Supélec

Coalgèbres et Observations

G. Vidal-Naquet

Many people seem to be using coalgebras in various situations, without being aware of it.
B. Jacobs

Supélec

Approche mathématique des objets traités

Années 1975-80: Approche Algébrique
Guttag, Goguen, Thatcher...

Propriétés mathématiques indépendantes de la réalisation

Description formelle des objets :Spécification

Propriétés décrites par des équations et induites par des congruences

Démonstration de propriétés:
Principe d'induction

Exemples de Spécification 1/2

```
Spec Liste
 étend Élément , Bool
 sorte Liste
 opérations
      nil :                          → Liste
      cons : Liste, Élement          → Liste
      null : Liste                   → Bool
      tête: Liste                    → Élément
      reste: Liste                   → Liste
 préconditions pré car(l) = ¬ null(l)
 axiomes e : Élément ; l : Liste
      null(nil) ≡ vrai
      null(cons(l,e)) ≡ faux
      tête(cons(l,e)) ≡ e
      reste(nil) ≡ nil
      reste(cons(l,e)) ≡ l
FSpec
```

Signature:
domaines,
codomaines
des symboles de fonctions

Exemples de Spécification 2/2

```
Spec Graphiques
étend Réel
sorte P(oint), S(egment), …
opérations
   cp:  Réel,Réel      → P
   cs:  P, P           → S
   tp:  P, P           → P
   ts:  S, P           → S
   abs: P              → Réel
   ord: P              → Réel
   milieu:S            → Point …
 préconditions pré cp(x,y)=-4000<x ^x<4000^-4000<y^y<4000
axiomes x,y,u,v:Réel, p1,p2,p3:P
abs(cp(x,y)) ≡ x
ord(cp(x,y)) ≡ y
tp(cp(x,y),cp(u,v)) ≡ cp(x+u,y+v)
ts(cs(p1,p2),p3) ≡ cs(tp(p1,p3), tp(p2,p3))
...
FSpec
```

Spécification et Algèbre

Algèbre associée:

Chaque symbole d'ensemble correspond à un ensemble

Chaque symbole de fonction correspond à une fonction

Les axiomes sont satisfaits

Exemple

$A_k = \langle R, \mathcal{P}, S, +, *, 0, cp, cs, tp, ts \rangle$

A_1, A_2, A_3 $\mathcal{P}$:ensemble de points

cs fonction de $\mathcal{P} \times \mathcal{P}$ dans S

$cs(p_1, p_2)$

A_1: $\{p_1, p_2\}$ A_2:  A_3: 

Autre exemple

```
Spec ExpBool
Sorte Rel,Bool
opération Rel,Bool
zero:                →Rel
true:                →Bool
false:               →Bool
inc:   Rel,Rel       →Rel
dec:   Rel, Rel      →Rel
inf:   Rel,Rel       →Bool
ou:    Bool,Bool     →Bool
axiomes
x:Nat, b,b':Bool
inc(dec(x)) ≡ dec(inc(x))  ≡ x
inf(x,x) ≡ false
inf(x,inc(x)) ≡ true
Si inf(x,y) ≡ true Alors inf((inc(x),inc(y)) ≡ true
ou(true,b)  ≡ true
ou(false,b)  ≡ b
…
```

Algèbres associés

$\langle Z,\{T,F\},+1,-1,T,F,<,\vee \rangle$

$\langle Z/5,\{T,F\},+2,-2,T,F,<,\vee \rangle$

$\langle Q,\{T,F\},+0{,}432,-0{,}432,T,F,<,\vee \rangle$

Algèbre non associé

$\langle Z,\{T,F\},+1,-1,T,F,\leq,\vee \rangle$

Algèbre des termes

```
Ou(inf(0,inc((inc(0))),inf(0,dec(0)))
```

terme de sorte (type) bool
congruence induite par les axiomes sur les termes

x ≡inc(dec(x))
inf(x,t) ≡ inf(inc(dec(x)),t)

Algèbre quotient
A_i=<$T_1/\equiv$, $T_2/\equiv$,…,$f_1/\equiv$…>

Propriété fondamentale : A_i est initiale

Pour toute algèbre A' associée,
il existe un morphisme unique de A_i dans A'

Supélec

Algèbres Initiales

Intuitivement en général
Algèbre initiale

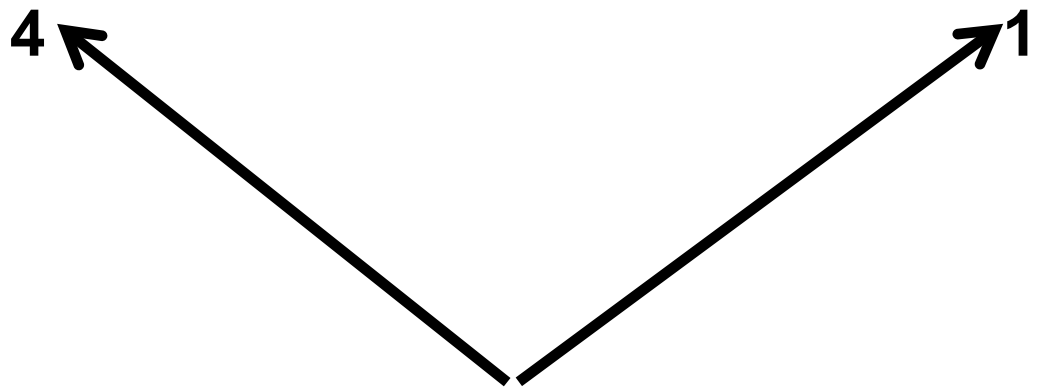
↔

Algèbre des termes
(quotienté par les équivalences induites par les axiomes)

Induction: Utilisation du caractère initial

Exemple

$A_1 = \langle Z, +1, -1, 0 \rangle$ $A_2 = \langle Z/3, +1, -1, 0 \rangle$



Supélec

Moralité(s)

A partir d'un état x de X, on construit un nouvel état $\mathcal{F}$(x)

Algèbre: $\mathcal{F}$(X) → X

Domaine des algèbres:

Construire des états (éléments)

Raisonner sur l'algèbre initiale

Prouver par induction des propriétés des états

Supélec

Evolutions

Evolution technologique:

Utilisation de modules tout faits (cots)

