義したが、ここでは2 という数値の m を法とする位数という意味であり、使い方が異なる。しかし現代数学では同じような性質のものには同じ言葉を使うことが多い（実際そうしないと、数学の概念の方が適切な言葉の数より多いので言葉が足りなくなってしまう）。これまでの考察をまとめると次のようになる。

定理 1. $2n$ 枚のカードの out shuffle の位数は 2 の $2n-1$ を法とする位数に等しい。$2n$ 枚のカードの in shuffle の位数は 2 の $2n+1$ を法とする位数に等しい。

一般に、p を素数とし、a を p で割り切れない整数とすると、a の p を法とする位数は $p-1$ の約数であることが知られている。このことの証明は比較的簡単で、Fermat の定理 $a^{p-1} \equiv 1 \pmod{p}$ に帰着される。たとえば、2 の $p = 53$ を法とする

位数は 52 の約数であるが、実は 52 であることが直接計算によって確かめられる。つまり、５２枚のカードの in shuffle の位数は 52 であることが上の定理よりわかる。前述の練習問題を実行した人はわかるはずだが、５２枚のカードの in shuffle を cycle notation で書くと長さ 52 の cycle ひとつから成ることがわかる。このことから次が言える。

定理 2. ５２枚のカードの in shuffle を何回か繰り返すことによって、一番上のカードを任意の位置に移すことができる。

これはたまたま 53 が素数で、かつ 2 の 53 を法とする位数が 52 だったから言えたことである。一般に p が素数でも 2 の p を法とする位数が $p-1$ になるとは限らない（例 $p=7$, 位数は 3)。2 の p を法とする位数が $p-1$ となるような素数 p が無限に存在するかどうかは Artin の予想と呼ばれている整数論の有名な未解決問題である。そうすると、一般に $2n$ 枚のカードを扱う時、一番上のカードを任意の位置に移すためには in shuffle だけではだめで、 out shuffle と組み合わせないといけない。しかしどのように組み合わせたら一番上のカードを思った通りの位置に移動させることができるであろうか。実は n の値によらない、エレガントな答えが Alex Elmsley によって得られている。その答えを予想するために、一番上（位置 0）のカードを位置 $1,2,3,4$ に移す out shuffle, in shuffle の組合せを探してみよう。まず 0 を 1 に移すのは in shuffle 一回で良い。次に 0 を 2 に移すには、in shuffle 一回でまず 0 を 1 に移し、その後 out shuffle で 1 を 2 に移せば良い、すなわち、積 OI（右から先に）により 0 が 2 に移る。 0 を 3 に移すには in shuffle を２回、すなわち I^2 でよい。 0 を 4 に移すには in shuffle 一回でまず 0 を 1 に移しておいて、その後 out shuffle ２回で 1 を 4 に移せば良い。これらを表にすると

f	I	OI	II	OOI
$f(0)$	1	2	3	4

この表を見ると、上段は下段の数値 $1,2,3,4$ の２進展開を左右逆転したもの（$O \leftrightarrow 0$, $I \leftrightarrow 1$）であることがわかる。実際、次が成り立つ。

定理 3 (A. Elmsley)**.** k を $2n-1$ 以下の正整数とし、 k の２進展開を $1a_1a_2\cdots a_t$ とする。 $N=\{0,1,\ldots,2n-1\}$ 上の置換 $f_1,f_2,\ldots,f_t$ を

$$f_i=\begin{cases} I & (a_i=1 \text{ のとき}) \\ O & (a_i=0 \text{ のとき}) \end{cases}$$

により定義し、 $F=f_tf_{t-1}\cdots f_1I$ とおくと $F(0)=k$ となる。

証明. k に関する帰納法を使う。$k=1$ のとき $F=I$ となり $I(0)=1$ より正しい。

次に $k>1$ とし、 k より小さい正整数については定理の主張が正しいと仮定する。$k>1$ より $t \geqq 1$ である。l を、２進展開が $1a_1a_2\cdots a_{t-1}$ となる正整数とすると

$$k=\begin{cases} 2l+1 & (a_t=1 \text{ のとき}) \\ 2l & (a_t=0 \text{ のとき}) \end{cases}$$

である。 $l < k$ より、l に帰納法の仮定が適用できて、$G = f_{t-1} \cdots f_1 I$ とおけば $G(0) = l$ となる。よって

$$\begin{aligned} F(0) &= f_t f_{t-1} \cdots f_1 I(0) \\ &= f_t(G(0)) \\ &= f_t(l) \\ &= \begin{cases} I(l) & (a_t = 1 \text{ のとき}) \\ O(l) & (a_t = 0 \text{ のとき}) \end{cases} \end{aligned}$$

