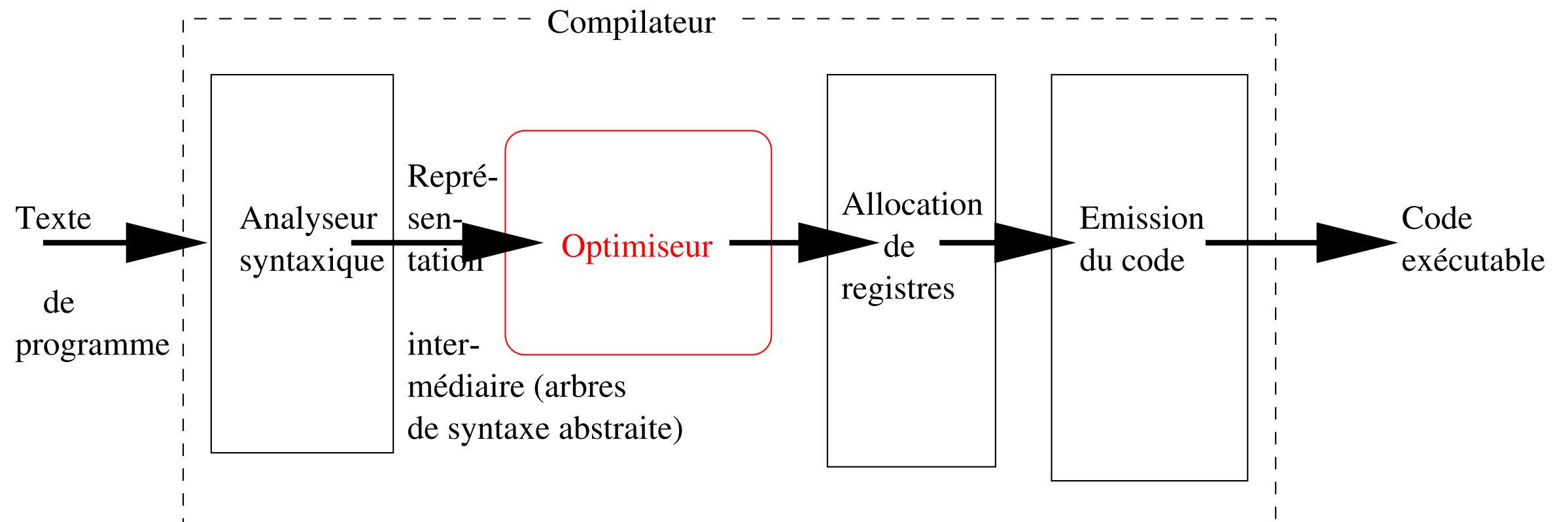


Analyse statique de programmes

Analyse statique

- But: découvrir **automatiquement** des propriétés (simples) des programmes
- Applications:
 - compilateurs optimisants (gcc, etc.)
 - preuve automatique d'absence d'erreurs à l'exécution (Polyspace, Astrée, etc.)
 - base d'autres outils (en sécurité par ex.)

Architecture d'un compilateur (pas le vôtre!)



Un exemple

```
int f (int m, int n) { int p = m+n;  return p+3; }
```

compilé par gcc 2.8.1 sans option en:

Mnémoniques assembleur	Explication
<code>movl 8(%ebp),%eax</code>	mettre m dans %eax
<code>movl 12(%ebp),%edx</code>	mettre n dans %edx
<code>leal (%edx,%eax),%ecx</code>	calculer <code>%ecx := %eax + %edx</code>
<code>movl %ecx,-4(%ebp)</code>	ranger %ecx dans p
<code>movl -4(%ebp),%edx</code>	mettre p dans %edx
<code>addl \$3,%edx</code>	ajouter 3 à %edx
<code>movl %edx,%eax</code>	retourner %edx

Un exemple

```
int f (int m, int n) { int p = m+n;  return p+3; }
```

compilé par gcc 2.8.1 sans option en:

Mnémoniques assembleur	Explication
<code>movl 8(%ebp),%eax</code>	mettre m dans %eax
<code>movl 12(%ebp),%edx</code>	mettre n dans %edx
<code>leal (%edx,%eax),%ecx</code>	calculer <code>%ecx := %eax + %edx</code>
<code>movl %ecx,-4(%ebp)</code>	ranger %ecx dans p
<code>movl -4(%ebp),%edx</code>	remplaçable par <code>movl %ecx, %edx</code>
<code>addl \$3,%edx</code>	
<code>movl %edx,%eax</code>	retourner %edx

Un exemple

```
int f (int m, int n) { int p = m+n;  return p+3; }
```

compilé par gcc 2.8.1 sans option en:

Mnémoniques assembleur	Explication
<code>movl 8(%ebp),%eax</code>	mettre m dans %eax
<code>movl 12(%ebp),%edx</code>	mettre n dans %edx
<code>leal (%edx,%eax),%ecx</code>	calculer $\%ecx := \%eax + \%edx$
<code>movl %ecx,-4(%ebp)</code>	inutile... car p ne sera jamais plus utilisée
<code>movl -4(%ebp),%edx</code>	remplaçable par <code>movl %ecx, %edx</code>
<code>addl \$3,%edx</code>	ajouter 3 à %edx
<code>movl %edx,%eax</code>	retourner %edx

Un exemple

```
int f (int m, int n) { int p = m+n;  return p+3; }
```

compilé par gcc 2.8.1 sans option en:

Mnémoniques assembleur	Explication
<code>movl 8(%ebp),%eax</code>	mettre m dans %eax
<code>movl 12(%ebp),%edx</code>	mettre n dans %edx
<code>leal (%edx,%eax),%ecx</code>	calculer $\%ecx := \%eax + \%edx$
<code>movl %ecx,-4(%ebp)</code>	inutile... car p ne sera jamais plus utilisée
<code>movl -4(%ebp),%edx</code>	remplaçable par <code>movl 8(%ebp),%edx</code>
<code>addl \$3,%edx</code>	ajouter 3 à %edx
<code>movl %edx,%eax</code>	retourner %eax

Propriété à démontrer,
automatiquement

Quelques propriétés

- *live variables*: variables définies à la ligne n qui seront possiblement utilisées plus tard
- *dead code*: code qui ne sera jamais exécuté
- *array overflow*: débordement de tableau
- *arithmetic overflow*: débordement arithmétique (cf. Ariane 5)

Le théorème de Rice

- **Thm:** toute propriété extensionnelle et non-triviale de prgms est **indécidable**.
- Extensionnelle = ne dépend que de la sémantique
- Non-triviale: fausse d'au moins 1 prgm, et vraie d'au moins 1 prgm
- (pour un langage de prog. Turing-complet.)

Exemple

- La propriété « la ligne de code #123 est-elle du code mort? » est indécidable
- (Mais... ceci n'est pas extensionnel:
comment utiliser Rice?)

Exemple

```
<P> // calcule b:bool  
if (b) {  
123: <code> // mort?  
}
```

- La propriété « la ligne de code #123 est-elle du code mort? » est indécidable
- (Mais... ceci n'est pas extensionnel: comment utiliser Rice?)

Exemple

```
⟨P⟩ // calcule b:bool
  if (b) {
123: ⟨code⟩ // mort?
  }
```

- La propriété « la ligne de code #123 est-elle du code mort? » est indécidable
- (Mais... ceci n'est pas extensionnel: comment utiliser Rice?)

Ou: par réduction à partir du problème de l'arrêt. Étant donné le code d'une machine de Turing $\langle M \rangle$, on produit:

```
b := ⟨M⟩ // b:bool
  if (b) {
123: ⟨code⟩ // mort?
  }
```

Exemple

```
<P> // calcule b:bool
  if (b) {
123: <code> // mort?
  }
```

- La propriété « la ligne de code #123 est-elle du code mort? » est indécidable
- (Mais... ceci n'est pas extensionnel: comment utiliser Rice?)
- Morale: « toute propriété intéressante de programmes est indécidable ».

Ou: par réduction à partir du problème de l'arrêt. Etant donné le code d'une machine de Turing $\langle M \rangle$, on produit:

```
b := <M> // b:bool
  if (b) {
123: <code> // mort?
  }
```

L'interprétation abstraite

- On va construire des **approximations** calculables de propriétés P de prgms:
 - Si l'analyseur dit OK, P est vraie
 - Sinon, on ne sait pas...
 - mais l'analyseur termine

Illustration: la règle des signes

- But: détecter quelles variables x sont ≥ 0 et à quelles lignes d'un programme π
- Deux signes: '+' et '-'
- Règles de calcul:
 $'+' \times '+' = '+'$ $'+' \times '-' = '-'$ etc.
- Quelles règles pour l'addition?

Top

- ‘+’ + ‘−’ = $\top$ (top, « je ne sais pas, ça peut être n’importe quoi »)
- Pas $\perp$ (bottom): pourquoi?

Concrétisation

- = fonction de sémantique γ des valeurs abstraites (ici, les signes) vers l'ensemble des propriétés (=sous-ensembles des valeurs possibles)
- $\gamma('+') = \{n \in \mathbf{Z} \mid n \geq 0\}$
 $\gamma('-') = \{n \in \mathbf{Z} \mid n < 0\}$
 $\gamma(\top) = \mathbf{Z}$... monotone!
 $\gamma(\perp) = \emptyset$

Concrétisation

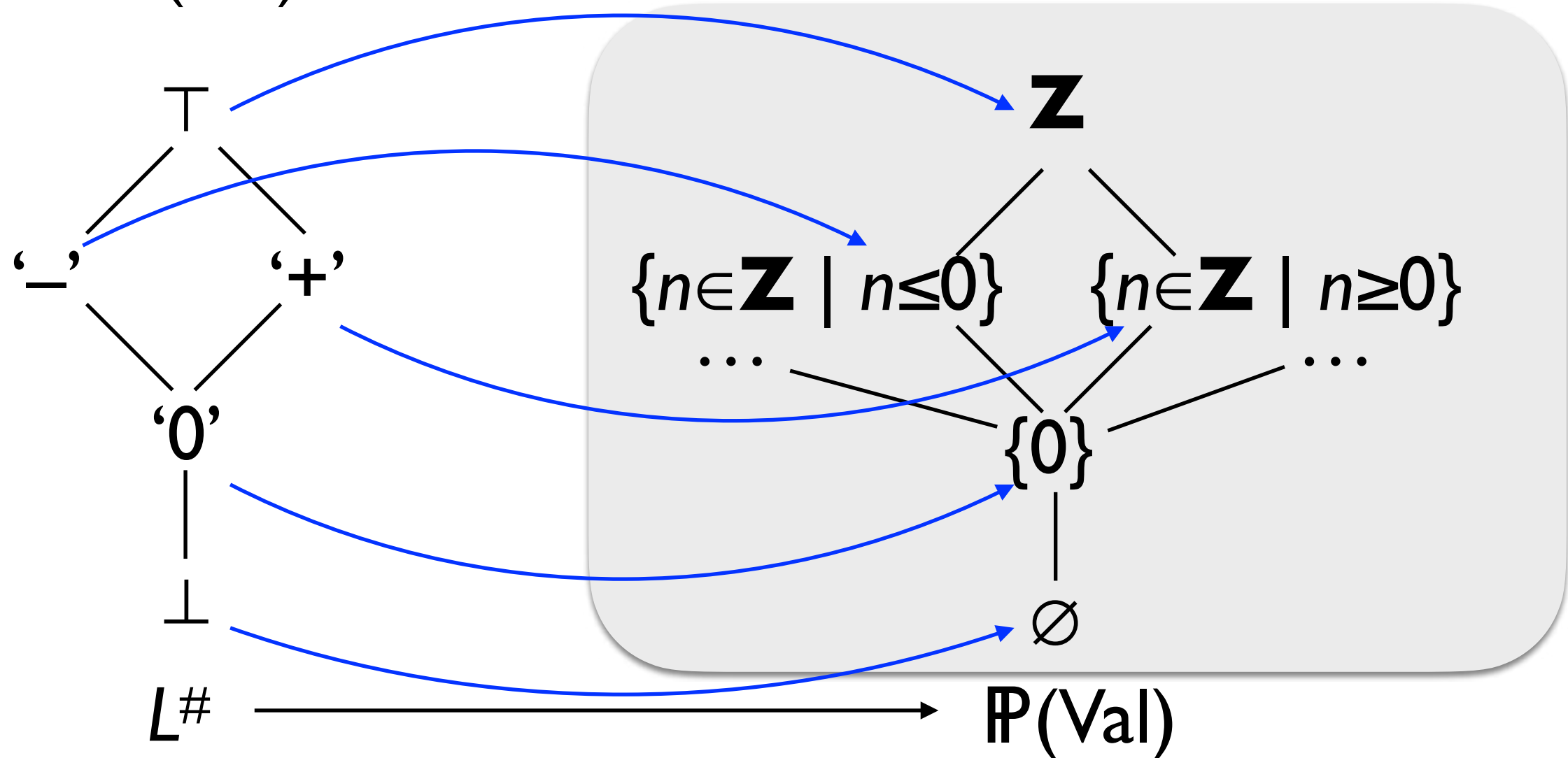
- = fonction de sémantique γ des valeurs abstraites (ici, les signes) vers l'ensemble des propriétés (=sous-ensembles des valeurs possibles)
- $\gamma('+') = \{n \in \mathbf{Z} \mid n \geq 0\}$
 $\gamma('-') = \{n \in \mathbf{Z} \mid n < 0\}$
 $\gamma(\top) = \mathbf{Z}$
 $\gamma(\perp) = \emptyset$

Pourquoi cette dissymétrie?
(Beurk)

... monotone!