Evolution conceptuelle

Description mathématique des interactions

L'important n'est plus

"Comment on obtient les résultats"

mais

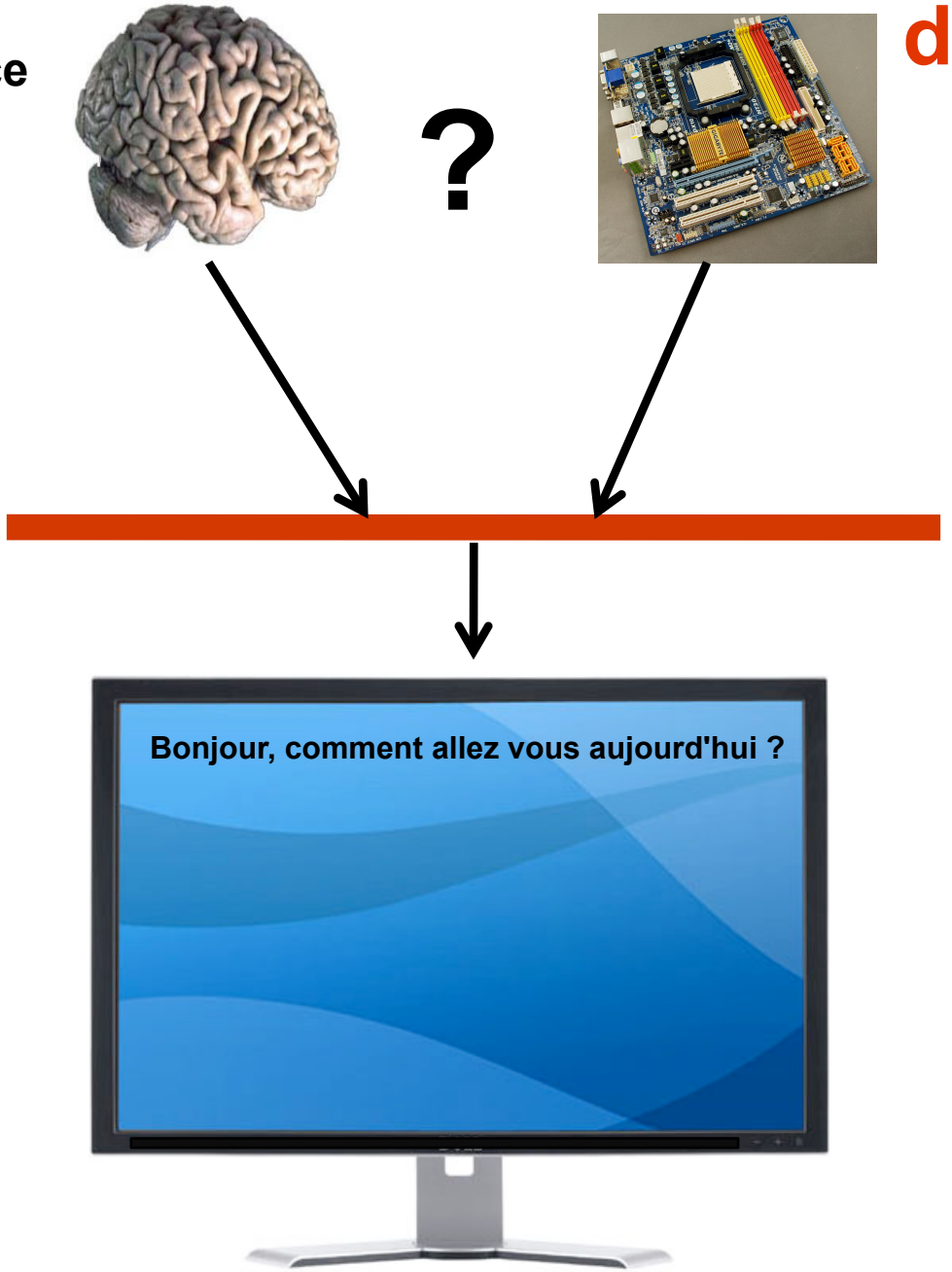
"Quels résultats on peut observer"

L'importance de l'observation ne date pas d'hier

Première mention de l'importance de l'observation :

Computing machinery and intelligence

1950 A. Turing



Supélec

Motivations

Les coalgèbres sont de plus en plus utilisées pour la description de la sémantique des systèmes caractérisés par l'observation en particulier les systèmes réactifs et les objets

Niveau d'abstraction adéquat:
Possibilités d'expression des systèmes.
Possibilités d'expression de propriétés et d'analyse

Permet d'unifier des concepts (bisimulation, congruences,...)

Sont fondées mathématiquement (par la théorie des catégories)

Supélec

Utilisation des Coalgèbres

Observation d'objets

```
estvide
longueur
tête
reste
```

Étant donné un état X, observation de l'état F(X)

X→ F(X)

Démonstrations de propriétés sur les observations

Complémentarité des approches

La description des sytèmes fait intervenir les deux approches.
Frontières parfois floues.
Relations entre algèbres et co-algèbres utilisées pour un même système

Example: `Listes`

- `nil`
- `cons`

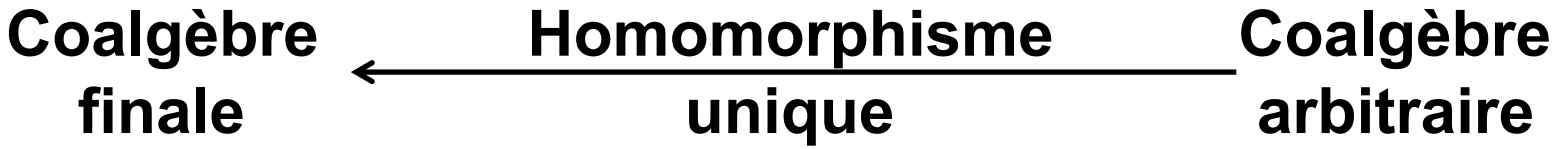
} Constructeurs

- `estvide`
- `longueur`
- `tête`
- `reste`

} Observateurs (déconstructeurs)

Supélec

Coalgèbres finales



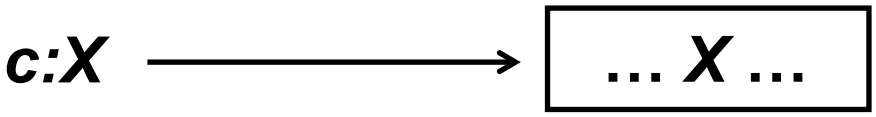
Co-induction: Utilisation du caractère final

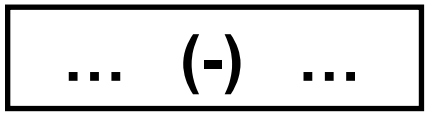
Présentation intuitive

Définition d'une coalgèbre

X **espace des états**

c **fonction de** ***S*** **dans un codomaine structuré faisant éventuellement intervenir** ***X***





Signature de la co-algèbre

Supélec

Formellement(1/2)

$\mathcal{F}$ **à un ensemble *X* fait correspondre une structure faisant intervenir éventuellement *X***

Coalgèbre de (pour) $\mathcal{F}$

(*S*,*c*) *c*:*S* → $\mathcal{F}$ (*S*)

***S*:ensemble des états (carrier)**

***c*: fonction de transition (manière d'évoluer)**

Supélec

Formellement (2/2)

Mathématiquement $\mathcal{F}$

foncteur

de `Ensembles` dans `Ensembles`

$\mathcal{F}$ foncteur de signature

Remarques:

Études pour $\mathcal{F}$ foncteur dans des catégories plus générales que les ensembles

***S* peut être un ensemble quelconque (discret ou pas),**

$\mathcal{F}$ peut être une observation "pure" ou indiquer également le type d'évolution

