Japan Journal of Research

Review Article

Initiation Of Cryptology Thanks To A Scilab™ Project Using Perfect Magic Shuffles

P. Schott

Laboratoire d'Informatique, Image et Signal, Télécom et Electronique (LISITE), Isep, Paris, France

Correspondence

P. Schott

Laboratoire d'Informatique, Image et Signal, Télécom et Electronique (LISITE), Isep, Paris, France

Email: pierrot.schott@laposte.net, pierre.schott@isep.fr

- Received Date: 27 Jun 2023
- Accepted Date: 03 Jul 2023
- Publication Date: 09 Jul 2023

Keywords

Higher education, engineer, educational method, cryptography, informatics security, mathematical functions, idempotence, project pedagogy, Scilab, Java, programming application

Abstract

Why use Magic for teaching cryptology and algorithmic notions through thanks to Scilab/Matlab programs? During a magic performance, the audience will seek to understand how the trick works once the surprise has worn off. So the teacher can use that in order to interest their students, and a magic trick will lead them to ask how does it work? After discovering the secret, the students could want to create one trick themselves .

I had the idea to use magic shuffles to explain the basis of cryptology in 2016. I presented it during a conference in INSA only for their students [1].
In this article I present the main notions of cryptology as message representation, encrypt function and decrypt function. I discuss about the integrity of the cryptology. In fact, these encrypt/decrypt method is based on the secret of algorithm. We know that this method can no more use for real application. What it is explained can be teach either with a top-bottom method or with a bottom-top method as project pedagogy. All the figures come from Scilab programs.

To be understable by students, I use playing cards and magic shuffles !

- *the message is represented by playing cards (as Hearts, Spades, Diamonds and Clubs),*
- *the encrypt function is the function which describes the Faro shuffle using in many cards trick,*
- *the decrypt function is not the inverse of the encrypt function but we use a magic property of this shuffle, i.e the idempotency.*

The students know the magic trick secret and like that they are able to "perform" a magic representation for their friends and family. After that, if one (or more !) spectator wants to know the secret, they would be able to explain and so enjoy a certain success amount.
So the students have to work hardly on but they think/feel that it isn't work but game ! Sharing a mathematical / informatics / cryptography notions and demonstrations is not easy but becomes it with this approach. Isn't this the aim of all teaching?
Whatever the students will be able to see the impact that originality and creativity have when com-bined with an interest in a professional area. But it isn't enough without trainings !

Introduction

I am fascinated by Magic (or rather conjuring!) and for many years I have used this way of teaching, both in my physics classes and as higher education teacher trainer.

I present all the notions in this paper, the researchers who have used Magic to teach and/or to research and finally I present my contributions.

The magician aim is to hide the principles he uses (using sleight of hand, Psychology, Maths, Physics, etc...) by disguising the trick. It would be great that the audience has no way of discovering how it is done thus allowing the Magic to remain.

The teacher can do exactly the opposite: unraveling a Magic trick to highlight the principles used!

Card magic as the vector of research and teaching

From 1886 till 1896, Poincaré occupied the chair of "probability Calculus" in the Paris university 'La Sorbonne'. He wrote a work named 'probability calculus' [2,3] which was printed for the first time in 1896. In the second edition, he brings very fundamental new reflections on the groups and the hypercomplex systems and on the ergodic theory. He is brought to these innovations by the study of the card shuffling and liquids mixing. The problems of card shuffling and liquid diffusion studied by Poincaré are application cases of the

Citation: Schott P. Initiation Of Cryptology Thanks To A Scilab™ Project Using Perfect Magic Shuffles. Japan J Res. 2023;4(5):1-7.

ergodic theory which is in the center of the probability leveling phenomenon: if the deck was shuffled for a long time, all the possible permutations have the same probability.

Both principles of Gilbreath [4-6] are fascinating principles, allowing to do extraordinary card tricks!

Some Mathematicians such as M. Gardner [7-9], P. Diaconis [10-12] or C. Mulcahy [13-15], some computer specialists - as G. Huet [16] one of creator of COQ language which allows to make automatic mathematical proof - studied the principle (and they are not the only ones !).

We shall not present this principle here but it is necessary to know that it is based on a commonly used card shuffles on both sides of the Atlantic Ocean: the American shuffle named riffle shuffle too !