Concrétisation, essai 2

- Je vais plutôt prendre le treillis $L^\#$ et $\gamma : L^\# \rightarrow \mathbb{P}(\text{Val})$ comme suit:



Sémantique abstraite des expressions

$$\begin{aligned}\llbracket x \rrbracket \rho &= \rho(x) \\ \llbracket n \rrbracket \rho &= n \\ \llbracket e_1 + e_2 \rrbracket \rho &= \llbracket e_1 \rrbracket \rho + \llbracket e_2 \rrbracket \rho \\ \llbracket -e \rrbracket \rho &= -\llbracket e \rrbracket \rho.\end{aligned}$$

- $\llbracket x \rrbracket \# \rho \# \stackrel{\text{def}}{=} \rho \#(x)$
- $\llbracket n \rrbracket \# \rho \# \stackrel{\text{def}}{=} \text{'0' si } n=0, \text{'+' si } n>0, \text{'-' si } n<0$
- $\llbracket e_1 + e_2 \rrbracket \# \rho \# \stackrel{\text{def}}{=} \llbracket e_1 \rrbracket \# \rho \# + \# \llbracket e_2 \rrbracket \# \rho \#$
- $\llbracket -e \rrbracket \# \rho \# \stackrel{\text{def}}{=} - \# \llbracket e \rrbracket \# \rho \#$

$+ \#$	$\perp$	'0'	'+'	'-'	$\top$
$\perp$	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$
'0'	$\perp$	'0'	'+'	'-'	$\top$
'+'	$\perp$	'+'	'+'	$\top$	$\top$
'-'	$\perp$	'-'	$\top$	'-'	$\top$
$\top$	$\perp$	$\top$	$\top$	$\top$	$\top$

$- \#$	$\perp$
$\perp$	$\perp$
'0'	0
'+'	'-'
'-'	'+'
$\top$	$\top$

Sémantique abstraite des expressions

- **Prop.** Si $\forall x, \rho(x) \in \gamma(\rho^\#(x))$,
alors $\llbracket e \rrbracket \rho \in \gamma(\llbracket e \rrbracket^\# \rho^\#)$

$$\begin{aligned}\llbracket x \rrbracket \rho &= \rho(x) \\ \llbracket n \rrbracket \rho &= n \\ \llbracket e_1 + e_2 \rrbracket \rho &= \llbracket e_1 \rrbracket \rho + \llbracket e_2 \rrbracket \rho \\ \llbracket -e \rrbracket \rho &= -\llbracket e \rrbracket \rho.\end{aligned}$$

- **Dém.:** par réc. sur e .
- Les cas de $+\#$ et de $-\#$ sont des énumérations de cas un peu pénibles...

$$\begin{aligned}\llbracket x \rrbracket^\# \rho^\# &\stackrel{\text{def}}{=} \rho^\#(x) \\ \llbracket n \rrbracket^\# \rho^\# &\stackrel{\text{def}}{=} \text{'0' si } n=0, \text{'+' si } n>0, \text{'-' si } n<0 \\ \llbracket e_1 + e_2 \rrbracket^\# \rho^\# &\stackrel{\text{def}}{=} \llbracket e_1 \rrbracket^\# \rho^\# ++ \llbracket e_2 \rrbracket^\# \rho^\# \\ \llbracket -e \rrbracket^\# \rho^\# &\stackrel{\text{def}}{=} -\# \llbracket e \rrbracket^\# \rho^\#\end{aligned}$$

$+\#$	$\perp$	'0'	'+'	'-'	T
$\perp$	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$
'0'	$\perp$	'0'	'+'	'-'	T
'+'	$\perp$	'+'	'+'	T	T
'-'	$\perp$	'-'	T	'-'	T
T	$\perp$	T	T	T	T

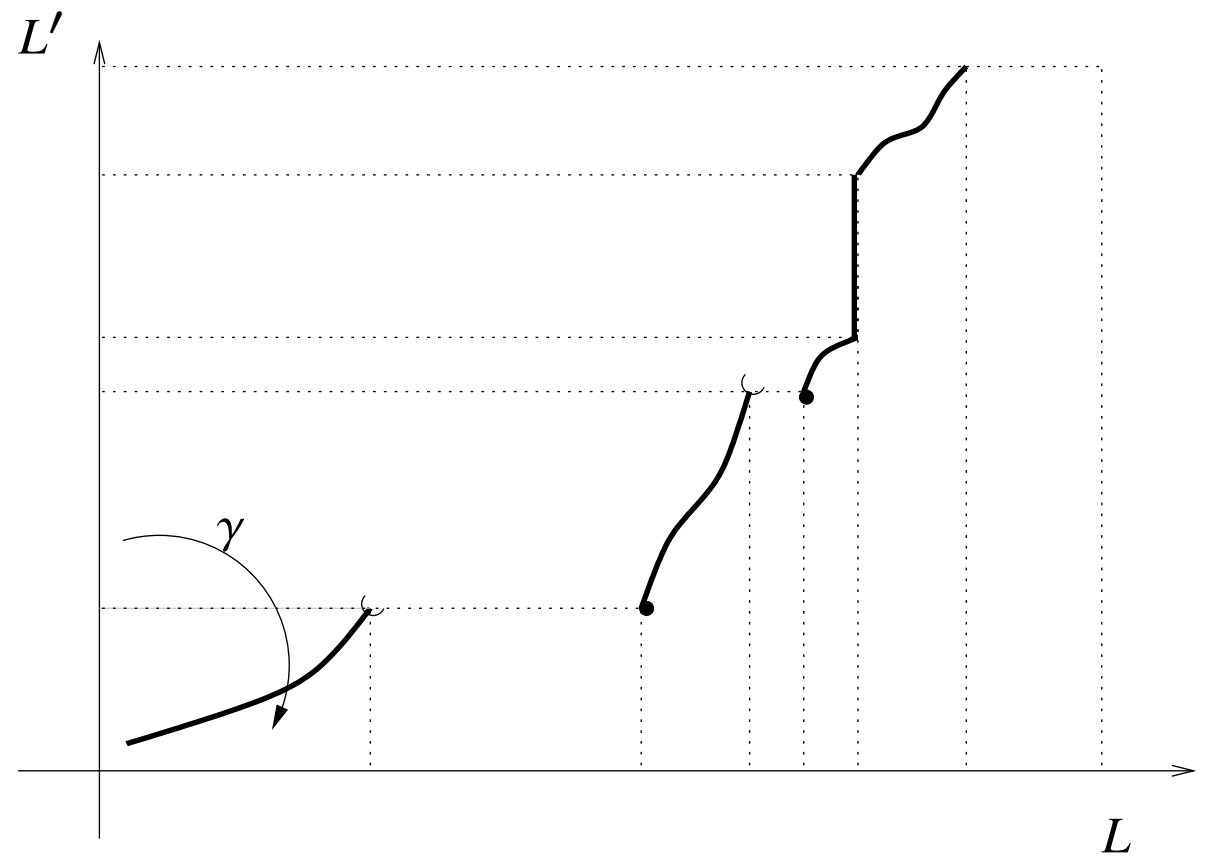
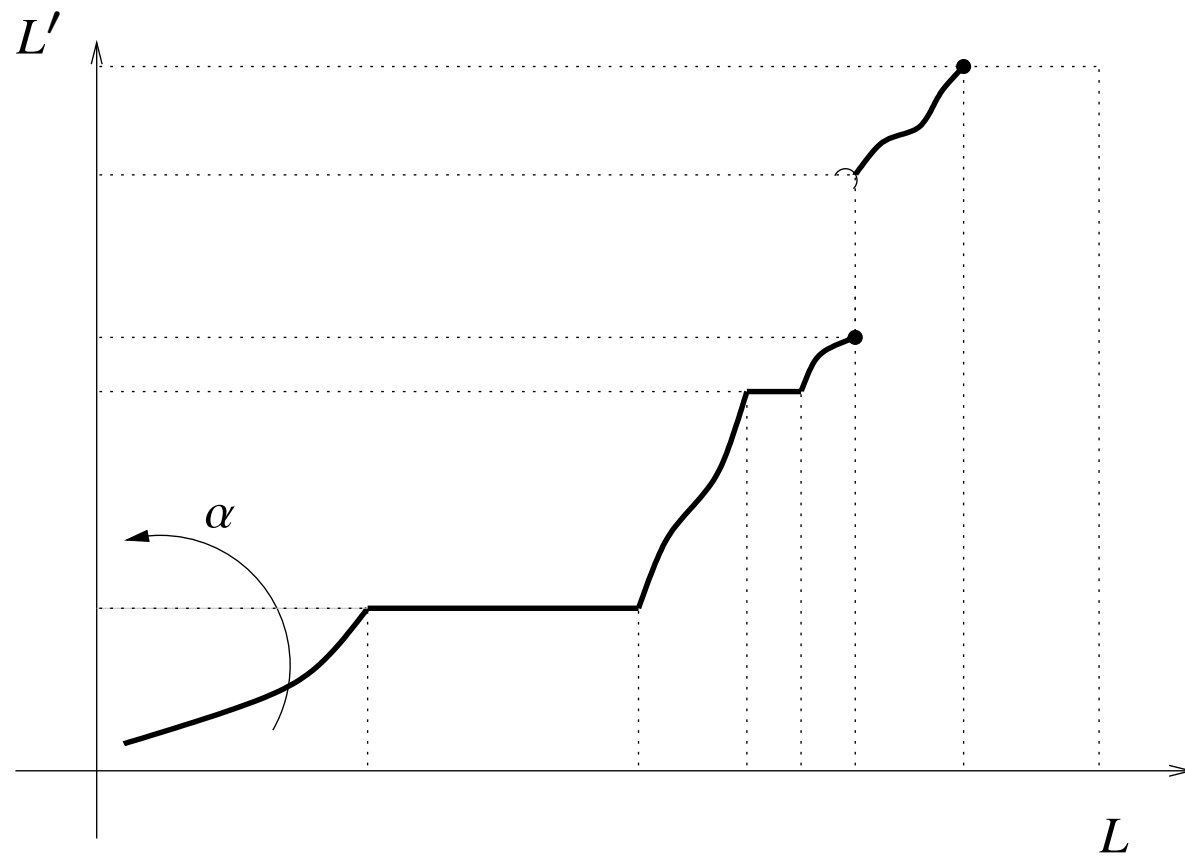
$-\#$	$\perp$
$\perp$	$\perp$
'0'	'0'
'+'	'-'
'-'	'+'
T	T

Comment obtenir la
meilleure des
sémantiques abstraites
possibles

Faire mieux

- Peut-on, connaissant γ et la sémantique concrète, **déduire** la sémantique abstraite?
... de sorte que cette dernière soit la plus précise possible?
- Correspondances de Galois

Correspondances de Galois



Correspondances de Galois

- Soit $\gamma : L^\# \rightarrow L$, $\alpha : L \rightarrow L^\#$ monotones.
Les propriétés suivantes sont équivalentes:
- (1) pour tous $x, y^\#$, $\alpha(x) \leq y^\#$ ssi $x \leq \gamma(y^\#)$
- (2) pour tous $x, y^\#$, $\alpha(\gamma(y^\#)) \leq y^\#$ et $x \leq \gamma(\alpha(x))$
- On dit alors que $\alpha \dashv \gamma$ est une **correspondance de Galois**

Les deux définitions de $\alpha \dashv \gamma$

$\alpha \dashv \gamma$:

(1) pour tous $x, y^\#$, $\alpha(x) \leq y^\#$ ssi $x \leq \gamma(y^\#)$

(2) pour tous $x, y^\#$, $\alpha(\gamma(y^\#)) \leq y^\#$ et $x \leq \gamma(\alpha(x))$

- Si (1):

- $\gamma(y^\#) \leq \gamma(y^\#)$, donc $\alpha(\gamma(y^\#)) \leq y^\#$ par (1)

Les deux définitions de $\alpha \dashv \gamma$

$\alpha \dashv \gamma$:

(1) pour tous $x, y^\#, \alpha(x) \leq y^\#$ ssi $x \leq \gamma(y^\#)$

(2) pour tous $x, y^\#, \alpha(\gamma(y^\#)) \leq y^\#$ et $x \leq \gamma(\alpha(x))$

- Si (1):
- $\gamma(y^\#) \leq \gamma(y^\#)$, donc $\alpha(\gamma(y^\#)) \leq y^\#$ par (1)
- $\alpha(x) \leq \alpha(x)$, donc $x \leq \gamma(\alpha(x))$ par (1)

Les deux définitions de $\alpha \dashv \gamma$

$\alpha \dashv \gamma$:

(1) pour tous $x, y^\#, \alpha(x) \leq y^\#$ ssi $x \leq \gamma(y^\#)$

(2) pour tous $x, y^\#, \alpha(\gamma(y^\#)) \leq y^\#$ et $x \leq \gamma(\alpha(x))$

- Si (1):
 - $\gamma(y^\#) \leq \gamma(y^\#)$, donc $\alpha(\gamma(y^\#)) \leq y^\#$ par (1)
 - $\alpha(x) \leq \alpha(x)$, donc $x \leq \gamma(\alpha(x))$ par (1)
- Si (2) **et** α, γ monotones:

Les deux définitions de $\alpha \dashv \gamma$

$\alpha \dashv \gamma$:

(1) pour tous $x, y^\#$, $\alpha(x) \leq y^\#$ ssi $x \leq \gamma(y^\#)$

(2) pour tous $x, y^\#$, $\alpha(\gamma(y^\#)) \leq y^\#$ et $x \leq \gamma(\alpha(x))$

- Si (1):
 - $\gamma(y^\#) \leq \gamma(y^\#)$, donc $\alpha(\gamma(y^\#)) \leq y^\#$ par (1)
 - $\alpha(x) \leq \alpha(x)$, donc $x \leq \gamma(\alpha(x))$ par (1)
- Si (2) **et** α, γ monotones:
 - Si $\alpha(x) \leq y^\#$, alors $\gamma(\alpha(x)) \leq \gamma(y^\#)$ [γ monotone]
donc $x \leq \gamma(\alpha(x)) \leq \gamma(y^\#)$ par (2)

Les deux définitions de $\alpha \dashv \gamma$

$\alpha \dashv \gamma$:

(1) pour tous $x, y^\#$, $\alpha(x) \leq y^\#$ ssi $x \leq \gamma(y^\#)$

(2) pour tous $x, y^\#$, $\alpha(\gamma(y^\#)) \leq y^\#$ et $x \leq \gamma(\alpha(x))$

- Si (1):
 - $\gamma(y^\#) \leq \gamma(y^\#)$, donc $\alpha(\gamma(y^\#)) \leq y^\#$ par (1)
 - $\alpha(x) \leq \alpha(x)$, donc $x \leq \gamma(\alpha(x))$ par (1)
- Si (2) **et** α, γ monotones:
 - Si $\alpha(x) \leq y^\#$, alors $\gamma(\alpha(x)) \leq \gamma(y^\#)$ [γ monotone]
donc $x \leq \gamma(\alpha(x)) \leq \gamma(y^\#)$ par (2)
 - Si $x \leq \gamma(y^\#)$, alors $\alpha(x) \leq \alpha(\gamma(y^\#))$ [α monotone]
donc $\alpha(x) \leq \alpha(\gamma(y^\#)) \leq y^\#$ par (2).

Une 3ème définition de

$$\alpha \dashv \gamma$$

- Soit $\gamma : L^\# \rightarrow L$, $\alpha : L \rightarrow L^\#$ monotones, L et $L^\#$ **treillis complets** et $\alpha \dashv \gamma$ (pensez $L = \mathbb{P}(\text{Val})$)
- Alors $\alpha(x)$ est la valeur abstraite $y^\#$ **la plus précise** (la plus petite) qui soit **correcte** par rapport à x ($x \leq \gamma(y^\#)$), comme on va le voir tout de suite

$\alpha \dashv \gamma$, version 3

- Si (1)/(2):
- $\alpha(x)$ minore
 $A_x \stackrel{\text{def}}{=} \{y^\# \mid x \leq \gamma(y^\#)\}$ par (1)

Si α et γ monotones, les propriétés suivantes sont équivalentes (i.e., $\alpha \dashv \gamma$):

- (1) pour tous $x, y^\#$, $\alpha(x) \leq y^\#$ ssi $x \leq \gamma(y^\#)$
- (2) pour tous $x, y^\#$, $\alpha(\gamma(y^\#)) \leq y^\#$ et $x \leq \gamma(\alpha(x))$
- (3) pour tout x , $\alpha(x) = \mathbf{min} \{y^\# \mid x \leq \gamma(y^\#)\}$
- (4) pour tout $y^\#$, $\gamma(y^\#) = \mathbf{max} \{x \mid \alpha(x) \leq y^\#\}$

$\alpha \dashv \gamma$, version 3

- Si (1)/(2):
 - $\alpha(x)$ minore
 $A_x \stackrel{\text{def}}{=} \{y^\# \mid x \leq \gamma(y^\#)\}$ par (1)
 - $\alpha(x) \in A_x$, par (2)

Si α et γ monotones, les propriétés suivantes sont équivalentes (i.e., $\alpha \dashv \gamma$):

- (1) pour tous $x, y^\#$, $\alpha(x) \leq y^\#$ ssi $x \leq \gamma(y^\#)$
- (2) pour tous $x, y^\#$, $\alpha(\gamma(y^\#)) \leq y^\#$ et $x \leq \gamma(\alpha(x))$
- (3) pour tout x , $\alpha(x) = \mathbf{min} \{y^\# \mid x \leq \gamma(y^\#)\}$
- (4) pour tout $y^\#$, $\gamma(y^\#) = \mathbf{max} \{x \mid \alpha(x) \leq y^\#\}$

$\alpha \dashv \gamma$, version 3

- Si (1)/(2):
 - $\alpha(x)$ minore
 $A_x \stackrel{\text{def}}{=} \{y^\# \mid x \leq \gamma(y^\#)\}$ par (1)
 - $\alpha(x) \in A_x$, par (2)
 - donc $\alpha(x) = \mathbf{min} A_x$.

