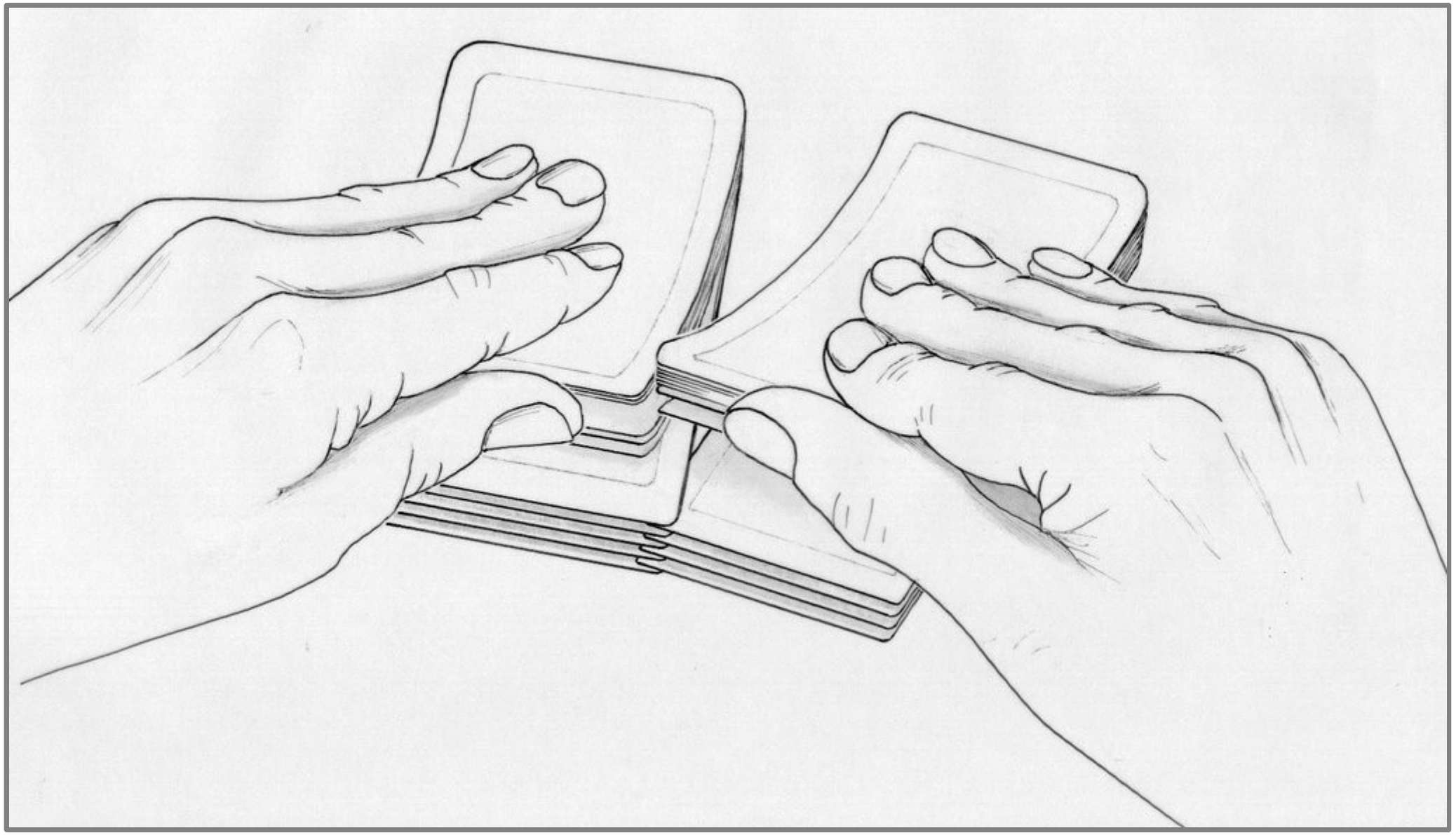
Mélanges Faros et cryptographie (exposé didactique - INSA LYON)

Aimé Lachal

INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
LYON

Mélanges Faros et cryptographie

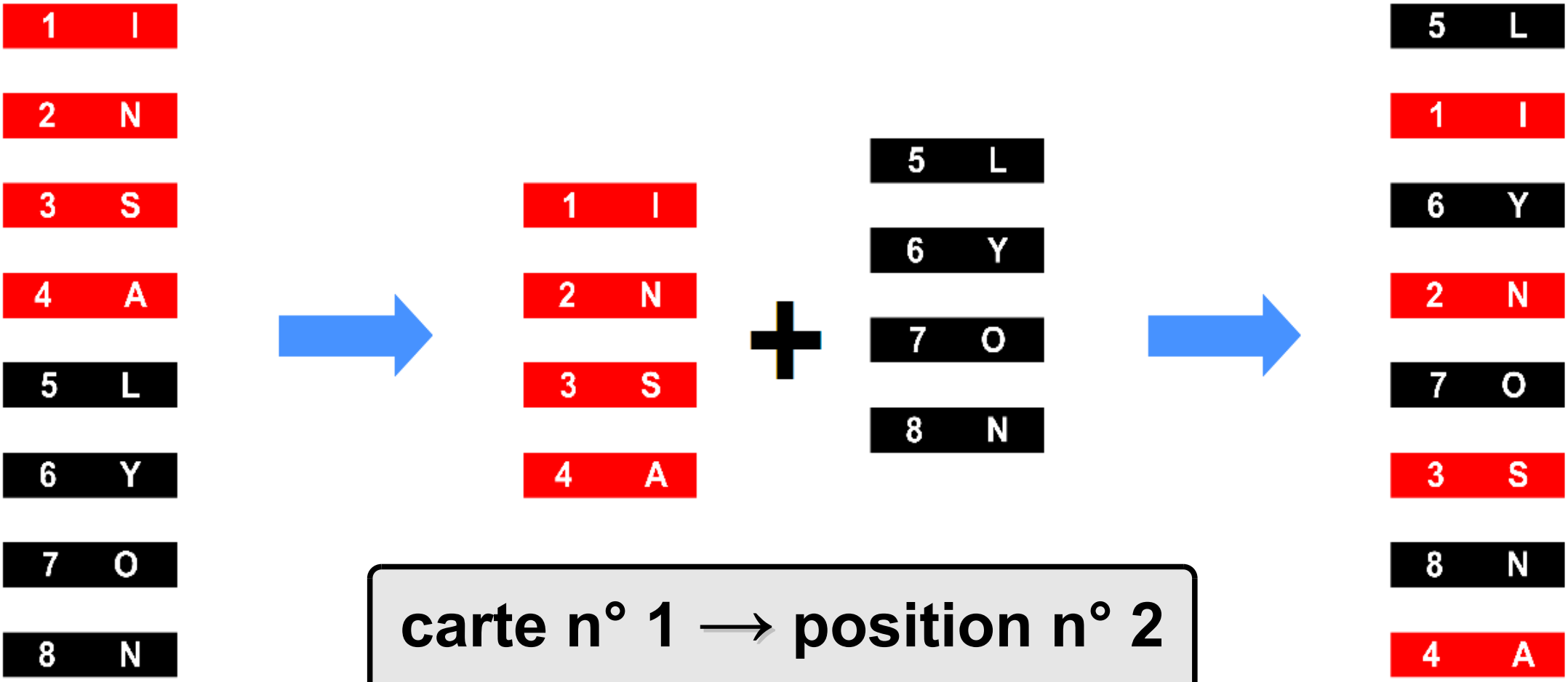
« Riffle shuffle »



« Riffle shuffle »

