Topologie algébrique et systèmes répartis asynchrones

Frédéric Tronel

ftronel@irisa.fr

IRISA - INRIA Rennes

Les problèmes

Étant donné un système distribué asynchrone sujet aux défaillances. Étant donné une tâche $\mathcal{P}$ à exécuter dans ce système.

- Peut-on résoudre $\mathcal{P}$ (quelque soit le nombre de défaillances) ?
- Pour un nombre de défaillances fixé ?
- Peut-on décider ces questions (dans le cas général) ?
- Sinon dans quelles sous-classes de tâches ?

Les outils

Topologie générale.

Théorie des groupes.

Topologie algébrique.

Du courage ...

Et encore du courage !

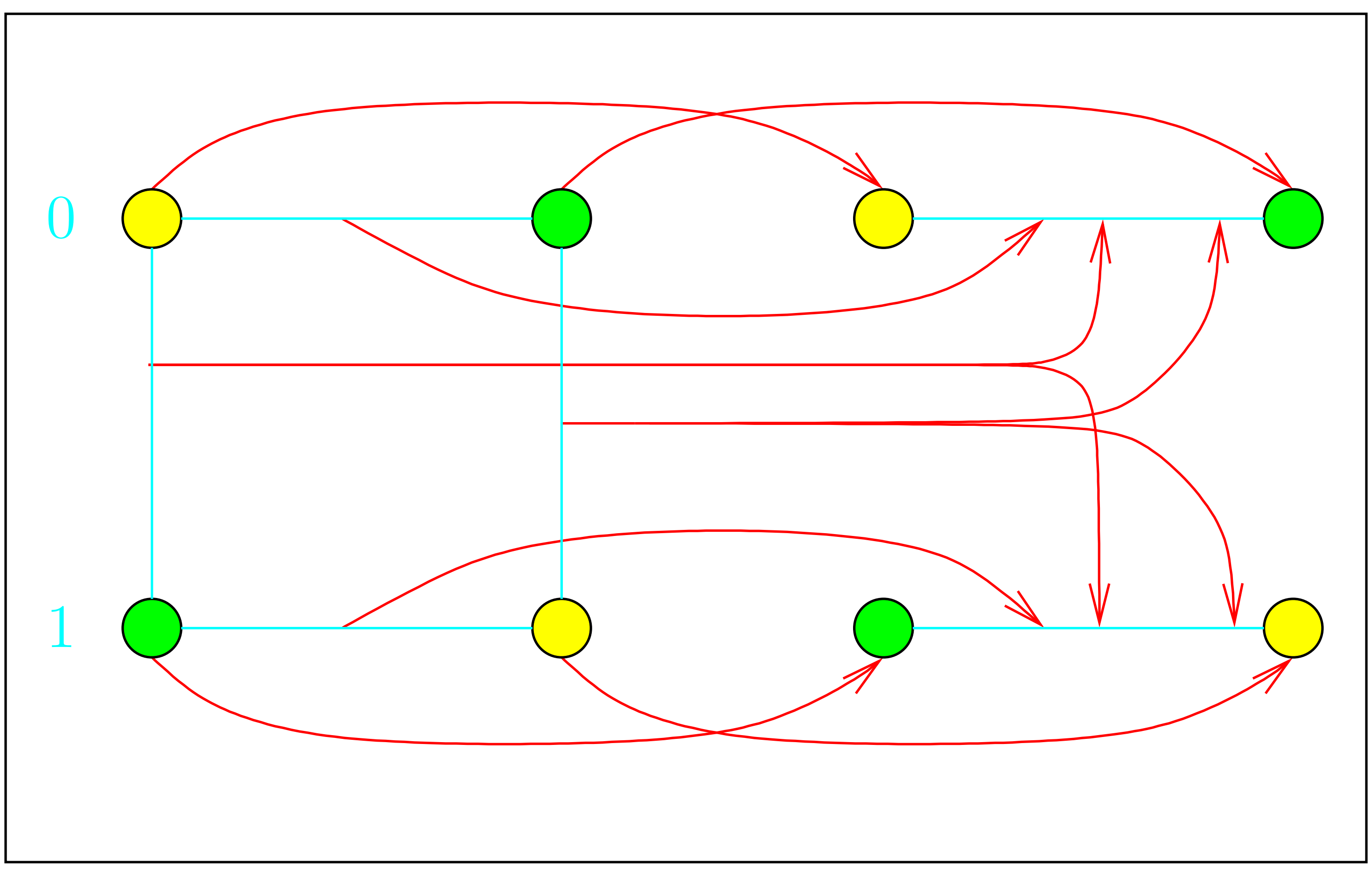
Un aperçu

Les problèmes posés dans le cadre des systèmes asynchrones répartis s'expriment souvent sous la forme de structure de données discrètes décrivant :

- Configurations possibles pour les entrées.
- Configurations possibles pour les sorties.
- Une fonction (*mapping*) des entrées vers les sorties.

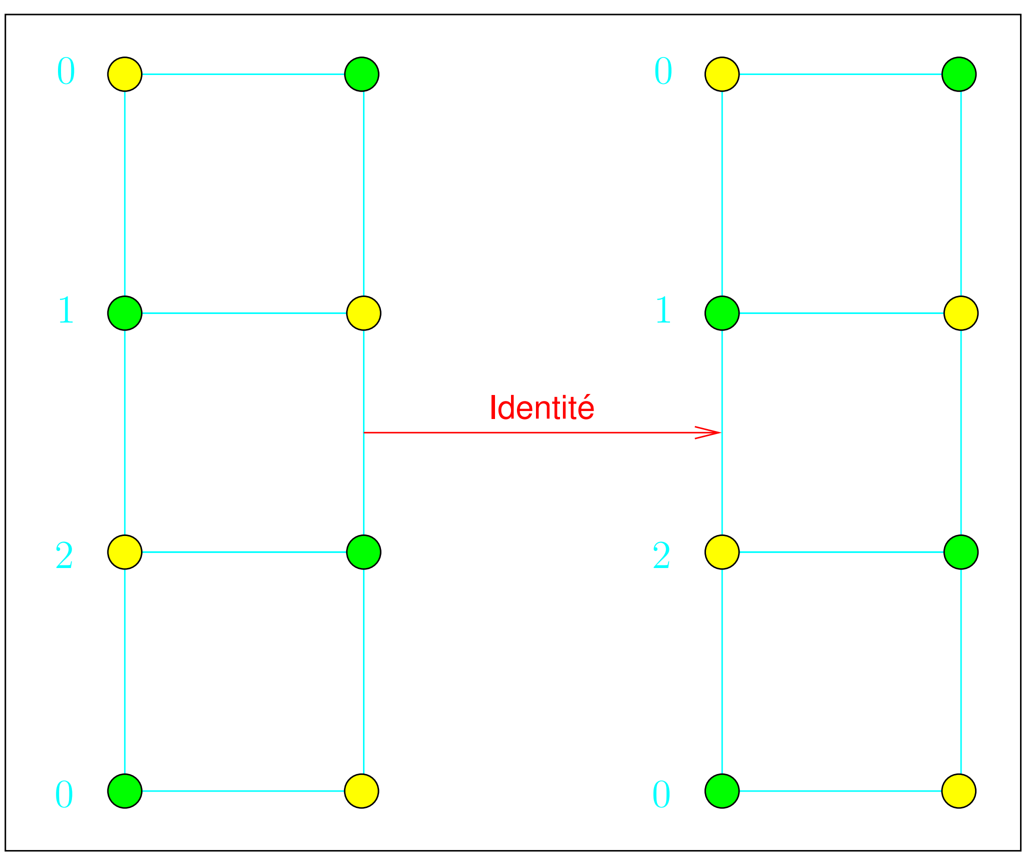
Un premier exemple

Le problème du consensus avec deux processus



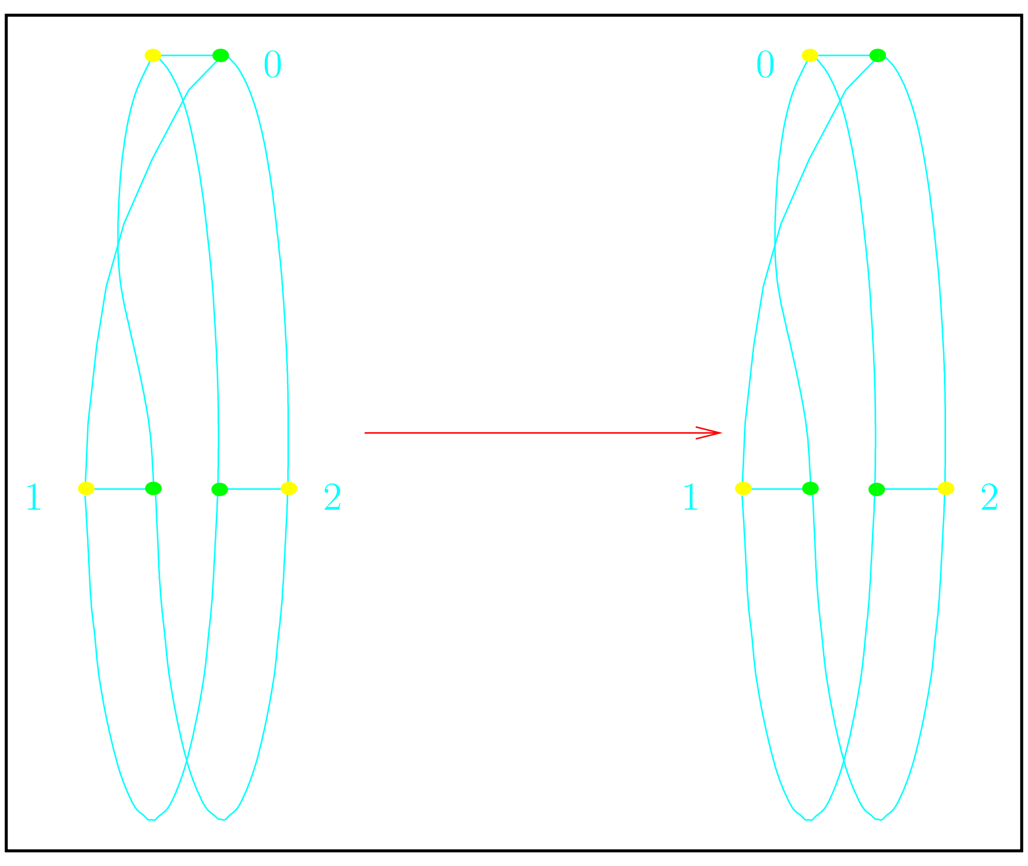
Un second exemple

Le problème du 2-*set agreement* avec deux processus



Un second exemple

Le problème du 2-*set agreement* avec deux processus



Le modèle de calcul

- $n+1$ processus;
- Chaque processus exécute le même protocole déterministe;
- Les processus ont accès à une mémoire globale partagée;
- La mémoire est de taille $n+1$ (une entrée par processus);
- La mémoire supporte deux opérations :
  - SCAN : Le processus obtient une copie de la mémoire entière
  - UPDATE(V) : Le processus étend son entrée par la valeur V
- Le système est *asynchrone*, car l'ordonnancement des actions des processus est complètement arbitraire;
- Les processus peuvent subir des défaillances.

Complexes simpliciaux abstraits

Un complexe simplicial $\mathcal{K}$ est une famille d'ensembles finis close par inclusion.

Exemples :

$\mathcal{K}_1 = \{\{a, b, c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a\}, \{b\}, \{c\}\}$

$\mathcal{K}_1 = \{\{a, b, c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a\}, \{b\}, \{c\}\}$

$\mathcal{K}_2 = \{\{a, b\}, \{b, c\}, \{a, c\}, \{a\}, \{b\}, \{c\}\}$

$\mathcal{K}_2 = \{\{a, b\}, \{b, c\}, \{a, c\}, \{a\}, \{b\}, \{c\}\}$

Un sous-ensemble $\mathcal{L} \subseteq \mathcal{K}$ est un sous-complexe de $\mathcal{K}$ (par exemple $\mathcal{K}_2$ par rapport à $\mathcal{K}_1$).

Un complexe simplicial $\mathcal{K}$ est généré par un ensemble K si :

$$\mathcal{K} = \{X' \neq \emptyset, X' \subseteq X \in K\}$$

Simplexes abstraits

Soit $X \in \mathcal{K}$, X est un simplexe abstraits de $\mathcal{K}$.
Les éléments de X sont ses sommets.
Par exemple, $X = \{a, b, c\}$ est un simplexe dont les sommets sont a, b et c.

Si $|X| = k + 1$, X est un k-simplexe, et sa dimension est k.
La dimension d'un complexe $\mathcal{K}$ est :

$$\sup_{X \in \mathcal{K}} \dim X$$

L'ensemble des sommets de $\mathcal{K}$ est $\mathcal{K}^{(0)} = \bigcup_{X \in \mathcal{K}} X$

Soit X un simplexe. $X' \subseteq X$ est une face de X. Soit X un simplexe. $X' \subset X$ est une face propre de X. L'ensemble des faces propres de X est un complexe noté ∂X.

Fonctions simpliciales

Soit $\mathcal{K}$ et $\mathcal{L}$ deux complexes. Soit $V = \mathcal{K}^{(0)}$ et $W = \mathcal{L}^{(0)}$.
Soit $f : V \to W$.
Extension de f à $\mathcal{P}(V) \to \mathcal{P}(W)$:

$$\forall\, X \subseteq V, \quad f(X) = \bigcup_{x \in X} f(x) \subseteq W$$

f est une fonction simpliciale, si :

$$\forall\, X \in \mathcal{K} \quad f(X) \in \mathcal{L}$$

Elle transporte les simplexes de $\mathcal{K}$ vers les simplexes de $\mathcal{L}$.

Fonctions simpliciales

L'identité est une fonction simpliciale.
La composée de fonctions simpliciales est simpliciale.
L'inverse d'une fonction simpliciale bijective, est simpliciale et bijective.
On a :

$$\forall X \in \mathcal{K} \quad \dim f(X) \leq \dim X.$$

f est non dégénérative si :

$$\forall X \in \mathcal{K} \quad \dim f(X) = \dim X.$$

Squelette

Soit $\mathcal{K}$ un complexe de dimension d.
On appelle squelette de $\mathcal{K}$ de dimension $0 \leq k \leq d$, noté $\mathcal{K}^{(k)}$, le sous-complexe de $\mathcal{K}$ défini par :

$$\mathcal{K}^{(k)} = \{X \in \mathcal{K}, \dim X \leq k\}$$

Engendré par les simplexes de $\mathcal{K}$ de dimension exactement k

Complexes simpliciaux concrets

Représentation géométriques des complexes abstraits.

On doit trouver un sous-ensemble de $\mathbb{R}^d$ (pour un d suffisamment large) qui capture correctement les propriétés inhérentes aux complexes.

Enveloppe convexe

Soit $x_0, \dots x_k$, $k+1$ points de $\mathbb{R}^d$.
Une combinaison convexe des x_i est :

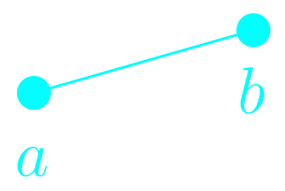
$$t_0 x_0 + \cdots + t_k x_k \text{ où } \sum_{0 \leq i \leq k} t_i = 1$$

L'enveloppe convexe des x_i est l'ensemble des combinaisons convexes des x_i. On la note $[x_0, \dots, x_k]$.