となる。 $k \leqq 2n-1$ なので $l \leqq n-1$ となり、$I(l) = 2l+1$, $O(l) = 2l$ が成り立つから $F(0) = k$ である。 □

3 Shuffle 群 $\langle O, I \rangle$

n を正整数とし、 $N = \{0, 1, 2, \ldots, 2n-1\}$ 上の out shuffle O と in shuffle I を何度か繰り返して得られる N 上の置換全体を $\langle O, I \rangle$ と表し、これを shuffle 群と呼ぶ。「群」とは現代数学の用語で、その公理を知っている人はなぜこれが群になるのか確かめたくなるかも知れないが、ここでは次のことだけ注意しておく。

まず、 $f, g \in \langle O, I \rangle$ ならば $fg \in \langle O, I \rangle$ が成り立つ。すなわち、 f, g それぞれが O, I の何回かの繰り返しで得られる置換ならば、その積 fg はまず g をやってから次に f を行うわけだから、それも O, I の何回かの繰り返して得られる置換であることは自明である。

次に、$f \in \langle O, I \rangle$ ならば、その逆置換 f^{-1} も $\langle O, I \rangle$ の元である。ここで逆置換 f^{-1} とは、$ff^{-1} = 1_N$, $f^{-1}f = 1_N$ となる置換である。例えば O の逆置換は次のように言い表せる。

> 「一山のカードを一番上から右、左、右、左、と交互に１枚ずつ二山に分けた後、右の山を左の山の上に乗せる」

どんな置換も cycle notation で書くとその位数がわかることはすでに述べた。特に、どんな置換 f に対しても $f^t = 1_N$ となる正の整数 t が存在する。すると f^{t-1} が f の逆置換である。つまり、操作 f を $t-1$ 回繰り返したものが f の逆置換である。ということは、 f が O, I を何回か繰り返したものであれば、 f^{t-1} もそうであり、したがって $f^{-1} \in \langle O, I \rangle$ が示せたことになる。

Shuffle 群 $\langle O, I \rangle$ は例えば、

$$1_N, O, I, O^2, OI, IO, I^2, O^3, O^2I, OIO, OII, IOO, \ldots$$

等を含む。恒等置換 1_N は O, I を共に０回繰り返したものと解釈できる。繰り返しの操作は無限にあるように見えるが、例えば５２枚のカードのとき $O^8 = 1_N$ が成り立

つように、違う操作なのにカードの並び方が結果的に同じになるものもある。$\langle O, I\rangle$ の元は置換であるから、それを施した結果並び方が同じであれば同じものと見なすのである。そうすると、$\langle O, I\rangle$ には一体何種類の異なる置換が含まれているのであろうか。そもそも N は $2n$ 個の元から成るから、その上の置換は全部で $(2n)!$ 個あることがわかる。しかし実際は shuffle 群に含まれている置換の数は $(2n)!$ よりもずっと少ない。一般に、$f_1, f_2, \ldots, f_k$ を集合 N 上の置換とするとき、$f_1, f_2, \ldots, f_k$ を何回か繰り返して得られる置換全体を $\langle f_1, f_2, \ldots, f_k\rangle$ と書き、$f_1, f_2, \ldots, f_k$ で生成された置換群と呼ぶ。さらに、置換群 $\langle f_1, f_2, \ldots, f_k\rangle$ に含まれる置換の数をその置換群の位数と呼び、$|\langle f_1, f_2, \ldots, f_k\rangle|$ で表す。「位数」ということばはすでに 2 回出てきた。そのうちの一回の、例えば out shuffle の位数というのは、実は置換群 $\langle O\rangle$ の位数に他ならない。

定理 4. Shuffle 群の位数は少なくとも、2 の $2n-1$ を法とする位数に $2n$ を乗じた数以上である。

証明. 2 の $2n-1$ を法とする位数を t とすると、O の位数は t である（定理 1）。一方、定理 3 より、任意の $k \in N$ に対して 0 を k に移すような置換 $f_k \in \langle O, I\rangle$ が存在する。このとき、$2nt$ 個の置換

$$f_k O^i \quad (0 \leqq i < t,\ 0 \leqq k < 2n) \tag{1}$$

が相異なることを示せば証明が終わる。そこで、今 $f_k O^i = f_l O^j$ $(0 \leqq i, j < t,\ 0 \leqq k, l < 2n)$ とする。このとき $f_k O^i(0) = f_l O^j(0)$ だから $O(0) = 0$ より $f_k(0) = f_l(0)$ となり $k = l$ でなければならないことがわかる。そうすると $f_k O^i = f_k O^j$ となるが、f_k の逆置換 f_k^{-1} との積を考えることにより $O^i = O^j$ を得る。$i \leqq j$ のときは $(O^i)^{-1}$ との積を考えて $O^{j-i} = 1_N$ となるが、これは O の位数が t であることから $i = j$ を意味してしまう。同様に $i \geqq j$ としても $i = j$ が出る。従って (1) の $2nt$ 個の置換は相異なる $\langle O, I\rangle$ の置換である。 □

