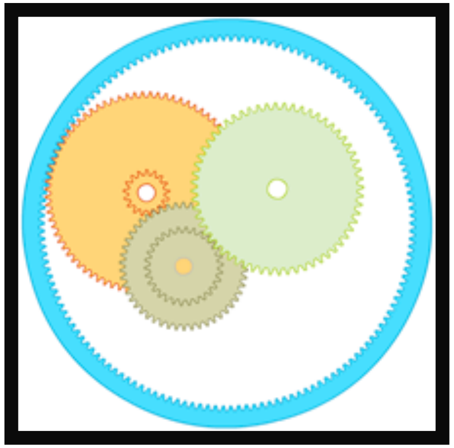
Coalgèbres et Observations

G. Vidal-Naquet

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

Approche Algébrique

SYSTÈME



Objet d'étude:
le mécanisme

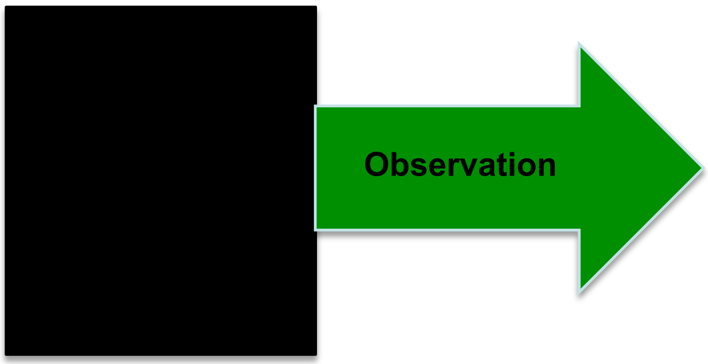
Construction d'un état

Mécanisme « typique » décrit par
Algèbre initiale

(Un des) Aspect étudié Congruence:
A partir de deux états équivalents
deux états équivalents sont obtenus

Approche CoAlgébrique

SYSTÈME



Objet d’étude: l’observation

Utilisation de l'observation

Observation « typique » décrite par CoAlgèbre finale

(Un des) Aspect étudié Bisimilarité:
A partir de deux états équivalents
deux observations équivalentes sont faites

Motivations et limites de l'exposé

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

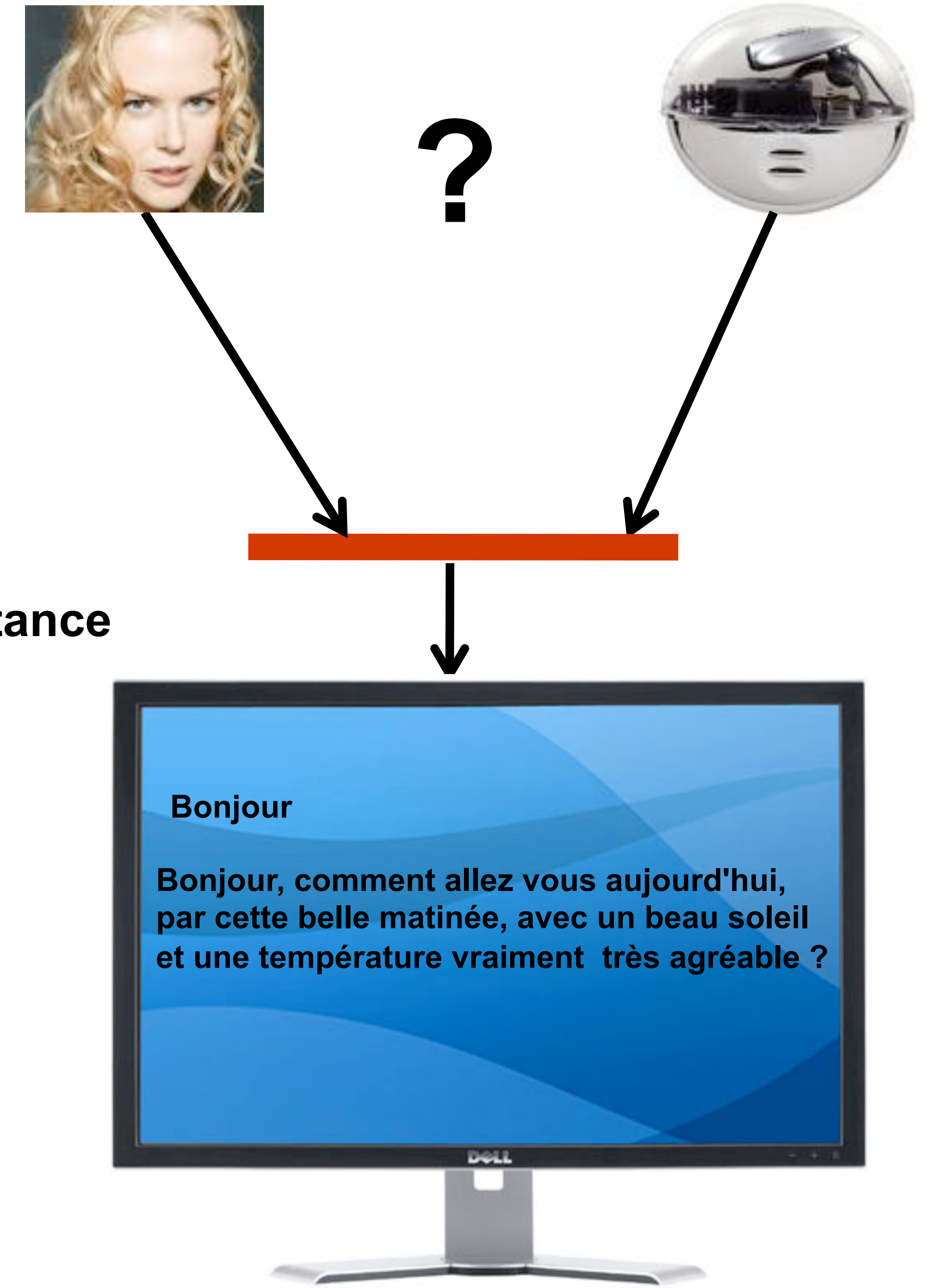
Niveau d'abstraction adéquat:
Possibilités d'expression des systèmes.
Possibilités d'expression de propriétés et d'analyse

