2種類のシャフリングの関係性について

学習院大学 理学部 数学科
山口 友加里

平成 20 年 2 月 2 日

目 次

1 目的 3

2 方法 3
2.1 シャフリングをするにあたって必要なプログラム 4
2.2 ４分シャフリング 6
2.3 ２分シャフリング 8
2.4 ２分シャフリング（逆転バージョン） 9

3 結果 10

4 考察 13
4.1 例えば… 13
4.2 一般の場合 15
4.3 ２分シャフリングと 4 分シャフリングの周期について 17

5 最後に 19

1　目的

この研究において、トランプのシャッフルの仕方で２分考えるシャフリング（英語で modified perfect faro shuffle)、４分考えるシャフリングの周期を比較し、２種類のシャフリングの関係性を研究した。

2　方法

2 分シャフリングの仕方（枚数 8 枚で考える）☆☆☆

1 2 3 4 5 6 7 8

◎半分で分ける。
1 2 3 4　　5 6 7 8

◎後ろ半分を前半分の上に並べる。

5 6 7 8
1 2 3 4

◎左上から下へ順に並べていく。
5 1 6 2 7 3 8 4

4 分シャフリングの仕方（枚数 8 枚で考える）☆☆☆

1 2 3 4 5 6 7 8

◎ 4 つに分ける。
1 2　　3 4　　5 6　　7 8

◎後ろの組から上に並べる。
7 8
5 6
3 4
1 2

◎左上から下へ順に並べていく。
7 5 3 1 8 6 4 2

このやり方のプログラムを Prolog で作成し、実行する。

2.1 シャフリングをするにあたって必要なプログラム

```
/** リストを生成するプログラム **/

genlist(A,Z,[]):- A>Z,!.
genlist(A,Z,[A|List]):- A1 is A+1,
genlist(A1,Z,List).

/** 繰り返すプログラム **/

for(I=<J,I):- I =<J.
for(I=<J,K):- I =<J,
     I1 is I+1,for(I1 =<J,K).


/** 素因数分解するプログラム **/

factor(P/2):- Q is P//2,P=:=2*Q,!.
factor(P/I):-P1 is floor(sqrt(P)),
     for(1=< P1 ,J),
       J1 is  2*J+1,
       Q is P//J1,
       P=:= J1*Q,I=J1,!.

factor(P/P):-!.


factorize(P,[P]):-factor(P/X),X==P,!.
factorize(P,List):-factor(P/I),
P1 is P//I,
List=[I|List1],
factorize(P1,List1),!.

ffact(N,L):-N1 is N+1,factorize(N1,L).


/** 残り物を示すプログラム **/

left(A=[]+A,0):- !.
left(A=B+C,N):- N>0,N1 is N-1,!,
left(A=B1+[X|C],N1),append0(B=B1+[X]),!.
```

```
/** リストの足し算 **/

append0(Z=[]+Z).
append0([A|Z]=[A|X]+Y):-append0(Z=X+Y).

/** 3つに分けるプログラム **/

mid(L=A+C+B,N,M):-
left(L=A+D,N),left(D=C+B,M).

/** 三等分するプログラム **/

third(L=A+B+C):-
length(L,N),N1 is N/3,N2 is N/3,mid(L=A+B+C,N1,N2).
```

2.2 ４分シャフリング

```
/** ４分シャフリング **/
shf4([]+[]+[]+[]=[]).
shf4([X|D]+[Y|C]+[Z|B]+[W|A]=[X,Y,Z,W|M]):-
shf4(D+C+B+A=M).

shuffle4(L=M):-fourth(L=A+B+C+D),shf4(D+C+B+A=M),!.


fourth(L=A+B+C+D):-
length(L,N),N1 is N/4,N2 is N/4,N3 is N/4,
left(L=A+E,N1),mid(E=B+C+D,N2,N3).

shuffle4(L,0):-
write(L),nl.
shuffle4(L,N):-
shuffle4(L=M),N1 is N-1,
write(L),nl,
shuffle4(M,N1).

shuffle4(L,0,A):-write(L),nl.
shuffle4(L,N,A):-shuffle4(L=M),N1 is N-1,N0 is 3001-N,
write(N0),tab(2),
write(L),nl,
(M \==A,shuffle4(M,N1,A);write(m=N0),true).


bigshf4(N):-genlist(1,N,L),
shuffle4(L,3000,L).


shf44(L,0,A):-!.
shf44(L,N,A):-shuffle4(L=M),N1 is N-1,N0 is 30001-N,!,


(M \==A -> shf44(M,N1,A);(write(m=N0),tab(2))).


shf444(L,N,A) :- shf44(L,N,A),!.
```

```
bbig44(N):-genlist(1,N,L),write(n=N),tab(2),
N1 is N+1,factorize(N1,List),write(l=List),
    tab(2),shf444(L,30000,L),!.

ff44(L,M):-for(L=<M,N),
  P is N*4,nl,
bbig44(P),
nl,fail.

ff44(L,M).
```

