Mélanges Faros (exposé didactique - INSA LYON)

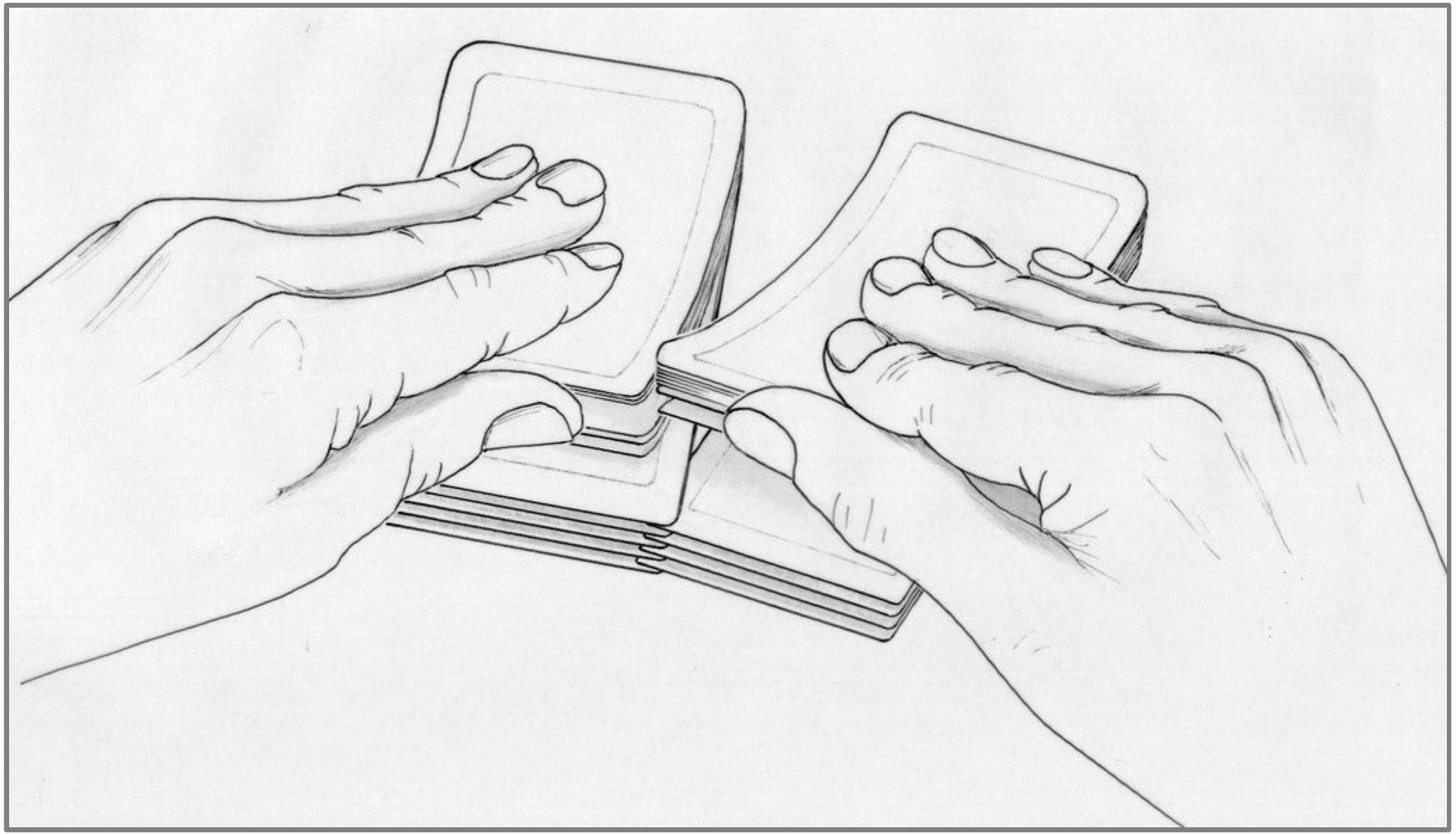
Aimé Lachal

INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
LYON

Mélanges Faros

« Mélange américain » ou « Riffle shuffle »

« Mélange Pharaon » ou « Faro »



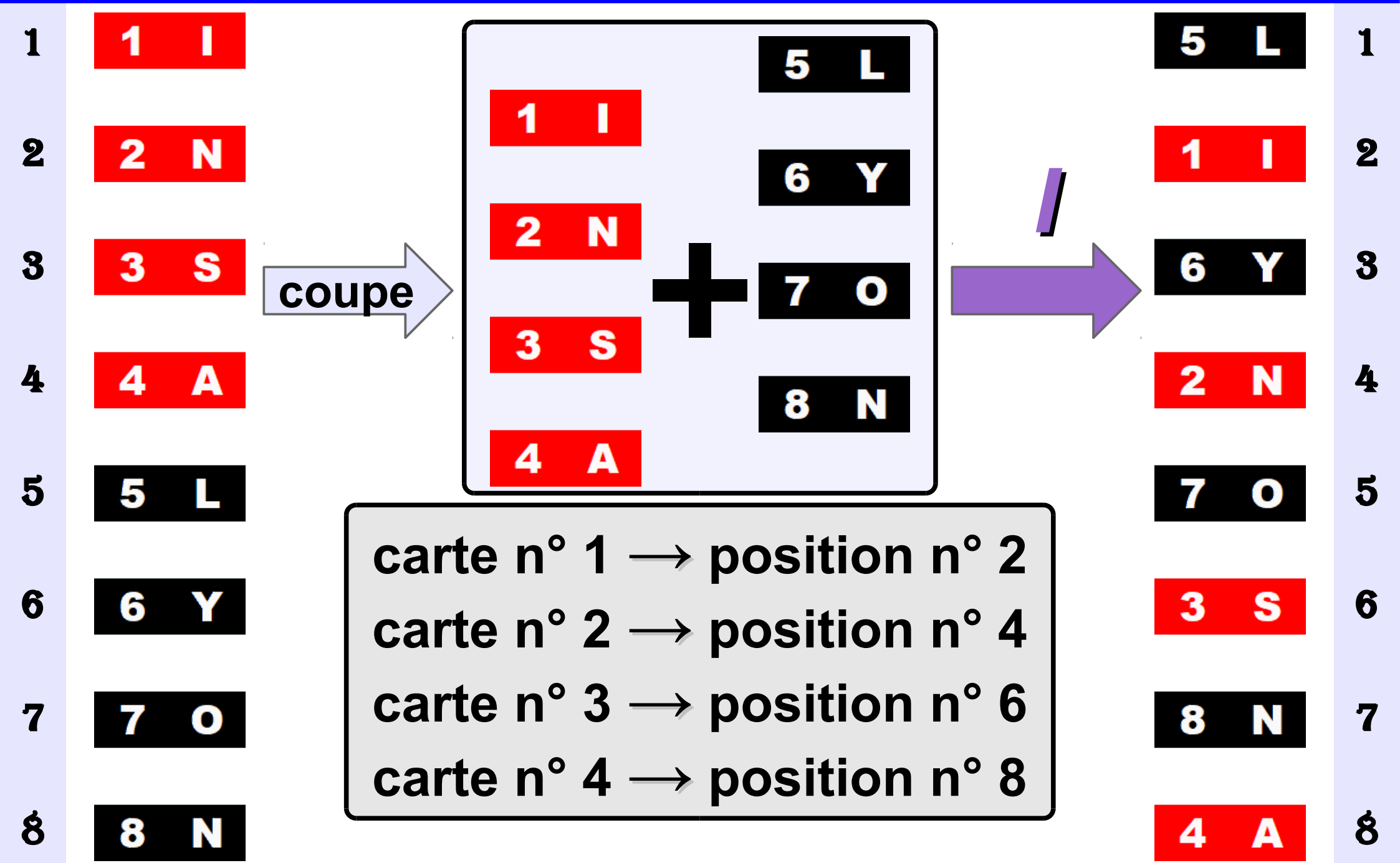
CASINO ROYAL

MODÉLISATION


INSA
LYON

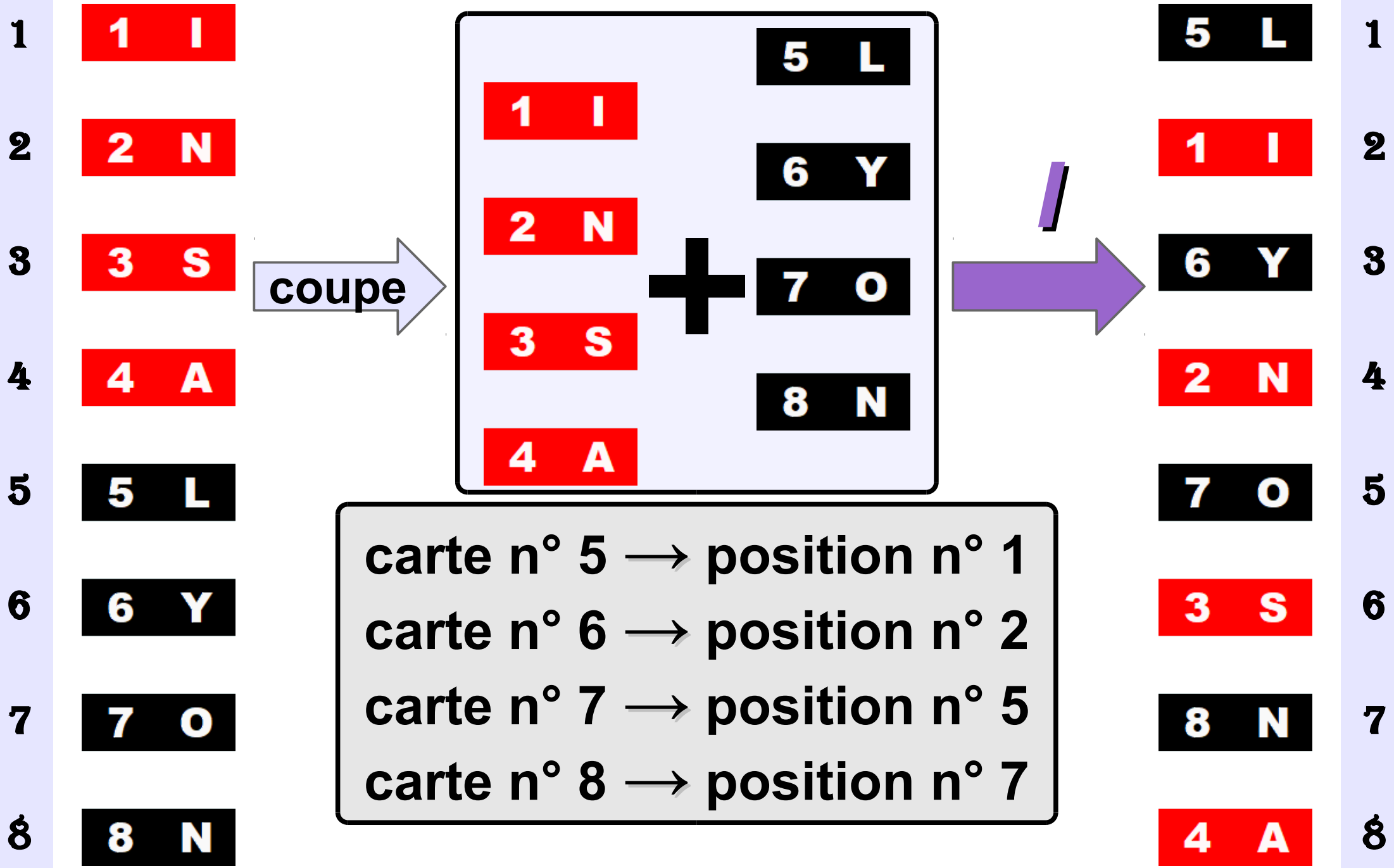
FARO-IN

Mélange « Faro-in »



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

Mélange « Faro-in »



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

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

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

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

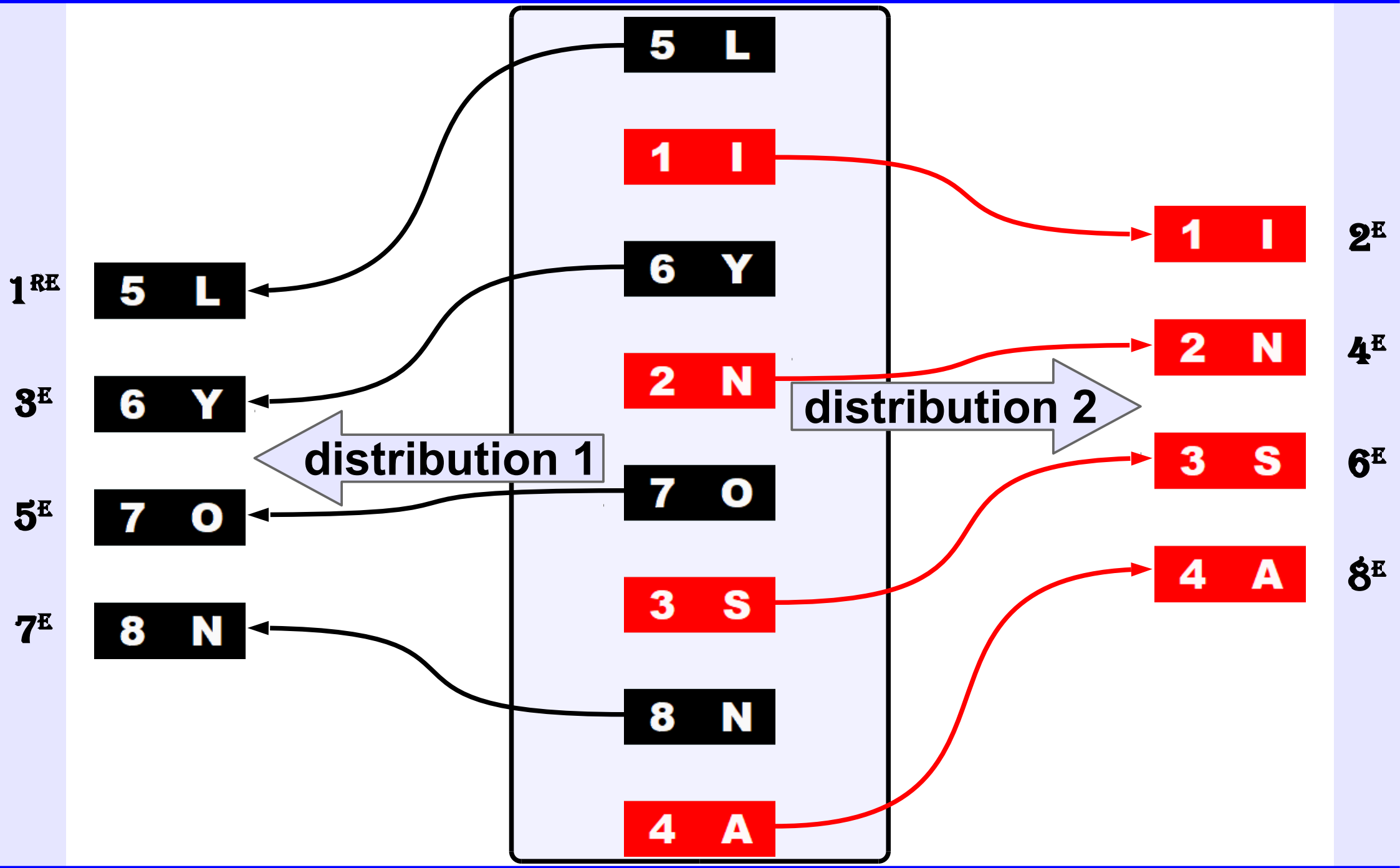
Modélisation : et sa réciproque

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

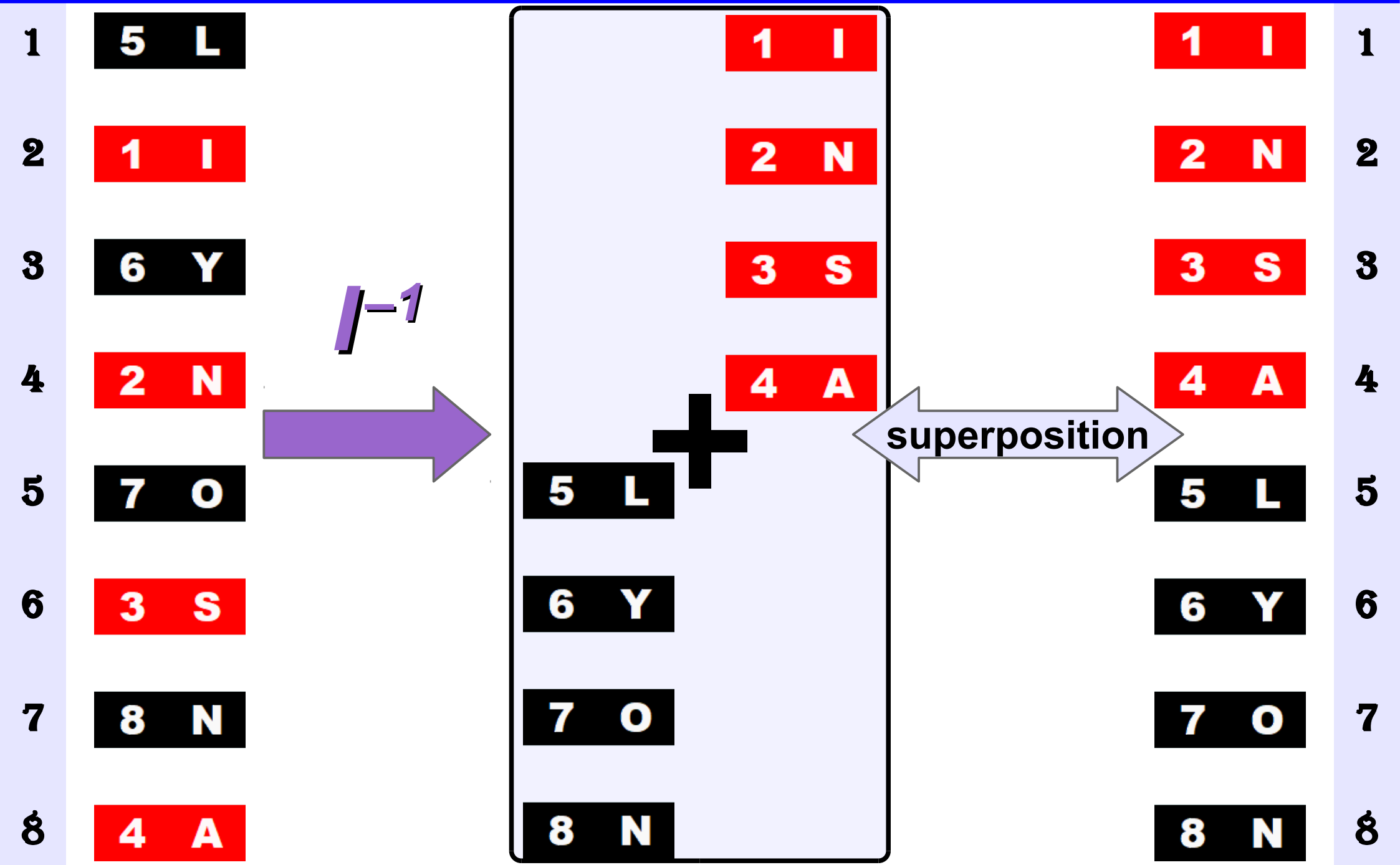
$$\Rightarrow \quad \begin{cases} f^{-1}(1)=5 \\ f^{-1}(2)=1 \\ f^{-1}(3)=6 \\ f^{-1}(4)=2 \end{cases} \quad \begin{cases} f^{-1}(5)=7 \\ f^{-1}(6)=3 \\ f^{-1}(7)=8 \\ f^{-1}(8)=4 \end{cases}$$

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

Mélange « anti-Faro-in » : donne équitable

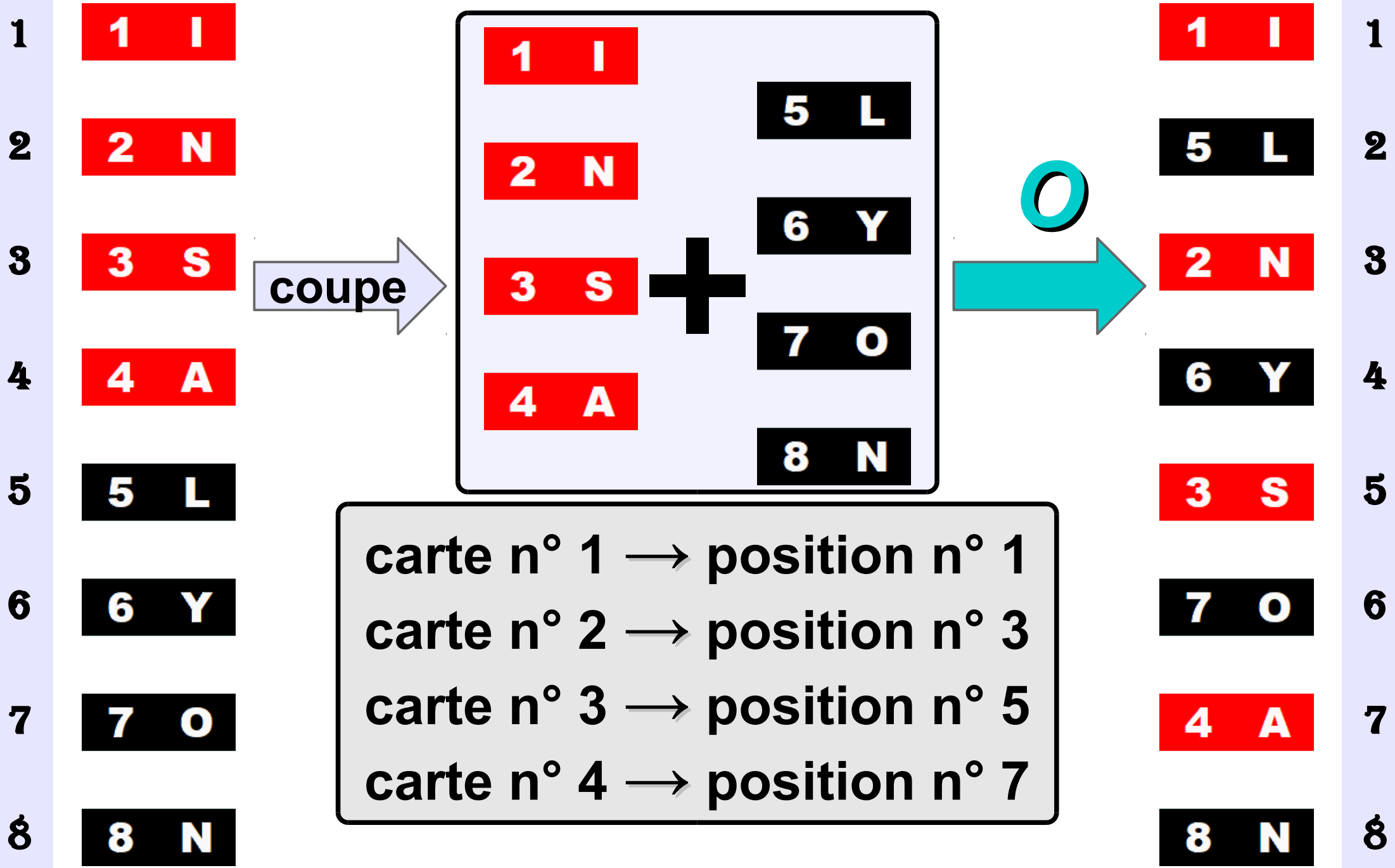


Mélange « anti-Faro-in » : donne équitable



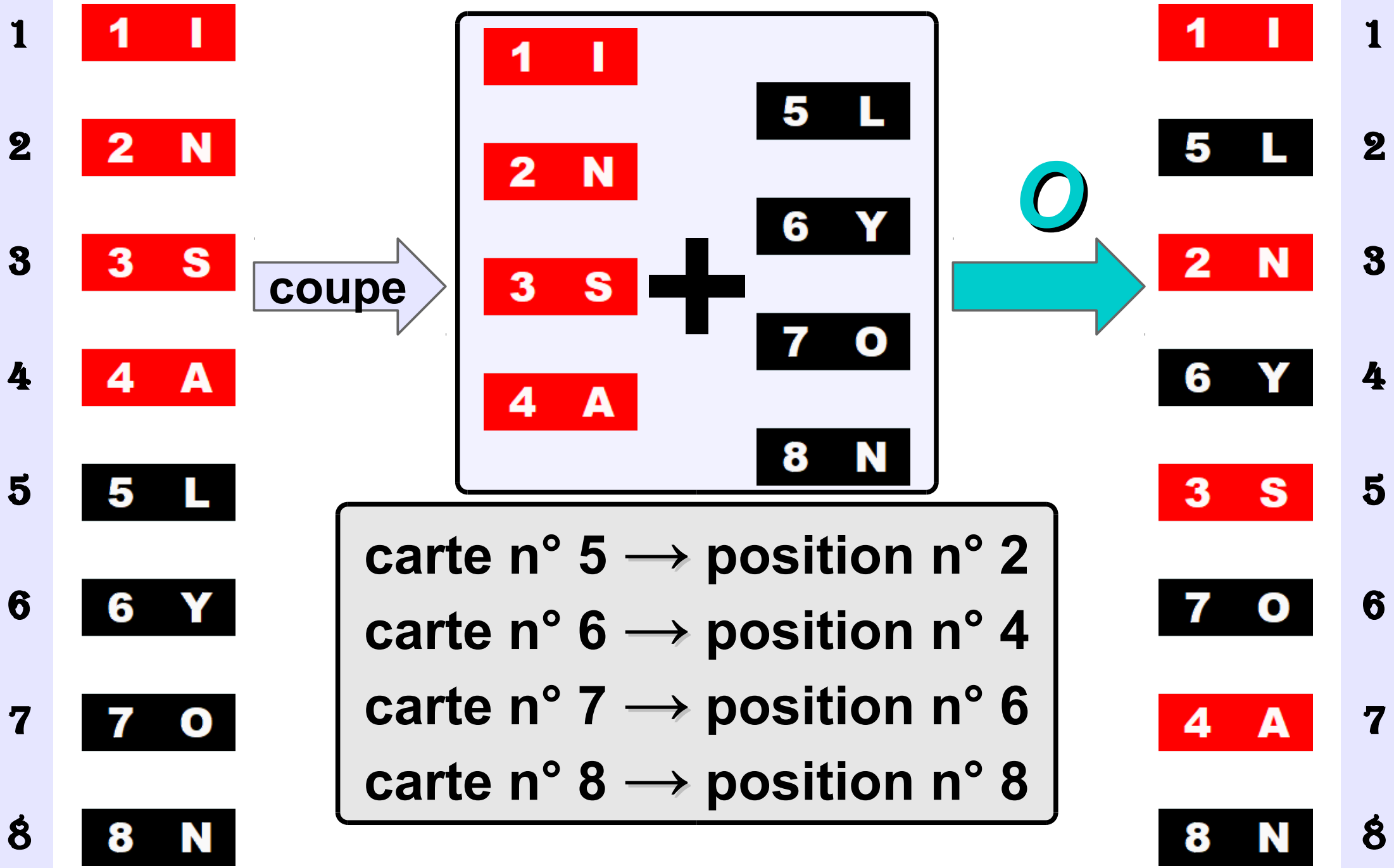
FARO-OUT

Mélange « Faro-out »



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

Mélange « Faro-out »