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

Base sémantique de systèmes de composants (Rosetta…)

Sont fondées par la théorie des catégories

Ne date pas d'hier: Le test de Turing



Première mention de l'importance de l'observation :

Computing machinery and intelligence

1950 A. Turing

Construction d'objets

Constructeurs

Example: **Listes**

$$\left.\begin{array}{l}\texttt{nil}\\ \texttt{cons}\end{array}\right\}\ \text{Constructeurs}$$

Pour une machine constructions du type
$F(X) \rightarrow X$
Le nouvel état est calculé à partir de l'ancien

Démonstration de propriété $\mathcal{P}$ par induction,
$\mathcal{P}(\texttt{nil})$,
$\mathcal{P}(\texttt{cons(l,e)})$

Algèbres Initiales

$$\text{Algèbre Initiale} \xrightarrow[\text{unique}]{\text{Homomorphisme}} \text{Algèbre arbitraire}$$

Induction: Utilisation du caractère initial

Utilisation des Coalgèbres

Observation d'objets

```
estvide
longueur
head
tail
```

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

$X \rightarrow F(X)$

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`

$\Big\}$ **Constructeurs**

`estvide`
`longueur`
`head`
`tail`

$\Bigg\}$ **Observateurs (destructeurs)**

Coalgèbres finales

$$\text{Coalgèbre finale} \xleftarrow{\text{Homomorphisme unique}} \text{Coalgèbre arbitraire}$$

Co-induction: Utilisation du caractère final

Présentation intuitive

Définition d'une coalgèbre

S espace des états

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

$c : S \longrightarrow \boxed{\ldots\ S\ \ldots}$

$\boxed{\ldots\quad (\text{-})\quad \ldots}$ Signature de la co-algèbre

A partir de *S* on peut obtenir des informations par *c*

Formellement

$\mathcal{F}$ foncteur de `Sets` dans `Sets`

$\mathcal{F}$ foncteur de signature

foncteur opérateur sur les ensembles et les fonctions,
préserve l'identité et la composition

Coalgèbre de $\mathcal{F}$

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

S:ensemble des états (base, carrier)

c: fonction d'observation

Remarques:

Études pour $\mathcal{F}$ foncteur dans des catégories plus générales que les ensembles
S peut être un ensemble quelconque (discret ou pas),
c peut être une observation "pure" ou indiquer également le type d'évolution

Exemples

$c{:}S \rightarrow A$ Signature $\mathcal{F} : A$	Observation sur un état
$c{:}S \rightarrow \{\perp\} \cup S$ $\mathcal{F} : \{\perp\} + \mathtt{id}$	Changement d'état, arrêt
$c{:}S \rightarrow \mathcal{P}(S)$ $\mathcal{F} : \mathcal{P}(\mathtt{id})$	Changement d'état non déterministe
$c{:}S \rightarrow A \times (\{\perp\} \cup S)$ $\mathcal{F} : A \times (\{\perp\} + \mathtt{id})$	Changement d'état avec observation,arrêt
$c{:}S \rightarrow \{0,1\} \times S^A$ $\mathcal{F} : \{0,1\} \times \mathtt{id}^A$	Automate
$c{:}S \rightarrow (S \times O)^A$ $\mathcal{F} : (\mathtt{id} \times O)^A$	Automate avec sortie
$c{:}S \rightarrow \mathcal{P}(A \times S)$ $\mathcal{F} : \mathcal{P}(A \times \mathtt{id})$	Système de transitions étiquetées

Exemple: observation

$c:S \longrightarrow A = \mathcal{F}(S)$

Signature $\mathcal{F}$: A={j,v,r}

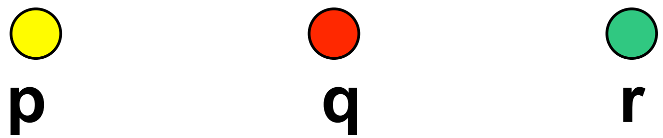
S= {u,t,w,x,y,z} c(u)=j, c(t)=r, c(w)= j, c(x)=r, c(y)=v, c(z)=v.

Représentation graphique

Autre coalgèbre de même signature

$c':S' \longrightarrow A = \mathcal{F}(S')$

S'= {p,q,r} c'(p)=n, c'(q)=r, c'(r)= b.