The fields I teach with Magic

Naturally, the first project I gave was in optics [17] for my students in university for the engineering program.

I thought that the amazing Gilbreath principle was based on mathematics because it is a self-working trick. That's why I began to think how to teach math with magic from primary school to the higher education [18,19]. Thus, after I have readen an article about shuffles [20], and I wrote with the author a demonstration of Gilbreath's principle [21].

I teached numerical electronics thanks a magic trick [22,23].

I think that all areas can be teached with magic but not all knowledge [24] !

The aim of this paper is to introduce by magic way a part of cryptography notions.

The main important thing for me remains to use my passion for the magic as a teaching vector which also weaves a human bond between the professor and the student.

Summary

Imagine that a secret agent ‘A’ must send an important message to another secret agent ‘B’. This message is: “Japan Journal of Research”.

“The agent A must naturaly encrypt the original message and the agent B must decrypt it ! ”

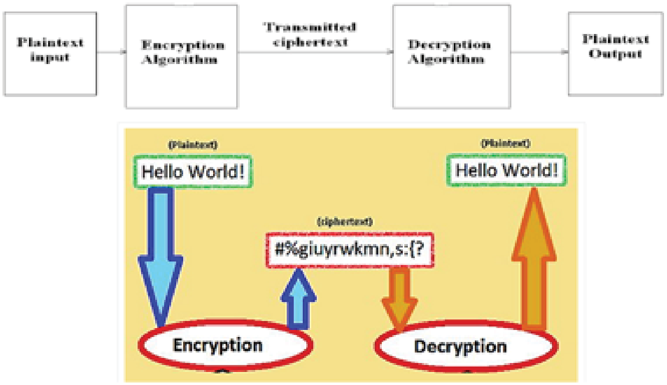

Figure 1. *Basic block diagram of En/Decryption*

I present the main cryptography notions :

- the representation of the message (here with playing cards but normally it is done with binary),
- the encrypt phase of the message by the agent A thanks to an algorithm -which is based on cards shuffles,
- the decrypt phase of the message by the agent B, by the same algorithm -and not with the inverse encrypt function,

The figure 1 represents a simplified block diagram of En/Decryption with an classic example.

Or you can teach with an up-bottom pedagogy (but you have to programming before !) either with a bottom-up pedagogy by giving a project under Scilab or Java for example.

First Step : Letters representation by playing cards and informatics implementation

Letters representation : 26 cards for 26 letters

The aim of the project is to crypt a message constituted by latin alphabetical letters. Let us note that 26 letters are used and 26 is equal to 2*13 (or 2*52/4). Therefore 2 whole card families are necessary to encode all of the letters but only two families!

4 families are usually used in a 52 card deck. One of the 6 possibilities must be chosen. The figure 2 shows the used solution.

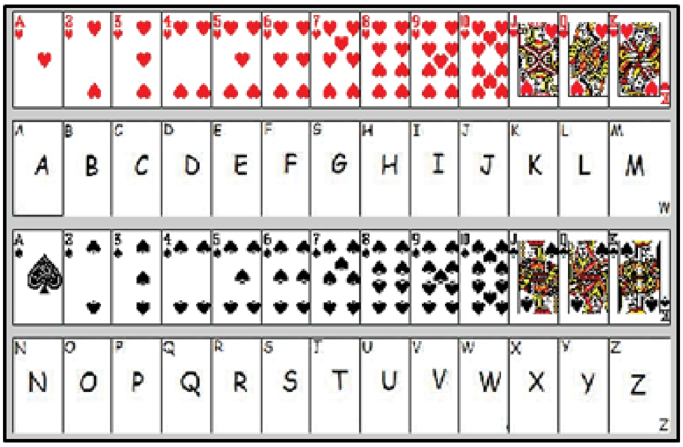

Figure 2*. Letters representation with Heart and Spade.*

Let us take the following message “Japan Journal of Research” as the sending message. The message representation thanks playing cards is shown in figure 3.

