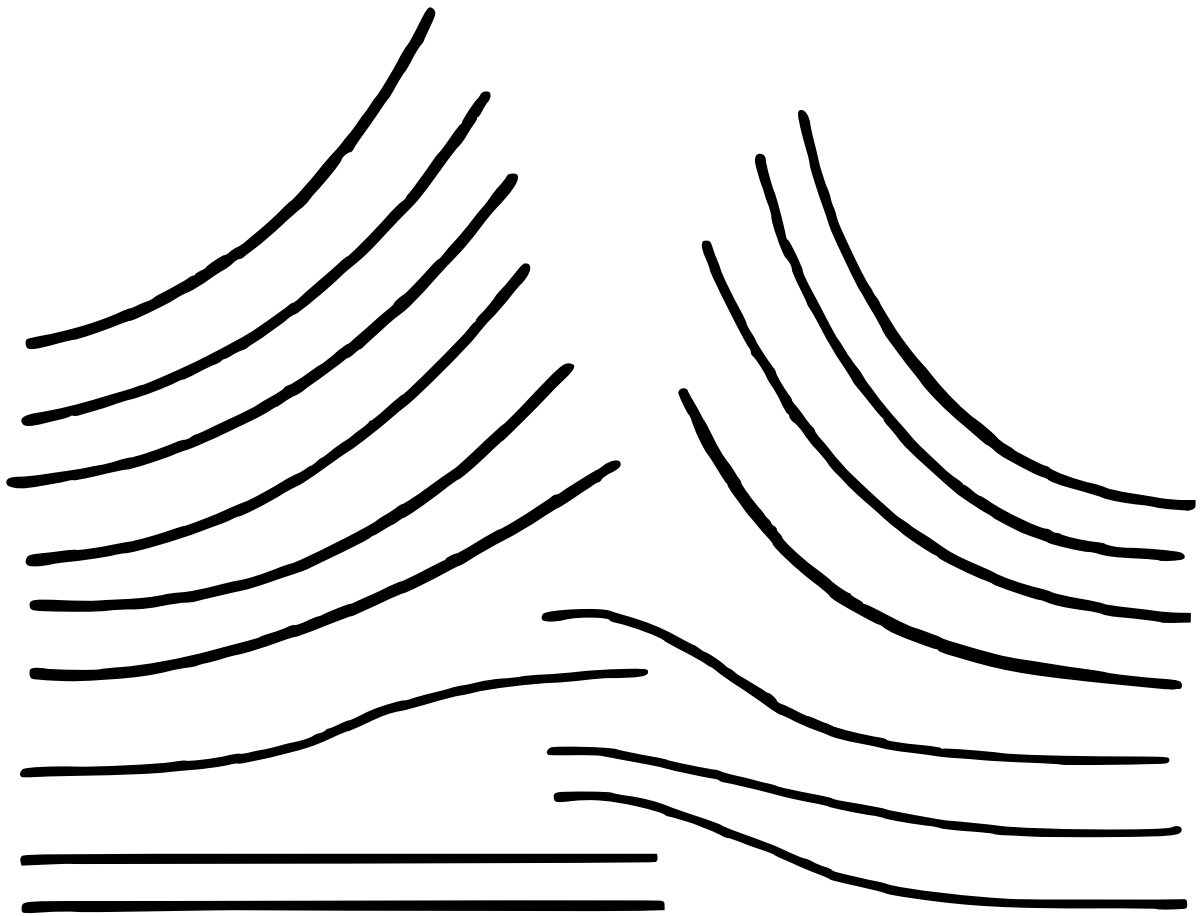
ギルブレスの原理

日本ユニシス株式会社
川辺治之

2013 年 11 月 20 日

リフル・シャフル



ギルブレスの第1原理

- カードの束を好きな位置でカットする。(何度カットしてもよい。)
- そして、その束を裏向きに持ち、その束のほぼ半分程度を裏向きのまま机上の山としてに配る。(厳密に半分である必要はない。)
- 手元と机上それぞれにできたカードの山をリフル・シャフルで一つにまとめる。(このときも、二つの山のカードがきちんと交互に並ぶ必要はない。)
- そして、この束をの上から2枚ずつを表返して配ると…

