

# Transformations d'images

A.-M. Aebischer / Journées nationales de l'APMEP 2012

IREM de Franche-Comté

31 Novembre 2012

- 1 Brouiller une image : la méthode du photomaton
- 2 Exemples
- 3 Simplification du problème
- 4 Retour d'une image
- 5 Temps de retour d'une image

- Une image numérique est composée de pixels ;
- *Brouiller une image*, c'est appliquer une méthode pour mélanger les pixels.

- Une image numérique est composée de pixels ;
- *Brouiller une image*, c'est appliquer une méthode pour mélanger les pixels.

## La transformation du photomaton

Pour transformer une image de dimension paire :

Image initiale

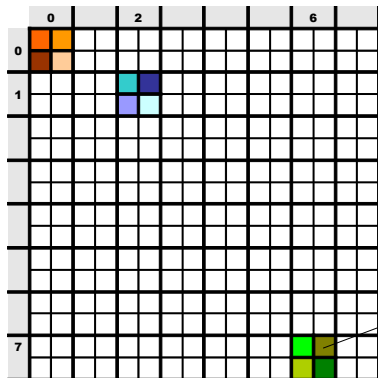
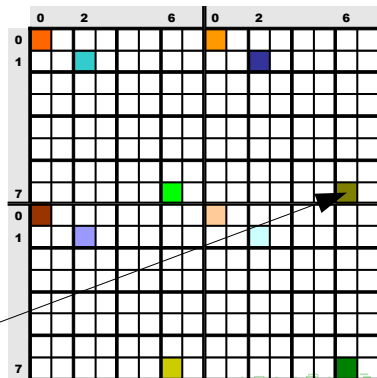


Image après transformation



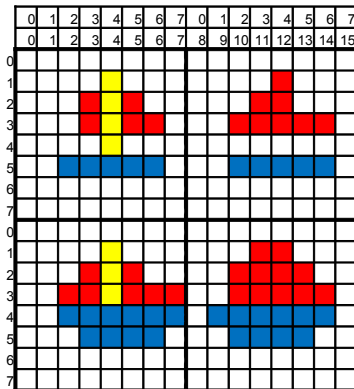
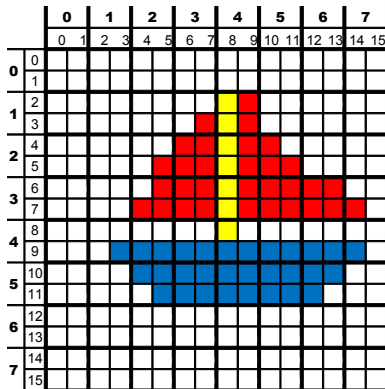
# La transformation du photomaton

## Exemple 1

	0		1		2		3		4		5		6		7	
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0																
1																
2																
3																
4																
5																
6																
7																
8																
9																
10																
11																
12																
13																
14																
15																

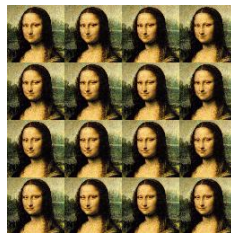
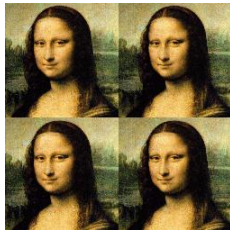
# La transformation du photomaton

## Exemple 1



# La transformation du photomaton

## Exemple 2



Et si on continue ?



## Bilan des essais

On retrouve toujours l'image initiale au bout d'un nombre fini d'essais.

Ce nombre d'essais est très variable :

- *La Joconde* de taille 256x256 : 8 étapes ;
- *La Joconde* de taille 260x260 : 36 étapes ;
- *La Joconde* de taille 512x512 : 9 étapes ;
- *Les manchots* de taille 640x640 : 210 étapes.

## Bilan des essais

On retrouve toujours l'image initiale au bout d'un nombre fini d'essais.

Ce nombre d'essais est très variable :

- *La Joconde* de taille 256x256 : 8 étapes ;
- *La Joconde* de taille 260x260 : 36 étapes ;
- *La Joconde* de taille 512x512 : 9 étapes ;
- *Les manchots* de taille 640x640 : 210 étapes.