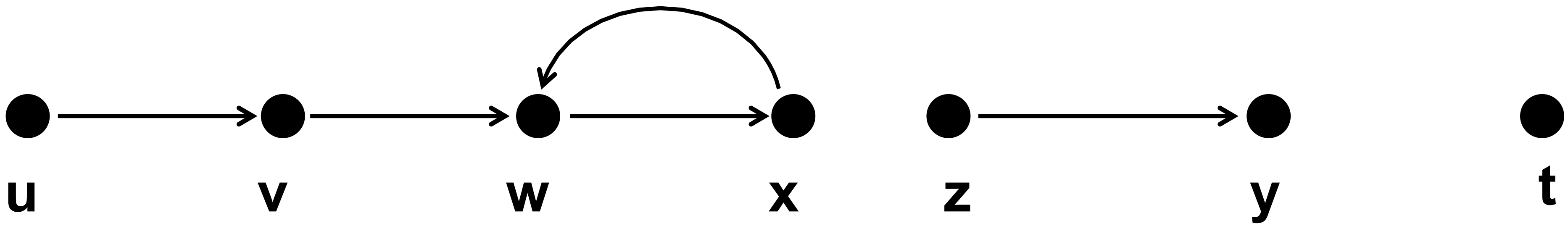
Exemple usuel: Feux de croisement

Exemples: changement d'état

$c : S \longrightarrow \{\perp\} \cup S$ **Signature $\mathcal{F}$:{⊥} + `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)=⊥.**

Représentation graphique



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

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

c(s) peut être l'état précédent, état initial si c(s)= ⊥

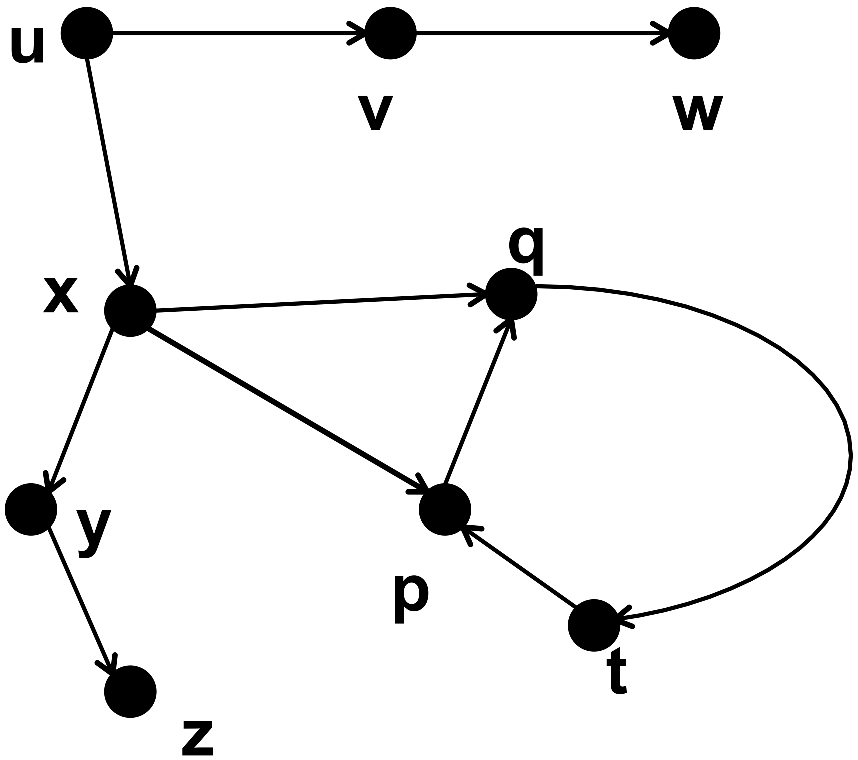
Exemples: changement d'état non déterministe

$c : S \longrightarrow \mathcal{P}(S)$

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

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



Exemple: changement et observation

$c: S \longrightarrow (\{\perp\} \cup S) \times A$ Signature $\mathcal{F}: (\{\perp\} + \mathtt{id}) \times A$

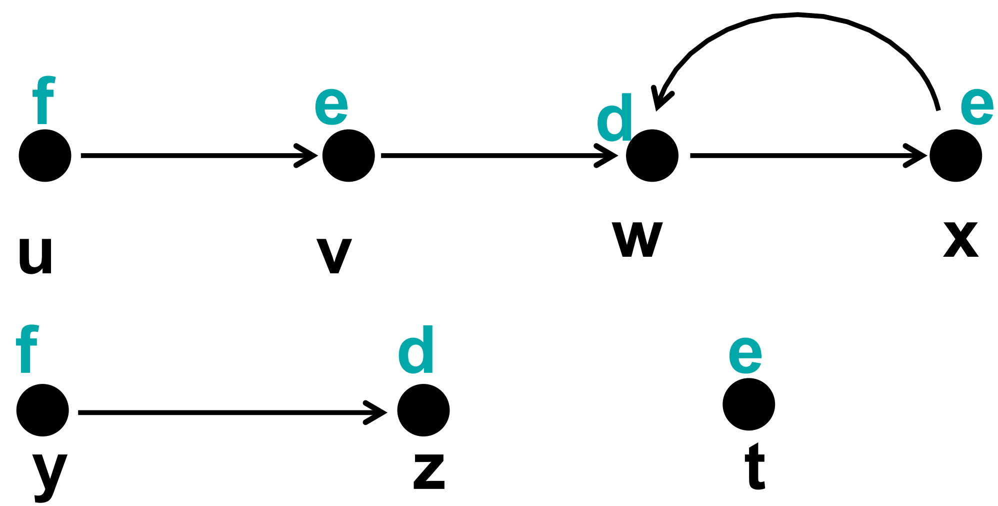
$S = \{u,v,w,x,y,z,t\}$ $A = \{d,e,f\}$

$c(u) = (f,v)$,
$c(v) = (e,w)$,
$c(w) = (d,x)$,
$c(x) = (e,w)$,
$c(y) = (f,z)$,
$c(z) = (d, \perp)$,
$c(t) = (e, \perp)$

$c = (o,n)$

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

Représentation graphique



Détour:Application d'un foncteur à une fonction

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

Manière canonique d'obtenir $\mathcal{F}$(f)

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

$\mathcal{F}$(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 $\mathcal{F}$