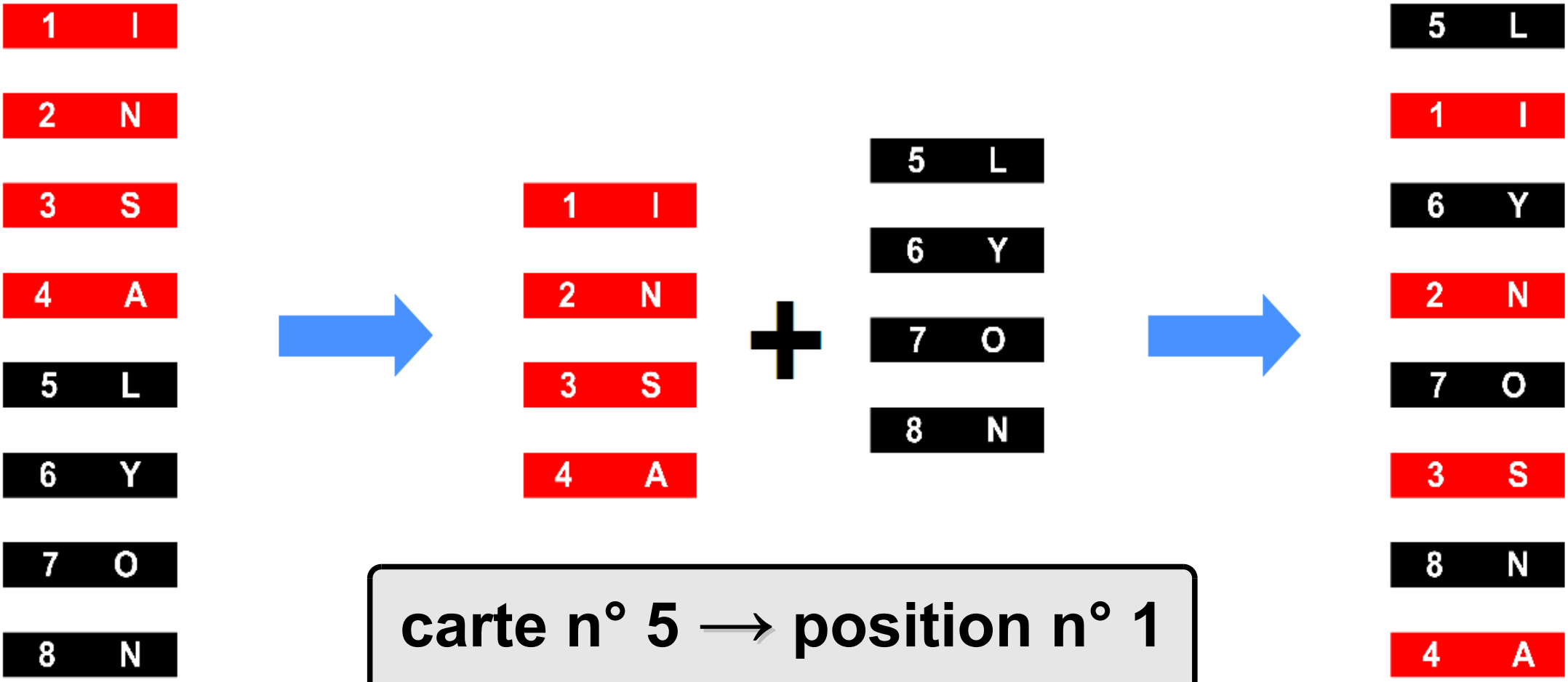

INSA
LYON

1er 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

1er 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

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

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

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

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

Modélisation : une permutation

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

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

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

$$\begin{cases} f(5) = 1 \equiv 10 \ [\text{mod } 9] \\ f(6) = 3 \equiv 12 \ [\text{mod } 9] \\ f(7) = 5 \equiv 14 \ [\text{mod } 9] \\ f(8) = 7 \equiv 16 \ [\text{mod } 9] \end{cases}$$

$$f(i) = \begin{cases} 2i & \text{si } i \leqslant 4 \\ 2i - 9 & \text{si } i \geqslant 5 \end{cases} \equiv 2i \ [\text{mod } 9]$$

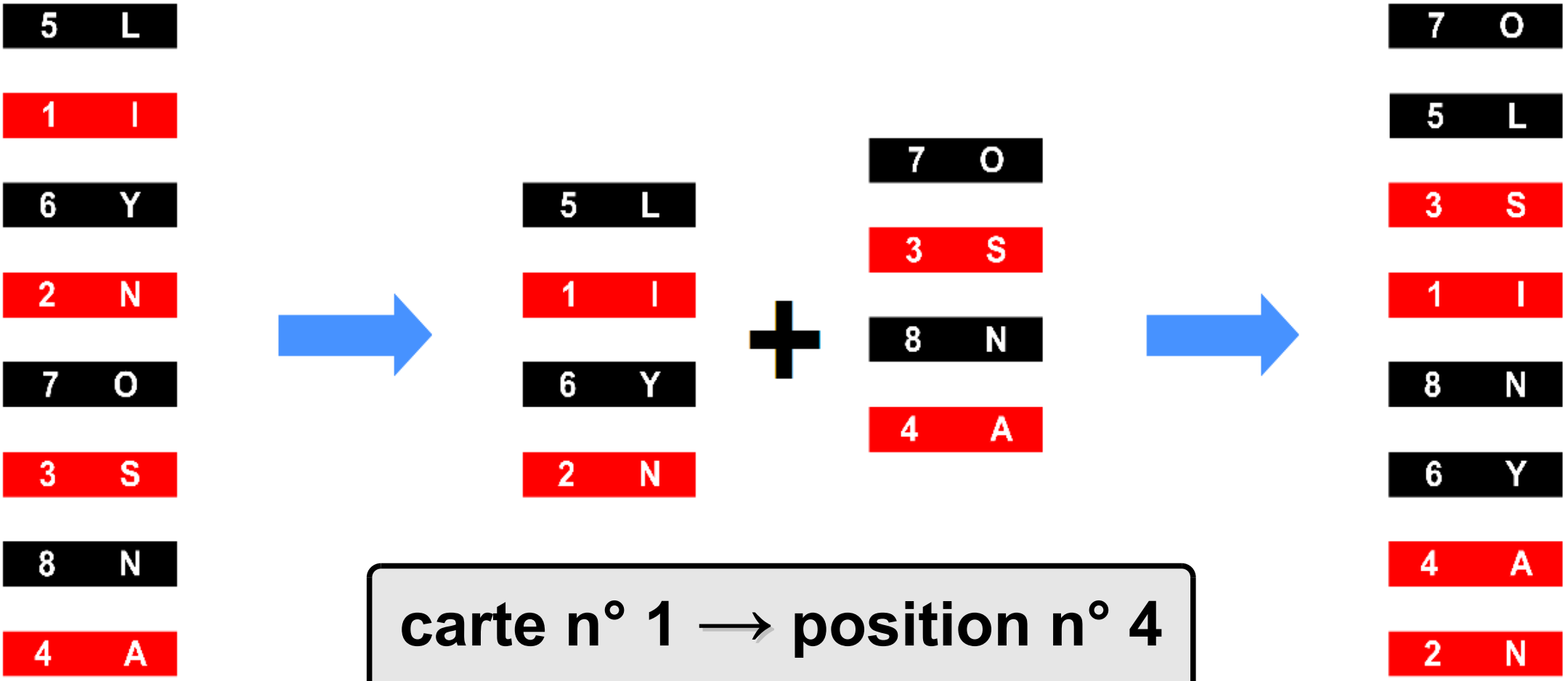
Modélisation : réciproque

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

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

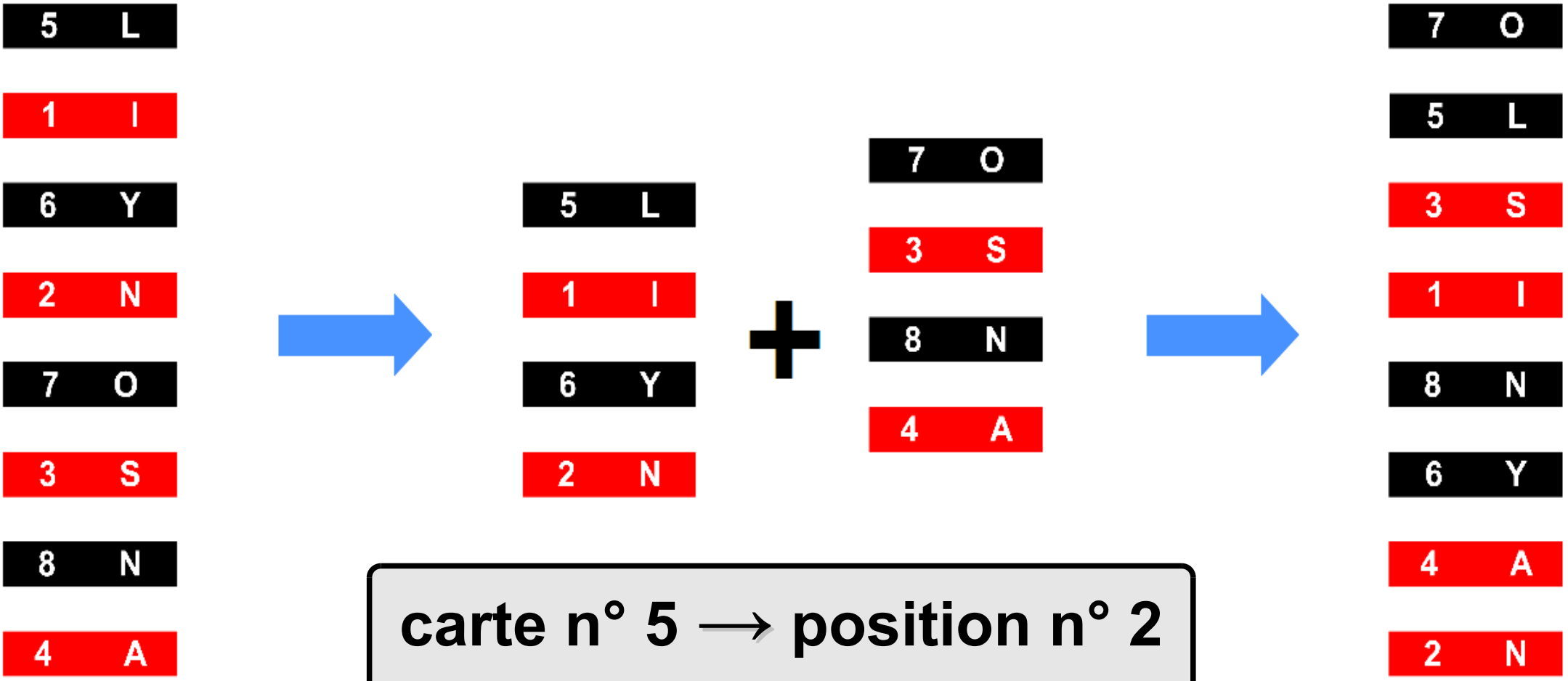
$$f^{-1}(j) = \begin{cases} j/2 & \text{si } j \text{ est pair} \\ (j+9)/2 & \text{si } j \text{ est impair} \end{cases}$$