Si α et γ monotones, les propriétés suivantes sont équivalentes (i.e., $\alpha \dashv \gamma$):

- (1) pour tous $x, y^\#$, $\alpha(x) \leq y^\#$ ssi $x \leq \gamma(y^\#)$
- (2) pour tous $x, y^\#$, $\alpha(\gamma(y^\#)) \leq y^\#$ et $x \leq \gamma(\alpha(x))$
- (3) pour tout x , $\alpha(x) = \mathbf{min} \{y^\# \mid x \leq \gamma(y^\#)\}$
- (4) pour tout $y^\#$, $\gamma(y^\#) = \mathbf{max} \{x \mid \alpha(x) \leq y^\#\}$

$\alpha \dashv \gamma$, version 3

- Si (1)/(2):
 - $\alpha(x)$ minore
 $A_x \stackrel{\text{def}}{=} \{y^\# \mid x \leq \gamma(y^\#)\}$ par (1)
 - $\alpha(x) \in A_x$, par (2)
 - donc $\alpha(x) = \mathbf{min} A_x$.
- Si (3) $\alpha(x) = \min A_x$

Si α et γ monotones, les propriétés suivantes sont équivalentes (i.e., $\alpha \dashv \gamma$):

- (1) pour tous $x, y^\#$, $\alpha(x) \leq y^\#$ ssi $x \leq \gamma(y^\#)$
- (2) pour tous $x, y^\#$, $\alpha(\gamma(y^\#)) \leq y^\#$ et $x \leq \gamma(\alpha(x))$
- (3) pour tout x , $\alpha(x) = \mathbf{min} \{y^\# \mid x \leq \gamma(y^\#)\}$
- (4) pour tout $y^\#$, $\gamma(y^\#) = \mathbf{max} \{x \mid \alpha(x) \leq y^\#\}$

$\alpha \dashv \gamma$, version 3

- Si (1)/(2):
 - $\alpha(x)$ minore
 $A_x \stackrel{\text{def}}{=} \{y^\# \mid x \leq \gamma(y^\#)\}$ par (1)
 - $\alpha(x) \in A_x$, par (2)
 - donc $\alpha(x) = \mathbf{min} A_x$.
- Si (3) $\alpha(x) = \min A_x$
 - si $x \leq \gamma(y^\#)$, alors $\alpha(x) \leq y^\#$ [$\alpha(x)$ minore A_x]

Si α et γ monotones, les propriétés suivantes sont équivalentes (i.e., $\alpha \dashv \gamma$):

- (1) pour tous $x, y^\#$, $\alpha(x) \leq y^\#$ ssi $x \leq \gamma(y^\#)$
- (2) pour tous $x, y^\#$, $\alpha(\gamma(y^\#)) \leq y^\#$ et $x \leq \gamma(\alpha(x))$
- (3) pour tout x , $\alpha(x) = \mathbf{min} \{y^\# \mid x \leq \gamma(y^\#)\}$
- (4) pour tout $y^\#$, $\gamma(y^\#) = \mathbf{max} \{x \mid \alpha(x) \leq y^\#\}$

$\alpha \dashv \gamma$, version 3

- Si (1)/(2):
 - $\alpha(x)$ minore
 $A_x \stackrel{\text{def}}{=} \{y^\# \mid x \leq \gamma(y^\#)\}$ par (1)
 - $\alpha(x) \in A_x$, par (2)
 - donc $\alpha(x) = \mathbf{min} A_x$.
- Si (3) $\alpha(x) = \min A_x$
 - si $x \leq \gamma(y^\#)$, alors $\alpha(x) \leq y^\#$ [$\alpha(x)$ minore A_x]
 - si $\alpha(x) \leq y^\#$, alors $x \leq \gamma(\alpha(x))$ [$\alpha(x) \in A_x$] $\leq \gamma(y^\#)$ [γ monotone]

Si α et γ monotones, les propriétés suivantes sont équivalentes (i.e., $\alpha \dashv \gamma$):

- (1) pour tous $x, y^\#$, $\alpha(x) \leq y^\#$ ssi $x \leq \gamma(y^\#)$
- (2) pour tous $x, y^\#$, $\alpha(\gamma(y^\#)) \leq y^\#$ et $x \leq \gamma(\alpha(x))$
- (3) pour tout x , $\alpha(x) = \mathbf{min} \{y^\# \mid x \leq \gamma(y^\#)\}$
- (4) pour tout $y^\#$, $\gamma(y^\#) = \mathbf{max} \{x \mid \alpha(x) \leq y^\#\}$

Donc (1)

$\alpha \dashv \gamma$, version 3

- Si (1)/(2):
 - $\alpha(x)$ minore
 $A_x \stackrel{\text{def}}{=} \{y^\# \mid x \leq \gamma(y^\#)\}$ par (1)
 - $\alpha(x) \in A_x$, par (2)
 - donc $\alpha(x) = \mathbf{min} A_x$.
- Si (3) $\alpha(x) = \min A_x$
 - si $x \leq \gamma(y^\#)$, alors $\alpha(x) \leq y^\#$ [$\alpha(x)$ minore A_x]
 - si $\alpha(x) \leq y^\#$, alors $x \leq \gamma(\alpha(x))$ [$\alpha(x) \in A_x$] $\leq \gamma(y^\#)$ [γ monotone]

Si α et γ monotones, les propriétés suivantes sont équivalentes (i.e., $\alpha \dashv \gamma$):

- (1) pour tous $x, y^\#$, $\alpha(x) \leq y^\#$ ssi $x \leq \gamma(y^\#)$
- (2) pour tous $x, y^\#$, $\alpha(\gamma(y^\#)) \leq y^\#$ et $x \leq \gamma(\alpha(x))$
- (3) pour tout x , $\alpha(x) = \mathbf{min} \{y^\# \mid x \leq \gamma(y^\#)\}$
- (4) pour tout $y^\#$, $\gamma(y^\#) = \mathbf{max} \{x \mid \alpha(x) \leq y^\#\}$

Donc (1)

Donc (2), puisque (1) $\Leftrightarrow$ (2)

$\alpha \dashv \gamma$, version 3

- Si (1)/(2):
 - $\alpha(x)$ minore
 $A_x \stackrel{\text{def}}{=} \{y^\# \mid x \leq \gamma(y^\#)\}$ par (1)
 - $\alpha(x) \in A_x$, par (2)
 - donc $\alpha(x) = \mathbf{min} A_x$.
- Si (3) $\alpha(x) = \min A_x$
 - si $x \leq \gamma(y^\#)$, alors $\alpha(x) \leq y^\#$ [$\alpha(x)$ minore A_x]
 - si $\alpha(x) \leq y^\#$, alors $x \leq \gamma(\alpha(x))$ [$\alpha(x) \in A_x$] $\leq \gamma(y^\#)$ [γ monotone]

Si α et γ monotones, les propriétés suivantes sont équivalentes (i.e., $\alpha \dashv \gamma$):

- (1) pour tous $x, y^\#$, $\alpha(x) \leq y^\#$ ssi $x \leq \gamma(y^\#)$
- (2) pour tous $x, y^\#$, $\alpha(\gamma(y^\#)) \leq y^\#$ et $x \leq \gamma(\alpha(x))$
- (3) pour tout x , $\alpha(x) = \mathbf{min} \{y^\# \mid x \leq \gamma(y^\#)\}$
- (4) pour tout $y^\#$, $\gamma(y^\#) = \mathbf{max} \{x \mid \alpha(x) \leq y^\#\}$

(4) se montre de façon symétrique à (3)

Donc (1)

Donc (2), puisque (1) $\Leftrightarrow$ (2)

α en fonction de γ

- Une fonction $\gamma : L^\# \rightarrow L$ entre treillis complets est la partie droite d'une correspondance de Galois $\alpha \dashv \gamma$ ssi γ **préserve tous les infs.**

α en fonction de γ

- Une fonction $\gamma : L^\# \rightarrow L$ entre treillis complets est la partie droite d'une correspondance de Galois $\alpha \dashv \gamma$ ssi γ **préserve tous les infs**.
- Alors α est déterminée de façon unique par:

$$\alpha(x) = \inf \{y^\# \mid x \leq \gamma(y^\#)\}$$

α en fonction de γ

- Une fonction $\gamma : L^\# \rightarrow L$ entre treillis complets est la partie droite d'une correspondance de Galois $\alpha \dashv \gamma$ ssi γ **préserve tous les infs**.
- Alors α est déterminée de façon unique par:
$$\alpha(x) = \inf \{y^\# \mid x \leq \gamma(y^\#)\}$$
- ... et l'inf est **atteint**
(c'est un **min**—on l'a déjà vu).

α en fonction de γ

- Si $\alpha \dashv \gamma$, alors pour tout x ,

$$x \leq \gamma(\inf_{i \in I} y_i^\#) \dots$$

Si $\alpha \dashv \gamma$ alors γ **préserve tous les infs.**

α en fonction de γ

- Si $\alpha \dashv \gamma$, alors pour tout x ,

$$x \leq \gamma(\inf_{i \in I} y_i^\#) \dots$$

- ssi

$$\alpha(x) \leq \inf_{i \in I} y_i^\# \text{ ssi}$$

Si $\alpha \dashv \gamma$ alors γ **préserve tous les infs.**

α en fonction de γ

- Si $\alpha \dashv \gamma$, alors pour tout x ,

$$x \leq \gamma(\inf_{i \in I} y_i^\#) \dots$$

Si $\alpha \dashv \gamma$ alors γ **préserve tous les infs.**

- ssi $\alpha(x) \leq \inf_{i \in I} y_i^\#$ ssi
- ssi pour tout $i \in I$, $\alpha(x) \leq y_i^\#$ ssi

α en fonction de γ

- Si $\alpha \dashv \gamma$, alors pour tout x ,

$$x \leq \gamma(\inf_{i \in I} y_i^\#) \dots$$

Si $\alpha \dashv \gamma$ alors γ **préserve tous les infs.**

- ssi $\alpha(x) \leq \inf_{i \in I} y_i^\#$ ssi
- ssi pour tout $i \in I$, $\alpha(x) \leq y_i^\#$ ssi
- ssi pour tout $i \in I$, $x \leq \gamma(y_i^\#)$ ssi

α en fonction de γ

- Si $\alpha \dashv \gamma$, alors pour tout x ,

Si $\alpha \dashv \gamma$ alors γ **préserve tous les infs.**

$$x \leq \gamma(\inf_{i \in I} y_i^\#) \dots$$

- ssi $\alpha(x) \leq \inf_{i \in I} y_i^\#$ ssi
- ssi pour tout $i \in I$, $\alpha(x) \leq y_i^\#$ ssi
- ssi pour tout $i \in I$, $x \leq \gamma(y_i^\#)$ ssi
- ssi $x \leq \inf_{i \in I} \gamma(y_i^\#)$

α en fonction de γ

- Si $\alpha \dashv \gamma$, alors pour tout x ,

Si $\alpha \dashv \gamma$ alors γ **préserve tous les infs.**

$$x \leq \gamma(\inf_{i \in I} y_i^\#) \dots$$

- ssi $\alpha(x) \leq \inf_{i \in I} y_i^\#$ ssi
- ssi pour tout $i \in I$, $\alpha(x) \leq y_i^\#$ ssi
- ssi pour tout $i \in I$, $x \leq \gamma(y_i^\#)$ ssi
- ssi $x \leq \inf_{i \in I} \gamma(y_i^\#)$
- En prenant $x \stackrel{\text{def}}{=} \gamma(\inf_{i \in I} y_i^\#)$, on obtient
$$\gamma(\inf_{i \in I} y_i^\#) \leq \inf_{i \in I} \gamma(y_i^\#)$$

α en fonction de γ

- Si $\alpha \dashv \gamma$, alors pour tout x ,

Si $\alpha \dashv \gamma$ alors γ **préserve tous les infs.**

$$x \leq \gamma(\inf_{i \in I} y_i^\#) \dots$$

- ssi $\alpha(x) \leq \inf_{i \in I} y_i^\#$ ssi
- ssi pour tout $i \in I$, $\alpha(x) \leq y_i^\#$ ssi
- ssi pour tout $i \in I$, $x \leq \gamma(y_i^\#)$ ssi
- ssi $x \leq \inf_{i \in I} \gamma(y_i^\#)$
- En prenant $x \stackrel{\text{def}}{=} \gamma(\inf_{i \in I} y_i^\#)$, on obtient
$$\gamma(\inf_{i \in I} y_i^\#) \leq \inf_{i \in I} \gamma(y_i^\#)$$
- En prenant $x \stackrel{\text{def}}{=} \inf_{i \in I} \gamma(y_i^\#)$, on obtient
$$\inf_{i \in I} \gamma(y_i^\#) \leq \gamma(\inf_{i \in I} y_i^\#)$$

α en fonction de γ

- On a vu que si $\alpha \dashv \gamma$,
alors (3) $\alpha(x) = \min \{y^\# \mid x \leq \gamma(y^\#)\}$
- Posons $\alpha(x) \stackrel{\text{def}}{=} \inf \{y^\# \mid x \leq \gamma(y^\#)\}$, pour tout x

Si γ préserve tous les infs, alors $\alpha \dashv \gamma$
où $\alpha(x)$ vaut (nécessairement) $\inf \{y^\# \mid x \leq \gamma(y^\#)\}$

α en fonction de γ

- On a vu que si $\alpha \dashv \gamma$,
alors (3) $\alpha(x) = \min \{y^\# \mid x \leq \gamma(y^\#)\}$
- Posons $\alpha(x) \stackrel{\text{def}}{=} \inf \{y^\# \mid x \leq \gamma(y^\#)\}$, pour tout x
- Ceci définit une fonction monotone α (exercice)

Si γ préserve tous les infs, alors $\alpha \dashv \gamma$
où $\alpha(x)$ vaut (nécessairement) $\inf \{y^\# \mid x \leq \gamma(y^\#)\}$

α en fonction de γ

- On a vu que si $\alpha \dashv \gamma$,
alors (3) $\alpha(x) = \min \{y^\# \mid x \leq \gamma(y^\#)\}$
- Posons $\alpha(x) \stackrel{\text{def}}{=} \inf \{y^\# \mid x \leq \gamma(y^\#)\}$, pour tout x
- Ceci définit une fonction monotone α (exercice)
- $\gamma(\alpha(x)) = \inf \{\gamma(y^\#) \mid x \leq \gamma(y^\#)\} \geq x$ [γ préserve tous les infs]

Si γ préserve tous les infs, alors $\alpha \dashv \gamma$
où $\alpha(x)$ vaut (nécessairement) $\inf \{y^\# \mid x \leq \gamma(y^\#)\}$

α en fonction de γ

Si γ préserve tous les infs, alors $\alpha \dashv \gamma$
où $\alpha(x)$ vaut (nécessairement) $\inf \{y^\# \mid x \leq \gamma(y^\#)\}$

- On a vu que si $\alpha \dashv \gamma$,
alors (3) $\alpha(x) = \min \{y^\# \mid x \leq \gamma(y^\#)\}$
- Posons $\alpha(x) \stackrel{\text{def}}{=} \inf \{y^\# \mid x \leq \gamma(y^\#)\}$, pour tout x
- Ceci définit une fonction monotone α (exercice)
- $\gamma(\alpha(x)) = \inf \{\gamma(y^\#) \mid x \leq \gamma(y^\#)\} \geq x$ [γ préserve tous les infs]
- $\alpha(\gamma(y^\#)) = \inf \{y'^\# \mid \gamma(y^\#) \leq \gamma(y'^\#)\} \leq y^\#$ car $y^\#$ est un $y'^\#$ tel que $\gamma(y^\#) \leq \gamma(y'^\#)$.