第1原理の応用

リフル・シャフルをした後のカードの束の上から20枚が赤黒黒赤黒赤赤黒赤黒黒赤赤黒黒赤赤黒黒赤であったとすると、それを二つの山に交互に配り分けると、

赤	黒	黒	赤	赤	黒	赤	黒	赤	黒
黒	赤	赤	黒	黒	赤	黒	赤	黒	赤

となる。

一方の10枚の赤札/黒札の並びから、もう一方の10枚の赤札/黒札の並びを知ることができる。

ギルブレスの第2原理

クラブ、ハート、スペード、ダイヤ、クラブ、ハート、スペード、ダイヤ、…と繰り返すように並べたカードの束を用意する。

このカードの束を無作為にカットし、好きなだけの枚数を机上の山として裏向けに配り（カードの順序は逆順になる。）、その山と手元に残った束をリフル・シャフルでひとまとめにする。

すると、この束の上から４枚には、それぞれのマークが１枚ずつ含まれ、その次の４枚にも同じようにそれぞれのマークが１枚ずつ含まれ、それが束の最後の４枚まで続く。

ギルブレス・シャフル

1、2、3、...と番号づけられたN枚のカードの束を考える。（通常のトランプでは$N = 52$）

一番上は1で、その次は2で、と続き、一番下はNになるように並べたカードの束から始める。

ある1以上N以下の数jをひとつ決め、カードの束の上からj枚のカードが逆順になるように、裏向きのまま机上の山に配る。

そして、このj枚のカードを手元に残った$N - j$枚のカードの束とリフル・シャフルする。

この並べ替えを「ギルブレス・シャフル」と呼ぶことにする。

ギルブレス・シャフルの例

$N = 10$ で $j = 4$ の場合に、リフル・シャフルをした結果はたとえば次のようになる。

1						4
2						5
3		5				6
4		6	4			3
5	→	7	3	→		7
6		8	2			2
7		9	1			8
8		10				9
9						1
10						10

ギルブレス・シャフルの結果

ギルブレス・シャフルを 1 回行っても、N 枚のカードの並びは、$N!$ 通りのすべてが起こるわけではない。

N 枚のカードの束にギルブレス・シャフルを行って得られる並びの場合の数は 2^{N-1} 通りだけであることを後で示す。

たとえば、$N = 10$ ならば $2^{N-1} = 512$ で、$N = 52$ ならば $2^{51} \approx 2.25 \times 10^{15}$ である。これは、（仕掛けをバレにくくし、トリックを興味深いものにするには）十分大きな値である。

ギルブレス置換

1、2、3、…、Nと並んでいたカードの束を並び換えて得られた新しい並びをπとすると、$\pi(1)$でその新しい並びの一番上のカードを、$\pi(2)$で上から2番目のカードを,…、そして$\pi(N)$でN番目のカードを表す。

たとえば、ギルブレス・シャフルを行った後の5枚のカードの並びが、3、5、1、2、4だったとすると、$\pi(1) = 3$、$\pi(2) = 5$、$\pi(3) = 1$、$\pi(4) = 2$、$\pi(5) = 4$である。

1、2、3、…、NのN枚のカードの束をギルブレス・シャフルして$\pi(1)$、$\pi(2)$、…、$\pi(N)$という並びが得られることを、「πはギルブレス置換である」と表記する。

ギルブレスの究極原理

$\{1, 2, 3, \ldots, N\}$の置換πに対して、次の四つの条件は同値となる。

1. πはギルブレス置換である。
2. 任意のjに対して、束の上からj枚のカード$\{\pi(1), \pi(2), \pi(3), \ldots, \pi(j)\}$は$j$を法として相異なる。
3. $kj \leq N$となる任意のjおよびkに対して、j枚のカード$\{\pi((k-1)j+1), \pi((k-1)j+2), \ldots, \pi(kj)\}$は$j$を法として相異なる。
4. 任意のjに対して、束の上からj枚のカード$\{\pi(1), \pi(2), \pi(3), \ldots, \pi(j)\}$は、$1, 2, 3, \ldots, N$の中の$j$個の連続した整数になる。

ギルブレス置換の例

ギルブレス置換 4 5 6 3 7 2 8 9 1 10 では条件 (2) が成り立つ。

4	→0	(mod 1)
45	→01	(mod 2)
456	→120	(mod 3)
4563	→0123	(mod 4)
45637	→40132	(mod 5)
456372	→450312	(mod 6)
4563728	→4563021	(mod 7)
45637289	→45637201	(mod 8)
456372891	→456372801	(mod 9)
4563728910	→4563728910	(mod 10)