2e 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

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

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

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

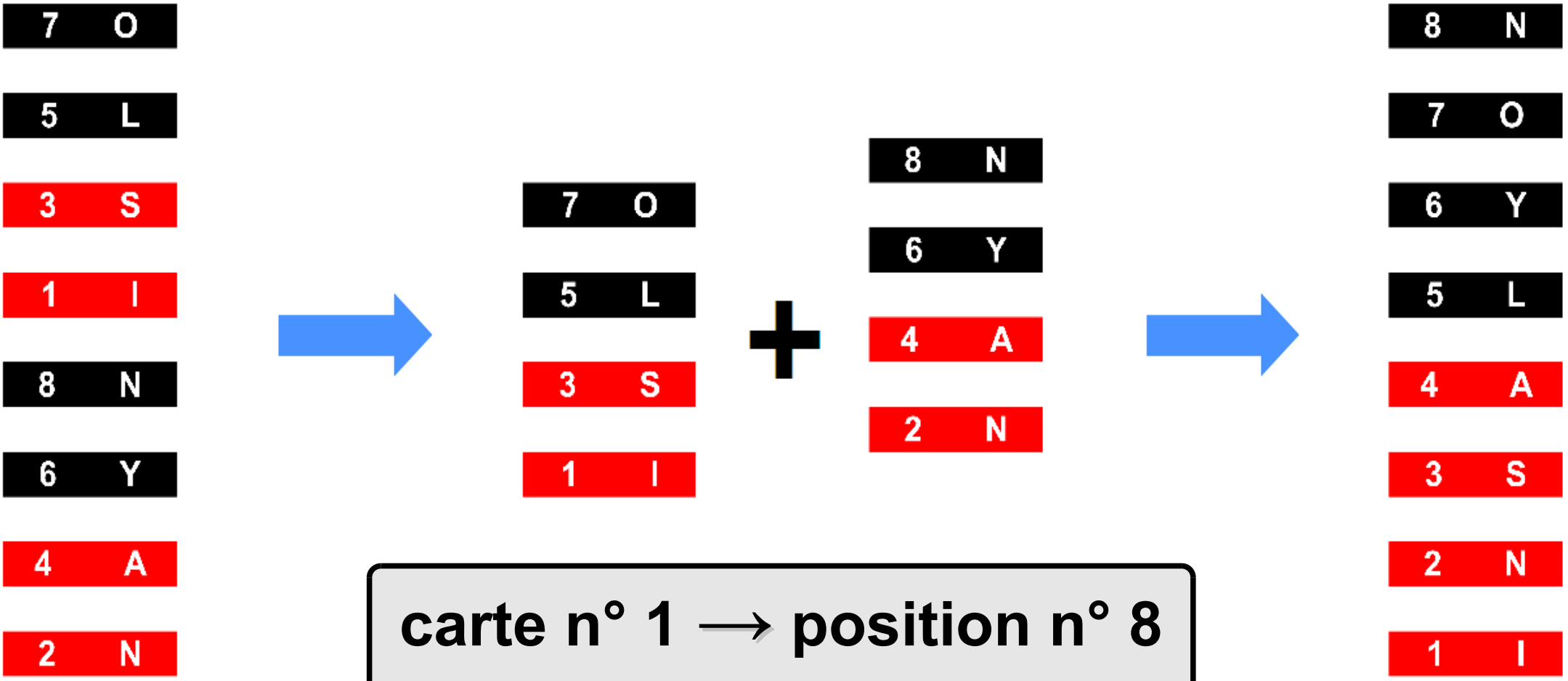
Modélisation : composition

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

$$\begin{cases} f^2(1) = 4 \equiv 4 \ [9] \\ f^2(2) = 8 \equiv 8 \ [9] \\ f^2(3) = 3 \equiv 12 \ [9] \\ f^2(4) = 7 \equiv 16 \ [9] \end{cases} \qquad \begin{cases} f^2(5) = 2 \equiv 20 \ [9] \\ f^2(6) = 6 \equiv 24 \ [9] \\ f^2(7) = 1 \equiv 28 \ [9] \\ f^2(8) = 5 \equiv 32 \ [9] \end{cases}$$

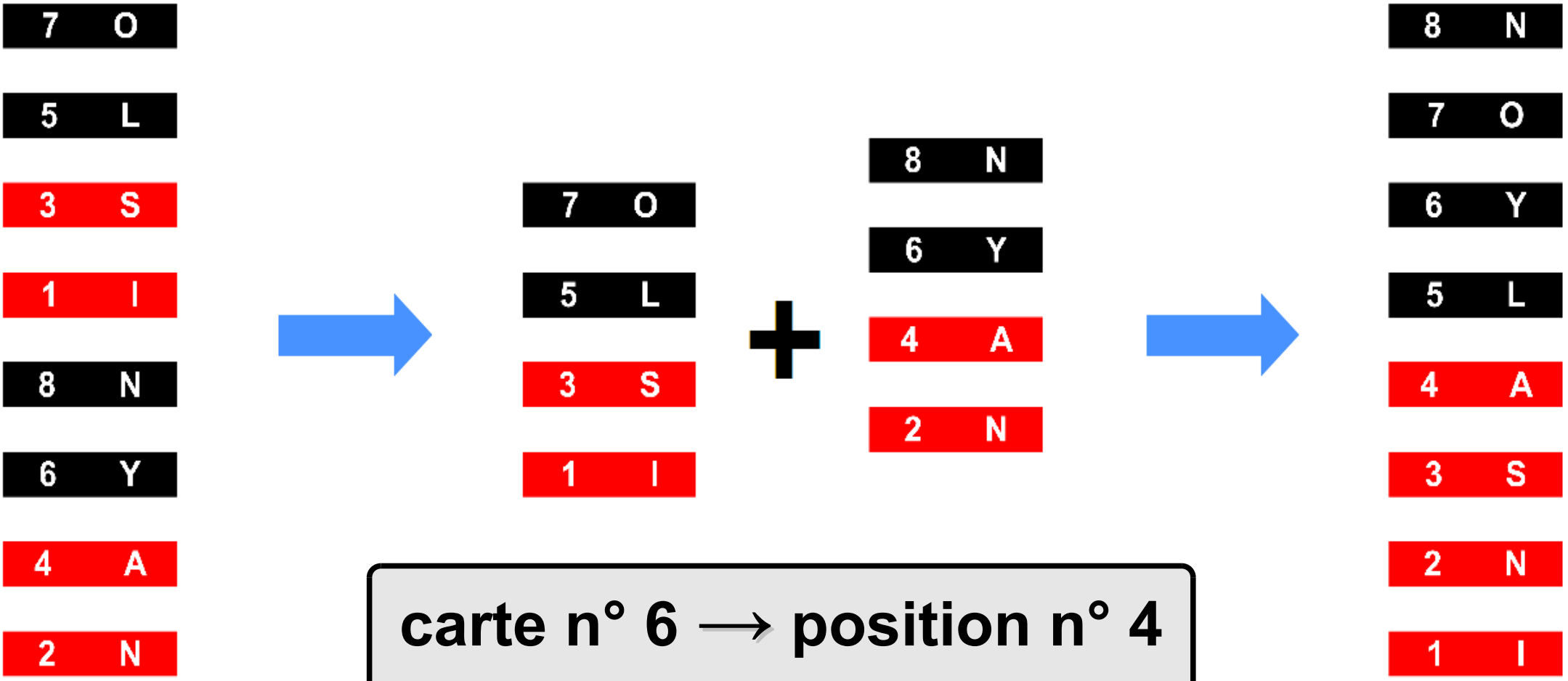
$$f^2(i) = f(f(i)) \equiv 4i \ [\text{mod } 9]$$