α en fonction de γ

- On a vu que si $\alpha \dashv \gamma$,
alors (3) $\alpha(x) = \min \{y^\# \mid x \leq \gamma(y^\#)\}$
- Posons $\alpha(x) \stackrel{\text{def}}{=} \inf \{y^\# \mid x \leq \gamma(y^\#)\}$, pour tout x
- Ceci définit une fonction monotone α (exercice)
- $\gamma(\alpha(x)) = \inf \{\gamma(y^\#) \mid x \leq \gamma(y^\#)\} \geq x$ [γ préserve tous les infs]
- $\alpha(\gamma(y^\#)) = \inf \{y'^\# \mid \gamma(y^\#) \leq \gamma(y'^\#)\} \leq y^\#$ car $y^\#$ est un $y'^\#$ tel que $\gamma(y^\#) \leq \gamma(y'^\#)$.
- Donc $\alpha \dashv \gamma$.

Si γ préserve tous les infs, alors $\alpha \dashv \gamma$
où $\alpha(x)$ vaut (nécessairement) $\inf \{y^\# \mid x \leq \gamma(y^\#)\}$

Si α et γ monotones, les propriétés suivantes
sont équivalentes, $\alpha \dashv \gamma$ ssi:
(2) pour tous $x, y^\#$, $\alpha(\gamma(y^\#)) \leq y^\#$ et $x \leq \gamma(\alpha(x))$

La correspondance de Galois des signes

- Je vous laisse vérifier que:

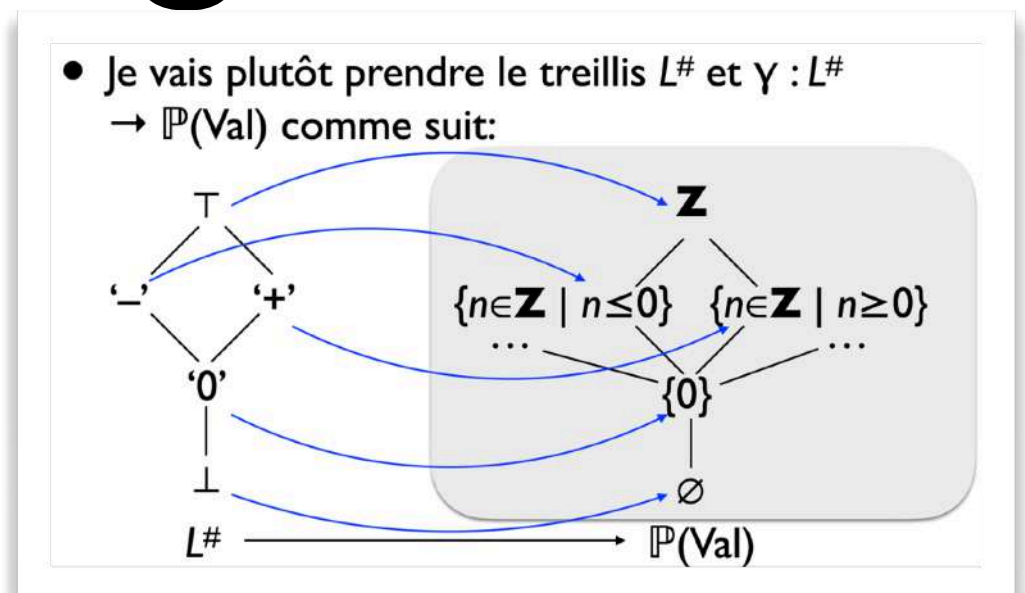
- $\alpha(\emptyset) = \perp$

$$\alpha(\{0\}) = '0'$$

$\alpha(E) = '+'$ si E ne contient que des nombres ≥ 0 et au moins un > 0

$\alpha(E) = '-'$ si E ne contient que des nombres ≤ 0 et au moins un < 0

$$\alpha(E) = \top \text{ sinon}$$



La meilleure approximation d'une fonction

- Soit $\alpha \dashv \gamma$ entre treillis complets $L, L^\#$,
et $f : L^n \rightarrow L$ monotone
- Alors
 $f^\# : (y_1^\#, \dots, y_n^\#) \mapsto \alpha(f(\gamma(y_1^\#), \dots, \gamma(y_n^\#)))$
est la meilleure approximation de f :

La meilleure approximation d'une fonction

- Soit $\alpha \dashv \gamma$ entre treillis complets $L, L^\#$,
et $f : L^n \rightarrow L$ monotone
- Alors
 $f^\# : (y_1^\#, \dots, y_n^\#) \mapsto \alpha(f(\gamma(y_1^\#), \dots, \gamma(y_n^\#)))$
est la meilleure approximation de f :
- [approx.] si $x_i \leq \gamma(y_i^\#)$ pour tout i , alors
$$f(x_1, \dots, x_n) \leq \gamma(f^\#(y_1^\#, \dots, y_n^\#))$$

La meilleure approximation d'une fonction

- Soit $\alpha \dashv \gamma$ entre treillis complets $L, L^\#$,
et $f : L^n \rightarrow L$ monotone
- Alors
$$f^\# : (y_1^\#, \dots, y_n^\#) \mapsto \alpha(f(\gamma(y_1^\#), \dots, \gamma(y_n^\#)))$$

est la meilleure approximation de f :
- [approx.] si $x_i \leq \gamma(y_i^\#)$ pour tout i , alors
$$f(x_1, \dots, x_n) \leq \gamma(f^\#(y_1^\#, \dots, y_n^\#))$$
- [meilleure] si g est une autre approximation
alors $f^\# \leq g$

La meilleure approximation d'une fonction

- Soit $y^\# \stackrel{\text{def}}{=} f^\#(y_1^\#, \dots, y_n^\#)$
- Par déf., $y^\# = a(x)$
où $x \stackrel{\text{def}}{=} f(\gamma(y_1^\#), \dots, \gamma(y_n^\#))$

$f^\# : (y_1^\#, \dots, y_n^\#) \mapsto a(f(\gamma(y_1^\#), \dots, \gamma(y_n^\#)))$
est la meilleure approximation de f

[approx.] si $x_i \leq \gamma(y_i^\#)$ pour tout i , alors

$$f(x_1, \dots, x_n) \leq \gamma(f^\#(y_1^\#, \dots, y_n^\#))$$

[meilleure] si g est une autre approximation
alors $f^\# \leq g$

La meilleure approximation d'une fonction

- Soit $y^\# \stackrel{\text{def}}{=} f^\#(y_1^\#, \dots, y_n^\#)$
- Par déf., $y^\# = \alpha(x)$
où $x \stackrel{\text{def}}{=} f(\gamma(y_1^\#), \dots, \gamma(y_n^\#))$
- Autrement dit, $y^\#$ est
le plus petit / $x \leq \gamma(y^\#)$

$f^\# : (y_1^\#, \dots, y_n^\#) \mapsto \alpha(f(\gamma(y_1^\#), \dots, \gamma(y_n^\#)))$
est la meilleure approximation de f

[approx.] si $x_i \leq \gamma(y_i^\#)$ pour tout i , alors

$$f(x_1, \dots, x_n) \leq \gamma(f^\#(y_1^\#, \dots, y_n^\#))$$

[meilleure] si g est une autre approximation
alors $f^\# \leq g$

α est déterminée de façon unique par:

$$\alpha(x) = \inf \{y^\# \mid x \leq \gamma(y^\#)\}$$

... et l'inf est **atteint** (c'est un **min**).

La meilleure approximation d'une fonction

- Soit $y^\# \stackrel{\text{def}}{=} f^\#(y_1^\#, \dots, y_n^\#)$
- Par déf., $y^\# = \alpha(x)$
où $x \stackrel{\text{def}}{=} f(\gamma(y_1^\#), \dots, \gamma(y_n^\#))$
- Autrement dit, $y^\#$ est
le plus petit / $x \leq \gamma(y^\#)$
- Ceci est vrai
pour tous $y_1^\#, \dots, y_n^\#$:
 $f^\#(y_1^\#, \dots, y_n^\#)$ est le plus petit $y^\#$ /
 $f(\gamma(y_1^\#), \dots, \gamma(y_n^\#)) \leq \gamma(y^\#)$

$f^\# : (y_1^\#, \dots, y_n^\#) \mapsto \alpha(f(\gamma(y_1^\#), \dots, \gamma(y_n^\#)))$
est la meilleure approximation de f

[approx.] si $x_i \leq \gamma(y_i^\#)$ pour tout i , alors

$$f(x_1, \dots, x_n) \leq \gamma(f^\#(y_1^\#, \dots, y_n^\#))$$

[meilleure] si g est une autre approximation
alors $f^\# \leq g$

α est déterminée de façon unique par:

$$\alpha(x) = \inf \{y^\# \mid x \leq \gamma(y^\#)\}$$

... et l'inf est **atteint** (c'est un **min**).

La meilleure approximation d'une fonction

- Soit $y^\# \stackrel{\text{def}}{=} f^\#(y_1^\#, \dots, y_n^\#)$
- Par déf., $y^\# = \alpha(x)$
où $x \stackrel{\text{def}}{=} f(\gamma(y_1^\#), \dots, \gamma(y_n^\#))$

- Autrement dit, $y^\#$ est le plus petit / $x \leq \gamma(y^\#)$

- Ceci est vrai pour tous $y_1^\#, \dots, y_n^\#$:
 $f^\#(y_1^\#, \dots, y_n^\#)$ est le plus petit $y^\#$ /
 $f(\gamma(y_1^\#), \dots, \gamma(y_n^\#)) \leq \gamma(y^\#)$

- Et donc tel que pour tous $x_1 \leq \gamma(y_1^\#), \dots, x_n \leq \gamma(y_n^\#)$,
 $f(x_1, \dots, x_n) \leq \gamma(y^\#)$

$f^\# : (y_1^\#, \dots, y_n^\#) \mapsto \alpha(f(\gamma(y_1^\#), \dots, \gamma(y_n^\#)))$
est la meilleure approximation de f

[approx.] si $x_i \leq \gamma(y_i^\#)$ pour tout i , alors

$$f(x_1, \dots, x_n) \leq \gamma(f^\#(y_1^\#, \dots, y_n^\#))$$

[meilleure] si g est une autre approximation
alors $f^\# \leq g$

α est déterminée de façon unique par:

$$\alpha(x) = \inf \{y^\# \mid x \leq \gamma(y^\#)\}$$

... et l'inf est **atteint** (c'est un **min**).

L'exemple des signes

- Justement, $+\#$ et $-\#$ ont été obtenues comme les meilleures approximations de $+$ et $-$, respectivement.

$+\#$	$\perp$	'0'	'+'	'-'	T
$\perp$	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$
'0'	$\perp$	'0'	'+'	'-'	T
'+'	$\perp$	'+'	'+'	T	T
'-'	$\perp$	'-'	T	'-'	T
T	$\perp$	T	T	T	T

$-\#$	$\perp$
$\perp$	$\perp$
'0'	0'
'+'	'-'
'-'	'+'
T	T

L'exemple des signes

- Justement, $+\#$ et $-\#$ ont été obtenues comme les meilleures approximations de $+$ et $-$, respectivement.
- La proposition de correction est une instance d'une proposition bien plus **générale**... et plus facile à démontrer.

$+\#$	$\perp$	'0'	'+'	'-'	$\top$
$\perp$	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$
'0'	$\perp$	'0'	'+'	'-'	$\top$
'+'	$\perp$	'+'	'+'	$\top$	$\top$
'-'	$\perp$	'-'	$\top$	'-'	$\top$
$\top$	$\perp$	$\top$	$\top$	$\top$	$\top$

$-\#$	$\perp$
$\perp$	$\perp$
'0'	0'
'+'	'-'
'-'	'+'
$\top$	$\top$

Prop. Si $\forall x, \rho(x) \in \gamma(\rho^\#(x))$,
alors $\llbracket e \rrbracket \rho \in \gamma(\llbracket e \rrbracket^\# \rho^\#)$

Correction

- **Prop.** Supposons: pour chaque opération $\dot{f}$ ($\dot{+}$, $\dot{-}$, $\dot{n}$ par exemple) on a une approximation $f^\#$ de sa sémantique [concrète] f .

Correction

- **Prop.** Supposons: pour chaque opération $\dot{f}$ ($\dot{+}$, $\dot{-}$, $\dot{n}$ par exemple) on a une approximation $f^\#$ de sa sémantique [concrète] f .
- Ceci permet de définir une **sémantique abstraite** $\llbracket e \rrbracket^\# \rho^\#$ par
$$\llbracket \dot{f}(e_1, \dots, e_n) \rrbracket^\# \rho^\# \stackrel{\text{def}}{=} f^\#(\llbracket e_1 \rrbracket^\# \rho^\#, \dots, \llbracket e_n \rrbracket^\# \rho^\#)$$

Correction

- **Prop.** Supposons: pour chaque opération $\dot{f}$ ($\dot{+}$, $\dot{-}$, $\dot{n}$ par exemple) on a une approximation $f^\#$ de sa sémantique [concrète] f .
- Ceci permet de définir une **sémantique abstraite** $\llbracket e \rrbracket^\# \rho^\#$ par
$$\llbracket \dot{f}(e_1, \dots, e_n) \rrbracket^\# \rho^\# \stackrel{\text{def}}{=} f^\#(\llbracket e_1 \rrbracket^\# \rho^\#, \dots, \llbracket e_n \rrbracket^\# \rho^\#)$$
- Alors, si $\forall x, \rho(x) \in \gamma(\rho^\#(x))$, on a
$$\llbracket e \rrbracket \rho \in \gamma(\llbracket e \rrbracket^\# \rho^\#) \quad (\text{Preuve: réc. sur } e)$$

Une question de précision

- Non, en général $\llbracket e \rrbracket^{\#} \rho^{\#}$ n'est **pas** la meilleure approximation de $\llbracket e \rrbracket \rho$
- Sur l'exemple des signes,
$$\llbracket 3+(-3) \rrbracket^{\#} \rho^{\#} = '+' \# '-' = \top$$
mais la meilleure approximation était '0'

