



HAL
open science

Mélanges Faros et cryptographie (exposé didactique - INSA LYON)

Aimé Lachal

► **To cite this version:**

Aimé Lachal. Mélanges Faros et cryptographie (exposé didactique - INSA LYON). École d'ingénieur. France. 2022. hal-04451783v1

HAL Id: hal-04451783

<https://hal.science/hal-04451783v1>

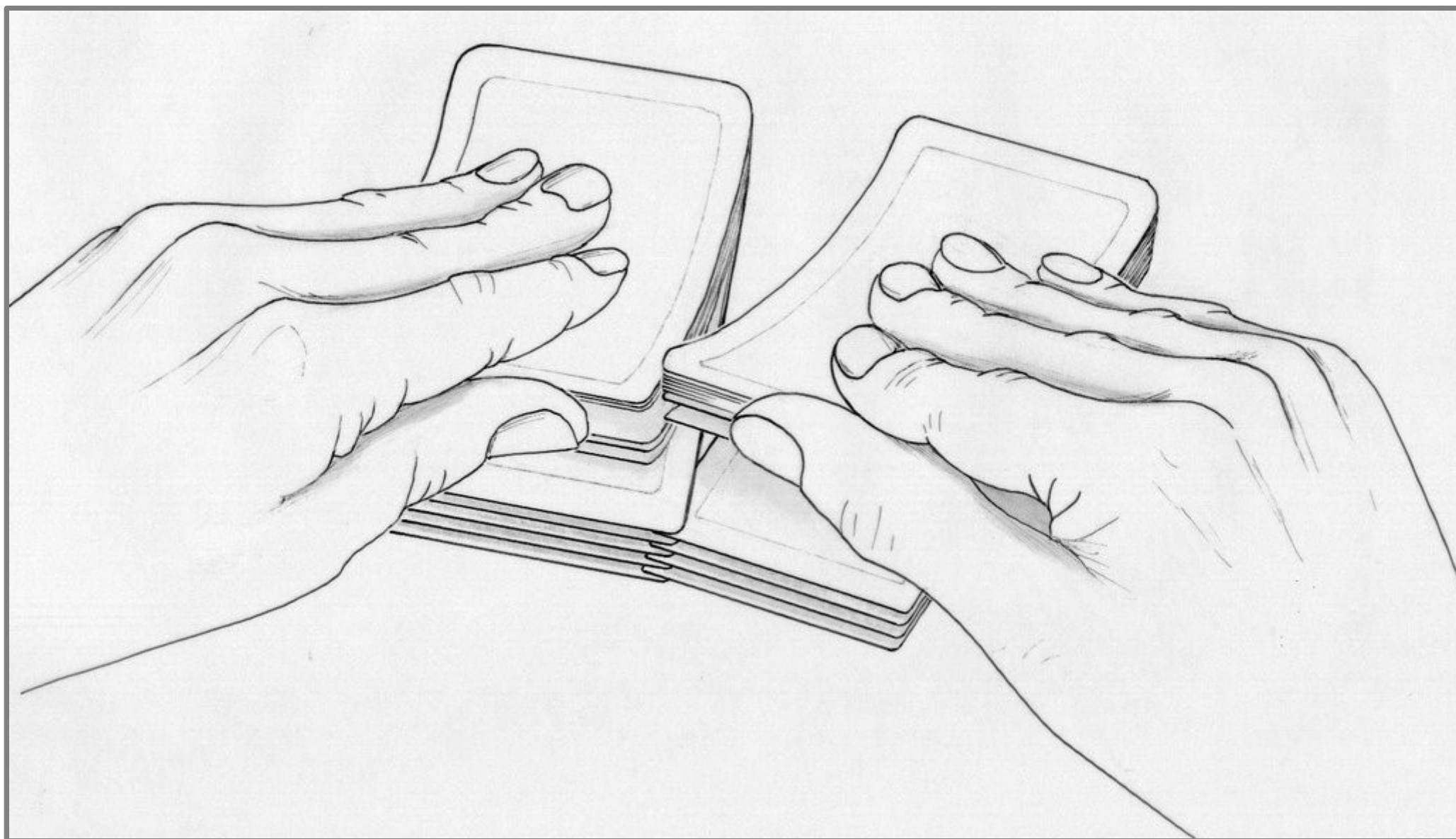
Submitted on 12 Feb 2024 (v1), last revised 29 Mar 2024 (v2)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Mélanges Faros et cryptographie

« Riffle shuffle »



« Riffle shuffle »