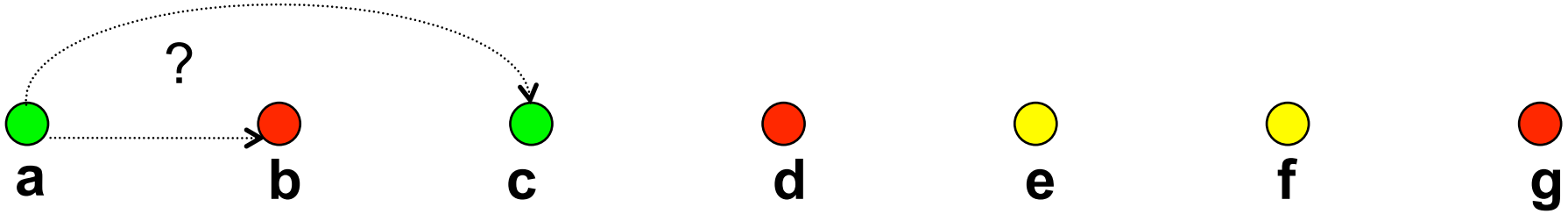
Observation sur l'état

Foncteur de signature $\mathcal{F}(X) = L$ $\mathcal{F} : L$

$$L=\{v,o,r\}$$

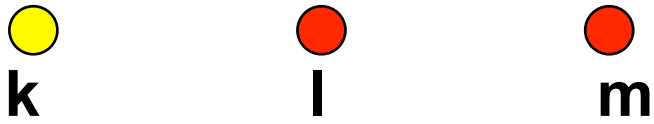
S= {a,b,c,d,e,f,g} $c(a)=v$, $c(b)=r$, $c(c)= v$, $c(d)=r$, $c(e)=o$, $c(f)=o$, $c(g)=r$.

Représentation graphique



Autre coalgèbre de même signature

S'= {k,l,m} $c'(k)=o$, $c'(l)=r$, $c'(m)= r$.

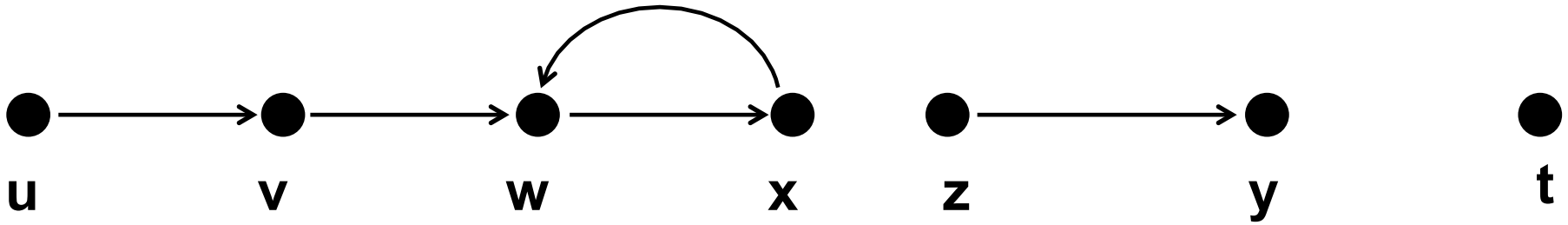


Changement d'état, arrêt

$\mathcal{F}(X) = \{\perp\} \cup X$ $\mathcal{F}$: {⊥} + id

$S = \{u,v,w,x,y,z\}$ $c(u)=v$, $c(v)=w$, $c(w)= x$, $c(x)=w$, $c(z)=y$, $c(y)= c(t)=\perp$.

Représentation graphique



Remarques: On peut ne rien savoir sur la manière de détermination de l' état suivant (relève de l'algèbre)

$S=Z^3$ $c(z, z', z'') = \begin{cases} \perp & \text{si } z'+z''\geq z \\ (z, z'+z'', z'') & \text{sinon} \end{cases}$

$c(s)$ peut être l'état précédent, état initial si $c(s)= \perp$

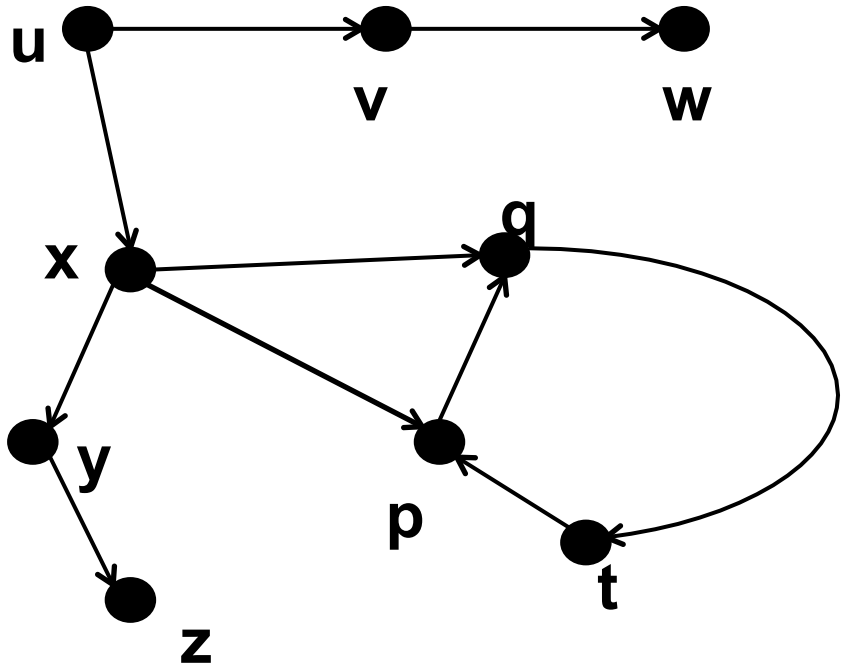
Changement d'état non-déterministe

$\mathcal{F}(X) = \mathcal{P}_f(X)$

Signature $\mathcal{F} : \mathcal{P}_f(\mathtt{id})$

c(u)={v,x}, c(v)={w}, c(w)=∅, c(x)={y,p,q} c(y)=z,
c(z)= ∅, c(p)={q,t} , c(t)={q} , c(q)={p}.

Représentation graphique



Observation de l'état et du changement

$\mathcal{F}(X) = (\{\perp\} \cup X) \times A$ Signature $\mathcal{F}$:$(\{\perp\} + \texttt{id}) \times A$

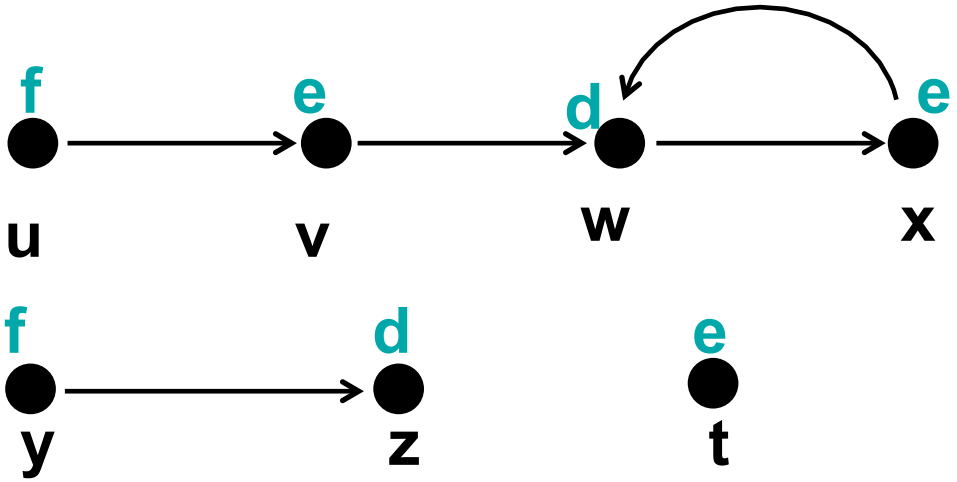
S= {u,v,w,x,y,z,t} A= {d,e,f}

c(u)= (f,v),
c(v)= (e,w),
c(w)= (d,x),
c(x)=(e,w),
c(y)=(f,z),
c(z)= (d, ⊥),
c(t) = (e, ⊥)