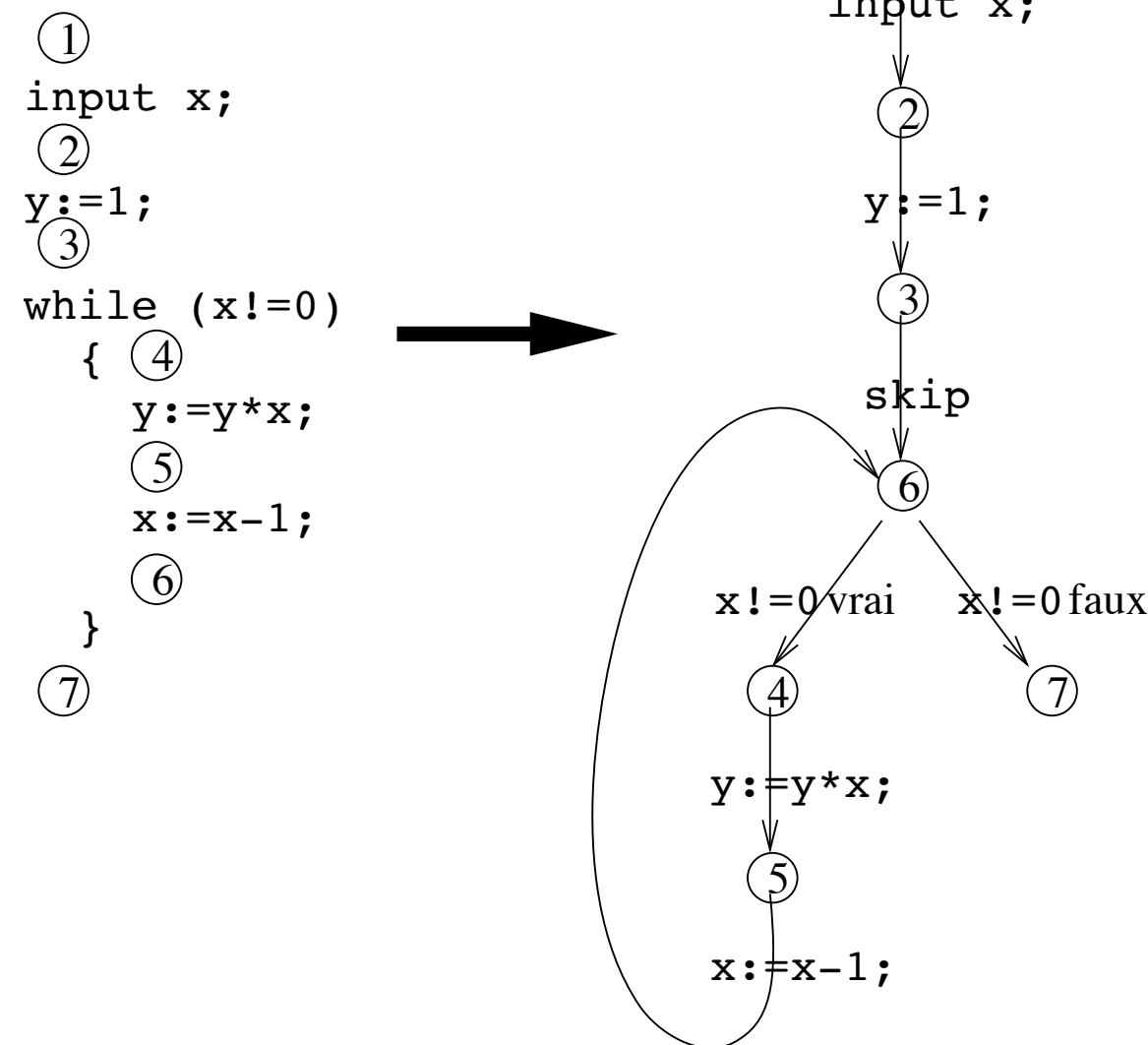
Les commandes

Sémantique abstraite des commandes

- La sémantique (abstraite) des expressions n'est pas le point délicat
- ... mais celle des commandes, en particulier des **boucles while**

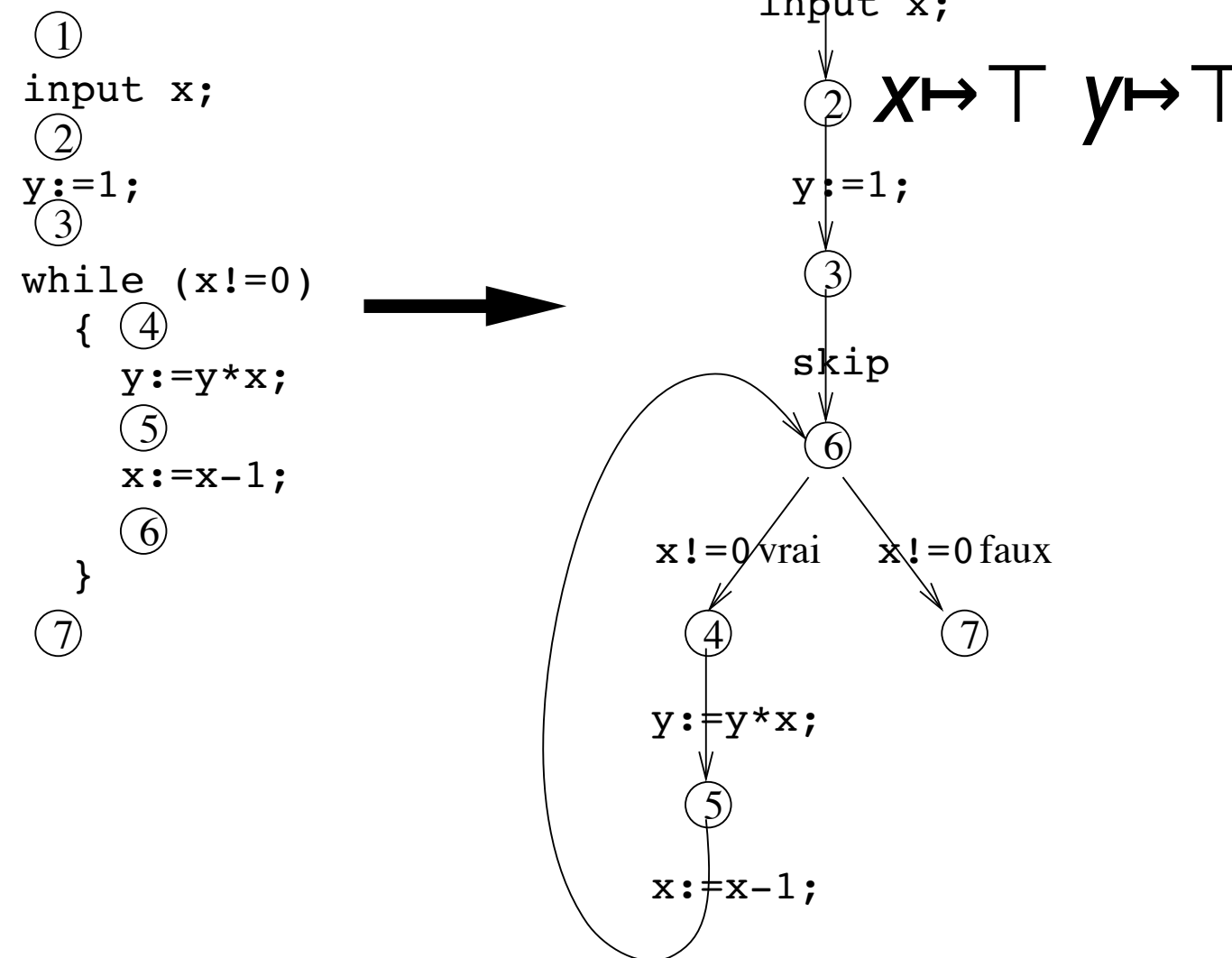
Exemple

- En pratique on analyse des graphes de flot de contrôle (CFG)



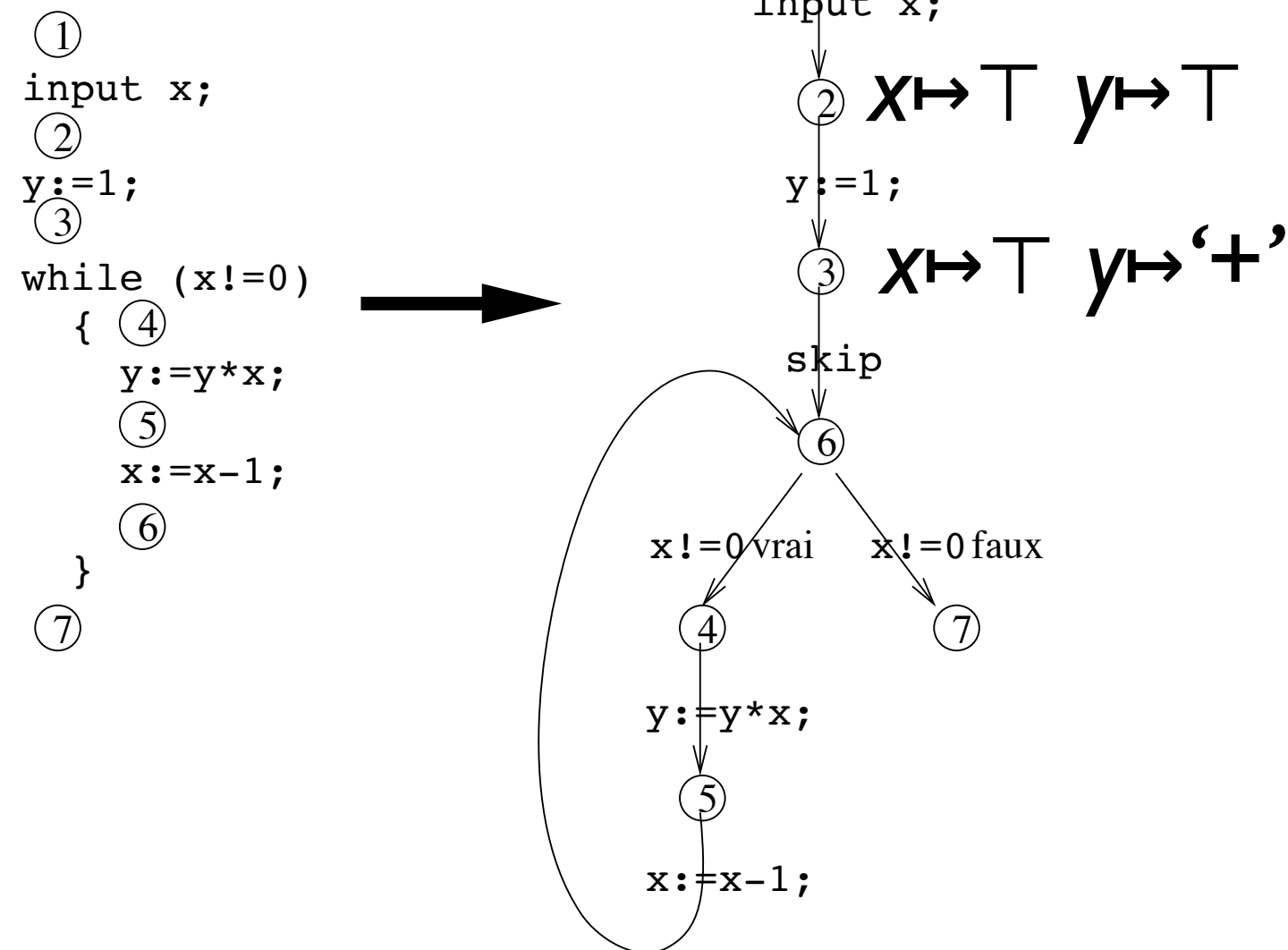
Exemple

- En pratique on analyse des graphes de flot de contrôle (CFG)



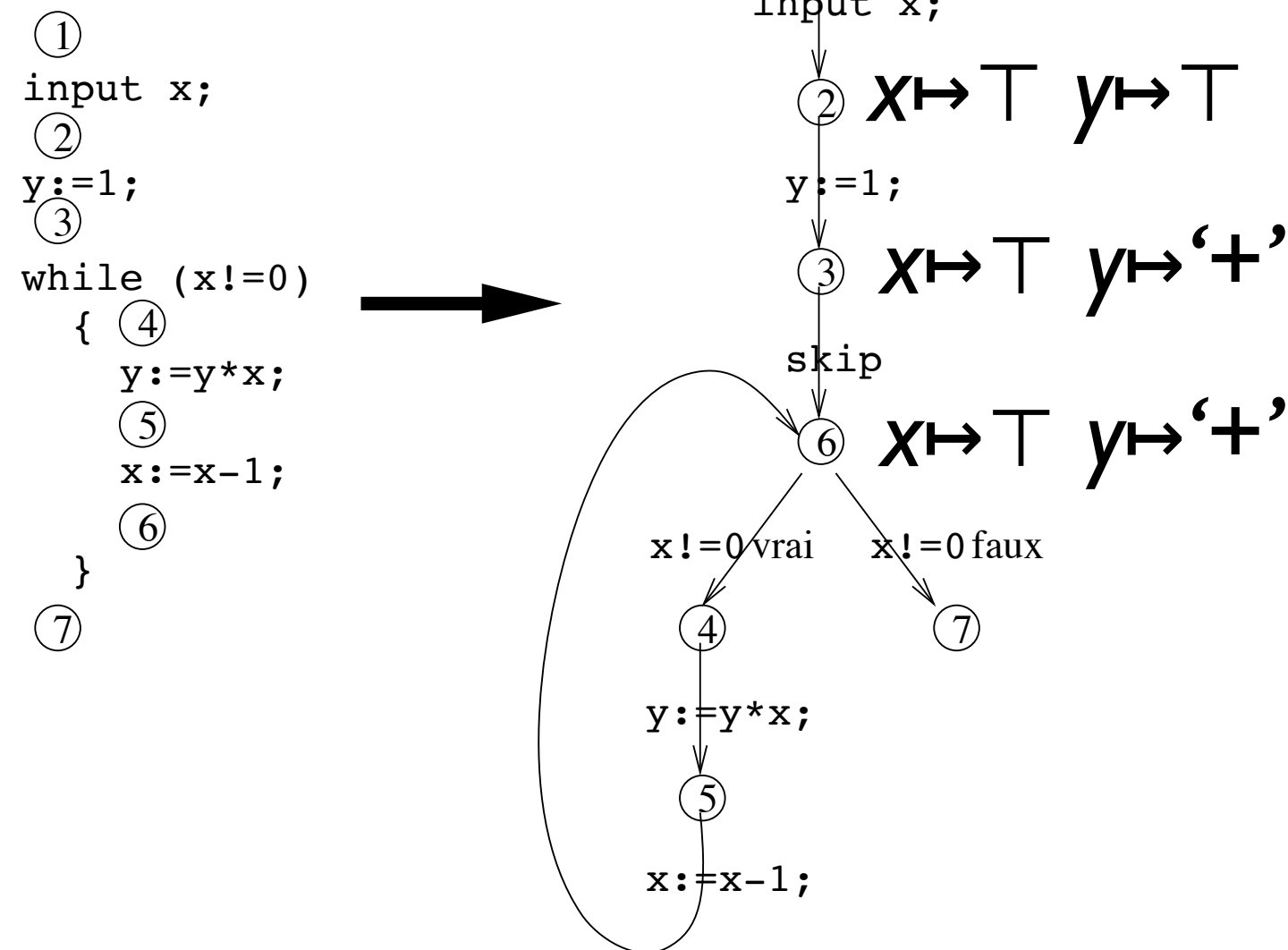
Exemple

- En pratique on analyse des graphes de flot de contrôle (CFG)