ギルブレス置換の例（続き）

ギルブレス置換 4 5 6 3 7 2 8 9 1 10 では条件 (3) が成り立つ。

$$4\,5\,6\,3\,7\,2\,8\,9\,1\,10 \to 0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \pmod 1$$
$$4\,5\,6\,3\,7\,2\,8\,9\,1\,10 \to 0\,1\,0\,1\,1\,0\,0\,1\,1\,0 \pmod 2$$
$$4\,5\,6\,3\,7\,2\,8\,9\,1\,10 \to 1\,2\,0\,0\,1\,2\,2\,0\,1 \pmod 3$$
$$4\,5\,6\,3\,7\,2\,8\,9\,1\,10 \to 0\,1\,2\,3\,3\,2\,0\,1 \pmod 4$$
$$4\,5\,6\,3\,7\,2\,8\,9\,1\,10 \to 4\,0\,1\,3\,2\,2\,3\,4\,1\,0 \pmod 5$$
$$4\,5\,6\,3\,7\,2\,8\,9\,1\,10 \to 4\,5\,0\,3\,1\,2 \pmod 6$$
$$4\,5\,6\,3\,7\,2\,8\,9\,1\,10 \to 4\,5\,6\,3\,0\,2\,1 \pmod 7$$
$$4\,5\,6\,3\,7\,2\,8\,9\,1\,10 \to 4\,5\,6\,3\,7\,2\,0\,1 \pmod 8$$
$$4\,5\,6\,3\,7\,2\,8\,9\,1\,10 \to 4\,5\,6\,3\,7\,2\,8\,0\,1 \pmod 9$$
$$4\,5\,6\,3\,7\,2\,8\,9\,1\,10 \to 4\,5\,6\,3\,7\,2\,8\,9\,1\,0 \pmod{10}$$

ギルブレス置換の例（続き）

ギルブレス置換 4 5 6 3 7 2 8 9 1 10 では条件 (4) が成り立つ。

4 → 4
45 → 45
456 → 456
4563 → 3456
45637 → 34567
456372 → 234567
4563728 → 2345678
45637289 → 23456789
456372891 → 123456789
4563728910 → 12345678910

ギルブレス置換の総数

$\{2, 3, \ldots, N\}$の任意の部分集合$S = \{s_1, s_2, \ldots, s_j\}$（$s_1 < s_2 < \cdots < s_j$）に対して、カード jを１番目に、カード $j-1$を s_1番目に、カード $j-2$を s_2番目に、$\cdots$というように置き、jより大きいカードはSに含まれない位置に昇順に置くとギルブレス置換になる。

すべてのギルブレス置換はこの方法で一意に構成することができる。

このような部分集合Sを選ぶ方法は2^{N-1}通りあるので、N枚のカードに対するギルブレス置換の総数は2^{N-1}通りとなる。

究極原理の証明$(1 \Rightarrow 2)$

ギルブレス・シャフルを行った結果の上から j 枚のカードの集合は、ある値 a に対して、$\{a, a+1, \ldots, a+(j-1)\}$ または $\{a, a-1, \ldots, a-(j-1)\}$ となる。この集合は、j を法として相異なる値で構成されている。

究極原理の証明(2 ⇔ 3)

πが条件(2)を満たすと仮定する。すると、上から$2j$枚のカードは$2j$を法として相異なるので、jを法として$\{0, 1, \ldots, j-1\}$がちょうど2度ずつ現れることになる。

そして、上からj枚のカードはjを法として$\{0, 1, \ldots, j-1\}$が1度ずつ現れるのだから、$\pi(j+1), \pi(j+2), \ldots, \pi(2j)$は$j$を法として相異ならなければならない。

同様にして、$\pi(2j+1), \pi(2j+2), \ldots, \pi(3j)$は$j$を法として相異なることがわかる。

一方、あきらかに(3)は(2)を含意するので、(2)と(3)は同値である。

究極原理の証明(2 ⇒ 4)