I

N

S

A

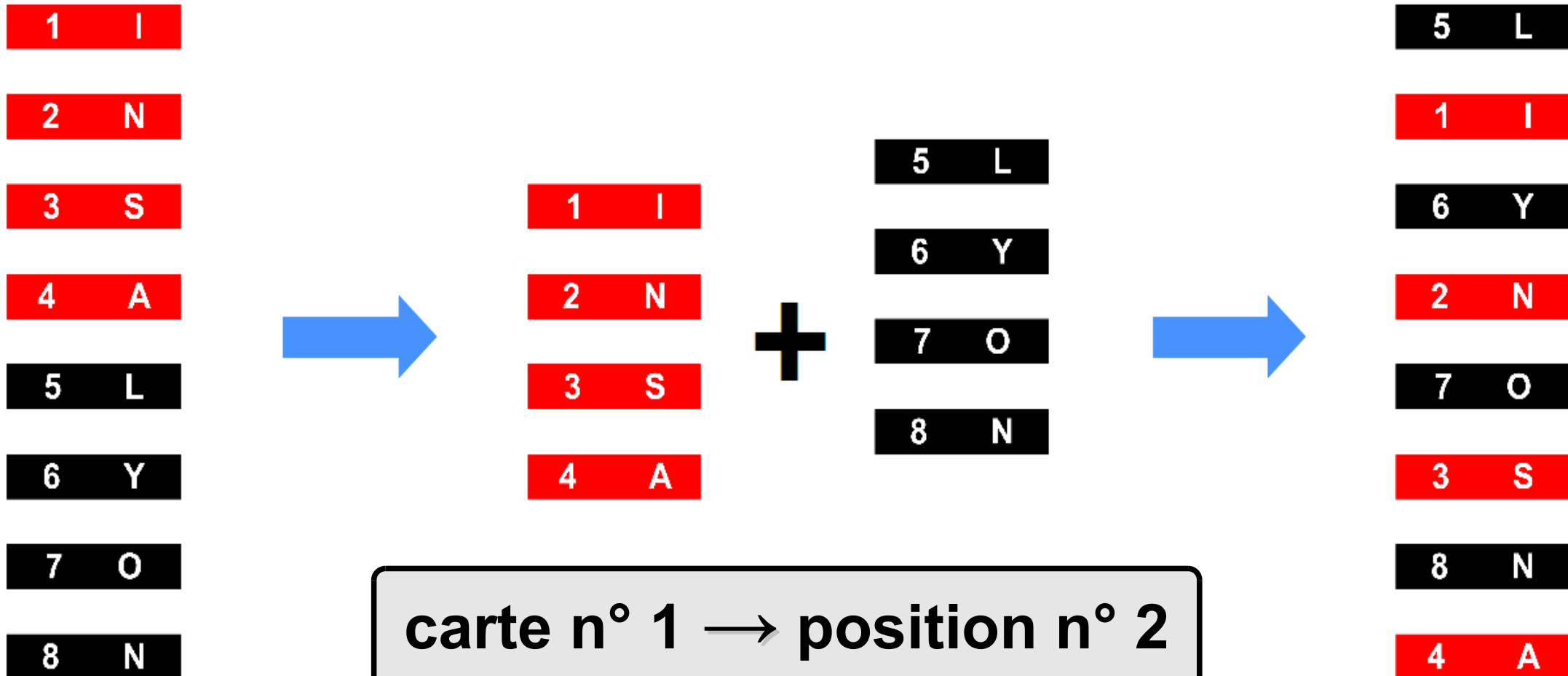
L

Y

O

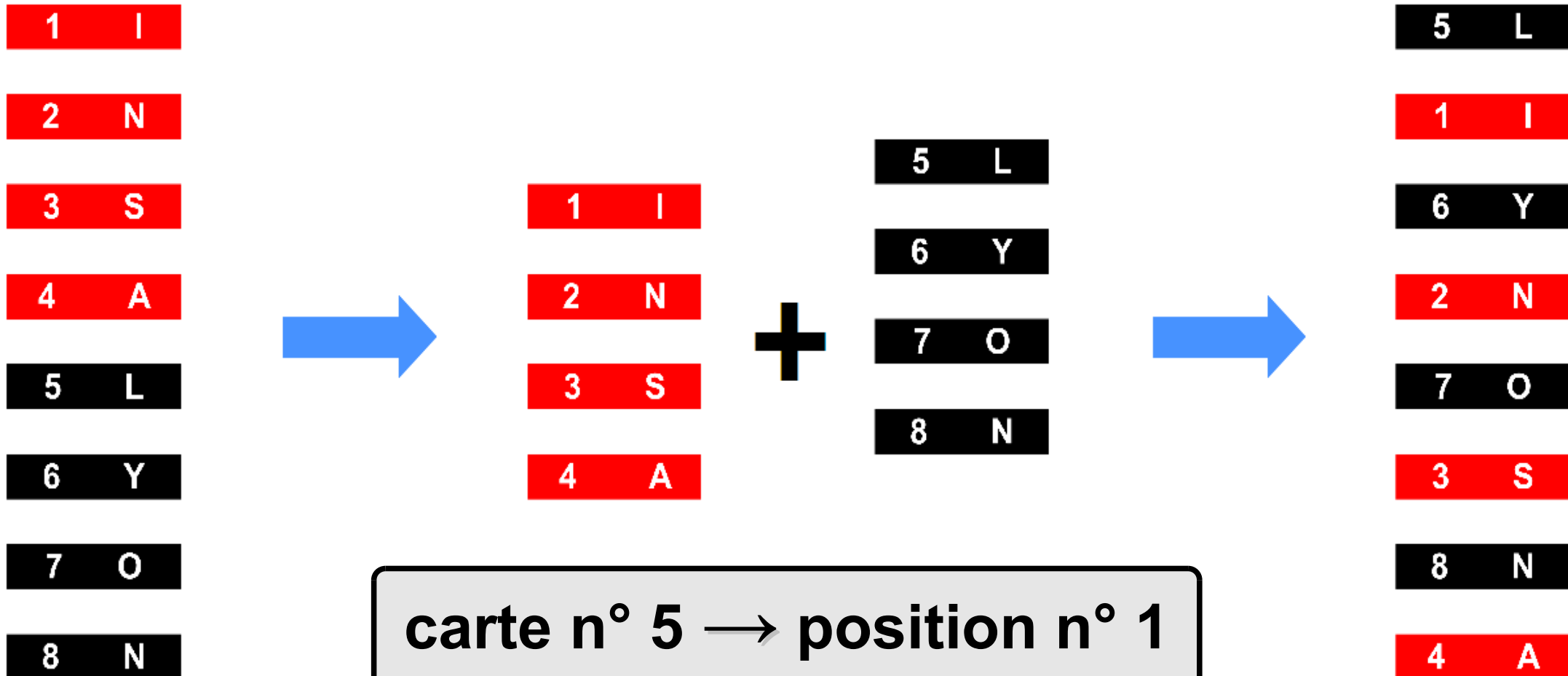
N

1^{er} mélange



carte n° 1 → position n° 2
carte n° 2 → position n° 4
carte n° 3 → position n° 6
carte n° 4 → position n° 8

1^{er} mélange



carte n° 5 → position n° 1
carte n° 6 → position n° 3
carte n° 7 → position n° 5
carte n° 8 → position n° 7

Modélisation : une permutation

$$f: \{1, 2, 3, 4, 5, 6, 7, 8\} \rightarrow \{1, 2, 3, 4, 5, 6, 7, 8\}$$

i : position *avant* mélange $\leftrightarrow j = f(i)$: position *après* mélange

$$\begin{cases} f(1) = 2 \\ f(2) = 4 \\ f(3) = 6 \\ f(4) = 8 \end{cases} \quad \begin{cases} f(5) = 1 \\ f(6) = 3 \\ f(7) = 5 \\ f(8) = 7 \end{cases}$$

$$f(i) = \begin{cases} 2i & \text{si } i \leq 4 \\ 2i - 9 & \text{si } i \geq 5 \end{cases}$$

Modélisation : une permutation

$$f: \{1, 2, 3, 4, 5, 6, 7, 8\} \rightarrow \{1, 2, 3, 4, 5, 6, 7, 8\}$$

i : position *avant* mélange $\leftrightarrow j = f(i)$: position *après* mélange

$$\left\{ \begin{array}{l} f(1) = 2 \\ f(2) = 4 \\ f(3) = 6 \\ f(4) = 8 \end{array} \right. \quad \left\{ \begin{array}{l} f(5) = 1 \equiv 10 \pmod{9} \\ f(6) = 3 \equiv 12 \pmod{9} \\ f(7) = 5 \equiv 14 \pmod{9} \\ f(8) = 7 \equiv 16 \pmod{9} \end{array} \right.$$

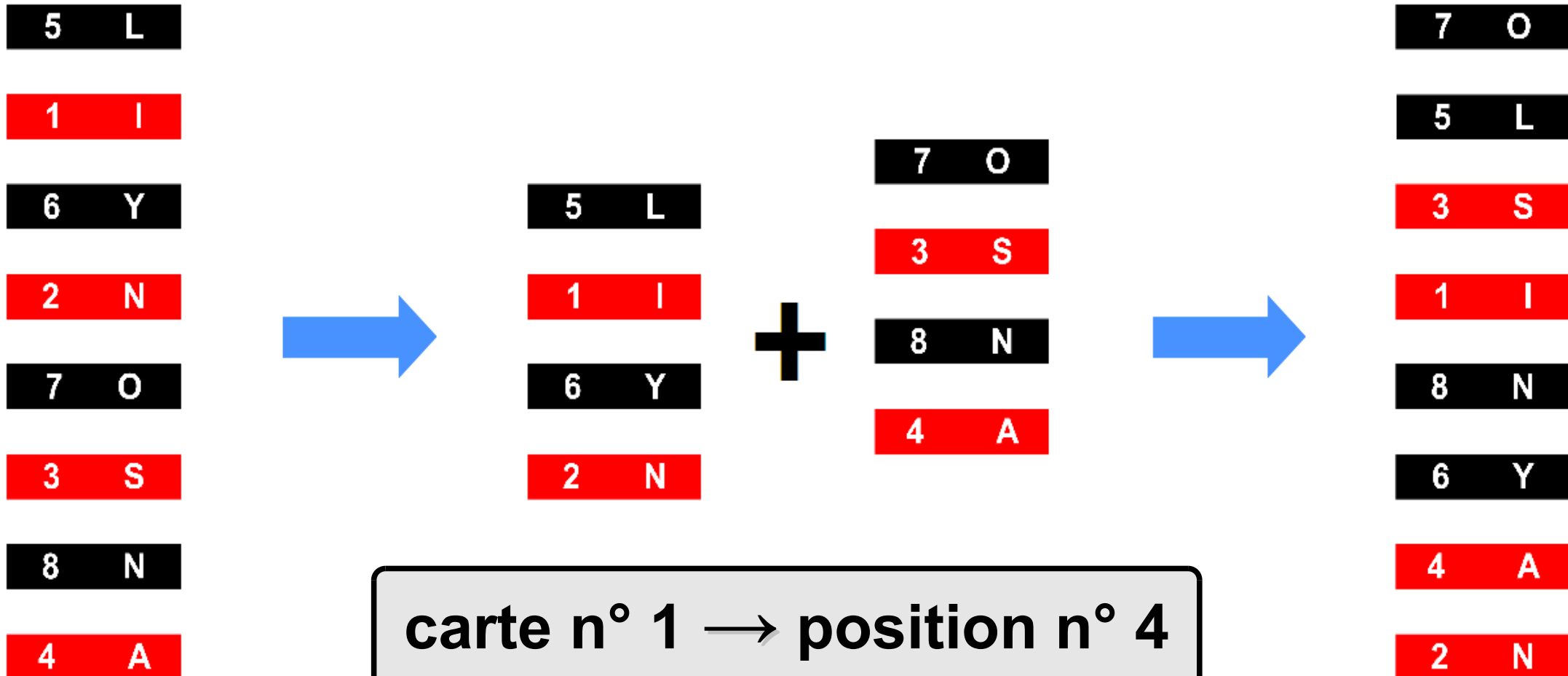
$$f(i) = \left\{ \begin{array}{ll} 2i & \text{si } i \leq 4 \\ 2i - 9 & \text{si } i \geq 5 \end{array} \right\} \equiv 2i \pmod{9}$$

Modélisation : réciproque

$$\left\{ \begin{array}{l} f(5) = 1 \\ f(1) = 2 \\ f(6) = 3 \\ f(2) = 4 \end{array} \right. \left\{ \begin{array}{l} f(7) = 5 \\ f(3) = 6 \\ f(8) = 7 \\ f(4) = 8 \end{array} \right. \xrightarrow{\text{blue arrow}} \left\{ \begin{array}{l} f^{-1}(1) = 5 \\ f^{-1}(2) = 1 \\ f^{-1}(3) = 6 \\ f^{-1}(4) = 2 \end{array} \right. \left\{ \begin{array}{l} f^{-1}(5) = 7 \\ f^{-1}(6) = 3 \\ f^{-1}(7) = 8 \\ f^{-1}(8) = 4 \end{array} \right.$$