3e 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

3e 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

Notation : $f^3 = f \circ f \circ f$

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

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

Au bout de 3 mélanges, le jeu est inversé…

Modélisation : composition

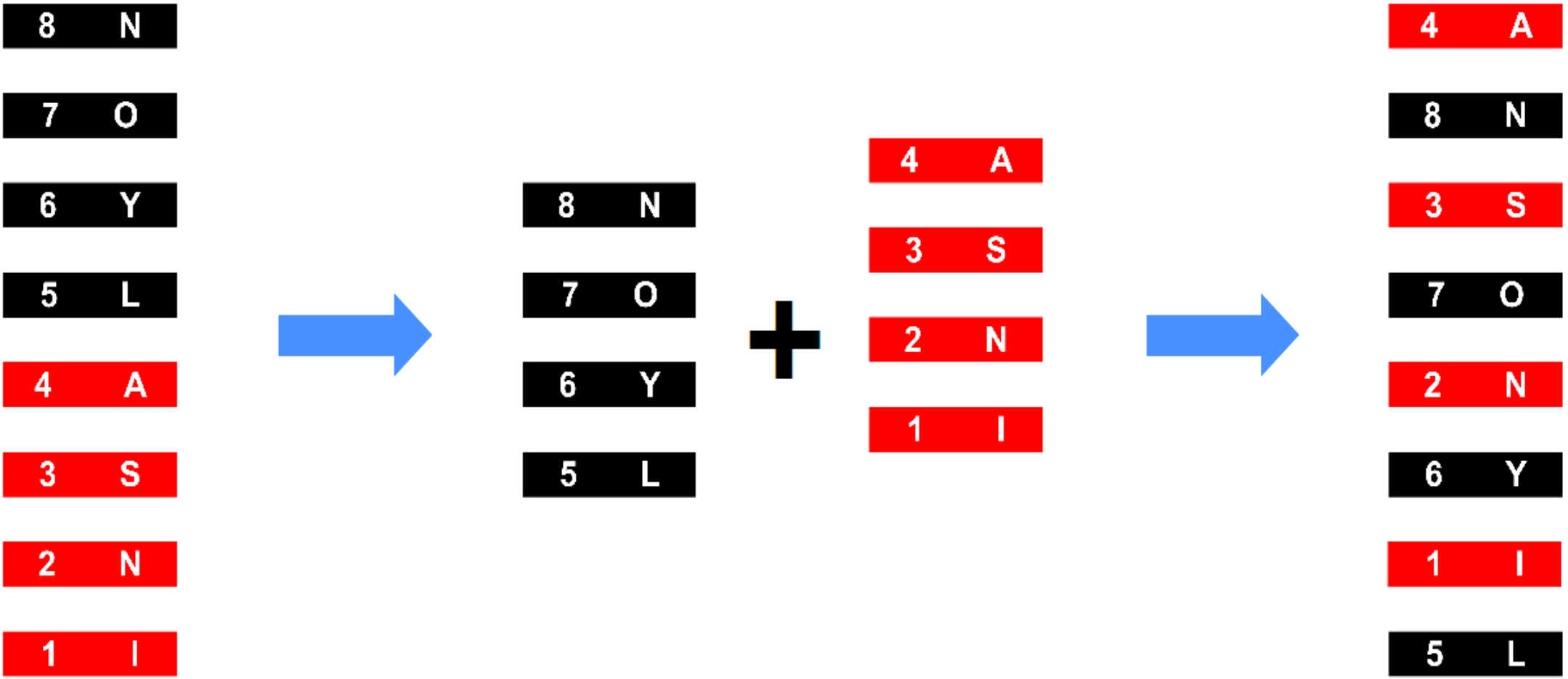
Notation : $f^3 = f \circ f \circ f$

$$\begin{cases} f^3(1) = 8 \equiv 8 \ [9] \\ f^3(2) = 7 \equiv 16 \ [9] \\ f^3(3) = 6 \equiv 24 \ [9] \\ f^3(4) = 5 \equiv 32 \ [9] \end{cases} \qquad \begin{cases} f^3(5) = 4 \equiv 40 \ [9] \\ f^3(6) = 3 \equiv 48 \ [9] \\ f^3(7) = 2 \equiv 56 \ [9] \\ f^3(8) = 1 \equiv 64 \ [9] \end{cases}$$

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

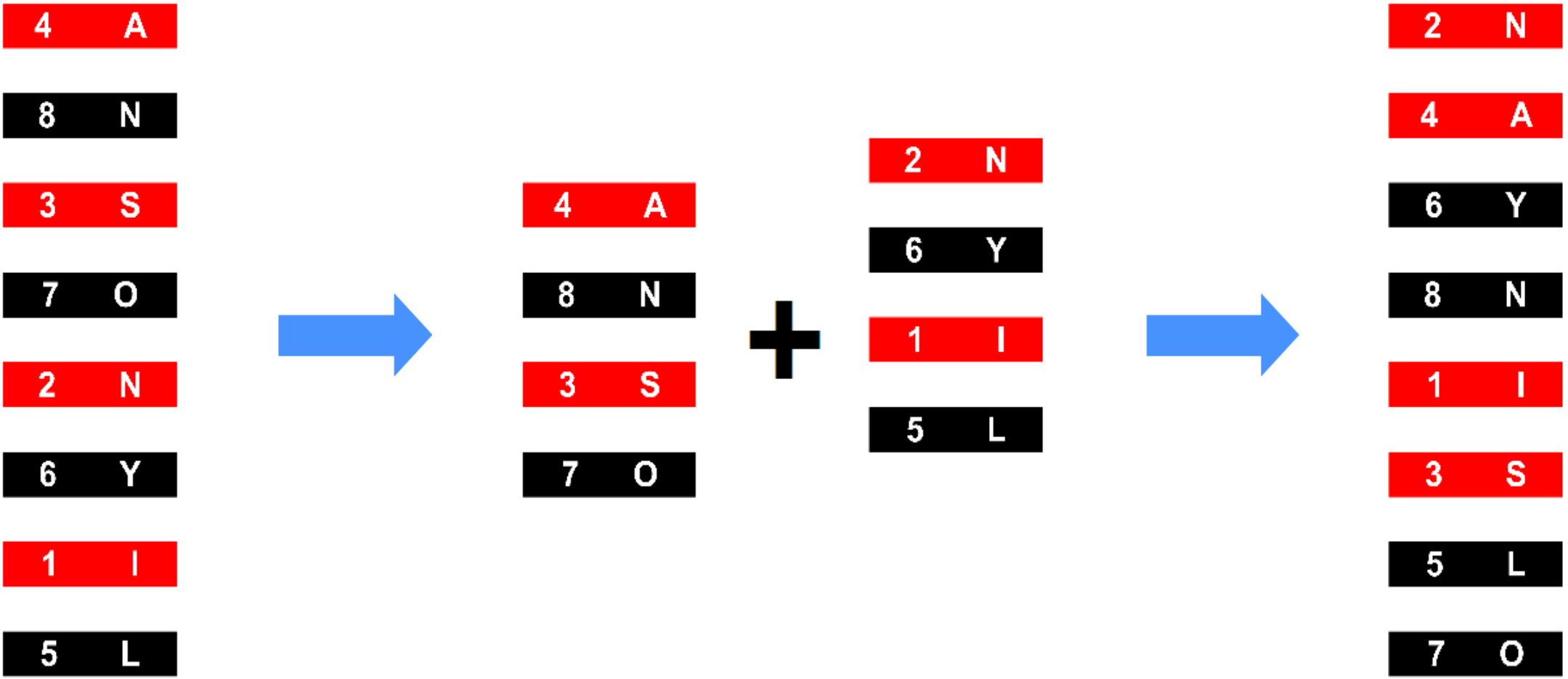
Au bout de 3 mélanges, le jeu est inversé…

4e mélange



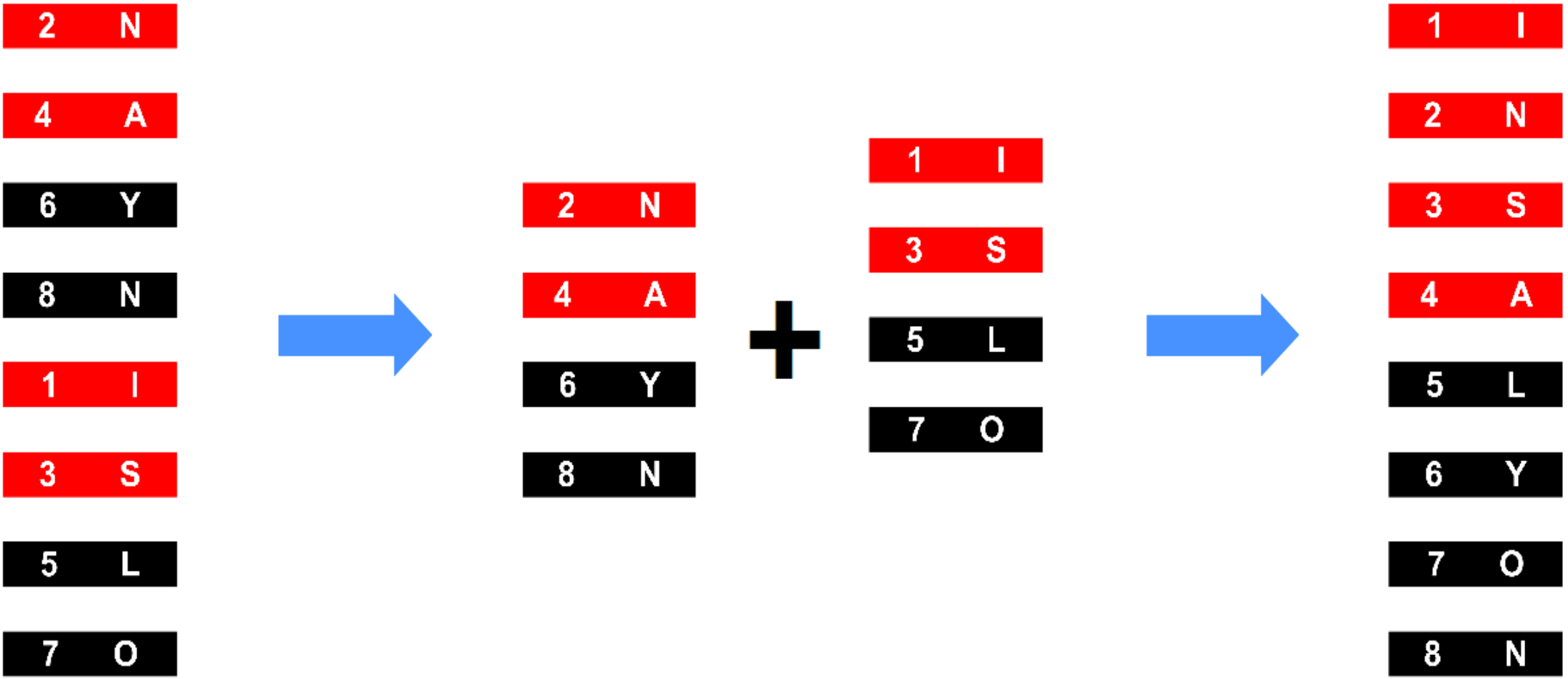
$$f^4(i) \equiv 16i \equiv -2i \ [\mathrm{mod}\ 9]$$