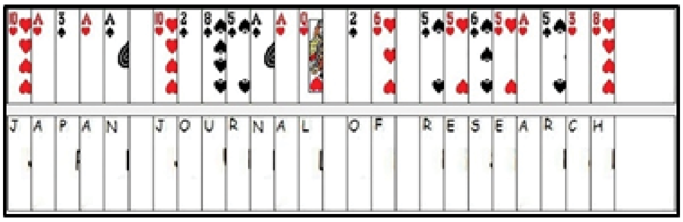

Figure 3*. Letters representation with Heart and Spade.*

Informatics card deck representation

Each playing card could be represented by a number between 1 and N where N is the total card number in the deck. The figure 4 shows the case where N is equal to 52. Therefore each card is numbered from 1 to 52.

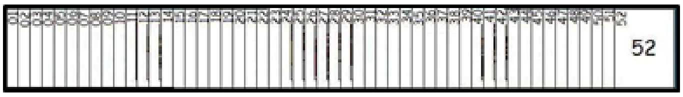

Figure 4. *A numbered card deck from 1 to 52.*

The figure 5 shows one of thousand possibility of informatics representation of a 52 playing card deck. For example, the 10 of Diamond is represented by the number 30, the ace of Heart by the number 1 and the ace of spade by the number 52.

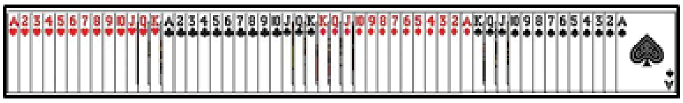

Figure 5. *A New card deck with the bicycle*^{TM} *order.*

An another way to represent the cards could be to give a number between 1 (for the Ace) and 13 (for the King). Therefore the first hundred would be for the Heart, the second hundred for the Spade, the third hundred for the Diamond and the fourth hundred for the Club. So the 10 of Diamond is represented by the number 310.

The Faro shuffle : definition and usefull propertie for a cryptography process

Returning to our example described above : sending the following message " Japan Journal of Research".

The Faro shuffle has many properties that have been widely studied as much by magicians and mathematicians. I made a rather informatic study described in [19]. In [20], the study is discussed under a mathematical formulation showed in annex A.

I present a mathematical modelisation of the FARO shuffle.

The IN-Faro and OUT-Faro shuffle definition

The card deck -numbered from the bottom to the up- in the order 1, 2, 3, …, 2n is cut in the middle. The first half subdeck is numbered from 1 to n and the second is numbered from (n+1) to 2n. A new 2n card deck is created by taking alternately the first card of each subdeck.

Initially, the 52 card deck is in the following order (presented on figure 4). Each card is numbered from1 to 52:

By cutting the deck between the cards 26 and 27 we obtain 2 subdeck (presented on figure 6). Its modelisation is shown in figure 7.