2.3 ２分シャフリング

```
/** ２分シャフリング **/

half(L=A+B):-
length(L,N),N1 is N/2,left(L=A+B,N1).


shf([]+[]=[]).
shf([X|B]+[Y|A]=[X,Y|M]):-
shf(B+A=M).
shuffle(L=M):-half(L=A+B),shf(B+A=M),!.


shuffle(L,0):-
write(L),nl.
shuffle(L,N):-
shuffle(L=M),N1 is N-1,
write(L),nl,
shuffle(M,N1).



shuffle34(L,0,A):-write(L),nl.
shuffle34(L,N,A):-shuffle(L=M),N1 is N-1,N0 is 3001-N,
write(N0),tab(2),
write(L),nl,
(M \==A,shuffle34(M,N1,A);write(m=N0),true).


bigshf34(N):-genlist(1,N,L),
shuffle34(L,3000,L).


shf4(L,0,A):-!.
shf4(L,N,A):-shuffle(L=M),N1 is N-1,N0 is 30001-N,!,


(M \==A -> shf4(M,N1,A);(write(m=N0),tab(2))).

shf40(L,N,A) :- shf4(L,N,A),!.
```

```
bbig4(N):-genlist(1,N,L),write(n=N),tab(2),
N1 is N+1,factorize(N1,List),write(l=List),
   tab(2),shf40(L,30000,L),!.

ff4(L,M):-for(L=<M,N),
  P is N*2,
bbig4(P),
nl,fail.

ff4(L,M).
```

2.4　２分シャフリング（逆転バージョン）

```
/**　２分シャフリング（逆転 Ver.）**/
shf5(L,0,A):-!.
shf5(L,N,A):-reverse(A,AA),shuffle(L=M),N1 is N-1,N0 is 30001-N,!,


(M \==AA -> shf5(M,N1,A);(write(m=N0),tab(2))).



shf5(L,N,A):-shf5(L,N,A),!.


bbig5(N):-genlist(1,N,L),write(n=N),tab(2),
N1 is N+1,factorize(N1,List),write(l=List),
   tab(2),shf5(L,30000,L),!.



ff5(L,M):-for(L=<M,N),
  P is N*2,
bbig5(P),
nl,fail.

ff5(L,M).
```

3　結果

シャフリングをした結果以下のとおりになった。

表 1: シャフリングの結果その 1

枚数	周期 (2 分 Ver.)	周期 (4 分 Ver.)
4	4	2
6	3	
8	6	3
10	10	
12	12	6
14	4	
16	8	4
18	18	
20	6	3
22	11	
24	20	10
26	18	
28	28	14
30	5	
32	10	5
34	12	
36	36	18
38	12	
40	20	10
42	14	
44	12	6
46	23	
48	21	21
50	8	
52	52	26
54	20	
56	18	9
58	58	
60	60	30
62	6	
64	12	6
66	66	
68	22	11
70	35	

表 2: シャフリングの結果その 2

枚数	周期 (2 分 Ver.)	周期 (4 分 Ver.)
72	9	9
74	20	
76	30	15
78	39	
80	54	27
82	82	
84	8	4
86	28	
88	11	11
90	12	
92	10	5
94	36	
96	48	24
98	30	
100	100	50
102	51	
104	12	6
106	106	
108	36	18
110	36	
112	28	14
114	44	
116	12	6
118	24	
120	110	55
122	20	
124	100	50
126	7	
128	14	7
130	130	
132	18	9
134	36	
136	68	34
138	138	
140	46	23

表 3: シャフリングの結果その 3

枚数	周期 (2 分 Ver.)	周期 (4 分 Ver.)
142	60	
144	28	14
146	42	
148	148	74
150	15	
152	24	12
154	20	
156	52	26
158	52	
160	33	33
162	162	
164	20	10
166	83	
168	156	78
170	18	
172	172	86
174	60	
176	58	29
178	178	
180	180	90
182	60	
184	36	18
186	40	
188	18	9
190	95	
192	96	48
194	12	
196	196	98
198	99	
200	66	33