5e mélange



$$f^5(i) \equiv 32i \equiv -4i \ [\mathrm{mod}\ 9]$$

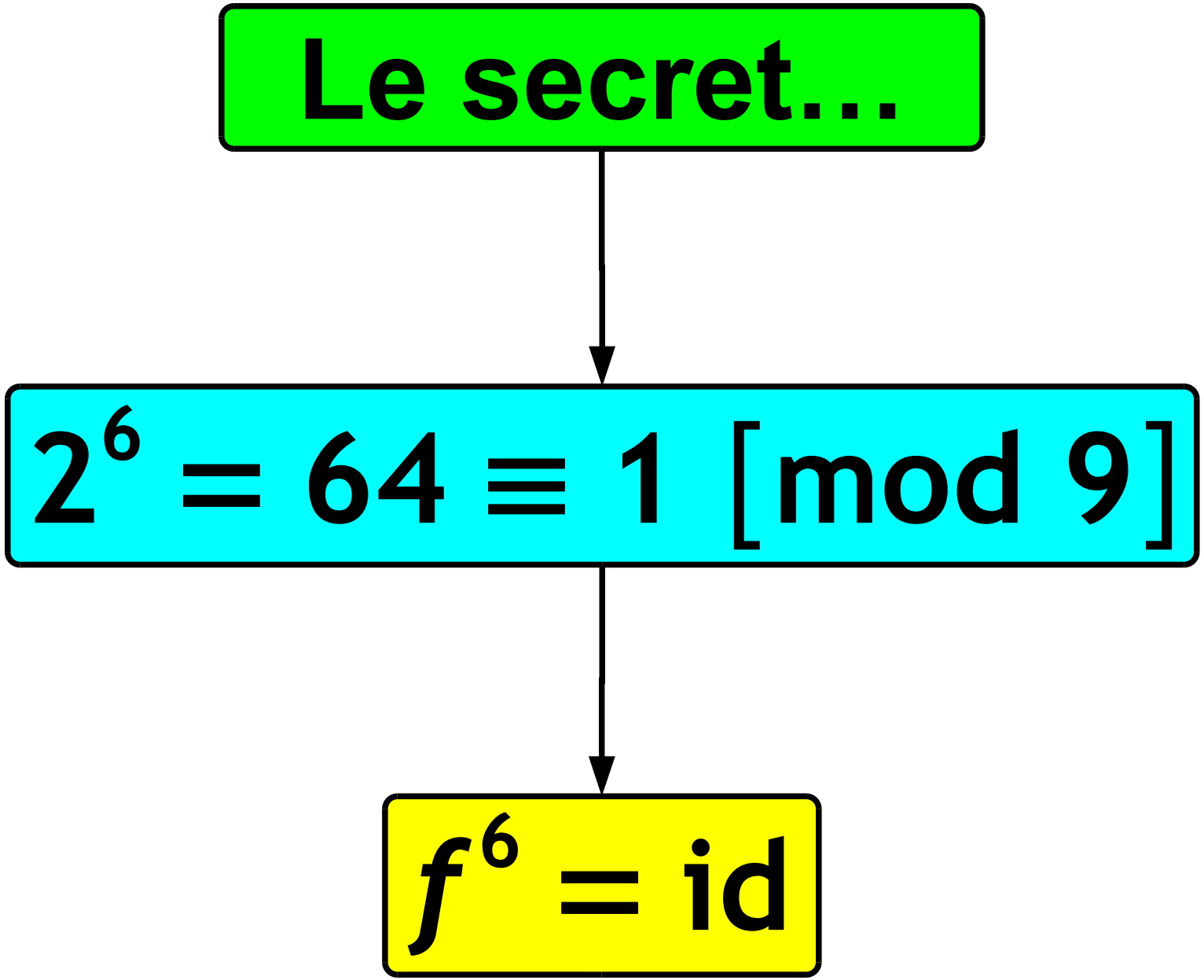
6^e mélange



$$f^6(i) \equiv 64i \equiv -8i \equiv i \ [\text{mod } 9]$$

Au bout de 6 mélanges : retour à l'état initial !

Modélisation : une période



En résumé

Une période…

$f^6 = \mathrm{id}$

6e mélange : jeu initial

Au passage :

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

5e mélange : anti-Faro

Une demi-période…

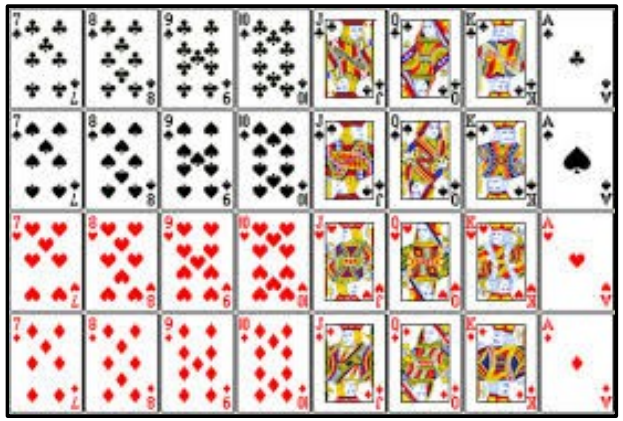
$f^3 = 9 - \mathrm{id}$

3e 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 $2^r \equiv 1 \ [\mathrm{mod}\ (n+1)]$