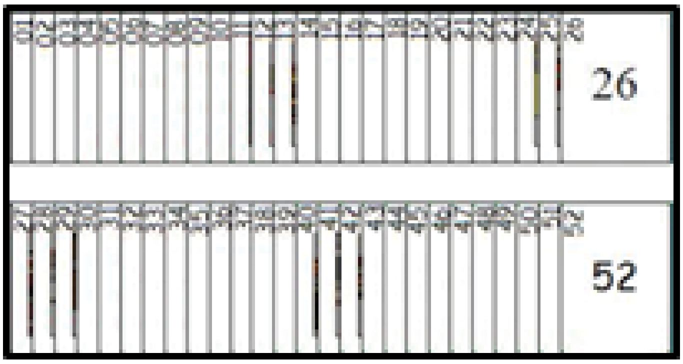

Figure 6. *A New card deck with the bicycle*^{TM} *order.*

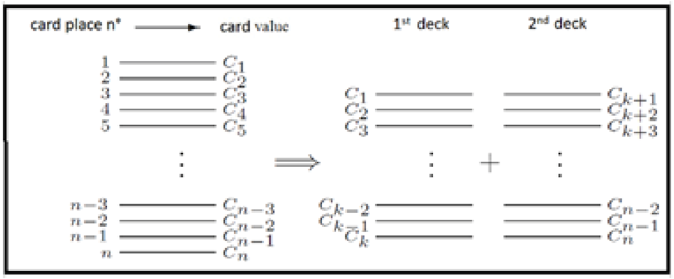

Figure 7. *Two subdecks from a numbered n card deck – modelisation.*

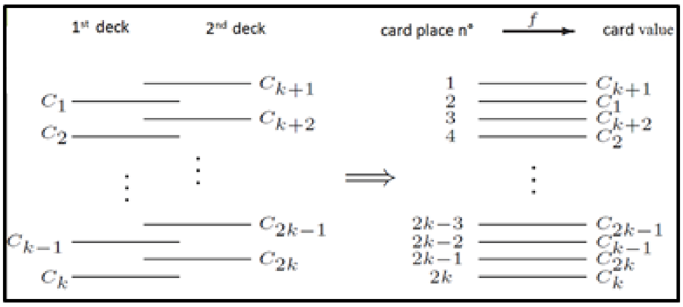

Figure 8. *In-shuffle : permutation f.*

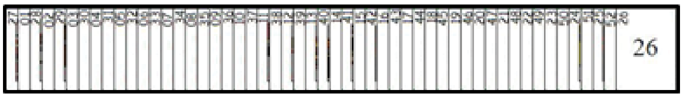

Figure 9. *A numbered card deck from 1 to 52 deck after one IN-Faro shuffle.*

The IN-Faro (in-shuffle)

If the first card (from the bottom) is taken of the second subdeck (in-shuffle), the new 2n card deck is numbered as follows: n+1, 1, n+2, 2, n+3, 3, … , 2n-1, n-1, 2n, n -as presented on figures 8 and 9.

Let's say that the card which has the ith position will be at the jth position after a IN-Faro. There is a bijection noted f defined as follows :

$$f(i) = E\left[\frac{i+1}{2}\right] + n\,\varepsilon(i)$$

where ε(i)=0 if i is even and ε(i)=1 if i is odd. The reciprocal permutation is given in appendix A.

The OUT-Faro (the out-shuffle)

If the first card (from the bottom) is taken of the first subdeck (out-shuffle), the new 2n card deck is numbered as follows : 1, n+1, 2, n+2, 3, n+3, … , n-1, 2n-1, n, 2n -as presented on figures 10 and 11.

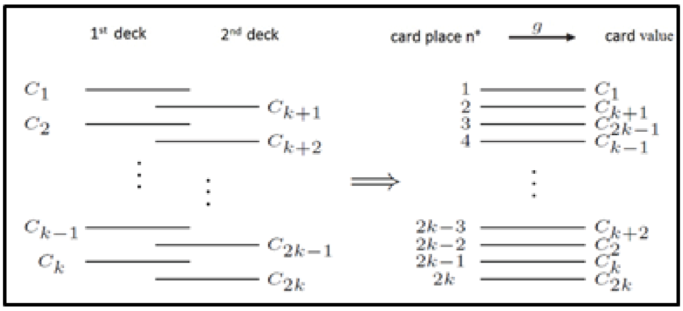

Figure 10. *Out-shuffle : permutation g.*

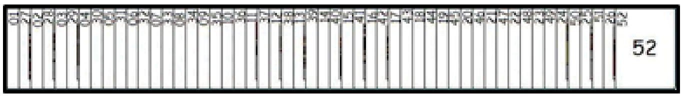

Figure 11. *A numbered card deck from 1 to 52 deck after one OUT-Faro shuffle.*

Let's say that the card which has the i^th^ position will be at the j^th^ position after a OUT-Faro. There is a bijection noted g defined as follows :

$$g(i) = \begin{cases} \dfrac{i}{2} + n \\ \dfrac{i+1}{2} \end{cases}$$

The reciprocal permutation is given in appendix B.

An interesting property of the Faro shuffle: its idempotency

Considering a deck of n=2p cards. After a Faro shuffle we determine if the card's order is the same as before. If it is not, we repeat the process until it's done.

We say that the function φ is N-times idempotent if :

$$\text{Id} = \varphi \text{ o } \varphi \text{ o } \dots \text{ o } \varphi = \gamma(N) \qquad (3)$$

Figure 12 shows the number of necessary shuffles needed in order to a card deck return to its initial position versus the number of card deck.

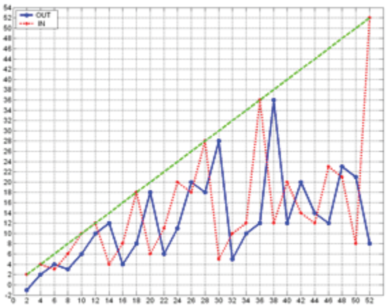

Figure 12. Number of successive shuffles needed in order to a card deck returns to its initial position versus the number of card in the deck.