4　考察

4.1　例えば…

　枚数を与えると周期がわかった。
逆に周期を与えた場合、枚数がわかるだろうか。

　10 枚で 2 分シャフリングを考える。
最初の並び方を x とし、1 回シャフリングした時の並び方を y とする。

表 4: 10 枚で 2 分シャフリング

x	1	2	3	4	5	6	7	8	9	10
y	6	1	7	2	8	3	9	4	10	5
2y	12	2	14	4	16	6	18	8	20	10
2y − x	11	0	11	0	11	0	11	0	11	0

　となる。
このことから

$$2y - x \equiv 0 \mod 11$$

$$y \equiv \frac{1}{2}x \mod 11 \cdots (1)$$

　例えば、

$$2 \times 6 = 12 \equiv 1 \mod 11$$

$$6 \equiv \frac{1}{2} \mod 11$$

　(1) より、

$$y \equiv 6x \mod 11$$

　これを用いて先ほどの表 4 を考えると、

表 5: x を 6 倍して mod 11 で考える

x	1	2	3	4	5	6	7	8	9	10
6x	6	12	18	24	30	36	42	48	54	
6x (mod11)	6	1	7	2	8	3	9	4	10	5

　表 5 より、x をそれぞれ 6 倍して mod 11 で考えると 1 回シャフリングした y になる。

さらに、2 回 x をシャフリングしたものを z とすると、同様にして

$$z \equiv 6y \mod 11$$

よって、$y \equiv 6x \mod 11$ なので、

$$z \equiv 6 \times 6x = 6^2x \mod 11$$

これを繰り返し、m 回シャフリングをしたときに元に戻るとしたら、

$$6^m x \equiv x \mod 11$$

$x \neq 0$ なので x で両辺割ると、

$$6^m \equiv 1 \mod 11$$

となる最小の整数 m が周期となる。

$m = 1$ のとき $6^1 = 6 \equiv 6$、 $m = 2$ のとき $6^2 = 6 \times 6 = 36 \equiv 3$、 $m = 3$ のとき $6^3 \equiv 3 \times 6 \equiv 7$
$m = 4$ のとき $6^4 \equiv 7 \times 6 \equiv 9$、 $m = 5$ のとき $6^5 \equiv 9 \times 6 \equiv 10$、 $m = 6$ のとき $6^6 \equiv 10 \times 6 \equiv 5$
$m = 7$ のとき $6^7 \equiv 5 \times 6 \equiv 8$、 $m = 8$ のとき $6^8 \equiv 8 \times 6 \equiv 4$、 $m = 9$ のとき $6^9 \equiv 4 \times 6 \equiv 2$
$m = 10$ のとき $6^{10} \equiv 2 \times 6 \equiv 1$
となるので、$m = 10$ のとき、に元に戻る。よって周期は 10 である。

◎ 6 と 2 の位数は同じである。

4.2　一般の場合

☆☆☆ 2 分シャフリング Ver. ☆☆☆

4,1 では例として枚数 10 枚の場合について考えたが、一般の場合についても考よう。

枚数 2n 枚のとき、

$$2^m \equiv 1 \mod 2n+1$$

上の式を満たす 最小の正の整数 m が周期となる。

周期と枚数の関係式

枚数 2n 枚、周期 m のとき

$$2^m - 1 = k(2n + 1)$$

これにより、周期からシャフリングする枚数を考えることができる。
同様にして 4 分シャフリングも考えることができる。
ただし、枚数は 4 枚 からとなるので注意する。

周期と枚数の関係式

枚数を 4n、周期を m とすると、

$$4^m - 1 = k(4n + 1)$$

例 周期 $m = 6$ のとき、周期と枚数の関係式に代入する。

$$2^6 - 1 = k(2n + 1)$$

$$63 = k(2n + 1)$$

よって $2n + 1 = 3, 7, 9, 21, 63$ なので

$$2n = 2, 6, 8, 20, 62$$

つまり周期が 6 のときの枚数は 8 枚、20 枚、62 枚である。表 1 でもこの結果は確認できる。
注：枚数が 2 枚ならば周期が 2、枚数が 6 枚のときは周期が 3 となり最小の整数ではないので除く。