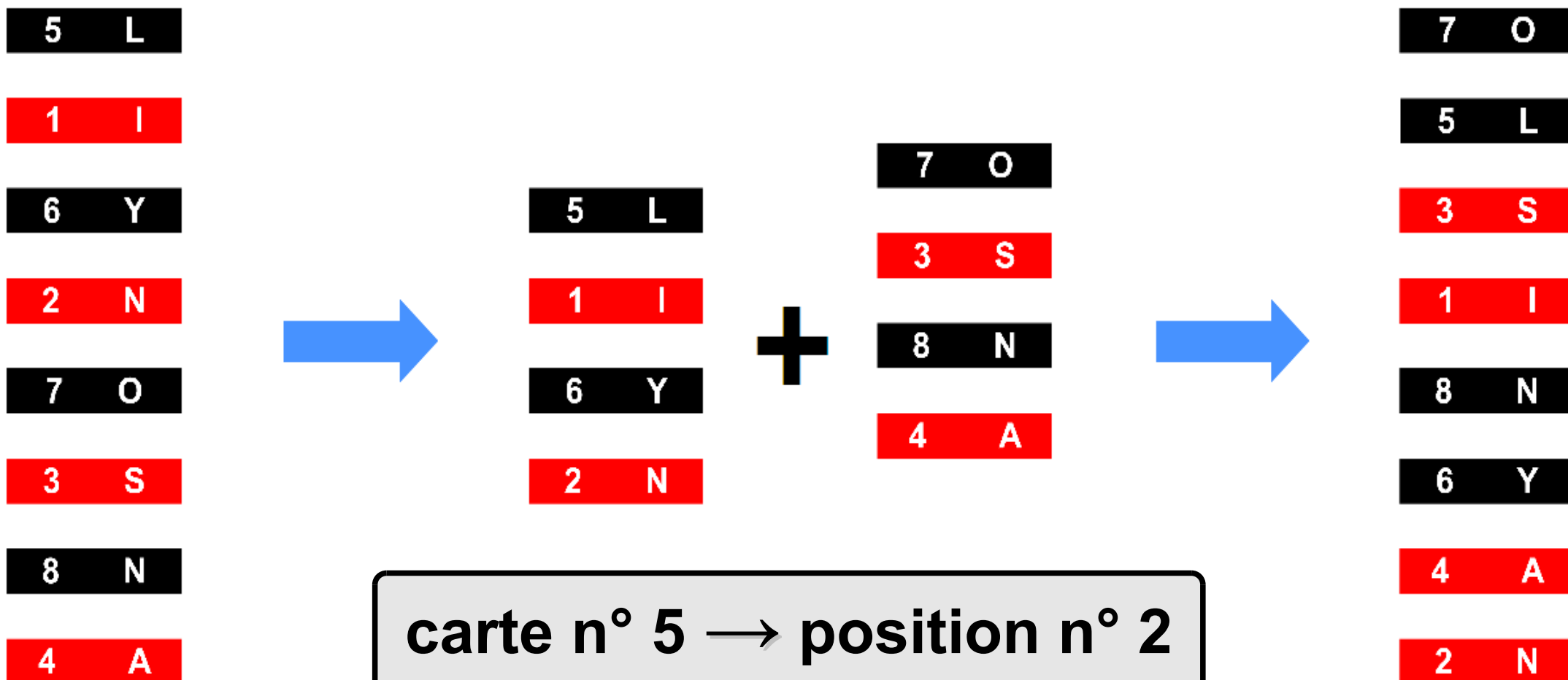
$$f^{-1}(j) = \left\{ \begin{array}{ll} j/2 & \text{si } j \text{ est pair} \\ (j+9)/2 & \text{si } j \text{ est impair} \end{array} \right.$$

2^e mélange



carte n° 1 → position n° 4
carte n° 2 → position n° 8
carte n° 3 → position n° 3
carte n° 4 → position n° 7

2^e mélange



carte n° 5 → position n° 2
carte n° 6 → position n° 6
carte n° 7 → position n° 1
carte n° 8 → position n° 5

Modélisation : composition

Notation : $f^2 = f \circ f$

$$\begin{cases} f^2(1) = 4 \\ f^2(2) = 8 \\ f^2(3) = 3 \\ f^2(4) = 7 \end{cases}$$

$$\begin{cases} f^2(5) = 2 \\ f^2(6) = 6 \\ f^2(7) = 1 \\ f^2(8) = 5 \end{cases}$$

$$f^2(i) = f(f(i))$$

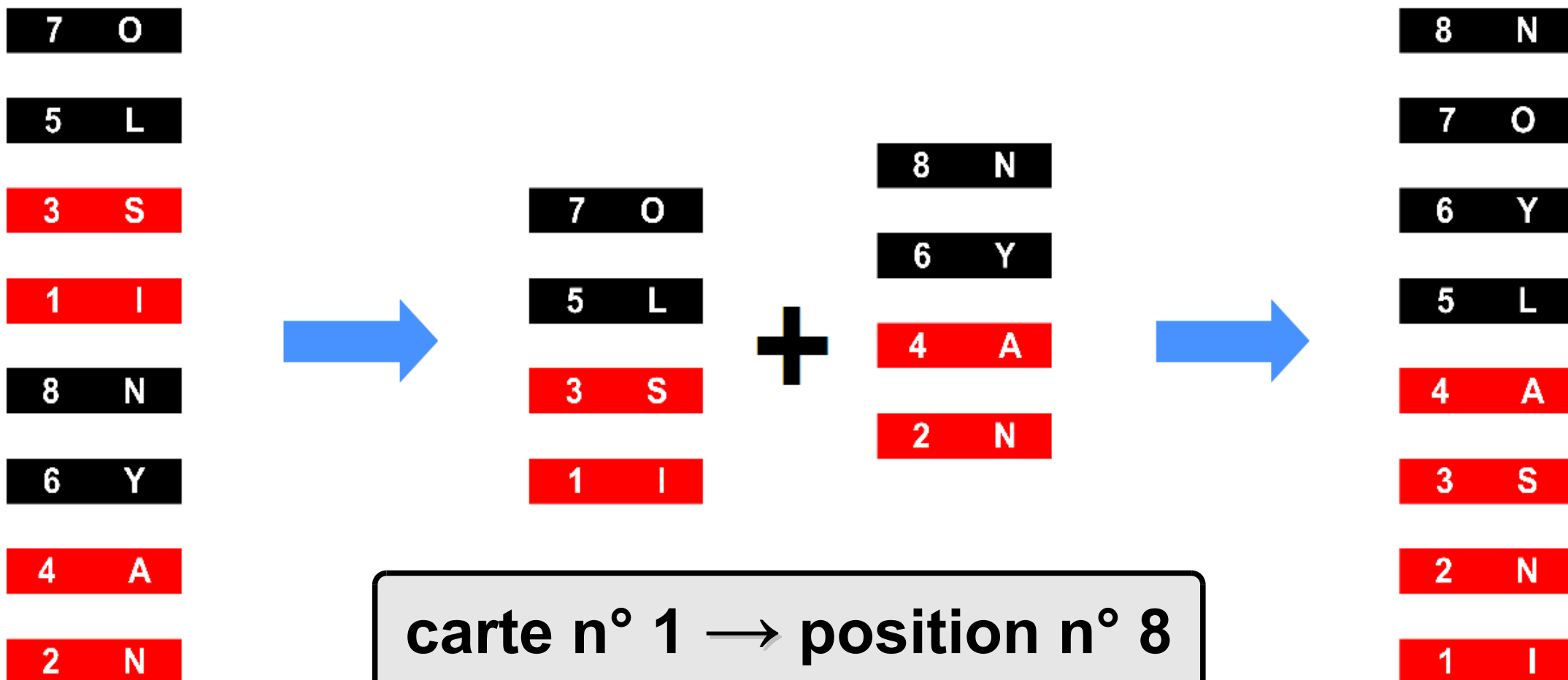
Modélisation : composition

Notation : $f^2 = f \circ f$

$$\left\{ \begin{array}{l} f^2(1) = 4 \equiv 4 [9] \\ f^2(2) = 8 \equiv 8 [9] \\ f^2(3) = 3 \equiv 12 [9] \\ f^2(4) = 7 \equiv 16 [9] \end{array} \right. \quad \left\{ \begin{array}{l} f^2(5) = 2 \equiv 20 [9] \\ f^2(6) = 6 \equiv 24 [9] \\ f^2(7) = 1 \equiv 28 [9] \\ f^2(8) = 5 \equiv 32 [9] \end{array} \right.$$

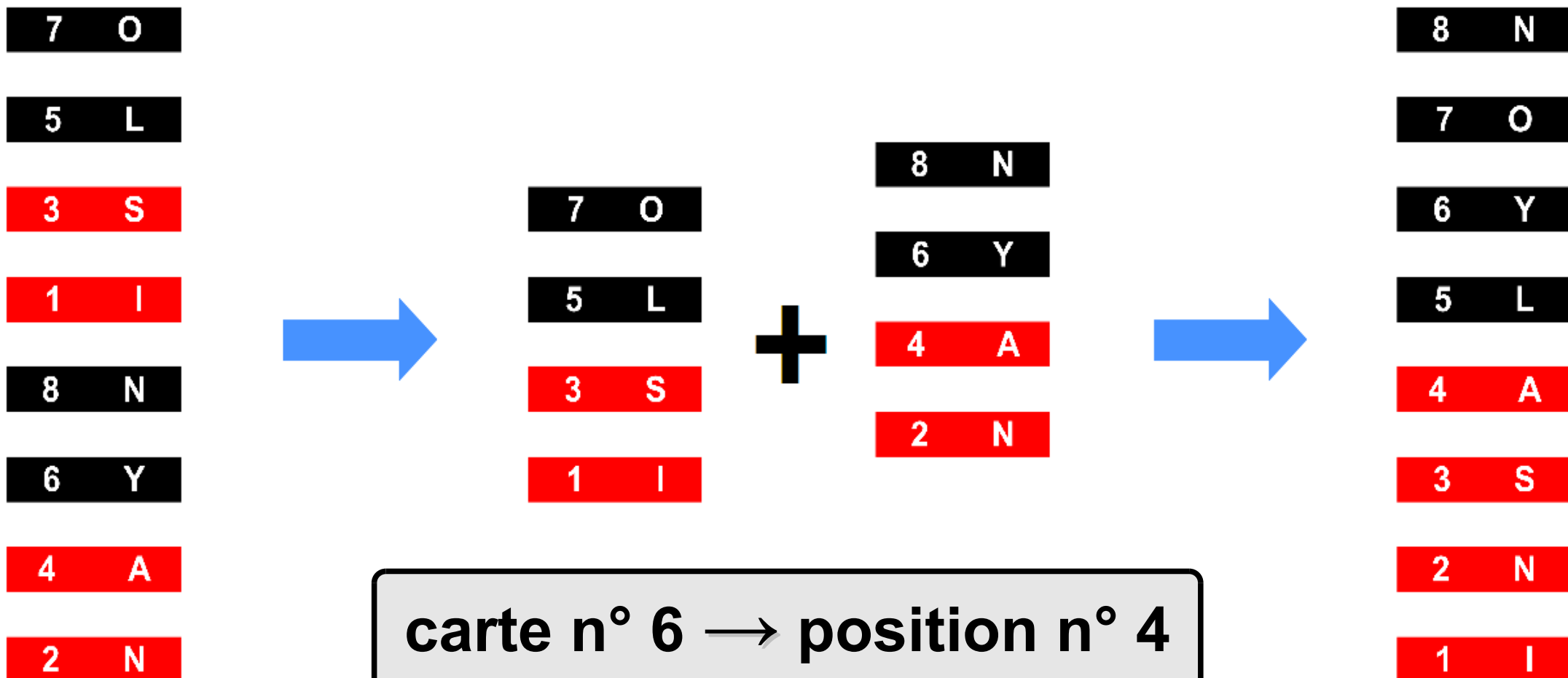
$$f^2(i) = f(f(i)) \equiv 4i \pmod{9}$$

3^e mélange



carte n° 1 → position n° 8
carte n° 2 → position n° 7
carte n° 3 → position n° 6
carte n° 4 → position n° 5