It is interesting to note that:

- for n=2k, the number of OUT-Faro shuffle is exactly k,
- the number of IN-Faro shuffle for a deck of n cards is the same as the OUT-Faro shuffle for a deck of (n+2) cards,
- the number of Faro shuffle to do is never greater than the number of cards in the deck.

In step 2, I present the message encryption phases of the message done by agent A. In step 3, I present the agent B's decryption phase.

Step 2 : Encrypting phase made by the secret agent A

The message contains 25 characters. But to do a Faro shuffle, you need an even number of cards. That's why we add a space at the end of the message. So the message to encrypt contain now 26 characters, as shown on figure 3.

Thanks to figure 12, 18 IN-Faro (or 20 OUT-Faro) are needed in order to the deck returns to its initial order. Let's take the fewest number of shuffle, i.e : 18 IN-Faro. Mathematically, it is written so :

$$\text{Id} = \text{f o f o f o f o f o} \dots \text{o f} = f^{(18)} \qquad (4)$$

To get the number of Faro to do in order to encrypt the message, the total number of Faro N has to be divided by two. If the result is not an integer, only the integer part of the division is used : in this case, the deck is shuffling 9 times to encrypt the initial message. The following figures (13 and 14) are respectively the result of the first and the 9^th^ IN-Faro shuffles.

The final shuffled deck is given by the secret agent A to the secret agent B.

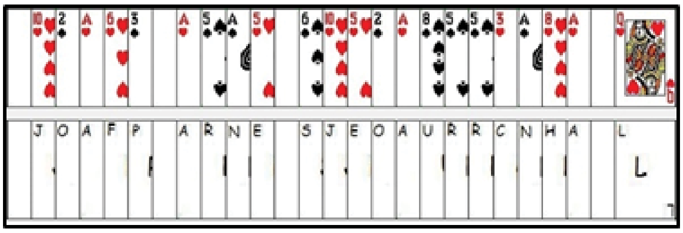

Figure 13. *Encrypt message after one IN-Faro.*

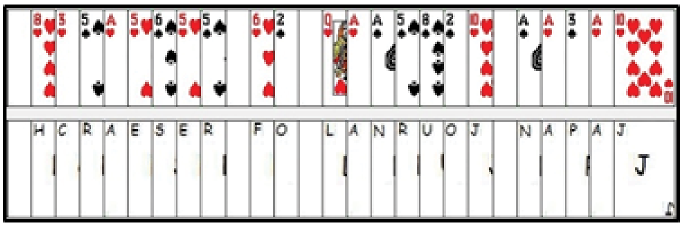

Figure 14. *Encrypt message after nine IN-Faro : the sending message to the secret agent B.*

Mathematically the encrypt function can be written so :

$$E = \text{f o f o f o f o f o f o f o f o f} = f^{(9)} \qquad (5)$$

Step 3 : Decrypting phase made by the secret agent B

The secret agent B counts the number of cards which gives him information on the total number of Faro to perform (and if it is IN or OUT-Faro!). Therefore he knows how many shuffles he has to do to decrypt the message (here 9 IN-Faro has to be done). The following figures (15, 16 and 3) show the first, the 8th and the 9th IN-Faro shuffle from the encrypt message shown on figure 14.

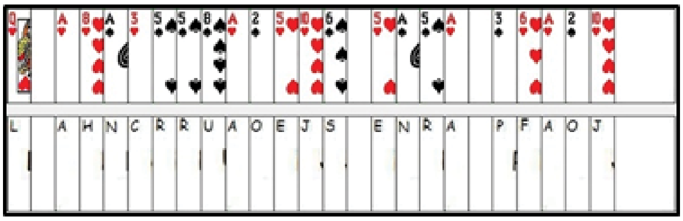

Figure 15. *Decrypt message after one (ten) IN-Faro..*

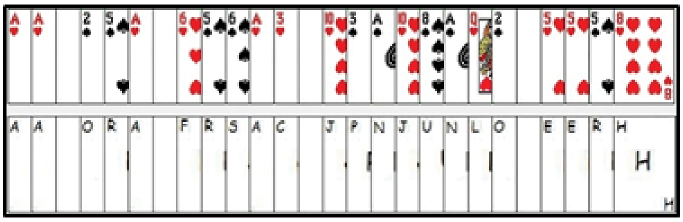

Figure 16. *Decrypt message after eight (seventeen) IN-Faro.*

Mathematically the decrypt function can be written so :

$$D = f \circ f \circ f \circ f \circ f \circ f \circ f \circ f \circ f = f^{(9)} \qquad (6)$$

Synthesis, conclusion, going further and prospects

Before I used magic to teach many different fields of knowledge : math, optics, electronics. This time, it is to introduce many elements of the cryptology chain.