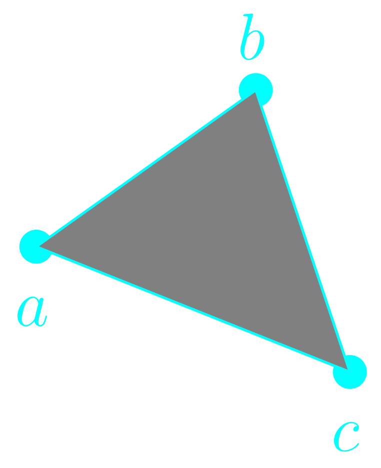
Polyèdres

Exemples d'enveloppes convexes

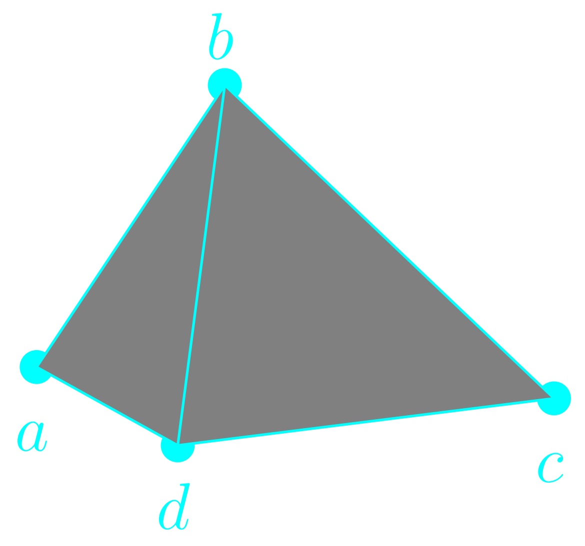
$[a]$



$[a, b]$



$[a, b, c]$

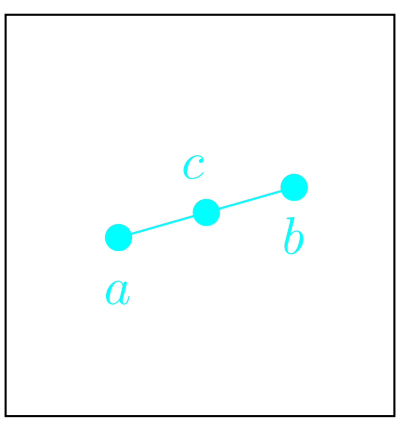


$[a, b, c, d]$

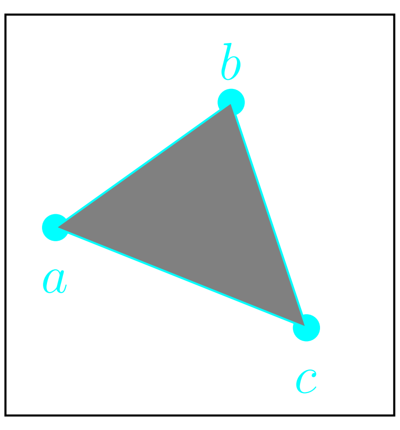
Polyèdres

Soit $x_0, \ldots x_k$, $k+1$ points de $\mathbb{R}^d$. Ces points sont affinement indépendants si chaque point de $[x_0, \ldots, x_k]$ s'écrit de manière unique comme une combinaison convexe des x_i. L'unicité de l'écriture sert de coordonnées; on écrira $x = (t_0, \ldots, t_k)$, si $x = \sum t_i x_i$.

a, b, c ne sont pas affinement indépendants



a, b, c sont affinement indépendants



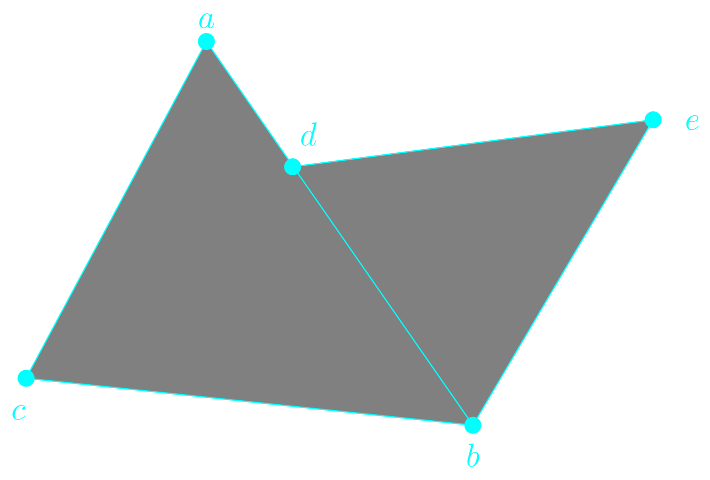
car $c = 0.a + 0.b + 1.c = \frac{1}{2}.a + \frac{1}{2}.b + 0.c$

Complexes simpliciaux concrets

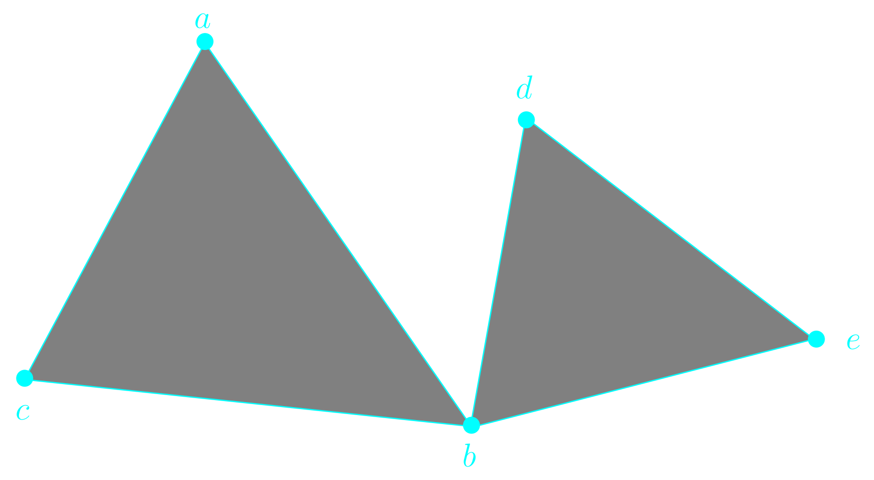
On décide de représenter un complexe $\mathcal{K}$ par l'union des représentations polyédrales de chacun des simplexes qui le génère. On veut de plus que :

$$\forall\, X, Y \in \mathcal{K} \quad |X| \bigcap |Y| = |X \bigcap Y|$$

Représentation incorrecte



Représentation correcte



car $|\{a, b, c\}| \bigcap |\{b, d, e\}| = |\{b, d\}| \neq |\{b\}|$

Subdivisions

Une subdivision d'un complexe $\mathcal{K}$, est un complexe $\sigma(\mathcal{K})$ qui vérifie :

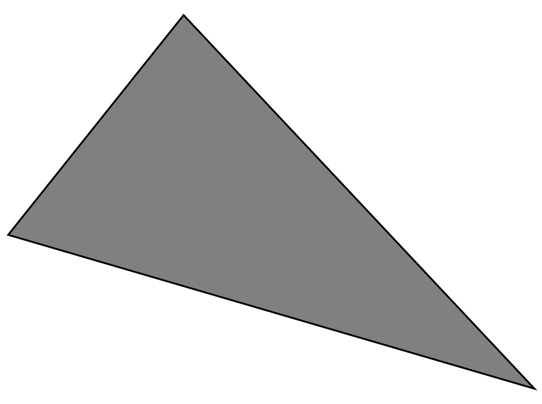
(1) $|\mathcal{K}| = |\sigma(\mathcal{K})|$
(2) $\forall\, S \in \sigma(\mathcal{K}), \quad \exists\, X \in \mathcal{K}, \quad |S| \subseteq |X|$
(3) Le plus petit X vérifiant (2) est le simplexe porteur de S dans $\mathcal{K}$, noté carrier$(S, \mathcal{K})$

(4) $\forall X \in \mathcal{K}, \quad \exists\, S_1, \ldots, S_r \in \sigma(\mathcal{K}), \quad |X| = \bigcup |S_i|$

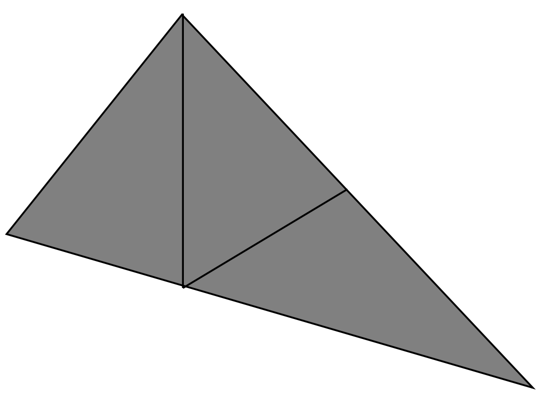
Subdivisions

Exemples

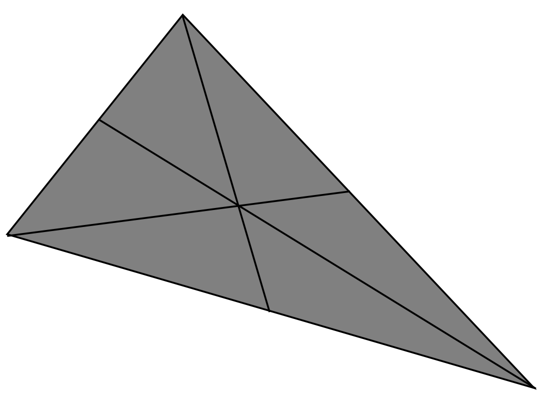
Le simplexe S_2



Une subdivision quelconque

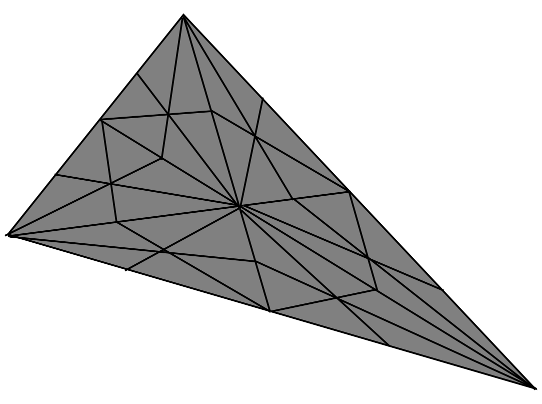


La subdivision barycentrique



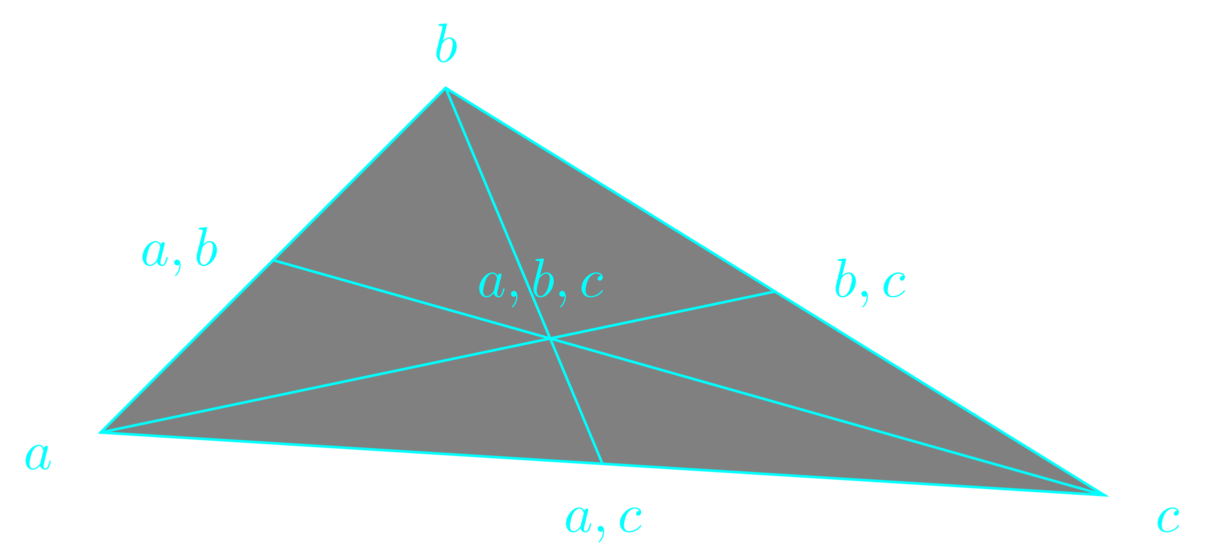
à l'ordre 1

La subdivision barycentrique



à l'ordre 2

Subdivision barycentrique



Complexes chromatiques

Une coloration d'un complexe $\mathcal{K}$ de dimension n, est une fonction simpliciale non dégénérative $\chi : \mathcal{K} \to \mathcal{S}_n$.

Cela correspond à associer à chaque sommet une couleur représentant l'identité d'un des $n+1$ processus du système.

Un complexe chromatique $(\mathcal{K}, \chi_\mathcal{K})$, est un complexe $\mathcal{K}$ et une coloration $\chi_\mathcal{K}$ associée

Fct simpliciale chromatique

Une fonction simpliciale $\mu : (\mathcal{K}, \chi_\mathcal{K}) \to (\mathcal{L}, \chi_\mathcal{L})$ est chromatique si :

$$\forall\, x \in \mathcal{K}^{(0)} \quad \chi_\mathcal{K}(x) = \chi_\mathcal{L}(\mu(x))$$

Elle préserve la coloration. Elle est donc non dégénérative.

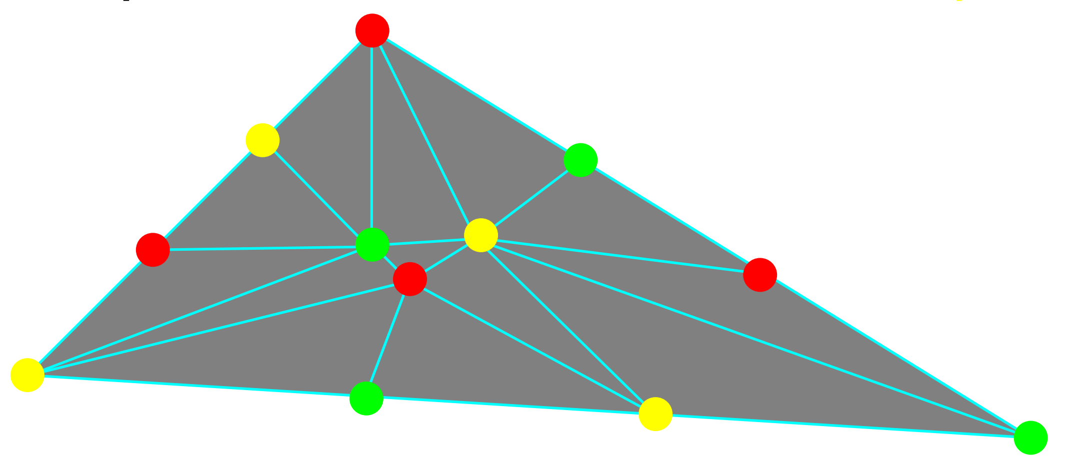
Subdivisions chromatiques

Une subdivision $(\sigma(\mathcal{K}), \chi_{\sigma(\mathcal{K})})$ d'un complexe chromatique $(\mathcal{K}, \chi_{\mathcal{K}})$ est chromatique si :

(1) $\sigma(\mathcal{K})$ est une subdivision de $\mathcal{K}$;
(2) $(\sigma(\mathcal{K}), \chi_{\sigma(\mathcal{K})})$ est un complexe chromatique;
(3) $\forall\, S \in \sigma(\mathcal{K}) \quad \chi_{\sigma(\mathcal{K})}(S) \subseteq \chi_{\sigma(\mathcal{K})}(\text{carrier}(S, \mathcal{K}))$

La subdivision barycentrique n'est pas chromatique.

On la remplace par la subdivision chromatique normale.



Tâches distribuées

Un $(n+1)$-vecteur d'entrée I est un vecteur de taille $n+1$ où chaque composante est :

- Une valeur d'un ensemble de départ D_I
- La valeur distinguée $\perp$

Au moins une des composantes de I est différente de $\perp$.

Un $(n+1)$-vecteur de sortie O est un vecteur de taille $n+1$ où chaque composante est :

- Une valeur d'un ensemble de sortie D_O
- La valeur distinguée $\perp$

Au moins une des composantes de O est différente de $\perp$.

Tâches distribuées

Un vecteur U est le préfixe d'un vecteur V, noté $U \leq V$ si :

$U[i] = V[i]$

$U[i] = \perp$

$$U = \begin{pmatrix} \perp \\ 1 \\ 2 \\ \perp \end{pmatrix} \leq V = \begin{pmatrix} 3 \\ 1 \\ 2 \\ \perp \end{pmatrix}$$

Un ensemble $\mathcal{W}$ est clos par préfixe si :

$$\forall V \in \mathcal{W}, \quad U \leq V \Longrightarrow U \in \mathcal{W}$$

Tâches distribuées

Soit I et O deux ensembles de vecteurs d'entrées et de sorties clos par préfixe, $\Delta \subseteq I \times O$ est la spécification d'une tâche distribuée.

Exemple du consensus binaire avec deux processus

$\langle 0,0\rangle$	$\{\langle 0,0\rangle\}$
$\langle 1,1\rangle$	$\{\langle 1,1\rangle\}$
$\langle 0,1\rangle$	$\{\langle 0,0\rangle,\langle 1,1\rangle\}$
$\langle 1,0\rangle$	$\{\langle 0,0\rangle,\langle 1,1\rangle\}$
$\langle 0,\perp\rangle$	$\{\langle 0,\perp\rangle\}$
$\langle 1,\perp\rangle$	$\{\langle 1,\perp\rangle\}$
$\langle \perp,0\rangle$	$\{\langle \perp,0\rangle\}$
$\langle \perp,1\rangle$	$\{\langle \perp,1\rangle\}$

Protocoles

On ne considérera que des protocoles complètement informés, c'est-à-dire qui connaissent la totalité de leur passé causal.

Forme normale d'un protocole complètement informé

```
UPDATE(input_value)
for(round=1; round< r ; round++){
    local_state = SCAN();
    UPDATE(local_state);
}
return(δ(local_state));
```

Le théorème ACT

Un problème $\langle \mathcal{I}, \mathcal{O}, \Delta \rangle$ a une solution totalement résiliente ssi :

- Il existe une subdivision chromatique σ de $\mathcal{I}$
- Il existe une fonction simpliciale chromatique $\mu : \sigma(\mathcal{I}) \to \mathcal{O}$ telle que :

$$\forall\, S \in \sigma(\mathcal{I}) \quad \mu(S) \in \Delta(\text{carrier}(S, \mathcal{I}))$$

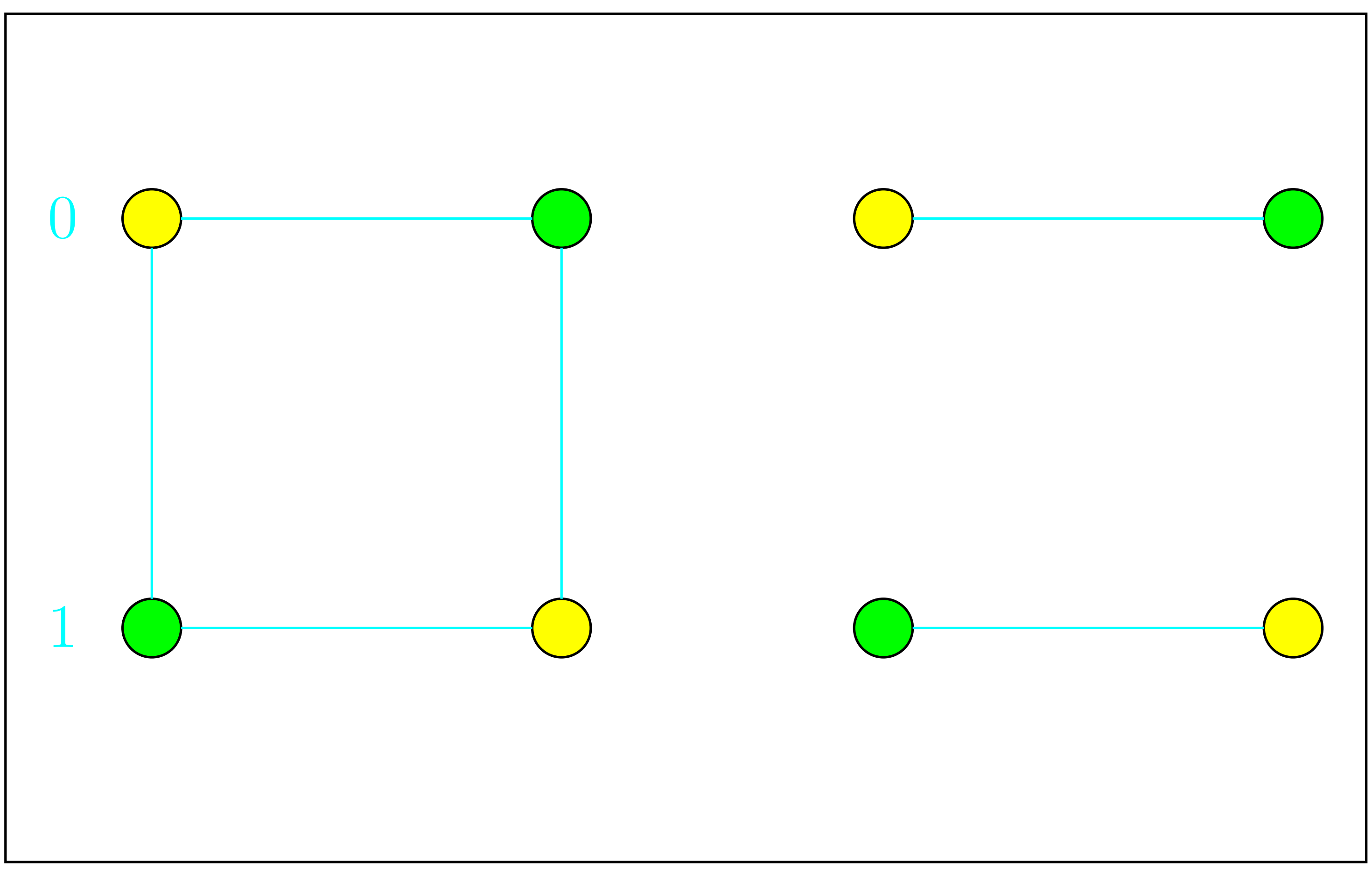
Application

Résoudre le consensus avec à $n+1$ processus et n fautes $\Rightarrow$ on peut le résoudre avec 2 processus et 1 faute.
Preuve : On arrête initialement $n-1$ processus, et on utilise l'algorithme pour un système à $n+1$ processus.