4 中心対称性

スペードの A, 1, 2,. . . ,10 とクラブの 10, 9, 8,. . . ,2, A の合計２０枚のカードをこの順番で一山に積む。それらに out shuffle や in shuffle を何回施しても、一番上のカードと一番下のカードは、同じ数字のスペードとクラブのカードが現れる。それだけでなく、２０枚のカードを表にしてその並び方を見ると奇妙なことに気がつく。スペードとクラブの違いを無視すると、同じ数字が上から１０枚と下から１０枚の順で並んでいる。もともと上からスペードの A から 10 を、下からクラブの A から 10 を並べておいたのだが、その後何度 out shuffle や in shuffle を施しても、順番こそ変わるものの、上から数えて１０枚と下から数えて１０枚に同じ数字が並んでいるのである。この状況は２０枚の場合に限ったことではない。一般に $2n$ 枚のカードの場合でも全く同様であることがわかる。一番上を０番目と数えることにしたので、位置 k

のカードは実際は上から数えて $k+1$ 番目のことで、一方下から数えて $k+1$ 番目のカードの位置は $2n-1-k$ である。まず、 out shuffle によって位置 k のカードと位置 $2n-1-k$ のカードがどこに動くかを調べよう。位置 k は上半分にあるとしてよいから、 $O(k)=2k$ である。一方 $O(2n-1-k)\equiv 2(2n-1-k)\equiv 2n-1-2k \pmod{2n-1}$ だから、$O(2n-1-k)=2n-1-2k$ となる。このようにして、中心に関して対称な、位置 k と 位置 $2n-1-k$ の 2 枚のカードは、out shuffle によって再び中心に関して対称な、位置 $2k$ と 位置 $2n-1-2k$ に移ることがわかった。In shuffle については、カードの一番上と一番下に一枚ずつ実際には動かないカードを付け加えて out shuffle をしているのと同じであるから、$2n+2$ 枚のカードの場合に out shuffle を考えることにより、やはり中心に関して対称な 2 枚は中心に関して対称な 2 枚に移ることがわかる。

Out shuffle も in shuffle も、中心に関して対称な 2 組を崩すことができないので、shuffle 群のどの置換も中心に関して対称な 2 組を崩すことができない。中心に関して対称な組全体の集合を $\overline{N}$ とおく。

$$\overline{N}=\{\{0,2n-1\},\{1,2n-2\},\{2,2n-3\},\dots,\{n-1,n\}\}$$

すると、Out shuffle も in shuffle も、集合 $\overline{N}$ 上の置換を引き起こす。実際、$O(0)=0$, $O(2n-1)=2n-1$ だから $\{0,2n-1\}$ は自分自身に移る、また $O(1)=2, O(2n-2)=2n-3$ だから $\{1,2n-2\}$ は $\{2,2n-3\}$ に移る、という具合である。今

$$\overline{0}=\{0,2n-1\},\ \overline{1}=\{1,2n-2\},\ \overline{2}=\{2,2n-3\},\ \overline{3}=\{3,2n-4\},\dots$$

と略記すると、out shuffle によって引き起こされた $\overline{N}$ 上の置換 $\overline{O}$ は

$\overline{k}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\dots$
$\overline{O}(\overline{k})$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$	$\dots$

となる。In shuffle についても同様に、 $\overline{I}$ を定義できて、それらで生成された置換群を $\langle\overline{O},\overline{I}\rangle$ と書く。もし f,g が中心に関して対称な 2 組を崩さない置換であれば、それらの積 fg も中心に関して対称な 2 組を崩さない置換であり、f,g,fg の引き起こす $\overline{N}$ 上の置換をそれぞれ $\overline{f},\overline{g},\overline{fg}$ と書くことにすると、$\overline{f}\,\overline{g}=\overline{fg}$ が成り立つ。まとめると、 f,g が Shuffle 群に属する置換であれば、$\overline{f}\,\overline{g}=\overline{fg}$ は $\langle\overline{O},\overline{I}\rangle$ に属する $\overline{N}$ 上の置換となる。