I think that the objectives are reached and different function representing different shuffles can be used too.

But a discussion about security of this kind of encrypt function must be done.

Synthesis

We have described :

- the message to send is represented by playing cards (as Hearts, Spades, Diamonds and Clubs),
- the encrypt function is based on the function which describes the Faro shuffle using in many cards trick,
- the decrypt function is not the inverse of the encrypt function but we use a magic property of this shuffle, i.e the idempotency.

Table 1. *Parallel of the reality and my method in the cryptology chain*

	In reality	With the magic method
Message representation	Binary with ASCII code	Playing cards
Encrypt function E	Many algo-rithms exist	The function representing a real card shuffle (f or g) is used N times depending the message length.
Decrypt function D	Usually D=E-1	The same function (f or g) but the iteration number M can be changed

Conclusion : the security of this encrypt function

Nowdays the algorithm based on card shuffle cannot be used as a encrypt function because it is unsecure!

In fact, if the cryptography process is based on the secret of the algorithm so one day somebody will discover the algorithm!

Going further and prospects

To secure this cryptography chain, a private key can be introduced. So the figure 1 becomes the figure 17:

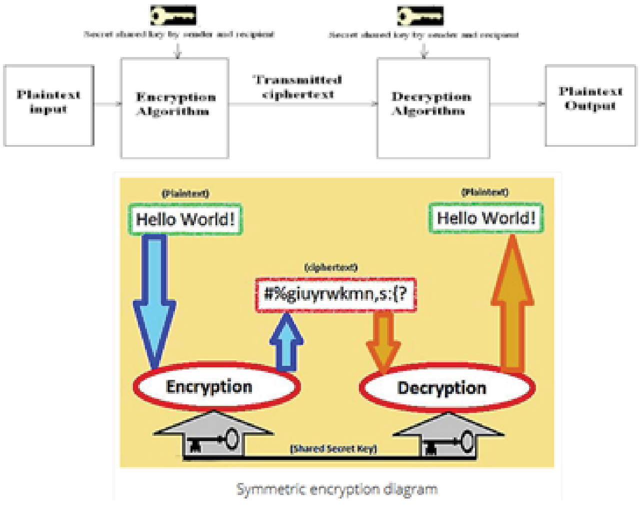

Figure 17. *Basic block diagram of En/Decryption with private key : symmetric encryption diagram.*

To be sure that the received message is the well encryption message, the Hamming code can be used too.

Appendix A : The mathematical formulation of the IN-Faro shuffle

If the first card (from the bottom) is taken of the second subdeck (in-shuffle), the new 2n card deck is numbered as follows: n+1, 1, n+2, 2, n+3, 3, … , 2n-1, n-1, 2n, n -as presented on figure 8.

One relation exists between serial numbers before and after the shuffle: after shuffling the first card is the card initially numbered (n+1), the second's is the card initially numbered 1, the third's is the card initially numbered (n+2), the fourth's is the card initially numbered 2, and so on.

So the ith card is the card initially numbered (i/2) if i is even and ((i+1)/2+n) if i is odd. This relation defines a permutation named f of integers 1, 2, 3, … , 2n that gives the new card place of the initially ith card after shuffling :

$$f(i) = \begin{cases} \dfrac{i}{2} \\ \dfrac{i+1}{2} + n \end{cases} \qquad (7)$$

This equation can be written as follows, where ε(i)=0 if i is even and ε(i)=1 if i is odd:

$$f(i) = E\left[\frac{i+1}{2}\right] + n\varepsilon(i) \qquad (8)$$

The reciprocal permutation is simpler to write:

$$\mathrm{f}^{-1}(\mathrm{j}) = \begin{cases} 2\mathrm{j} & \text{if } 1 \le \mathrm{j} \le \mathrm{n} \\ 2\mathrm{j}\text{-}2\mathrm{n}\text{-}1 & \text{if } \mathrm{n}+1 \le \mathrm{j} \le 2\mathrm{n} \end{cases} \qquad (9)$$