Prouver l'impossibilité du consensus dans un système à 2 processus, prouve l'impossibilité pour $n > 2$.

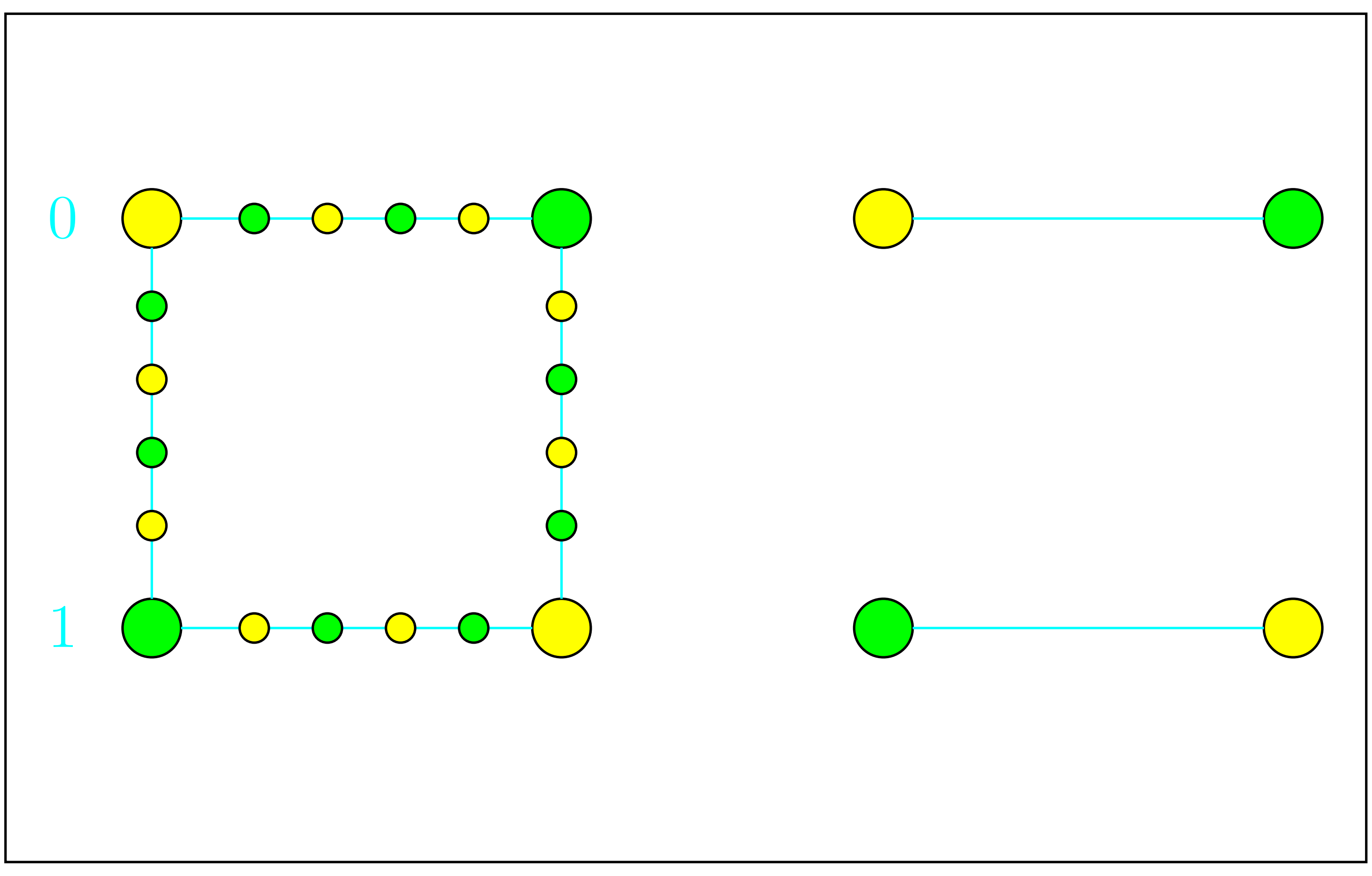
Application

Le problème du consensus binaire avec deux processus.



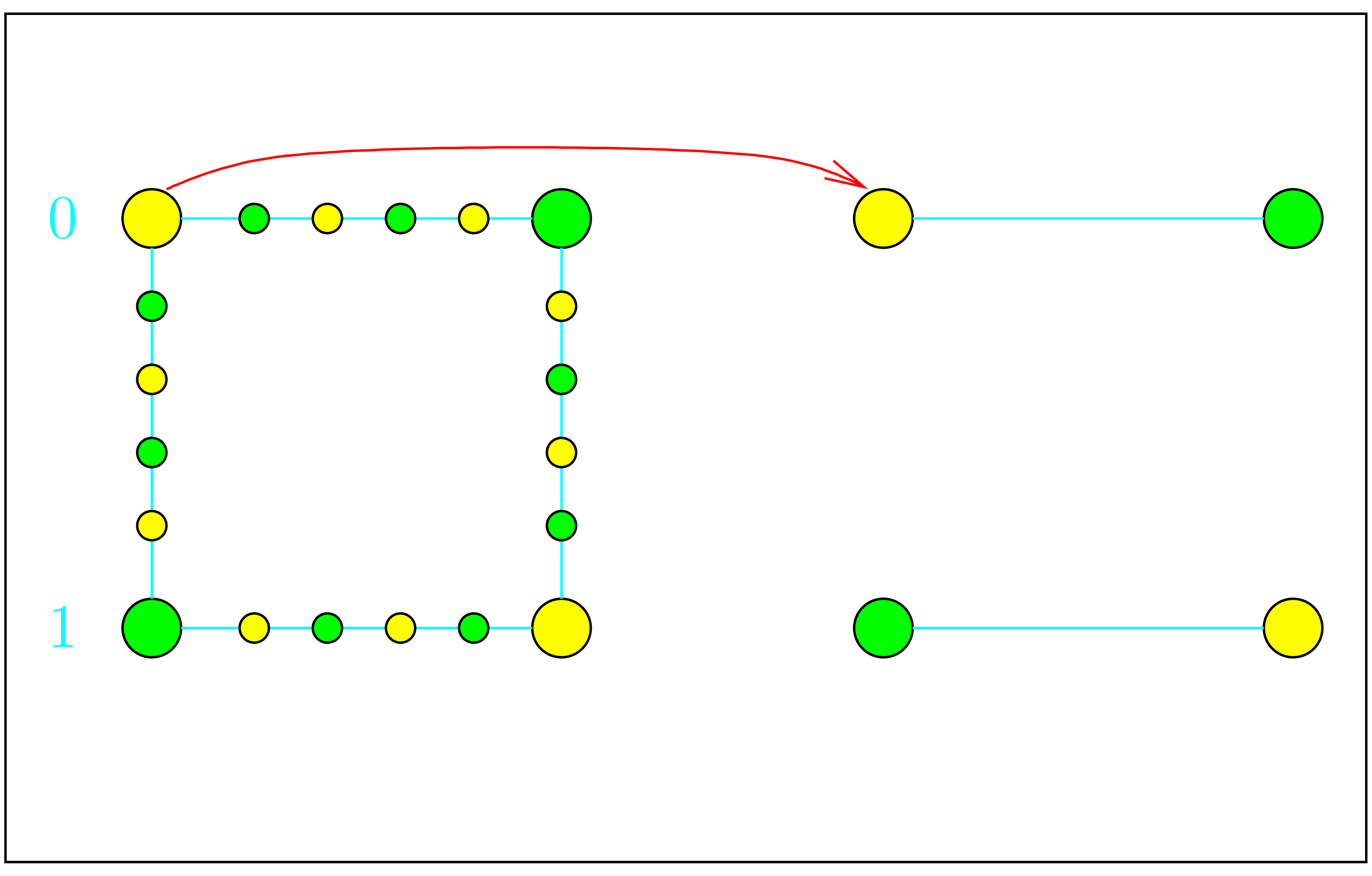
Application

Il existe une subdivision chromatique.



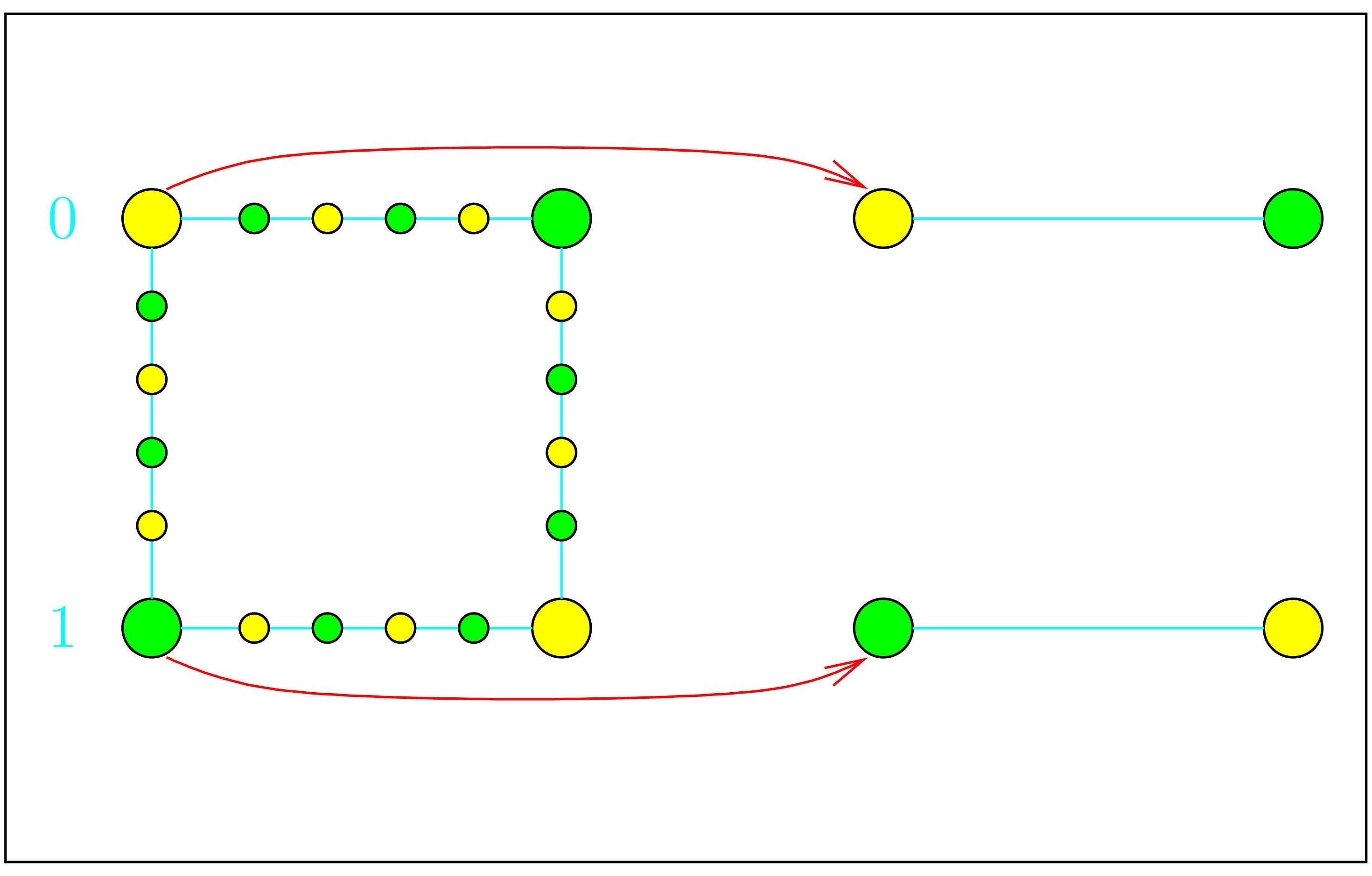
Application

Le processus jaune est seul, a choisi 0 et donc décide 0.



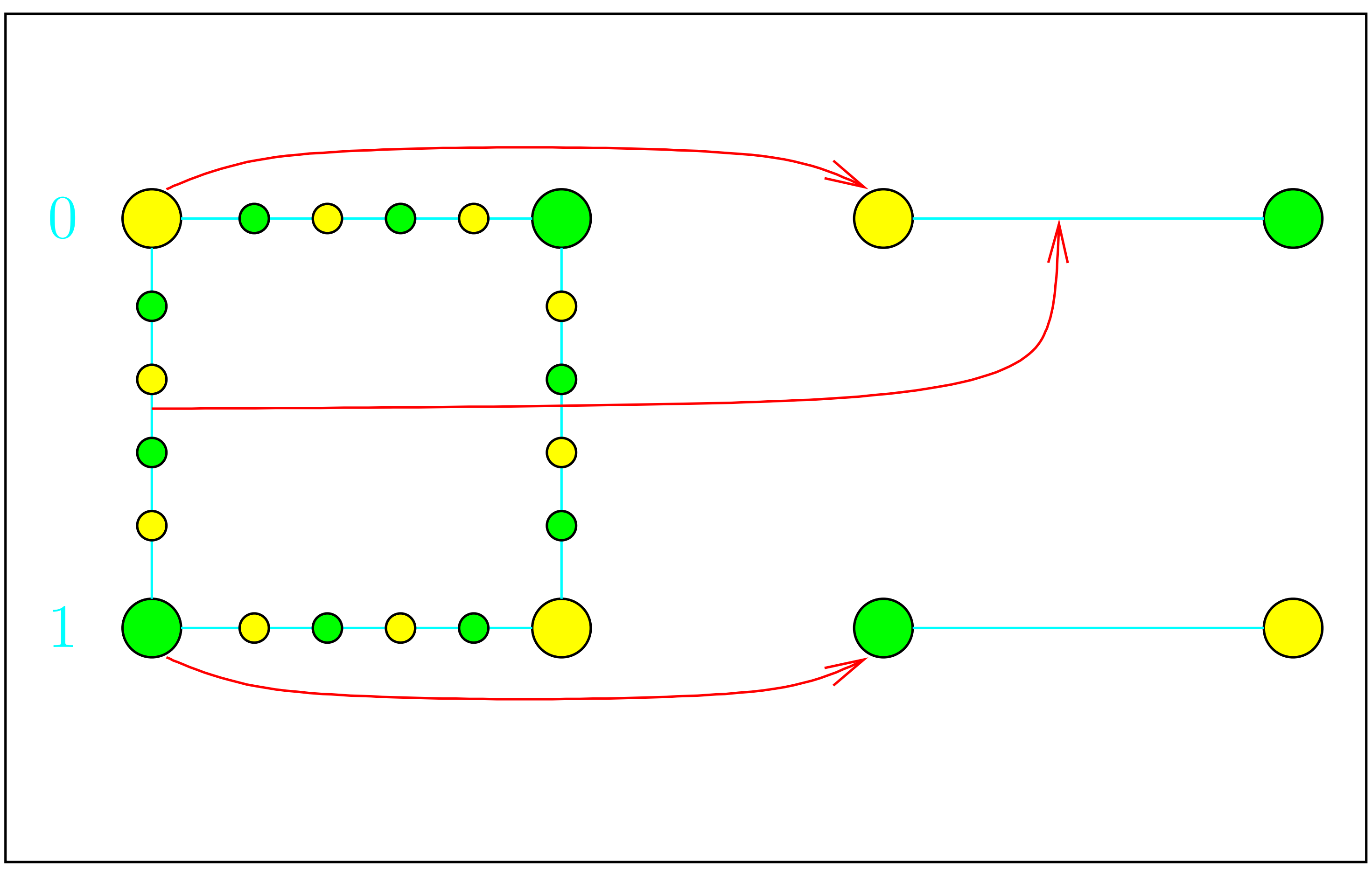
Application

Le processus vert est seul, a choisi 1 et donc décide 1.