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

Modélisation : une autre permutation

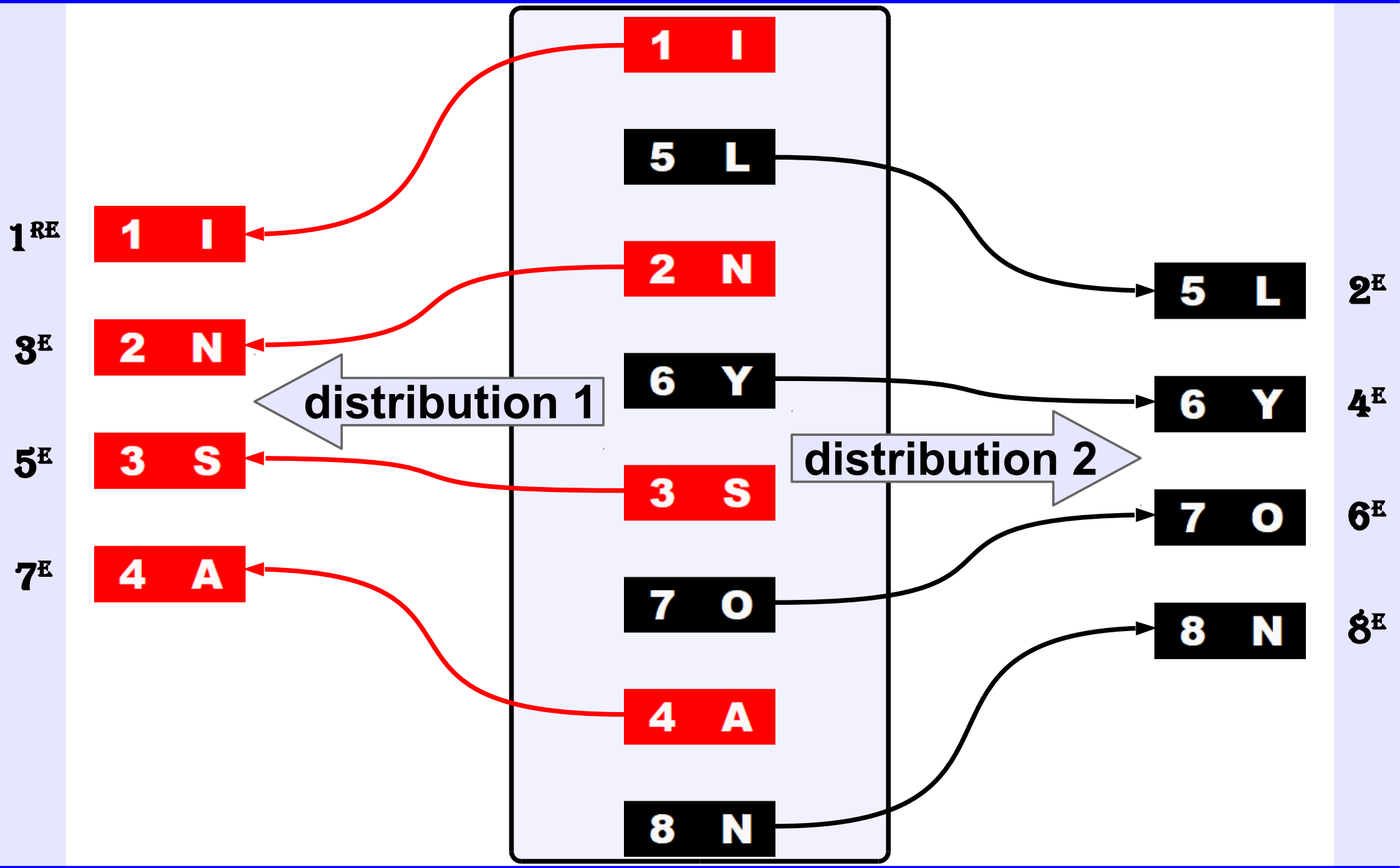
$$g : \{1,2,3,4,5,6,7,8\} \to \{1,2,3,4,5,6,7,8\}$$

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

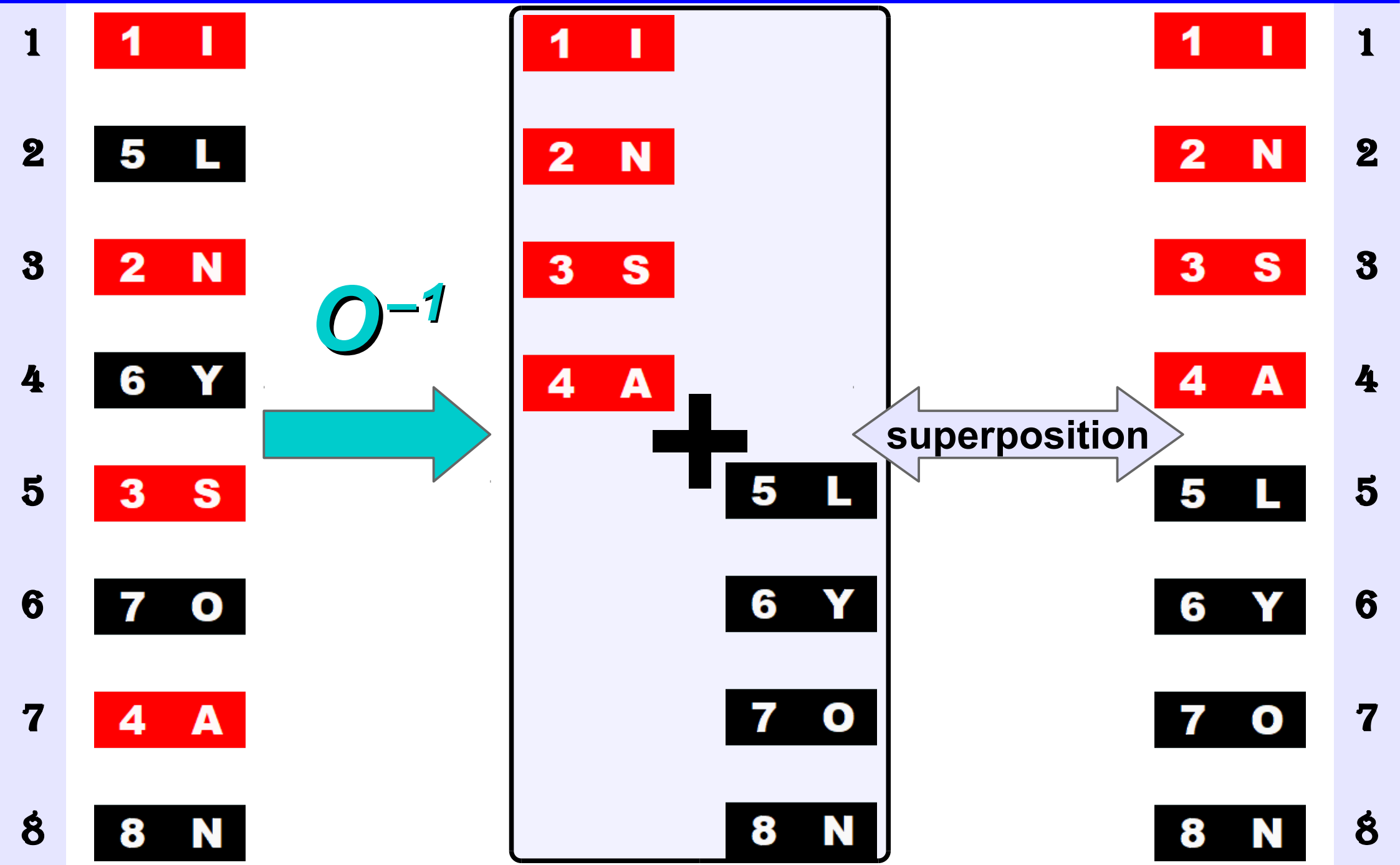
$$\begin{cases} g(1) = 1 \\ g(2) = 3 \\ g(3) = 5 \\ g(4) = 7 \end{cases} \qquad \begin{cases} g(5) = 2 \equiv 9 \pmod 7 \\ g(6) = 4 \equiv 11 \pmod 7 \\ g(7) = 6 \equiv 13 \pmod 7 \\ g(8) = 8 \equiv 15 \pmod 7 \end{cases}$$

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

Mélange « anti-Faro-out » : donne équitable

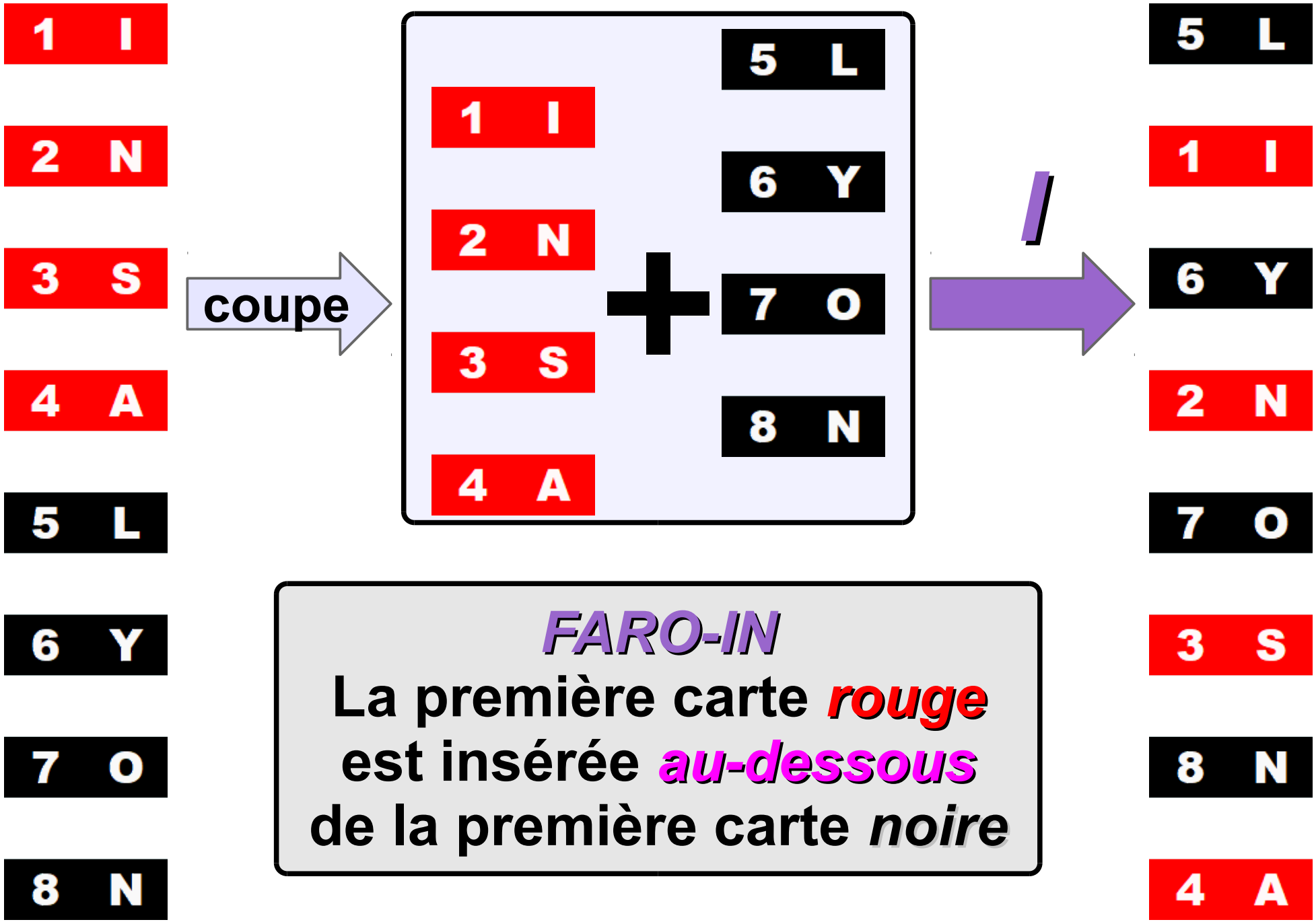


Mélange « anti-Faro-out » : donne équitable



COMPARAISON FARO-IN vs FARO-OUT

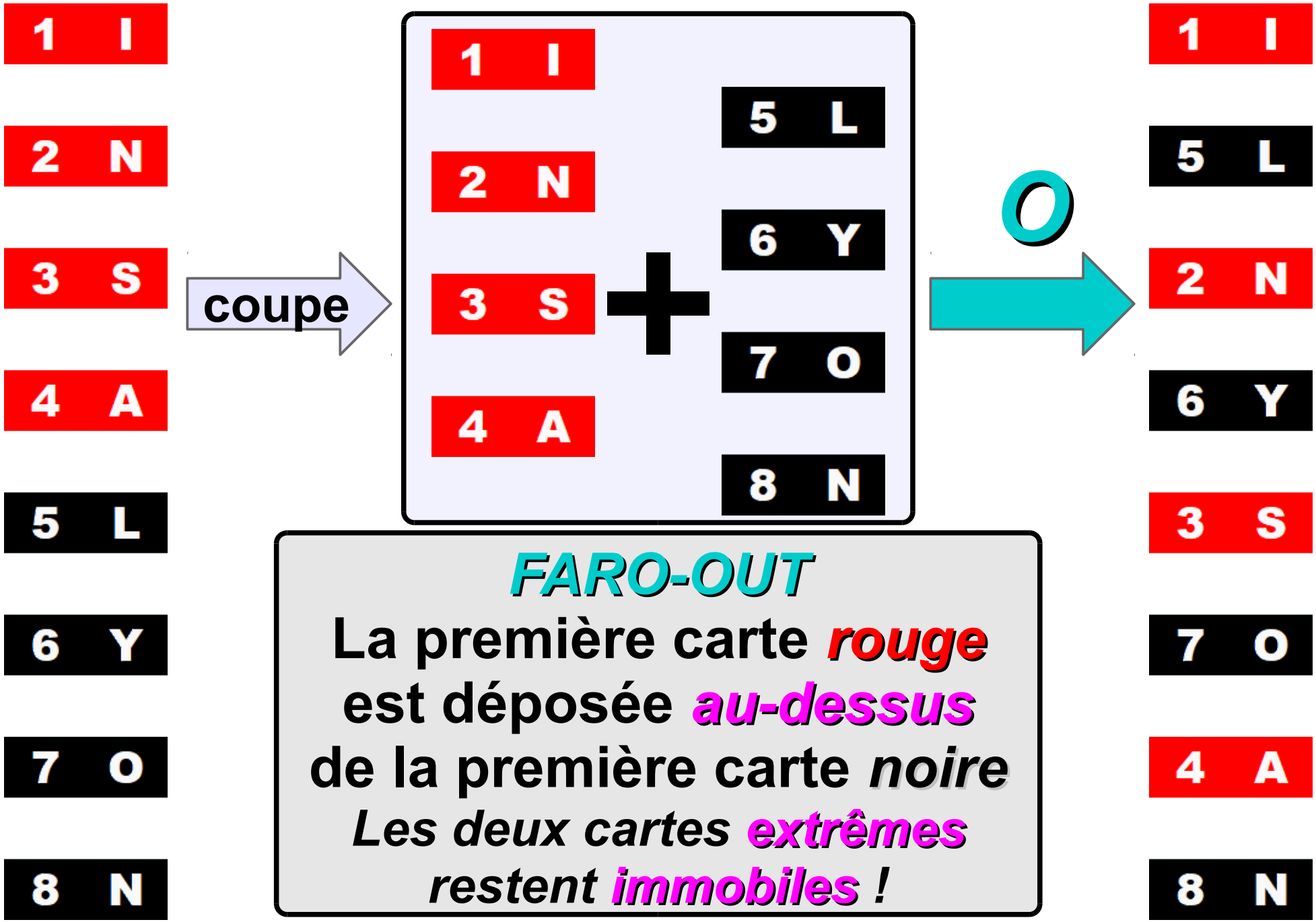
Comparaison : « Faro-in » et « Faro-out »



FARO-IN

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

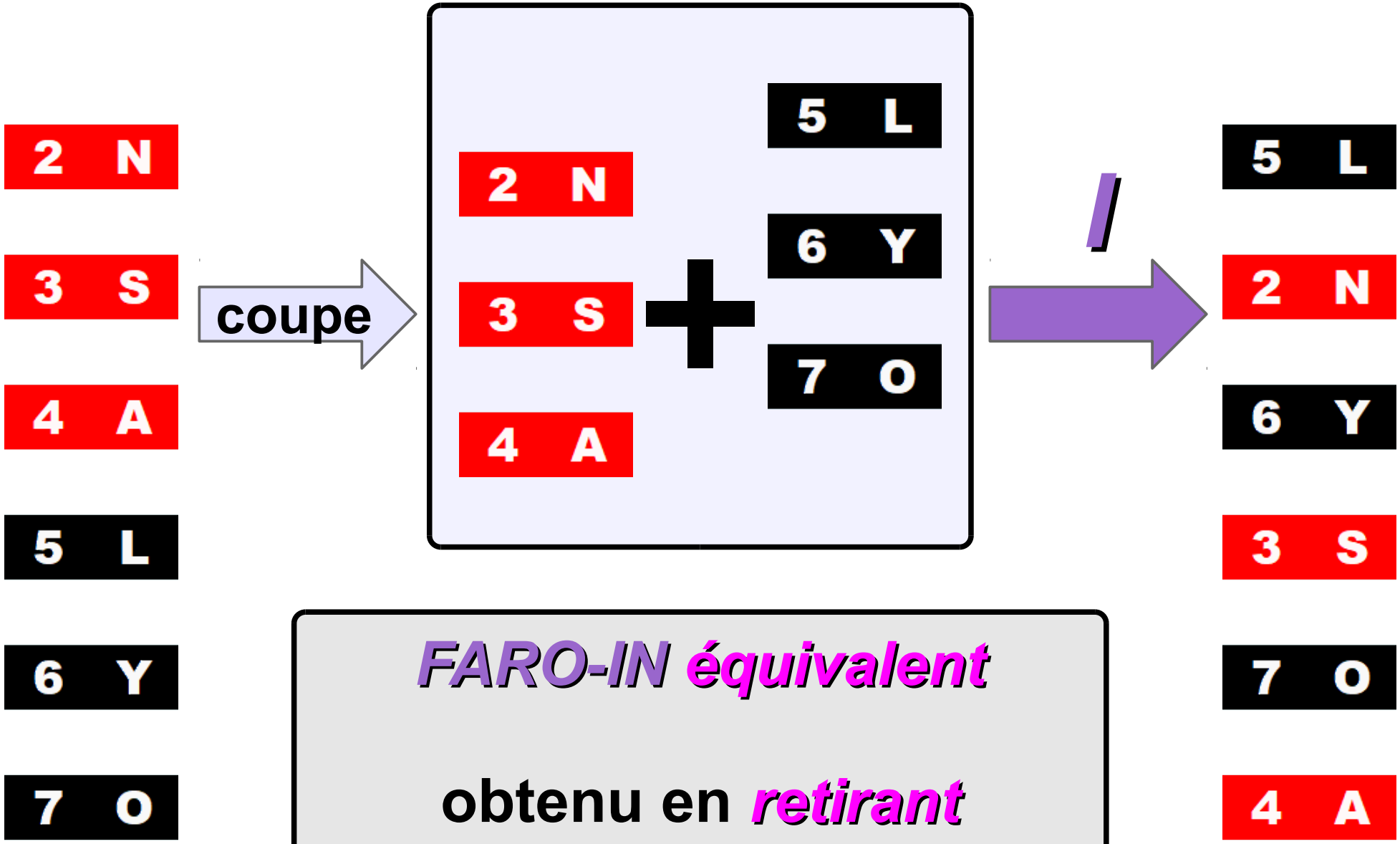
Comparaison : « Faro-in » et « Faro-out »



FARO-OUT

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

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



FARO-IN équivalent

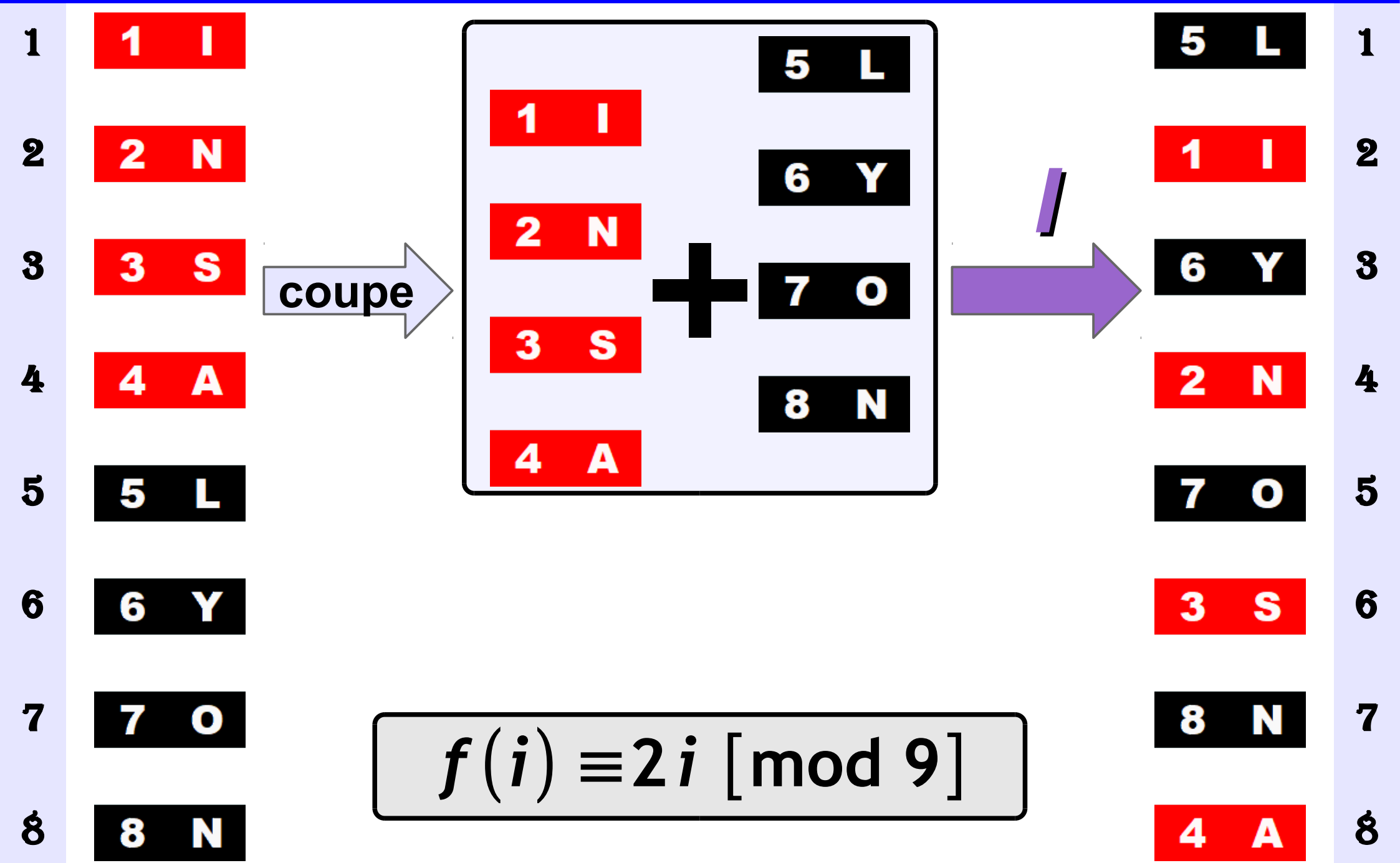
obtenu en **retirant**
les deux cartes **extrêmes**

CASINO ROYAL

ITÉRATIONS SUCCESSIVES

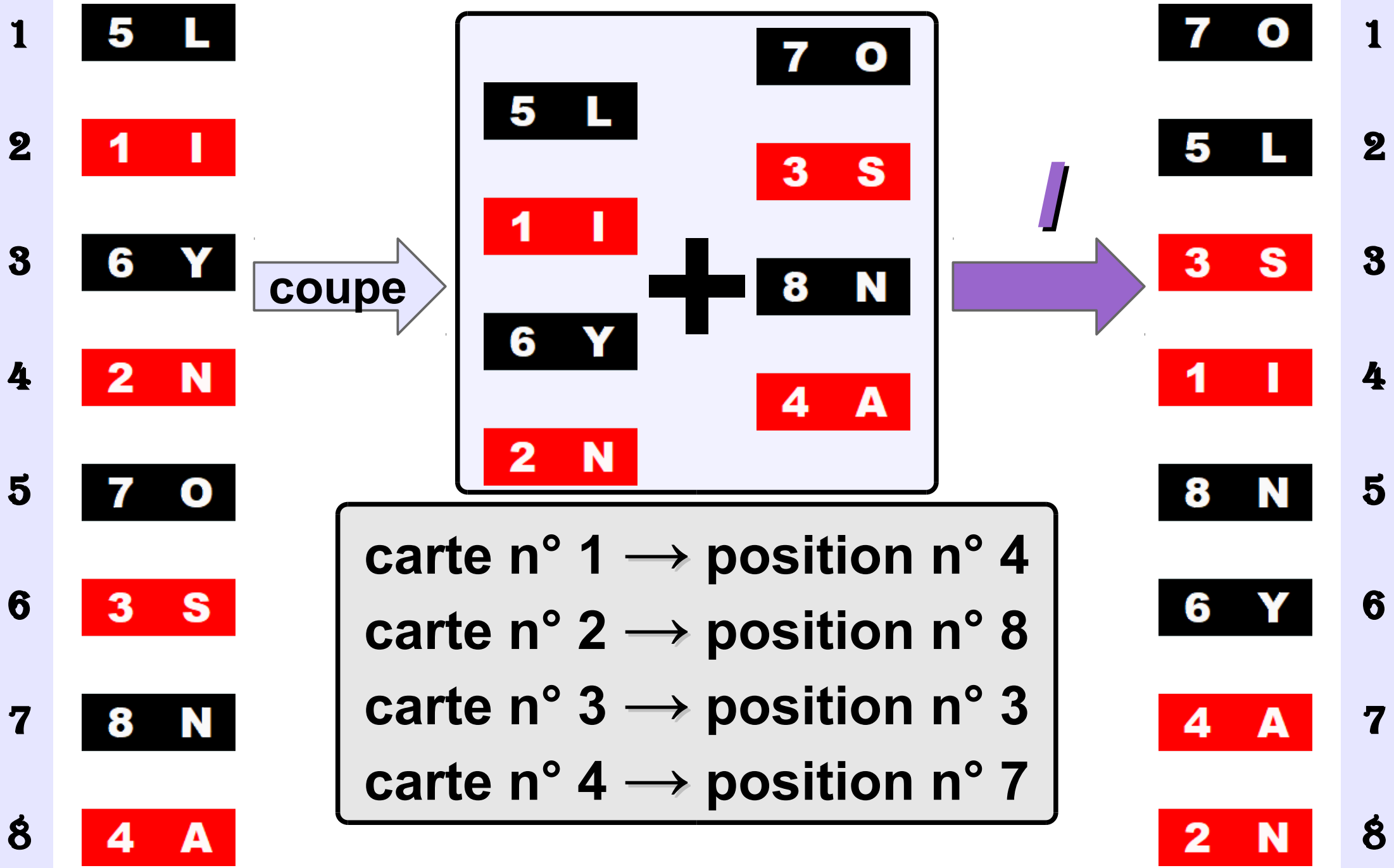
FAROS-IN

1er mélange « Faro-in »



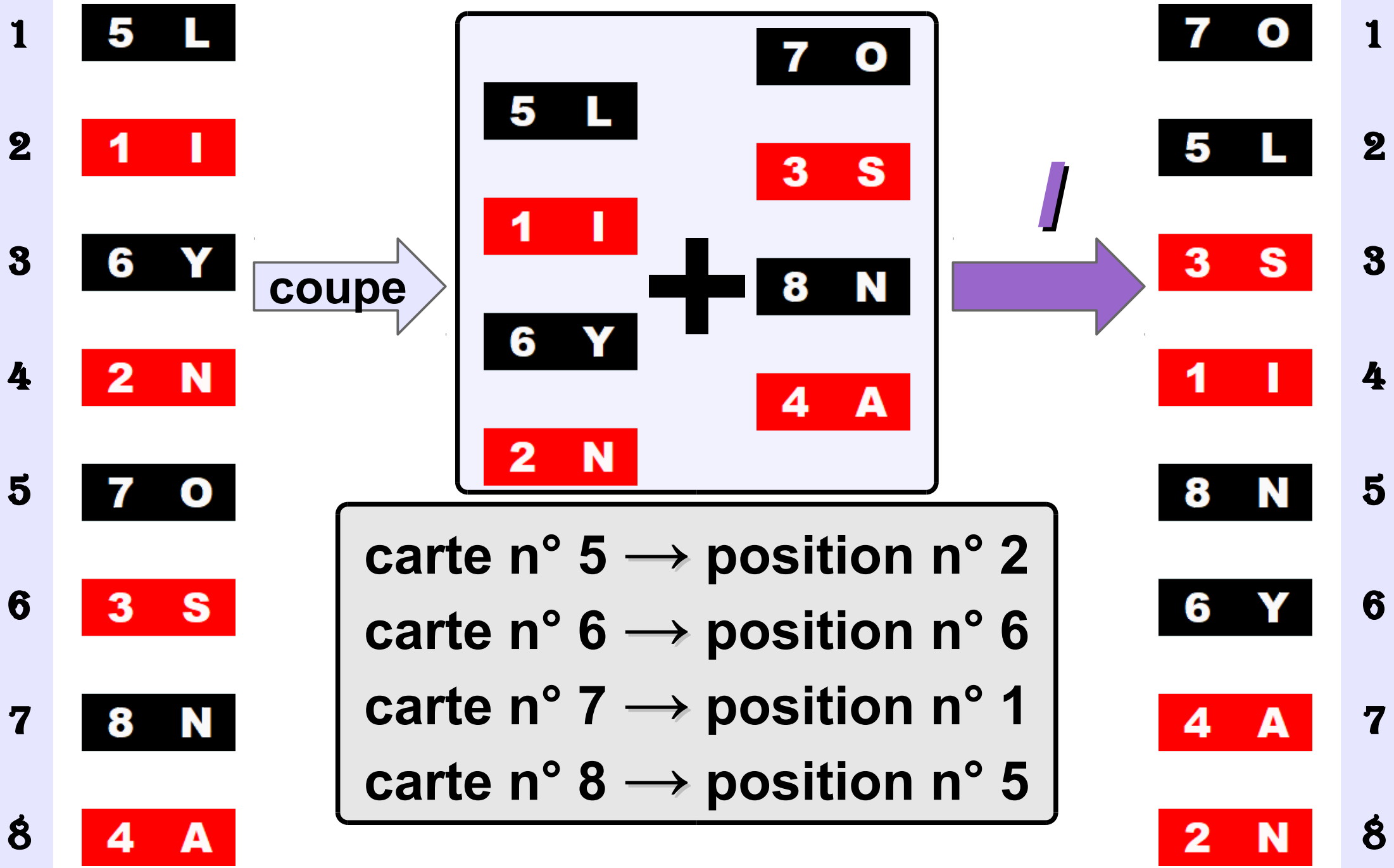
$$f(i) \equiv 2i \ [\mathrm{mod}\ 9]$$

2e mélange « Faro-in »