We note the definition of the arithmetic congruence: a=b[n] means 'a-b is divisible by n'. This notation with congruence is very useful to determine the f-period.

$$\mathrm{f}^{-1}(\mathrm{j}) \equiv 2\mathrm{j}\left[2\mathrm{n}+1\right] \qquad (10)$$

This last relation indicates that a card initially numbered j between 1 (resp. n+1) and n (resp. 2n) will be, after shuffling, at the place numbered 2j (resp. 2j-2n-1).

For example, the card numbered 1 will be at the place numbered 2, the card numbered 4 will be at the place 8,   , the card numbered n will be at the place 2n, the card numbered (n+1) will be at the place 1, the card numbered (n+2) will be at the place 3, and so on as presented on figure 8.

It is useful to translate the card numbering in order to obtain card position between 0 and (2n-1). So the new permutation f, named , becomes so :

$$\mathrm{f}^{\sim}(\mathrm{i}) = \begin{cases} \dfrac{\mathrm{i}}{2} + \mathrm{n} & \text{if i is even} \\ \dfrac{\mathrm{i}-1}{2} & \text{if i is odd} \end{cases} \qquad (11)$$

The new reciprocal is $\tilde{f}^{-1}$ so defined:

$$\mathrm{f}^{\sim -1}(\mathrm{j}) = \begin{cases} 2\mathrm{j}+1 & \text{if } 0 \le \mathrm{j} \le \mathrm{n}\text{-}1 \\ 2\mathrm{j}\text{-}2\mathrm{n} & \text{if } \mathrm{n} \le \mathrm{j} \le 2\mathrm{n}\text{-}1 \end{cases} \qquad (12)$$

Thanks to the introduced permutations, it is allowed to determine explicitly the in-shuffle period for an n=2p-1 and n=2p-1 -1 card deck.

Appendix B : The mathematical formulation of the OUT-Faro shuffle

If the first card (from the bottom) is taken of the first subdeck (out-shuffle), the new 2n card deck is numbered as follows : 1,n+1,2,n+2,3,n+3, … ,n-1,2n-1, n, 2n -as presented on figure 10.

This process defines then the permutation g of integers 1,2,3, … , 2n presented below:

$$\mathrm{g}(\mathrm{i}) = \begin{cases} \dfrac{\mathrm{i}}{2} + \mathrm{n} \\ \dfrac{\mathrm{i}+1}{2} \end{cases} \qquad (13)$$

its reciprocal permutation is :

$$\mathrm{g}^{-1}(\mathrm{j}) = \begin{cases} 2\mathrm{j}\text{ - }1 & \text{if } 1 \le \mathrm{j} \le \mathrm{n} \\ 2\mathrm{j}\text{-}2\mathrm{n} & \text{if } \mathrm{n}+1 \le \mathrm{j} \le 2\mathrm{n} \end{cases} \qquad (14)$$

The only cards, whose positions are unchanged by the permutation are the first and the last ones i.e. g(1)=1 and g(2n)=2n.

It is useful to translate the card numbering in order to obtain card position between 0 and (2n-1). So the new permutation f, named $\tilde{\mathrm{g}}^{-1}$, becomes so:

$$\tilde{\mathrm{g}}^{-1}(\mathrm{i}) = \begin{cases} \dfrac{\mathrm{i}}{2} & \text{if i is even} \\ \dfrac{\mathrm{i}-1}{2} + \mathrm{n} & \text{if i is odd} \end{cases} \qquad (15)$$

its reciprocal permutation is :

$$\tilde{\mathrm{g}}^{-1}(\mathrm{j}) = \begin{cases} 2\mathrm{j} & \text{if } 0 \le \mathrm{j} \le \mathrm{n}\text{-}1 \\ 2\mathrm{j}\text{-}2\mathrm{n}+1 & \text{if } \mathrm{n} \le \mathrm{j} \le 2\mathrm{n}\text{-}1 \end{cases} \qquad (16)$$

Let us note in particular the congruence

$$\tilde{\mathrm{g}}^{-1}(\mathrm{j}) \equiv 2\mathrm{j}\left[2\mathrm{n}-1\right] \qquad (17)$$

If the first and the last card are gone away (so the numeration set is now {1, … , 2n-2}) then a new permutation is created. It's properties are the same as the in-shuffle permutation with only (2n-2) cards.