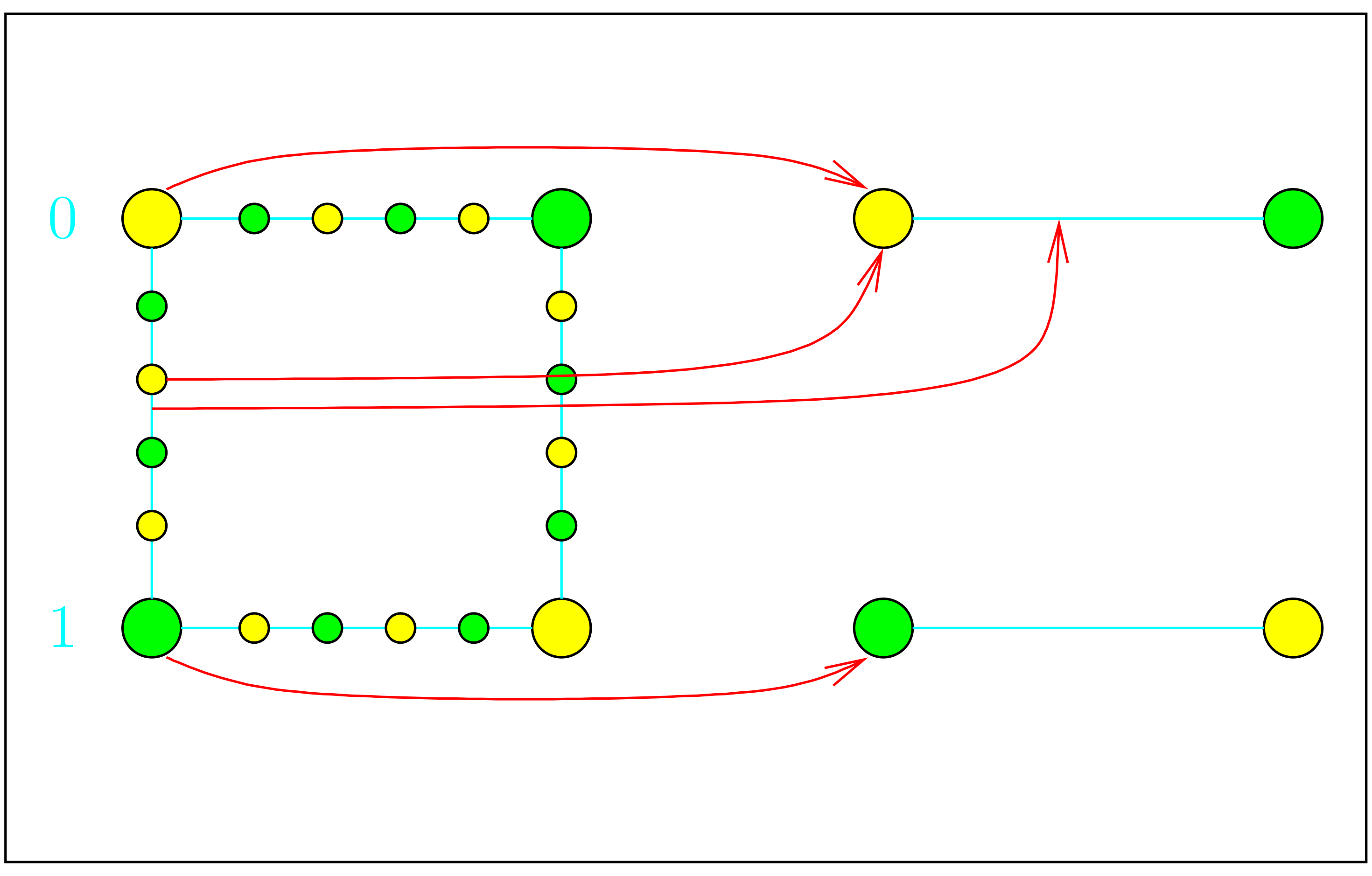
Application

Les deux processus participent, ont choisi des valeurs différentes et décide 0.



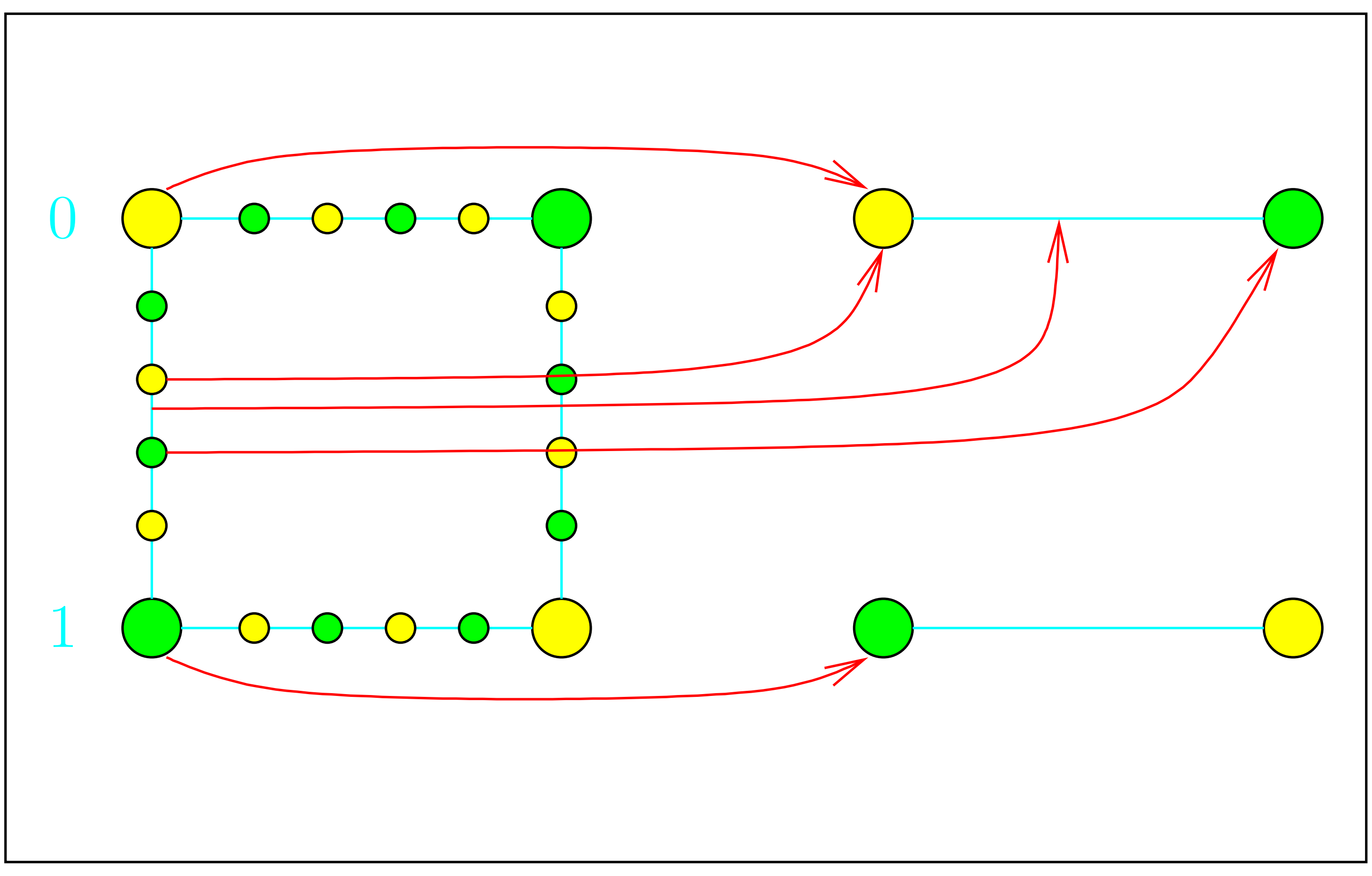
Application

μ est simpliciale et chromatique.



Application

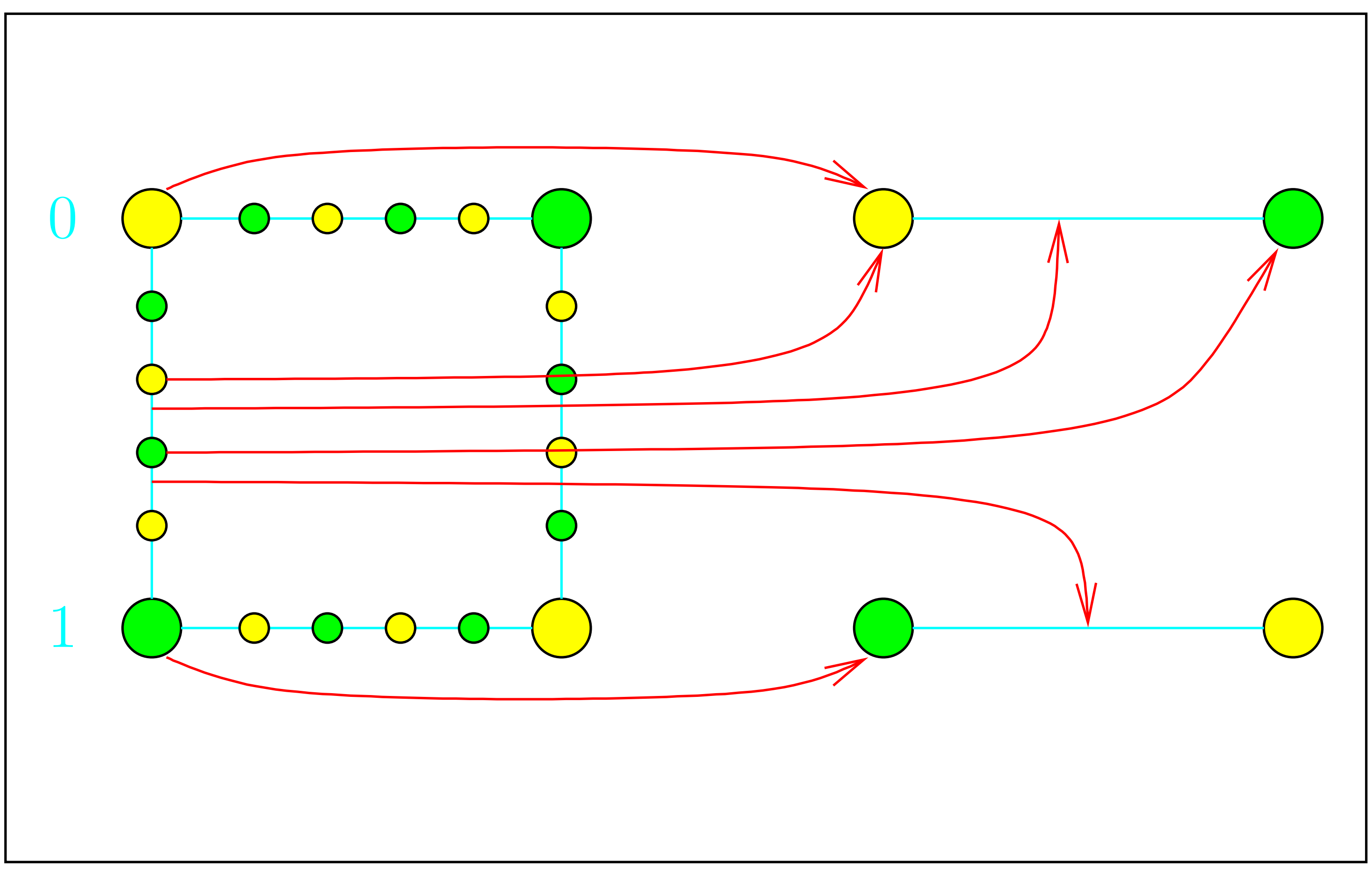
μ est simpliciale et chromatique.



Application

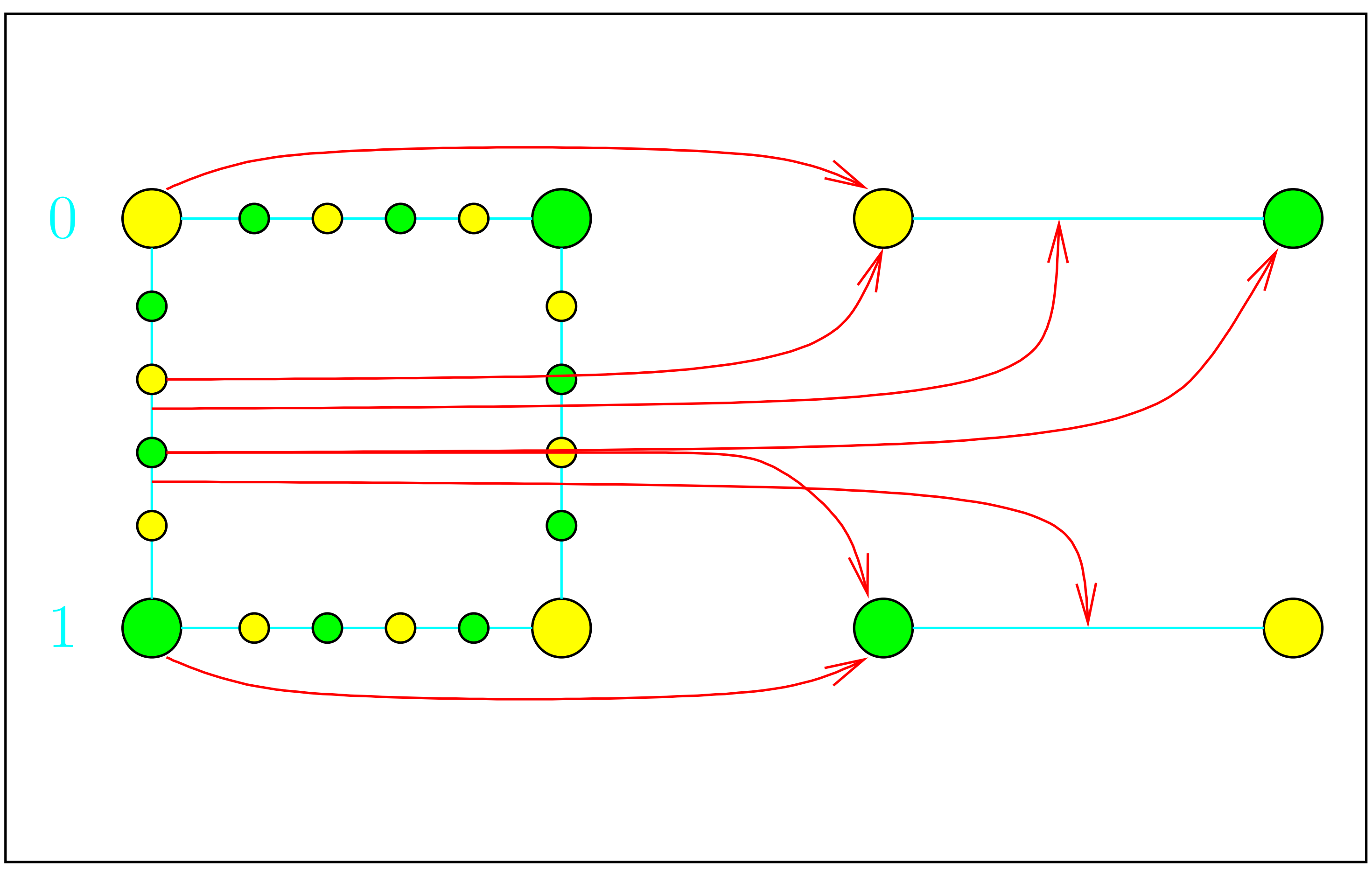
Le même état initial voisin du précédent.

Les processus décident 1.



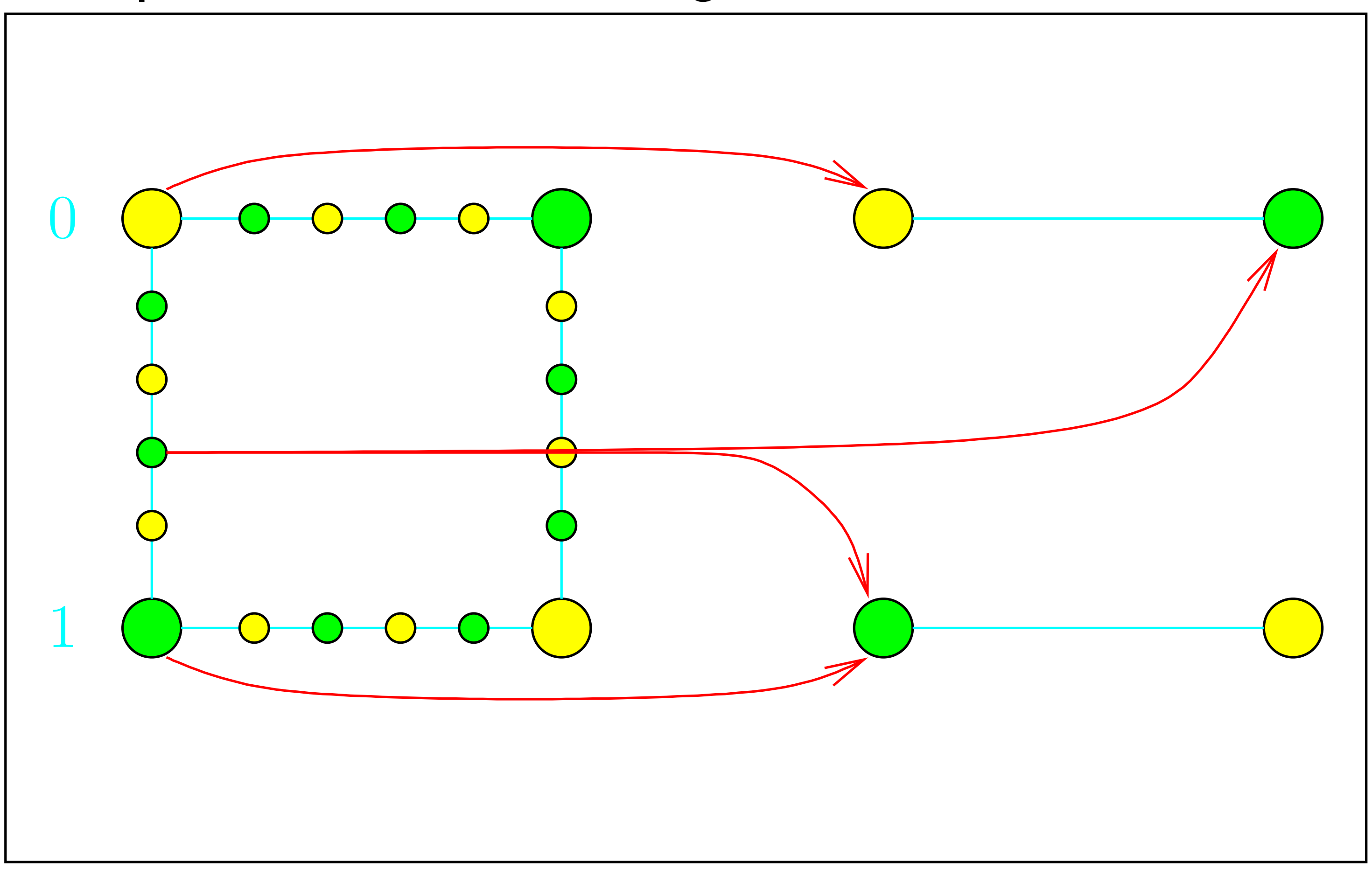
Application

μ est simpliciale et chromatique.