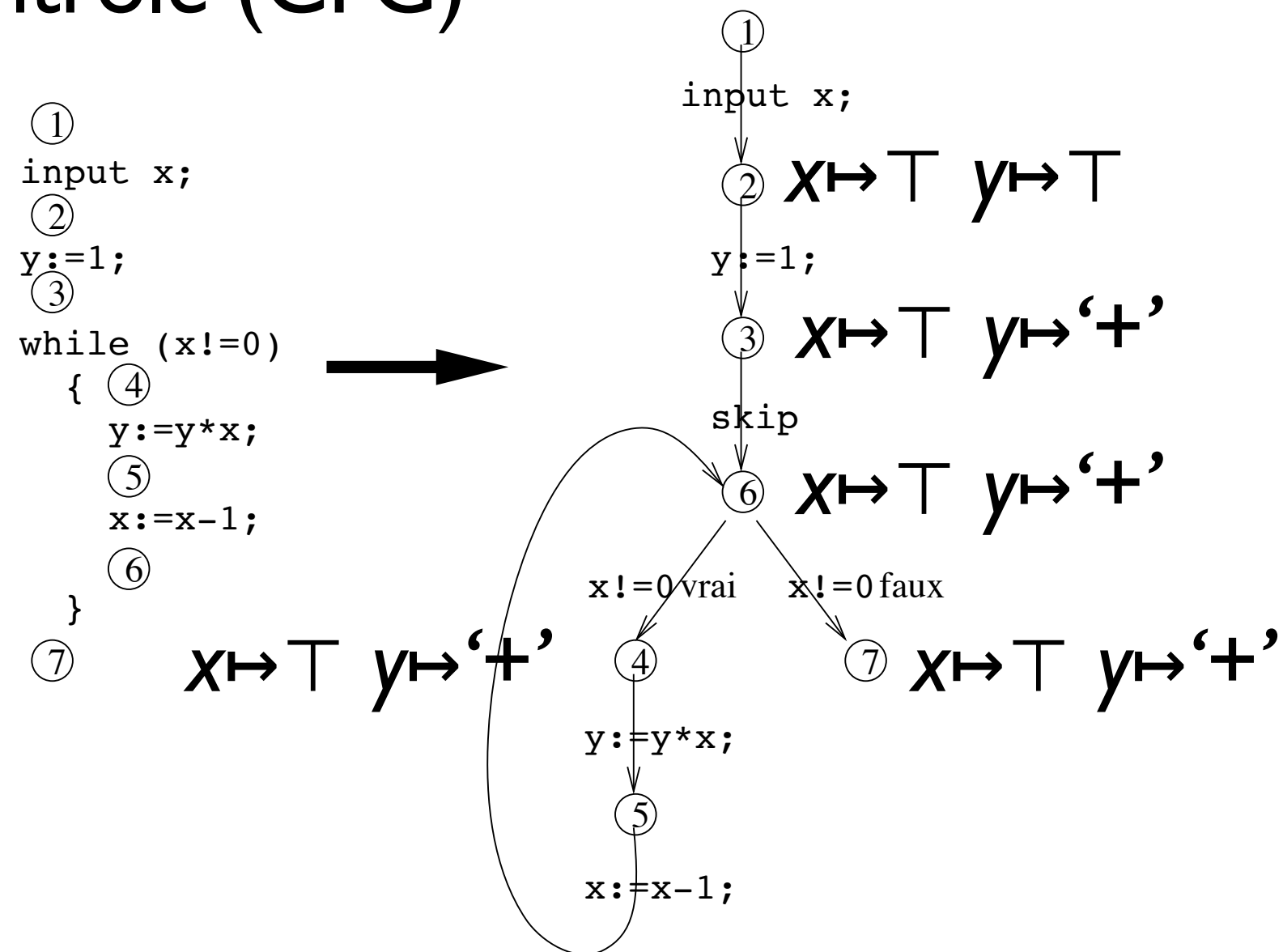
Exemple

- En pratique on analyse des graphes de flot de contrôle (CFG)



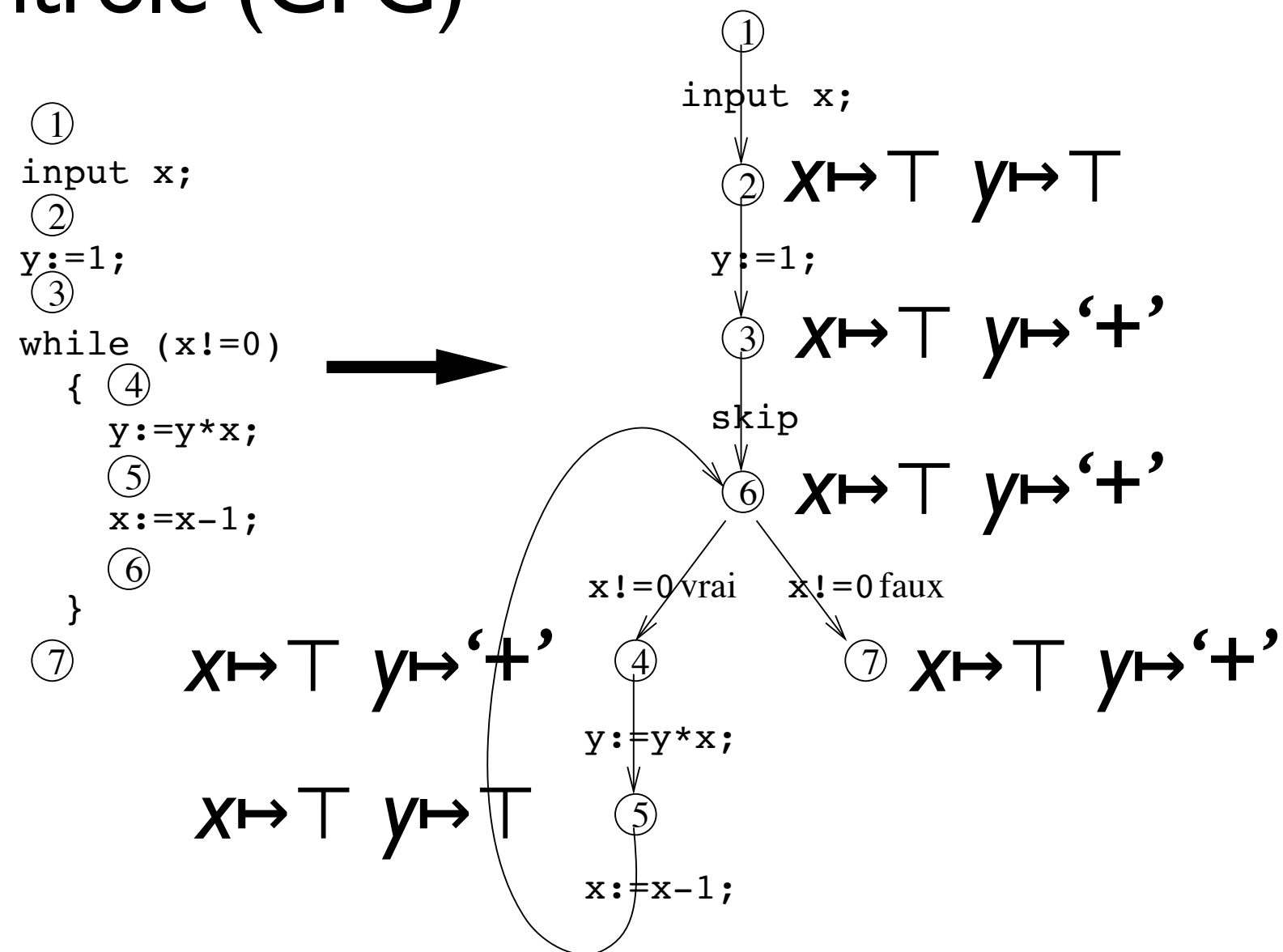
Exemple

- En pratique on analyse des graphes de flot de contrôle (CFG)



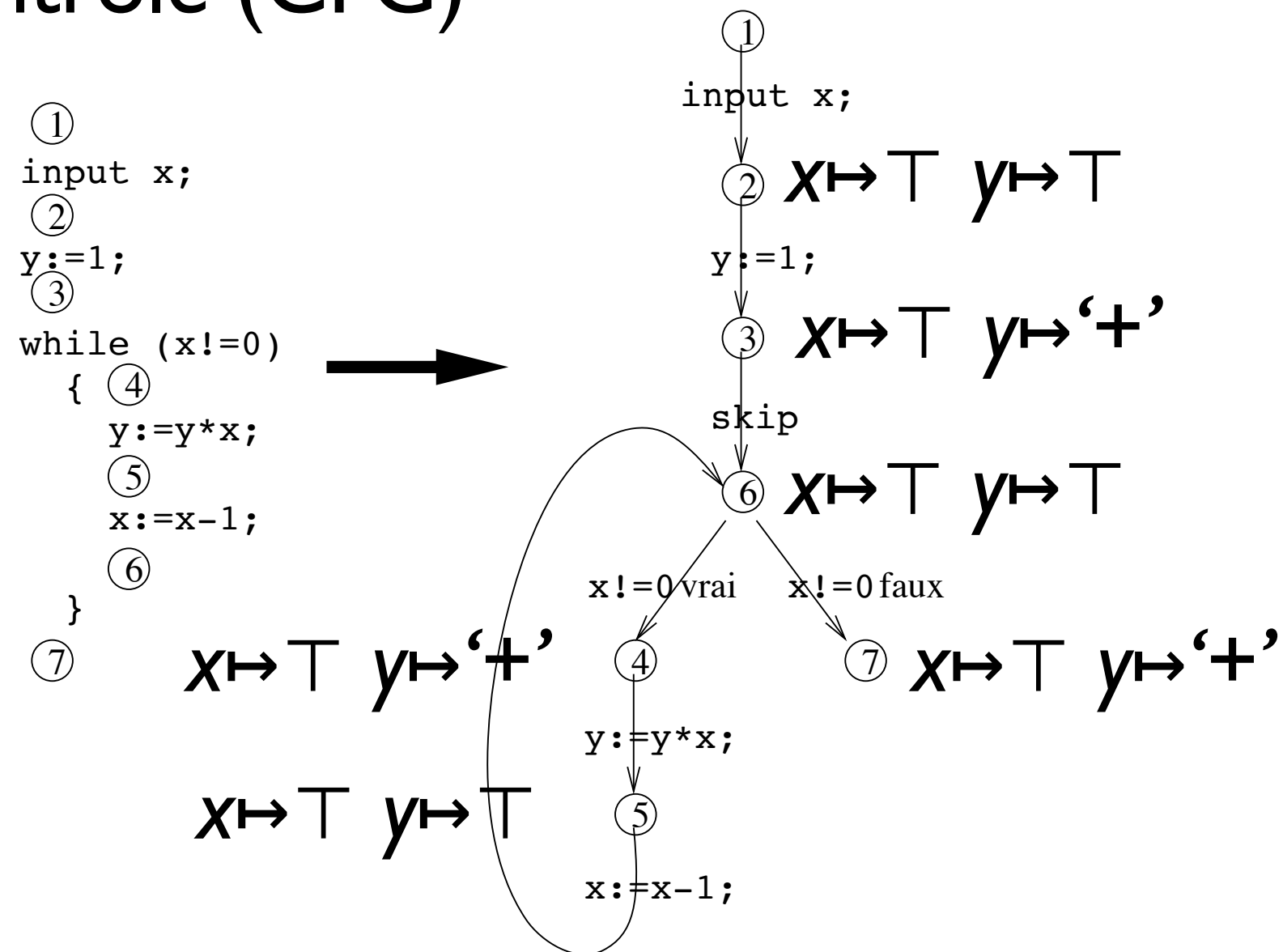
Exemple

- En pratique on analyse des graphes de flot de contrôle (CFG)



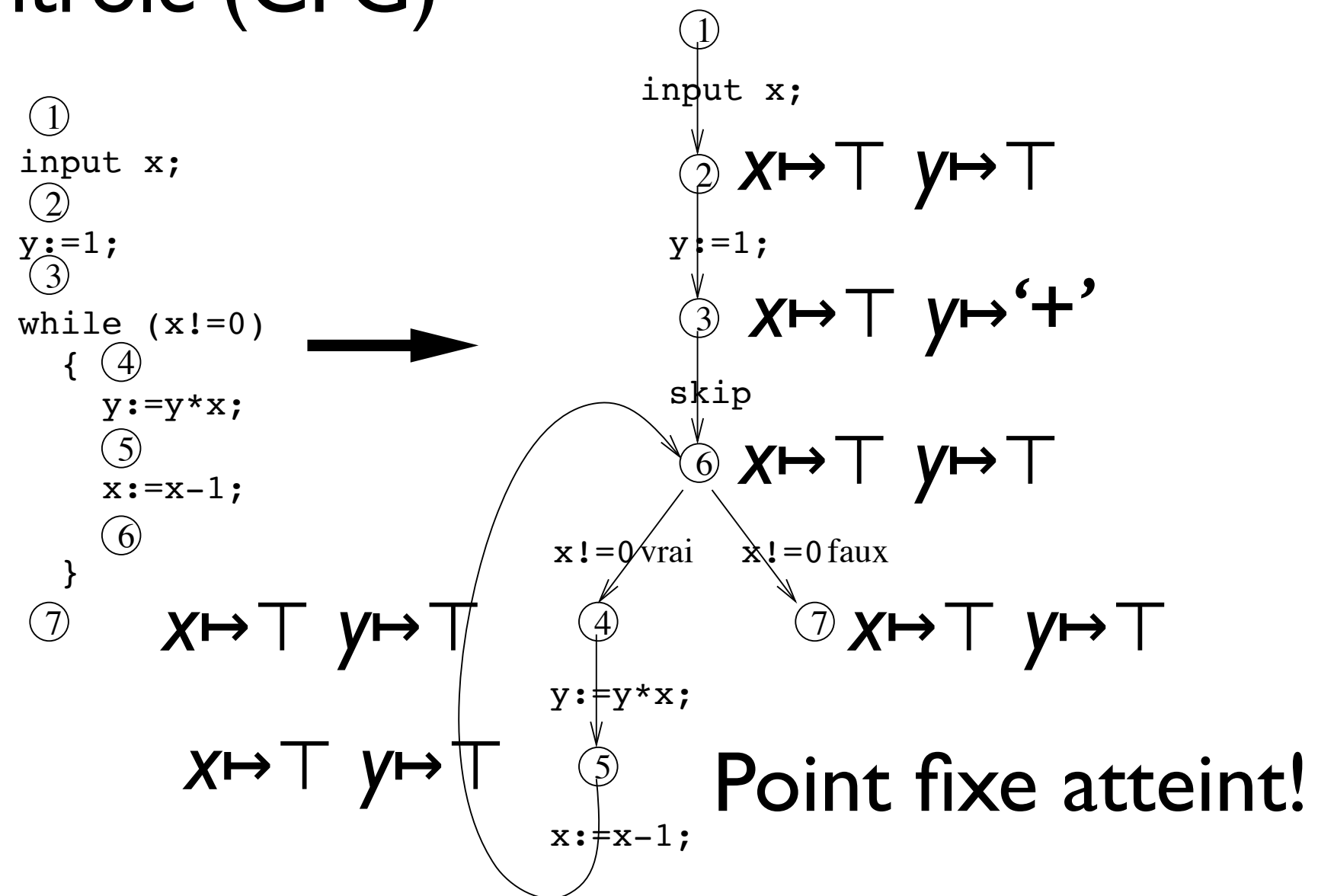
Exemple

- En pratique on analyse des graphes de flot de contrôle (CFG)