$c=(o,n)$

$c(s)=(o(s),n(s))$

Représentation graphique



Application d'un foncteur à une fonction

$\mathcal{F}$ **foncteur, f fonction de *S* dans *T***

Intuitivement

$\mathcal{F}$**(s) défini par exp(**s_1**,**s_2**,…)**

$\mathcal{F}$**(f) de** $\mathcal{F}$**(S) dans** $\mathcal{F}$**(T)**
($\mathcal{F}$ **(f))(s)=exp(**$s_1 \leftarrow f(s_1)$**,** $s_2 \leftarrow f(s_2)$**)**

Example: $\mathcal{F}(S)=A \times S$
$\mathcal{F}(s)=(a,q)$
$f(q)=r$
$\Rightarrow \mathcal{F}(f)(s)=(a,r)$

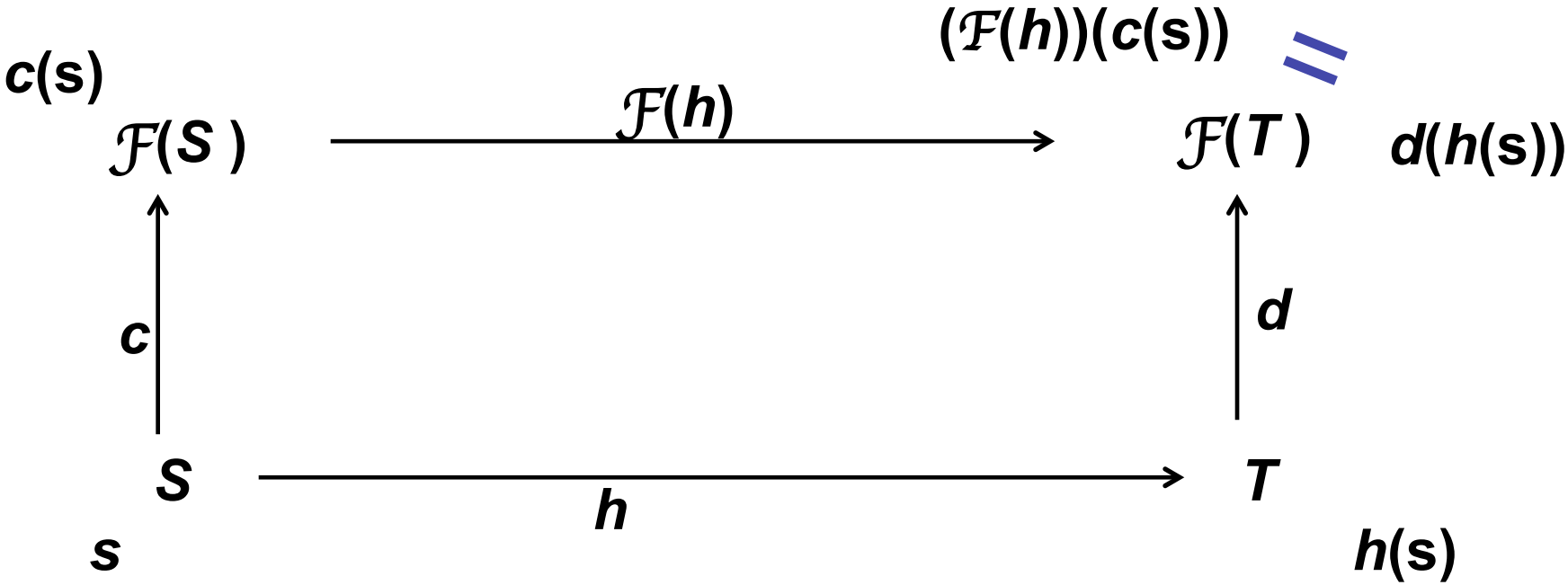
Homomorphisme de Coalgèbres

Définition

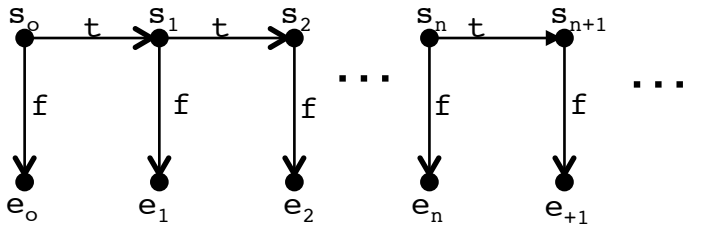
Soit $\mathcal{F}$ un foncteur,
c: $S \longrightarrow \mathcal{F}(S)$ et d: $\mathcal{F}(T)$ deux coalgèbres de $\mathcal{F}$

h: $S \longrightarrow T$ est un homomorphisme de coalgèbre
quand $d \circ h = \mathcal{F}(h) \circ c$

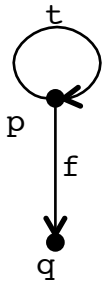
c.a.d que le diagramme suivant commute



Exemple



$\mathcal{F}:\mathcal{P}(A \times S)$



$S=\{s_o, s_1, s_2, \ldots, e_o, e_1, \ldots\}$

$T=\{p, q\}$

$c(s_i)=\{(t, s_{i+1}), (f, e_i)\}$

$c(e_i)= \varnothing$

$d(p)=\{(t,p),(f,q)\}$

$d(q)= \varnothing$

$h(s_i)=p \quad h(e_i)=q$

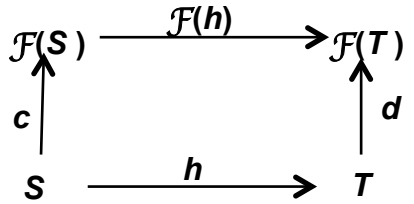
Vérification que *h* est un homomorphisme:

$c(s_i)=\{(t, s_{i+1}), (f, e_i)\}$ $\quad \mathcal{F}(h)c(s_i)=\{(t,p),(f,q)\}$

$h(s_i)=p \quad d(h(s_i))=d(p)= \{(t,p),(f,q)\}$

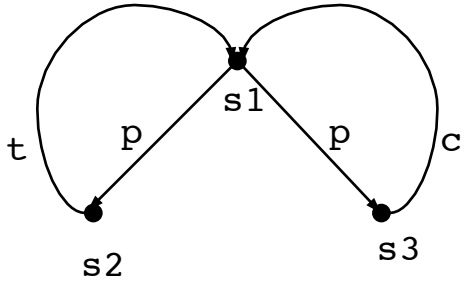
$c(e_i)=\varnothing \qquad \mathcal{F}(h)c(e_i)= \varnothing$

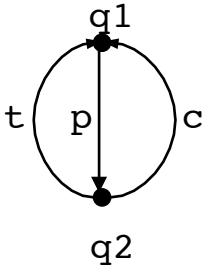
$h(e_i)=q \quad d(q)= \varnothing$



Exemples

$\mathcal{F}$: $\mathcal{P}$(A ×id)