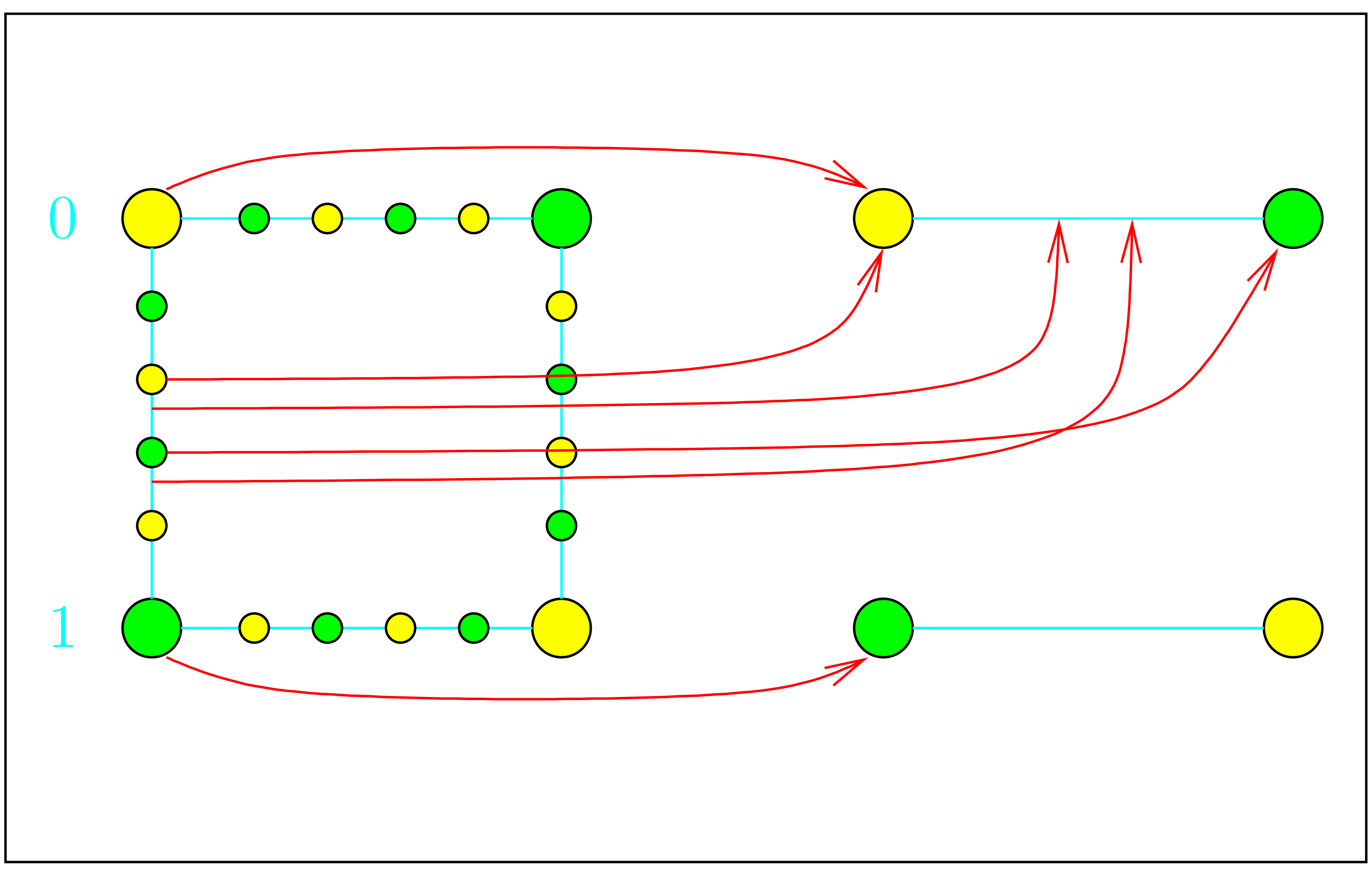
Application

μ est une fonction, elle ne peut projeter
un même point vers deux images.



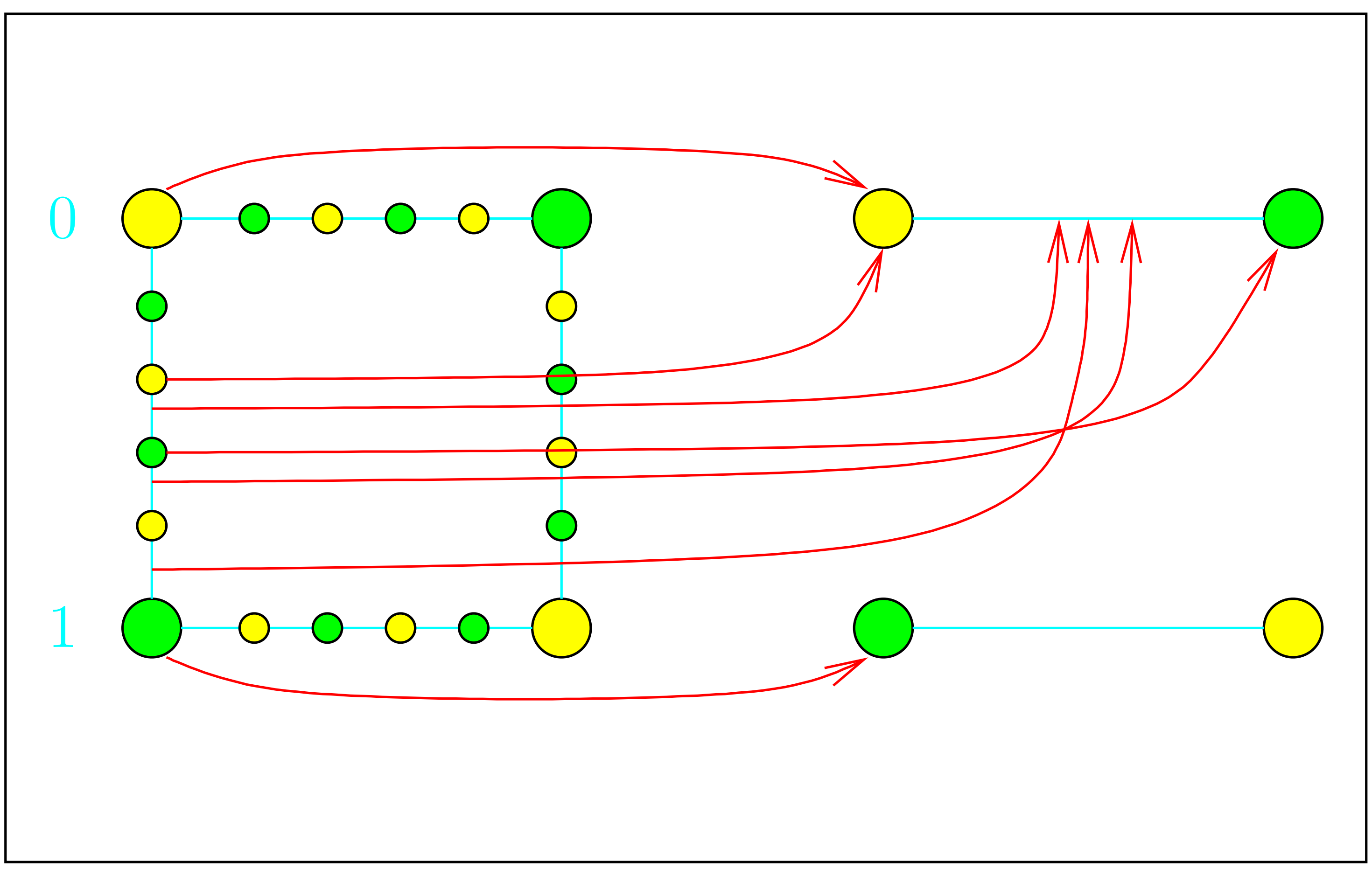
Application

Donc les deux processus décident 0.



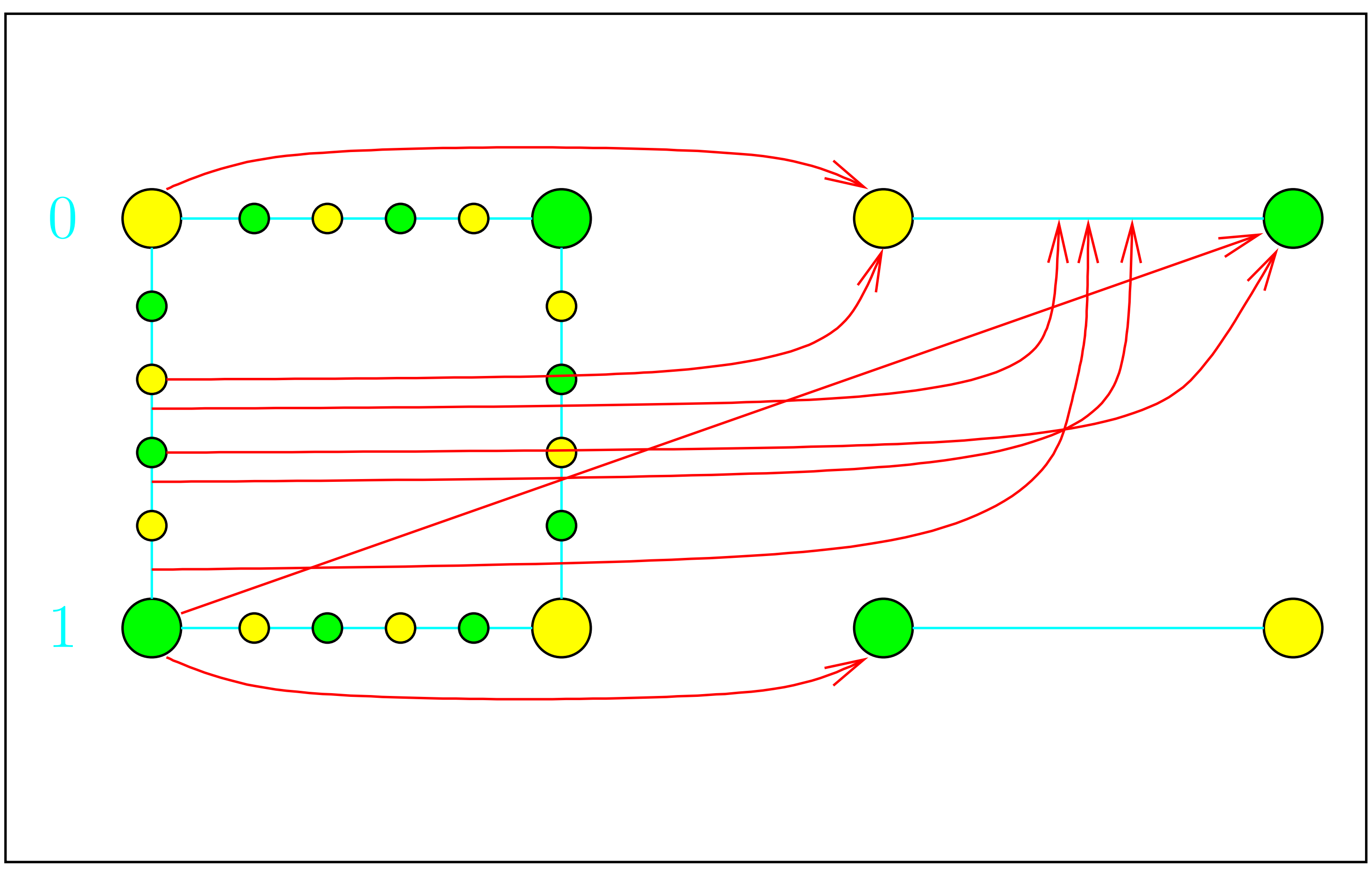
Application

Par récurrence, toutes les configurations initiales décident 0.



Application

μ est simpliciale et chromatique.



La suite ...

Rappels de topologie : continuité, limite, ...

Homologie

Groupe fondamental

Preuve de nécessité

Quelques éléments à propos de la suffisance

Espaces topologiques

Un espace *topologique* $(X, \mathcal{T})$ est un couple :

- X un ensemble
- $\mathcal{T}$ famille de sous-ensemble de X appelés *ouverts*
- $\emptyset \in \mathcal{T}$, $X \in \mathcal{T}$
- $\mathcal{T}$ est clos par union arbitraire, et intersection finie.

Espaces topologiques

La topologie associée à un espace permet de capturer les notions de :

- Limite d'une suite à valeurs dans X;
- Continuité d'une fonction $f : X \to X$;
- Voisinage d'un point $x \in X$.

Espaces métriques

Distance

d est une *distance* si :

$$d : X \times X \to \mathbb{R}^+$$

$$\forall x \in X \quad d(x,x) = 0$$

$$\forall x, y \in X \quad d(x,y) = d(y,x)$$

$$\forall x, y, z \in X \quad d(x,y) \leq d(x,z) + d(z,y)$$

Espaces métriques

Boules ouvertes, fermées, sphères

On peut alors définir la boule ouverte de centre x de rayon ε :

$$B_\varepsilon(x) = \{y \in X : d(x,y) < \varepsilon\}$$

La boule fermée de centre x de rayon ε :

$$\overline{B_\varepsilon(x)} = \{y \in X : d(x,y) \leq \varepsilon\}$$

La sphère de centre x de rayon ε :

$$\partial B_\varepsilon(x) = \{y \in X : d(x,y) = \varepsilon\}$$

Espaces métriques

Topologie induite

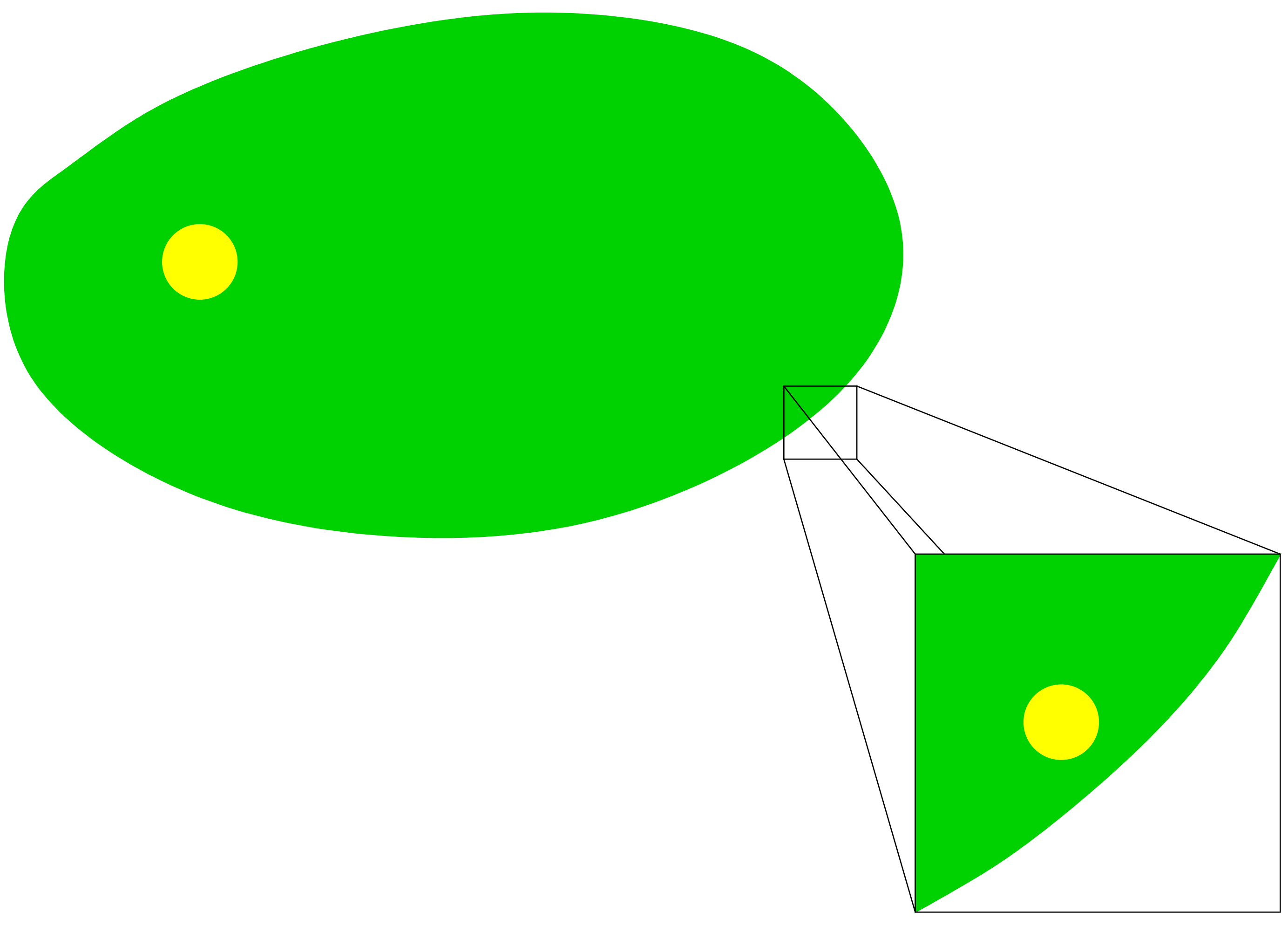
Un ouvert $Y \in \mathcal{T}$ est définie par :

$$\forall y \in Y \quad \exists \varepsilon > 0 \text{ tel que } B_\varepsilon(y) \subseteq Y$$

$\mathcal{T}$ est appelée la *topologie métrique* induite par d sur X

Espaces métriques

Un exemple d'ouvert



Continuité

Voisinage

U est un voisinage du point x, s'il existe un ouvert contenant x inclus dans U. On notera $\mathcal{U}(x)$, l'ensemble des voisinages de x.