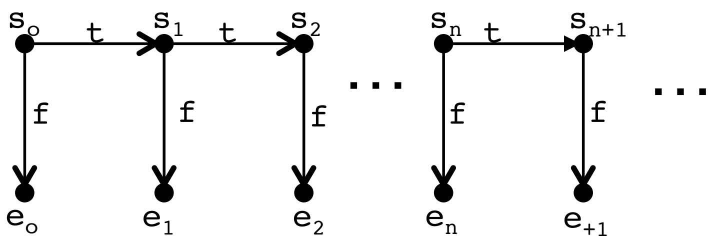
$h: S \longrightarrow T$ est un **homomorphisme de coalgèbre** quand $d \circ h = \mathcal{F}(h) \circ c$

c.a.d que le diagramme suivant commute

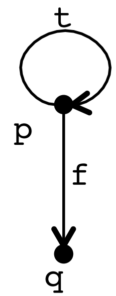
$(\mathcal{F}(h))(c(s)) = d(h(s))$

$$\begin{tikzcd}
c(s) & & & \\
\mathcal{F}(S) \arrow[rr, "\mathcal{F}(h)"] & & \mathcal{F}(T) & d(h(s)) \\
S \arrow[u, "c"] \arrow[rr, "h"'] & & T \arrow[u, "d"'] & \\
s & & & h(s)
\end{tikzcd}$$

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:

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

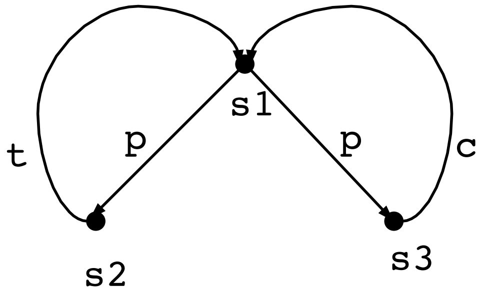
$h(s_i)=p \quad d(h(s_i))=d(p)=\{(t,p),(f,q)\}$

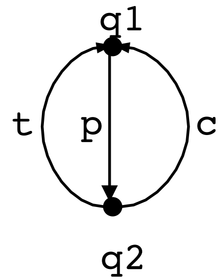
$$\begin{tikzcd} \mathcal{F}(S) \arrow[r, "\mathcal{F}(h)"] & \mathcal{F}(T) \\ S \arrow[u, "c"] \arrow[r, "h"] & T \arrow[u, "d"'] \end{tikzcd}$$

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

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

$\mathcal{F}$: $\mathcal{P}$(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$_1$)}

$\neq$

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

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

qui est un homomorphisme

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

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

$$\begin{tikzcd} \mathcal{F}(S) \arrow[r, "\mathcal{F}(beh) = beh"] & \mathcal{F}(S_f) \\ S \arrow[u, "c"] \arrow[r, "beh"] & S_f \arrow[u, "c_f"'] \end{tikzcd}$$

Exemple: Coalgèbre finale pour l'observation

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

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

$c\!:S \longrightarrow A$

$$\begin{tikzcd} \mathcal{F}(S)=A \arrow[r, "\mathcal{F}(beh)"] & \mathcal{F}(A)= A \\ S \arrow[u, "c"] \arrow[r, "beh=c"'] & A \arrow[u, "id"'] \end{tikzcd}$$

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.

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

Exemple:Coalgèbre finale pour le changement d'état

$$c: S \longrightarrow \mathcal{F}(S) = \{\perp\} \cup S$$

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

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

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

$$\begin{tikzcd}
u \arrow[r] & v \arrow[r] & w \arrow[r] & x \arrow[l, bend right] & z \arrow[r] & y \arrow[r] & t
\end{tikzcd}$$

$beh(u) = beh(v) = beh(w) = beh(x) = \omega$
$beh(z) = 2,\ beh(y) = 1$
$beh(t) = 0$

$$\begin{tikzcd}
\mathcal{F}(S) \arrow[r, "beh"] & \mathcal{F}(S_f) \\
S \arrow[u, "c"] \arrow[r, "beh"] & S_f \arrow[u, "c_f"']
\end{tikzcd}$$

Vérification que *beh* est un morphisme

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

$c_f(beh(z)) = c_f(2) = beh(c(z)) = beh(y) = 1$

Exemple:Coalgèbre finale pour les changements ND avec observation

$c{:}S \longrightarrow A \times \mathcal{P}_{\text{fin}}(S)$ **Signature:** $A \times \mathcal{P}_{\text{fin}}(\mathtt{id})$