## Bilan des essais

On retrouve toujours l'image initiale au bout d'un nombre fini d'essais.

Ce nombre d'essais est très variable :

- *La Joconde* de taille 256x256 : 8 étapes ;
- *La Joconde* de taille 260x260 : 36 étapes ;
- *La Joconde* de taille 512x512 : 9 étapes ;
- *Les manchots* de taille 640x640 : 210 étapes.

## Bilan des essais

On retrouve toujours l'image initiale au bout d'un nombre fini d'essais.

Ce nombre d'essais est très variable :

- *La Joconde* de taille 256x256 : 8 étapes ;
- *La Joconde* de taille 260x260 : 36 étapes ;
- *La Joconde* de taille 512x512 : 9 étapes ;
- *Les manchots* de taille 640x640 : 210 étapes.

## Questions

- Pourquoi retrouve-t-on **toujours** l'image initiale en mélangeant les pixels suivant cette méthode ?
- Cette propriété est-elle liée à la transformation utilisée ?
- Comment prévoir en fonction de la taille de l'image **le nombre d'essais** qui la feront réapparaître à l'identique ?

## Questions

- Pourquoi retrouve-t-on **toujours** l'image initiale en mélangeant les pixels suivant cette méthode ?
- Cette propriété est-elle liée à la transformation utilisée ?
- Comment prévoir en fonction de la taille de l'image **le nombre d'essais** qui la feront réapparaître à l'identique ?

## Questions

- Pourquoi retrouve-t-on **toujours** l'image initiale en mélangeant les pixels suivant cette méthode ?
- Cette propriété est-elle liée à la transformation utilisée ?
- Comment prévoir en fonction de la taille de l'image **le nombre d'essais** qui la feront réapparaître à l'identique ?

## Simplification du problème : les lignes

Lorsqu'on applique la transformation du photomaton, les pixels d'une ligne sont tous envoyés sur une même ligne.

Exemple : cas d'une image à 8 pixels

0	1	2	3	4	5	6	7	Position initiale
0	2	4	6	1	3	5	7	Position après transformation

La transformation reclasse les entiers : les pairs d'abord, suivis des entiers impairs.



## Simplification du problème : les colonnes

Lorsqu'on applique la transformation du photomaton, les pixels d'une colonne sont tous envoyés sur une même colonne.

Exemple : cas d'une image à 8 pixels

Position initiale	Position après transformation
0	0
1	2
2	4
3	6
4	1
5	3
6	5
7	7

Le déplacement d'un pixel par la méthode du photomaton s'obtient en appliquant la même transformation  $\sigma$  sur le numéro de ligne et sur le numéro de colonne :

$$(i, j) \mapsto (\sigma(i), \sigma(j))$$

Il suffit d'étudier la transformation sur les lignes !

## Quelques cas particuliers

### Cas d'une image à 8 pixels

0	1	2	3	4	5	6	7	Position initiale
0	2	4	6	1	3	5	7	après 1 transformation
0	4	1	5	2	6	3	7	après 2 transformations
0	1	2	3	4	5	6	7	après 3 transformations

Temps de retour = 3

## Quelques cas particuliers

### Cas d'une image à 10 pixels

0	1	2	3	4	5	6	7	8	9	Position initiale
0	2	4	6	8	1	3	5	7	9	après 1 transformation
0	4	8	3	7	2	6	1	5	9	après 2 transformations
0	8	7	6	5	4	3	2	1	9	après 3 transformations
0	7	5	3	1	8	6	4	2	9	après 4 transformations
0	5	1	6	2	7	3	8	4	9	après 5 transformations
0	1	2	3	4	5	6	7	8	9	après 6 transformations

Temps de retour = 6

## Quelques cas particuliers

- Pourquoi retrouve-t-on **toujours** l'image initiale en mélangeant les pixels suivant cette méthode ?
- Cette propriété est-elle liée à la transformation utilisée ?
- Comment prévoir en fonction de la taille de l'image **le nombre d'essais** qui la feront réapparaître à l'identique ?