3^e mélange



carte n° 6 → position n° 4
carte n° 7 → position n° 3
carte n° 8 → position n° 2
carte n° 9 → position n° 1

Modélisation : composition

$$\text{Notation : } f^3 = f \circ f \circ f$$

$$\begin{cases} f^3(1) = 8 \\ f^3(2) = 7 \\ f^3(3) = 6 \\ f^3(4) = 5 \end{cases}$$

$$\begin{cases} f^3(5) = 4 \\ f^3(6) = 3 \\ f^3(7) = 2 \\ f^3(8) = 1 \end{cases}$$

$$f^3(i) = f(f(f(i))) = 9 - i$$

Au bout de 3 mélanges, le jeu est inversé...

Modélisation : composition

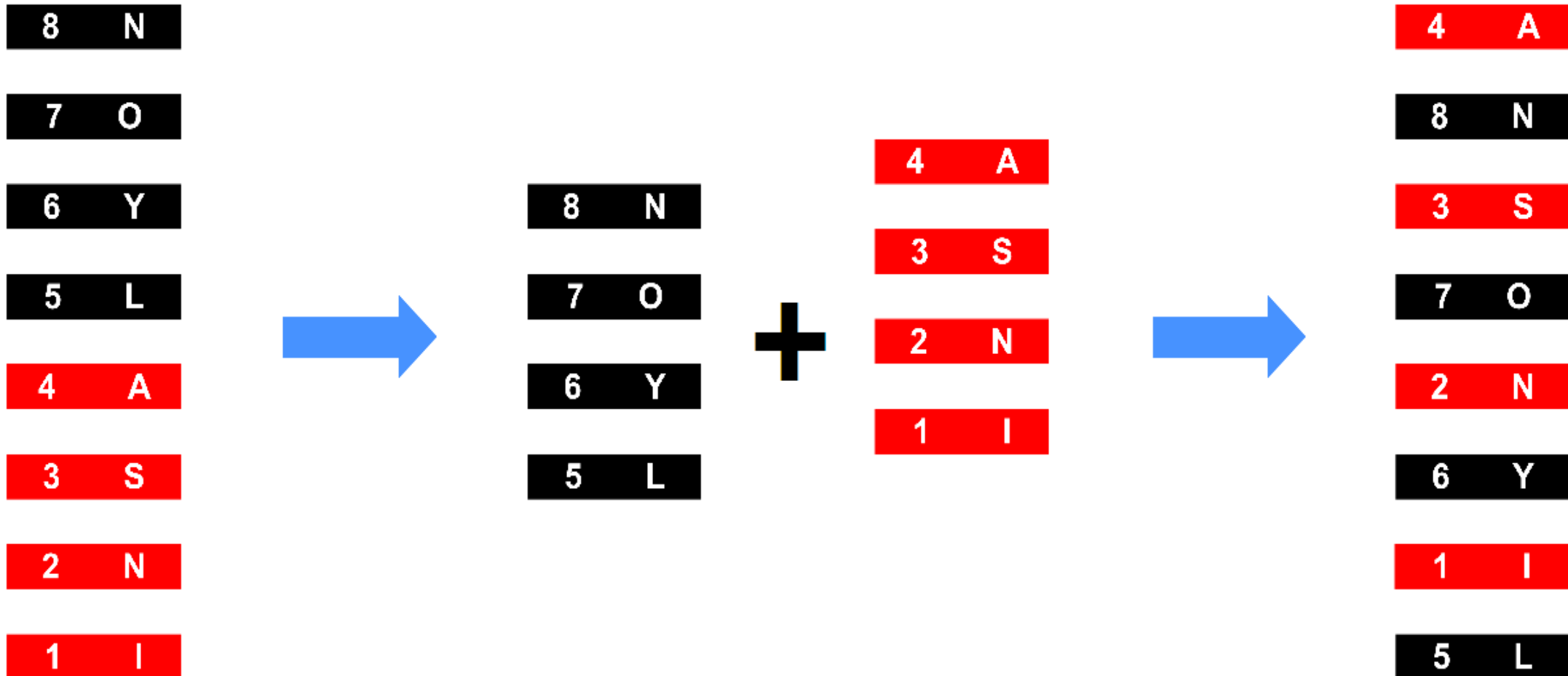
$$\text{Notation : } f^3 = f \circ f \circ f$$

$$\left\{ \begin{array}{l} f^3(1) = 8 \equiv 8 \ [9] \\ f^3(2) = 7 \equiv 16 \ [9] \\ f^3(3) = 6 \equiv 24 \ [9] \\ f^3(4) = 5 \equiv 32 \ [9] \end{array} \right. \quad \left\{ \begin{array}{l} f^3(5) = 4 \equiv 40 \ [9] \\ f^3(6) = 3 \equiv 48 \ [9] \\ f^3(7) = 2 \equiv 56 \ [9] \\ f^3(8) = 1 \equiv 64 \ [9] \end{array} \right.$$

$$f^3(i) = f(f(f(i))) = 9 - i \equiv 8i \equiv -i \ [\text{mod } 9]$$

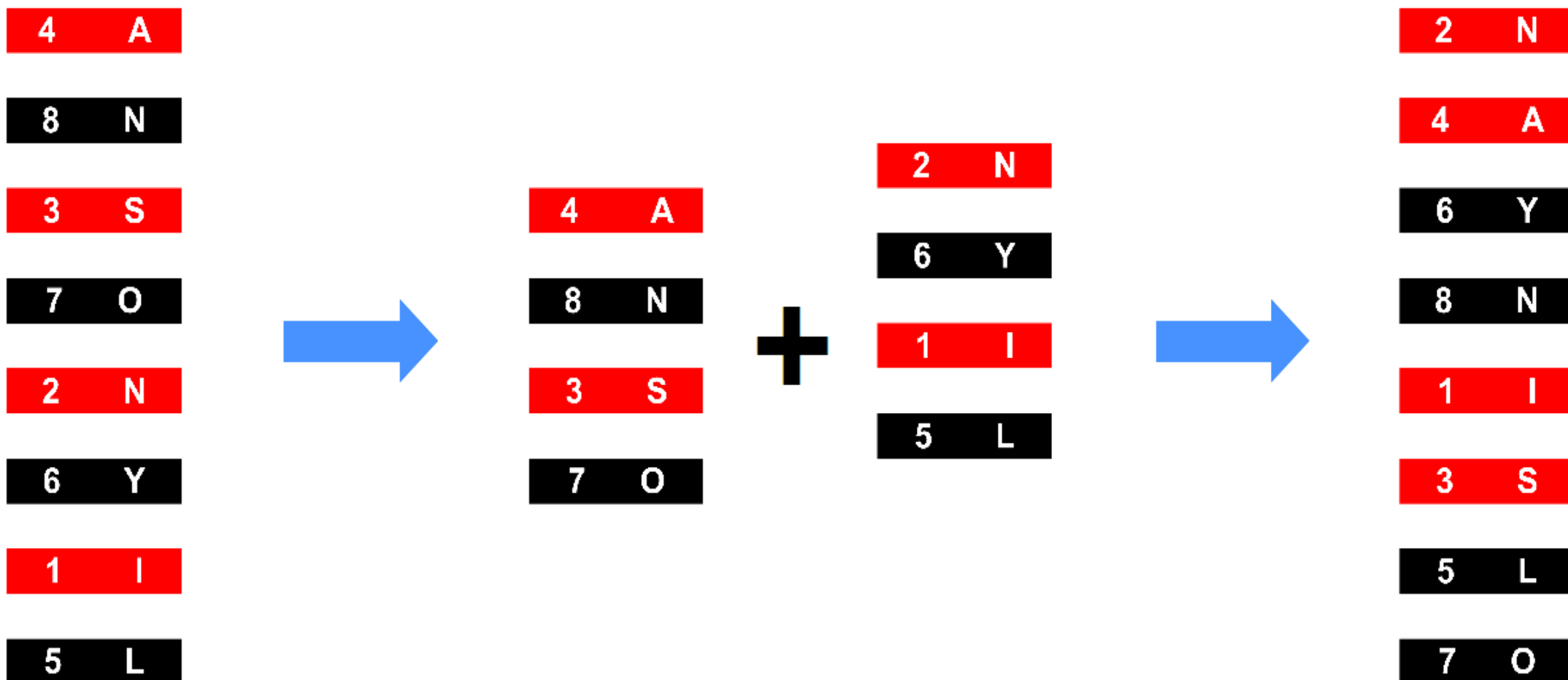
Au bout de 3 mélanges, le jeu est inversé...