$S=\{s_1,s_2,s_3)$

$S'=\{q_1, q_2)$

$c(s_1)=\{(p, s_2),(p,s_3)\}$
$c(s_2)=\{(t,s_1)\}$
$c(s_3)=\{(c,s_1)\}$

$c'(q_1)=\{(p, q_2)\}$
$c'(q_2)=\{(t, q_1),(c, q_1)\}$

$m(s_1)= q_1$ $m(s_2) = m(s_3)=q_2$

pas un homomorphisme

$c(s_2)=\{(t, s_1)\}$,$(\mathcal{F}(m))(c(s_2)) =\{(t, q_1)\}$

≠

$m(s_2)= q_2$ $c'(m(s_2))= c'(q_2)=\{(t, q_1),(c, q_1)\}$

Coalgèbre finale

Définition:

Une coalgèbre c_f: $S_f \longrightarrow \mathcal{F}(S_f)$ de $\mathcal{F}$ est finale pour $\mathcal{F}$ quand:

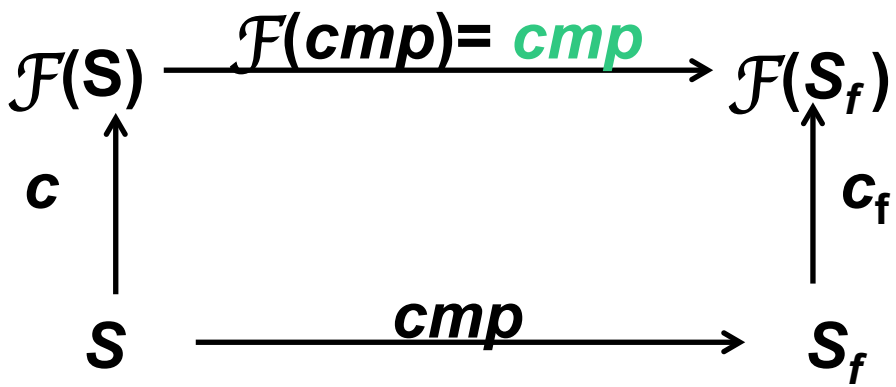
pour toute coalgèbre c: $S \longrightarrow \mathcal{F}(S)$

il existe une fonction unique *cmp* de S dans S_f

qui est un homomorphisme

de la coalgèbre c: $S \longrightarrow \mathcal{F}(S)$

dans la coalgèbre c_f: $S_f \longrightarrow \mathcal{F}(S_f)$

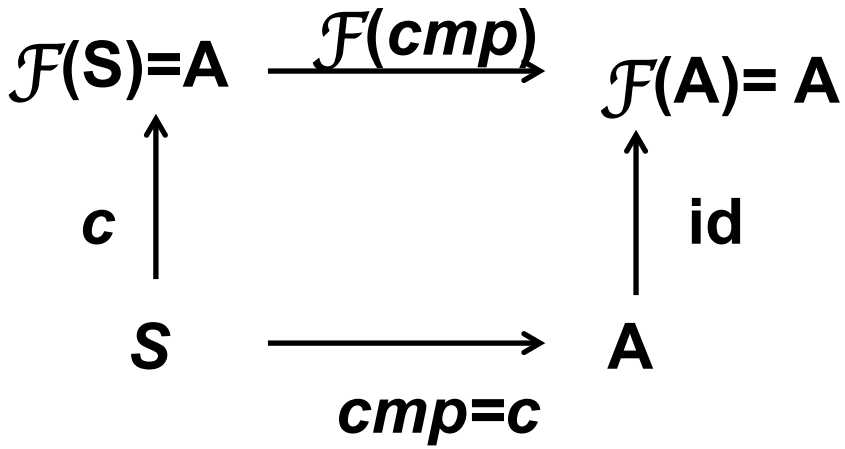


Coalgèbre finale pour l'observation

$id = c_f : A = S_f \longrightarrow A$

Signature:A, A={n,b,r}

$c : S \longrightarrow A$



S= {u,v,w,x,y,z} c(u)=n, c(v)=r, c(w)= n, c(x)=b, c(y)=b, c(z)=r.

cmp(u)=n, *cmp*(v)=r, *cmp*(w)= n, *cmp*(x)=b, *cmp*(y)=b, *cmp*(z)=r.

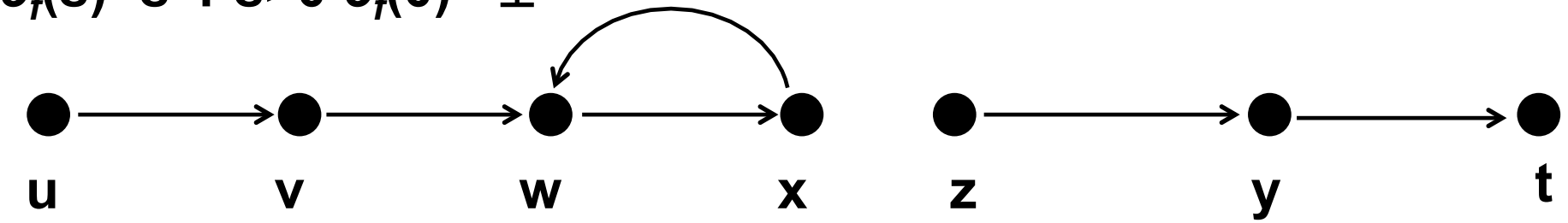
Coalgèbre finale pour le changement d'état

$\mathcal{F}(X) = \{\perp\} \cup X$

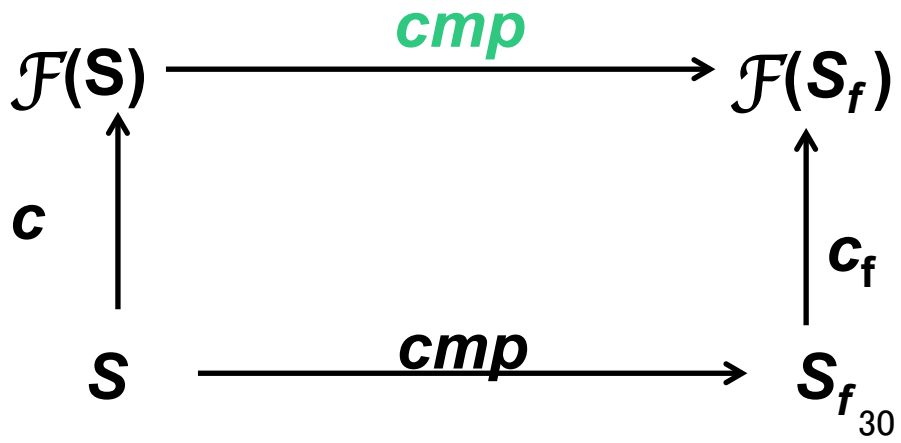
$c_f: S_f \longrightarrow \mathcal{F}(S_f) = \{\perp\} \cup S_f$

$S_f = \mathbf{N}^{\omega} = \mathbf{N} \cup \{\omega\}$, $\omega\text{-}1 = \omega$