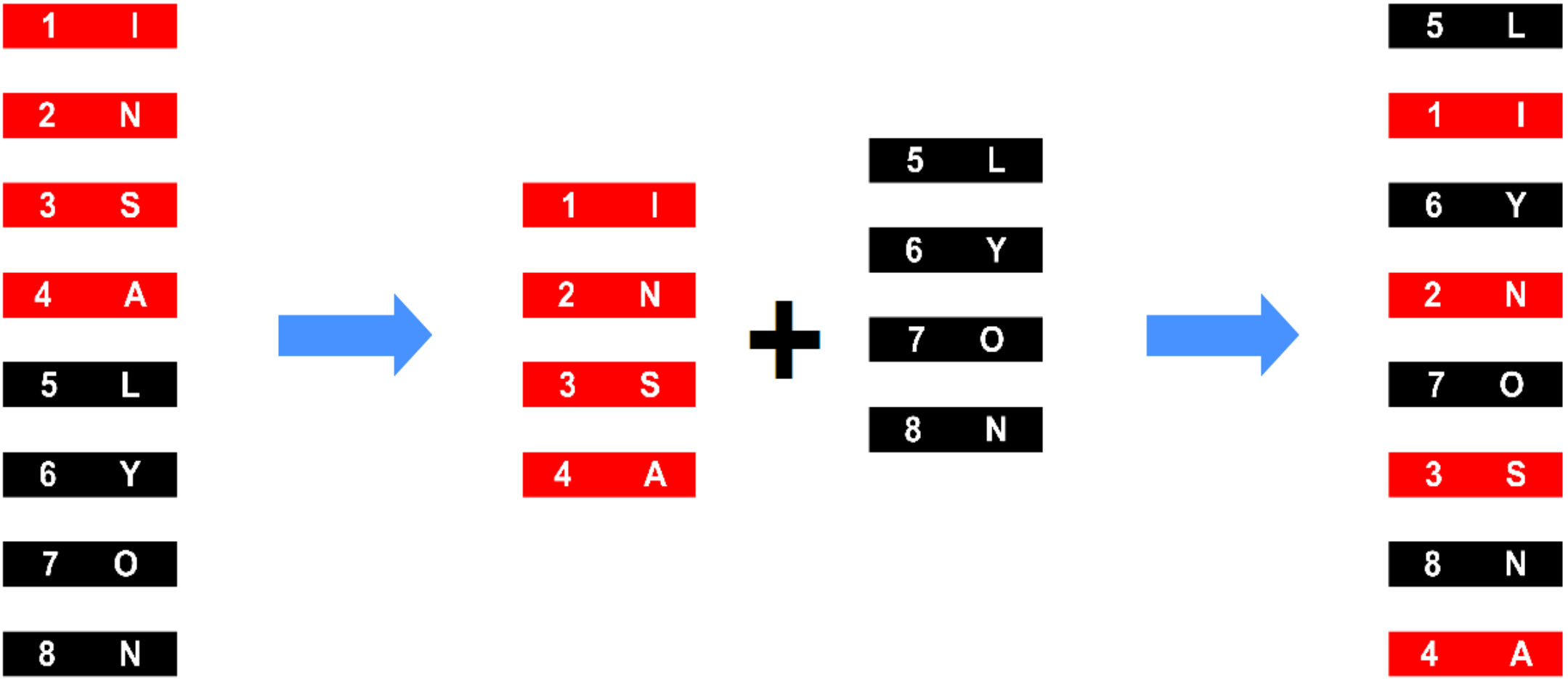
Chiffrement

On chiffre
avec *p* mélanges

Déchiffrement

On déchiffre
avec $q = r - p$ mélanges

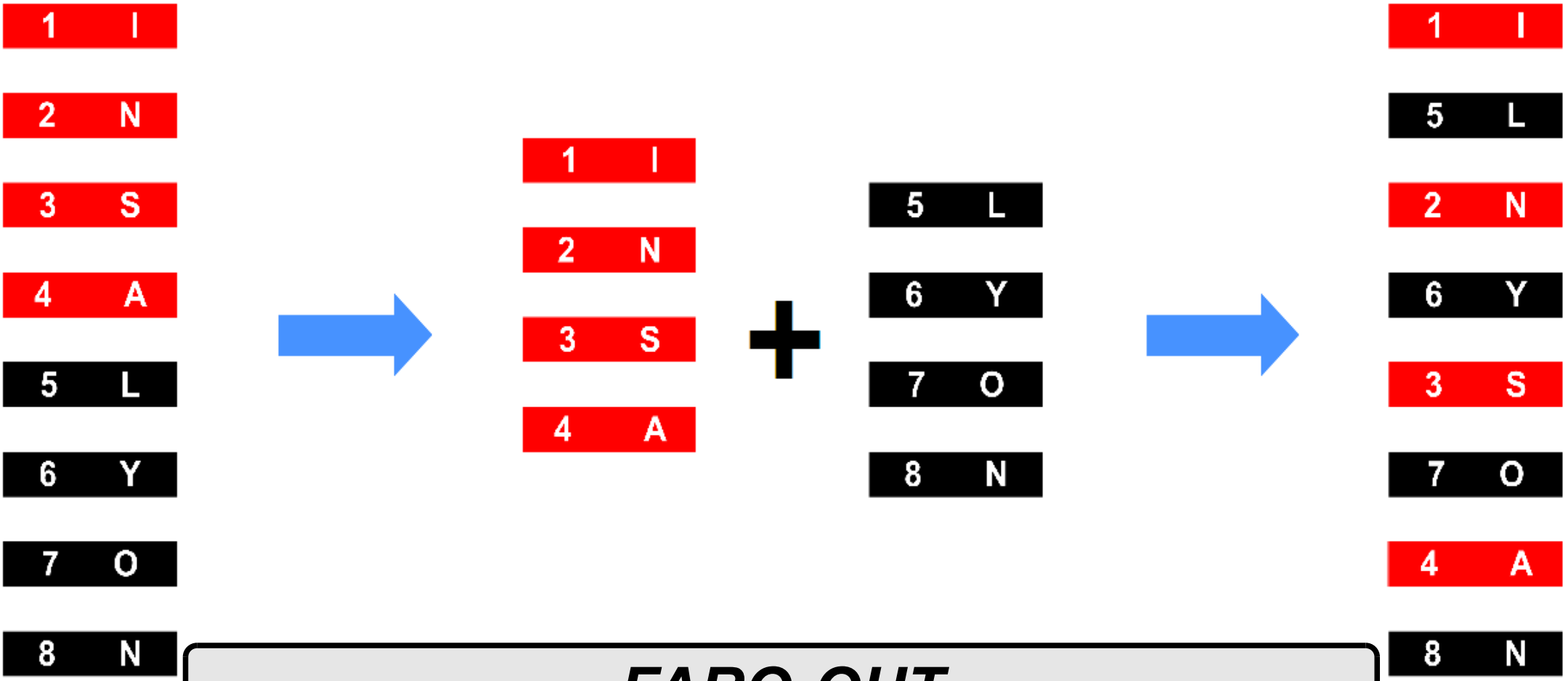
Complément : « Faro-in » et « Faro-out »



FARO-IN

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

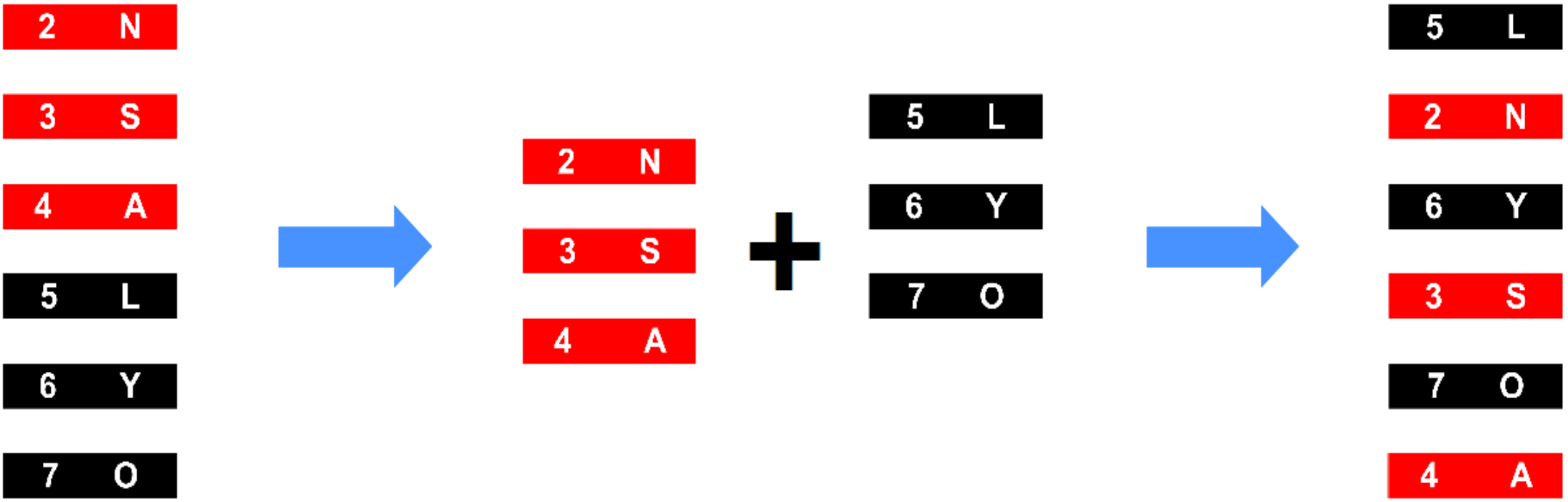
Complément : « Faro-in » et « Faro-out »