4^e mélange



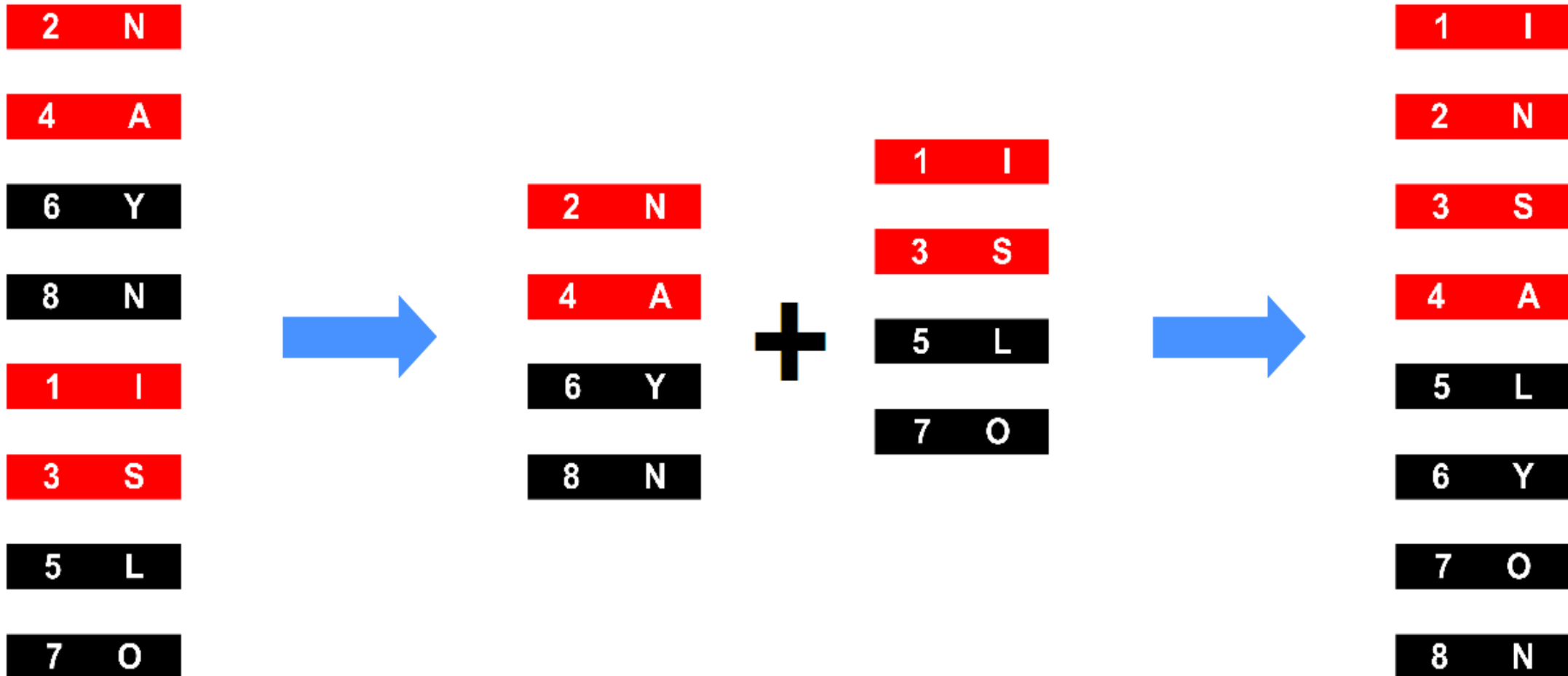
$$f^4(i) \equiv 16i \equiv -2i \pmod{9}$$

5^e mélange



$$f^5(i) \equiv 32i \equiv -4i \pmod{9}$$

6^e mélange



$f^6(i) \equiv 64i \equiv -8i \equiv i \pmod{9}$
Au bout de 6 mélanges : retour à l'état initial !

Le secret...

$$2^6 = 64 \equiv 1 \pmod{9}$$

$$f^6 = \text{id}$$

En résumé

Une période...

$$f^6 = \text{id}$$

6^e mélange : jeu **initial**

Au passage :

$$f^{-1} = f^5$$

5^e mélange : **anti-Faro**

Une demi-période...

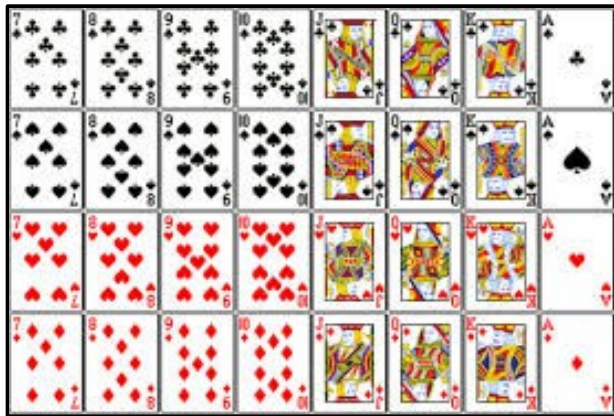
$$f^3 = 9 - \text{id}$$

3^e mélange : jeu **inversé**

Généralisation

Théorème : pour un jeu de 2^p cartes,

- $2p$ mélanges Faros ramènent le jeu à son ordre *initial*
- p mélanges Faros emmènent le jeu dans un ordre *inversé*



Exemple : pour un jeu de 32 cartes,
 10 mélanges Faros ramènent le jeu
à son ordre *initial*

Application au cryptage

Théorème :

Pour tout entier pair n ,
un jeu de n cartes revient
à sa position **initiale**
après r mélanges Faros
avec $2^r \equiv 1 \pmod{(n+1)}$