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 « Faro-in »



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 : $f^2 = f \circ f$

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

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

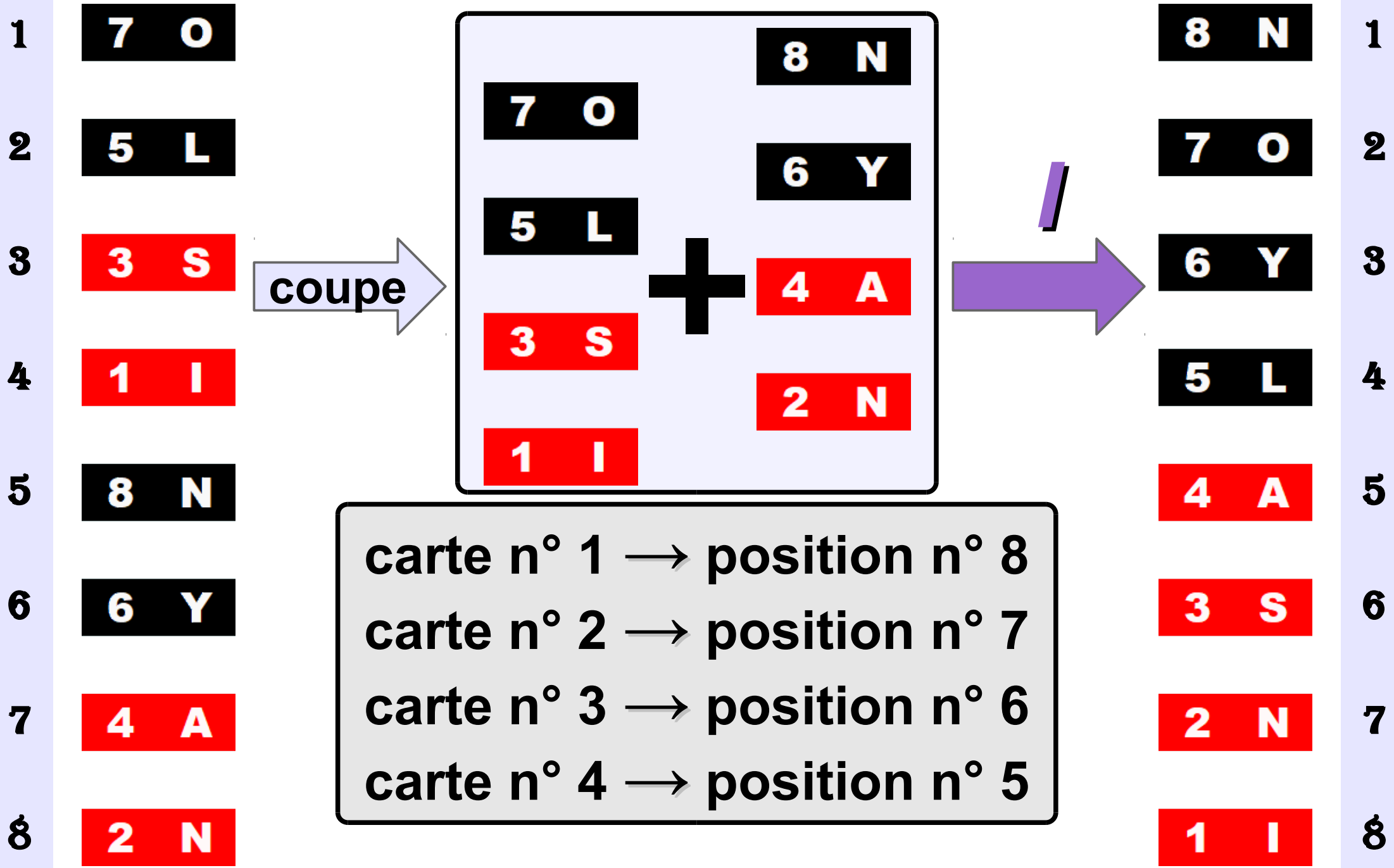
Modélisation : composition

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

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

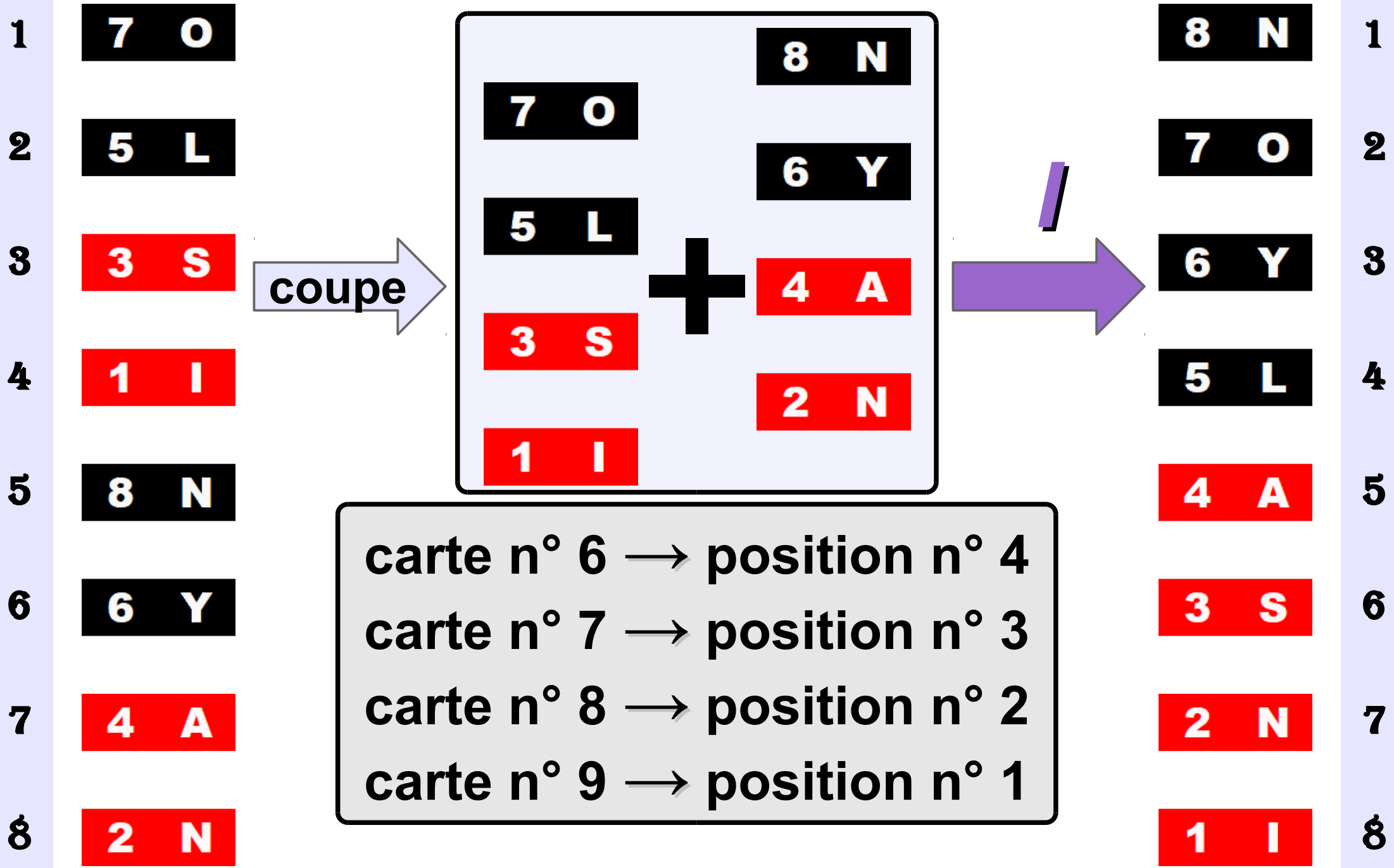
$$f^2(i) = f(f(i)) \equiv 4i \ [\text{mod } 9]$$

3e mélange « Faro-in »



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 « Faro-in »



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 et symétrie

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 et symétrie

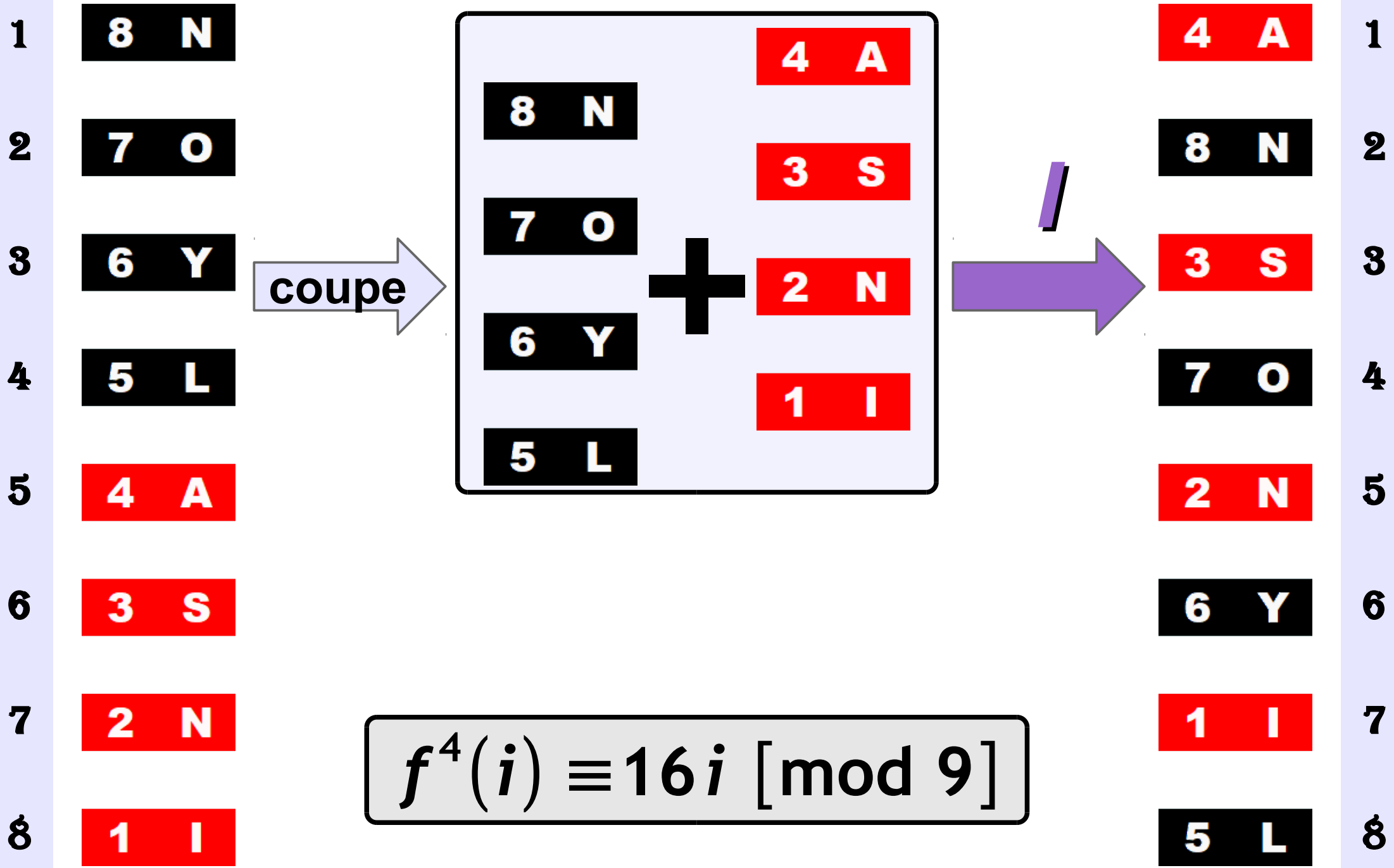
Notation : $f^3 = f \circ f \circ f$

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

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

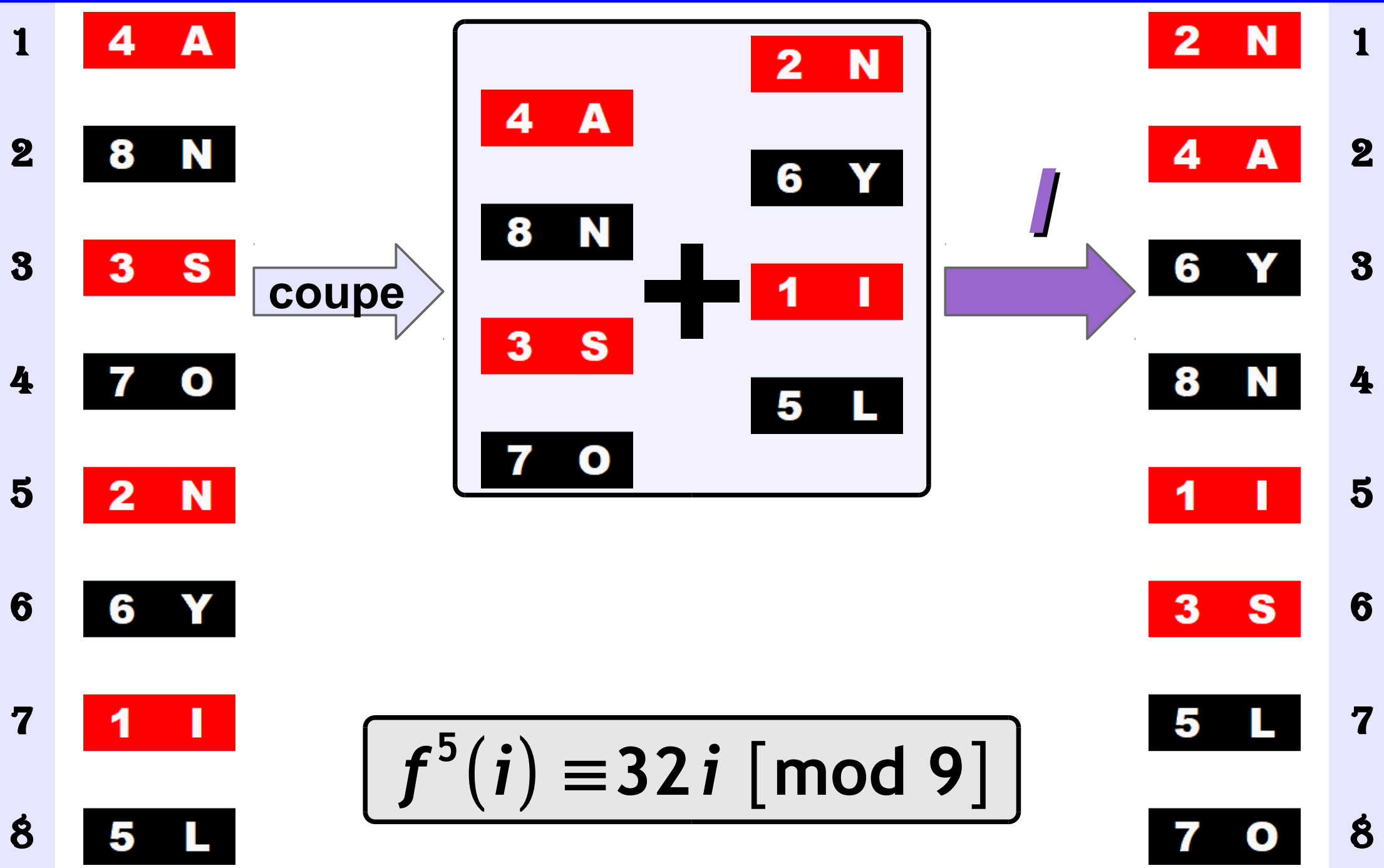
Au bout de 3 mélanges, le jeu est inversé…

4e mélange « Faro-in »



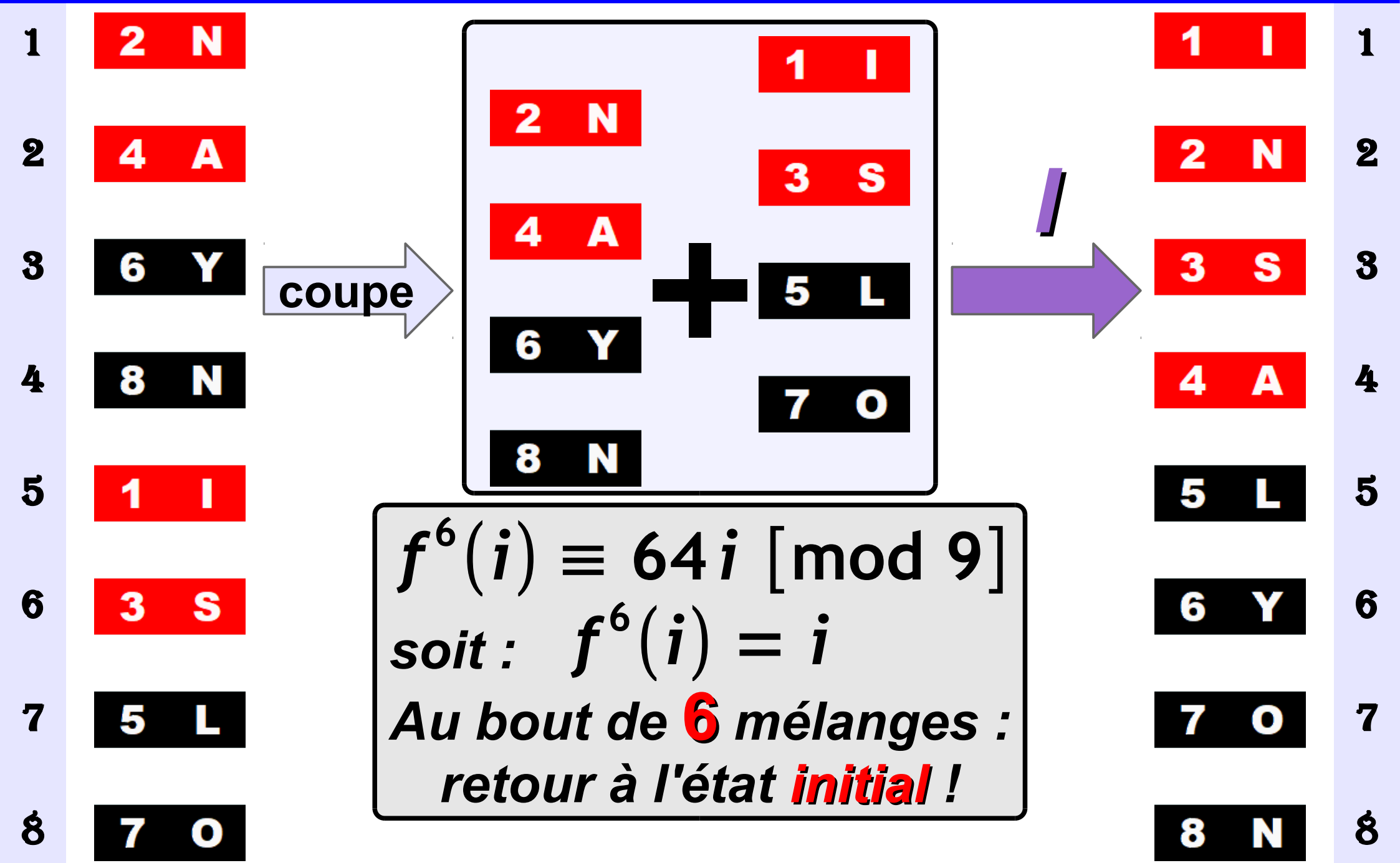
$$f^4(i) \equiv 16i \ [\mathrm{mod}\ 9]$$

5e mélange « Faro-in »



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

6e mélange « Faro-in »

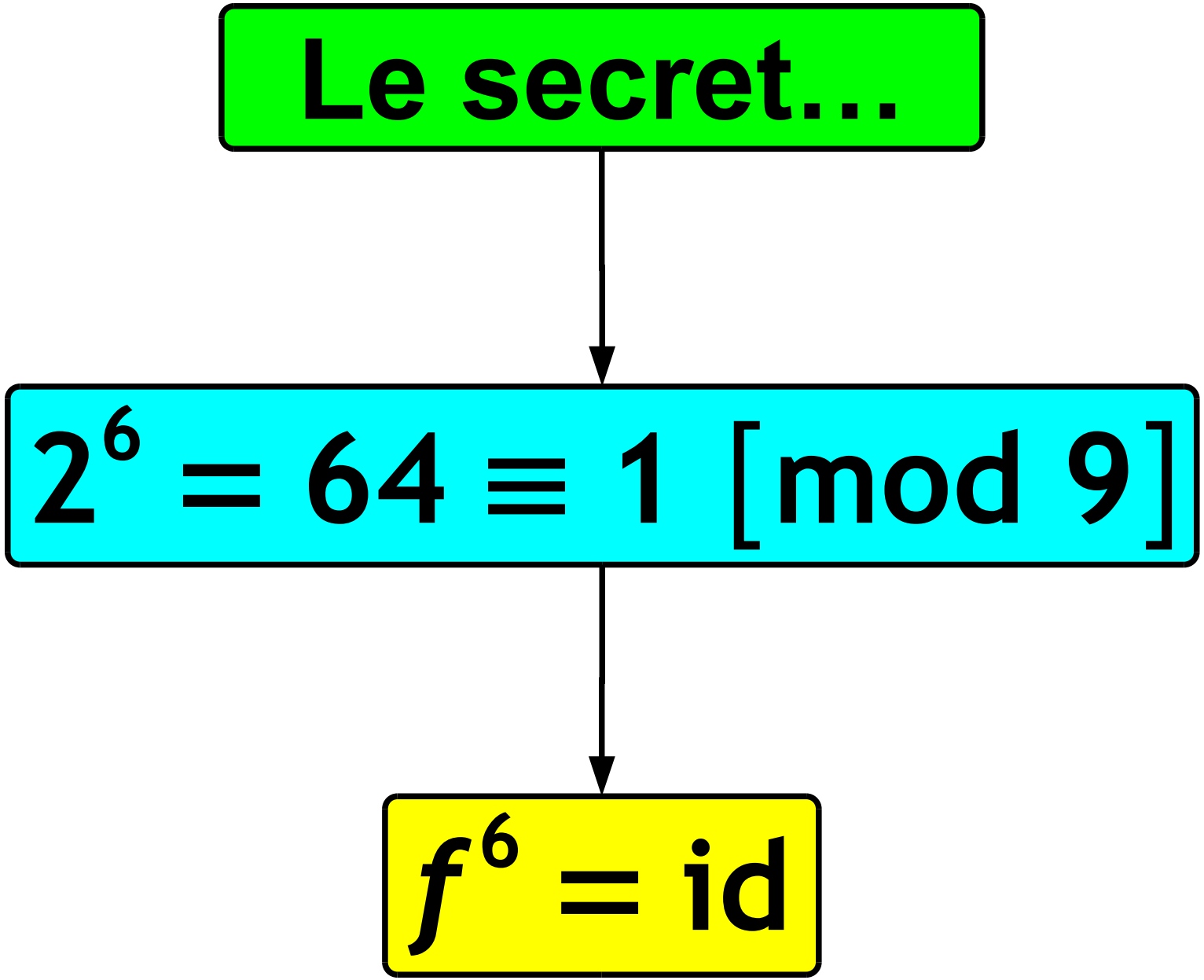


$$f^6(i) \equiv 64\,i \ [\mathrm{mod}\ 9]$$

soit : $f^6(i) = i$

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*…

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

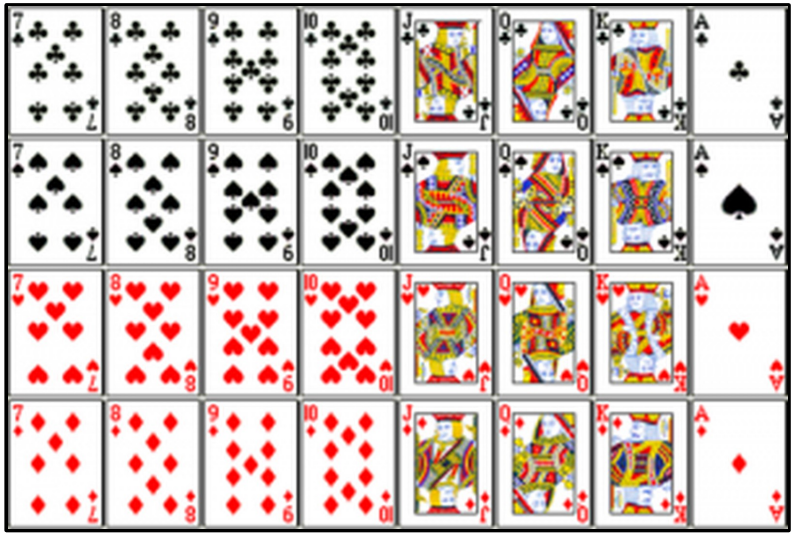
3e mélange : jeu *inversé*

Périodicité : généralisation

Théorème :

pour un jeu de 2^p cartes,

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



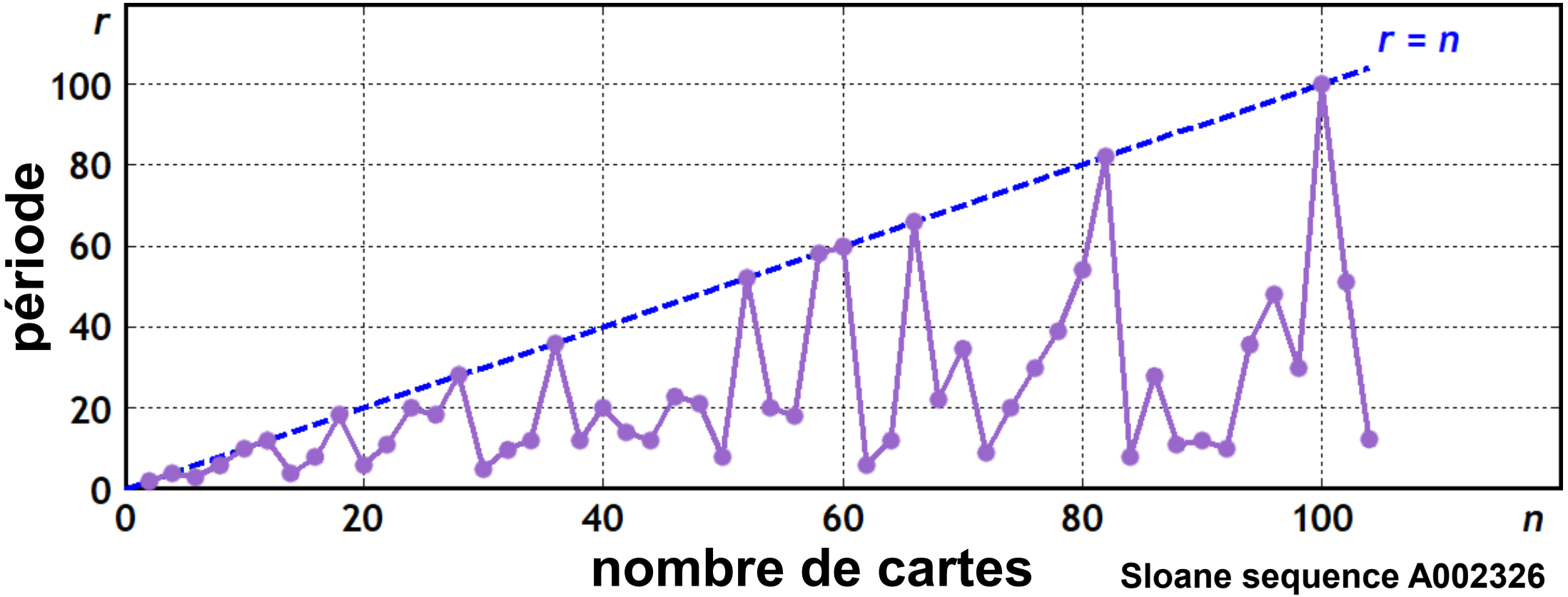
Exemple :

pour un jeu de 32 cartes,

10 mélanges Faros-in ramènent le jeu à son ordre initial

Périodicité : généralisation

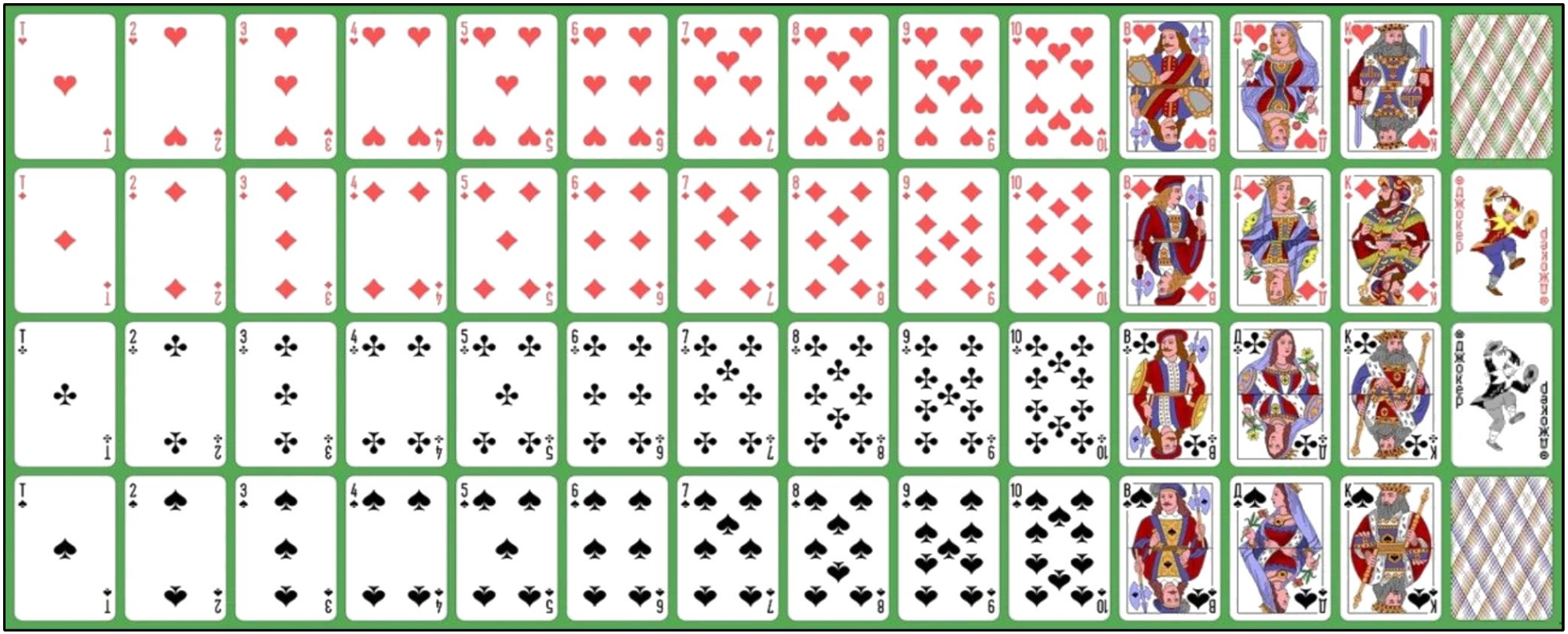
Théorème : **pour tout entier pair *n*,**
un jeu de n cartes revient à sa configuration initiale
après r mélanges Faros-in avec $2^r \equiv 1 \ [\mathrm{mod}\,(n+1)]$