束の上から j 枚のカードの集合はある連続する整数の区間になることを示す。

束の一番上のカードが k だとすると、その次のカードは $k+1$ か $k-1$ でなければならない。なぜなら、もしある $d>1$ に対してそのカードが $k \pm d$ であったとすると、上から d 枚のカードは d を法として相異なることに反する。

同様にして、上から $j+1$ 枚のカードが $a, a+1, \ldots, a+j$ であったとき、その次のカードは $j+2$ を法としてこれら $j+1$ 枚のカードと相異ならなければならないが、$a-1$ でも $a+j+1$ でもないならば、ある正整数 n に対して $d=1+n(j+2)>1$ として $a-d$ または $a+j+d$ でなければならない。$d>j+2$ であることに注意すると、束の上から d 枚のカードを考えると、d を法としてそれぞれ a または $a+j$ に一致してしまう。

究極原理の証明(4 ⇒ 1)

πが条件(4)の「区間」を構成することから、πが$k+1, k+2, \ldots, n$という昇順列と$k, k-1, \ldots, 1$という降順列に分解できることを示す。

これは、束の上からカードを順に調べていけばよい。一番上のカードがkならば、その次のカードは$k+1$か$k-1$でなければならない。

それぞれのカードによって、それまでの区間の最大値を増加させるのであれば昇順列の末尾にその値を追加し、最小値を減少させるのであれば降順列の末尾にその値を追加する。

こうしてできあがった昇順列と降順列によってπはギルブレス置換であることがわかる。

デブロインの拡張

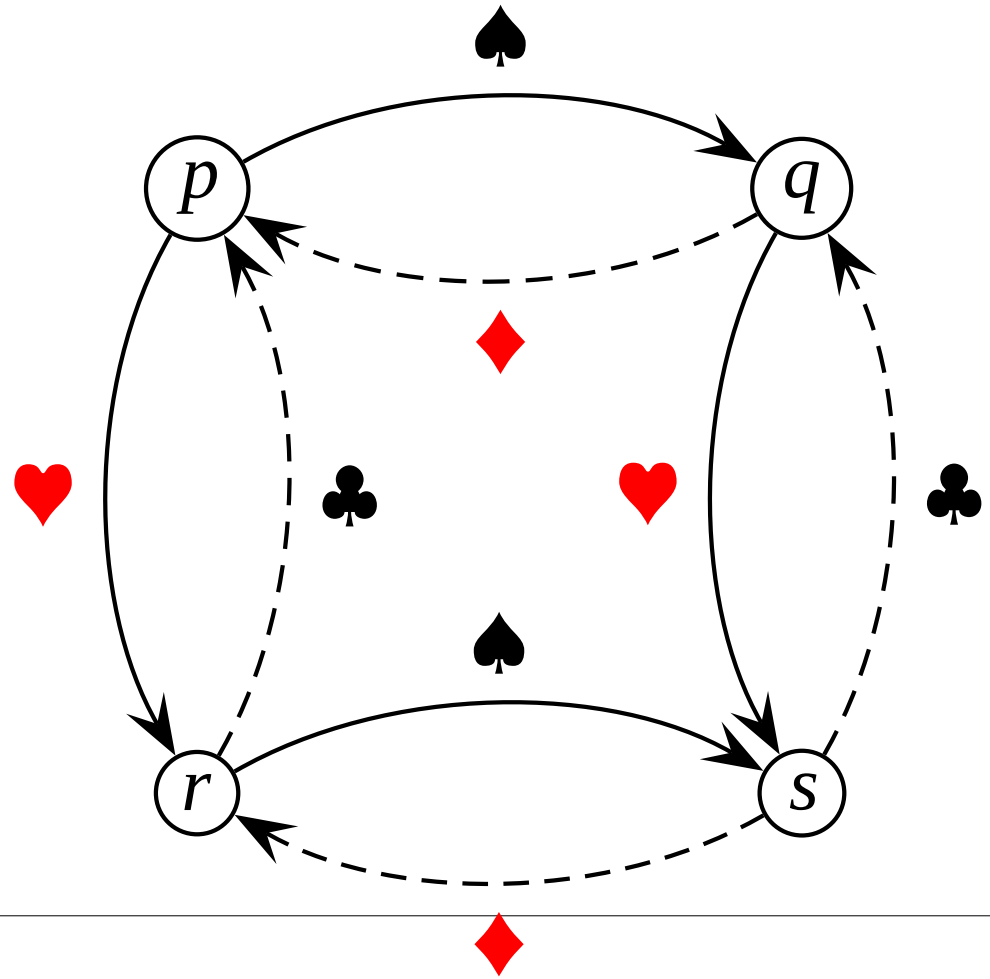
スペードとダイヤを♠♦♠♦・・・と交互に並べて26枚のカードの山を作り、ハートとクラブを♥♣♥♣・・・と交互に並べて26枚のカードの山を作る。