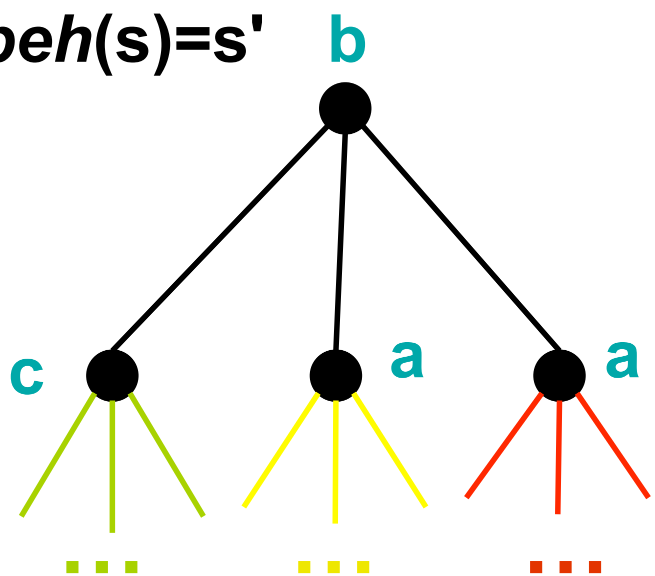
$A=\{a,b,c\}$

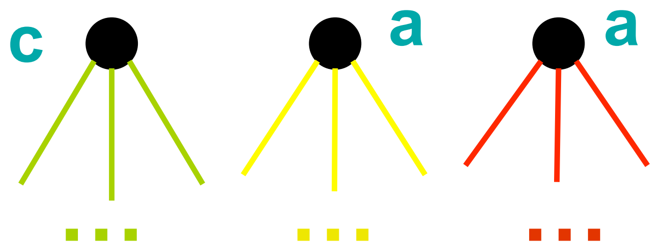
$c(s) = (b,\{s_1,s_2, s_3\})$ $c = (o,n)$ $o: S \longrightarrow A$,$n: S \longrightarrow \mathcal{P}_{\text{fin}}(S)$

$o(s_1) = c$, $o(s_2) = a$, $o(s_3) = a$

S_f: ensemble des arbres de degré fini, sommets étiquetés par A,identification des sous-arbres « identiques »

$beh(s)=s'$



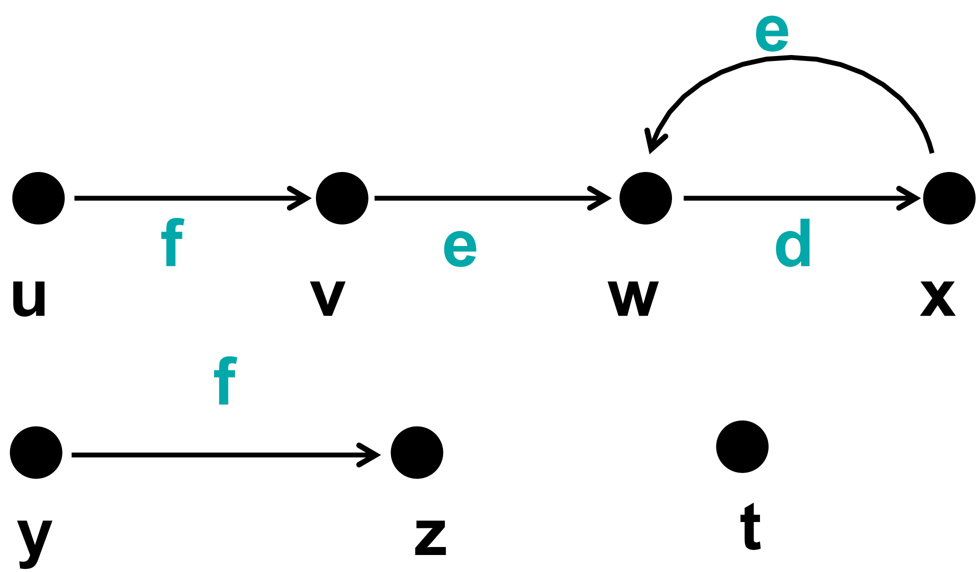
$c_f(s')=(b,$ $\{$  $\})$

Coalgèbre finale pour le foncteur $\mathcal{F}_o$: $\{\perp\} + (A \times \mathtt{id})$?

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

Coalgèbre finale pour les changements avec observation 3/5

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

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

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

$c_f(\varepsilon) = \perp$

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

L'itération de c_f **fournit tous les éléments observables**

Remarque: c_f **est un isomorphisme**

Proposition:

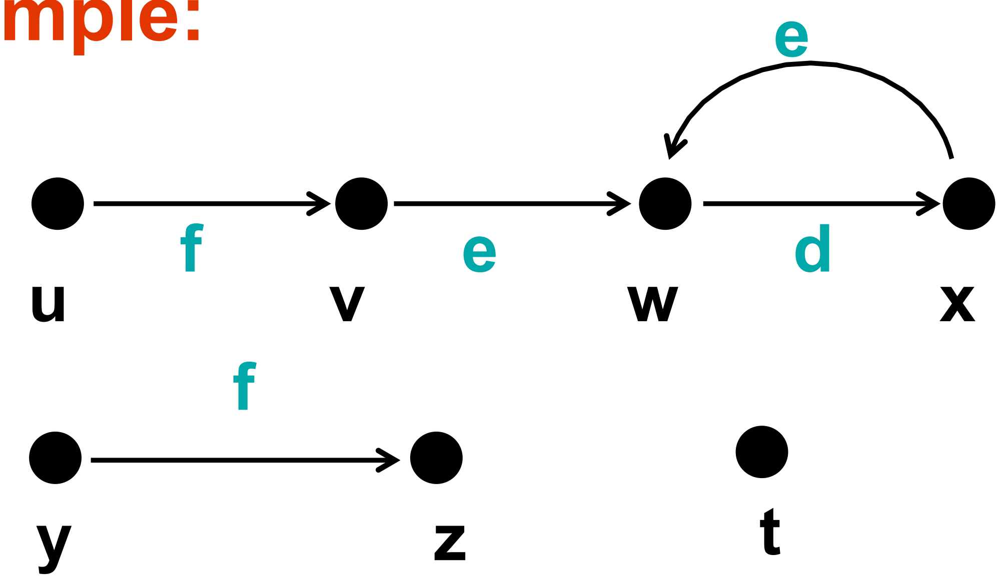
La coalgèbre c_f: $A^\infty \longrightarrow \{\perp\} \cup A \times A^\infty$ est finale pour $\mathcal{F}_o$.