$c_f(s) = s-1$ $s>0$ $c_f(0) = \perp$



cmp(u)=*cmp* (v)= *cmp* (w)= *cmp* (x)= ω
cmp(z)=2, *cmp*(y)= 1
cmp(t)= 0



Vérification que *cmp* est un morphisme

$c_f(cmp(u)) = c_f(\omega) = cmp(c(u)) = cmp(v) = \omega$

$c_f(cmp(z)) = c_f(2) = cmp(c(z)) = cmp(v) = 1$

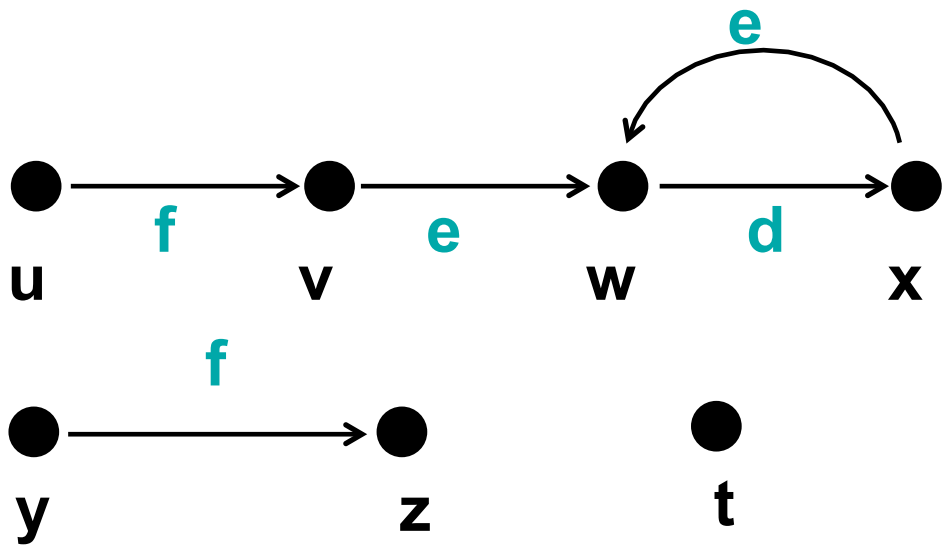
Coalgèbre finale pour les changements avec observation 1/5

Coalgèbre finale pour le foncteur $\mathcal{F}_o$: {⊥} +(A ×id) ?

Exemple:

S={u,v,w,x,y,z,t} A={d,e,f}

***c*(u)=(f,v), *c*(v)=(e,w), *c*(w)=(d,x), *c*(x)=(e,w)**
***c*(y)=(f,z), *c*(z)= ⊥, *c*(t)= ⊥**



Coalgèbre finale pour les changements avec observation 2/5

A ensemble donné

A^*
ensemble des suites finies d'éléments de A
ε suite vide

$A^\omega = A^{\mathbb{N}}$
ensemble des suites infinies d'éléments de A

$A^\infty = A^* \cup A^\omega$
ensemble des suites infinies ou infinies d'éléments de A

Supélec

Coalgèbre finale pour les changements avec observation 3/5

$S_f = A^\infty$ $\quad c_f : A^\infty \longrightarrow \{\perp\} \cup A \times A^\infty$

$\sigma = \sigma_o \sigma_1 \sigma_2 \ldots$

Si $\sigma \neq \varepsilon$ $\quad c_f(\sigma) = (\sigma_o, \sigma_1 \sigma_2 \ldots)$ $\quad o_f(\sigma) = \sigma_o$ $n_f(\sigma) = \sigma_1 \sigma_2 \ldots$

$c_f(\varepsilon) = \perp$

pour $\sigma \neq \varepsilon$ $c_f = (n_f, o_f)$

L'itération de c_f fournit tous les éléments observables

Remarque: c_f définit un isomorphisme

Coalgèbre finale pour les changements avec observation 4/5

Proposition:

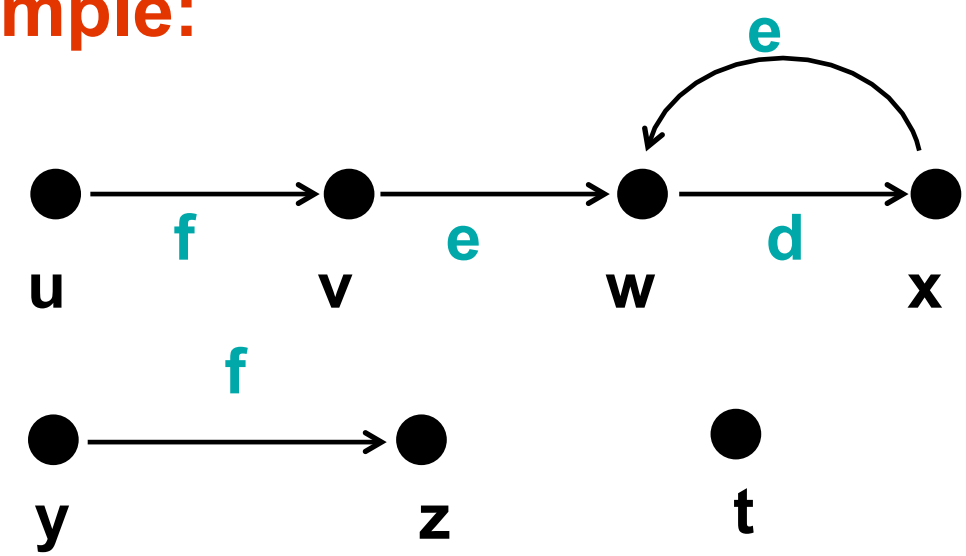
La coalgèbre c_f: $A^\infty \longrightarrow \{\perp\} \cup A \times A^\infty$ est finale pour $\mathcal{F}_o$.

Pour toute coalgèbre *c*: $S \longrightarrow \{\perp\} \cup A \times S$ construite sur un ensemble *S*, il existe une fonction unique *cmp* de *S* dans A^∞ qui est un morphisme de coalgèbre

- **Si *c*(x) = ⊥ alors c_f(*cmp*(x))= ⊥**
- **Si *c*(x) =(a,x') alors c_f(*cmp*(x))=(a, *cmp*(x'))**

Coalgèbre finale pour les changements avec observation 5/5

Exemple:



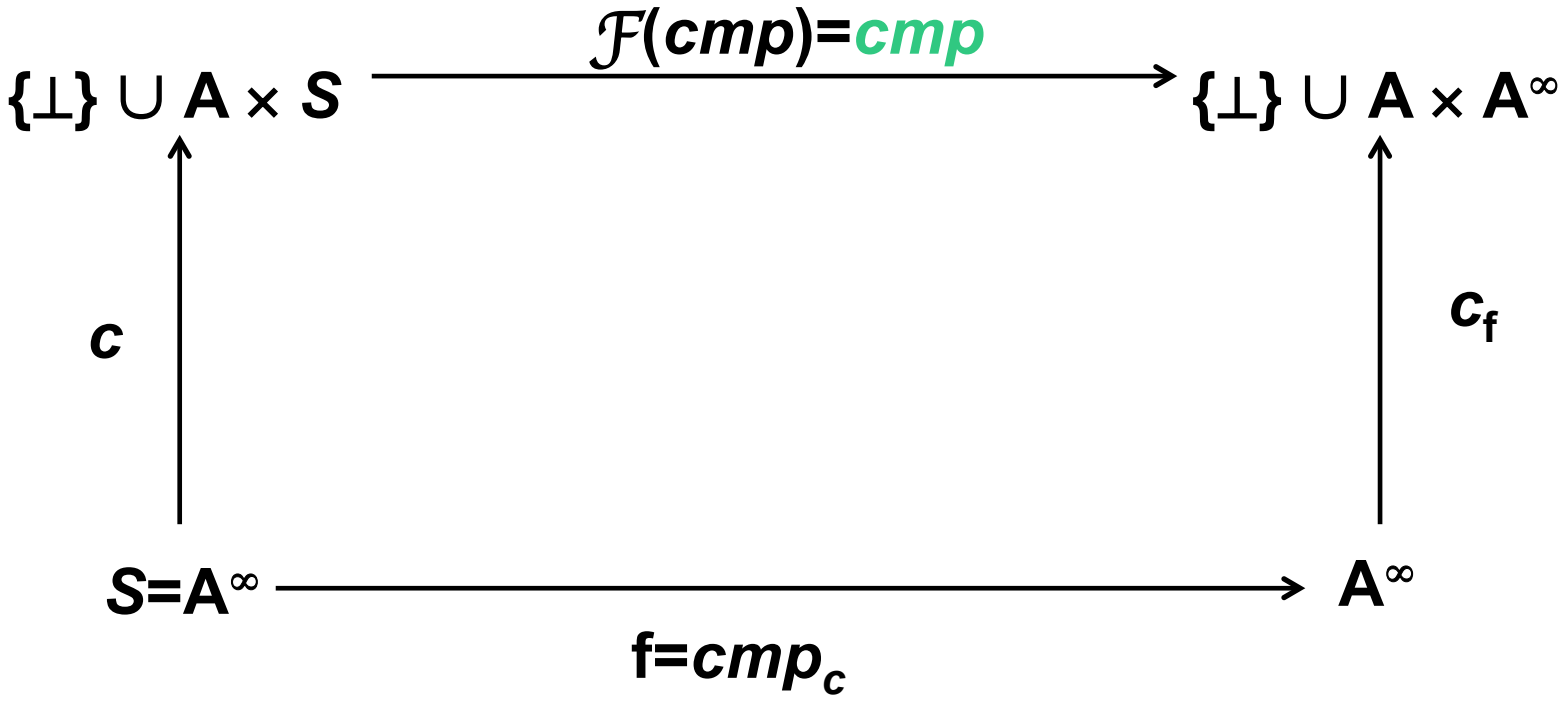
cmp_c(u)= fedededede...
cmp_c (v)= edededede...
cmp_c (w)= dedededede...
cmp_c (x)= edededede...
cmp_c (y)= f
cmp_c (z)= cmp_c (t)= ε

c(u)=(f,v) $c_f(cmp_c(u))$=(f,ededed...)=(f, cmp_c(v))
c(v)=(e,w) $c_f(cmp_c(v))$=(e,deded...)=(e, cmp_c(w))
c(w)=(d,x) $c_f(cmp_c(w))$=(d,eded...)=(d, cmp_c(x))

Définition coinductive

Définition sur les observateurs (sur la fonction de transition)

Définition de f: $A^\infty \longrightarrow A^\infty$



On définit f en définissant *c*

Illustration du principe de coinduction 1/3

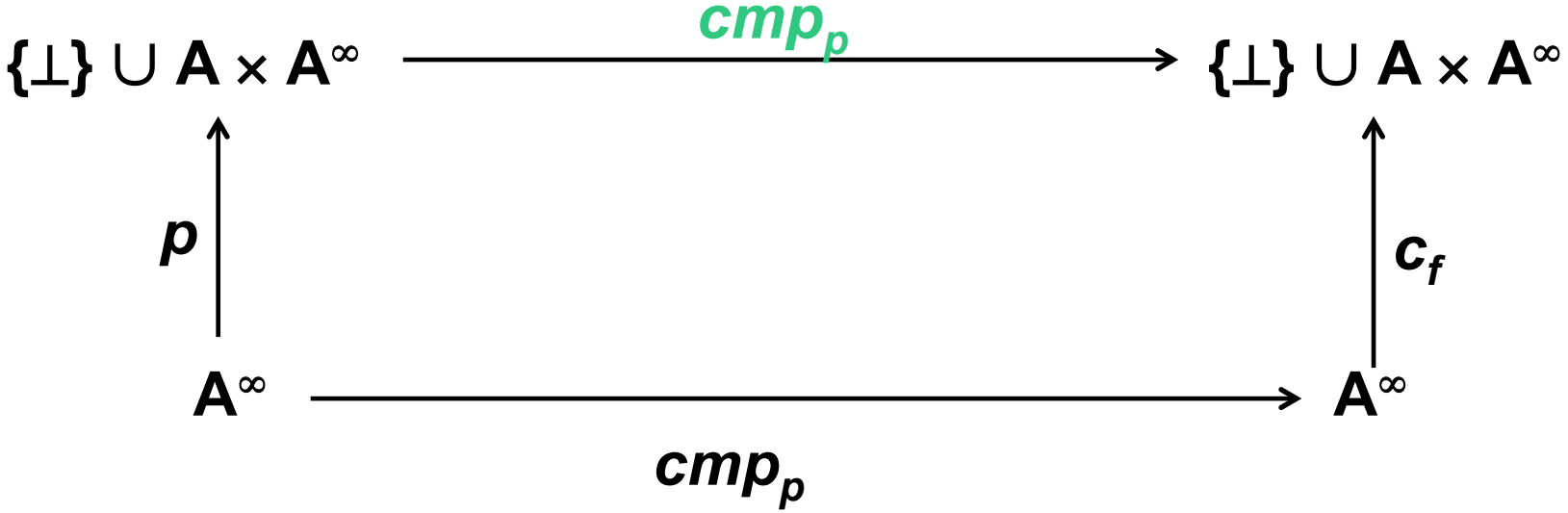
On veut définir l'observation des symboles qui ont une occurrence paire

$\sigma=\sigma_o\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5....$ σ_o σ_2 σ_4 σ_6

***p*: $A^\infty \longrightarrow \{\perp\} \cup A \times A^\infty$ défini par**

$$p(\sigma)= \begin{cases} \perp & \text{si } \sigma=\varepsilon \\ (a,\varepsilon) & \text{si } \sigma=a \\ (a, \sigma'') & \text{si } \sigma= ab\sigma'' \end{cases}$$

Illustration du principe de coinduction 2/3



$p(\sigma_o\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5...) = (\sigma_o, \sigma_2\sigma_3\sigma_4\sigma_5...)$