## Quelques cas particuliers

- Pourquoi retrouve-t-on **toujours** l'image initiale en mélangeant les pixels suivant cette méthode ?
- Cette propriété est-elle liée à la transformation utilisée ?
- Comment prévoir en fonction de la taille de l'image **le nombre d'essais** qui la feront réapparaître à l'identique ?

## Quelques cas particuliers

- Pourquoi retrouve-t-on **toujours** l'image initiale en mélangeant les pixels suivant cette méthode ?
- Cette propriété est-elle liée à la transformation utilisée ?
- Comment prévoir en fonction de la taille de l'image **le nombre d'essais** qui la feront réapparaître à l'identique ?

## Explication « locale » pour une permutation quelconque

Considérons la permutation  $\sigma$  de 8 éléments suivante :

0	1	2	3	4	5	6	7	Position initiale
1	4	5	2	6	3	0	7	après 1 transformation

Il semble naturel de suivre les images successives d'un élément.

- 7  $\rightarrow$  7 (invariant)
- 1  $\rightarrow$  0  $\rightarrow$  6  $\rightarrow$  6  $\rightarrow$  4 (retour en 4 itérations)
- 2  $\rightarrow$  3  $\rightarrow$  5 (retour en 3 itérations)

Ainsi, on est assuré que  $\sigma^{12} = \text{id}$ .



## Explication « locale » pour une permutation quelconque

Considérons la permutation  $\sigma$  de 8 éléments suivante :

0	1	2	3	4	5	6	7	Position initiale
1	4	5	2	6	3	0	7	après 1 transformation

Il semble naturel de suivre les images successives d'un élément.

- $7 \rightarrow 7$  (invariant)
- $1 \rightarrow 0 \rightarrow 6 \rightarrow 6 \rightarrow 4$  (retour en 4 itérations)
- $2 \rightarrow 3 \rightarrow 5$  (retour en 3 itérations)

Ainsi, on est assuré que  $\sigma^{12} = \text{id}$ .

## Explication « locale » pour une permutation quelconque

Considérons la permutation  $\sigma$  de 8 éléments suivante :

0	1	2	3	4	5	6	7	Position initiale
1	4	5	2	6	3	0	7	après 1 transformation

Il semble naturel de suivre les images successives d'un élément.

- $7 \rightarrow 7$  (invariant)
- $1 \rightarrow 0 \rightarrow 6 \rightarrow 6 \rightarrow 4$  (retour en 4 itérations)
- $2 \rightarrow 3 \rightarrow 5$  (retour en 3 itérations)

Ainsi, on est assuré que  $\sigma^{12} = \text{id}$ .

## Explication « locale » pour une permutation quelconque

Considérons une ligne  $(1, 2, \dots, N)$  et un entier  $i_0$ ,  $1 \leq i_0 \leq N$ .

- tant que la valeur initiale n'a pas réapparu, les images successives de  $i_0$  sont deux à deux distinctes (**bijection**) ;
- les images successives de  $i_0$  par une permutation donnée prennent au maximum  $N$  valeurs distinctes ;
- la valeur initiale du nombre réapparaît donc au bout d'une nombre fini d'itérations.

## Explication « locale » pour une permutation quelconque

Considérons une ligne  $(1, 2, \dots, N)$  et un entier  $i_0$ ,  $1 \leq i_0 \leq N$ .

- tant que la valeur initiale n'a pas réapparu, les images successives de  $i_0$  sont deux à deux distinctes (**bijection**) ;
- les images successives de  $i_0$  par une permutation donnée prennent au maximum  $N$  valeurs distinctes ;
- la valeur initiale du nombre réapparaît donc au bout d'une nombre fini d'itérations.

## Explication « locale » pour une permutation quelconque

Considérons une ligne  $(1, 2, \dots, N)$  et un entier  $i_0$ ,  $1 \leq i_0 \leq N$ .