この二つの山をリフル・シャフルでひとまとめにして、上から2枚ずつを対にすると、それぞれの対は赤札と黒札が1枚ずつになる。

しかし、この52枚のカードの束を自由にカットしてしまうと、もはやこの性質は成り立たなくなるが、上から2枚ずつの対は、赤札と黒札の対になるか、またはメジャー（♠ ♥）とマイナー（♣ ♦）の対になる。

状態遷移図

ノード p または s から 2 ステップ進むと必ずノード p または s に移り、ノード q または r から 2 ステップ進むと必ずノード q または r に移る。



ディスク・ストライピング

ディスクを増設してデータの読み書きの処理速度を向上させる方法のひとつに、大きなファイルに対するディスク・ストライピングの技法がある。

D 個のディスク装置 $0, 1, \ldots, D-1$ があり、L 個のブロック $a_0 a_1 \cdots a_{L-1}$ からなるファイルがあるとき、このファイルを D 個のディスクにストライプするとは、ブロック a_j をディスク $j \bmod D$ に置くことを意味する。

したがって、ディスク 0 にはブロック $a_0 a_D a_{2D} \cdots$ が、ディスク 1 にはブロック $a_1 a_{D+1} a_{2D+1} \cdots$ が、というように置かれる。

スーパーブロック

このとき、同時に読み書きを行うことのできる D 個のブロックの集まり $a_0 a_1 \cdots a_{D-1}, a_D a_{D+1} \cdots a_{2D-1}, \ldots$ をスーパーブロックと呼ぶ。

キーによってソートされている二つのファイルに対して、等しいキーのレコードの照合を行うとき、スーパーブロックのストライピングに対して次のような改良を行う。

ストライピングの改良

一方のファイルのブロック $a_0 a_1 a_2 \cdots$ を前述のように D 個のディスクにストライプし、もう一方のファイルのブロック $b_0 b_1 b_2 \cdots$ は逆向き、すなわちブロック b_j をディスク $(D - 1 - j) \bmod D$ にストライプしておく。

たとえば、$D = 5$ の場合は、ブロック a_j は順にディスク $0, 1, 2, 3, 4, 0, 1, 2, \ldots$ に置かれ、ブロック b_j は順にディスク $4, 3, 2, 1, 0, 4, 3, 2, \ldots$ に置かれることになる。

ブロック a_j の最後のキーを α_j、ブロック b_j の最後のキーを β_j とすると、これらを調べることで次に読み込むデータブロックの並びを予測することになる。

データブロックの並びの例

読み込むデータブロックの並びが、たとえば

$$a_0 b_0 a_1 a_2 b_1 \quad a_3 a_4 b_2 a_5 a_6 \quad a_7 a_8 b_3 b_4 b_5 \quad b_6 b_7 b_8 b_9 b_{10} \quad \cdots$$