Périodicité : généralisation

Exemples :

- **pour un jeu de 52 cartes,**
  52 mélanges Faros-in ramènent le jeu à son ordre initial
- ***pour un jeu de 54 cartes,***
  20 mélanges Faros-in ramènent le jeu à son ordre initial



Périodicité : généralisation

Complément : **pour tout entier pair n,**

la période r d'un mélange de n cartes

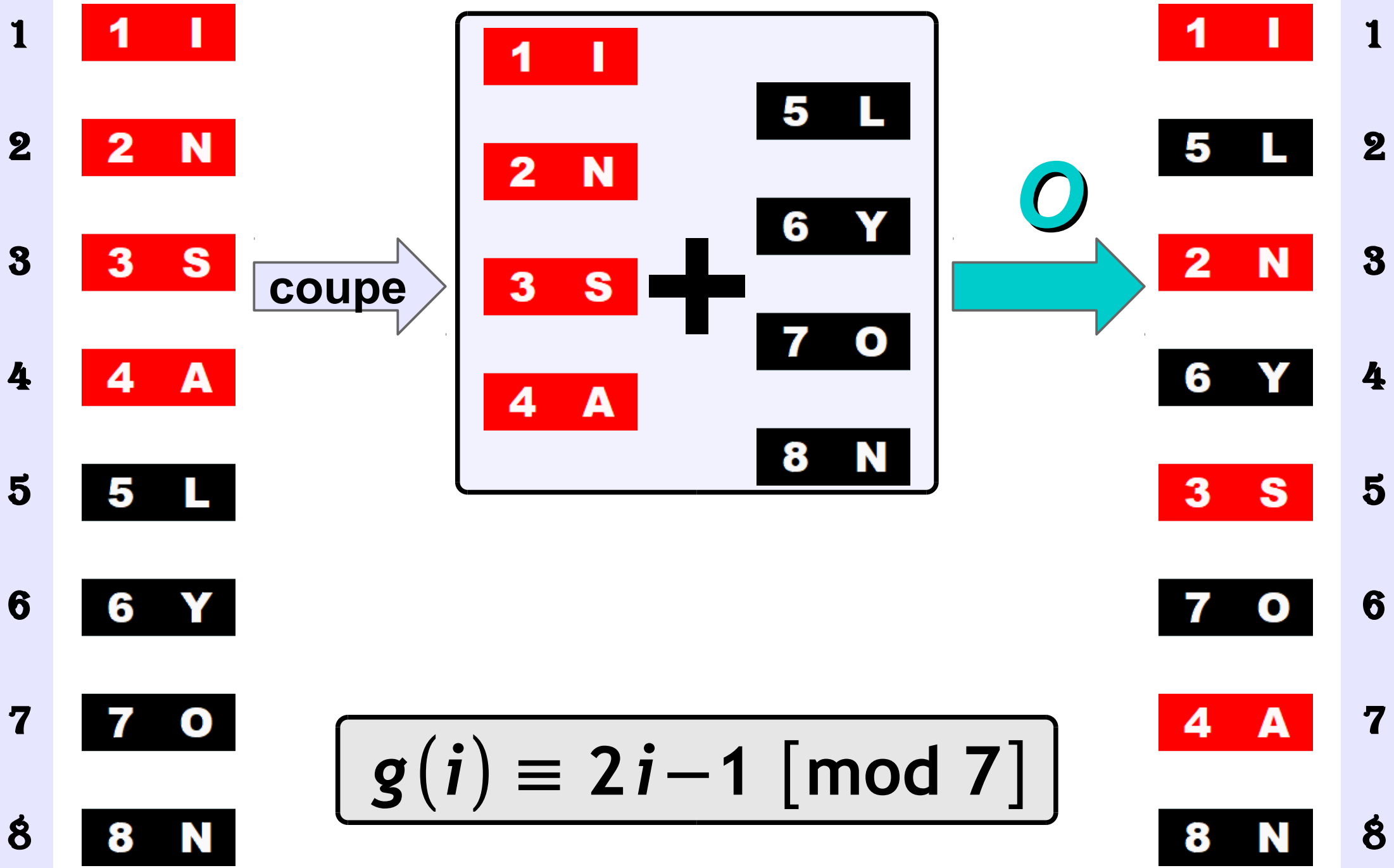
- ***est un diviseur de l'indicatrice d'Euler $\varphi(n+1)$***
  [$\varphi(N)$ est le nombre de nombres premiers avec N compris entre 1 et N]
- ***est un diviseur de n lorsque $n+1$ est premier***

Exemples :

n	32	34	52	54	78
$\varphi(n+1)$	20	24	52	40	78
r	10	12	52	20	39

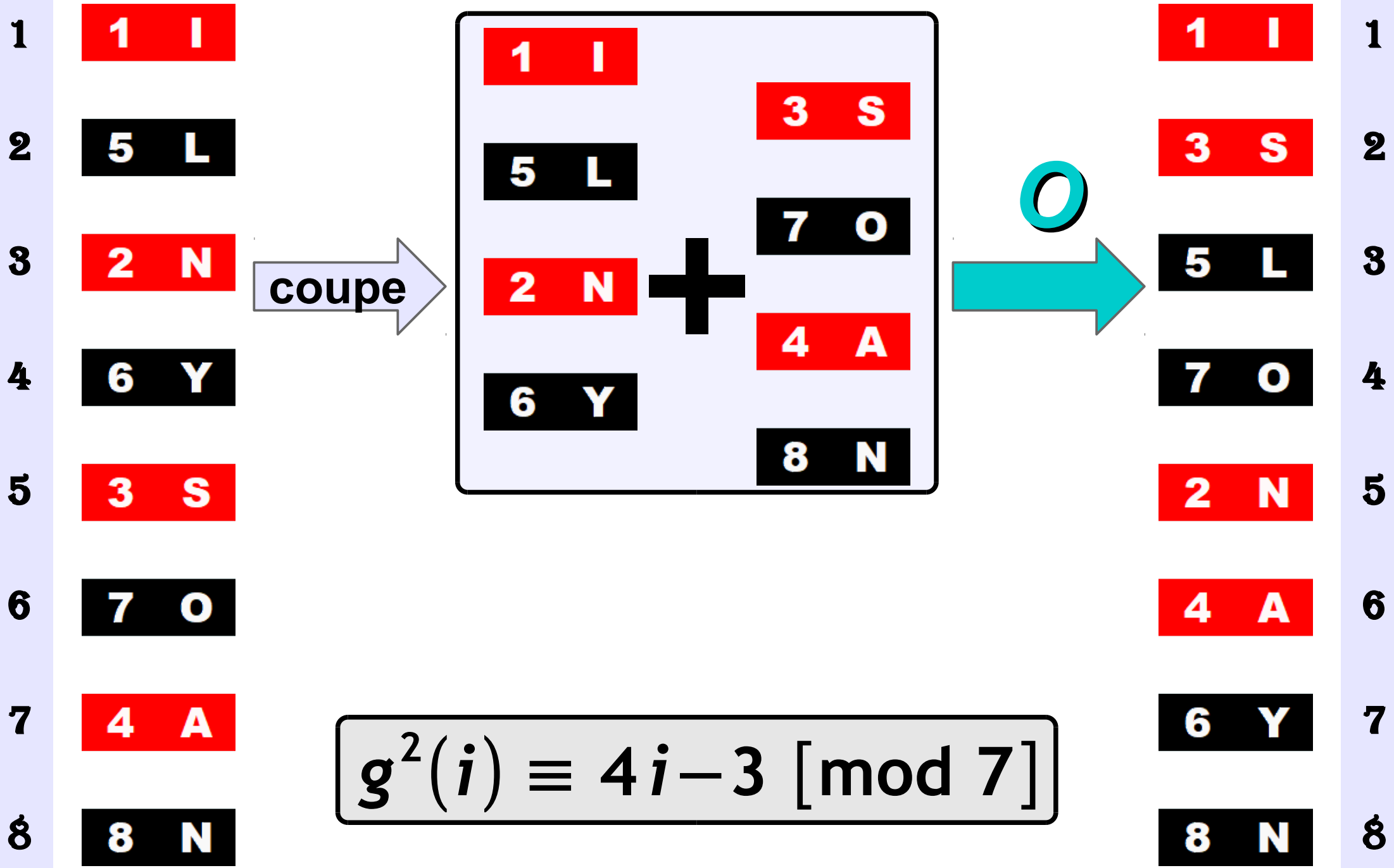
FAROS-OUT

1er mélange « Faro-out »



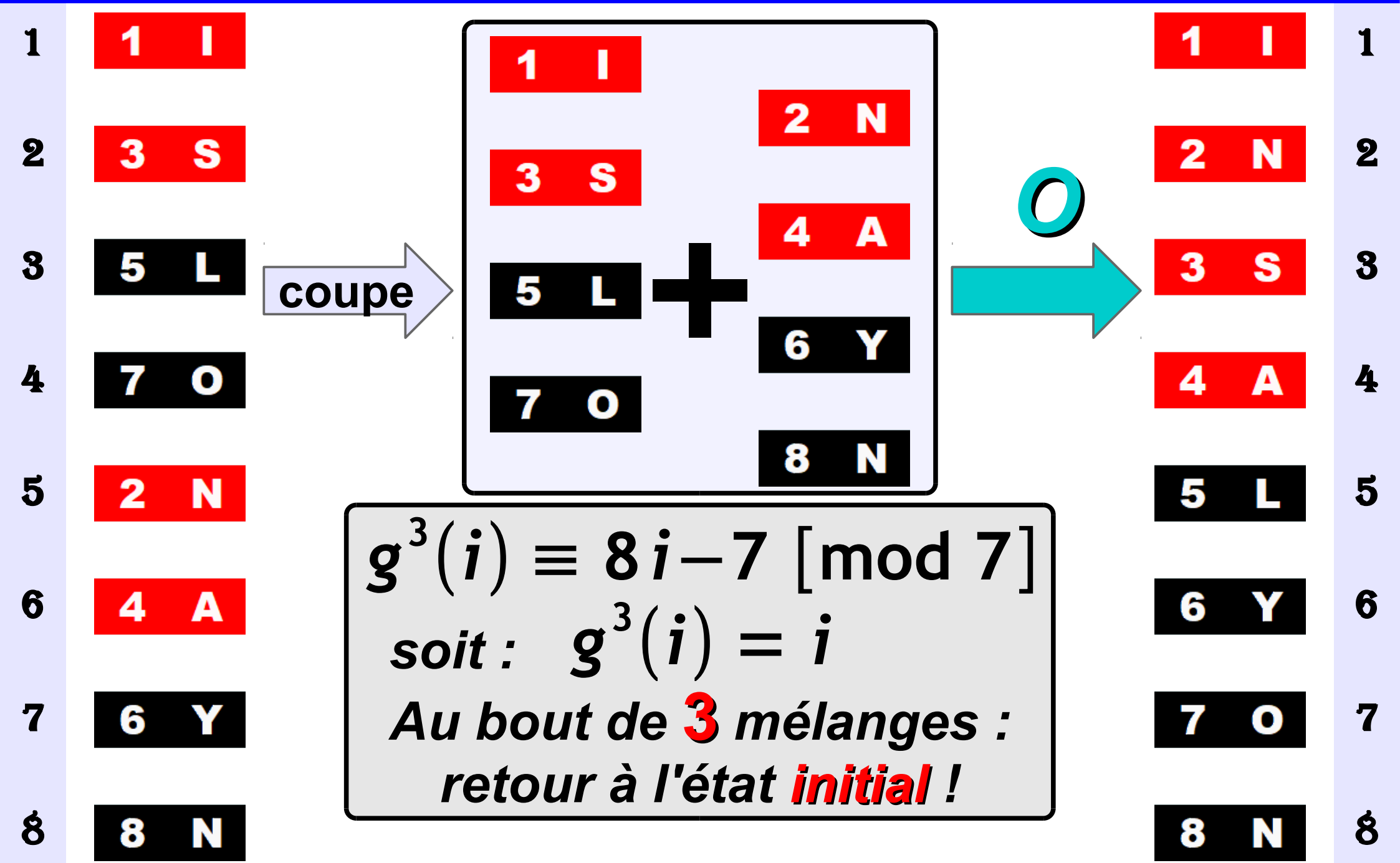
$$g(i) \equiv 2i - 1 \ [\mathrm{mod}\ 7]$$

2e mélange « Faro-out »



$$g^2(i) \equiv 4i - 3 \ [\mathrm{mod}\ 7]$$

3e mélange « Faro-out »

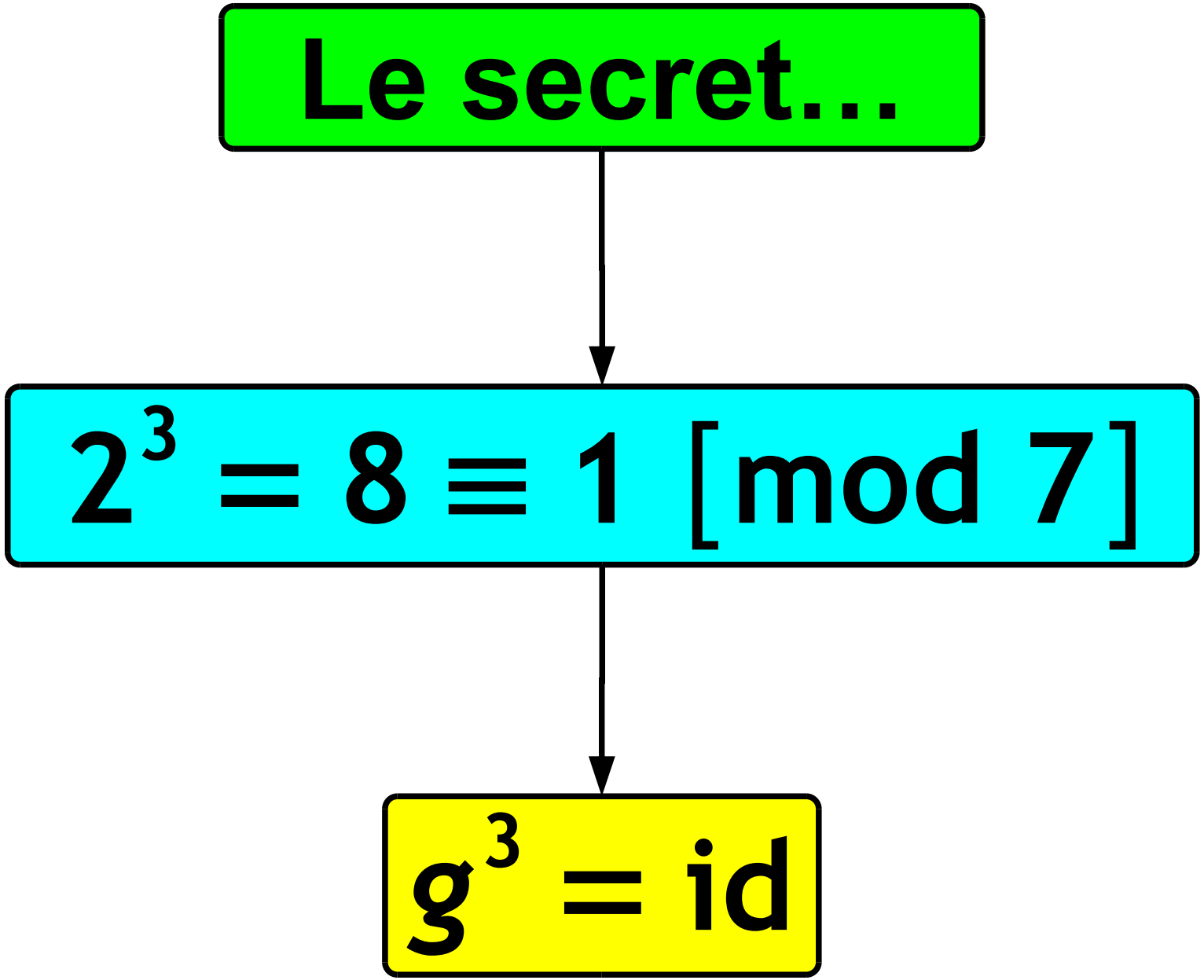


$$g^3(i) \equiv 8i - 7 \ [\text{mod } 7]$$

soit : $g^3(i) = i$

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

Modélisation : une période



Périodicité : généralisation

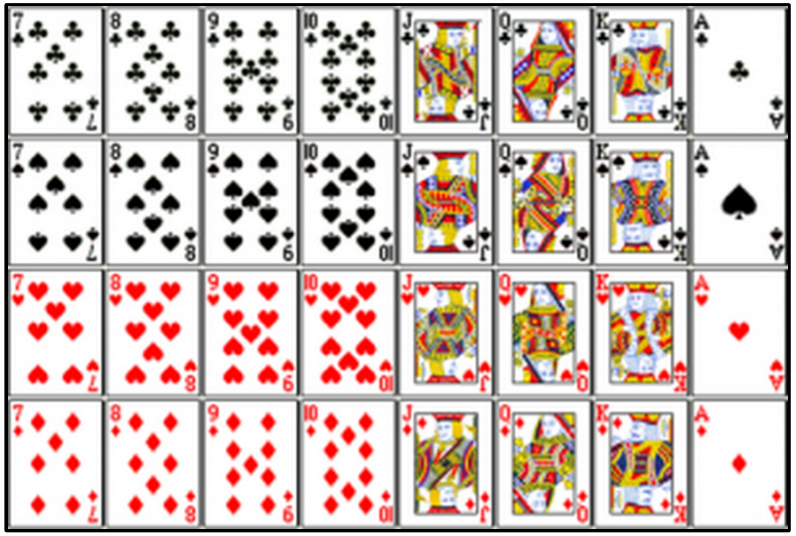
Théorème :

- **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

CASINO ROYAL

APPROCHE BINAIRE

FARO-IN

Approche binaire : Faro-in

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$f^3 = 7 - \mathrm{id}$$

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

FARO-OUT

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

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

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

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

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

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

Approche binaire : Faro-out Renumérotation

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

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

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

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

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

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

FARO-IN/OUT

$$f\left((abc)_2\right) = (bc\bar{a})_2$$
$$g\left((abc)_2\right) = (bca)_2$$

$$f \circ g\left((abc)_2\right) = (ca\bar{b})_2$$
$$g \circ f\left((abc)_2\right) = (c\bar{a}b)_2$$

$$f \circ g \neq g \circ f$$

Approche binaire : 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 $\bar{i}_q = 1 - i_q$:

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

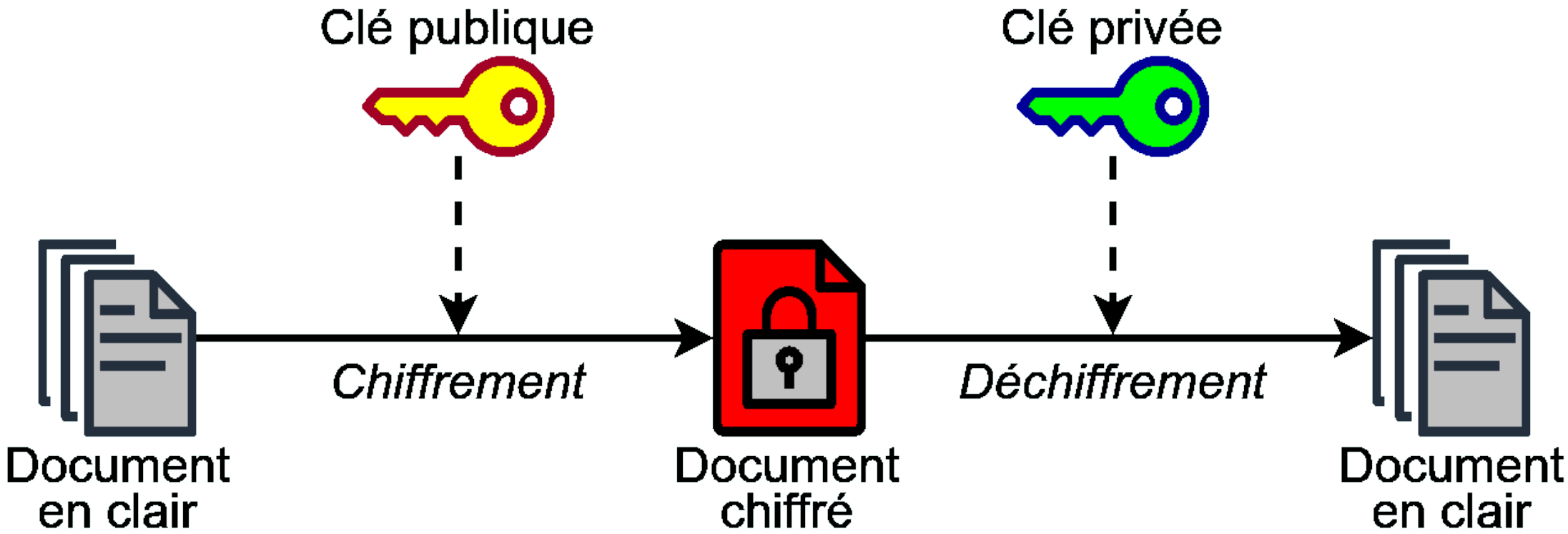
$$g\left((i_{p-1}\, i_{p-2} \cdots i_1\, i_0)_2\right) = (i_{p-2} \cdots i_1\, i_0\, i_{p-1})_2$$

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

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

CASINO ROYAL

APPLICATION EN CRYPTOGRAPHIE


Clé publique
Clé privée
Chiffrement
Déchiffrement
Document en clair
Document chiffré
Document en clair

COMME-LES-
MATHÉMATIQUES-
SONT-PASSIONNANTES-!

C O M M E - L E S - M A T H É M A T I Q U E S - S O N T - P A S S I O N N A N T E S - !

paquet entier
$N = 44$ cartes

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	
	C	O	M	M	E	-	L	E	S	-	M	A	T	H	É	M	A	T	I	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!	
1	S	C	-	O	S	M	O	M	N	E	T	-	-	L	P	E	A	S	S	-	S	M	I	A	O	T	N	H	N	É	A	M	N	A	T	T	E	I	S	Q	-	U	!	E	1
2	I	S	A	C	O	-	T	O	N	S	H	M	N	O	É	M	A	N	M	E	N	T	A	-	T	-	T	L	E	P	I	E	S	A	Q	S	-	S	U	-	!	S	E	M	2
3	A	I	-	S	T	A	-	C	T	O	L	-	E	T	P	O	I	N	E	S	S	H	A	M	Q	N	S	O	-	É	S	M	U	A	-	N	!	M	S	E	E	N	M	T	3
4	A	A	M	I	Q	-	N	S	S	T	O	A	-	-	É	C	S	T	M	O	U	L	A	-	-	E	N	T	!	P	M	O	S	I	E	N	E	E	N	S	M	S	T	H	4
5	A	A	-	A	-	M	E	I	N	Q	T	-	!	N	P	S	M	S	O	T	S	O	I	A	E	-	N	-	E	É	E	C	N	S	S	T	M	M	S	O	T	U	H	L	5
6	I	A	A	A	E	-	-	A	N	-	-	M	E	E	É	I	E	N	C	Q	N	T	S	-	S	!	T	N	M	P	M	S	S	M	O	S	T	O	U	T	H	S	L	O	6
7	S	I	-	A	S	A	!	A	T	E	N	-	M	-	P	A	M	N	S	-	S	-	M	M	O	E	S	E	T	É	O	I	U	E	T	N	H	C	S	Q	L	N	O	T	7
8	M	S	M	I	O	-	E	A	S	S	E	A	T	!	É	A	O	T	I	E	U	N	E	-	T	M	N	-	H	P	C	A	S	M	Q	N	L	S	N	-	O	S	T	-	8
9	E	M	-	S	T	M	M	I	N	O	-	-	H	E	P	A	C	S	A	S	S	E	M	A	Q	T	N	!	L	É	S	A	N	O	-	T	O	I	S	E	T	U	-	N	9
10	M	E	A	M	Q	-	T	S	N	T	!	M	L	M	É	I	S	N	A	O	N	-	O	-	-	H	T	E	O	P	I	A	S	C	E	S	T	A	U	S	-	S	N	E	10
11	O	M	-	E	-	A	H	M	T	Q	E	-	O	T	P	S	I	N	A	T	S	!	C	M	E	L	S	M	T	É	A	I	U	S	S	N	-	A	S	O	N	N	E	-	11
	C	O	M	M	E	-	L	E	S	-	M	A	T	H	É	M	A	T	I	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!	

FARO-*IN*
période 12

paquet entier
$N = 44$ cartes

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	
	C	O	M	M	E	-	L	E	S	-	M	A	T	H	É	M	A	T	I	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!	
1	C	S	O	-	M	S	M	O	E	N	-	T	L	-	E	P	S	A	-	S	M	S	A	I	T	O	H	N	É	N	M	A	A	N	T	T	I	E	Q	S	U	-	E	!	1
2	C	A	S	I	O	T	-	O	M	H	S	N	M	É	O	N	E	M	N	A	-	A	T	N	L	T	-	T	E	I	P	E	S	Q	A	S	-	U	S	-	M	E	S	!	2
3	C	T	A	N	S	L	I	T	O	-	T	T	-	E	O	I	M	P	H	E	S	S	N	Q	M	A	É	S	O	-	N	U	E	S	M	-	N	M	A	E	-	S	A	!	3
4	C	N	T	Q	A	M	N	A	S	É	L	S	I	O	T	-	O	N	-	U	T	E	T	S	-	M	E	-	O	N	I	M	M	A	P	E	H	-	E	S	S	A	S	!	4
5	C	T	N	S	T	-	Q	M	A	E	M	-	N	O	A	N	S	I	É	M	L	M	S	A	I	P	O	E	T	H	-	-	O	E	N	S	-	S	U	A	T	S	E	!	5
6	C	S	T	A	N	I	S	P	T	O	-	E	Q	T	M	H	A	-	E	-	M	O	-	E	N	N	O	S	A	-	N	S	S	U	I	A	É	T	M	S	L	E	M	!	6
7	C	-	S	E	T	N	A	N	N	O	I	S	S	A	P	-	T	N	O	S	-	S	E	U	Q	I	T	A	M	É	H	T	A	M	-	S	E	L	-	E	M	M	O	!	7
8	C	E	-	U	S	Q	E	I	T	T	N	A	A	M	N	É	N	H	O	T	I	A	S	M	S	-	A	S	P	E	-	L	T	-	N	E	O	M	S	M	-	O	S	!	8
9	C	S	E	M	-	S	U	-	S	A	Q	S	E	P	I	E	T	-	T	L	N	T	A	-	A	N	M	E	N	O	É	M	N	S	H	M	O	-	T	O	I	S	A	!	9
10	C	A	S	-	E	A	M	N	-	M	S	E	U	N	-	O	S	É	A	M	Q	N	S	S	E	H	P	M	I	O	E	-	T	T	-	O	T	I	L	S	N	A	T	!	10
11	C	S	A	S	S	E	-	H	E	P	A	M	M	I	N	O	-	E	M	-	S	T	E	T	U	-	N	O	-	T	O	I	S	L	É	S	A	N	M	A	Q	T	N	!	11
12	C	E	S	T	A	U	S	-	S	N	E	O	-	-	H	T	E	O	P	I	A	S	M	L	M	É	I	S	N	A	O	N	-	M	E	A	M	Q	-	T	S	N	T	!	12
13	C	M	E	L	S	M	T	É	A	I	U	S	S	N	-	A	S	O	N	N	E	-	O	M	-	E	-	A	H	M	T	Q	E	-	O	T	P	S	I	N	A	T	S	!	13
	C	O	M	M	E	-	L	E	S	-	M	A	T	H	É	M	A	T	I	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!	