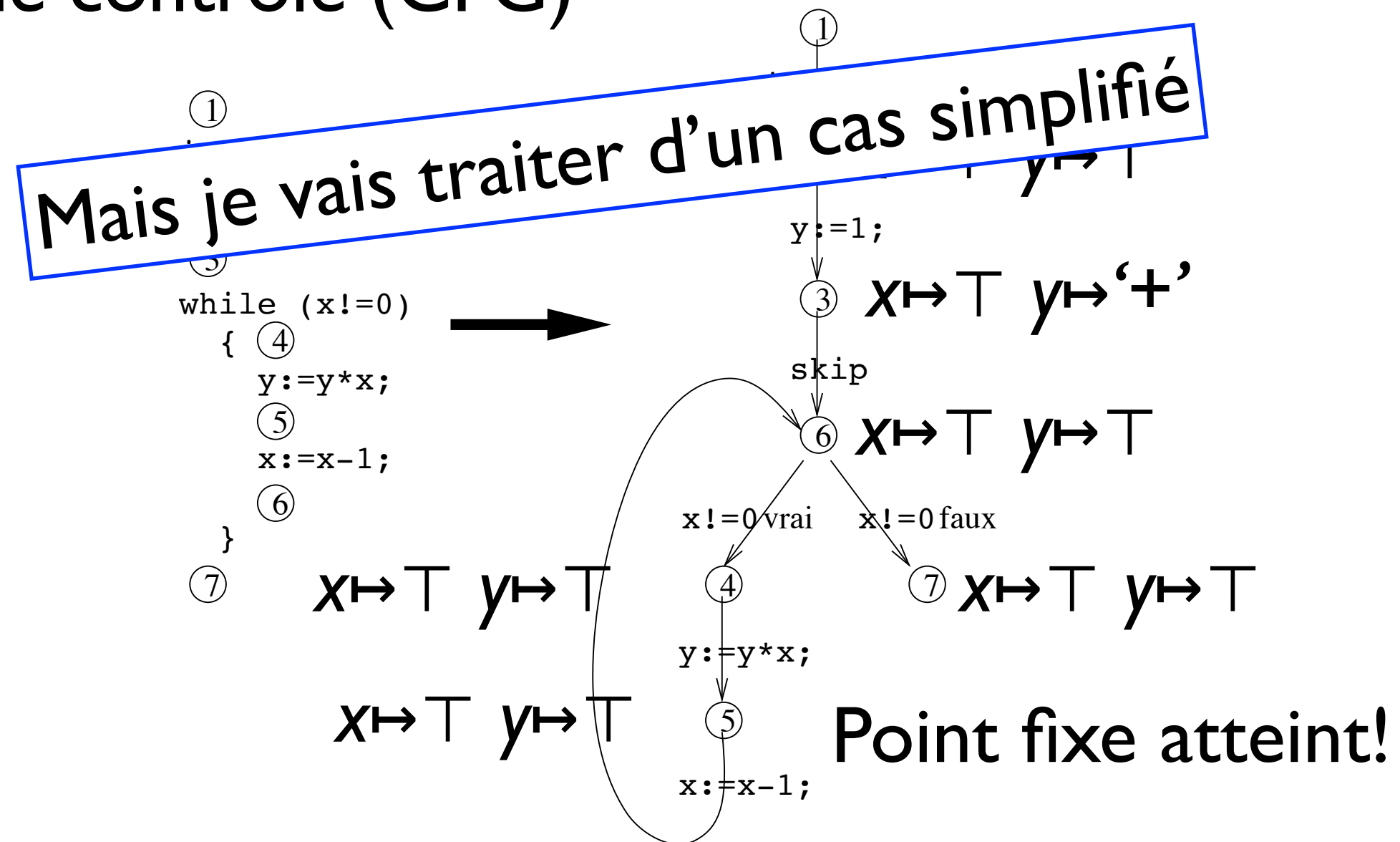
Exemple

- En pratique on analyse des graphes de flot de contrôle (CFG)



Exemple

- En pratique on analyse des graphes de flot de contrôle (CFG)



Sémantique abstraite

(exemple, style dénotationnel)

- Soit $L^\#$ un treillis complet
(de valeurs abstraites),
 $\text{Env}^\# = \text{Var} \rightarrow L^\#$
(treillis complet aussi)

Sémantique abstraite

(exemple, style dénotationnel)

- Soit $L^\#$ un treillis complet
(de valeurs abstraites),
 $\text{Env}^\# = \text{Var} \rightarrow L^\#$
(treillis complet aussi)

Envoie chaque variable vers
(une approximation de)
l'ensemble de ses valeurs possibles

Sémantique abstraite

(exemple, style dénotationnel)

- Soit $L^\#$ un treillis complet
(de valeurs abstraites),
 $\text{Env}^\# = \text{Var} \rightarrow L^\#$
(treillis complet aussi)
- $\llbracket \text{skip} \rrbracket^\# \rho^\# = \rho^\#$

Envoie chaque variable vers
(une approximation de)
l'ensemble de ses valeurs possibles

Sémantique abstraite

(exemple, style dénotationnel)

- Soit $L^\#$ un treillis complet
(de valeurs abstraites),
 $\text{Env}^\# = \text{Var} \rightarrow L^\#$
(treillis complet aussi)

Envoie chaque variable vers
(une approximation de)
l'ensemble de ses valeurs possibles

- $\llbracket \text{skip} \rrbracket^\# \rho^\# = \rho^\#$

Les valeurs de x sont celles **avant**
union celles **après** l'affectation

- $\llbracket x=e \rrbracket^\# \rho^\# = \rho^\# [x \mapsto \llbracket e \rrbracket^\# \rho^\# \vee \rho^\#(x)]$

Sémantique abstraite

(exemple, style dénotationnel)

- Soit $L^\#$ un treillis complet
(de valeurs abstraites),
 $\text{Env}^\# = \text{Var} \rightarrow L^\#$
(treillis complet aussi)

Envoie chaque variable vers
(une approximation de)
l'ensemble de ses valeurs possibles

- $\llbracket \text{skip} \rrbracket^\# \rho^\# = \rho^\#$
- $\llbracket x=e \rrbracket^\# \rho^\# = \rho^\# [x \mapsto \llbracket e \rrbracket^\# \rho^\# \vee \rho^\#(x)]$
- $\llbracket \text{if } e \text{ then } c \text{ else } c' \rrbracket^\# \rho^\# = \llbracket c \rrbracket^\# \rho^\# \vee \llbracket c' \rrbracket^\# \rho^\#$

Les valeurs de x sont celles **avant**
union celles **après** l'affectation

Sémantique abstraite

(exemple, style dénotationnel)

- Soit $L^\#$ un treillis complet
(de valeurs abstraites),
 $\text{Env}^\# = \text{Var} \rightarrow L^\#$
(treillis complet aussi)

Envoie chaque variable vers
(une approximation de)
l'ensemble de ses valeurs possibles

- $\llbracket \text{skip} \rrbracket^\# \rho^\# = \rho^\#$

Les valeurs de x sont celles **avant**
union celles **après** l'affectation

- $\llbracket x=e \rrbracket^\# \rho^\# = \rho^\# [x \mapsto \llbracket e \rrbracket^\# \rho^\# \vee \rho^\#(x)]$

- $\llbracket \text{if } e \text{ then } c \text{ else } c' \rrbracket^\# \rho^\# = \llbracket c \rrbracket^\# \rho^\# \vee \llbracket c' \rrbracket^\# \rho^\#$

- $\llbracket \text{while } e \text{ do } c \rrbracket^\# \rho^\# = \text{lfp}_{\rho^\#} (\llbracket c \rrbracket^\#)$

Opérateur « plus petit point fixe
au-dessus de $q^\#$ ». Qu'est-ce?

lfp_v

- $f: L^\# \rightarrow L^\#$ est **inflationnaire** ssi $f(x) \geq x$
- **Thm:** Soit $L^\#$ un treillis complet.
Si $f: L^\# \rightarrow L^\#$ est monotone+inflationnaire,
pour tout $V \in L^\#$, f a un plus petit point fixe
au-dessus de V . On le note $\text{lfp}_V(f)$.
(Note: monotonie pas nécessaire [Bourbaki-Witt])
- Deux démonstrations (et il y en a d'autres!)

Points fixes au-dessus de V (si vous ne connaissez pas Bourbaki-Witt)

- $\uparrow V$ est un treillis complet:

- les sups des familles $\neq \emptyset$ sont comme dans $L^\#$
- le sup de $\emptyset$ est V

Thm: Soit $L^\#$ un treillis complet. Si $f: L^\# \rightarrow L^\#$ est monotone+inflationnaire, pour tout $V \in L^\#$, f a un plus petit point fixe **au-dessus de V** . On le note $\text{lfp}_V(f)$.

Points fixes au-dessus de V (si vous ne connaissez pas Bourbaki-Witt)

- $\uparrow V$ est un treillis complet:

- les sups des familles $\neq \emptyset$ sont comme dans $L^\#$
- le sup de $\emptyset$ est V

- Comme f inflationnaire, $f|_{\uparrow V}$ va de $\uparrow V$ dans $\uparrow V$:
si $V \leq x$ alors $V \leq x \leq f(x)$

Thm: Soit $L^\#$ un treillis complet. Si $f: L^\# \rightarrow L^\#$ est monotone + inflationnaire, pour tout $V \in L^\#$, f a un plus petit point fixe **au-dessus de V** . On le note $\text{lfp}_V(f)$.

Points fixes au-dessus de V (si vous ne connaissez pas Bourbaki-Witt)

Thm: Soit $L^\#$ un treillis complet. Si $f: L^\# \rightarrow L^\#$ est monotone+inflationnaire, pour tout $V \in L^\#$, f a un plus petit point fixe **au-dessus de V** . On le note $\text{lfp}_V(f)$.

- $\uparrow V$ est un treillis complet:
 - les sups des familles $\neq \emptyset$ sont comme dans $L^\#$
 - le sup de $\emptyset$ est V
- Comme f inflationnaire, $f|_{\uparrow V}$ va de $\uparrow V$ dans $\uparrow V$:
si $V \leq x$ alors $V \leq x \leq f(x)$
- Par Tarski, $f|_{\uparrow V}$ a un plus petit point fixe x_0 dans $\uparrow V$

Points fixes au-dessus de V (si vous ne connaissez pas Bourbaki-Witt)

Thm: Soit $L^\#$ un treillis complet. Si $f: L^\# \rightarrow L^\#$ est monotone+inflationnaire, pour tout $V \in L^\#$, f a un plus petit point fixe **au-dessus de V** . On le note $\text{lfp}_V(f)$.

- $\uparrow V$ est un treillis complet:
 - les sups des familles $\neq \emptyset$ sont comme dans $L^\#$
 - le sup de $\emptyset$ est V
- Comme f inflationnaire, $f|_{\uparrow V}$ va de $\uparrow V$ dans $\uparrow V$:
si $V \leq x$ alors $V \leq x \leq f(x)$
- Par Tarski, $f|_{\uparrow V}$ a un plus petit point fixe x_0 dans $\uparrow V$
- Si x est un autre point fixe de f au-dessus de V , c'est un point fixe de $f|_{\uparrow V}$, donc $x_0 \leq x$. $\square$

2ème démonstration

- Soit $f^V(x) \stackrel{\text{def}}{=} f(x) \vee V$.

Thm: Soit $L^\#$ un treillis complet. Si $f: L^\# \rightarrow L^\#$ est monotone+inflationnaire, pour tout $V \in L^\#$, f a un plus petit point fixe **au-dessus de V** . On le note $\text{lfp}_V(f)$.

2ème démonstration

- Soit $f^V(x) \stackrel{\text{def}}{=} f(x) \vee V$.
- Les points fixes de f^V dans $L^\#$ sont les points fixes de f au-dessus de V :

Thm: Soit $L^\#$ un treillis complet. Si $f: L^\# \rightarrow L^\#$ est monotone+inflationnaire, pour tout $V \in L^\#$, f a un plus petit point fixe **au-dessus de V** . On le note $\text{lfp}_V(f)$.

2ème démonstration

Thm: Soit $L^\#$ un treillis complet. Si $f: L^\# \rightarrow L^\#$ est monotone+inflationnaire, pour tout $V \in L^\#$, f a un plus petit point fixe **au-dessus de V** .
On le note $\text{lfp}_V(f)$.

- Soit $f^V(x) \stackrel{\text{def}}{=} f(x) \vee V$.
- Les points fixes de f^V dans $L^\#$ sont les points fixes de f au-dessus de V :
- Si $x = f^V(x)$, alors $x = f(x) \vee V$ donc
 - $x \geq f(x)$... donc $x = f(x)$ puisque f inflationnaire
 - $x \geq V$

2ème démonstration

Thm: Soit $L^\#$ un treillis complet. Si $f: L^\# \rightarrow L^\#$ est monotone+inflationnaire, pour tout $V \in L^\#$, f a un plus petit point fixe **au-dessus de V** .
On le note $\text{lfp}_V(f)$.

- Soit $f^V(x) \stackrel{\text{def}}{=} f(x) \vee V$.
- Les points fixes de f^V dans $L^\#$ sont les points fixes de f au-dessus de V :
 - Si $x = f^V(x)$, alors $x = f(x) \vee V$ donc
 - $x \geq f(x)$... donc $x = f(x)$ puisque f inflationnaire
 - $x \geq V$
 - Si $x = f(x)$ et $x \geq V$, alors
$$x \leq f(x) \leq f^V(x) = f(x) \vee V = x \vee V = x$$

2ème démonstration

Thm: Soit $L^\#$ un treillis complet. Si $f: L^\# \rightarrow L^\#$ est monotone+inflationnaire, pour tout $V \in L^\#$, f a un plus petit point fixe **au-dessus de V** .
On le note $\text{lfp}_V(f)$.

- Soit $f^V(x) \stackrel{\text{def}}{=} f(x) \vee V$.
- Les points fixes de f^V dans $L^\#$ sont les points fixes de f au-dessus de V :
 - Si $x = f^V(x)$, alors $x = f(x) \vee V$ donc
 - $x \geq f(x)$... donc $x = f(x)$ puisque f inflationnaire
 - $x \geq V$
 - Si $x = f(x)$ et $x \geq V$, alors
$$x \leq f(x) \leq f^V(x) = f(x) \vee V = x \vee V = x$$
- Donc $\text{lfp}_V(f)$ existe et vaut $\text{lfp}(f^V)$. $\square$

Correction

- Dans le cas de Imp:

$$\begin{aligned} (x := e \cdot C, \rho) &\rightarrow (C, \rho[x \mapsto \llbracket e \rrbracket \rho]) & (3) \\ (\text{skip} \cdot C, \rho) &\rightarrow (C, \rho) & (4) \\ (c_1; c_2 \cdot C, \rho) &\rightarrow (c_1 \cdot c_2 \cdot C, \rho) & (5) \\ (\text{if } e \text{ then } c_1 \text{ else } c_2 \cdot C, \rho) &\rightarrow (c_1 \cdot C, \rho) \quad \text{si } \llbracket e \rrbracket \rho \neq 0 & (6) \\ (\text{if } e \text{ then } c_1 \text{ else } c_2 \cdot C, \rho) &\rightarrow (c_2 \cdot C, \rho) \quad \text{si } \llbracket e \rrbracket \rho = 0 & (7) \\ (\text{while } e \text{ do } c \cdot C, \rho) &\rightarrow (c \cdot \text{while } e \text{ do } c \cdot C, \rho) \quad \text{si } \llbracket e \rrbracket \rho \neq 0 & (8) \\ (\text{while } e \text{ do } c \cdot C, \rho) &\rightarrow (C, \rho) \quad \text{si } \llbracket e \rrbracket \rho = 0 & (9) \end{aligned}$$

- **Prop:** Soit $L^\#$ un treillis complet, et $\alpha \dashv \gamma$ entre $L^\#$ et $L \stackrel{\text{def}}{=} \mathbb{P}(\text{Val})$.
Si $\rho(x) \in \gamma(\rho^\#(x))$ pour tout x ,
et si $(c.C, \rho) \rightarrow^* (c'.C', \rho')$
alors $\rho'(x) \in \gamma((\llbracket c;C \rrbracket^\# \rho^\#)(x))$ pour tout x .
- **Dém.:** réc. sur longueur du calcul $\rightarrow^*$
+ analyse de cas (exercice!)