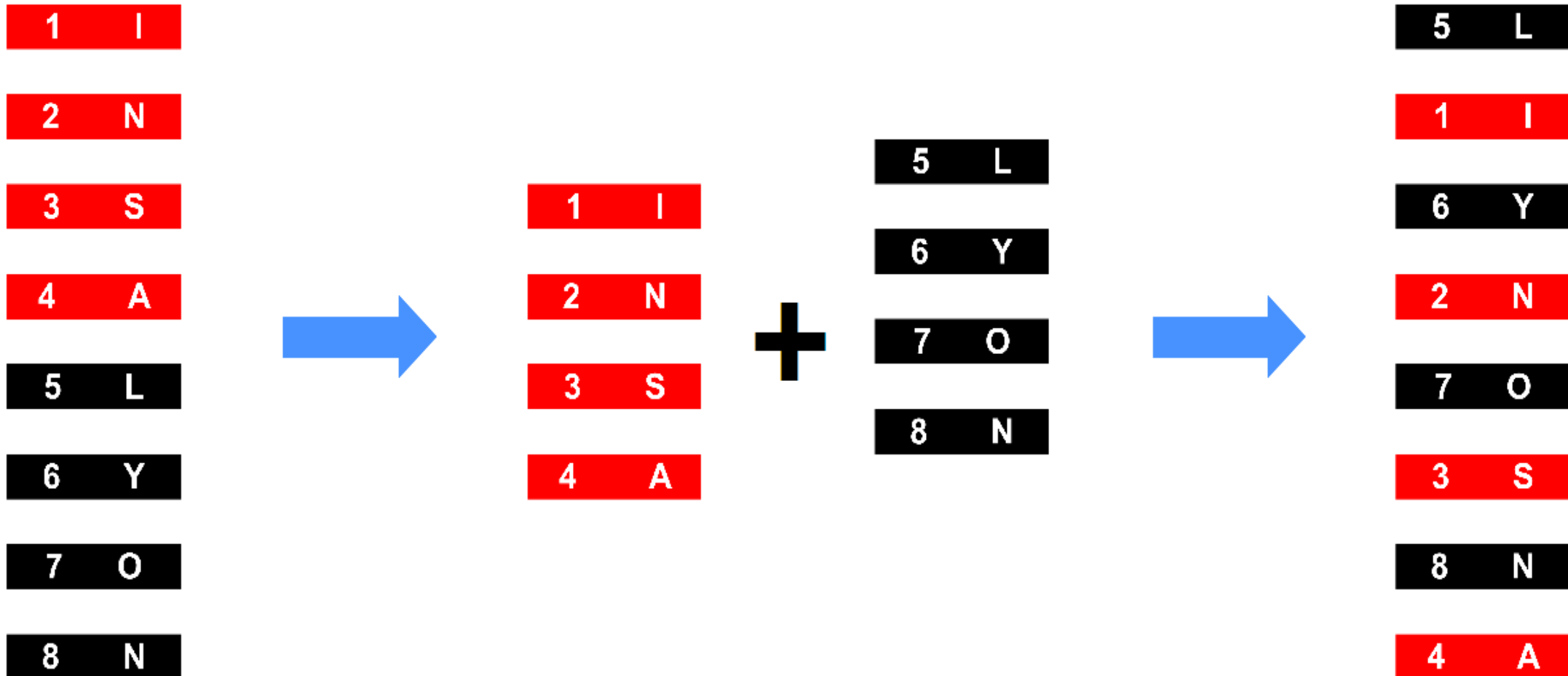
Chiffrement

On chiffre
avec p mélanges

Déchiffrement

On déchiffre
avec $q = r - p$ mélanges

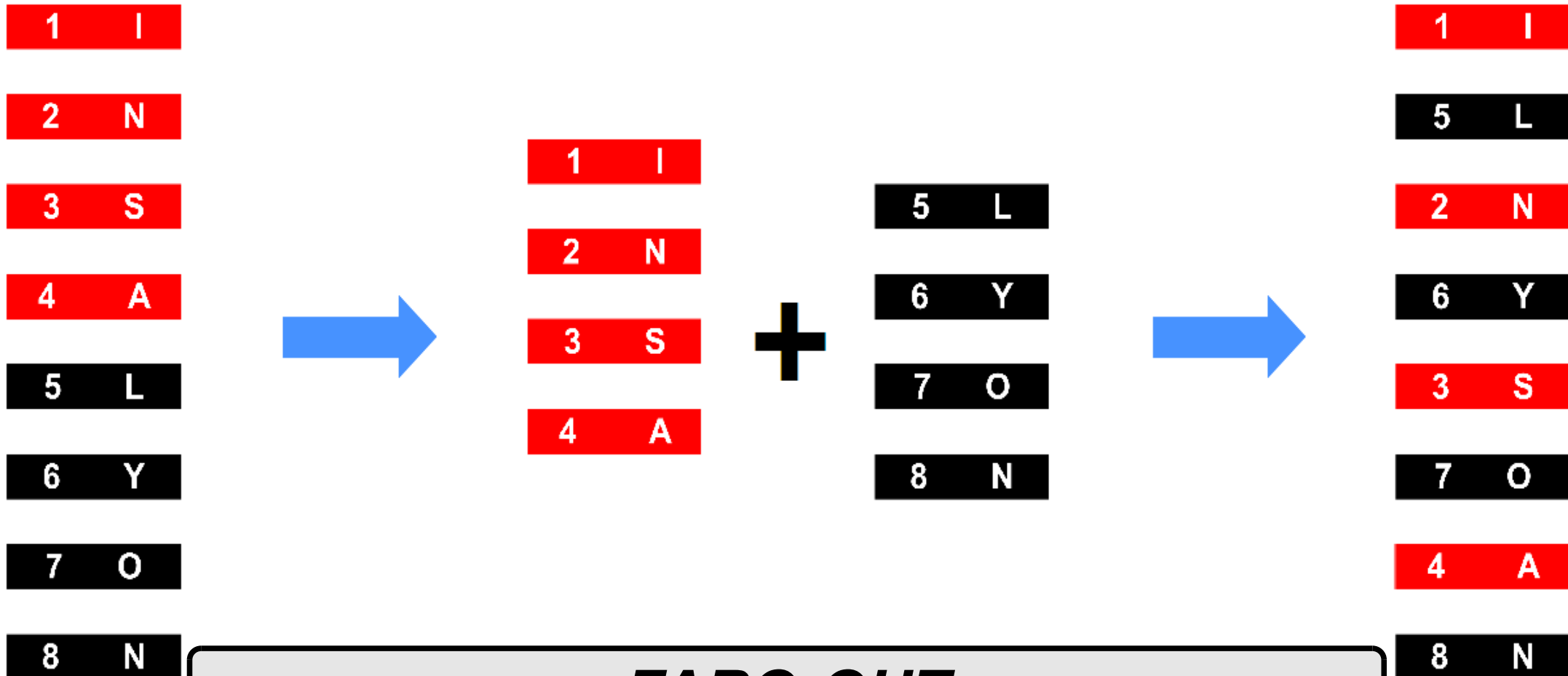
Complément : « Faro-in » et « Faro-out »



FARO-IN

La première carte rouge est insérée *au-dessous* de la première carte noire

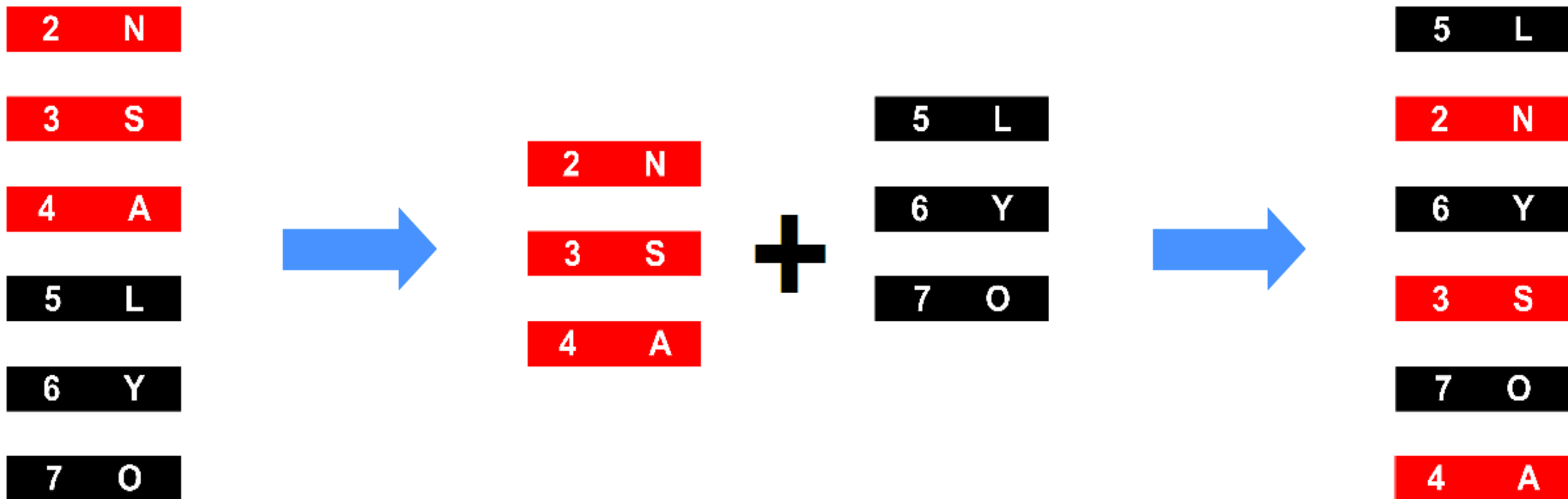
Complément : « Faro-in » et « Faro-out »



FARO-OUT

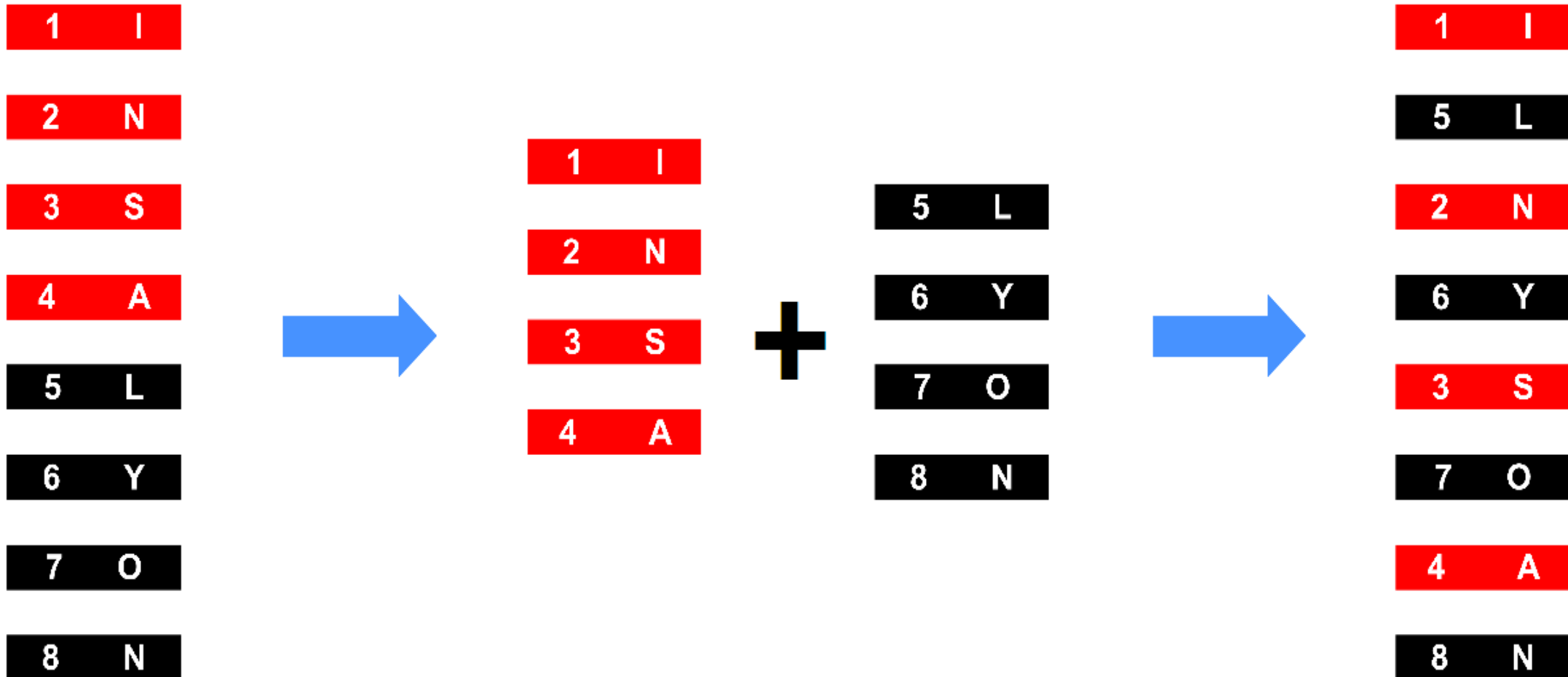
La première carte rouge est insérée *au-dessus* de la première carte noire
Les deux cartes extrêmes restent immobiles !