FARO-*OUT*
période *14*

paquet entier
$N = 44$ cartes

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
C	O	M	M	E	-	L	E	S	-	M	A	T	H	É	M	A	T	I	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!

1	S	C	-	O	S	M	O	M	N	E	T	-	-	L	P	E	A	S	S	-	S	M	I	A	O	T	N	H	N	É	A	M	N	A	T	T	E	I	S	Q	-	U	!	E
2	I	S	A	C	O	-	T	O	N	S	H	M	N	O	É	M	A	N	M	E	N	T	A	-	T	-	T	L	E	P	I	E	S	A	Q	S	-	S	U	-	!	S	E	M
3	A	I	-	S	T	A	-	C	T	O	L	-	E	T	P	O	I	N	E	S	S	H	A	M	Q	N	S	O	-	É	S	M	U	A	-	N	!	M	S	E	E	N	M	T
4	A	A	M	I	Q	-	N	S	S	T	O	A	-	-	É	C	S	T	M	O	U	L	A	-	-	E	N	T	!	P	M	O	S	I	E	N	E	E	N	S	M	S	T	H
5	A	A	-	A	-	M	E	I	N	Q	T	-	!	N	P	S	M	S	O	T	S	O	I	A	E	-	N	-	E	É	E	C	N	S	S	T	M	M	S	O	T	U	H	L

FARO-*IN*
5 **mélanges**

C O M M E - L E S - M A T H É M A T I Q U E S - S O N T - P A S S I O N N A N T E S - !

Chiffrement
en 5 mélanges

A A - A - M E I N Q T - ! N P S M S O T S O I A E - N - E É E C N S S T M M S O T U H L

Le message à déchiffrer

AA-A-MEINQT-!
NPSMSOTSOIAE-N-
EÉECNSSTMMSOTUHL

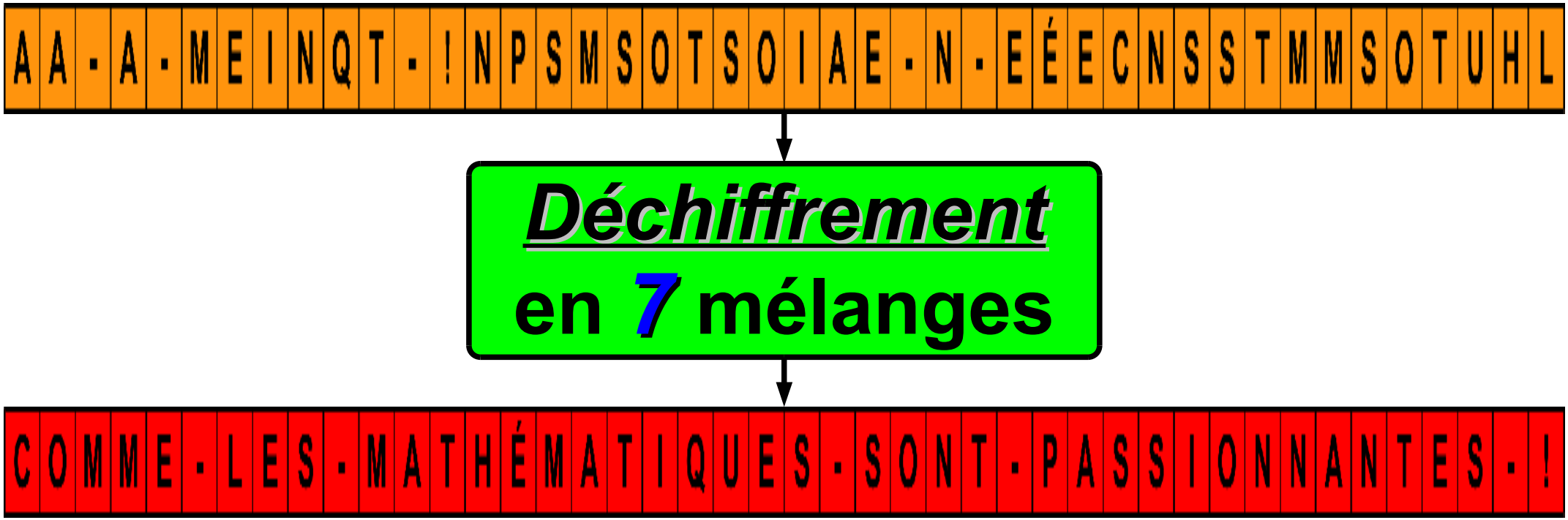
A A - A - M E I N Q T - ! N P S M S O T S O I A E - N - E É E C N S S T M M S O T U H L

paquet entier
$N = 44$ cartes

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
A	A	-	A	-	M	E	I	N	Q	T	-	!	N	P	S	M	S	O	T	S	O	I	A	E	-	N	-	E	É	E	C	N	S	S	T	M	M	S	O	T	U	H	L

1	I	A	A	A	E	-	-	A	N	-	-	M	E	E	É	I	E	N	C	Q	N	T	S	-	S	!	T	N	M	P	M	S	S	M	O	S	T	O	U	T	H	S	L	O	1
2	S	I	-	A	S	A	!	A	T	E	N	-	M	-	P	A	M	N	S	-	S	-	M	M	O	E	S	E	T	É	O	I	U	E	T	N	H	C	S	Q	L	N	O	T	2
3	M	S	M	I	O	-	E	A	S	S	E	A	T	!	É	A	O	T	I	E	U	N	E	-	T	M	N	-	H	P	C	A	S	M	Q	N	L	S	N	-	O	S	T	-	3
4	E	M	-	S	T	M	M	I	N	O	-	-	H	E	P	A	C	S	A	S	S	E	M	A	Q	T	N	!	L	É	S	A	N	O	-	T	O	I	S	E	T	U	-	N	4
5	M	E	A	M	Q	-	T	S	N	T	!	M	L	M	É	I	S	N	A	O	N	-	O	-	-	H	T	E	O	P	I	A	S	C	E	S	T	A	U	S	-	S	N	E	5
6	O	M	-	E	-	A	H	M	T	Q	E	-	O	T	P	S	I	N	A	T	S	!	C	M	E	L	S	M	T	É	A	I	U	S	S	N	-	A	S	O	N	N	E	-	6
7	C	O	M	M	E	-	L	E	S	-	M	A	T	H	É	M	A	T	I	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!	7

FARO-*IN*
7 mélanges


A A - A - M E I N Q T - ! N P S M S O T S O I A E - N - E É E C N S S T M M S O T U H L
Déchiffrement
en 7 mélanges
C O M M E - L E S - M A T H É M A T I Q U E S - S O N T - P A S S I O N N A N T E S - !

C O M M E - L E S - M A T H É M A T I Q U E S - S O N T - P A S S I O N N A N T E S - !

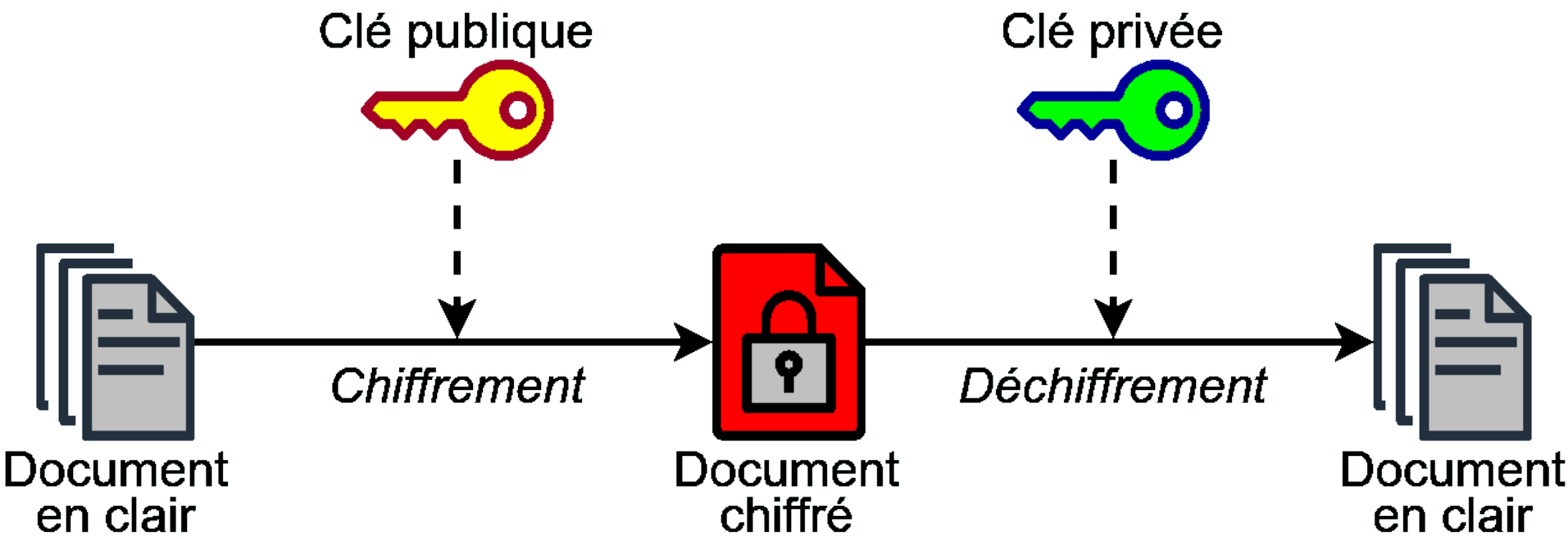
Chiffrement
en 5 mélanges

A A - A - M E I N Q T - ! N P S M S O T S O I A E - N - E É E C N S S T M M S O T U H L

Déchiffrement
en 7 mélanges

C O M M E - L E S - M A T H É M A T I Q U E S - S O N T - P A S S I O N N A N T E S - !

Concept : pour un jeu de N cartes, de période r :



Chiffrement

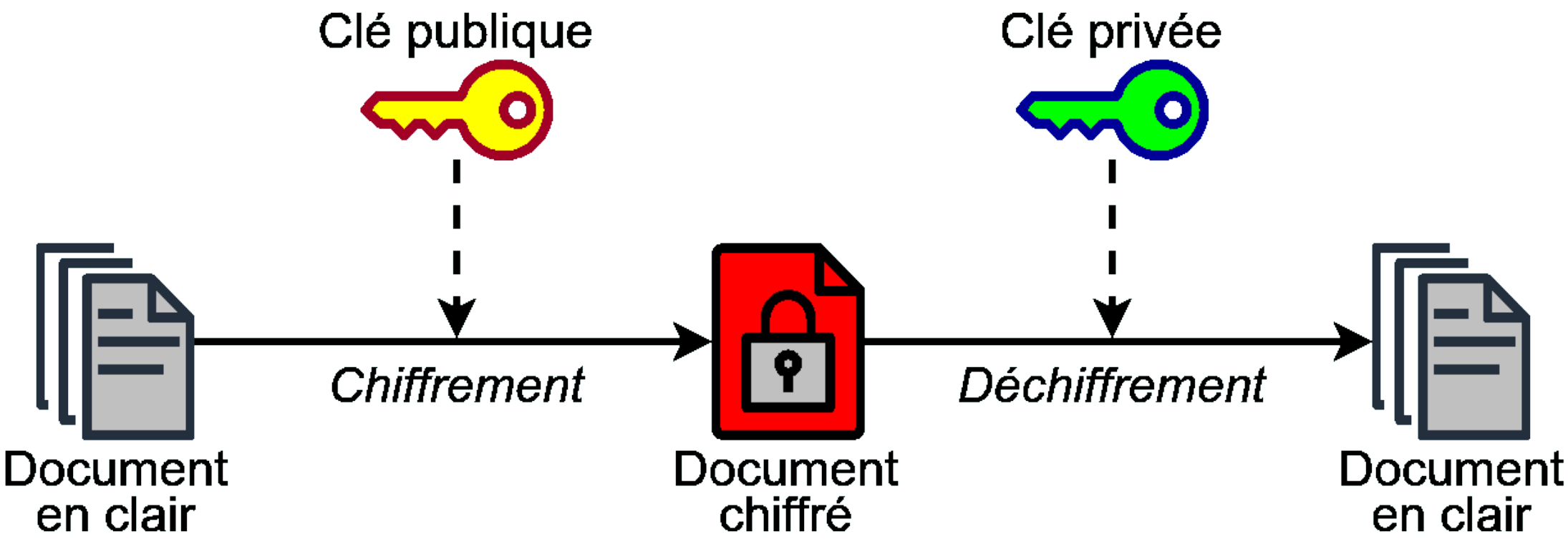
On ***chiffre***

avec p mélanges

Déchiffrement

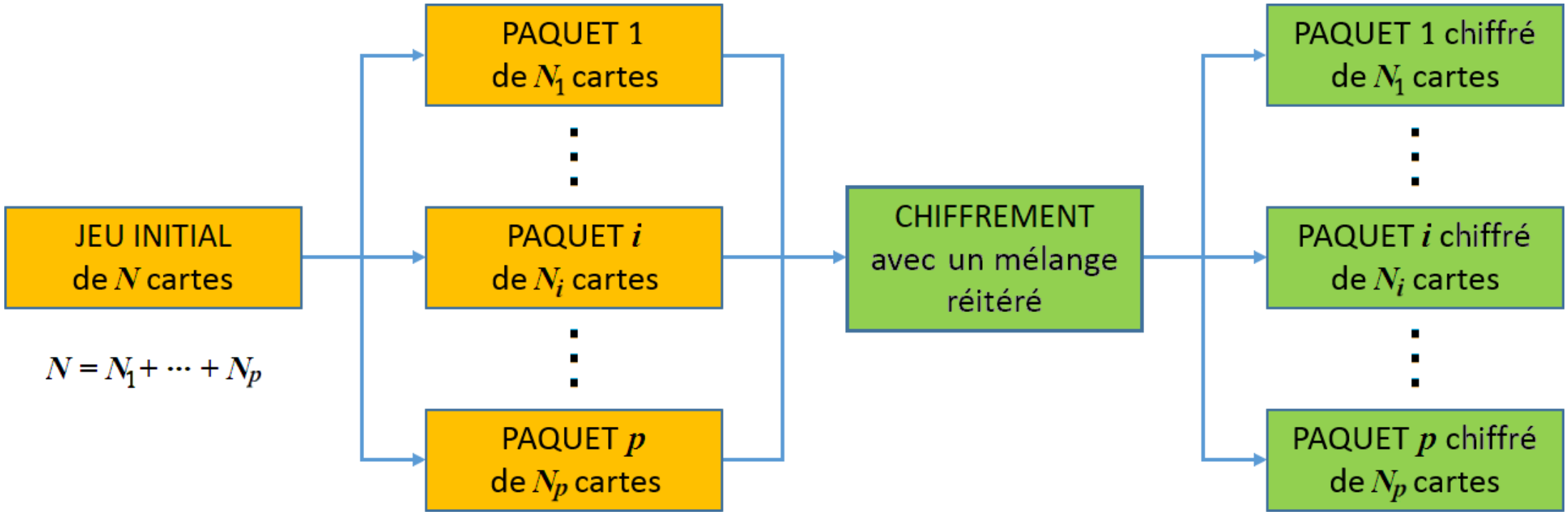
On ***déchiffre***

avec $q = r - p$ mélanges



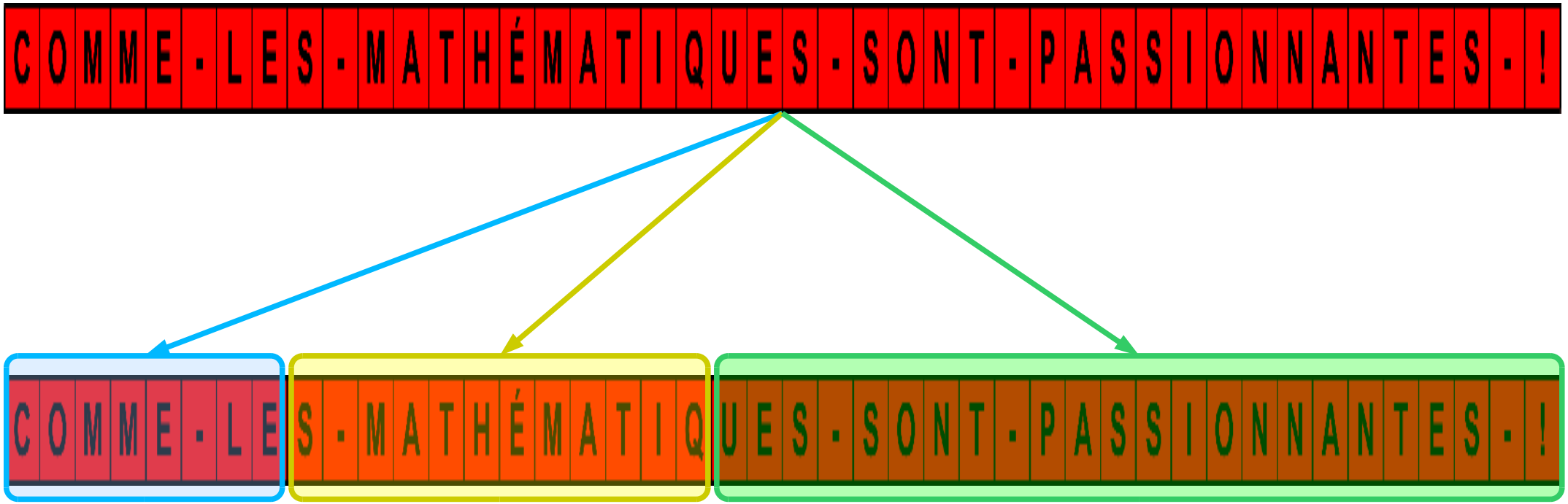
La sécurité du chiffrement ne repose que sur le secret de l'algorithme. Autant dire qu'elle est (quasi) nulle !

$$N = N_1 + \cdots + N_p$$



Pour augmenter la sécurité, on pourrait partager une clé secrète entre l'émetteur et le récepteur (*clé privée partagée*) qui définit le nombre de sous-paquets qui seront chiffrés puis réassemblés

Le message à chiffrer



Cryptographie

Le message à chiffrer

1er paquet	2e paquet	3e paquet
$N_1 = 8$ cartes	$N_2 = 12$ cartes	$N_3 = 24$ cartes

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
C	O	M	M	E	-	L	E	S	-	M	A	T	H	É	M	A	T	I	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!

Cryptographie — Les mélanges par blocs

1er paquet	2e paquet	3e paquet
$N_1 = 8$ cartes	$N_2 = 12$ cartes	$N_3 = 24$ cartes

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
C	O	M	M	E	-	L	E	S	-	M	A	T	H	É	M	A	T	I	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!

1	E	C	-	O	L	M	E	M
2	L	E	M	C	E	-	M	O
3	E	L	-	E	M	M	O	C
4	M	E	M	L	O	-	C	E
5	O	M	-	E	C	M	E	L
6	C	O	M	M	E	-	L	E

FARO-*IN*
période 6

Cryptographie — Les mélanges par blocs

1er paquet	2e paquet	3e paquet
$N_1 = 8$ cartes	$N_2 = 12$ cartes	$N_3 = 24$ cartes

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
C	O	M	M	E	-	L	E	S	-	M	A	T	H	É	M	A	T	I	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!

1	E	C	-	O	L	M	E	M	S	É	-	M	M	A	A	T	T	I	H	Q																								1
2	L	E	M	C	E	-	M	O	S	A	É	T	-	T	M	I	M	H	A	Q																								2
3	E	L	-	E	M	M	O	C	S	M	A	I	É	M	T	H	-	A	T	Q																								3
4	M	E	M	L	O	-	C	E	S	T	M	H	A	-	I	A	É	T	M	Q																								4
5	O	M	-	E	C	M	E	L	S	I	T	A	M	É	H	T	A	M	-	Q																								5
6	C	O	M	M	E	-	L	E	S	H	I	T	T	A	A	M	M	-	É	Q																								6
7									S	A	H	M	I	M	T	-	T	É	A	Q																								7
8									S	T	A	-	H	T	M	É	I	A	M	Q																								8
9									S	M	T	É	A	I	-	A	H	M	T	Q																								9
10									S	-	M	A	T	H	É	M	A	T	I	Q																								10

FARO-*IN* période **6**

FARO-*OUT* période **10**

Cryptographie — Les mélanges par blocs

1er paquet	2e paquet	3e paquet
$N_1 = 8$ cartes	$N_2 = 12$ cartes	$N_3 = 24$ cartes

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
C	O	M	M	E	-	L	E	S	-	M	A	T	H	É	M	A	T	I	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!

1	E	C	-	O	L	M	E	M	S	É	-	M	M	A	A	T	T	I	H	Q	S	U	I	E	O	S	N	-	N	S	A	O	N	N	T	T	E	-	S	P	-	A	!	S	1
2	L	E	M	C	E	-	M	O	S	A	É	T	-	T	M	I	M	H	A	Q	N	S	N	U	T	I	T	E	E	O	-	S	S	N	P	-	-	N	A	S	!	A	S	O	2
3	E	L	-	E	M	M	O	C	S	M	A	I	É	M	T	H	-	A	T	Q	S	N	N	S	P	N	-	U	-	T	N	I	A	T	S	E	!	E	A	O	S	-	O	S	3
4	M	E	M	L	O	-	C	E	S	T	M	H	A	-	I	A	É	T	M	Q	A	S	T	N	S	N	E	S	!	P	E	N	A	-	O	U	S	-	-	T	O	N	S	I	4
5	O	M	-	E	C	M	E	L	S	I	T	A	M	É	H	T	A	M	-	Q	A	A	-	S	O	T	U	N	S	S	-	N	-	E	T	S	O	!	N	P	S	E	I	N	5
6	C	O	M	M	E	-	L	E	S	H	I	T	T	A	A	M	M	-	É	Q	-	A	E	A	T	-	S	S	O	O	!	T	N	U	P	N	S	S	E	S	I	-	N	N	6
7									S	A	H	M	I	M	T	-	T	É	A	Q	N	-	U	A	P	E	N	A	S	T	S	-	E	S	S	S	I	O	-	O	N	!	N	T	7
8									S	T	A	-	H	T	M	É	I	A	M	Q	E	N	S	-	S	U	S	A	I	P	O	E	-	N	O	A	N	S	!	T	N	S	T	-	8
9									S	M	T	É	A	I	-	A	H	M	T	Q	-	E	N	N	O	S	A	-	N	S	S	U	!	S	T	A	N	I	S	P	T	O	-	E	9
10									S	-	M	A	T	H	É	M	A	T	I	Q	!	-	S	E	T	N	A	N	N	O	I	S	S	A	P	-	T	N	O	S	-	S	E	U	10
11																					S	!	A	-	P	S	-	E	T	T	N	N	O	A	S	N	-	N	S	O	E	I	U	S	11
12																					O	S	A	!	S	A	N	-	-	P	N	S	S	-	O	E	E	T	I	T	U	N	S	N	12
13																					S	O	-	S	O	A	E	!	E	S	T	A	I	N	T			U	-	N	P	S	N	N	S	13
14																					I	S	N	O	T	-	-	S											S	E	N	S	N	T	S	A	14
15																					N	I	E	S	P	N	!	C											N	U	T	O	S	-	A	A	15
16																					N	N	-	I	S	E	S	S											S	S	-	T	A	E	A	-	16
17																					T	N	!	N	O	-	O	I	S	S	S	E	-	S	I	S	A	N	E	P	A	U	-	N	17
18																					-	T	S	N	T	!	S	N	A	O	N	-	E	O	P	I	A	S	U	S	-	S	N	E	18
19																					E	-	O	T	P	S	I	N	A	T	S	!	U	S	S	N	-	A	S	O	N	N	E	-	19
20																					U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!	20

FARO-*IN* période 6

FARO-*OUT* période 10

FARO-*IN* période 20

1er paquet	2e paquet	3e paquet
$N_1 = 8$ cartes	$N_2 = 12$ cartes	$N_3 = 24$ cartes

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
C	O	M	M	E	-	L	E	S	-	M	A	T	H	É	M	A	T	I	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!

1	E	C	-	O	L	M	E	M																																					1
2	L	E	M	C	E	-	M	O																																					2

FARO-*IN*

2 **mélanges**

1er paquet	2e paquet	3e paquet
$N_1 = 8$ cartes	$N_2 = 12$ cartes	$N_3 = 24$ cartes

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
C	O	M	M	E	-	L	E	S	-	M	A	T	H	É	M	A	T	I	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!

1	E	C	-	O	L	M	E	M	S	É	-	M	M	A	A	T	T	I	H	Q																								1
2	L	E	M	C	E	-	M	O	S	A	É	T	-	T	M	I	M	H	A	Q																								2
3									S	M	A	I	É	M	T	H	-	A	T	Q																								3
4									S	T	M	H	A	-	I	A	É	T	M	Q																								4
5									S	I	T	A	M	É	H	T	A	M	-	Q																								5
6									S	H	I	T	T	A	A	M	M	-	É	Q																								6
7									S	A	H	M	I	M	T	-	T	É	A	Q																								7

FARO-*IN*
2 **mélanges**

FARO-*OUT*
7 **mélanges**

Cryptographie — Chiffrement par blocs

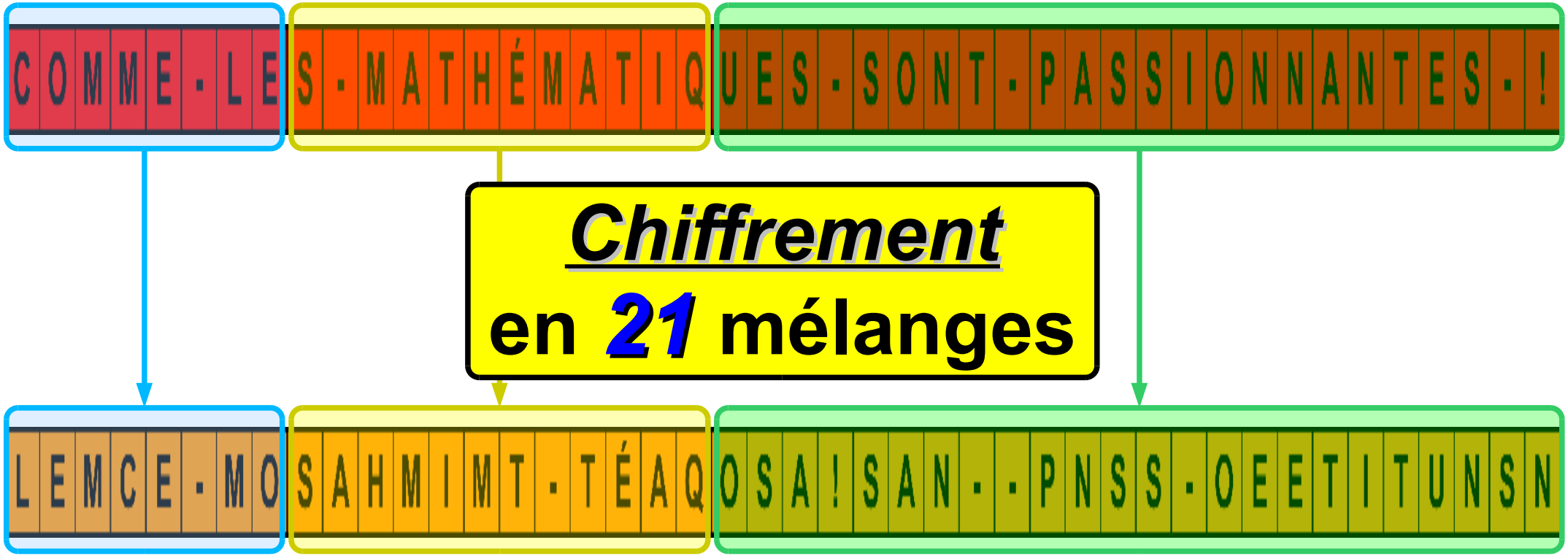
1er paquet	2e paquet	3e paquet
$N_1 = 8$ cartes	$N_2 = 12$ cartes	$N_3 = 24$ cartes