Continuité

Limite d'une suite

Soit $u = (u_n)_{n \in \mathbb{N}}$ une suite à valeurs dans X, espace topologique. On dit que u tend vers $x \in X$, si :

$$\forall\, U \in \mathcal{U}(x), \quad \exists n_0 \in \mathbb{N} \quad \forall\, n \geq n_0 \quad u_n \in U.$$

On le note :

$$\lim_{n \to +\infty} u_n = x.$$

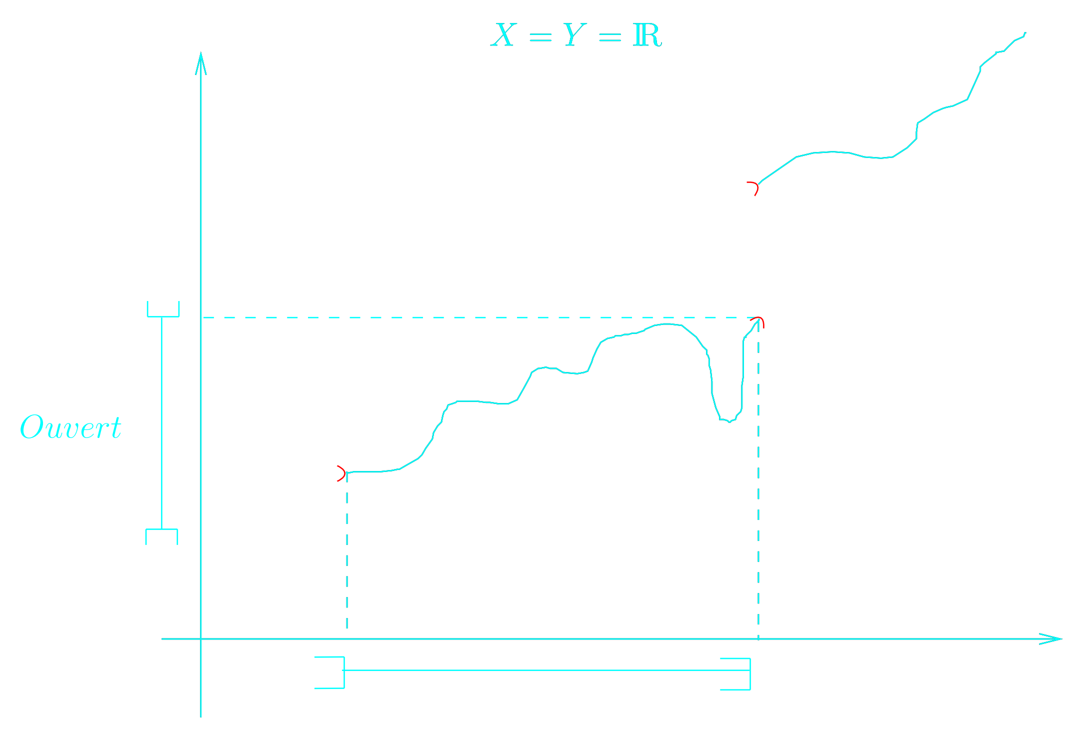
Continuité

On peut définir la notion de continuité des fonctions entre espaces topologiques. Soit f une fonction de X vers Y où X, Y sont des espaces topologiques. On dit que f est continue au point $x_0 \in X$ si :

$$\forall V \in \mathcal{U}(f(x_0)) \quad \exists U \in \mathcal{U}(x_0) \quad f(U) \subseteq V.$$

Par extension f est continue sur $A \subseteq X$, si f est continue en tout point de A.

Continuité



Continuité

Si $f : X \to Y$, $g : Y \to Z$ sont continues alors $g \circ f : X \to Z$ définie par :

$$\forall x \in X \quad g \circ f(x) = g(f(x))$$

est continue.

L'application $Id_X : X \to X$, définie par :

$$\forall x \in X \quad Id_X(x) = x$$

est continue.

Homéomorphisme

Deux espace topologiques X et Y sont dits homéomorphes, lorsqu'il existe une fonction $f : X \to Y$ continue, bijective, et d'inverse $f^{-1} : Y \to X$ continue.
f est appelée homéomorphisme.

Ceci signifie que l'on peut passer de X à Y
(et réciproquement) par des déformations réversibles.

Homotopie

Deux fonctions continues $f, g : X \to Y$ sont homotopes, s'il existe une fonction continue F :

$$F : X \times [0,1] \to Y$$

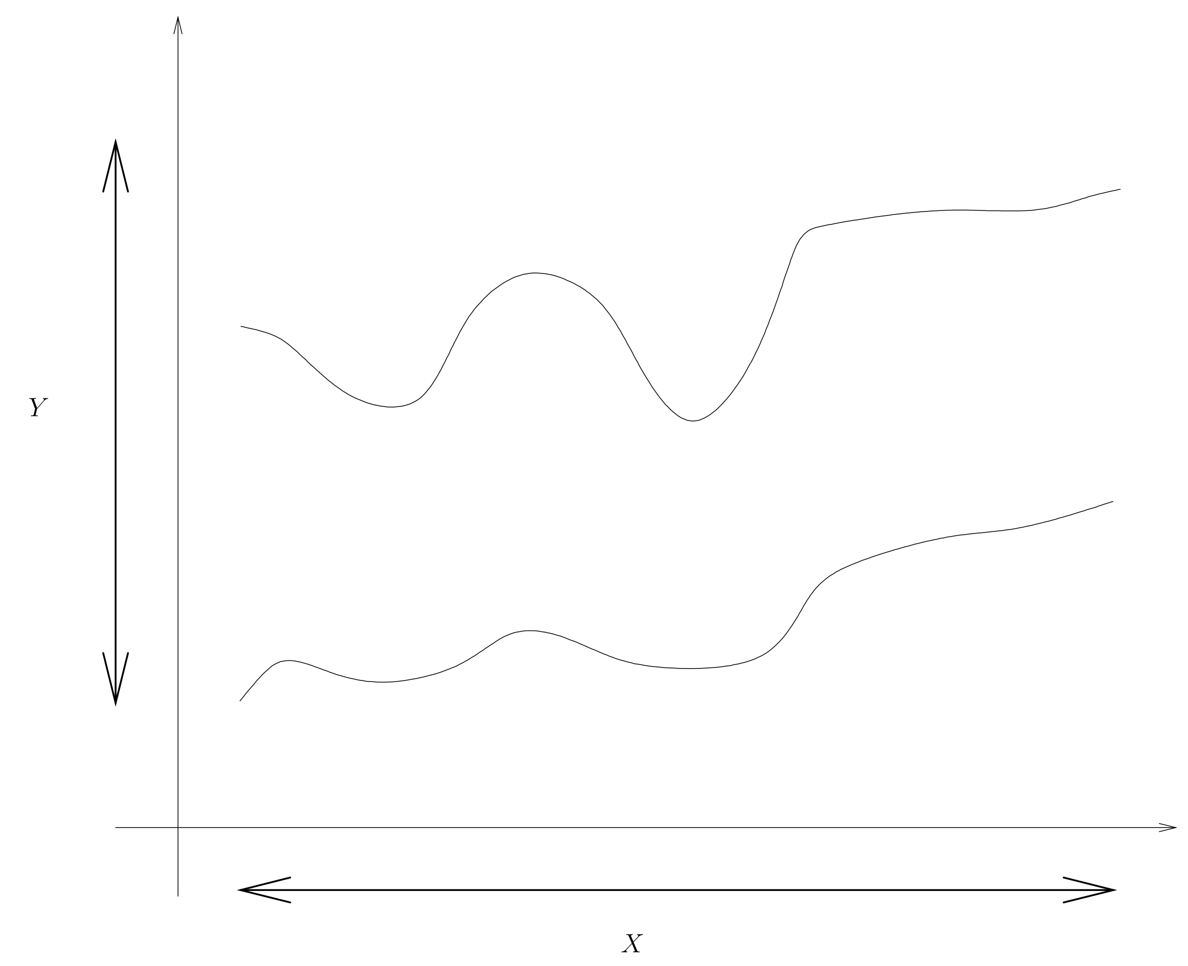
telle que :

$$\forall x \in X \begin{cases} F(x,0) = f(x) \\ F(x,1) = g(x) \end{cases}$$

On le note $f \simeq g$, et c'est une relation d'équivalence.

On peut déformer continûment f en g.

Exemples d'homotopie



Homotopie

En prenant $F(x,t) = f(x)$, f est homotope à elle-même.

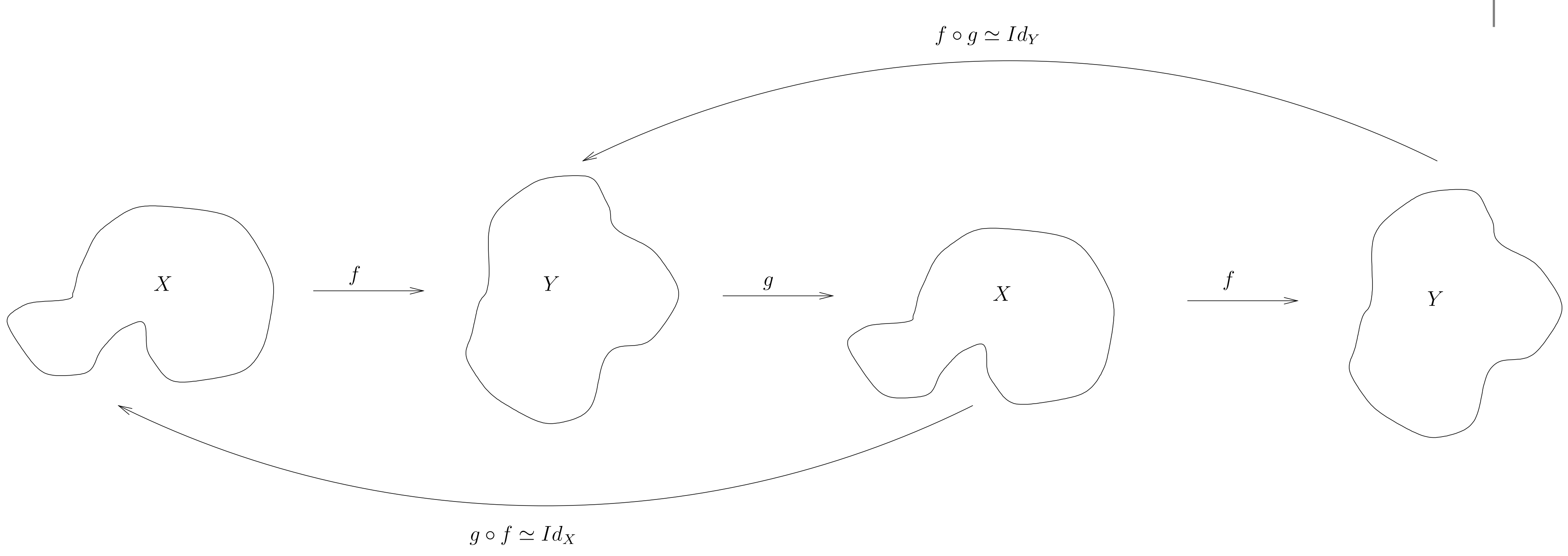
Soit $f : X \to X$ définie par $f = c$, et $g = Id_X$, alors $f \simeq g$ par $F(x,t) = t(x-c) + c$.

Homotopie

Soient $f : X \to Y$ et $g : Y \to X$.

- Si $f \circ \underline{g} \simeq Id_Y$, alors g est l'inverse homotope à *droite* de f.
- Si $\underline{g} \circ f \simeq Id_X$, alors g est l'inverse homotope à *gauche* de f.
- Si g est l'inverse à droite et à gauche de f, alors f est l'inverse à droite et à gauche de g.
- Dans ce cas X et Y sont dits homotopes.

Exemples d'espaces homotope



Homotopie

Soit $f : X \to Y$ un homéomorphisme.

Comme $f \circ f^{-1} = Id_Y$ et $f^{-1} \circ f = Id_X$, f et f^{-1} sont des inverses homotopes.

$\Rightarrow$ X et Y homéomorphes $\Rightarrow$ X et Y homotopes.

Cycle

Un cycle c d'origine $x \in X$ est une fonction continue de $[0,1] \to X$ telle que :

$$c(0) = c(1) = x$$

Homotopie de cycles

Soit c_0 et c_1 deux cycles d'origine x , s'ils sont homotopes on les confond par la relation d'équivalence induite par l'homotopie. Il existe au moins une classe d'équivalence notée $[\![x]\!]$ associée au cycle constant $c([0,1]) = \{x\}$. On définit $\mathcal{C}(x)$ l'ensemble des cycles d'origine x.

Composition de cycles

On définit une opération $\circ$ de composition des cycles :

$$\begin{array}{rcccl} \circ : & \mathcal{C}(x) & \times & \mathcal{C}(x) & \rightarrow & \mathcal{C}(x) \\ & c_1 & \circ & c_2 & = & c\,, \end{array}$$

où :

$$c(x) = \begin{cases} 0 \leq x \leq 0.5 & c(x) = c_1(2x) \\ 0.5 \leq x \leq 1 & c(x) = c_2(2x-1) \end{cases}$$

Composition de classes

L'opération de composition des cycles est compatible avec la relation d'équivalence $\simeq$ induite par la relation d'homotopie :

$$[\![c_1 \circ c_2]\!] = [\![c_1]\!] \circ [\![c_2]\!]$$

Groupe fondamental

On peut définir $\Pi(X,x)$ le groupe fondamental associé à un point x par :

$$\Pi(X,x) = (\{[\![c]\!],\ c \in \mathcal{C}(x)\}, \circ)$$

L'élément neutre est la classe d'équivalence $[\![x]\!]$. L'inverse d'un élément $[\![c]\!]$ est défini par :

$$[\![c]\!]^{-1} = [\![c^{-1}]\!],$$

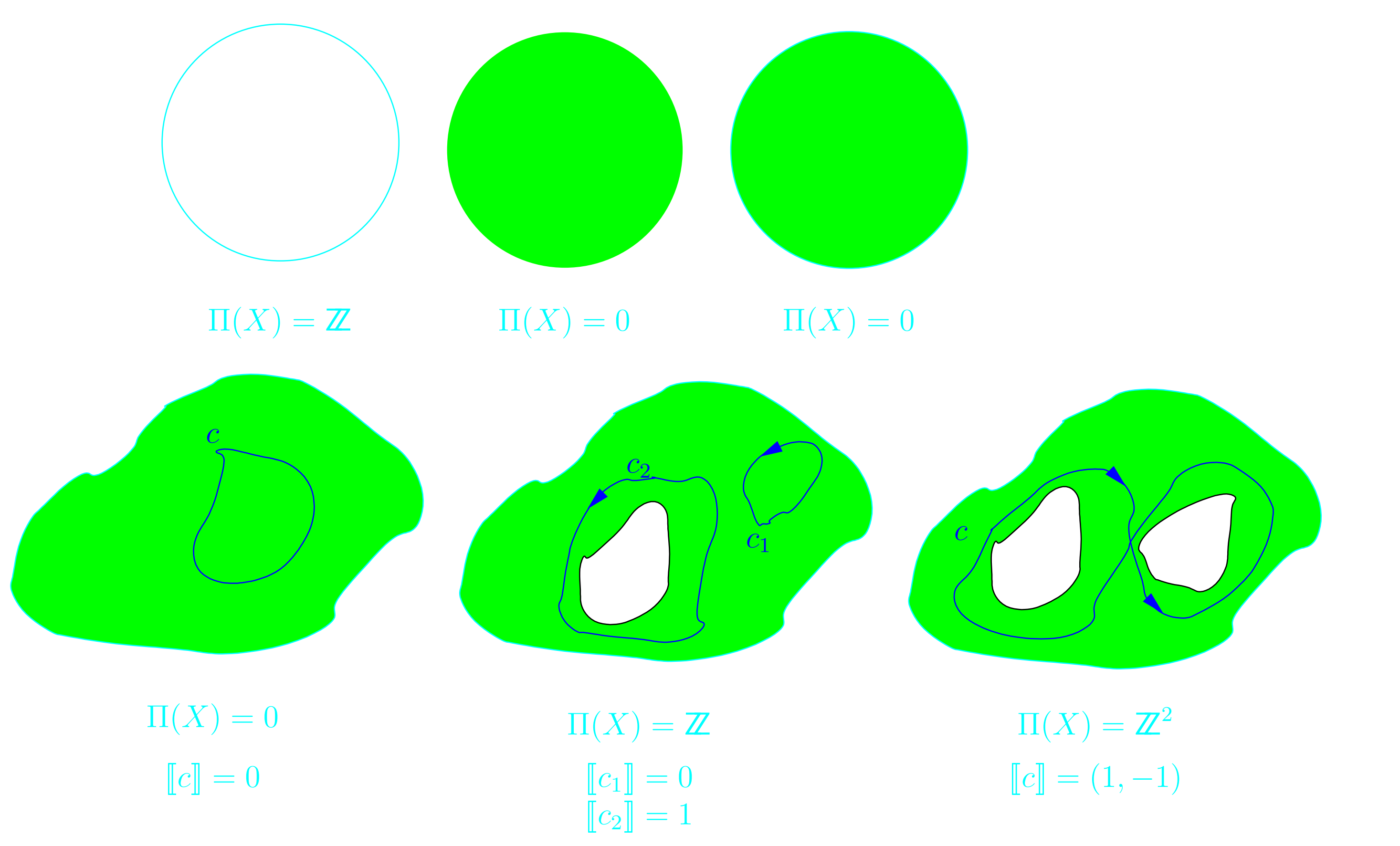
où :

$$c^{-1}(x) = c(1-x)$$

Indépendance

Pour un espace X simplement connexe, le groupe fondamental ne dépend pas du choix du point x. Pour des espaces non simplement connexes, c'est le produit des groupes fondamentaux de chacune des composantes connexes considérée séparément.