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

- **Si $c(x) = \perp$ alors $c_f(\, beh(x)\,) = \perp$**
- **Si $c(x) = (a,x')$ alors $c_f(\, beh(x)\,) = (a,\, beh(x')\,)$**

Coalgèbre finale pour les changements avec observation 5/5

Exemple:



beh_c(u)= fededededede...

beh_c(v)= edededede...

beh_c(w)= dededede...

beh_c(x)= edededede...

beh_c(y)= f

beh_c(z)= beh_c(t)= ε

c(u)=(f,v) c_f(beh_c(u))=(f,ededed...)=(f, beh_c(v))

c(v)=(e,w) c_f(beh_c(v))=(e,deded...)=(e, beh_c(w))

c(w)=(d,x) c_f(beh_c(w))=(d,eded...)=(d, beh_c(x))

Définition coinductive

Définition sur les observateurs (sur la fonction de transition)

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

$$
\begin{tikzcd}
\{\perp\} \cup A \times S \arrow[rr, "\mathcal{F}(beh_c)=beh_c"] & & \{\perp\} \cup A \times A^\infty \\
S=A^\infty \arrow[u, "c"] \arrow[rr, "f=beh_c"'] & & A^\infty \arrow[u, "c_f"']
\end{tikzcd}
$$

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

$\sigma = \sigma_o \sigma_1 \sigma_2 \sigma_3 \sigma_4 \sigma_5 \ldots. \quad \sigma_o \quad \sigma_2 \quad \sigma_4 \quad \sigma_6$

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

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

Illustration du principe de coinduction 2/3

$$
\begin{tikzcd}
\{\perp\} \cup A \times A^{\infty} \arrow[rr, "beh_p"] & & \{\perp\} \cup A \times A^{\infty} \\
A^{\infty} \arrow[u, "p"] \arrow[rr, "beh_p"'] & & A^{\infty} \arrow[u, "c_f"']
\end{tikzcd}
$$

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

$beh_p\,(\sigma_o\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\ldots) = \sigma_o\sigma_2\sigma_4\sigma_6.$

Vérification que le diagramme commute

$c_f\,(\,beh_p\,(\sigma_o\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\ldots)) = c_f\,(\,\sigma_o\sigma_2\sigma_4\sigma_6\,) = (\sigma_o, \sigma_2\sigma_4\sigma_6\ldots)$

$beh_p\,(p(\sigma_o\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\ldots)) = beh_p\,((\sigma_o, \sigma_2\sigma_3\sigma_4\sigma_5\ldots\,)) = (\sigma_o, \sigma_2\sigma_4\sigma_6\ldots)$

Illustration du principe de coinduction 3/3

$$\begin{tikzcd}
A \times A^\omega \times A^\omega \arrow[r, "beh_m"] & A \times A^\omega \\
A^\omega \times A^\omega \arrow[u, "m"] \arrow[r, "beh_m"'] & A^\omega \arrow[u, "c_f=(o,n)"']
\end{tikzcd}$$

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

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

beh_m est la fonction merge

Propriétés des coalgèbres finales 1/3

Propriétés:

Une coalgèbre finale est définie à un isomorphisme près

Une coalgèbre finale définit un isomorphisme

Corollaire:

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

Exemple:

$S \longrightarrow \mathcal{P}(S)$

Changement d'état non déterministe, non déterminisme non-borné

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 avec un ensemble donné.

Foncteurs polynomiaux (finis) de Kripke:
Passage aux parties (finies), aux suites finies.

Théorème:

Tout foncteur polynomial fini de Kripke
a une coalgèbre finale dans la catégorie des ensembles

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 $\mathcal{F}$ 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 finale

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

Définition:

Soit $\mathcal{F}$ un foncteur, 2 coalgèbres de $\mathcal{F}$ c:$S \longrightarrow \mathcal{F}(S)$, d:$T \longrightarrow \mathcal{F}(T)$
Une relation $R \subseteq S \times T$ est une bisimulation ssi
$\exists$ une coalgèbre g:R $\longrightarrow \mathcal{F}(R)$ telle que les deux morphismes de projection π_1:R$\longrightarrow S$ et π_2:R$\longrightarrow T$
soient des morphismes de coalgèbres, c.a.d. que le diagramme suivant commute

$$\begin{tikzcd}
\mathcal{F}(S) & \mathcal{F}(R) \arrow[l, "\mathcal{F}(\pi_1)"'] \arrow[r, "\mathcal{F}(\pi_2)"] & \mathcal{F}(T) \\
S \arrow[u, "c"] & R \arrow[l, "\pi_1"] \arrow[r, "\pi_2"'] \arrow[u, "g"] & T \arrow[u, "d"]
\end{tikzcd}$$

Remarque:

Première définition de la bisimulation (Aczel,Mendler 1989)

Lifting d'une relation

A partir de $\quad$ ***R*** **relation entre** ***S*** **et** ***T***

$\mathcal{F}$ **foncteur polynomial de Kripke**

On déduit de manière canonique

R' **relation entre** $\mathcal{F}(S)$ **et** $\mathcal{F}(T)$

$$R \subseteq S \times T \quad \Rightarrow \quad R' \subseteq \mathcal{F}(S) \times \mathcal{F}(T)$$

Lifting d'une relation *R* pour $\mathcal{F}$ **:** $R' = \mathrm{Rel}(\mathcal{F})(R)$

Intuitivement:

élément de $\mathcal{F}(S)$ **défini par** $\exp(s_1 \ldots s_n)$

$\exp(s_1 \ldots s_n)\ \mathrm{Rel}(\mathcal{F})(R)\ \exp(t_1 \ldots t_n)$

ssi

$s_1\, R\, t_1, \ldots, s_n\, R\, t_n$

Règles pour le lifting d'une relation

1) $\mathcal{F}$: id $\Rightarrow$ Rel($\mathcal{F}$)(R)=R

2) $\mathcal{F}$: S $\longrightarrow$ A $\Rightarrow$ Rel($\mathcal{F}$)(R)={(a,a)/a$\in$A}