	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	
	C	O	M	M	E	-	L	E	S	-	M	A	T	H	É	M	A	T	I	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!	
1	E	C	-	O	L	M	E	M	S	É	-	M	M	A	A	T	T	I	H	Q	S	U	I	E	O	S	N	-	N	S	A	O	N	N	T	T	E	-	S	P	-	A	!	S	1
2	L	E	M	C	E	-	M	O	S	A	É	T	-	T	M	I	M	H	A	Q	N	S	N	U	T	I	T	E	E	O	-	S	S	N	P	-	-	N	A	S	!	A	S	O	2
3									S	M	A	I	É	M	T	H	-	A	T	Q	S	N	N	S	P	N	-	U	-	T	N	I	A	T	S	E	!	E	A	O	S	-	O	S	3
4									S	T	M	H	A	-	I	A	É	T	M	Q	A	S	T	N	S	N	E	S	!	P	E	N	A	-	O	U	S	-	-	T	O	N	S	I	4
5									S	I	T	A	M	É	H	T	A	M	-	Q	A	A	-	S	O	T	U	N	S	S	-	N	-	E	T	S	O	!	N	P	S	E	I	N	5
6									S	H	I	T	T	A	A	M	M	-	É	Q	-	A	E	A	T	-	S	S	O	O	!	T	N	U	P	N	S	S	E	S	I	-	N	N	6
7									S	A	H	M	I	M	T	-	T	É	A	Q	N	-	U	A	P	E	N	A	S	T	S	-	E	S	S	S	I	O	-	O	N	!	N	T	7
8																					E	N	S	-	S	U	S	A	I	P	O	E	-	N	O	A	N	S	!	T	N	S	T	-	8
9																					-	E	N	N	O	S	A	-	N	S	S	U	!	S	T	A	N	I	S	P	T	O	-	E	9
10																					!	-	S	E	T	N	A	N	N	O	I	S	S	A	P	-	T	N	O	S	-	S	E	U	10
11																					S	!	A	-	P	S	-	E	T	T	N	N	O	A	S	N	-	N	S	O	E	I	U	S	11
12																					O	S	A	!	S	A	N	-	-	P	N	S	S	-	O	E	E	T	I	T	U	N	S	N	12

FARO-*IN*	FARO-*OUT*	FARO-*IN*
2 mélanges	7 mélanges	12 mélanges

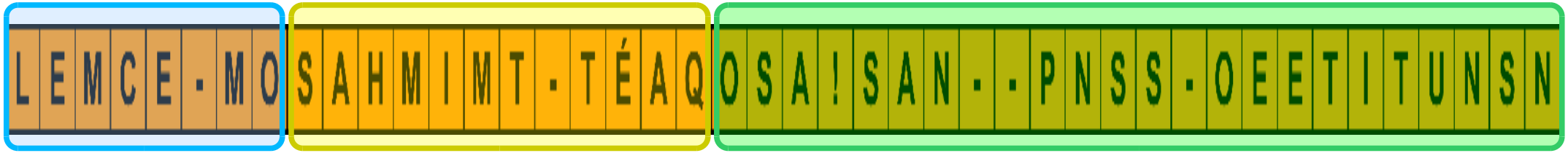
1er paquet	2e paquet	3e paquet
$N_1 = 8$ cartes	$N_2 = 12$ cartes	$N_3 = 24$ cartes

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
C	O	M	M	E	-	L	E	S	-	M	A	T	H	É	M	A	T	I	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!
L	E	M	C	E	-	M	O	S	A	H	M	I	M	T	-	T	É	A	Q	O	S	A	!	S	A	N	-	-	P	N	S	S	-	O	E	E	T	I	T	U	N	S	N


COMME-LES-MATHÉMATIQUES-SONT-PASSIONNANTES-!
Chiffrement
en 21 mélanges
LEMCE-MOSAHMIMT-TÉAQOSA!SAN--PNSS-OEETITUNSN

Le message à déchiffrer

LEMCE-MOSAHMIMT-TÉAQOSA!SAN--PNSS-OEETITUNSN



Cryptographie

Le message à déchiffrer

1er paquet	2e paquet	3e paquet
$N_1 = 8$ cartes	$N_2 = 12$ cartes	$N_3 = 24$ cartes

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
L	E	M	C	E	-	M	O	S	A	H	M	I	M	T	-	T	É	A	Q	O	S	A	!	S	A	N	-	-	P	N	S	S	-	O	E	E	T	I	T	U	N	S	N

Cryptographie — Déchiffrement par blocs

1er paquet	2e paquet	3e paquet
$N_1 = 8$ cartes	$N_2 = 12$ cartes	$N_3 = 24$ cartes

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
L	E	M	C	E	-	M	O	S	A	H	M	I	M	T	-	T	É	A	Q	O	S	A	!	S	A	N	-	-	P	N	S	S	-	O	E	E	T	I	T	U	N	S	N

3	E	L	-	E	M	M	O	C
4	M	E	M	L	O	-	C	E
5	O	M	-	E	C	M	E	L
6	C	O	M	M	E	-	L	E

FARO-*IN*
4 **mélanges**

Cryptographie — Déchiffrement par blocs

1er paquet	2e paquet	3e paquet
$N_1 = 8$ cartes	$N_2 = 12$ cartes	$N_3 = 24$ cartes

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
L	E	M	C	E	-	M	O	S	A	H	M	I	M	T	-	T	É	A	Q	O	S	A	!	S	A	N	-	-	P	N	S	S	-	O	E	E	T	I	T	U	N	S	N

8	E	L	-	E	M	M	O	C	S	T	A	-	H	T	M	É	I	A	M	Q																								8
9	M	E	M	L	O	-	C	E	S	M	T	É	A	I	-	A	H	M	T	Q																								9
10	O	M	-	E	C	M	E	L	S	-	M	A	T	H	É	M	A	T	I	Q																								10
	C	O	M	M	E	-	L	E																																			

FARO-*IN*
4 **mélanges**

FARO-*OUT*
3 **mélanges**

Cryptographie — Déchiffrement par blocs

1er paquet	2e paquet	3e paquet
$N_1 = 8$ cartes	$N_2 = 12$ cartes	$N_3 = 24$ cartes

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
L	E	M	C	E	-	M	O	S	A	H	M	I	M	T	-	T	É	A	Q	O	S	A	!	S	A	N	-	-	P	N	S	S	-	O	E	E	T	I	T	U	N	S	N
E	L	-	E	M	M	O	C	S	T	A	-	H	T	M	É	I	A	M	Q	S	O	-	S	O	A	E	!	E	S	T	A	I	N	T	-	U	-	N	P	S	N	N	S
M	E	M	L	O	-	C	E	S	M	T	É	A	I	-	A	H	M	T	Q	I	S	N	O	T	-	-	S	U	O	-	A	N	E	P	!	S	E	N	S	N	T	S	A
O	M	-	E	C	M	E	L	S	-	M	A	T	H	É	M	A	T	I	Q	N	I	E	S	P	N	!	O	S	T	E	-	N	-	S	S	N	U	T	O	S	-	A	A
C	O	M	M	E	-	L	E													N	N	-	I	S	E	S	S	N	P	U	N	T	!	O	O	S	S	-	T	A	E	A	-
																				T	N	!	N	O	-	O	I	S	S	S	E	-	S	T	S	A	N	E	P	A	U	-	N
																				-	T	S	N	T	!	S	N	A	O	N	-	E	O	P	I	A	S	U	S	-	S	N	E
																				E	-	O	T	P	S	I	N	A	T	S	!	U	S	S	N	-	A	S	O	N	N	E	-
																				U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!

FARO-*IN*	FARO-*OUT*	FARO-*IN*
4 mélanges	*3* mélanges	*8* mélanges

Cryptographie

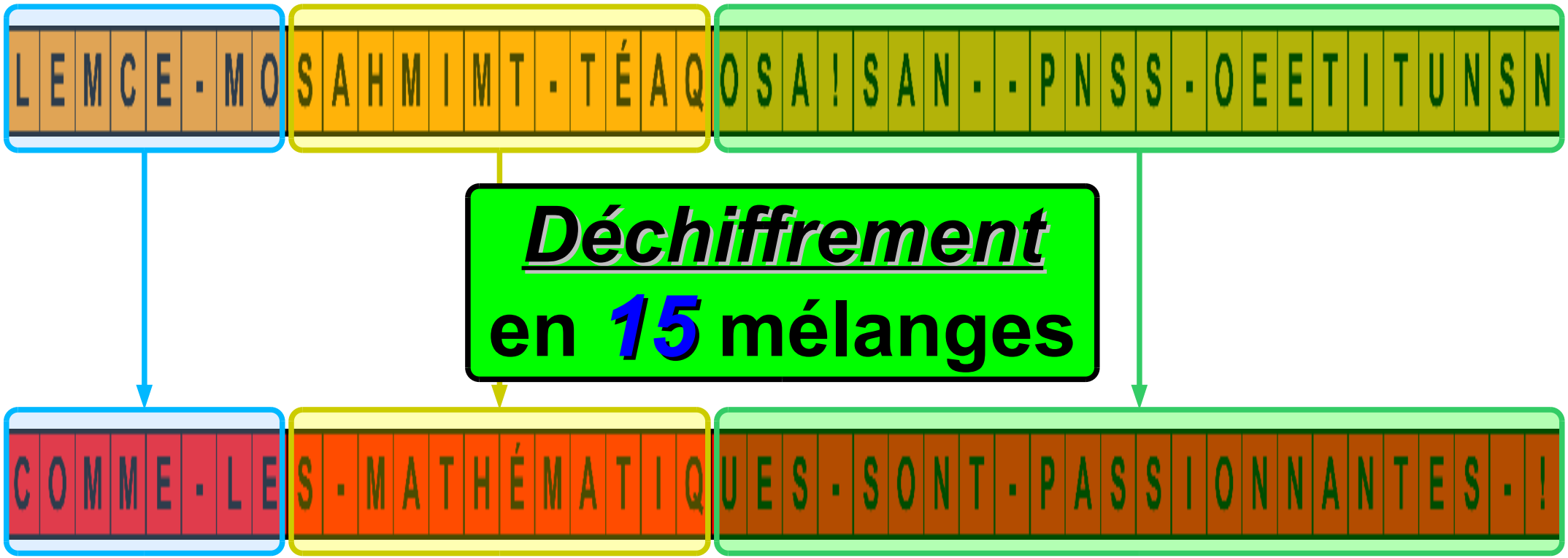
Le message déchiffré

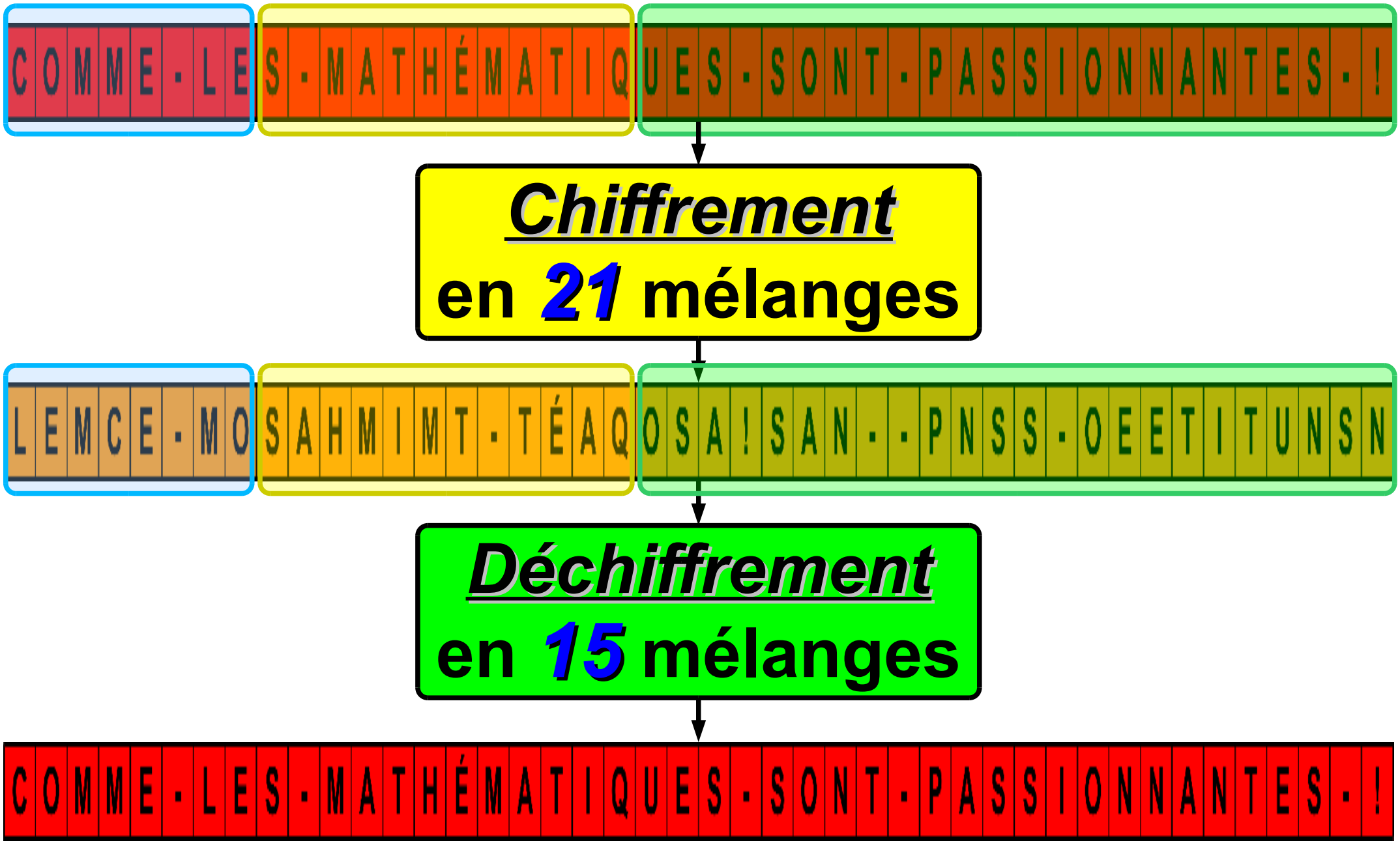
1^er paquet — $N_1 = 8$ cartes

2^e paquet — $N_2 = 12$ cartes

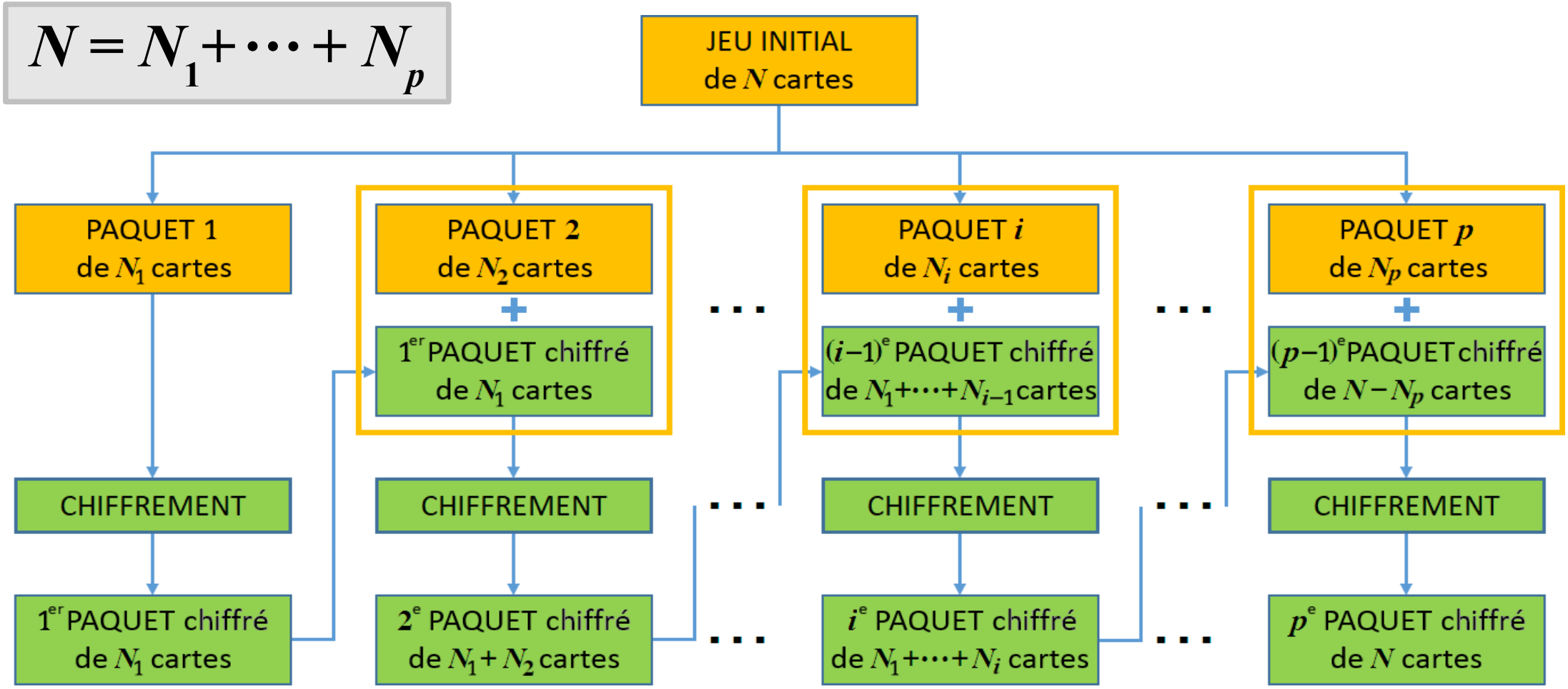
3^e paquet — $N_3 = 24$ cartes

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
L	E	M	C	E	-	M	O	S	A	H	M	I	M	T	-	T	É	A	Q	O	S	A	!	S	A	N	-	-	P	N	S	S	-	O	E	E	T	I	T	U	N	S	N
C	O	M	M	E	-	L	E	S	-	M	A	T	H	É	M	A	T	I	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!


L E M C E - M O S A H M I M T - T É A Q O S A ! S A N - - P N S S - O E E T I T U N S N
Déchiffrement
en 15 mélanges
C O M M E - L E S - M A T H É M A T I Q U E S - S O N T - P A S S I O N N A N T E S - !

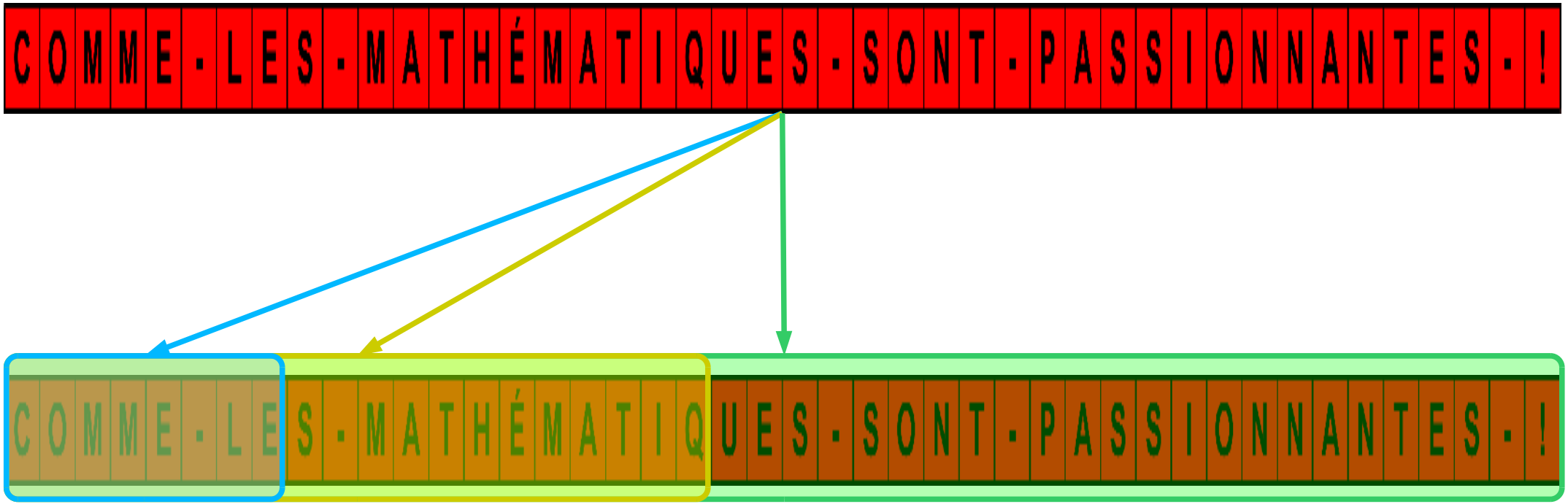

COMME-LES-MATHÉMATIQUES-SONT-PASSIONNANTES-!
Chiffrement
en 21 mélanges
LEMCE-MOSAHMIMT-TÉAQOSA!SAN--PNSS-OEETITUNSN
Déchiffrement
en 15 mélanges
COMME-LES-MATHÉMATIQUES-SONT-PASSIONNANTES-!

$$N = N_1 + \cdots + N_p$$



Pour augmenter la sécurité, on pourrait partager une clé secrète entre l'émetteur et le récepteur (*clé privée partagée*) qui définit le nombre de sous-paquets qui seront chiffrés puis réassemblés

Le message à chiffrer



Cryptographie

1er message à chiffrer

1er paquet	2e paquet	3e paquet
$N_1 = 8$ cartes	$N_2 = 12$ cartes	$N_3 = 24$ cartes

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
C	O	M	M	E	-	L	E	S	-	M	A	T	H	É	M	A	T	I	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!

1er paquet	2e paquet	3e paquet
$N_1 = 8$ cartes	$N_2 = 12$ cartes	$N_3 = 24$ cartes

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
C	O	M	M	E	-	L	E	S	-	M	A	T	H	É	M	A	T	I	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!

1	E	C	-	O	L	M	E	M
2	L	E	M	C	E	-	M	O
3	E	L	-	E	M	M	O	C
4	M	E	M	L	O	-	C	E
5	O	M	-	E	C	M	E	L
6	C	O	M	M	E	-	L	E

FARO-*IN*
période 6

1er paquet	2e paquet	3e paquet
$N_1 = 8$ cartes	$N_2 = 12$ cartes	$N_3 = 24$ cartes

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
C	O	M	M	E	-	L	E	S	-	M	A	T	H	É	M	A	T	I	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!

1	E	C	-	O	L	M	E	M
2	L	E	M	C	E	-	M	O
3	E	L	-	E	M	M	O	C
4	M	E	M	L	O	-	C	E

FARO-*IN*
4 **mélanges**

Cryptographie — 2e message regroupé à chiffrer

1er + 2e paquets	3e paquet
$N_1 + N_2 = 20$ cartes	$N_3 = 24$ cartes

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
M	E	M	L	O	-	C	E	S	-	M	A	T	H	É	M	A	T	I	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!

1er + 2e paquets
$N_1 + N_2 = 20$ cartes

3e paquet
$N_3 = 24$ cartes

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
M	E	M	L	O	-	C	E	S	-	M	A	T	H	É	M	A	T	I	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!

1	M	M	E	A	M	T	L	H	O	É	-	M	C	A	E	T	S	I	-	Q																								1
2	M	-	M	M	E	C	A	A	M	E	T	T	L	S	H	I	O	-	É	Q																								2
3	M	T	-	T	M	L	M	S	E	H	C	I	A	O	A	-	M	É	E	Q																								3
4	M	C	T	I	-	A	T	O	M	A	L	-	M	M	S	É	E	E	H	Q																								4
5	M	L	C	-	T	M	I	M	-	S	A	É	T	E	O	E	M	H	A	Q																								5
6	M	A	L	É	C	T	-	E	T	O	M	E	I	M	M	H	-	A	S	Q																								6
7	M	M	A	E	L	I	É	M	C	M	T	H	-	-	E	A	T	S	O	Q																								7
8	M	T	M	H	A	-	E	-	L	E	I	A	É	T	M	S	C	O	M	Q																								8
9	M	I	T	A	M	É	H	T	A	M	-	S	E	C	-	O	L	M	E	Q																								9
10	M	-	I	S	T	E	A	C	M	-	É	O	H	L	T	M	A	E	M	Q																								10
11	M	É	-	O	I	H	S	L	T	T	E	M	A	A	C	E	M	M	-	Q																								11
12	M	E	É	M	-	A	O	A	I	C	H	E	S	M	L	M	T	-	T	Q																								12
13	M	H	E	E	É	S	M	M	-	L	A	M	O	T	A	-	I	T	C	Q																								13
14	M	A	H	M	E	O									M	T	-	C	L	Q																								14
15	M	S	A	-	H	M									T	C	É	L	A	Q																								15
16	M	O	S	T	A	E									I	L	E	A	M	Q																								16
17	M	M	O	C	S	M	I	E	A	I	E	L	-	E	-	A	H	M	T	Q																								17
18	M	E	M	L	O	-	C	E	S	-	M	A	T	H	É	M	A	T	I	Q																								18

FARO-*OUT*
période *18*

1er + 2e paquets

$N_1 + N_2 = 20$ cartes

3e paquet

$N_3 = 24$ cartes

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
M	E	M	L	O	-	C	E	S	-	M	A	T	H	É	M	A	T	I	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!

1	M	M	E	A	M	T	L	H	O	É	-	M	C	A	E	T	S	I	-	Q																								1
2	M	-	M	M	E	C	A	A	M	E	T	T	L	S	H	I	O	-	É	Q																								2
3	M	T	-	T	M	L	M	S	E	H	C	I	A	O	A	-	M	É	E	Q																								3
4	M	C	T	I	-	A	T	O	M	A	L	-	M	M	S	É	E	E	H	Q																								4
5	M	L	C	-	T	M	I	M	-	S	A	É	T	E	O	E	M	H	A	Q																								5
6	M	A	L	É	C	T	-	E	T	O	M	E	I	M	M	H	-	A	S	Q																								6
7	M	M	A	E	L	I	É	M	C	M	T	H	-	-	E	A	T	S	O	Q																								7
8	M	T	M	H	A	-	E	-	L	E	I	A	É	T	M	S	C	O	M	Q																								8
9	M	I	T	A	M	É	H	T	A	M	-	S	E	C	-	O	L	M	E	Q																								9
10	M	-	I	S	T	E	A	C	M	-	É	O	H	L	T	M	A	E	M	Q																								10
11	M	É	-	O	I	H	S	L	T	T	E	M	A	A	C	E	M	M	-	Q																								11

FARO-*OUT*

11 **mélanges**

Cryptographie 3e message regroupé à chiffrer

1er + 2e + 3e paquets

$N_1 + N_2 + N_3 = 44$ **cartes**

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
M	É	-	O	I	H	S	L	T	T	E	M	A	A	C	E	M	M	-	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!

$1^{er} + 2^{e} + 3^{e}$ paquets

$N_1 + N_2 + N_3 = 44$ cartes

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
M	É	-	O	I	H	S	L	T	T	E	M	A	A	C	E	M	M	-	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!

1	S	M	-	É	S	-	O	O	N	I	T	H	-	S	P	L	A	T	S	T	S	E	I	M	O	A	N	A	N	C	A	E	N	M	T	M	E	-	S	Q	-	U	!	E	1
2	I	S	M	M	O	-	A	É	N	S	A	-	N	O	C	O	A	N	E	I	N	T	M	H	T	-	M	S	E	P	-	L	S	A	Q	T	-	S	U	T	!	S	E	E	2
3	M	I	H	S	T	M	-	M	M	O	S	-	E	A	P	É	-	N	L	S	S	A	A	-	Q	N	T	O	-	C	S	O	U	A	T	N	!	E	S	I	E	N	E	T	3
4	A	M	-	I	Q	H	N	S	T	T	O	M	-	-	C	M	S	M	O	O	U	S	A	-	T	E	N	A	!	P	E	É	S	-	I	N	E	L	N	S	E	S	T	A	4
5	A	A	-	M	T	-	E	I	N	Q	A	H	!	N	P	S	E	T	É	T	S	O	-	M	I	-	N	-	E	C	L	M	N	S	S	M	E	O	S	O	T	U	A	S	5
6	-	A	M	A	I	-	-	M	N	T	-	-	E	E	C	I	L	N	M	Q	N	A	S	H	S	!	M	N	E	P	O	S	S	E	O	T	T	É	U	T	A	S	S	O	6
7	S	-	H	A	S	M	!	A	M	I	N	-	E	-	P	M	O	N	S	T	S	-	E	-	O	E	T	E	T	C	É	I	U	L	T	N	A	M	S	Q	S	N	O	A	7
8	E	S	-	-	O	H	E	A	T	S	E	M	T	!	C	A	É	M	I	I	U	N	L	-	T	E	N	-	A	P	M	M	S	O	Q	N	S	S	N	T	O	S	A	-	8
9	L	E	-	S	T	-	E	-	N	O	-	H	A	E	P	A	M	T	M	S	S	E	O	M	Q	T	N	!	S	C	S	A	N	É	T	M	O	I	S	I	A	U	-	N	9
10	O	L	M	E	Q	-	T	S	N	T	!	-	S	E	C	-	S	N	A	O	N	-	É	H	T	A	M	E	O	P	I	A	S	M	I	T	A	M	U	S	-	S	N	E	10
11	É	O	H	L	T	M	A	E	M	Q	E	-	O	T	P	S	I	N	A	T	S	!	M	-	I	S	T	E	A	C	M	-	U	S	S	N	-	A	S	O	N	N	E	-	11
12	M	É	-	O	I	H	S	L	T	T	E	M	A	A	C	E	M	M	-	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!	12

FARO-*IN*
période *12*

$1^{er} + 2^{e} + 3^{e}$ paquets

$N_1 + N_2 + N_3 = 44$ cartes

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
M	É	-	O	I	H	S	L	T	T	E	M	A	A	C	E	M	M	-	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!