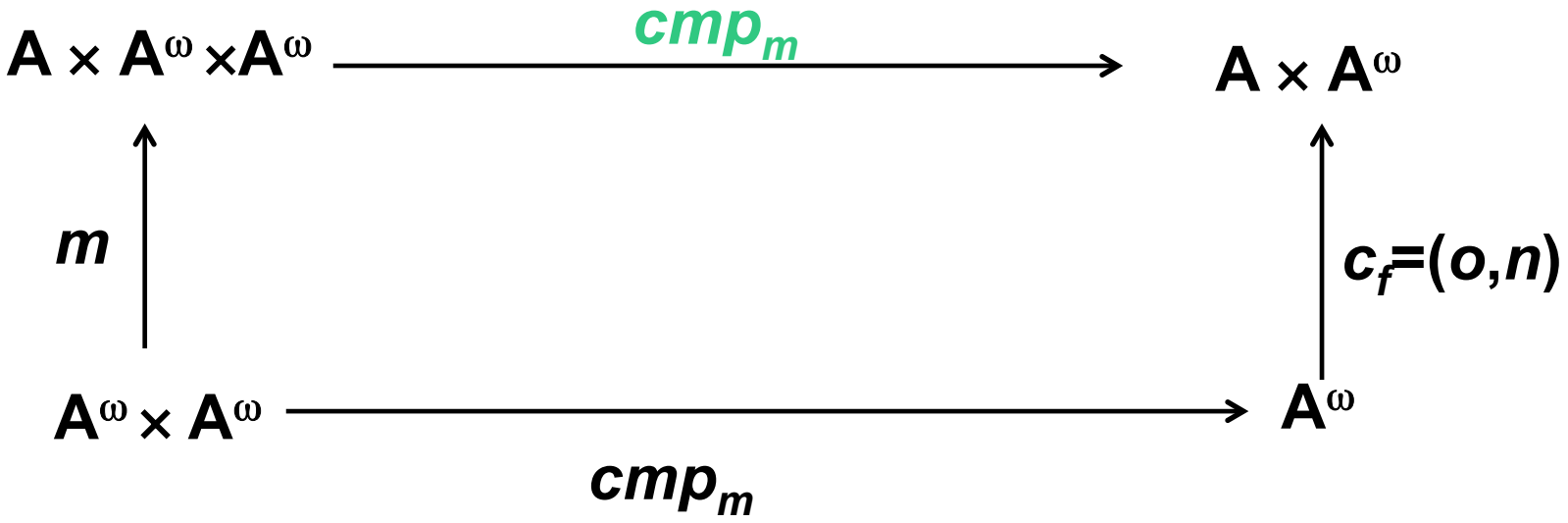
$cmp_p\ (\sigma_o\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5...) = \sigma_o\sigma_2\sigma_4\sigma_6.$

Vérification que le diagramme commute

$c_f\ (\ cmp_p\ (\sigma_o\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5...)) = c_f\ (\ \sigma_o\sigma_2\sigma_4\sigma_6\ ) = (\sigma_o, \sigma_2\sigma_4\sigma_6...)$

$cmp_p\ (p(\sigma_o\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5...)) = cmp_p\ ((\sigma_o, \sigma_2\sigma_3\sigma_4\sigma_5...\ )) = (\sigma_o, \sigma_2\sigma_4\sigma_6...)$

Illustration du principe de coinduction 3/3



$m(\sigma, \sigma') = (o(\sigma), \sigma', n(\sigma))$

$cmp_m(\alpha_o\alpha_1\alpha_2\alpha_3\ldots, \beta_o\beta_1\beta_2\beta_3\ldots) = \alpha_o\beta_o\alpha_1\beta_1\alpha_2\beta_2\ldots$

cmp_m est la fonction merge

Propriétés des coalgèbres finales 1/3

Propriétés:

Une coalgèbre finale est définie à un isomorphisme près
Une coalgèbre finale est un isomorphisme

Corollaire:

Il existe des foncteurs sans coalgèbre finale dans la catégorie des coalgèbres sur les ensembles

Exemple:

$\mathcal{F}(X) = \mathcal{P}(X)$
Changement d'état non déterministe, non déterminisme non-borné

Supélec

Propriétés des coalgèbres finales 2/3

Foncteurs polynomiaux:

Construits de manière « raisonnable » à partir de l'identité et des constantes,
fermée par produit, coproduit, exponentiation F^A

Foncteurs polynomiaux (finis) de Kripke:

Passage aux parties (finies), aux suites finies.

Théorème:

Tout foncteur polynomial fini de Kripke
a une coalgèbre finale

Propriétés des coalgèbres finales 3/3

Plus généralement, on a

Définition :Un foncteur $\mathcal{F}$ est **borné** si $\exists$ un cardinal κ tel que toute coalgèbre $\mathcal{A}$ pour F et tout a $\in \mathcal{A}$, on peut trouver une sous coalgèbre $\mathcal{U}_a$ avec a $\in \mathcal{U}_a$ et $|\mathcal{U}_a| < \kappa$

Théorème: Si $\mathcal{F}$ est borné, alors $\mathcal{F}$ a une coalgèbre final

Remarque: La coalgèbre finale n'a pas forcément de carrier dans la catégorie `Set`

Supélec

Conclusion

Spécification:

Obtenir les états: aspects algébriques

Observer les états: aspects coalgébriques

Nombreux résultats mathématiques

Logique temporelle pour $\mathcal{F}$: {⊥} +(A ×id)

Supélec

Bibliographie

Introduction to coalgebra:
Towards Mathematics of States and Observations
B. Jacobs 2005

A Tutorial on (Co)algebra and (Co)Induction
B. Jacobs J.Rutten 1997

Coalgebras and Modal Logic
A. Kurz

Defining a Formal Coalgebraic Semantics for The Rosetta Specification Language
C.Kong, C. Menon, P. Alexander 2003

Annexes 1: Citation de Turing

The Imitation Game
I propose to consider the question, 'Can machines think?' This should begin with definitions of the meaning of the term 'machine 'and 'think'.

The definitions might be framed so as to reflect so far as possible the normal use of the words, but this attitude is dangerous.

If the meaning of the words 'machine' and 'think 'are to be found by examining how they are commonly used it is difficult to escape the conclusion that the meaning and the answer to the question, 'Can machines think?' is to be sought in a statistical survey such as a Gallup poll. But this is absurd. Instead of attempting such a definition I shall replace the question by another, which is closely related to it and is expressed in relatively unambiguous words.

The new form of the problem can be described' in terms of a game which we call the 'imitation game'. It is played with three people, a man (A), a woman (B), and an interrogator (C) who may be of either sex. The interrogator stays in a room apart from the other two. The object of the game for the interrogator is to determine which of the other two is the man and which is the woman....

We now ask the question, 'What will happen when a machine takes the part of A in this game?' Will the interrogator decide wrongly as often when the game is played like this as he does when the game is played between a man and a woman?

These questions replace our original, 'Can machines think?'

Alan Turing 1950: Computing Machinery and Intelligence

Annexe 2 Exemples de signatures

$\mathcal{F}(X) = (A \times X) \cup \{\perp\}$ $\mathcal{F} : (A \times \mathtt{id}) + \{\perp\}$ **Observation du changement d'état, arrêt**

$\mathcal{F}(X) = \{0,1\} \times X^A$ $\mathcal{F} : \{0,1\} \times \mathtt{id}^A$ **Automate**

$\mathcal{F}(X) = (X \times O)^A$ $\mathcal{F} : (\mathtt{id} \times O)^A$ **Automate avec sortie**

$\mathcal{F}(X) = \mathcal{P}(A \times X)$ $\mathcal{F} : \mathcal{P}(A \times \mathtt{id})$ **Système de transitions étiquetées**