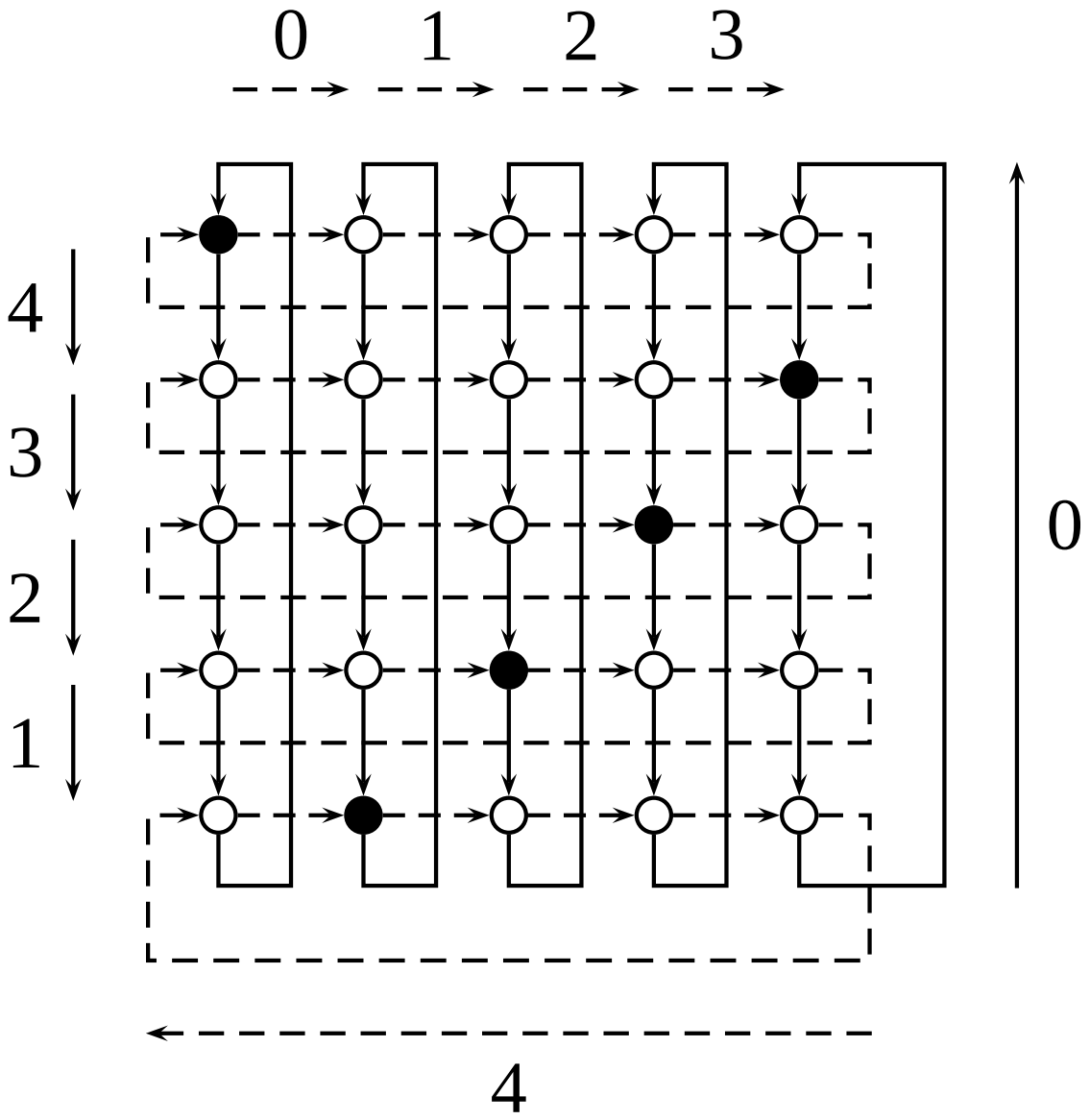
であったとすると、$D = 5$のときには、これらのブロックはそれぞれディスク

$$0\,4\,1\,2\,3 \quad 3\,4\,2\,0\,1 \quad 2\,3\,1\,0\,4 \quad 3\,2\,1\,0\,4 \quad \cdots$$

となる。

これらを一度に5個ずつ読み込めば、ディスク$\{0, 4, 1, 2, 3\}$,$\{3, 4, 2, 0, 1\}$,$\{2, 3, 1, 0, 4\}$,$\{3, 2, 1, 0, 4\}$,...から逐次読み込むことになり、同じディスクから同時に二つのブロックを読み込む衝突は起こらない。

$D = 5$の状態遷移図



参考文献

[1] Kunuth, Donald E. *The Art of Computer Programming* Vol.3 Sorting and Searching, 2nd ed. (邦訳：有澤誠/和田英一 監訳、アスキー、2006）

[2] de Bruijn, N.G. “A Riffle Shuffle Card Trick and Its Relation to Quasicrystal Theory,” *Nieuw Archief voor Wiskunde* (4) 5, no. 3 (1987): 285–301.

[3] Diaconis, Persi, and Ron Graham. *Magical Mathematics: The Mathematical Ideas that Animate Great Magic Tricks*. Princeton Univ. Press, 2011.（邦訳：川辺『数学で織りなす カードマジックのからくり』共立出版、2013）