1	S	M	-	É	S	-	O	O	N	I	T	H	-	S	P	L	A	T	S	T	S	E	I	M	O	A	N	A	N	C	A	E	N	M	T	M	E	-	S	Q	-	U	!	E
2	I	S	M	M	O	-	A	É	N	S	A	-	N	O	C	O	A	N	E	I	N	T	M	H	T	-	M	S	E	P	-	L	S	A	Q	T	-	S	U	T	!	S	E	E
3	M	I	H	S	T	M	-	M	M	O	S	-	E	A	P	É	-	N	L	S	S	A	A	-	Q	N	T	O	-	C	S	O	U	A	T	N	!	E	S	I	E	N	E	T
4	A	M	-	I	Q	H	N	S	T	T	O	M	-	-	C	M	S	M	O	O	U	S	A	-	T	E	N	A	!	P	E	É	S	-	I	N	E	L	N	S	E	S	T	A
5	A	A	-	M	T	-	E	I	N	Q	A	H	!	N	P	S	E	T	É	T	S	O	-	M	I	-	N	-	E	C	L	M	N	S	S	M	E	O	S	O	T	U	A	S

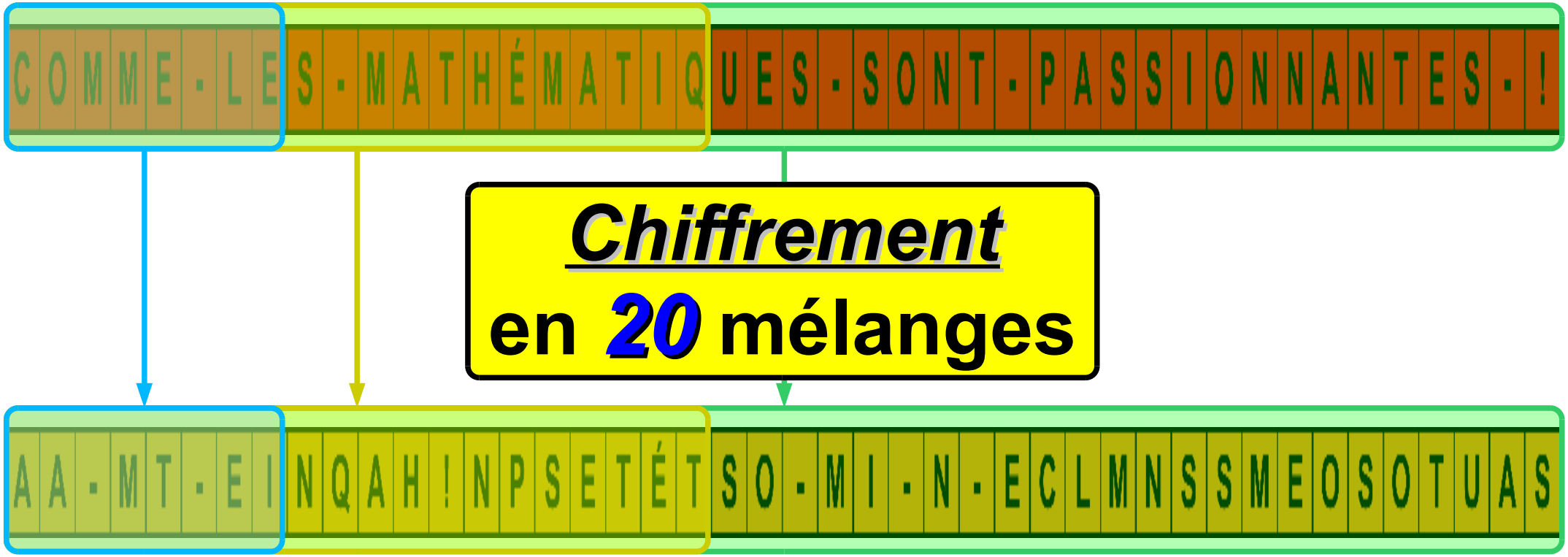
FARO-*IN*

5 **mélanges**

$1^{er} + 2^{e} + 3^{e}$ paquets

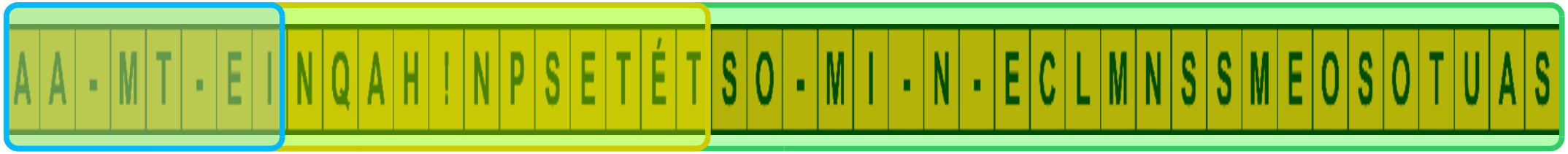
$N_1 + N_2 + N_3 = 44$ cartes

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
M	É	-	O	I	H	S	L	T	T	E	M	A	A	C	E	M	M	-	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!
A	A	-	M	T	-	E	I	N	Q	A	H	!	N	P	S	E	T	É	T	S	O	-	M	I	-	N	-	E	C	L	M	N	S	S	M	E	O	S	O	T	U	A	S


COMME-LES-MATHÉMATIQUES-SONT-PASSIONNANTES-!
Chiffrement
en 20 mélanges
AA-MT-EINQAH!NPSETÉTSO-MI-N-ECLMNSSMEOSOTUAS

Le message à déchiffrer

AA-MT-EINQAH !
NPSETÉTSO-MI-N-
ECLMNSSMEOSOTUAS



1er + 2e + 3e paquets

$N_1 + N_2 + N_3 = 44$ **cartes**

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
A	A	-	M	T	-	E	I	N	Q	A	H	!	N	P	S	E	T	É	T	S	O	-	M	I	-	N	-	E	C	L	M	N	S	S	M	E	O	S	O	T	U	A	S

1er + 2e + 3e paquets

$N_1 + N_2 + N_3 = 44$ **cartes**

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
A	A	-	M	T	-	E	I	N	Q	A	H	!	N	P	S	E	T	É	T	S	O	-	M	I	-	N	-	E	C	L	M	N	S	S	M	E	O	S	O	T	U	A	S

6	-	A	M	A	I	-	-	M	N	T	-	-	E	E	C	I	L	N	M	Q	N	A	S	H	S	!	M	N	E	P	O	S	S	E	O	T	T	É	U	T	A	S	S	O
7	S	-	H	A	S	M	!	A	M	I	N	-	E	-	P	M	O	N	S	T	S	-	E	-	O	E	T	E	T	C	É	I	U	L	T	N	A	M	S	Q	S	N	O	A
8	E	S	-	-	O	H	E	A	T	S	E	M	T	!	C	A	É	M	I	I	U	N	L	-	T	E	N	-	A	P	M	M	S	O	Q	N	S	S	N	T	O	S	A	-
9	L	E	-	S	T	-	E	-	N	O	-	H	A	E	P	A	M	T	M	S	S	E	O	M	Q	T	N	!	S	C	S	A	N	É	T	M	O	I	S	I	A	U	-	N
10	O	L	M	E	Q	-	T	S	N	T	!	-	S	E	C	-	S	N	A	O	N	-	É	H	T	A	M	E	O	P	I	A	S	M	I	T	A	M	U	S	-	S	N	E
11	É	O	H	L	T	M	A	E	M	Q	E	-	O	T	P	S	I	N	A	T	S	!	M	-	I	S	T	E	A	C	M	-	U	S	S	N	-	A	S	O	N	N	E	-
12	M	É	-	O	I	H	S	L	T	T	E	M	A	A	C	E	M	M	-	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!

FARO-*IN*

7 **mélanges**

1er + 2e paquets	3e paquet
$N_1 + N_2 = 20$ cartes	$N_3 = 24$ cartes

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
M	É	-	O	I	H	S	L	T	T	E	M	A	A	C	E	M	M	-	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!

Cryptographie

2e déchiffrement

1er + 2e paquets

$N_1 + N_2 = 20$ cartes

3e paquet

$N_3 = 24$ cartes

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
M	É	-	O	I	H	S	L	T	T	E	M	A	A	C	E	M	M	-	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!

12	M	E	É	M	-	A	O	A	I	C	H	E	S	M	L	M	T	-	T	Q																								12
13	M	H	E	E	É	S	M	M	-	L	A	M	O	T	A	-	I	T	C	Q																								13
14	M	A	H	M	E	O	E	T	É	A	S	-	M	I	M	T	-	C	L	Q																								14
15	M	S	A	-	H	M	M	I	E	M	O	T	E	-	T	C	É	L	A	Q																								15
16	M	O	S	T	A	E	-	-	H	T	M	C	M	É	I	L	E	A	M	Q																								16
17	M	M	O	C	S	M	T	É	A	I	E	L	-	E	-	A	H	M	T	Q																								17
18	M	E	M	L	O	-	C	E	S	-	M	A	T	H	É	M	A	T	I	Q																								18

FARO-*OUT*

7 **mélanges**

Cryptographie

3e déchiffrement

1er paquet	2e paquet	3e paquet
$N_1 = 8$ cartes	$N_2 = 12$ cartes	$N_3 = 24$ cartes

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
M	E	M	L	O	-	C	E	S	-	M	A	T	H	É	M	A	T	I	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!

Cryptographie

3e déchiffrement

1er paquet	2e paquet	3e paquet
$N_1 = 8$ cartes	$N_2 = 12$ cartes	$N_3 = 24$ cartes

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
M	E	M	L	O	-	C	E	S	-	M	A	T	H	É	M	A	T	I	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!

5	O	M	-	E	C	M	E	L																																					5
6	C	O	M	M	E	-	L	E																																					6

FARO-*IN*

2 **mélanges**

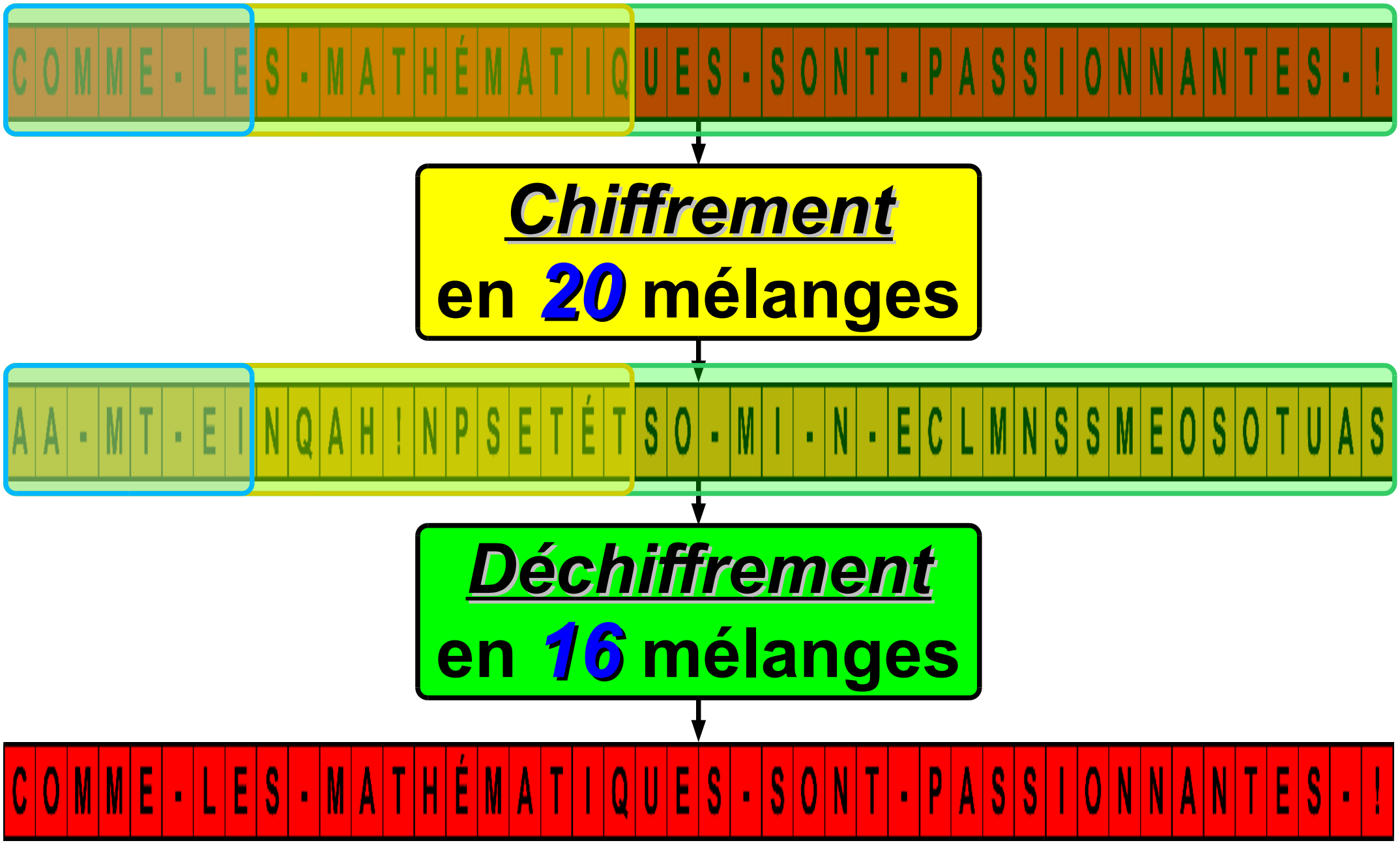
Cryptographie

Le message déchiffré

1er paquet	2e paquet	3e paquet
$N_1 = 8$ cartes	$N_2 = 12$ cartes	$N_3 = 24$ cartes

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
C	O	M	M	E	-	L	E	S	-	M	A	T	H	É	M	A	T	I	Q	U	E	S	-	S	O	N	T	-	P	A	S	S	I	O	N	N	A	N	T	E	S	-	!

Le message déchiffré

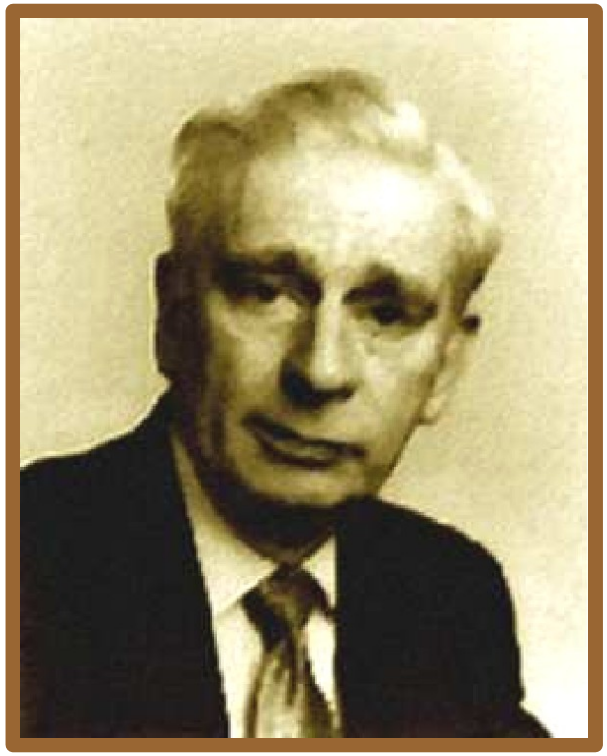

COMME-LES-MATHÉMATIQUES-SONT-PASSIONNANTES-!
Chiffrement
en 20 mélanges
AA-MT-EINQAH!NPSETÉTSO-MI-N-ECLMNSSMEOSOTUAS
Déchiffrement
en 16 mélanges
COMME-LES-MATHÉMATIQUES-SONT-PASSIONNANTES-!

CASINO ROYAL

LE PROBLÈME D'ELMSLEY

LE PROBLÈME D'ELMSLEY

Comment déplacer une carte vers une position fixée par une suite de Faros-*in* ou/et de Faros-*out* ?

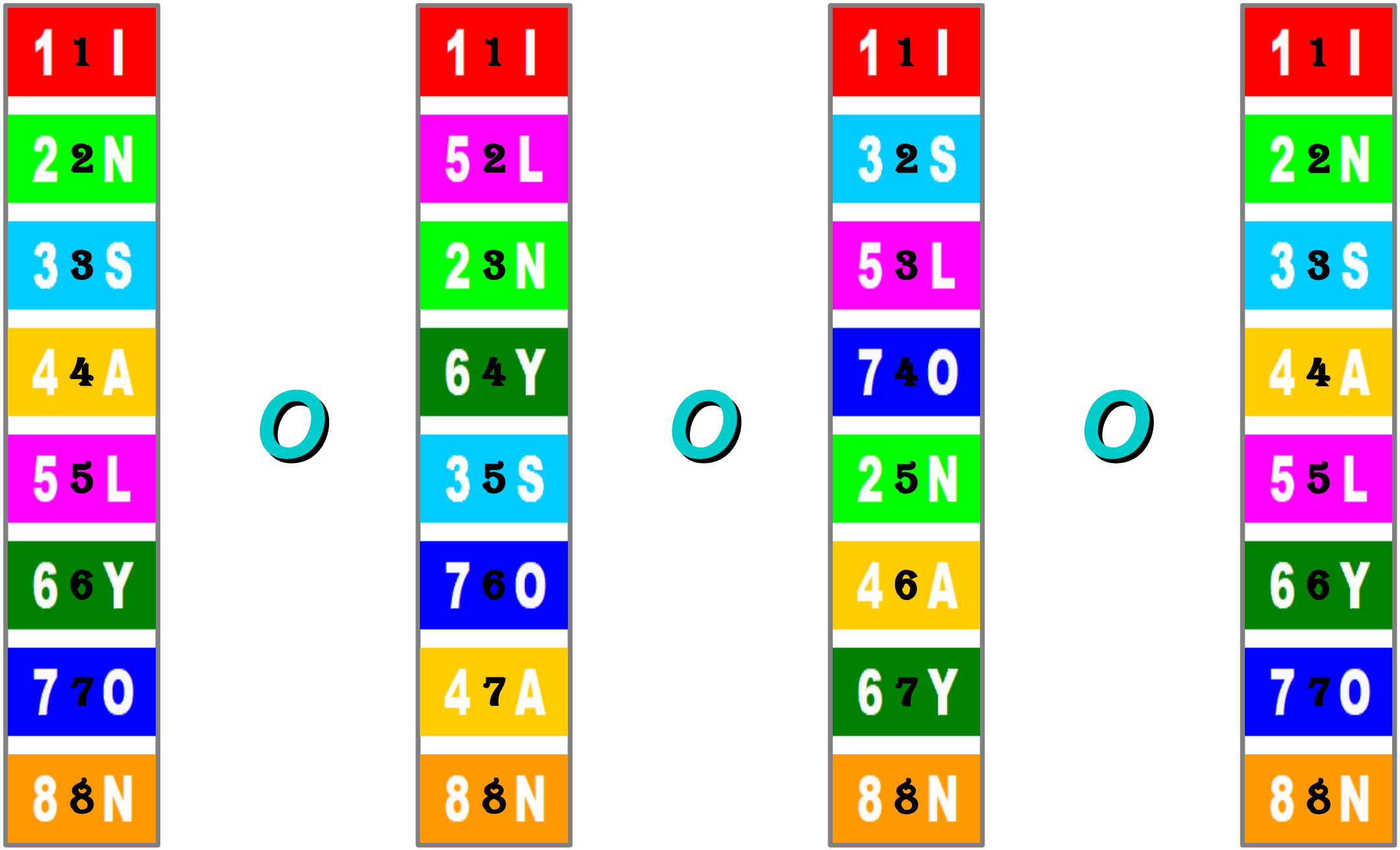


Alex Elmsley
(1929–2006)

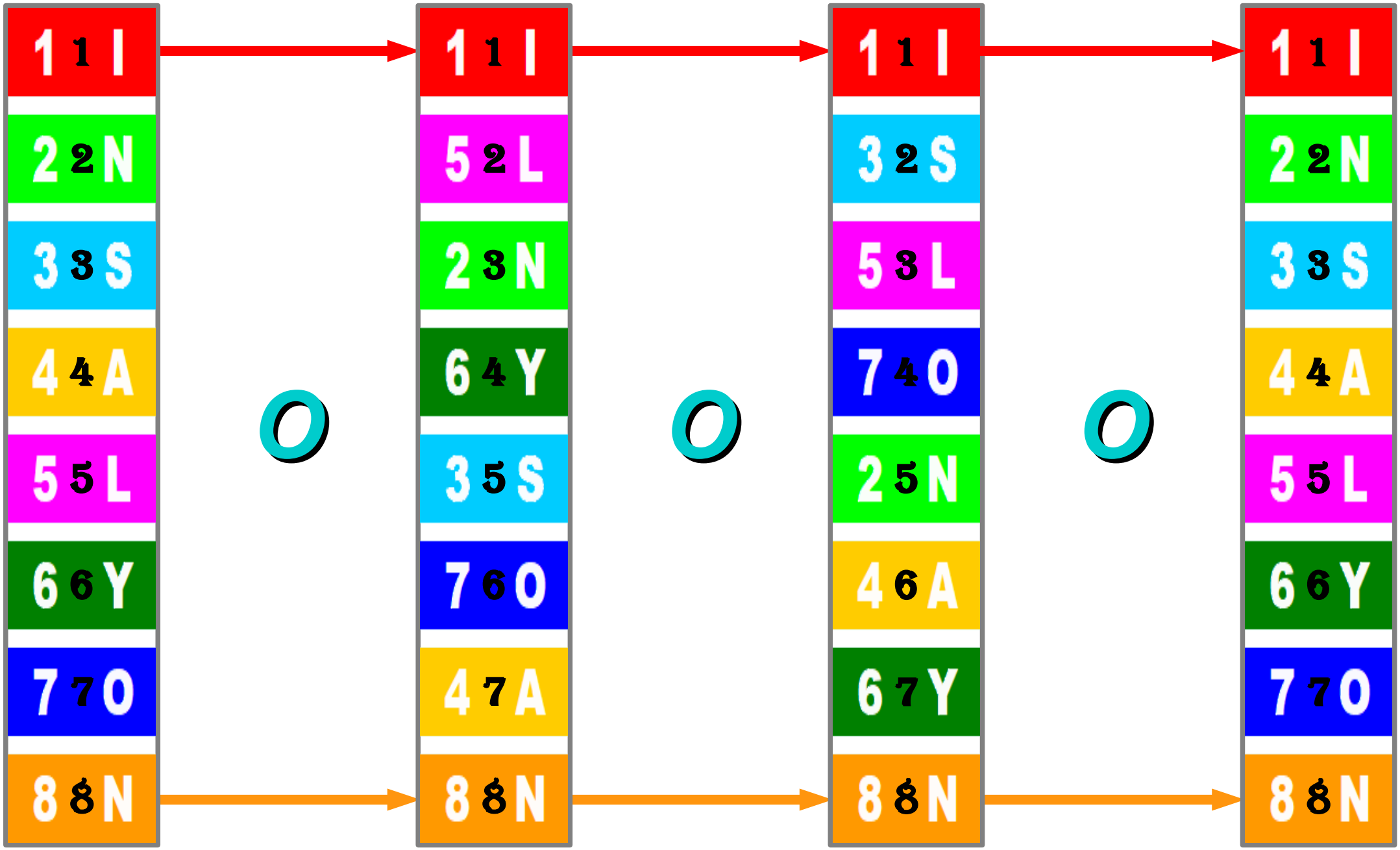
Magicien et informaticien écossais

FAROS-OUT

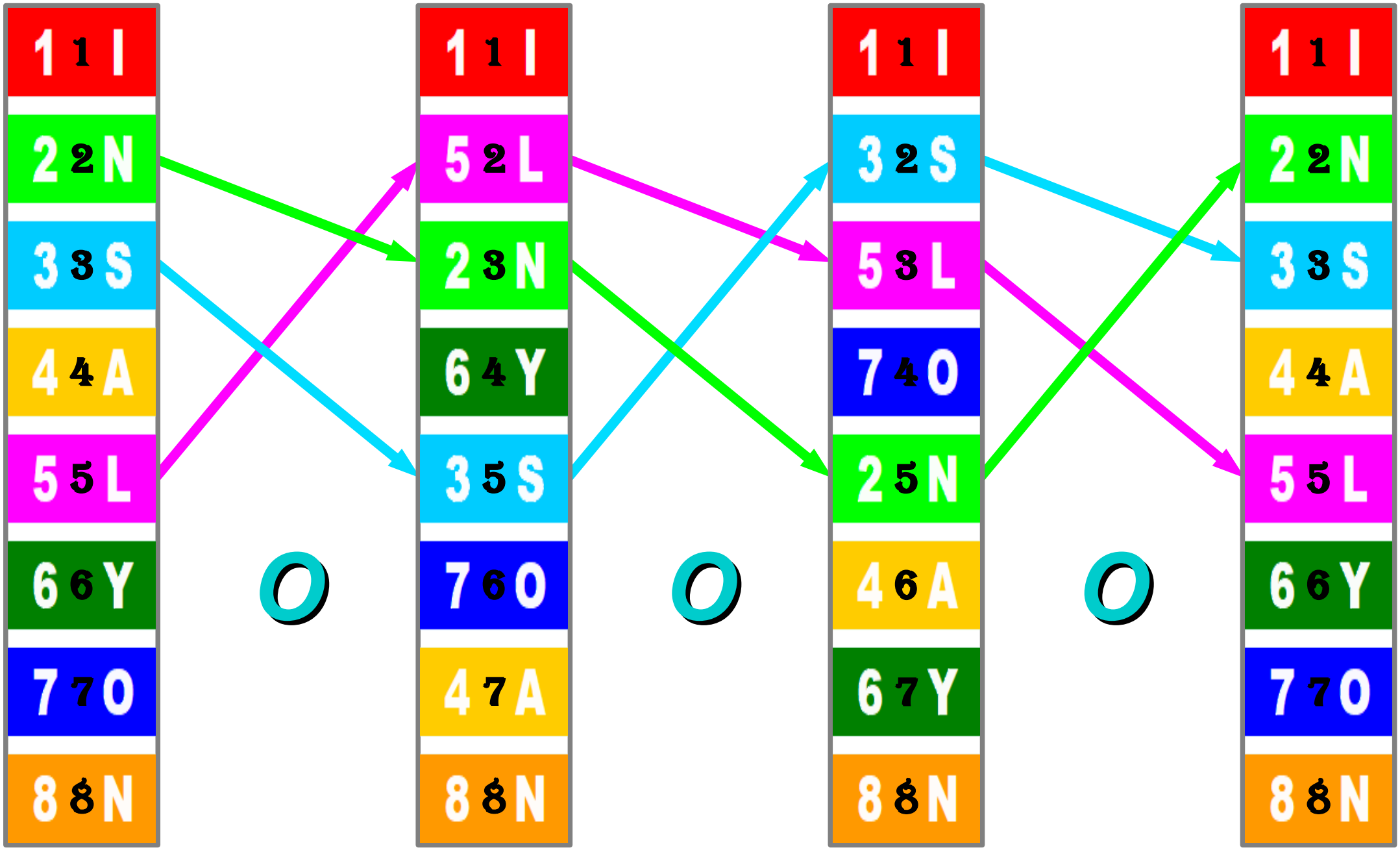
Orbites d'une suite de Faros-out



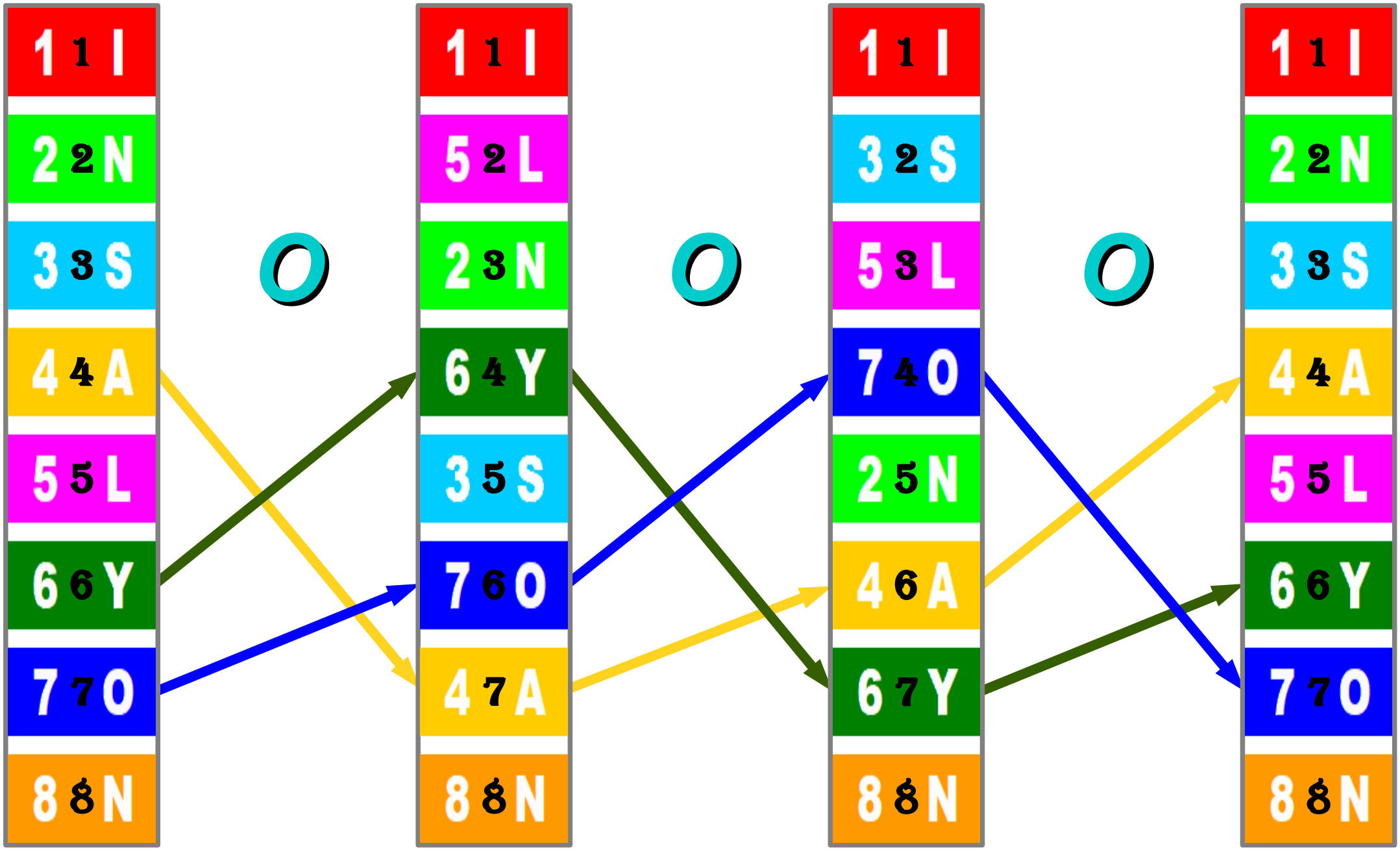
Orbites d'une suite de Faros-out



Orbites d'une suite de Faros-out



Orbites d'une suite de Faros-out



Orbites d'une suite de Faros-out

Constat :