- tant que la valeur initiale n'a pas réapparu, les images successives de  $i_0$  sont deux à deux distinctes (**bijection**) ;
- les images successives de  $i_0$  par une permutation donnée prennent au maximum  $N$  valeurs distinctes ;
- **la valeur initiale du nombre réapparaît donc au bout d'une nombre fini d'itérations.**

## Explication locale pour une permutation quelconque

$$(\forall i \in [1, M]) \quad (\exists n_i \in \mathbb{N}) \quad \sigma^{n_i}(i) = i$$

$M = \text{PPCM}(n_1, \dots, n_N)$  est donc un nombre d'itérations qui renvoie l'image initiale :

$$(\forall i \in [1, M]) \quad \sigma^M(i) = i$$

## Explication locale pour une permutation quelconque

C'est une méthode très naturelle qui correspond à la décomposition de la permutation en produit de cycles disjoints.

*Exemple* :  $\sigma$

0	1	2	3	4	5	6
2	5	4	6	0	3	1

Ici :

$6 \rightarrow 3 \rightarrow 5 \rightarrow 1 : \sigma^4(1) = 1$  idem pour 6, 3 et 5

$0 \rightarrow 4 \rightarrow 2 \rightarrow 0 : \sigma^3(0) = 0$ , idem pour 4, 2

Ainsi,  $\sigma^{12} = id$ .

$$\sigma = (042)(1635)$$

## Explication générale

L'ensemble  $\mathcal{S}_N$  des permutations d'un ensemble à  $N$  éléments a une structure de groupe :  $(\mathcal{S}_N, \circ)$ . C'est un groupe fini de cardinal  $N!$ .

$$(\forall f \in \mathcal{S}_N)(\exists k \in \mathbb{N}) \quad f^k = \text{id}$$

Le plus petit entier  $k$  vérifiant  $f^k = \text{id}$  est appelé *ordre* de  $f$ .

Quel est l'ordre de la permutation qui intervient dans la transformation du photomaton ?



## Ordre de la transformation du photomaton

La transformation du photomaton appliquée à une ligne de longueur  $2p$  peut se décrire ainsi :

$$\begin{cases} i \text{ pair} & \sigma(i) = \frac{i}{2} \\ i \text{ impair} & \sigma(i) = p + E\left[\frac{i}{2}\right] \end{cases}$$

## La taille de l'image est une puissance de 2

Appliquons la transformation du photomaton à une ligne de longueur  $2^N$ . Chaque nombre de 0 à  $2^N - 1$  se représente en base 2 par un nombre à  $N$  chiffres (0 ou 1).

$$i \text{ pair} \quad : \quad i = \underbrace{101\dots1}_i 0 \quad \sigma(i) = \frac{i}{2} = 0 \underbrace{101\dots1}_{\frac{i}{2}}$$

$$i \text{ impair} \quad : \quad i = \underbrace{101\dots1}_{E[\frac{i}{2}]} 1 \quad \sigma(i) = 2^{N-1} + E[\frac{i}{2}] = 1 \underbrace{101\dots1}_{E[\frac{i}{2}]}$$

La transformation se traduit par un décalage (circulaire) des chiffres d'un cran vers la droite.

## La taille de l'image est une puissance de 2

### Conclusion

Si une image est un carré de taille  $2^N \times 2^N$ , l'ordre de la permutation associée à la transformation du photomaton est  $N$ .

## Image de taille quelconque

- On commence par étudier la permutation sur une ligne de longueur  $2N$  ( $N$  n'étant pas une puissance de 2);
- on essaie de ramener le problème à une ligne de longueur  $2^P$ , ce qui ne peut pas se faire en mettant bout à bout les lignes de longueurs  $2N$ ;
- dans la transformation, la dernière case (ou la première) est invariante, on la met donc de côté et on étudie une ligne de longueur  $2N - 1$ .

## Image de taille quelconque

- On commence par étudier la permutation sur une ligne de longueur  $2N$  ( $N$  n'étant pas une puissance de 2) ;
- on essaie de ramener le problème à une ligne de longueur  $2^P$ , ce qui ne peut pas se faire en mettant bout à bout les lignes de longueurs  $2N$  ;
- dans la transformation, la dernière case (ou la première) est invariante, on la met donc de côté et on étudie une ligne de longueur  $2N - 1$ .