Complément : « Faro-in » et « Faro-out »



***FARO-IN* équivalent
obtenu en retirant les deux cartes extrêmes**

1^{er} mélange Faro-out



Modélisation : une autre permutation

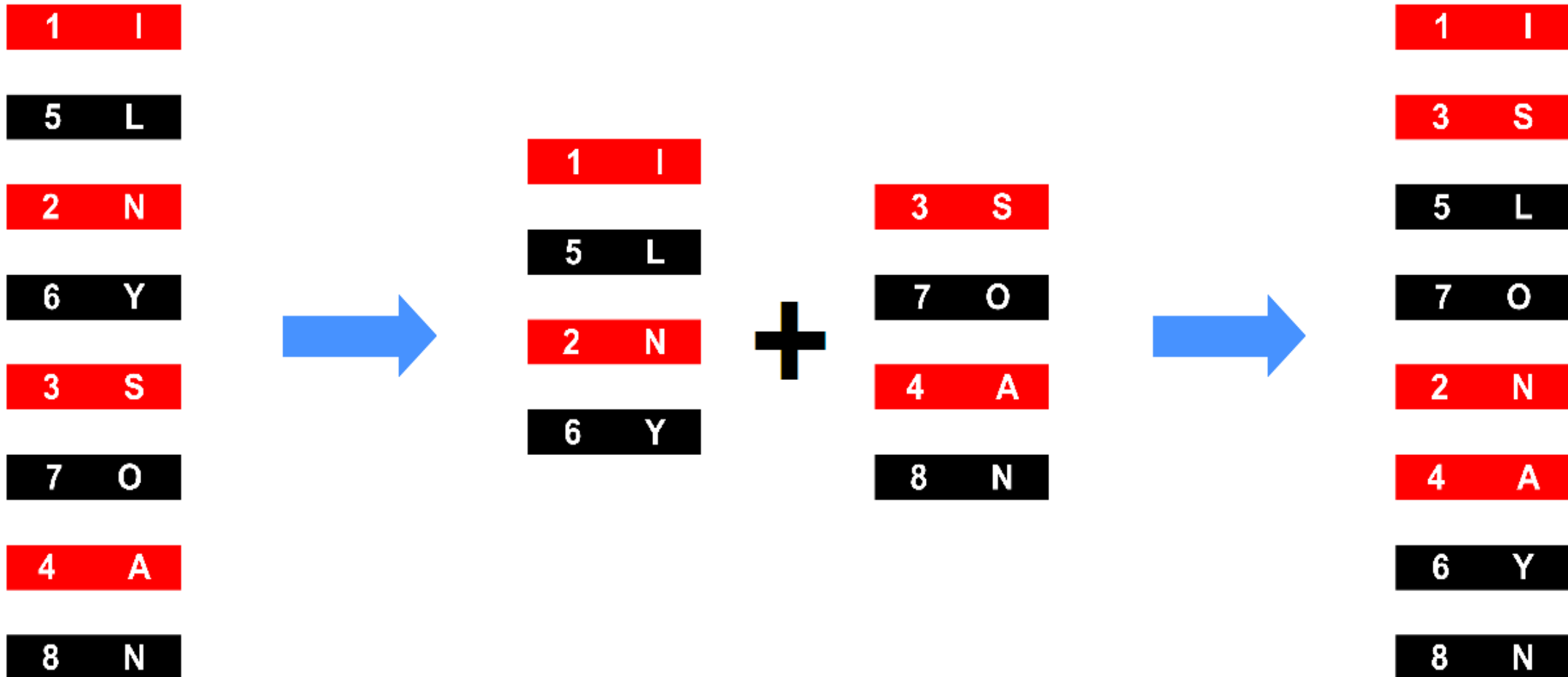
$$g: \{1, 2, 3, 4, 5, 6, 7, 8\} \rightarrow \{1, 2, 3, 4, 5, 6, 7, 8\}$$

i : position *avant* mélange $\leftrightarrow j = g(i)$: position *après* mélange

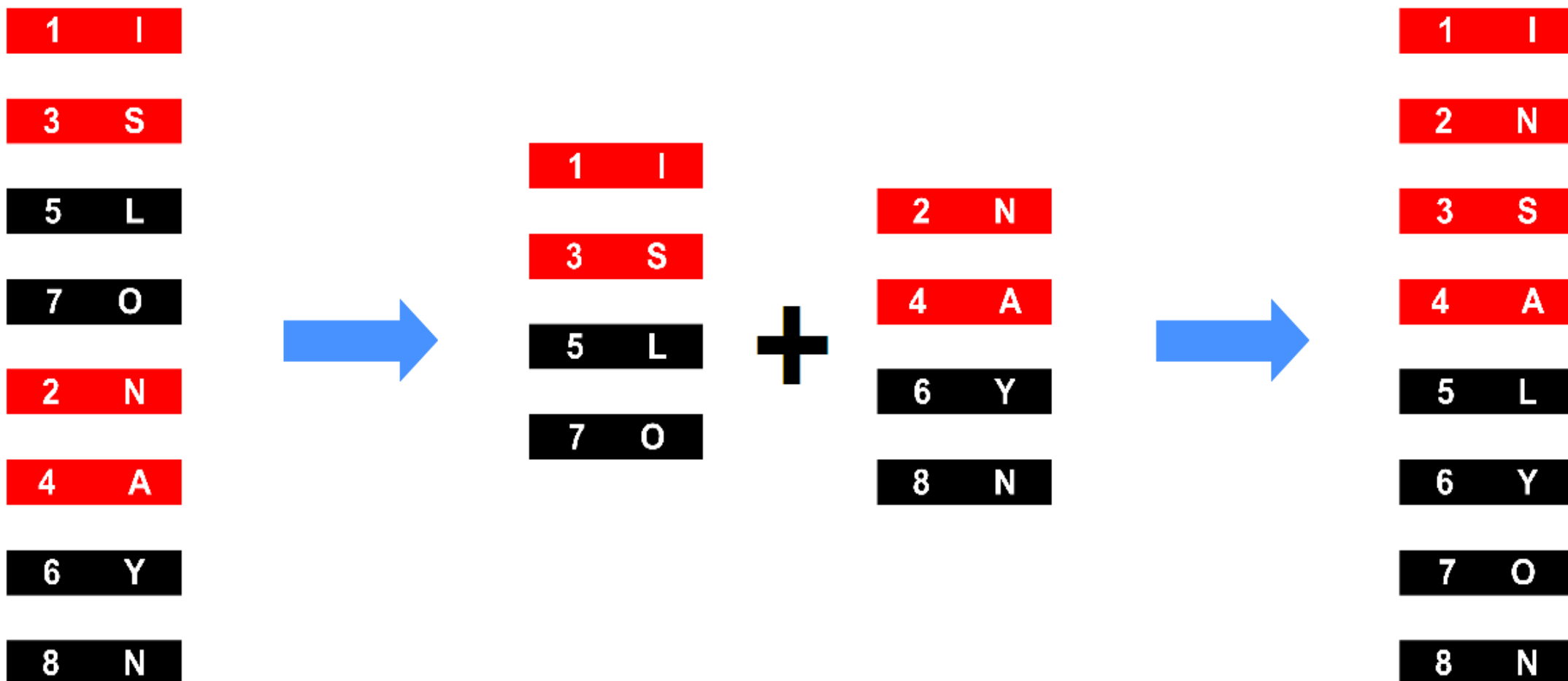
$$\left\{ \begin{array}{l} g(1) = 1 \\ g(2) = 3 \\ g(3) = 5 \\ g(4) = 7 \end{array} \right. \quad \left\{ \begin{array}{l} g(5) = 2 \equiv 9 \pmod{7} \\ g(6) = 4 \equiv 11 \pmod{7} \\ g(7) = 6 \equiv 13 \pmod{7} \\ g(8) = 8 \equiv 15 \pmod{7} \end{array} \right.$$

$$g(i) = \left\{ \begin{array}{ll} 2i-1 & \text{si } i \leq 4 \\ 2i-8 & \text{si } i \geq 5 \end{array} \right\} \equiv 2i-1 \pmod{7}$$

2^e mélange Faro-out



3^e mélange Faro-out



Au bout de 3 mélanges : retour à l'état initial !

Le secret...