さて、f,g が相異なる置換でも、$\overline{f},\overline{g}$ は同じ置換になることがある。実際、$\overline{1_N}=1_{\overline{N}}$ に注意すると、$\overline{f}^{-1}=\overline{f^{-1}}$ となり、従って $\overline{f^{-1}g}=1_{\overline{N}}$ となる。これは、$f^{-1}g$ が、$\overline{N}$ に属する各組をすべて固定することを意味している。$\overline{N}$ に属する各組をすべて固定するような置換はそれぞれの組に属する 2 つの数字を両方固定するか入れ替えるかのどちらかであるから、全部で 2^n 通りある。ということは、f を固定したとき、$\overline{f}=\overline{g}$ となるような g は全部で 2^n 個ある。もちろんそれら 2^n 個すべてが shuffle 群に属しているという保証はないが、そのことから shuffle 群の位数を上から押さえることができる。なぜなら shuffle 群に属する置換 f に対して、 $\overline{f}$ は $\overline{N}$ の置換であるから

高々 $n!$ 通りしかない。一方ひとつの $\overline{f}$ に対して、上で見たように $\overline{f} = \overline{g}$ となるような shuffle 群に属する置換 g は高々 2^n 個しかない。したがって、 shuffle 群の位数は高々 $M = 2^n \cdot n!$ であることがわかった。

この上界 M は、 $N = \{0, 1, \ldots, 2n-1\}$ の置換の総数 $(2n)!$ よりはかなり小さいが、定理 4 で与えられている下界よりもかなり大きい。実際、定理 4 で与えられている下界は高々 $2n(2n-2)$ である。では shuffle 群の位数は一体どれくらいなのだろうか。この問題の答えは次の節で与える。

5 Shuffle 群の位数

Shuffle 群の位数を決定する問題は、$n = 1$ のときは自明であるので、 $n = 2$ の場合を考えると、定理 4 の下界は 8 であり、また上界 $2^n n!$ も 8 であるから、shuffle 群の位数は 8 であることがわかる。もちろん、直接計算することにより確かめても良い。しかし $n \geqq 3$ のときは上界と下界は一致しないし、直接計算するのも大変である。一般の場合に shuffle 群の位数を決定したのは 1983 年、 Diaconis, Graham, Kantor の３人の論文である [1]。彼等はコンピュータを用いて shuffle 群の位数の表を $n \leqq 26$ まで作った（表１）。この表をもとに、彼等は一般の場合どうなるかを予想し、それを証明した。

定理 5 (Diaconis, Graham, Kantor)**.** Shuffle 群の位数は
(i) $n = 2^k$ のときは、$2^{k+1} \cdot (k+1)$.
(ii) n が 4 の倍数で (i) 以外のとき $M/4$. ただし $n = 12$ を除く。
(iii) n を 4 で割ると 2 余る時、M. ただし $n = 6$ を除く。
(iv) n が奇数のとき $M/2$.

この定理で例外となっている $n = 6, 12$ については表１に shuffle 群の位数が書かれている。実は $n = 12$ の場合、群 $\langle \overline{O}, \overline{I} \rangle$ は 1861 年に E. Mathieu が発見した Mathieu 群 M_{12} と呼ばれる群になっている。

Shuffle 群に関する基本的なことは以上であるが、時間が許す限り、Mathieu 群の特異な性質や、置換群の位数を求める Sims のアルゴリズムなどを解説したい。

表 1: Shuffle 群の位数（$M = 2^n \cdot n!$）

n	1	2	3	4	5	6	7	8	9
$\lvert\langle O, I\rangle\rvert$	M	M	$M/2$	$2^3 \cdot 3$	$M/2$	$M/6$	$M/2$	$2^4 \cdot 4$	$M/2$
n	10	11	12	13	14	15	16	17	18
$\lvert\langle O, I\rangle\rvert$	M	$M/2$	$M/(7! \cdot 2)$	$M/2$	M	$M/2$	$2^5 \cdot 5$	$M/2$	M
n	19	20	21	22	23	24	25	26	
$\lvert\langle O, I\rangle\rvert$	$M/2$	$M/4$	$M/2$	M	$M/2$	$M/4$	$M/2$	M	

参考文献

[1] P. Diaconis, R. L. Graham, and W. M. Kantor, The mathematics of perfect shuffles, Adv. in Appl. Math. 4 (1983), no. 2, 175–196.

[2] E. Mathieu, Mémoire sur l'étude des fonctions de plusieurs quantitiés, J. Math. Pures Appl. 6 (1861), 241–243.

[3] C. C. Sims, Computational methods in the study of permutation groups, in "Computational Problems in Abstract Algebra," Proc. Conf., Oxford, 1967 (J. Leech, Ed.), pp.169–183, Pergamon, Oxford, 1970.