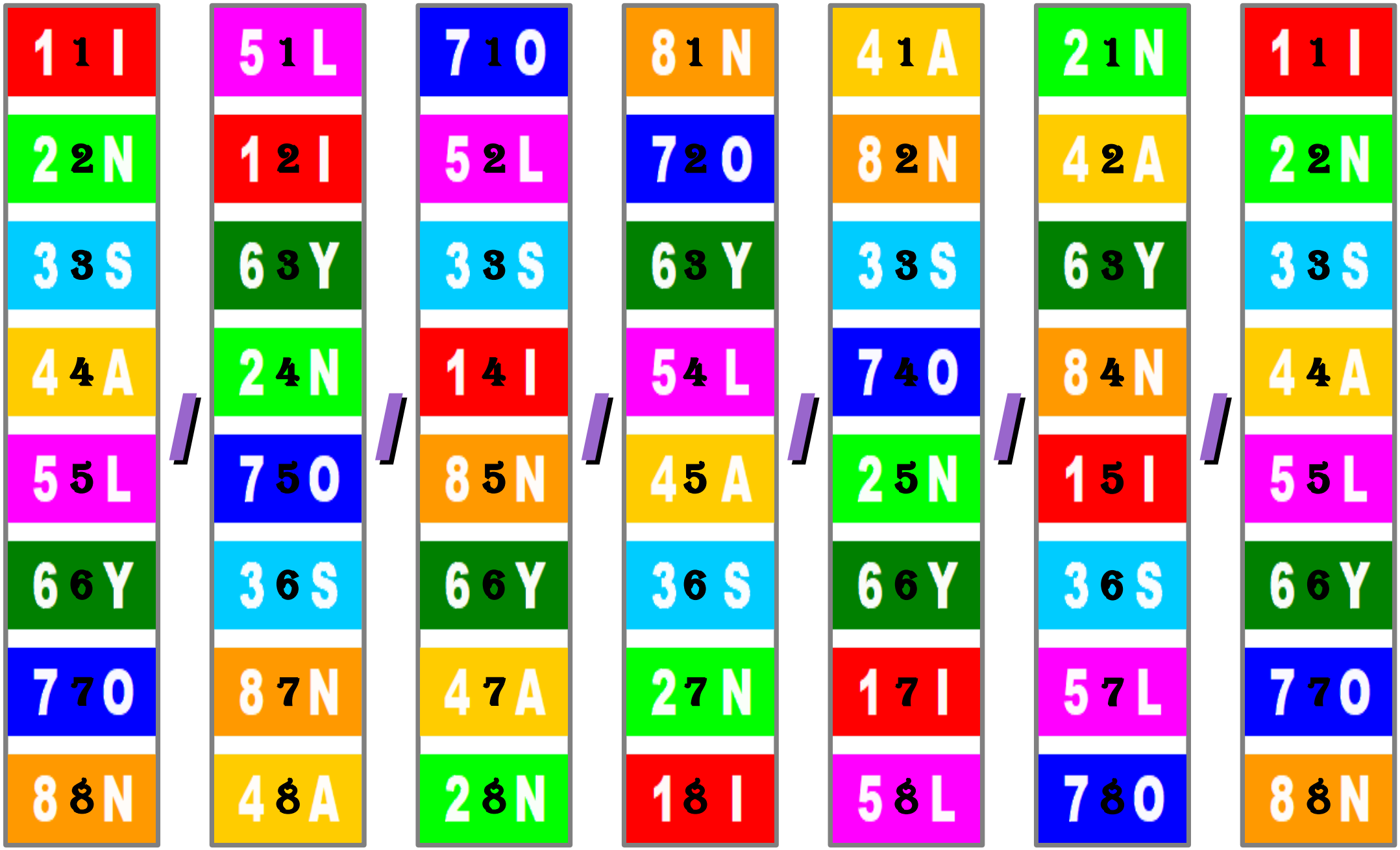
- *Une carte située en position 2, 3 ou 5 visite ces mêmes positions au cours d'une suite de Faros-out.*

  De même pour les positions 4, 6 ou 7.

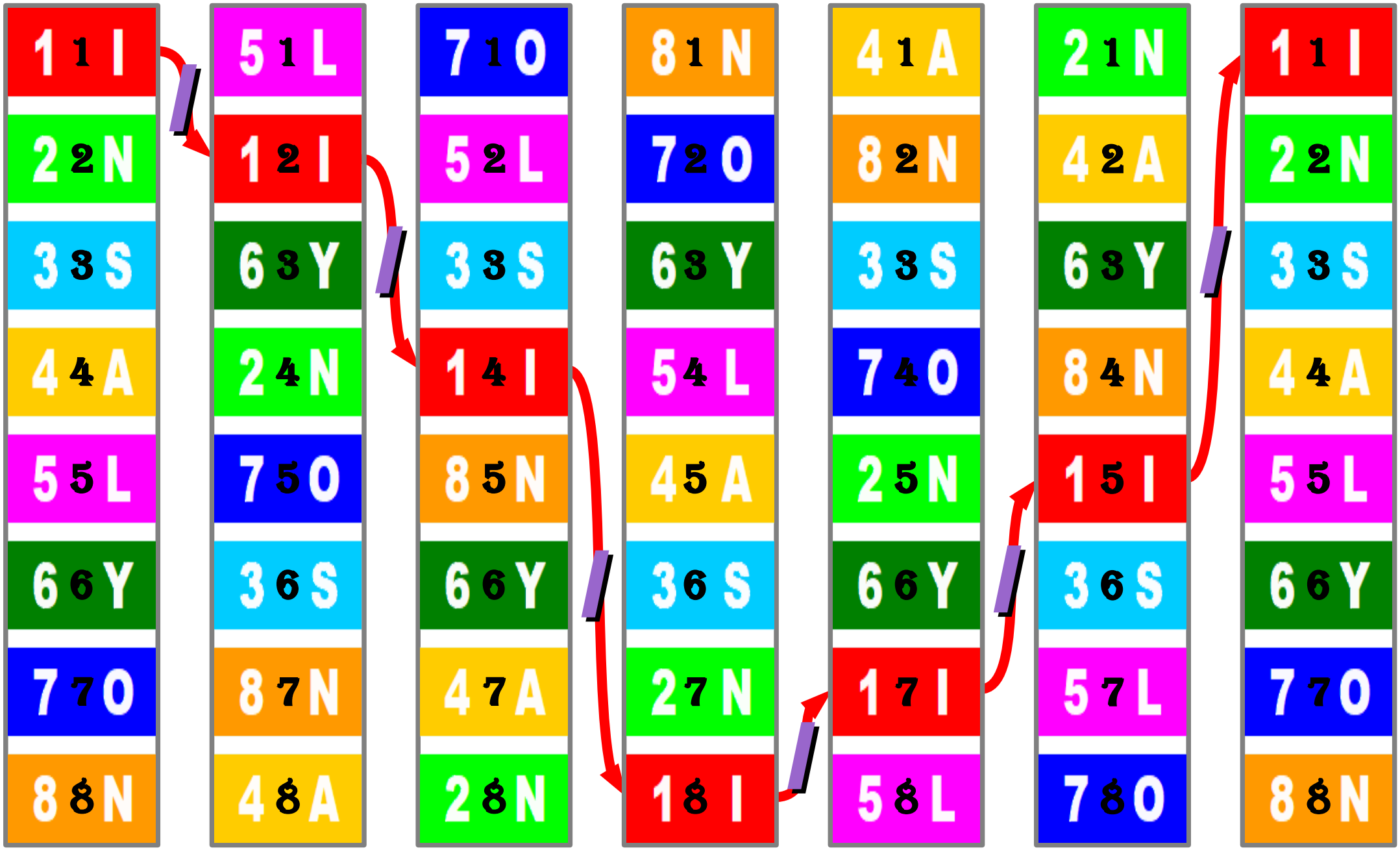
- *Il est donc impossible de déplacer une carte initialement située en position 2, 3 ou 5 vers l'une des positions 4, 6 ou 7 par une suite de Faros-out (et inversement).*

FAROS-IN

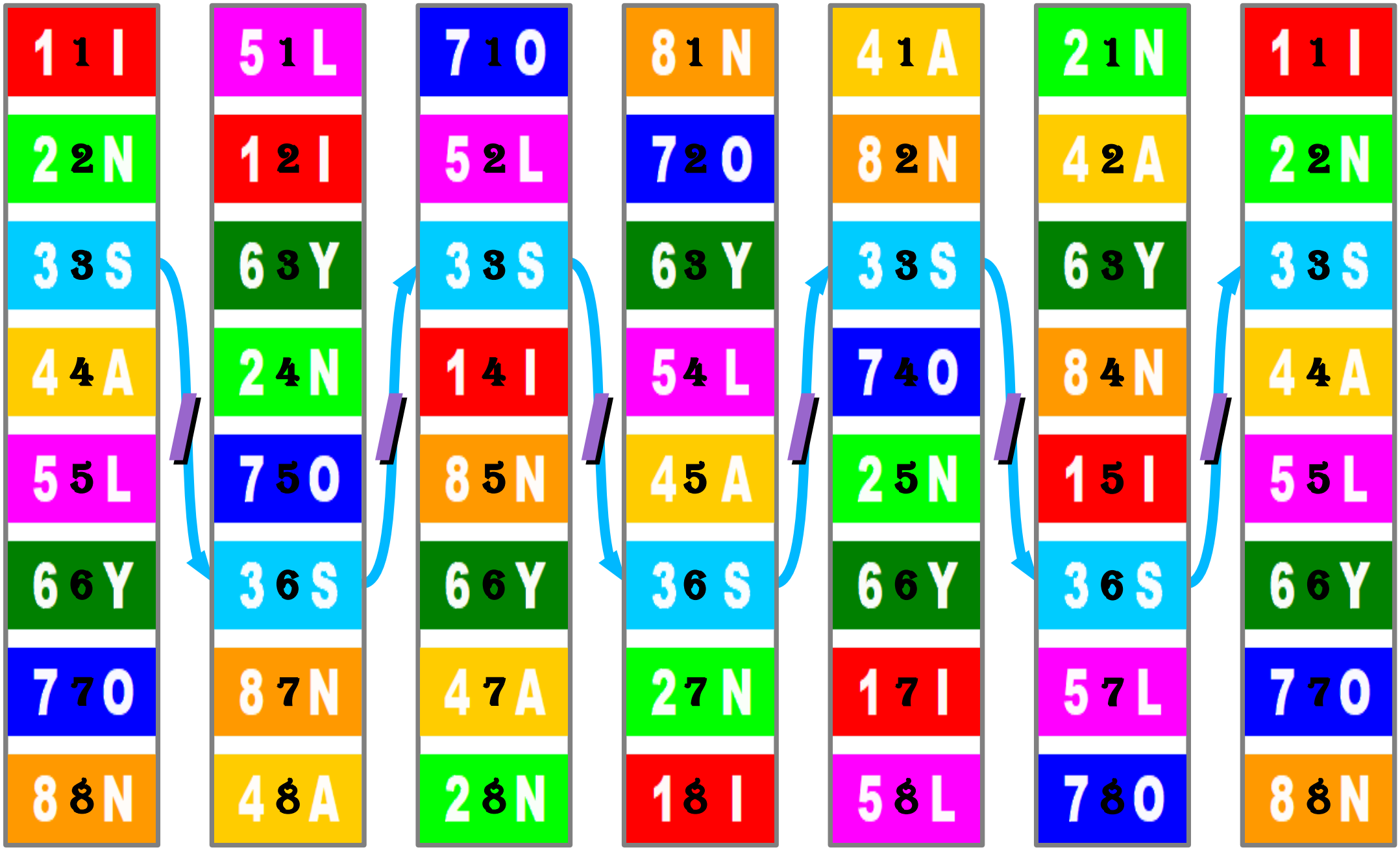
Orbites d'une suite de Faros-in



Orbites d'une suite de Faros-in



Orbites d'une suite de Faros-in



Orbites d'une suite de Faros-in

Constat :

- ***Une carte située en position 1, 2, 4, 5, 7 ou 8 visite ces mêmes positions au cours d'une suite de Faros-in.***

  De même pour les positions 3 et 6.

- ***Il est donc impossible de déplacer une carte initialement située en position 1, 2, 4, 5, 7 ou 8 vers l'une des positions 3 ou 6 par une suite de Faros-in (et inversement).***

FAROS-IN
&
FAROS-OUT

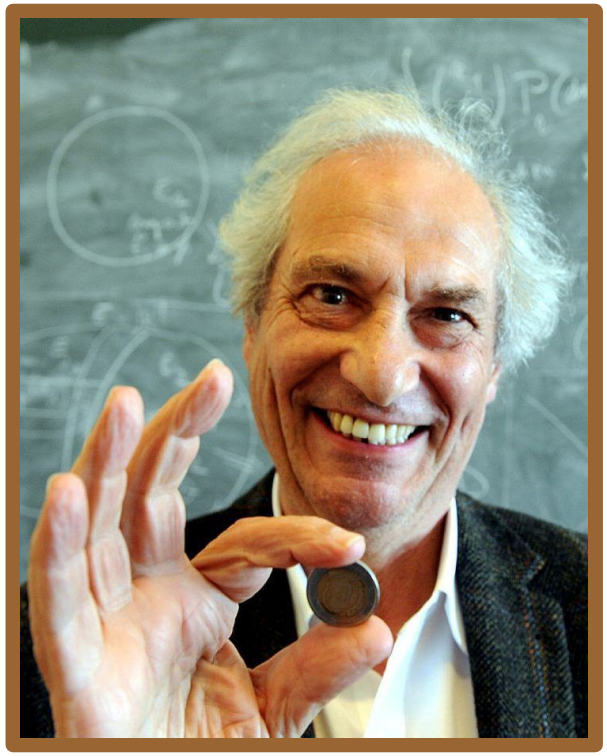
RÉSOLUTION

Un algorithme en binaire avec de Faros-in et -out

Référence :

P. Diaconis and R. Graham :

The solutions to Elmsley's Problem, Math Horizons 14 (2007), p. 22–27

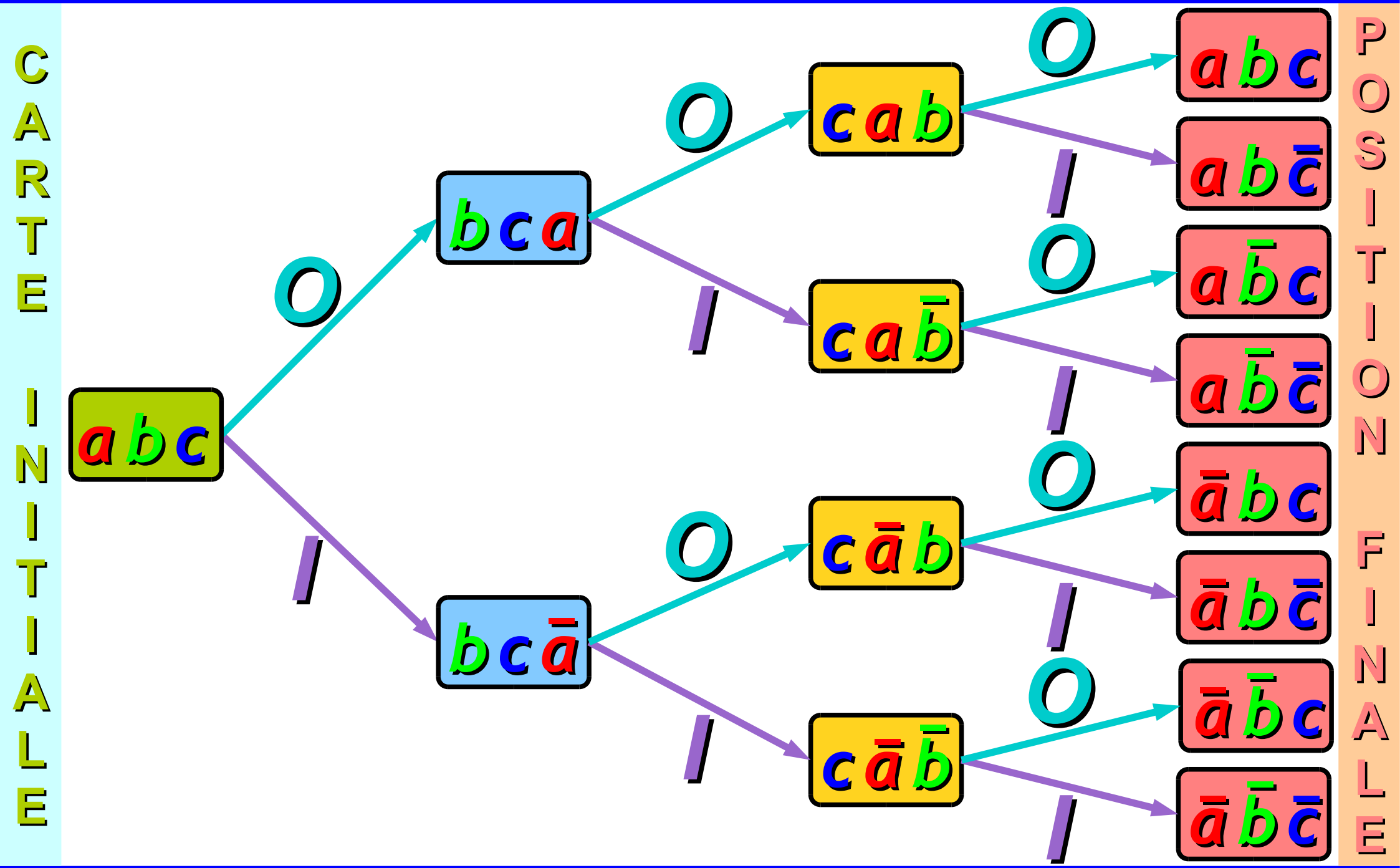


Persi Diaconis

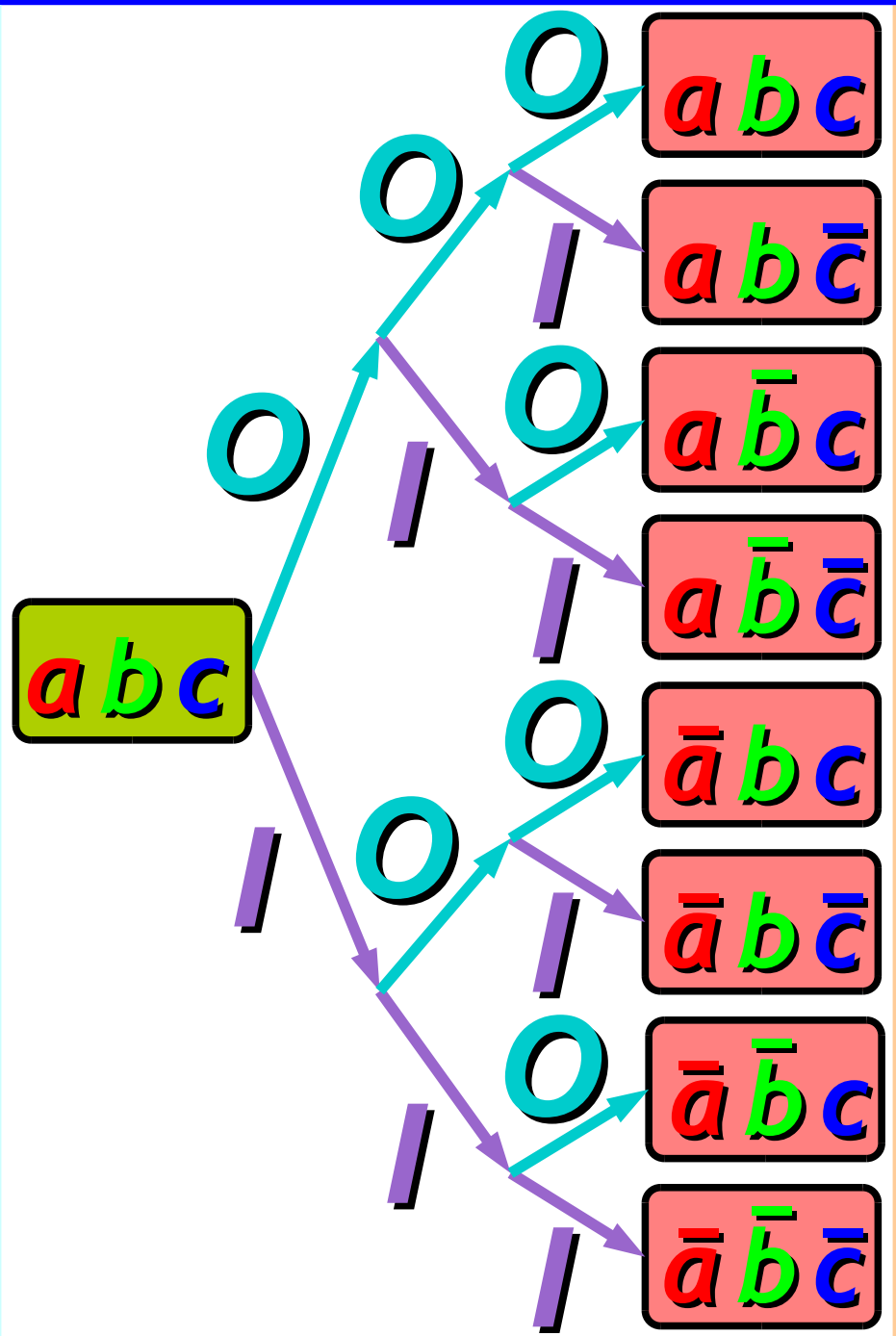
(1945–)

Magicien et mathématicien américain

Déplacement d'une carte vers une position



Un algorithme



Déplacement d'une carte

abc

vers une position finale

$a'b'c'$

si $a' = \begin{cases} a \rightarrow 1^{er} \text{ mélange OUT} \\ \bar{a} \rightarrow 1^{er} \text{ mélange IN} \end{cases}$

si $b' = \begin{cases} b \rightarrow 2^{e} \text{ mélange OUT} \\ \bar{b} \rightarrow 2^{e} \text{ mélange IN} \end{cases}$

si $c' = \begin{cases} c \rightarrow 3^{e} \text{ mélange OUT} \\ \bar{c} \rightarrow 3^{e} \text{ mélange IN} \end{cases}$

Un algorithme

a	b	c
a'	b'	c'
1^{er} mélange	2^{e} mélange	3^{e} mélange
si $a=a'$:	si $b=b'$:	si $c=c'$:
O	O	O
sinon :	sinon :	sinon :
I	I	I

Exemple : **pour un jeu de 8 cartes numérotées 1 à 8 :**

amener la 4^{e} carte à la 3^{e} position

En renumérotant de 0 à 7:

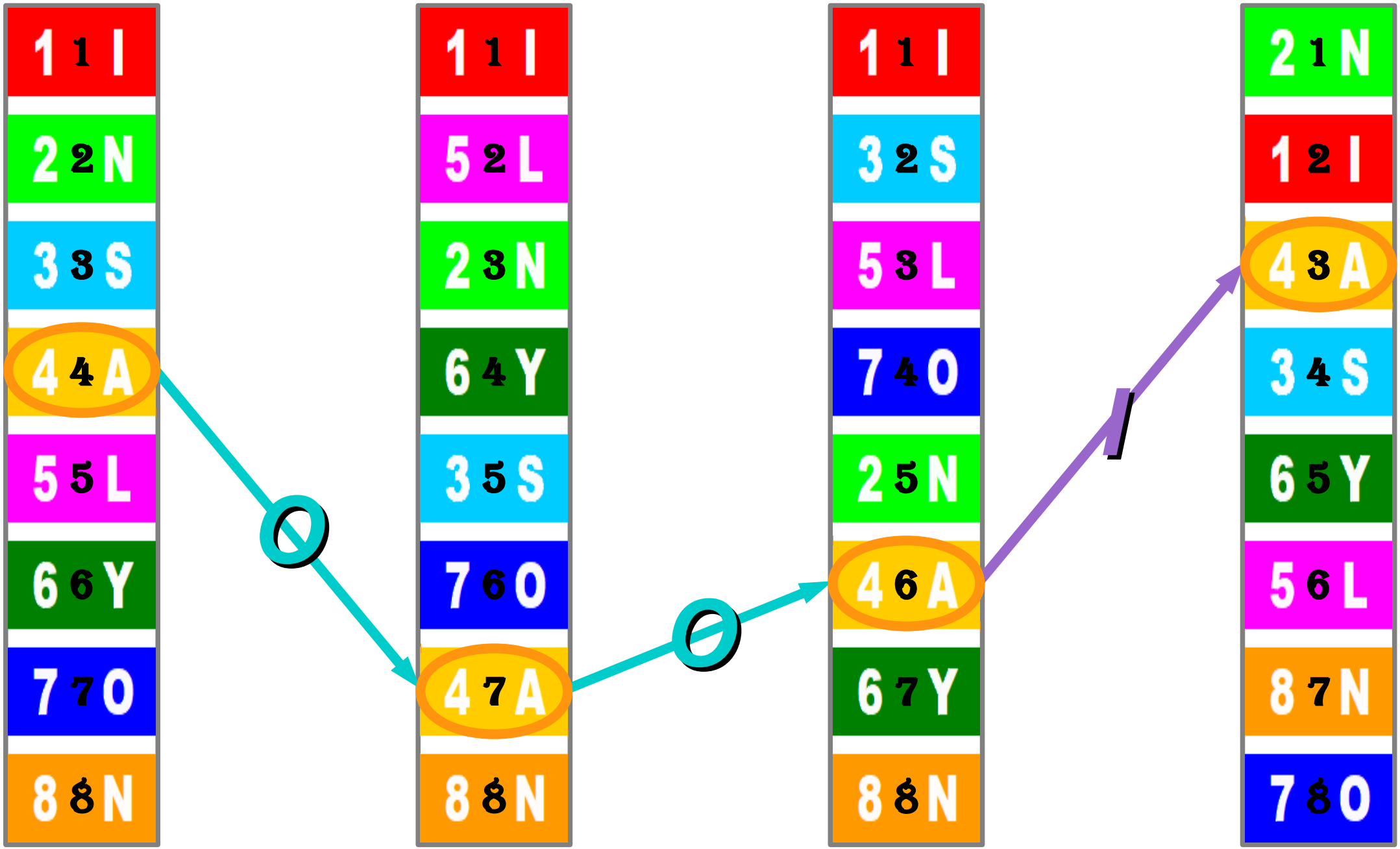
4^{e} carte → n° 3 = $(011)_2$

3^{e} position → n° 2 = $(010)_2$

$(0$	1	$1)_2$	
$(0$	1	$0)_2$	
O	O	I	

→ on réalisera 2 Faros-out suivis d'un Faro-in

Un algorithme



Un algorithme : généralisation

Théorème : **pour un jeu de 2^p cartes, pour amener une carte d'une position i vers une position j, on compare les bits de i et j :**

$$i = (\, i_{p-1} \;\; i_{p-2} \;\; \cdots \;\; i_1 \;\; i_0 \,)_2$$
$$j = (\, j_{p-1} \;\; j_{p-2} \;\; \cdots \;\; j_1 \;\; j_0 \,)_2$$

$= 0$	$= 0$		$= 0$	$= 0$
$\neq 1$	$\neq 1$		$\neq 1$	$\neq 1$

À chaque *coïncidence* est associé un Faro-out et à chaque *différence* est associé un Faro-in. On effectuera alors la suite de Faros correspondante *de la gauche vers la droite*.

CASINO ROYAL

CONCLUSION

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 !

MERCI DE VOTRE ATTENTION !

http://math.univ-lyon1.fr/~alachal/diaporamas/diaporama_melanges_faros.pdf