3) $\mathcal{F} = \mathcal{G}\times\mathcal{H} \Rightarrow$ Rel($\mathcal{F}$)(R)={((u,v),(x,y))/ (u,x) $\in$ Rel($\mathcal{G}$)(R),
(v,y) $\in$ Rel($\mathcal{H}$)(R)}

analogue pour le coproduit

4) $\mathcal{F} = \mathcal{G}^A \Rightarrow$ Rel($\mathcal{F}$)(R)={(f,g) / $\forall$a$\in$A f(a) Rel($\mathcal{G}$)(R) g(a)}

5) $\mathcal{F} = \mathcal{P}_{(fin)}\mathcal{G} \Rightarrow$ Rel($\mathcal{F}$)(R)= {(U,V) /$\forall$u$\in$U $\exists$v$\in$V u Rel($\mathcal{G}$)(R) v
$\wedge$
$\forall$v$\in$Y $\exists$u$\in$U u Rel($\mathcal{G}$)(R) v}

6) $\mathcal{F} = \mathcal{G}^* \Rightarrow$ Rel($\mathcal{F}$)(R)={($u_1\ldots u_n$,$v_1\ldots v_n$) / $\forall$i$\leq$n u_i) Rel($\mathcal{G}$)(R) v_i}

Exemple: $\mathcal{F}(S)$= A$\times$*S* R $\subseteq$ S $\times$ T xRy $\Rightarrow$(a,x)R'(a,y)

Caractérisation pour les foncteurs polynomiaux

Propriété (Rutten, Jacob):

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

Une relation $R \subseteq S \times T$ est une bisimulation ssi
$\forall x \in S, \forall y \in T, xRy \Rightarrow c(x)\ Rel(\mathcal{F})(R)\ d(y)$

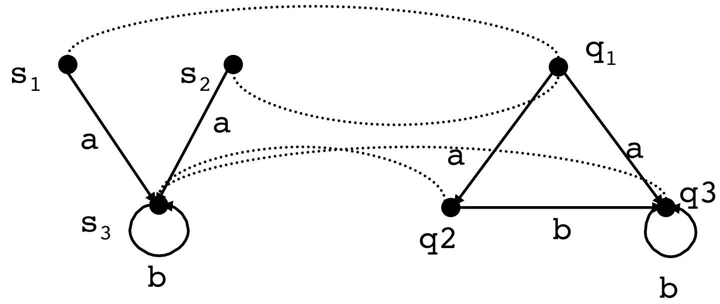
Si $R = T$, $c = d$ et R est une équivalence, on parle d'équivalence de bisimulation

Exemple de bisimulation

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

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

$c(s_1)=\{(a, s_3)\}$
$c(s_2)=\{(a, s_3)\}$
$c(s_3)=\{(b, s_3)\}$



$T=\{q_1, q_2, q_3\}$

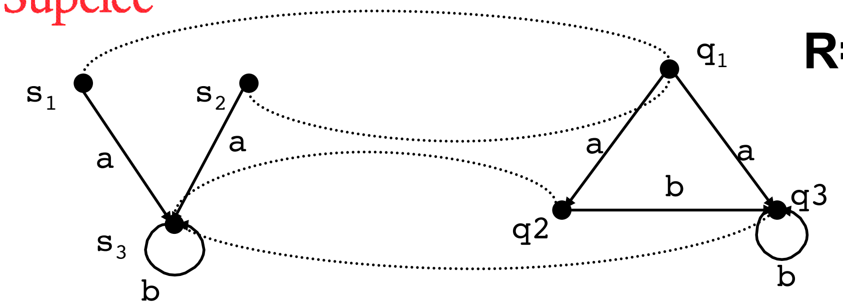
$c'(q_1)=\{(a, q_2), (a, q_3)\}$
$c'(q_2)=\{(b, q_3)\}$
$c'(q_3)=\{(b, q_3)\}$

$R=\{(s_1,q_1), (s_2,q_1), (s_3,q_2), \{(s_3,q_3)\}$

notation: e Rel(F)(R)$f \Leftrightarrow (e, f) \in$ Rel(F)(R)

Rel(F)(R)=
{
$(\{(a,s_1)\}, \{(a, q_1)\})$, $(\{(b,s_1)\}, \{(b, q_1)\})$, $(\{(a,s_1), (b,s_2)\}, \{(a, q_1),(b, q_1)\})$,
$(\{(a,s_3)\}, \{(a, q_2), (a, q_3)\})$
,
$(\{(b,s_3)\},\{(b,q_3)\})$...
}
$s_1Rq_1 \Rightarrow c(s_1)=\{(a, s_3)\}$ Rel(F)(R) $\{(a, q_2), (a, q_3)\} = c'(q_1)$

Caractérisation par projection



$R=\{(s_1,q_1), (s_2,q_1), (s_3,q_2), (s_3,q_3)\}$

$$
\begin{tikzcd}
\mathcal{F}(S) & & \mathcal{F}(R) \arrow[ll, "\mathcal{F}(\pi_1)"'] \arrow[rr, "\mathcal{F}(\pi_2)"'] & & \mathcal{F}(T) \\
S \arrow[u, "c"'] & & R \arrow[u, "g"'] \arrow[ll, "\pi_1"] \arrow[rr, "\pi_2"] & & T \arrow[u, "d"']
\end{tikzcd}
$$