## Image de taille quelconque

- On commence par étudier la permutation sur une ligne de longueur  $2N$  ( $N$  n'étant pas une puissance de 2);
- on essaie de ramener le problème à une ligne de longueur  $2^p$ , ce qui ne peut pas se faire en mettant bout à bout les lignes de longueurs  $2N$ ;
- dans la transformation, la dernière case (ou la première) est invariante, on la met donc de côté et on étudie une ligne de longueur  $2N - 1$ .

## Image de taille quelconque

Soit  $q$  le plus petit entier tel que  $2^q - 1$  soit multiple de  $2N - 1$ .

C'est possible car :  $\text{PGCD}(2, 2N - 1) = 1$ .

2 est donc inversible dans  $\mathbb{Z}/(2N - 1)\mathbb{Z}$  :

$$2 \in (\mathbb{Z}/(2N - 1)\mathbb{Z})^*$$

$[(\mathbb{Z}/(2N - 1)\mathbb{Z})^*, \times]$  est un groupe multiplicatif.

$q = \text{ordre de } 2 \text{ dans } (\mathbb{Z}/(2N - 1)\mathbb{Z})^* \text{ vérifie } 2^q \equiv 1 \pmod{2N - 1}$ .

## Image de taille quelconque

- Il donc un entier naturel  $k$  tel que  $2^q - 1 = k(2N - 1)$ ;
- si l'on met bout à bout  $k$  lignes de longueur  $2N - 1$ , on constitue ainsi une ligne de longueur  $2^q - 1$ ;
- on replace tout à la fin la dernière case mise en réserve pour obtenir une grande ligne de longueur  $2^q$ .
- au bout de  $q$  transformations, la nouvelle ligne retrouve sa forme initiale.



## Image de taille quelconque

- Il donc un entier naturel  $k$  tel que  $2^q - 1 = k(2N - 1)$  ;
- si l'on met bout à bout  $k$  lignes de longueur  $2N - 1$ , on constitue ainsi une ligne de longueur  $2^q - 1$  ;
- on replace tout à la fin la dernière case mise en réserve pour obtenir une grande ligne de longueur  $2^q$ .
- au bout de  $q$  transformations, la nouvelle ligne retrouve sa forme initiale.

## Image de taille quelconque

- Il donc un entier naturel  $k$  tel que  $2^q - 1 = k(2N - 1)$  ;
- si l'on met bout à bout  $k$  lignes de longueur  $2N - 1$ , on constitue ainsi une ligne de longueur  $2^q - 1$  ;
- on replace tout à la fin la dernière case mise en réserve pour obtenir une grande ligne de longueur  $2^q$ .
- au bout de  $q$  transformations, la nouvelle ligne retrouve sa forme initiale.

## Image de taille quelconque

- Il donc un entier naturel  $k$  tel que  $2^q - 1 = k(2N - 1)$  ;
- si l'on met bout à bout  $k$  lignes de longueur  $2N - 1$ , on constitue ainsi une ligne de longueur  $2^q - 1$  ;
- on replace tout à la fin la dernière case mise en réserve pour obtenir une grande ligne de longueur  $2^q$ .
- au bout de  $q$  transformations, la nouvelle ligne retrouve sa forme initiale.

## Image de taille quelconque

La transformation sur la « grande » ligne a-t-elle les mêmes effets que la transformation limitée à la ligne initiale ?

## Image de taille quelconque

- Les nombres de la ligne de longueur  $2^q$  sont numérotés de 0 à  $2^q - 1$  ;
- appliquer la méthode du photomaton, c'est regrouper d'abord tous les pairs, puis placer tous les impairs ;
- $k \geq 2$ , donc on a mis bout à bout au moins deux séquences de la ligne initiale tronquée ;
- les pairs s'écrivent  $0, 2, \dots, 2N - 2, 2N, 2N + 2, \dots, 4N - 2 \dots$  ;
- modulo  $2N - 1$ , cela devient :  
 $0, 2, \dots, 2N - 2, 1, 3, \dots, 2N - 1 \dots$