FARO-OUT

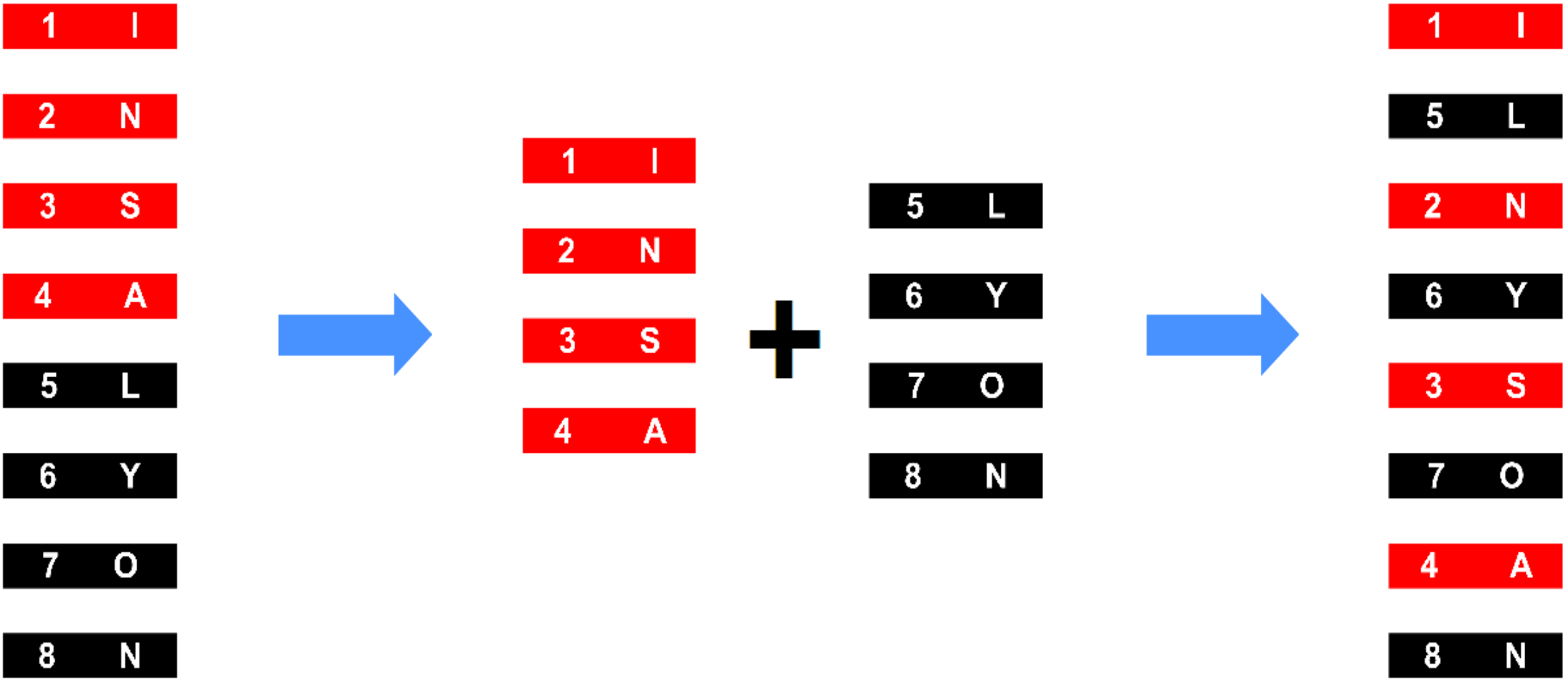
La première carte rouge est insérée
au-dessus **de la première carte noire**
Les deux cartes extrêmes restent immobiles !

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



FARO-IN équivalent
obtenu en retirant les deux cartes extrêmes

1er mélange Faro-out



Modélisation : une autre permutation

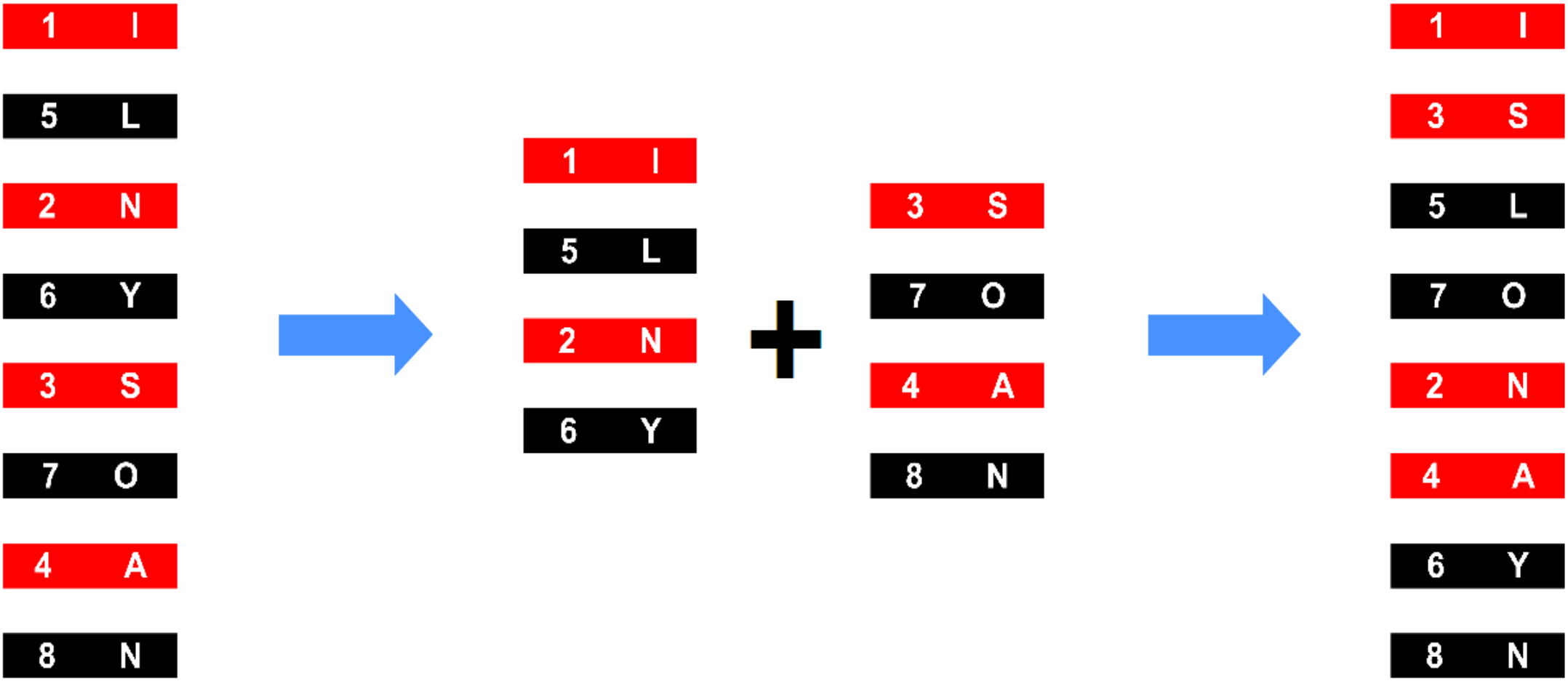
$$g:\{1,2,3,4,5,6,7,8\} \to \{1,2,3,4,5,6,7,8\}$$

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

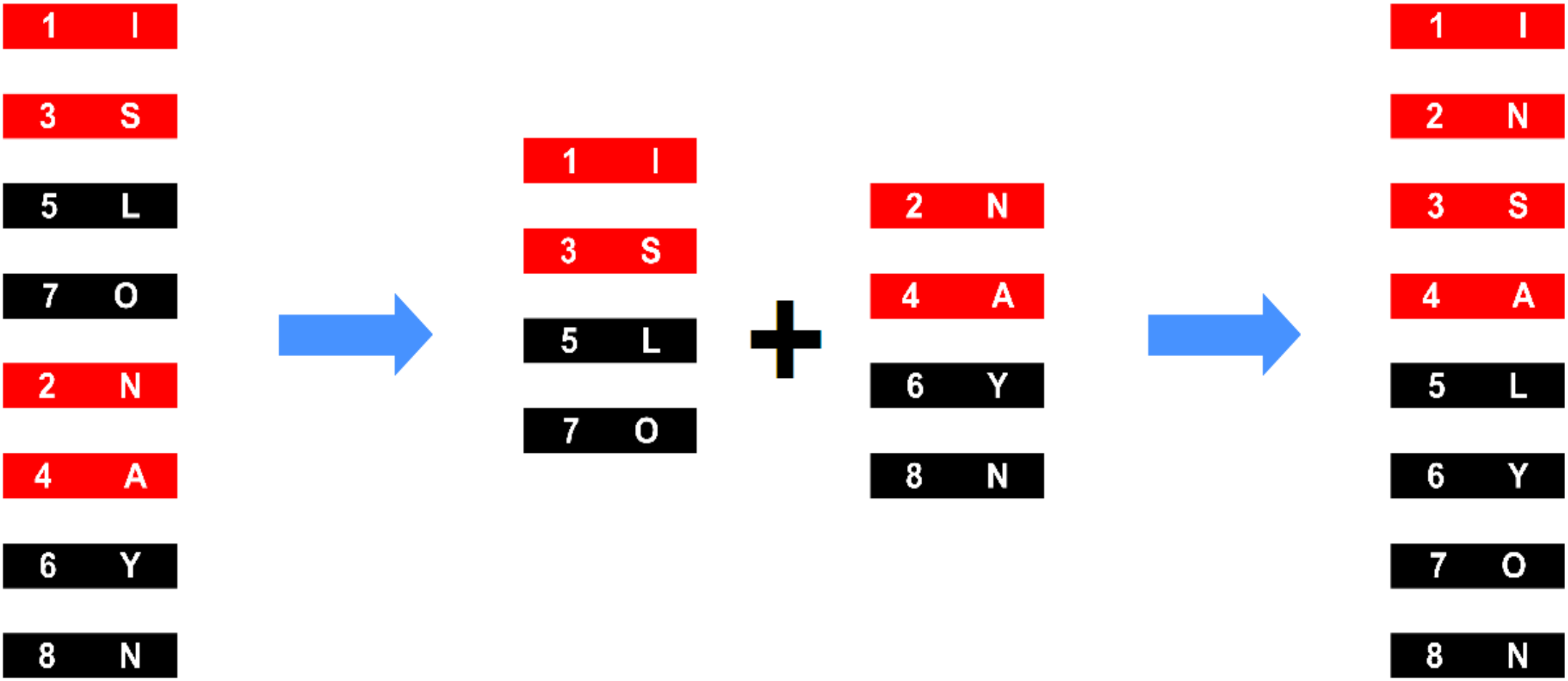
$$\begin{cases} g(1)=1 \\ g(2)=3 \\ g(3)=5 \\ g(4)=7 \end{cases} \qquad \begin{cases} g(5)=2 \equiv 9 \ [\text{mod } 7] \\ g(6)=4 \equiv 11 \ [\text{mod } 7] \\ g(7)=6 \equiv 13 \ [\text{mod } 7] \\ g(8)=8 \equiv 15 \ [\text{mod } 7] \end{cases}$$

$$g(i)=\begin{cases} 2i-1 & \text{si } i \leqslant 4 \\ 2i-8 & \text{si } i \geqslant 5 \end{cases} \equiv 2i-1 \ [\text{mod } 7]$$