Calcul de la sémantique abstraite

- On calcule $\llbracket c \rrbracket^\# \rho^\#$ par récurrence sur c
- Seul cas intéressant: $\llbracket \text{while } e \text{ do } c \rrbracket^\# \rho^\#$:
- $\llbracket \text{while } e \text{ do } c \rrbracket^\# \rho^\# = \text{lfp}_{\rho^\#} (\llbracket c \rrbracket^\#)$:
comment le calculer?

$$\llbracket \text{skip} \rrbracket^\# \rho^\# = \rho^\#$$

$$\llbracket x=e \rrbracket^\# \rho^\# = \rho^\# [x \mapsto \llbracket e \rrbracket^\# \rho^\# \vee \rho^\#(x)]$$

$$\llbracket \text{if } e \text{ then } c \text{ else } c' \rrbracket^\# \rho^\# = \llbracket c \rrbracket^\# \rho^\# \vee \llbracket c' \rrbracket^\# \rho^\#$$

$$\llbracket \text{while } e \text{ do } c \rrbracket^\# \rho^\# = \text{lfp}_{\rho^\#} (\llbracket c \rrbracket^\#)$$

Calcul de la sémantique abstraite

- On calcule $\llbracket c \rrbracket^\# \rho^\#$ par récurrence sur c
- Seul cas intéressant: $\llbracket \text{while } e \text{ do } c \rrbracket^\# \rho^\#$:
- $\llbracket \text{while } e \text{ do } c \rrbracket^\# \rho^\# = \text{lfp}_{\rho^\#} (\llbracket c \rrbracket^\#)$:
comment le calculer?

$$\llbracket \text{skip} \rrbracket^\# \rho^\# = \rho^\#$$

$$\llbracket x=e \rrbracket^\# \rho^\# = \rho^\# [x \mapsto \llbracket e \rrbracket^\# \rho^\# \vee \rho^\#(x)]$$

$$\llbracket \text{if } e \text{ then } c \text{ else } c' \rrbracket^\# \rho^\# = \llbracket c \rrbracket^\# \rho^\# \vee \llbracket c' \rrbracket^\# \rho^\#$$

$$\llbracket \text{while } e \text{ do } c \rrbracket^\# \rho^\# = \text{lfp}_{\rho^\#} (\llbracket c \rrbracket^\#)$$

Oh, oui, $\llbracket c \rrbracket^\#$ est monotone et
inflationnaire (réc. sur c)

Condition de chaîne croissante

- $\llbracket \text{while } e \text{ do } c \rrbracket^\# \rho^\# = \text{lfp}_{\rho^\#} (\llbracket c \rrbracket^\#)$

Condition de chaîne croissante

- $\llbracket \text{while } e \text{ do } c \rrbracket^\# \rho^\# = \text{lfp}_{\rho^\#} (\llbracket c \rrbracket^\#)$
- Si $L^\#$ a **la condition de chaîne croissante**,
(toute chaîne $y_0^\# \leq^\# y_1^\# \leq^\# \dots \leq^\# y_n^\# \leq^\# \dots$ stabilise:
 $\exists n_0, \forall n \geq n_0, y_n^\# = y_{n_0}^\#$)

Condition de chaîne croissante

C'est le cas du treillis des signes (toute chaîne croissante stricte est de hauteur ≤ 3)

- $\llbracket \text{while } e \text{ do } c \rrbracket^\# \rho^\# = \text{lfp}_{\rho^\#} (\llbracket c \rrbracket^\#)$
- Si $L^\#$ a **la condition de chaîne croissante**,
(toute chaîne $y_0^\# \leq^\# y_1^\# \leq^\# \dots \leq^\# y_n^\# \leq^\# \dots$ stabilise:
 $\exists n_0, \forall n \geq n_0, y_n^\# = y_{n_0}^\#$)

Condition de chaîne croissante

C'est le cas du treillis des signes (toute chaîne croissante stricte est de hauteur ≤ 3)

- $\llbracket \text{while } e \text{ do } c \rrbracket^\# \rho^\# = \text{lfp}_{\rho^\#} (\llbracket c \rrbracket^\#)$
- Si $L^\#$ a **la condition de chaîne croissante**,
(toute chaîne $y_0^\# \leq^\# y_1^\# \leq^\# \dots \leq^\# y_n^\# \leq^\# \dots$ stabilise:
 $\exists n_0, \forall n \geq n_0, y_n^\# = y_{n_0}^\#$)
- alors $\text{lfp}_{\rho^\#} (\llbracket c \rrbracket^\#) = \sup_n (\llbracket c \rrbracket^\#)^n (\rho^\#)$
et ce sup est **atteint**.

Condition de chaîne croissante

- $\llbracket \text{while } e \text{ do } c \rrbracket^\# \rho^\# = \text{lfp}_{\rho^\#} (\llbracket c \rrbracket^\#)$
- Si $L^\#$ a **la condition de chaîne croissante**, explicitement, la chaîne

$$\rho^\# \stackrel{\text{def}}{=} \rho_0^\# \leq^\# \rho_1^\# \leq^\# \dots \leq^\# \rho_n^\# \leq^\# \dots$$

$$\text{où } \rho_{n+1}^\# \stackrel{\text{def}}{=} \llbracket c \rrbracket^\# \rho_n^\#$$

stabilise (disons à n)

- alors $\llbracket \text{while } e \text{ do } c \rrbracket^\# \rho^\# = \rho_n^\#$

Condition de chaîne croissante

- $\llbracket \text{while } e \text{ do } c \rrbracket^\# \rho^\# = \text{lfp}_{\rho^\#} (\llbracket c \rrbracket^\#)$
- Si $L^\#$ a **la condition de chaîne croissante**, explicitement, la chaîne

$$\rho^\# \stackrel{\text{def}}{=} \rho_0^\# \leq^\# \rho_1^\# \leq^\# \dots \leq^\# \rho_n^\# \leq^\# \dots$$

où $\rho_{n+1}^\# \stackrel{\text{def}}{=} \llbracket c \rrbracket^\# \rho_n^\#$
stabilise (disons à n)

Mais comment sait-on qu'on a atteint l'étape où la chaîne se stabilise?

- alors $\llbracket \text{while } e \text{ do } c \rrbracket^\# \rho^\# = \rho_n^\#$

Condition de chaîne croissante

- $\llbracket \text{while } e \text{ do } c \rrbracket^\# \rho^\# = \text{lfp}_{\rho^\#} (\llbracket c \rrbracket^\#)$
- Si $L^\#$ a **la condition de chaîne croissante**, explicitement, la chaîne

$$\rho^\# \stackrel{\text{def}}{=} \rho_0^\# \leq^\# \rho_1^\# \leq^\# \dots \leq^\# \rho_n^\# \leq^\# \dots$$

où $\rho_{n+1}^\# \stackrel{\text{def}}{=} \llbracket c \rrbracket^\# \rho_n^\#$
stabilise (disons à n)

Mais comment sait-on qu'on a atteint l'étape où la chaîne se stabilise?

- alors $\llbracket \text{while } e \text{ do } c \rrbracket^\# \rho^\# = \rho_n^\#$

En principe, la chaîne pourrait « bégayer »: s'arrêter pendant quelques étapes puis redémarrer

Terminaison

- En général, soit f monotone inflationnaire sur un treillis complet avec la c.c.c.,

$$x_0 \leq x_1 \leq \dots \leq x_n \leq \dots$$

$$\text{où } x_{n+1} \stackrel{\text{def}}{=} f(x_n)$$

Terminaison

- En général, soit f monotone inflationnaire sur un treillis complet avec la c.c.c.,

$$x_0 \leq x_1 \leq \dots \leq x_n \leq \dots$$

$$\text{où } x_{n+1} \stackrel{\text{def}}{=} f(x_n)$$

- Cette chaîne stabilise
au premier indice n tel que $x_{n+1} = x_n$

Terminaison

- En général, soit f monotone inflationnaire sur un treillis complet avec la c.c.c.,

$$x_0 \leq x_1 \leq \dots \leq x_n \leq \dots$$

où $x_{n+1} \stackrel{\text{def}}{=} f(x_n)$

Donc pas de bégaiement pour cette forme particulière de chaîne croissante

- Cette chaîne stabilise
au premier indice n tel que $x_{n+1} = x_n$

Terminaison

- En général, soit f monotone inflationnaire sur un treillis complet avec la c.c.c.,

$$x_0 \leq x_1 \leq \dots \leq x_n \leq \dots$$
$$\text{où } x_{n+1} \stackrel{\text{def}}{=} f(x_n)$$

Donc pas de bégaiement pour cette forme particulière de chaîne croissante

- Cette chaîne stabilise
au premier indice n tel que $x_{n+1} = x_n$
- En effet, $x_{n+2} = f(x_{n+1}) = f(x_n) = x_{n+1}$
 $x_{n+3} = f(x_{n+2}) = f(x_{n+1}) = x_{n+2}$
etc.

Cas plus complexes

- On sait faire aussi de l'analyse statique avec des treillis complets n'ayant **pas** la c.c.c.
- Exemple: treillis des intervalles d'entiers $[m,n]$, ordonné par inclusion
- Approximation par excès de points fixes et **élargissements** [CousotCousot77], **itération sur les politiques** [GoubaultPutot05], etc.

Conclusion

- Il y aurait encore beaucoup à dire, mais on va s'arrêter là!

Annexe

Galois et points fixes

- **Thm:** Soit L treillis complet, $f : L \rightarrow L$ monotone, et $L : \alpha \dashv \gamma : L^\#$, alors
$$\text{lfp}(f) \leq \gamma(\text{lfp}^\#(f^\#)) \text{ où } f^\# = \alpha \circ f \circ \gamma$$

Galois et points fixes

- **Thm:** Soit L treillis complet, $f : L \rightarrow L$ monotone, et $L : \alpha \dashv \gamma : L^\#$, alors
$$\text{lfp}(f) \leq \gamma(\text{lfp}^\#(f^\#)) \text{ où } f^\# = \alpha \circ f \circ \gamma$$
- **Dém.:** $\text{lfp}^\#(f^\#) = f^\#(\text{lfp}^\#(f^\#))$

Galois et points fixes

- **Thm:** Soit L treillis complet, $f : L \rightarrow L$ monotone, et $L : \alpha \dashv \gamma : L^\#$, alors
$$\text{lfp}(f) \leq \gamma(\text{lfp}^\#(f^\#)) \text{ où } f^\# = \alpha \circ f \circ \gamma$$
- **Dém.:** $\text{lfp}^\#(f^\#) = f^\#(\text{lfp}^\#(f^\#))$
donc $\alpha(f(\gamma(\text{lfp}^\#(f^\#)))) \leq \text{lfp}^\#(f^\#)$ (en fait =)

Galois et points fixes

- **Thm:** Soit L treillis complet, $f : L \rightarrow L$ monotone, et $L : \alpha \dashv \gamma : L^\#$, alors
$$\text{lfp}(f) \leq \gamma(\text{lfp}^\#(f^\#)) \text{ où } f^\# = \alpha \circ f \circ \gamma$$
- **Dém.:** $\text{lfp}^\#(f^\#) = f^\#(\text{lfp}^\#(f^\#))$
donc $\alpha(f(\gamma(\text{lfp}^\#(f^\#)))) \leq \text{lfp}^\#(f^\#)$ (en fait =)
donc $f(\gamma(\text{lfp}^\#(f^\#))) \leq \gamma(\text{lfp}^\#(f^\#))$ ($\alpha \dashv \gamma$)

Galois et points fixes

- **Thm:** Soit $L, L^\#$ treillis complet, $f: L \rightarrow L$ monotone, et $\alpha: L \rightarrow L^\#$, $\gamma: L^\# \rightarrow L$, alors
$$\text{lfp}(f) \leq \gamma(\text{lfp}^\#(f^\#)) \text{ où } f^\# = \alpha \circ f \circ \gamma$$
- **Dém.:** $\text{lfp}^\#(f^\#) = f^\#(\text{lfp}^\#(f^\#))$
donc $\alpha(f(\gamma(\text{lfp}^\#(f^\#)))) \leq \text{lfp}^\#(f^\#)$ (en fait =)
donc $f(\gamma(\text{lfp}^\#(f^\#))) \leq \gamma(\text{lfp}^\#(f^\#))$ ($\alpha \dashv \gamma$)
i.e., $\gamma(\text{lfp}^\#(f^\#))$ post-point fixe de f

Galois et points fixes

- **Thm:** Soit $L, L^\#$ treillis complet, $f: L \rightarrow L$ monotone, et $\alpha: L \rightarrow L^\#$, $\gamma: L^\# \rightarrow L$, alors
$$\text{lfp}(f) \leq \gamma(\text{lfp}^\#(f^\#)) \text{ où } f^\# = \alpha \circ f \circ \gamma$$
- **Dém.:** $\text{lfp}^\#(f^\#) = f^\#(\text{lfp}^\#(f^\#))$
donc $\alpha(f(\gamma(\text{lfp}^\#(f^\#)))) \leq \text{lfp}^\#(f^\#)$ (en fait =)
donc $f(\gamma(\text{lfp}^\#(f^\#))) \leq \gamma(\text{lfp}^\#(f^\#))$ ($\alpha \dashv \gamma$)
i.e., $\gamma(\text{lfp}^\#(f^\#))$ post-point fixe de f
donc $\geq$ le plus petit, qui est $\text{lfp}(f)$ (Tarski).

Galois et points fixes

- **Thm:** Soit $L, L^\#$ treillis complet, $f: L \rightarrow L$ mon.+inflationnaire, et $L: \alpha \dashv \gamma: L^\#$, alors si $V \leq \gamma(V^\#)$ et $V^\# \in \text{Im } \alpha$ on a:
$$\text{lfp}_V(f) \leq \gamma(\text{lfp}_{V^\#}^\#(f^\#)) \text{ où } f^\# = \alpha \circ f \circ \gamma$$
- **Dém.:** soit $V^\# = \alpha(V')$
 $\alpha \dashv \gamma$ se restreint à $\uparrow V': \alpha \dashv \gamma: \uparrow V^\#$
puis $\text{lfp}_V(f) \leq \text{lfp}_{V'}(f)$ (par définition de lfp_V .)

Galois et points fixes

- **Thm:** Soit $L, L^\#$ treillis complet, $f: L \rightarrow L$ mon.+inflationnaire, et $L: \alpha \dashv \gamma: L^\#$, alors si $V \leq \gamma(V^\#)$ et γ **injective** on a:
$$\text{lfp}_V(f) \leq \gamma(\text{lfp}_{V^\#}^\#(f^\#)) \text{ où } f^\# = \alpha \circ f \circ \gamma$$
- **Dém.:** il suffit de voir que α est alors surjective. En effet, on a toujours $\gamma(x^\#) = \gamma(\alpha(\gamma(x^\#)))$ (exercice).