Groupe fondamental



Groupe fondamental

Soit X et Y deux espaces topologiques simplement connectés, soit f une fonction continue de X vers Y. Soit c_0, c_1 deux cycles appartenant à une même classe d'équivalence α de $\Pi(X)$. Alors $f \circ c_0$, et $f \circ c_1$ sont homotope et appartiennent à une même classe d'équivalence β de $\Pi(Y)$. On notera $\beta = f_\star(\alpha)$.
$f_\star : \Pi(X) \to \Pi(Y)$ est un homomorphisme de groupe :

$$\begin{cases} (1) & f_\star(0_X) = 0_Y \\ (2) & f_\star(a \circ b) = f_\star(a) \circ f_\star(b) \\ (3) & f_\star(a^{-1}) = f_\star(a)^{-1} \end{cases}$$

Groupe fondamental

Corollaire : si X et Y sont homéomorphes, alors $\Pi(X)$ et $\Pi(Y)$ sont isomorphes.

☞ La réciproque n'est pas vraie.

Groupe fondamental

Et après

Le groupe fondamental permet de mesurer les trous de dimension 2. Il permet de prouver que certains espaces ne sont pas homéomorphes. On peut étendre le procédé à des dimensions supérieures afin d'obtenir une équivalence entre homéomorphismes et groupes dans chaque dimension.

Homologie simpliciale

Soit $\mathcal{K}$ un complexe. Une chaîne de simplexes dans $\mathcal{K}$ de dimension k, est une somme formelle :

$$\sum n_i S_i,$$

où les n_i sont des éléments de $\mathbb{Z}$, et les S_i des éléments de $\mathcal{K}^{(k)}$.

Homologie simpliciale

On peut donc considérer le groupe des chaînes des dimension k dans un complexe $\mathcal{K}$:

- la somme de deux chaînes est une chaîne de même dimension, obtenue en sommant les coefficients des deux chaînes;
- l'inverse d'une chaîne est obtenue en inversant chacun des coefficients;
- l'élément neutre est la chaîne nulle (dont tous les coefficients sont nuls).

On le note $C_k(\mathcal{K})$.

Homologie simpliciale

Pour tout k-simplexe $S = [v_0, \ldots, v_k]$, on définit un opérateur de frontière de dimension k, noté ∂_k par :

$$\partial_k([v_0, \ldots, v_k]) = \sum_i (-1)^i [v_0, \ldots, \hat{v_i}, \ldots, v_k],$$

où $[v_0, \ldots, \hat{v_i}, \ldots, v_k]$ dénote le $(k-1)$-simplexe obtenu à partir de S en supprimant le sommet v_i. Ainsi défini, ∂_k associe à tout k-simplexe une chaîne de $C_{k-1}(\mathcal{K})$. On peut étendre linéairement ∂_k aux chaînes de $C_k(\mathcal{K})$:

$$\partial_k(\sum n_i S_i) = \sum_i n_i \partial_k(S_i)$$

On obtient un homomorphisme de groupes.

Homologie simpliciale

On obtient une chaîne d'homorphisme (un par dimension) :

$$C_n(\mathcal{K}) \xrightarrow{\partial} C_{(n-1)}(\mathcal{K}) \xrightarrow{\partial} \cdots \xrightarrow{\partial} C_1(\mathcal{K}) \xrightarrow{\partial} C_0(\mathcal{K})$$

L'opérateur de frontière vérifie :

$$\partial_k \circ \partial_{k+1} = 0$$

Exemple :

$$\begin{aligned}
\partial_1 \circ \partial_2([v_0, v_1, v_2]) &= \partial_1([v_1, v_2] - [v_0, v_2] + [v_1, v_2]) \\
&= (v_2 - v_1) - (v_2 - v_0) + (v_1 - v_0) \\
&= 0
\end{aligned}$$

Homologie simpliciale

Les éléments de

$$\text{Ker } \partial_k = \{c \in C_k(\mathcal{K}),\, \partial_k(c) = 0\},$$

sont appelés les cycles de dimension k.
Les éléments de

$$\text{Im } \partial_{k+1} = \{c \in C_k(\mathcal{K}),\, \exists\, c' \in C_{k+1}(\mathcal{K}),\, c = \partial_{k+1}(c')\},$$

sont appelés les frontières de dimension k.
Puisque $\partial_k \circ \partial_{k+1} = 0$, on a :

$$\text{Im } \partial_{k+1} \subseteq \text{Ker } \partial_k.$$

Toute frontière est un cycle. En général, la réciproque est fausse.

Homologie simpliciale

Soit c_1 et c_2 deux cycles de dimension k. Si $c_1 - c_2 = \partial_{k+1}(c)$, on dit qu'ils sont homologues.
L'homologie entre cycles est une relation d'équivalence notée $\simeq$:

$c \simeq c$ car

$$c - c = 0 = \partial_{k+1}(0)$$

$c_1 \simeq c_2 \Leftrightarrow c_1 \simeq c_2$ car

$$c_1 - c_2 = \partial_{k+1}(c) \Leftrightarrow c_2 - c_1 = \partial_{k+1}(-c)$$

$c_1 \simeq c_2 \wedge c_2 \simeq c_3 \Rightarrow c_1 \simeq c_3$

$$\begin{aligned} & c_1 - c_2 = \partial_{k+1}(c) \wedge c_2 - c_3 = \partial_{k+1}(c') \\ \Rightarrow\ & c_1 - c_3 = \partial_{k+1}(c) + \partial_{k+1}(c') = \partial_{k+1}(c + c') \end{aligned}$$

L'homologie entre cycles est une relation d'équivalence notée $\simeq$. Deux cycles sont homologues à une frontière près. Par ailleurs, les cycles homologues de dimension k forment un sous-groupe de Ker ∂_k. On le note Ker ∂_k/Im ∂_{k+1}, ou $H_k(\mathcal{K})$. On l'appelle le groupe d'homologie simpliciale d'ordre k du complexe $\mathcal{K}$

Homologie simpliciale

Les éléments de Im ∂_{k+1}, sont les représentants de la classe $[\![0]\!]$ dans $H_k(\mathcal{K})$.
Si tout cycle est une frontière, alors

$$\text{Ker } \partial_k = \text{Im } \partial_{k+1},$$

et $H_k(\mathcal{K})$ est le groupe trivial restreint à l'élément neutre.

Un élément non nul de $H_k(\mathcal{K})$ est un cycle, qui ne peut pas être vu comme étant la frontière d'un cycle de dimension $k+1$. C'est donc le bord (la frontière) d'un "trou" de dimension k.

Homologie réduite

Remarquons que H_0 mesure les trous de dimension 1, à savoir les couples de sommets qui ne sont pas la frontière d'une chaîne de 1-simplexe. Autrement dit les "trous" entre composantes connexes. Donc H_0 est isomorphe à $\mathbb{Z}^p$, òu p est le nombre de composantes connexes. Il est possible de modifier la définition de ∂_0, de manière à ce que H_0 soit isomorphe à $\mathbb{Z}^{p-1}$, donc réduit au groupe trivial, s'il n'y a qu'une seule composante connexe. C'est l'homologie réduite.

Exemples

Le n-disque $\mathcal{S}_n$ a des groupes d'homologie réduits triviaux dans toutes les dimensions.

La n-sphère $\partial\mathcal{S}_n$ a des groupes d'homologie réduits triviaux dans toutes les dimensions, sauf en dimension $n-1$, où $H_{n-1}(\mathcal{S}_n) = \mathbb{Z}$.

Un complexe $\mathcal{K}$ de dimension n , qui comme le n-disque a des groupes d'homologie réduites triviaux dans toutes les dimensions est dit acyclique.

Fonctions simpliciales

Une fonction simpliciale f d'un complexe $\mathcal{K}$ vers un complexe $\mathcal{L}$ induit une séquence d'homomorphismes $f_\#$ de groupe des chaînes de $\mathcal{K}$ vers les chaînes de $\mathcal{L}$. $f_\#$ est défini par :

$$
\begin{aligned}
\forall \mathcal{C} \in C_k(\mathcal{K}) \quad f_\#(\mathcal{C}) &= f_\#(\sum n_i S_i) \\
&= \sum n_i f_\#(S_i) \\
&= \sum n_i \begin{cases} 0 & \text{si } \dim f(S_i) < k \\ S_i & \text{sinon} \end{cases}
\end{aligned}
$$

Par ailleurs, on a :

$$\partial \circ f_\# = f_\# \circ \partial$$

Fonctions simpliciales

Par ailleurs, on a :

$$\partial \circ f_{\#} = f_{\#} \circ \partial$$

Donc les images par $f_{\#}$

des cycles de $\mathcal{K}$ sont des cycles de $\mathcal{L}$;

des frontières de $\mathcal{K}$ sont des frontières de $\mathcal{L}$;

Donc $f_{\#}$ induit une séquence d'homorphismes $f_{\star}$ de groupes entre les groupes d'homologie de $\mathcal{K}$ et les groupes d'homologie de $\mathcal{L}$.

Approximation simpliciale

Soit $\mathcal{K}$ et $\mathcal{L}$ deux complexes. Soit $f : \mathcal{K} \to \mathcal{L}$ une fonction simpliciale. On peut prolonger f en une fonction continue $|f| : |\mathcal{K}| \to |\mathcal{L}|$:

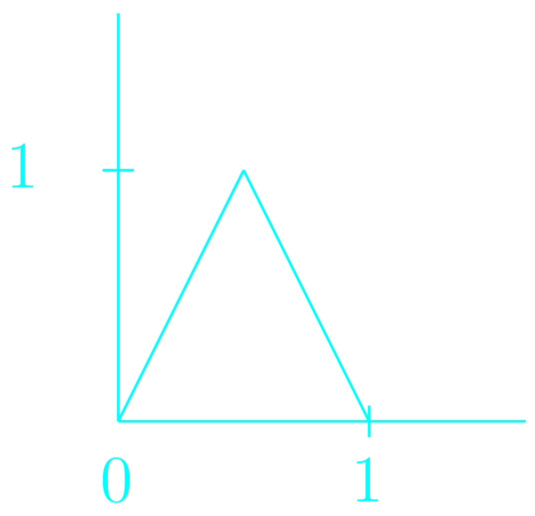
$\forall x \in |\mathcal{K}|, \exists X = \{x_0, \ldots, x_k\} \in \mathcal{K}$ t.q $x \in |X|$
avec $x = (t_0, \ldots t_k),$ on pose $|f|(x) = \sum t_i |f(x_i)|$

➨ La réciproque est-elle vraie ? Peut-on associer une fonction simpliciale à toute fonction continue ?

Approximation simpliciale

Les fonctions simpliciales de $\mathcal{K} = \{\{a, b\}, \{a\}, \{b\}\}$ dans lui-même, sont :
(1) la fonction constante égale à a
(2) la fonction constante égale à b
(3) l'identité Id de $\{a, b\}$
(4) la permutation σ de $\{a, b\}$, telle que $\sigma^2 = Id$
Donc en identifiant $|\mathcal{K}|$ à $[0, 1]$, la fonction $f : [0, 1] \rightarrow [0, 1]$ définie par :

$$\begin{cases} 0 \leq x \leq 0.5 & f(x) = 2x \\ 0.5 \leq x \leq 1 & f(x) = 2(1 - x) \end{cases}$$



ne peut être le prolongement d'aucune fonction simpliciale.

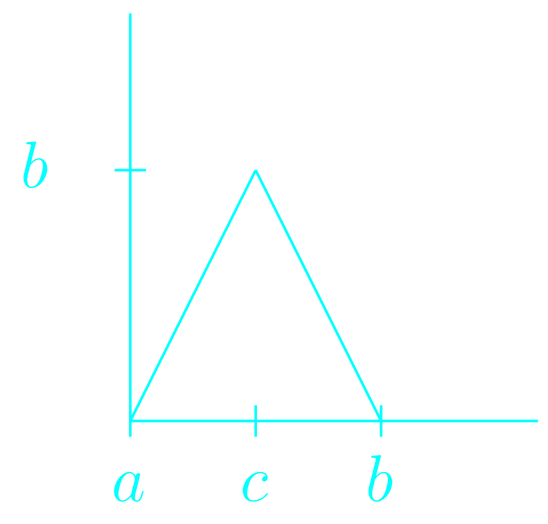
Approximation simpliciale

Cependant rajoutons un point intermédiaire dans $[0, 1]$, en $\frac{1}{2}$, ce qui revient à modifier $\mathcal{K}$ en :

$$\sigma(\mathcal{K}) = \{\{a, b\}, \{b, c\}, \{a\}, \{b\}, \{c\}\}.$$

On préserve $|\mathcal{K}| = |\sigma\mathcal{K}|$. Et la fonction simpliciale $g : \sigma(\mathcal{K}) \to \sigma(\mathcal{K})$ définie par :

$$\begin{cases} g(a) &= a \\ g(c) &= b \\ g(b) &= a \end{cases}$$



vérifie $|g| = f$.

Approximation simpliciale

Théorème d'approximation simpliciale

Soit $\mathcal{K}$ $\mathcal{L}$ deux complexes et $g : |\mathcal{K}| \to |\mathcal{L}|$, une fonction continue. Il existe une subdivision $\sigma(\mathcal{K})$ et une fonction simpliciale $f : \sigma(\mathcal{K}) \to \mathcal{L}$ qui satisfait :

$$\forall\, X \in \sigma(\mathcal{K}), \quad g(|X|) \subseteq \bigcup_{Y \in \mathcal{L} \wedge f(X) \subseteq Y} |Y|$$

Invariance par subdivisions

Soit $\mathcal{K}$ un complexe simplicial, soit $\sigma(\mathcal{K})$ une subdivision de $\mathcal{K}$. On a :

$$\forall\, k \in \mathbb{Z} \quad H_k(\mathcal{K}) \equiv H_k(\sigma(\mathcal{K}))$$

Les groupes d'homologies sont invariants par subdivision.

En effet une subdivision ne peut ni créer, ni remplir un "trou".

Fonctions continues

Ce qui était vrai pour les fonctions simpliciales vis à vis des groupes d'homologie, le reste pour les fonctions continues, d'après ce qui précède :

- Invariance des groupes d'homologie par subdivision;
- Approximation des fonctions continues par des fonctions simpliciales au travers d'une subdivision suffisamment fine.

Toute fonction continue f d'un complexe simplicial $\mathcal{K}$, vers un complexe simpliciale $\mathcal{L}$ induit une séquence homomorphismes $f_\star$ entre les groupes d'homologie de $\mathcal{K}$ et de $\mathcal{L}$

Invariance par homotopie

Soit f et g deux fonctions continues du complexe $\mathcal{K}$ vers le complexe $\mathcal{L}$.

- Si f est homotope à g, alors $f_\star = g_\star$.

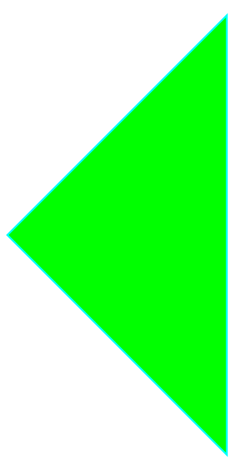
Soit f une fonction continue de $\mathcal{K}$ vers $\mathcal{L}$, et g une fonction continue de $\mathcal{L}$ vers $\mathcal{K}$.

- Si $f \circ g \simeq \mathrm{Id}_\mathcal{L}$, alors $f_\star \circ g_\star = \mathrm{Id}$.
  - $f_\star$ est surjective.
  - $g_\star$ est injective.
- Si $g \circ f \simeq \mathrm{Id}_\mathcal{K}$, alors $g_\star \circ f\star = \mathrm{Id}$.
  - $g_\star$ est surjective.
  - $f_\star$ est injective.
- Par conséquent, si $\mathcal{K}$ et $\mathcal{L}$ sont homotopes, on a :

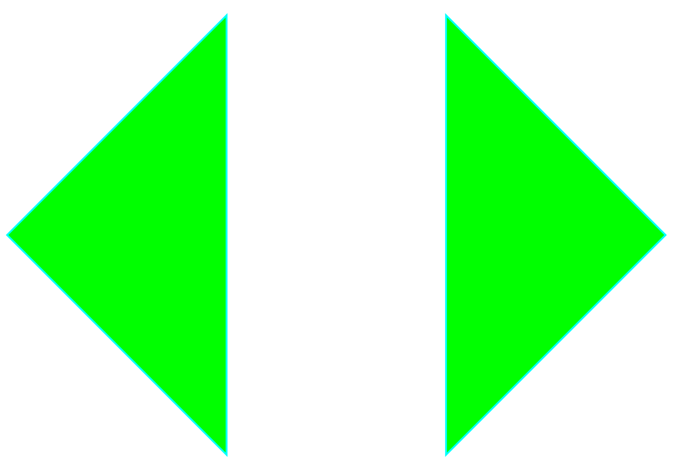
$$\forall\, k \in \mathbb{Z} \quad H_k(\mathcal{K}) \equiv H_k(\mathcal{L})$$

Mayer-Vietoris

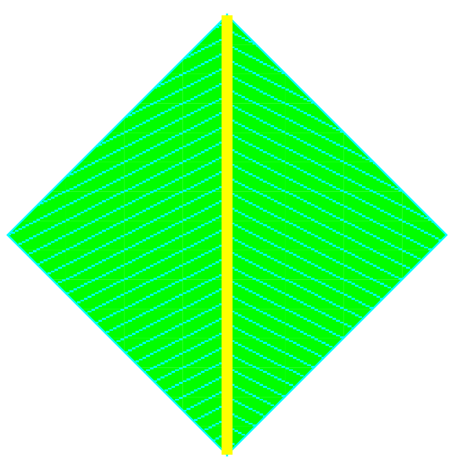
Soit $\mathcal{K}$ et $\mathcal{L}$ deux complexes simpliciaux acycliques, tels que $\mathcal{K} \cap \mathcal{L}$ soit aussi acyclique, alors $\mathcal{K} \cup \mathcal{L}$ est lui aussi acyclique.