与えられた周期に対して枚数が一通りしかない場合はどのような場合か。

命題

2^m-1 が素数ならば m も素数になる。

< 証明 >

背理法で示す。

m が素数でないと仮定すると、2^m-1 が合成数であることを証明する。

$m=uv$ とおくと、

$$2^{uv}-1=(2^u)^v-1$$

$2^u=X$ とおくと、

$$(2^u)^v-1=X^v-1$$

等比級数の和の公式を用いて、

$$X^v-1=(X-1)(X^{v-1}+X^{v-2}+\cdots+1)$$

$$=(2^u-1)\{(2^u)^{v-1}+(2^u)^{v-2}+\cdots+1\}$$

と因数分解できるから、2^m-1 は素数ではない。

よって、2^m-1 が素数ならば、周期 m は素数であることが証明された。

このように、2^m-1 が素数であれば、m も素数でなければならない。

素数 m に対して、2^m-1 の形の数をメルセンヌ数と呼び、これが素数のときに、メルセンヌ素数という。

しかし、m=11,29 については

$$2^{11}-1=2047=23\times89$$

$$2^{29}-1=536870991=223\times1103\times2089$$

となって素数ではない場合もある。

2^m-1 がメルセンヌ素数であれば、枚数は一通りしかない。

例

周期と枚数の関係式に $m=3$ を代入すると、

$$2^3-1=k(2n+1)$$

$$7=k(2n+1)$$

よって、$2n+1=1$ or 7 と考えられる。しかし、$2n\neq0$ より、

$$2n+1=7$$

$$2n=6$$

より枚数は一通りである。

4.3 2分シャフリングと4分シャフリングの周期について

結果の表を見てみると、枚数が同じのとき、4分シャフリングの周期は2分シャフリングの周期の2倍であることがわかる。

表 6: シャフリングの結果その1の1部分

枚数	周期 (2分 Ver.)	周期 (4分 Ver.)
4	4	2
6	3	
8	6	3
10	10	
12	12	6
14	4	
16	8	4

枚数が4の倍数のときの2分シャフリングと4分シャフリングの周期の関係式を考えたい。2分シャフリングの周期を p、4分シャフリングの周期を m とする。

$$2^p \equiv 1 \mod 2 \times 2n + 1 \ldots (1)$$

$$4^m \equiv 1 \mod 4n + 1 \ldots (2)$$

(2) を考える。

$$4^m = 2^{2m} \equiv 1 \mod 4n + 1$$

これを (1) と比較して、

$$p = 2m$$

となり2分シャフリングの周期は4分シャフリングの周期の2倍であることがわかる。

しかし、研究を続けていくと、2 分シャフリングの周期が奇数のとき に限り、

2 分シャフリングの周期＝4 分シャフリングの周期

ということがわかった。
☆証明☆
枚数が 2n 枚 (n=2n' とする。) で 2 分シャフリングの周期 m が奇数のとき、
m=2k+1 とおく。

$$2, 2^2, 2^3, \cdots, 2^{2k+1} \equiv 1 \mod 2n+1$$

である。$j \leq k$ のとき、

$$4^j = 2^{2j}$$

次に、

$$4, 4^2, 4^3, \cdots, 4^k, 4^{k+1} = 2^{2k+1} \times 2 \equiv 2 \mod 2n+1$$

$$4^{k+2} = 2^{2k+4} = 2^{2k+1} \times 2^3 \equiv 2^3 \mod 2n+1$$

以下これを繰り返すと、一般に、

$$4^{k+j} = 2^{2k+1} \times 2^{2j-1} \equiv 2^{2j-1} \mod 2n+1$$

となるので、$j = k$ のとき、

$$4^{k+k} = 4^{2k} = 2^{2k+1} \times 2^{2k-1} \equiv 2^{2k-1} \mod 2n+1$$

これを用いて、

$$4^{2k+1} = 4^{2k} \times 4 \equiv 2^{2k-1} \times 2^2 = 2^{2k+1} \equiv 1 \mod 2n+1$$

となり 2 分シャフリングの周期 m が奇数のとき、2 種類の周期が等しくなることが証明された。

参考文献

[1] NUMBER THORY(George E.Andrews)

5　最後に

普段、遊ぶときなどに使うトランプで、研究をするとは思いませんでした。研究を始めたころは Plorog の使い方も全くわからなくて、迷惑をかけてばかりでしたが、だんだんと内容がわかってきて、研究内容も決定して、プログラムにも自信がついてきて、そこからはシャフリングが数学に結びついていることを発見したりすることが楽しくなりました。電車の中でも考えたりしました。なんとか論文が形になってくると、手直しをしていくうちに、自分自身で気づくことがあったりなど、ひとつのことに夢中になって研究できてとても有意義な時間となりました。あれこれ試行錯誤しながら出来上がったこの論文は絶対捨てられません !! 飯高先生にいろいろくだらないことを聞いたり、うるさい学生でしたが、飯高先生の研究室に入ってとってもよかったと満足してます。ありがとうございました。