So the 2n card deck out-shuffled is the same as the (2n-2) card deck in-shuffled (by ejecting the first and last card of the 2n card deck!).

Acknowledgements

This paper could not have been written without the encouragements of Bernard SCHOTT, the invaluable help of Anne SERRIE, Claire LEROUX, the head of ARNUM and Lionel TROJMAN, the head of ISEP Research Department.

References

1. Lachal A, Schott P. Les Mathématiques au service de la Magie ? ou La Magie au service des Mathématiques ?. Conference at INSA Lyon (France). 4 April 2016.
2. Poincaré H. Calcul des probabilités. Rédaction de A. Quiquet.

Deuxième édition, revue et augmentée par l'auteur, Gauthier-Villars, Paris. 1912.

3. Sheynin OB. H. Poincaré's work on probability. Archive for History of Exact Sciences. 1991; 42(2): 137–171.
4. Gilbreath NL. Magnetic colors. The Linking Ring. 1958;38(5):60.
5. Gilbreath NL. Second Gilbreath Principle. Linking Ring. 1966.
6. Gilbreath NL. Magic for an Audience. series of 3 articles in Genii. 1989; 52(9-10-11).
7. Magid A. Notices. American Mathematical Society. 2005.
8. Gardner M. Mathematics, Magic and Mystery. Dover. 1958.
9. Gardner M. Martin Gardner's mathematical games : the entire collection of his scientific American columns. Mathematical Association of America. 2005.
10. Diaconis P. From Shuffling Cards to Walking Around the Building. An Introduction to Markov Chain Theory. Proc. Int. Congress, Berlin, Volume I, Plenary Lectures. 1998;187-204.
11. Diaconis P. Mathematical Developments from the Analysis of Riffle-Shuffling. In A. Fuanou, M. Liebeck (eds.) Groups Combinatorics and Geometry, World Scientific, N.J. 2003; pp.73-97.
12. Assaf S, Soundararajan K, Diaconis P. Riffle shuffles of a deck with repeated cards. DMTCS Proceedings, 21st International Conference on Formal Power Series and Algebraic Combinatorics. FPSAC 2009; 89-10.
13. Mulcahy C. Fitch Cheney's Five Card Trick. Maths Horizon. 2003;10(3):10-13.
14. Mulcahy C. Top 5 Reasons to Like Mathematical Card Tricks. Maths Horizon. 2004;11(3):5-7.
15. Mulcahy C. An ESPeriment with Cards. Maths Horizon. 2007;14(3):10-12.
16. Huet G. The Gilbreath trick: A case study in axiomatisation and proof development in the Coq Proof Assistant. Proceedings, Second Workshop on Logical Frameworks, Edinburgh, May 1991.
17. Schott P. The Use of Magic in Optics in Higher Education. Creative Education. 2010;1(1):11-17.
18. Schott P. The use of magic in mathematics: from primary school to higher education. Proceedings of ICERI2009 Conference, Madrid, Spain, pp58-70, 16th-18th Nov. 2009.
19. Schott P. How to introduce the cyclic group and its properties representation with Matlab ? Thanks to Magic using the perfect Faro shuffle. Creative Education. 2011;2(1):27-40.
20. Lachal A. Quelques mélanges parfaits de cartes. Quadrature. 2010;77:23-29.
21. Lachal A, Schott P. Cartomagie : principes de Gilbreath (III) – Diverses démonstrations. Quadrature. 2013;87:30-37.
22. Schott P. How to teach the combinatory part of digital electronics basis with project pedagogy ? Thanks to a self-working card trick named cyclic number. International Educational Scientific Reasearch Journal. 2016;2(9):40-44.
23. Schott P. How to teach the sequential part of digital electronics basis with project pedagogy ? Thanks to a self-working card trick named cyclic number. International Journal of Educational Technology and Learning. 2017;1(1):06-10.
24. Schott P. Can or should teach everything using magic ? Experiences from across the sciences. ECME. 2015;15:24-26.