$H_0(\mathcal{K}) = \mathbb{Z}$
$H_1(\mathcal{K}) = 0$

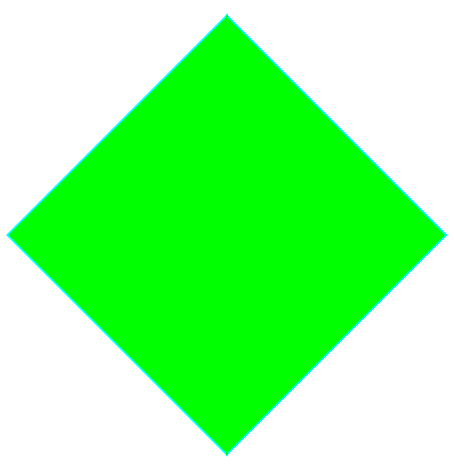


$H_0(\mathcal{K}) = \mathbb{Z}$ $H_0(\mathcal{L}) = \mathbb{Z}$
$H_1(\mathcal{K}) = 0$ $H_1(\mathcal{L}) = 0$



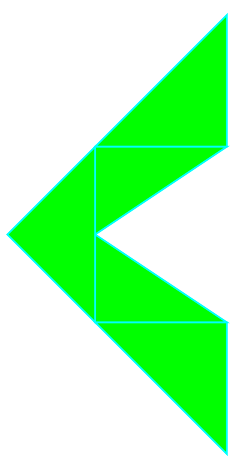
$H_0(\mathcal{K} \cap \mathcal{L}) = \mathbb{Z}$

$H_0(\mathcal{K}) = \mathbb{Z}$ $H_0(\mathcal{L}) = \mathbb{Z}$
$H_1(\mathcal{K}) = 0$ $H_1(\mathcal{L}) = 0$

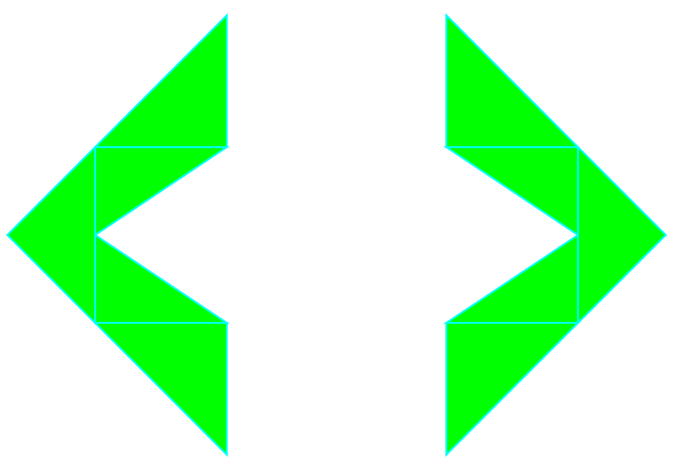


$H_0(\mathcal{K} \cup \mathcal{L}) = \mathbb{Z}$
$H_1(\mathcal{K} \cup \mathcal{L}) = 0$

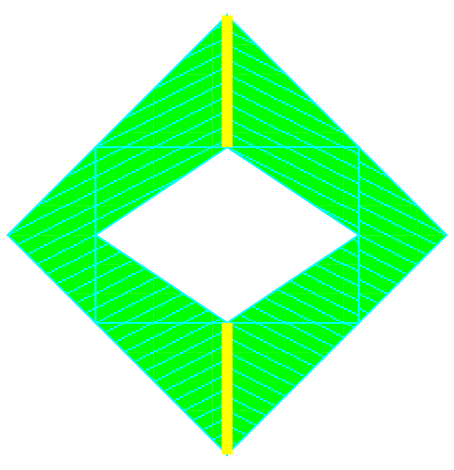
$H_0(\mathcal{K}) = \mathbb{Z}$ $H_0(\mathcal{L}) = \mathbb{Z}$
$H_1(\mathcal{K}) = 0$ $H_1(\mathcal{L}) = 0$



$H_0(\mathcal{K}) = \mathbb{Z}$
$H_1(\mathcal{K}) = 0$

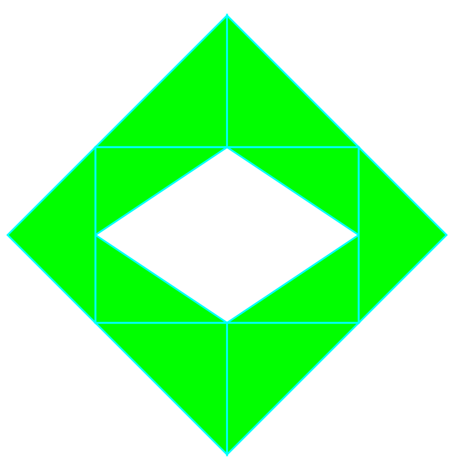


$H_0(\mathcal{K}) = \mathbb{Z}$ $H_0(\mathcal{L}) = \mathbb{Z}$
$H_1(\mathcal{K}) = 0$ $H_1(\mathcal{L}) = 0$



$H_0(\mathcal{K} \cap \mathcal{L}) = \mathbb{Z}^2$

$H_0(\mathcal{K}) = \mathbb{Z}$ $H_0(\mathcal{L}) = \mathbb{Z}$
$H_1(\mathcal{K}) = 0$ $H_1(\mathcal{L}) = 0$



$H_0(\mathcal{K} \cup \mathcal{L}) = \mathbb{Z}$
$H_1(\mathcal{K} \cup \mathcal{L}) = \mathbb{Z}$

$H_0(\mathcal{K}) = \mathbb{Z}$ $H_0(\mathcal{L}) = \mathbb{Z}$
$H_1(\mathcal{K}) = 0$ $H_1(\mathcal{L}) = 0$

Prédicat simplicial acyclique

Soit $\{\Phi_k\}_{k\in\mathbb{Z}}$ une séquence de prédicats sur les complexes simpliciaux. $\{\Phi_k\}_{k\in\mathbb{Z}}$ est un prédicat simplicial acyclique lorsque :

(1) Si $\mathcal{K}$ et $\mathcal{L}$ sont des complexes isomorphes, alors pour tout k on a

$$\Phi_k(\mathcal{K})=\Phi_k(\mathcal{L})$$

(2) Si $\mathcal{K}$ est le complexe engendré par un k-simplexe $(k \geq 0)$, alors

$$\Phi_k(\mathcal{K}) = 1$$

(3) Pour tout k, on a

$$\Phi_k(\mathcal{K}) \geq \Phi_{k+1}(\mathcal{K})$$

(4) Pour tout k, on a

$$\Phi_k(\mathcal{K} \cup \mathcal{L}) \geq \Phi_k(\mathcal{K})\Phi_k(\mathcal{L})\Phi_{k-1}(\mathcal{K} \cap \mathcal{K})$$

Prédicat acyclique

Exemples

Le prédicat (indépendant de k), qui est vrai ssi le complexe est simplement connexe;

Le prédicat qui est vrai ssi le groupe d'homologie de dimension k est nul.

Graphe des états

Un état global s du système est un ensemble d'états locaux (un par processus).

Un état initial s est état global, où chaque état local est une valeur initiale.

Dans un état global s, chaque processus i est sur le point d'appliquer une transition ε à son état local $s(i)$, qui le mène à $s'(i)$.

On note $s' = s.\varepsilon$ le nouvel état global ainsi obtenu.

On peut donc associer à tout ensemble I d'états initiaux un graphe $\mathcal{G}(I)$ dont les sommets sont des états globaux et les arcs les transitions.

Notations

Pour un état global s on notera $E(s)$ l'ensemble des transitions applicable à s (une par processus sauf les processus qui ont terminé).

$E(s)$ est partitionnable en deux sous-ensembles :

- $\Sigma(s)$ l'ensemble des SCAN applicables.
- $\Upsilon(s)$ l'ensemble des UPDATE applicables.

Complexe associé à un graphe

Un état global peut être représenté par un n-simplexe chromatique, où chaque sommet code l'état local d'un processus.

Pour un état global s, une transition $\varepsilon \in E(s)$, et $s' = s.\varepsilon$, les deux simplexes associés à s et s' partagent une face de dimension $n-1$ en commun, et ne diffère que d'un sommet. Celui associé au processus qui effectue la transition ε.

On peut donc associer un complexe dual à un graphe d'états.

Complexe final atteignable

On note $\mathcal{P}(s)$ l'ensemble des états finaux, dans lesquels le protocole peut conduire à partir de l'état s.

Soit $B \subset E(s)$. On note $\mathcal{P}^B(s)$, l'ensemble des états finaux, dans lesquels le protocole peut conduire à partir de l'état s, lorsque les processus de B restent bloqués à partir de s.

Soit $A \subseteq E(s) - B$. On note

$$\mathcal{P}_A^B(s) = \bigcap_{\varepsilon \in A} \mathcal{P}^B(s.\varepsilon)$$

C'est l'ensemble des états finaux, dans lesquels le protocole peut conduire à partir de l'état s, où les processus de B sont bloqués et les autres processus ne peuvent connaître quelle transition ε de A a été appliquée la première.

Propriétés

Soit s un état global, soit $E(s)$ les transitions applicables à s, soit $B \subset E(s)$, soit $R \subseteq \Sigma(s) - B$, soit $W \subseteq \Upsilon(s) - B$, on a :

$$
\begin{array}{lll}
(1) \quad \mathcal{P}^B_R(s) & = & \mathcal{P}^B(sR) \\
(2) \quad \mathcal{P}^B_W(s) & = & \mathcal{P}^B(sW) \\
(3) \quad \mathcal{P}^B_{R\cup W}(s) & = & \mathcal{P}^{B\cup R}_W(s) \\
 & = & \mathcal{P}^{B\cup R}(sW)
\end{array}
$$

Prédicat acyclique

Théorème

On considère un protocole complètement informé, et qui est totalement résilient sur un sous-ensemble I d'états initiaux. Soit s un état de I, $B \subseteq E(s)$, un sous-ensemble des transitions en attente à partir de s, tel que $|B| \leq n$, $R \subseteq \Sigma(s) - B$, et $W \subseteq \Upsilon(s) - B$, alors:

$$\begin{cases} (1) & \Phi_{n-|B|}(\mathcal{P}_R^B(s)) = 1 \\ (2) & \Phi_{n-|B|-|R|}(\mathcal{P}_{R\cup W}^B(s)) = 1 \\ (3) & \Phi_n(\mathcal{P}(s)) = 1 \end{cases}$$

Schéma de la preuve

La preuve est faite par induction ascendante sur le graphe fini $\mathcal{G}(I)$.

Cas de base

Si s est un état final, alors $E(s)$ est vide, par conséquence $B, R,$ et W aussi. Donc $\mathcal{P}(s)$ est réduit à un n-simplexe Z qui vérifie Φ_n.

Schéma de la preuve

Remontée du graphe vers un état initial

Soit s un sommet de $\mathcal{G}(I)$, tel que le théorème soit vérifié pour tout état $t > s$. On distingue les 3 cas suivants :

(1) R est non vide

(2) W est non vide

(3) R et W sont vides

Schéma de la preuve

(1) R est non vide

On sait que $\mathcal{P}_R^B(s) = \mathcal{P}^B(sR)$, et puisque $sR > s$ l'hypothèse d'induction assure que :

$$\Phi_{n-|B|}(\mathcal{P}_R^B(s))$$

Schéma de la preuve

(2) W est non vide

On sait que $\mathcal{P}^{B}_{R\cup W}(s) = \mathcal{P}^{B\cup R}(sW)$, et puisque $sW > s$ l'hypothèse d'induction assure que :

$$\Phi_{n-|B|-|R|}(\mathcal{P}^{B}_{R\cup B}(s))$$

Schéma de la preuve

(3) R et W sont vides

On pose $\alpha = n - |B|$. On veut montrer que $\mathcal{P}^B(s)$ satisfait Φ_α. On considère deux cas :

(1) Tous les processus qui ne sont pas bloqués (*i.e.* pas dans ids(B)), ont terminé dans s, alors $\mathcal{P}^B(s)$ est un α-simplexe et donc $\mathcal{P}^B(s)$ satisfait Φ_α.

(2) Sinon $E(s) - B$ est non vide et on a :

$$\mathcal{P}^B(s) = \bigcup_{\varepsilon \in E(s) - B} \mathcal{P}^B(s\varepsilon)$$

où chaque $\mathcal{P}^B(s\varepsilon)$ vérifie Φ_α (hypothèse de récurrence).

Schéma de la preuve

(3) R et W sont vides (suite)

On va utiliser le principe d'acyclicité.

Soit $R_1, \dots R_r$, r sous-ensemble non vide $\Sigma(s) - B$, on a :

$$\Phi_\alpha(\bigcup_{i=1}^{r} \mathcal{P}^B_{R_i}(s)) = 1$$

Ceci est vrai pour $r = 1$. On procède par récurrence. On pose :

$$\mathcal{A} = \bigcup_{i=1}^{r-1} \mathcal{P}^B_{R_i}(s)$$

On suppose que $\mathcal{A}$ satisfait Φ_α, comme $\mathcal{P}^B_{R_r}(s)$. On étudie $\mathcal{A} \bigcap \mathcal{P}^B_{R_r}(s)$.

$$\mathcal{A} \bigcap \mathcal{P}^B_{R_r}(s)$$

$$\mathcal{A} \bigcap \mathcal{P}^B_{R_r}(s) = \bigcup_{i=1}^{r-1} \mathcal{P}^B_{R_i}(s) \cap \mathcal{P}^B_{R_r}(s)$$

$$\mathcal{A} \bigcap \mathcal{P}^B_{R_r}(s) = \bigcup_{i=1}^{r-1} \mathcal{P}^B_{R_i}(s) \cap \mathcal{P}^B_{R_r}(s) = \bigcup_{i=1}^{r-1} \mathcal{P}^B_{R_i \cup R_r}(s)$$

qui satisfait Φ_α, donc $\Phi_{\alpha-1}$. Donc $\mathcal{A} \bigcup \mathcal{P}^B_{R_r}(s)$ satisfait Φ_α. On peut montrer de manière similaire que pour $W_1, \dots, W_w$ sous-ensembles non vide de $\Upsilon(s) - B$ on a :

$$\Phi_\alpha(\bigcup_{j=1}^{w} \mathcal{P}^B_{W_j}(s)) = 1$$

Schéma de la preuve

(3) R et W sont vides (suite)

Pour finir la preuve, on considère $R_1, \ldots R_m$, qui satisfont :

$$\exists \rho > 0 \text{ t.q. } \begin{array}{lrcl} (1) & |R_i| & \geq & \rho \\ (2) & |R_i - R_j| & \geq & 1 \end{array}$$

Cela assure $|R_i \bigcup R_j| \geq \rho + 1$. Les $W_1, \ldots, W_m$ sont quelconques. On montre par récurrence sur m que :

$$\Phi_{\alpha-\rho}(\bigcup_{i=1}^{m} \mathcal{P}^B_{R_i \cup W_i}(s)) = 1$$

Prédicat acyclique

Schéma de preuve

(3) R et W sont vides (suite)

Pour $m = 1$, on sait que :

$$\mathcal{P}^B_{R_i \cup W_i}(s) = \mathcal{P}^{B \cup R_i}(sW_i)$$

qui satisfait $\Phi_{\alpha - |R_i|}$, par hypothèse de récurrence, donc $\Phi_{\alpha-\rho}$ car $|R_i| \leq \rho$. On suppose maintenant que :

$$\mathcal{C} = \bigcup_{i=1}^{m-1} \mathcal{P}^B_{R_i \cup W_i}(s)$$

satisfait $\Phi_{\alpha-\rho}$, comme $\mathcal{P}^B_{R_m \cup W_m}$.

Prédicat acyclique

Schéma de preuve

(3) R et W sont vides (suite)

On étudie $\mathcal{C} \cap \mathcal{P}^B_{R_m \cup W_m}$:

$$\mathcal{C} \cap \mathcal{P}^B_{R_m \cup W_m} = \bigcup_{i=1}^{m-1} \mathcal{P}^B_{R_i \cup R_m \cup W_i \cup W_m}(s)$$

Or $|R_i \cup R_m| \leq \rho + 1$, donc $\mathcal{C} \cap \mathcal{P}^B_{R_m \cup W_m}$ satisfait $\Phi_{\alpha-\rho-1}$!

Prédicat acyclique

Corollaire

Soit un protocole complètement informé, et X une configuration initiale, pour laquelle le protocole est résilient. Alors $|\mathcal{P}(X)|$ est contractile.

Ossature

Une ossature φ (non chromatique), est une fonction simpliciale de $\sigma(\mathcal{I})$ vers $\mathcal{P}(\mathcal{I})$, telle que :

$$\forall\, S \in \sigma(\mathcal{I}) \quad \varphi(S) \in \mathcal{P}(\text{carrier}(S))$$