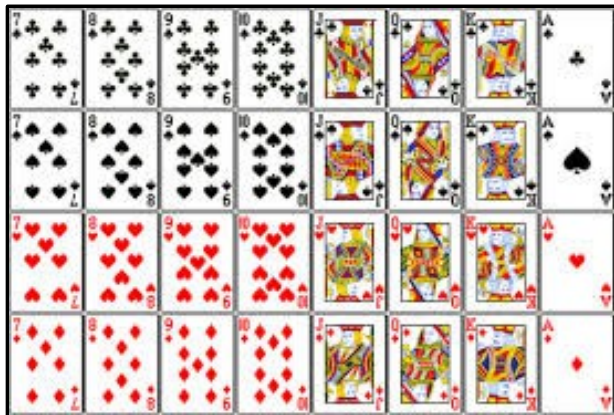
$$2^3 = 8 \equiv 1 \pmod{7}$$

$$g^3 = \text{id}$$

Généralisation

Théorème :

- pour un jeu de 2^p cartes,
 p mélanges **Faros-out** ramènent le jeu
à son ordre **initial**
- pour un jeu de $2^p - 2$ cartes,
 p mélanges **Faros-in** ramènent le jeu
à son ordre **initial**



Exemple : pour un jeu de 32 cartes,
 5 mélanges **Faros-out** ramènent le jeu
à son ordre **initial**

Approche binaire : Faro-in

$$f: \{1, 2, 3, 4, 5, 6, 7, 8\} \rightarrow \{1, 2, 3, 4, 5, 6, 7, 8\}$$

i : position *avant* mélange $\leftrightarrow j = f(i)$: position *après* mélange

$$\left\{ \begin{array}{l} f(1) = 2 \\ f(2) = 4 \\ f(3) = 6 \\ f(4) = 8 \end{array} \right. \quad \left\{ \begin{array}{l} f(5) = 1 \\ f(6) = 3 \\ f(7) = 5 \\ f(8) = 7 \end{array} \right.$$

$$f(i) = \left\{ \begin{array}{ll} 2i & \text{si } i \leq 4 \\ 2i - 9 & \text{si } i \geq 5 \end{array} \right\} \equiv 2i \pmod{9}$$

$$f: \{0, 1, 2, 3, 4, 5, 6, 7\} \rightarrow \{0, 1, 2, 3, 4, 5, 6, 7\}$$

i : position *avant* mélange $\leftrightarrow j = f(i)$: position *après* mélange

$$\left\{ \begin{array}{l} f(0) = 1 \\ f(1) = 3 \\ f(2) = 5 \\ f(3) = 7 \end{array} \right. \quad \left\{ \begin{array}{l} f(4) = 0 \\ f(5) = 2 \\ f(6) = 4 \\ f(7) = 6 \end{array} \right.$$

$$f(i) = \left\{ \begin{array}{ll} 2i+1 & \text{si } i \leq 3 \\ 2i-8 & \text{si } i \geq 4 \end{array} \right\} \equiv 2i+1 \pmod{9}$$

$$f: \{0, 1, 2, 3, 4, 5, 6, 7\} \rightarrow \{0, 1, 2, 3, 4, 5, 6, 7\}$$

i : position *avant* mélange $\leftrightarrow j = f(i)$: position *après* mélange

$$\begin{cases} f(000) = 001 \\ f(001) = 011 \\ f(010) = 101 \\ f(011) = 111 \end{cases}$$

$$\begin{cases} f(100) = 000 \\ f(101) = 010 \\ f(110) = 100 \\ f(111) = 110 \end{cases}$$

Pour $i = (abc)_2 = 2^2a + 2b + c$:

$$f(i) = f((abc)_2) = (bc\bar{a})_2 \text{ avec } \bar{a} = 1 - a$$

$$\begin{aligned} f\left(\left(\begin{matrix} a & b & c \end{matrix}\right)_2\right) &= \left(\begin{matrix} b & c & \bar{a} \end{matrix}\right)_2 \\ f^2\left(\left(\begin{matrix} a & b & c \end{matrix}\right)_2\right) &= \left(\begin{matrix} c & \bar{a} & \bar{b} \end{matrix}\right)_2 \\ f^3\left(\left(\begin{matrix} a & b & c \end{matrix}\right)_2\right) &= \left(\begin{matrix} \bar{a} & \bar{b} & \bar{c} \end{matrix}\right)_2 \end{aligned}$$

$$\begin{aligned} f^4\left(\left(\begin{matrix} a & b & c \end{matrix}\right)_2\right) &= \left(\begin{matrix} \bar{b} & \bar{c} & a \end{matrix}\right)_2 \\ f^5\left(\left(\begin{matrix} a & b & c \end{matrix}\right)_2\right) &= \left(\begin{matrix} \bar{c} & a & b \end{matrix}\right)_2 \\ f^6\left(\left(\begin{matrix} a & b & c \end{matrix}\right)_2\right) &= \left(\begin{matrix} a & b & c \end{matrix}\right)_2 \end{aligned}$$

$$f^3\left(\left(\begin{matrix} a & b & c \end{matrix}\right)_2\right) = \left(\begin{matrix} \bar{a} & \bar{b} & \bar{c} \end{matrix}\right)_2 \text{ et } f^6\left(\left(\begin{matrix} a & b & c \end{matrix}\right)_2\right) = \left(\begin{matrix} a & b & c \end{matrix}\right)_2$$

$$f^3 = 9\text{-id}$$

$$f^6 = \text{id}$$

Approche binaire : Faro-out

$$g: \{1, 2, 3, 4, 5, 6, 7, 8\} \rightarrow \{1, 2, 3, 4, 5, 6, 7, 8\}$$

i : position *avant* mélange $\leftrightarrow j = g(i)$: position *après* mélange

$$\left\{ \begin{array}{l} g(1) = 1 \\ g(2) = 3 \\ g(3) = 5 \\ g(4) = 7 \end{array} \right.$$

$$\left\{ \begin{array}{l} g(5) = 2 \\ g(6) = 4 \\ g(7) = 6 \\ g(8) = 8 \end{array} \right.$$

$$g(i) = \left\{ \begin{array}{ll} 2i-1 & \text{si } i \leq 4 \\ 2i-8 & \text{si } i \geq 5 \end{array} \right\} \equiv 2i-1 \pmod{7}$$

Approche binaire : Faro-out Renumérotation

$$g: \{0, 1, 2, 3, 4, 5, 6, 7\} \rightarrow \{0, 1, 2, 3, 4, 5, 6, 7\}$$

i : position *avant* mélange $\leftrightarrow j = g(i)$: position *après* mélange

$$\begin{cases} g(0) = 0 \\ g(1) = 2 \\ g(2) = 4 \\ g(3) = 6 \end{cases}$$

$$\begin{cases} g(4) = 1 \\ g(5) = 3 \\ g(6) = 5 \\ g(7) = 7 \end{cases}$$

$$g(i) = \begin{cases} 2i & \text{si } i \leq 3 \\ 2i - 7 & \text{si } i \geq 4 \end{cases} \equiv 2i \pmod{7}$$

Approche binaire : Faro-out Renumérotation

$$g: \{0, 1, 2, 3, 4, 5, 6, 7\} \rightarrow \{0, 1, 2, 3, 4, 5, 6, 7\}$$

i : position *avant* mélange $\leftrightarrow j = g(i)$: position *après* mélange

$$\left\{ \begin{array}{l} g(000) = 000 \\ g(001) = 010 \\ g(010) = 100 \\ g(011) = 110 \end{array} \right.$$

$$\left\{ \begin{array}{l} g(100) = 001 \\ g(101) = 011 \\ g(110) = 101 \\ g(111) = 111 \end{array} \right.$$

Pour $i = (abc)_2 = 2^2 a + 2b + c$:

$$g(i) = g((abc)_2) = (bca)_2$$

$$\begin{aligned} g \left((abc)_2 \right) &= (bca)_2 \\ g^2 \left((abc)_2 \right) &= (cab)_2 \\ g^3 \left((abc)_2 \right) &= (abc)_2 \end{aligned}$$

$$g^3 \left((abc)_2 \right) = (abc)_2$$

$$g^3 = \text{id}$$

Généralisation

Théorème : pour un jeu de 2^p cartes,

$$\text{pour } i = (i_{p-1} i_{p-2} \cdots i_1 i_0)_2$$

$$= 2^{p-1} i_{p-1} + 2^{p-2} i_{p-2} + \cdots + 2 i_1 + i_0$$

avec $i_0, i_1, \dots, i_{p-2}, i_{p-1} \in \{0, 1\}$, et en posant $\bar{i}_q = 1 - i_q$:

$$f \left((i_{p-1} i_{p-2} \cdots i_1 i_0)_2 \right) = (i_{p-2} \cdots i_1 i_0 \bar{i}_{p-1})_2$$

$$g \left((i_{p-1} i_{p-2} \cdots i_1 i_0)_2 \right) = (i_{p-2} \cdots i_1 i_0 i_{p-1})_2$$

$$f^{2p} = \text{id}$$

$$g^p = \text{id}$$

Et pour aller plus loin...



Réf. : A.L., Mélanges parfaits de cartes – (I) et (II), Quadrature 76 et 77 (2010)
<https://hal.archives-ouvertes.fr/hal-00864428/document> <https://hal.archives-ouvertes.fr/hal-00864433/document>

Et pour aller plus loin...

Conférences **MATH & MAGIE** — INSA

MATH & MAGIE

**Les MATHÉMATIQUES
au service de la MAGIE ?**

ou

**La MAGIE au service
des MATHÉMATIQUES ?**

Aimé Lachal & Pierre Schott

INSA
INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
LYON

INSA de Lyon – 4 avril 2016

esiea
ÉCOLE D'INGÉNIEURS
DU MONDE NUMÉRIQUE

MATH & MAGIE


**CASINO
ROYAL**

**La Mathématique
est-elle Magique ?**

Ou

**La Magie
est-elle Mathématique ?**

Aimé Lachal & Pierre Schott

INSA
INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
LYON

INSA de Lyon – 26 mars 2018



http://math.univ-lyon1.fr/~alachal/exposes/mathemagie_2012.pdf
http://math.univ-lyon1.fr/~alachal/exposes/mathemagie_2016.pdf
http://math.univ-lyon1.fr/~alachal/exposes/mathemagie_2018.pdf



MERCI !

**MERCI
DE
VOTRE ATTENTION !**