$g((s_1,q_1))=\{ (a, (s_3,q_2)), (a, (s_3,q_3)) \}$

$g((s_2,q_1))=\{ (a, (s_3,q_2)), (a, (s_3,q_3)) \}$

$g((s_3,q_2))=\{ (b, (s_3,q_3)) \}$

$g((s_3,q_3))=\{ (b, (s_3,q_3)) \}$

$\pi_1(s_1,q_1) = s_1$

$c(\pi_1(s_1,q_1)) = c(s_1)=\{(a,s_3)\}$

$g((s_1,q_1)) = \{(a, (s_3 , q_2)),(a, (s_3 , q_3))\}$

$\mathcal{F}(\pi_1)(g((s_1,q_1))) = \{(a,s_3)\}$

Exemples de résultats sur les bisimulations

La catégorie des bisimulations est close par

- inverse
- composition
- union
- image d'un homorphisme
- image inverse d'un homomorphisme

Théorème (Rutten):

Soit deux coalgèbres de même signature

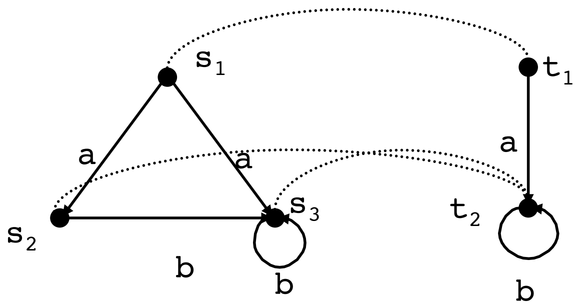
c:$S \longrightarrow \mathcal{F}(S)$**, d:**$T \longrightarrow \mathcal{F}(T)$

une application f de S dans T est un morphisme de coalgèbre

si et seulement si

son graphe est une relation de bisimulation

Application du théorème de Ruttten



S = {s_1 ,s_2 ,s_3)

T = {t_1, t_2)

$c(s_1) = \{(a, s_2) ,(a, s_3)\}$
$c(s_2) = \{(b, s_3)\}$
$c(s_3) = \{(b, s_3)\}$

$d(t_1) = \{(a, t_2)\}$
$d(t_2) = \{(b, t_2)\}$

$m(s_1)= t_1$, $m(s_2) = m(s_3) = t_2$

$\mathcal{F}(m)(c(s_1)) = \mathcal{F}(m)(\{(a, s_2), (a, s_3)\}) = \{(a, t_2)\}$
$d(m(s_1)) = d(t_1) = \{(a, t_2)\}$

$\mathcal{F}(m)(c(s_2)) = \mathcal{F}(m)(\{(b, s_3) \} = \{(b, t_2)\}$
$d(m(s_2)) = d(t_2) = \{(b, t_2)\}$

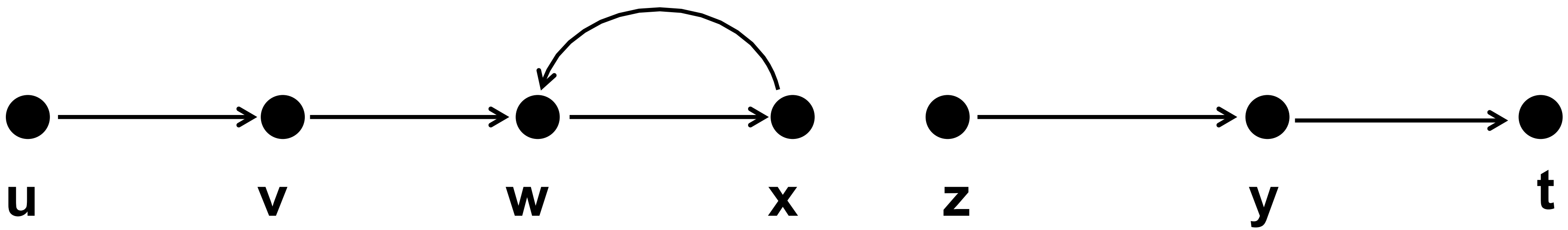
Relation de bisimilarité

Union de toutes les relations de bisimulation

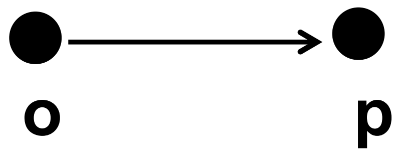
Etats bisimilaires (x,y) dans une relation de bisimulation

Même ensemble: états non distinguables par observation

Propriété: $x \approx y \Leftrightarrow beh_f(x) = beh_f(y)$



$u \approx v \approx w \approx x \approx y,\ o \approx y,\ p \approx t$



$beh_f(u) = beh_f(v) = beh_f(w) = beh_f(x) = \omega,$
$beh_f(o) = beh_f(y) = 1$

Résultat fondamental

Théorème (Gumm 99):

Soit $\mathcal{F}$ un foncteur admettant une coalgèbre finale $c_f : S_f \longrightarrow \mathcal{F}(S_f)$ pour $\mathcal{F}$.
Pour toute coalgèbre $c : S \longrightarrow \mathcal{F}(S)$ de $\mathcal{F}$

$\forall s \in S$, $\exists t \in S_f$ unique, s et t sont bisimilaires

Toute bisimulation sur la coalgèbre finale est incluse dans la relation d'égalité

Conclusion

Spécification:

Obtenir les états: aspects algébriques

Observer les états: aspects coalgébriques

Nombreux résultats mathématiques

Logique temporelle pour $\mathcal{F}$: $\{\perp\} + (A \times \mathtt{id})$

Bibliographie

Textes d'introduction (disponibles sur le web):

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 2001

Applications:

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

Components as Coalgebras: the Refinement Dimension
S. Meng, L.S. Barbosa 2004

Le test 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

Supélec