## Image de taille quelconque

- Les nombres de la ligne de longueur  $2^q$  sont numérotés de 0 à  $2^q - 1$  ;
- appliquer la méthode du photomaton, c'est regrouper d'abord tous les pairs, puis placer tous les impairs ;
- $k \geq 2$ , donc on a mis bout à bout au moins deux séquences de la ligne initiale tronquée ;
- les pairs s'écrivent  $0, 2, \dots, 2N - 2, 2N, 2N + 2, \dots, 4N - 2 \dots$  ;
- modulo  $2N - 1$ , cela devient :  
 $0, 2, \dots, 2N - 2, 1, 3, \dots, 2N - 1 \dots$

## Image de taille quelconque

- Les nombres de la ligne de longueur  $2^q$  sont numérotés de 0 à  $2^q - 1$  ;
- appliquer la méthode du photomaton, c'est regrouper d'abord tous les pairs, puis placer tous les impairs ;
- $k \geq 2$ , donc on a mis bout à bout au moins deux séquences de la ligne initiale tronquée ;
- les pairs s'écrivent  $0, 2, \dots, 2N - 2, 2N, 2N + 2, \dots, 4N - 2 \dots$  ;
- modulo  $2N - 1$ , cela devient :  
 $0, 2, \dots, 2N - 2, 1, 3, \dots, 2N - 1 \dots$

## Image de taille quelconque

- Les nombres de la ligne de longueur  $2^q$  sont numérotés de 0 à  $2^q - 1$  ;
- appliquer la méthode du photomaton, c'est regrouper d'abord tous les pairs, puis placer tous les impairs ;
- $k \geq 2$ , donc on a mis bout à bout au moins deux séquences de la ligne initiale tronquée ;
- les pairs s'écrivent  $0, 2, \dots, 2N - 2, 2N, 2N + 2, \dots, 4N - 2 \dots$  ;
- modulo  $2N - 1$ , cela devient :  
 $0, 2, \dots, 2N - 2, 1, 3, \dots, 2N - 1 \dots$



## Image de taille quelconque

- Les nombres de la ligne de longueur  $2^q$  sont numérotés de 0 à  $2^q - 1$  ;
- appliquer la méthode du photomaton, c'est regrouper d'abord tous les pairs, puis placer tous les impairs ;
- $k \geq 2$ , donc on a mis bout à bout au moins deux séquences de la ligne initiale tronquée ;
- les pairs s'écrivent  $0, 2, \dots, 2N - 2, 2N, 2N + 2, \dots, 4N - 2 \dots$  ;
- modulo  $2N - 1$ , cela devient :  
$$0, 2, \dots, 2N - 2, 1, 3, \dots, 2N - 1 \dots$$

## Image de taille quelconque

- La restriction de la transformation sur la ligne de longueur  $2^q - 1$  aux deux premières séquences est la transformation du photomaton appliqués aux  $2N - 1$  premiers éléments de la ligne de longueur  $2N$  ;
- la ligne de longueur  $2N$  revient donc à l'identique au bout de  $q$  itérations.

## Image de taille quelconque

- La restriction de la transformation sur la ligne de longueur  $2^q - 1$  aux deux premières séquences est la transformation du photomaton appliqués aux  $2N - 1$  premiers éléments de la ligne de longueur  $2N$  ;
- la ligne de longueur  $2N$  revient donc à l'identique au bout de  $q$  itérations.

## Image de taille quelconque

### Conclusion

Si l'image est un carré de taille  $2N \times 2N$ , et si  $\sigma$  est la permutation associée à la transformation du photomaton, **le plus petit entier  $q$  tel que  $2^q - 1$  est un multiple de  $2N - 1$  vérifie  $\sigma^q = \text{id}$ .**

## Image de taille quelconque

Si l'image est un rectangle de taille  $2P \times 2Q$ , l'ordre de la permutation associée à la transformation du photomaton est

$$\text{PPCM}(p, q)$$

- $p$  étant l'ordre de la permutation opérant sur les lignes ;
- $q$  étant l'ordre de la permutation opérant sur les colonnes.