2e mélange Faro-out

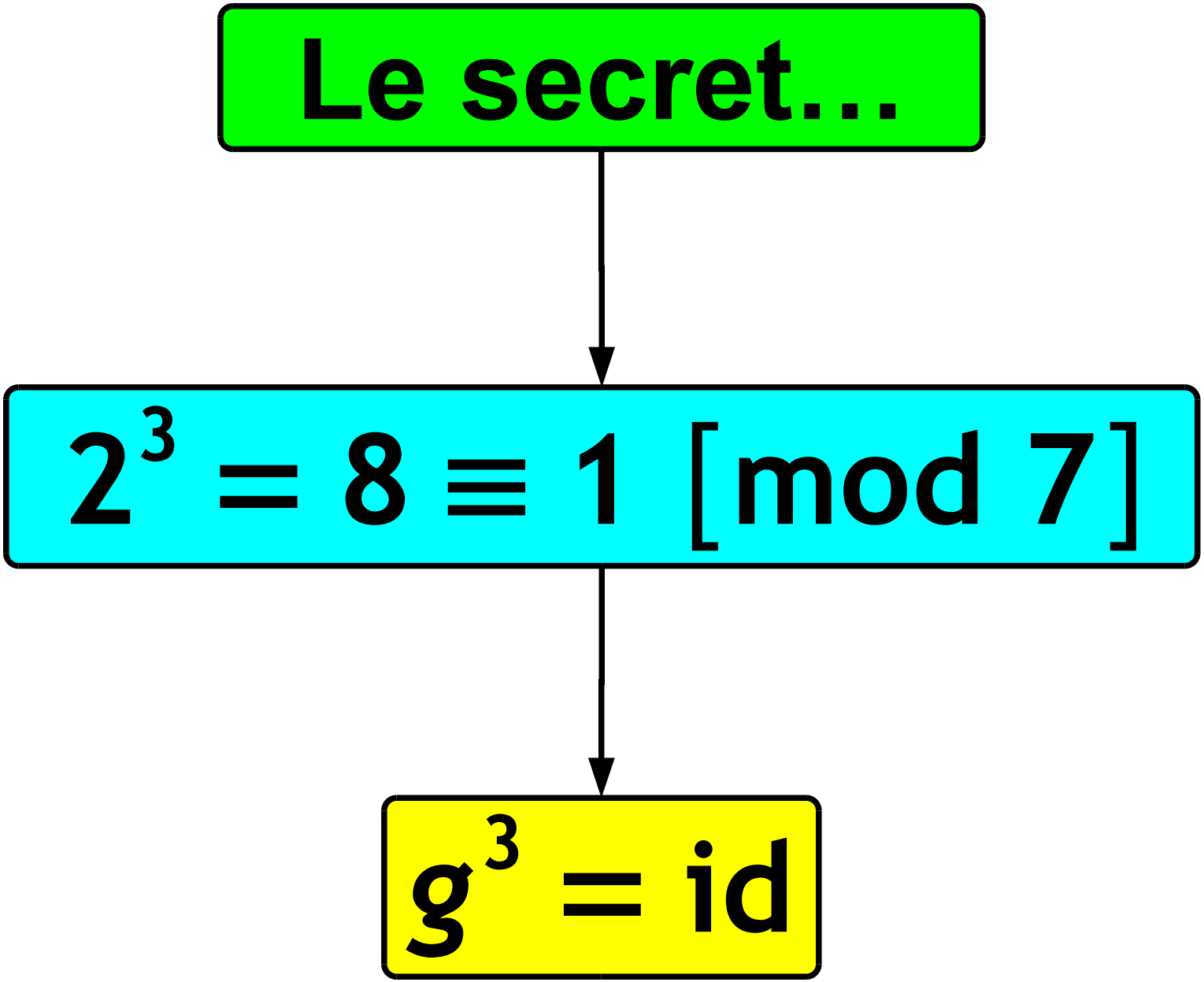


3e mélange Faro-out



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

Modélisation : une période

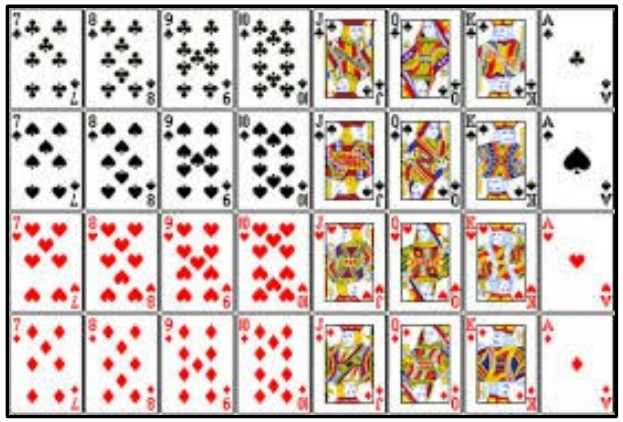


Généralisation

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

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

$$f(i) = \begin{cases} 2i & \text{si } i \leqslant 4 \\ 2i - 9 & \text{si } i \geqslant 5 \end{cases} \equiv 2i \ [\text{mod } 9]$$

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

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

$$\begin{cases} f(0)=1 \\ f(1)=3 \\ f(2)=5 \\ f(3)=7 \end{cases} \qquad \begin{cases} f(4)=0 \\ f(5)=2 \\ f(6)=4 \\ f(7)=6 \end{cases}$$

$$f(i)=\begin{cases} 2i+1 & \text{si } i \leqslant 3 \\ 2i-8 & \text{si } i \geqslant 4 \end{cases} \equiv 2i+1 \ [\text{mod } 9]$$

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

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

$$\begin{cases} f(000)=001 \\ f(001)=011 \\ f(010)=101 \\ f(011)=111 \end{cases} \qquad \begin{cases} f(100)=000 \\ f(101)=010 \\ f(110)=100 \\ f(111)=110 \end{cases}$$

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

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

Approche binaire : Faro-in

$$f\left((abc)_2\right) = (bc\bar{a})_2$$
$$f^2\left((abc)_2\right) = (c\bar{a}\bar{b})_2$$
$$f^3\left((abc)_2\right) = (\bar{a}\bar{b}\bar{c})_2$$
$$f^4\left((abc)_2\right) = (\bar{b}\bar{c}a)_2$$
$$f^5\left((abc)_2\right) = (\bar{c}ab)_2$$
$$f^6\left((abc)_2\right) = (abc)_2$$

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

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

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

Approche binaire : Faro-out

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

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

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

$$g(i)=\begin{cases} 2i-1 & \text{si } i \leqslant 4 \\ 2i-8 & \text{si } i \geqslant 5 \end{cases} \equiv 2i-1 \ [\text{mod } 7]$$

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

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

$$\begin{cases} g(0)=0 \\ g(1)=2 \\ g(2)=4 \\ g(3)=6 \end{cases} \qquad \begin{cases} g(4)=1 \\ g(5)=3 \\ g(6)=5 \\ g(7)=7 \end{cases}$$

$$g(i)=\begin{cases} 2i & \text{si } i \leqslant 3 \\ 2i-7 & \text{si } i \geqslant 4 \end{cases} \equiv 2i \ [\text{mod } 7]$$

Approche binaire : Faro-out Renumérotation

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

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

$$\begin{cases} g(000)=000 \\ g(001)=010 \\ g(010)=100 \\ g(011)=110 \end{cases} \qquad \begin{cases} g(100)=001 \\ g(101)=011 \\ g(110)=101 \\ g(111)=111 \end{cases}$$

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

$$g(i)=g\left((abc)_2\right)=(bca)_2$$

Approche binaire : Faro-out

$$g\left((abc)_2\right) = (bca)_2$$
$$g^2\left((abc)_2\right) = (cab)_2$$
$$g^3\left((abc)_2\right) = (abc)_2$$

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

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

Généralisation

Théorème : **pour un jeu de 2^p cartes,**

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

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

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

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

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

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

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

Moralité :

MERCI DE VOTRE ATTENTION !