Interprétation abstraite (les bases)

November 15, 2021

Objectif: la sûreté 1/2

Prouver que (certains) accès mémoire sont safe:

```
int main () {
  int v[10];
  v[0]=0; ✓
  return v[20]; ✗
}
```

- Ce programme a un accès illégal à un tableau.

Objectif: la sûreté 2/2

Prouver la correction (absence de bugs fonctionnels):

```
void find_mini (int a[N], int l, int u){
  unsigned int i=l;
  int b=a[l]
  while (i <= u){
    if(a[i]<b) b=a[i] ;
    i++ ;
  }
  // here b = min(a[l..u])
}
```

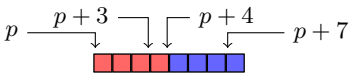
- Ce programme trouve le minimum du sous-tableau.

Objectif: la performance 1/2

Permettre le parallelisme dans une boucle:

```
void fill_array (char *p){
  unsigned int i;
  for (i=0; i<4; i++)
       *(p + i) = 0 ;
  for (i=4; i<8; i++)
       *(p + i) = 2*i ;
}
```

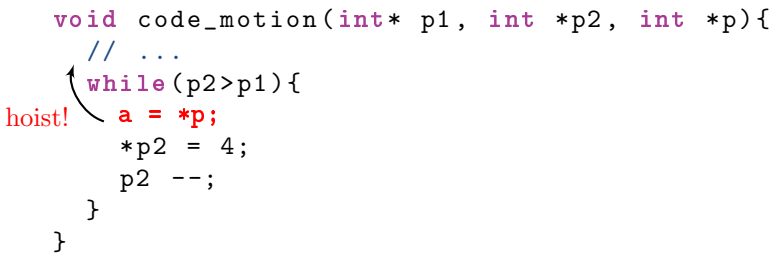
Parallel loops



- The two regions do not overlap.

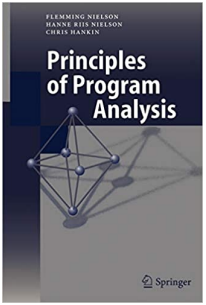
Objectif: la performance 2/2

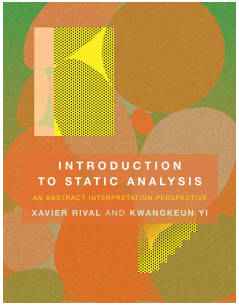
Permettre le déplacement de code:



- Si p et p_2 ne pointent pas sur la même adresse, a=*p est invariant.
- On sors l'instruction de la boucle pour économiser un `load` par itération.

Reference books





Objectifs

Compilation vs analyse de programme:

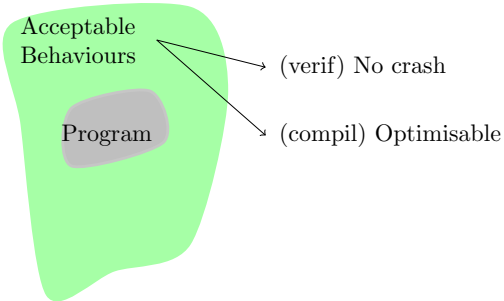
- Compilation: générer du code (en préservant la sémantique).
- Analyse de programme: découvrir des propriétés, prouver l'absence de bugs.

▶ Dans les deux cas, les programmes sont des entrées.

Remerciements: Slides basées sur du travail de L. Gonnord, D. Monniaux, D. Hirschkoff, P. Roux, ...

Prouver des propriétés (non-triviales) sur des programmes

- Idée: les programmes ont des **comportements définis mathématiquement**.
- Prouver **automatiquement** des propriétés.



Pas de recette miracle

indécidable: pas d'analyse statique "magique". Il est impossible de prouver des propriétés intéressantes:

- automatiquement
- de manière exacte
- sur des programmes non bornés.

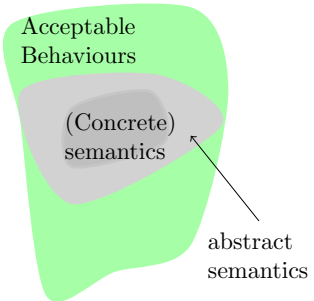
Pas de recette miracle

indécidable: pas d'analyse statique "magique". Il est ~~im~~ possible de prouver des propriétés intéressantes:

- automatiquement
- ~~de manière exacte~~ avec des faux positifs!
- sur des programmes non bornés.

▶ **Interprétation abstraite** = approximations conservatives.

Objectifs de la section



- Comportement du programme: sémantique **concrete**
- Comportements acceptables: cf. slide suivante
- Approximation du comportement du prog.: sémantique

Notre language: le "mini-while"

grammaire (abstraite):

$$
\begin{array}{rcll}
S(Smt) & ::= & x := e & \text{affectation} \\
& | & skip & \text{aucun effet} \\
& | & S_1; S_2 & \text{séquence} \\
& | & \texttt{if } b \texttt{ then } S_1 \texttt{ else } S_2 & \text{test} \\
& | & \texttt{while } b \texttt{ do } S \texttt{ done} & \text{boucle}
\end{array}
$$

$$
\begin{array}{rcll}
e & ::= & x \mid n \mid e + e \mid e * e & \ldots \\
& | & \texttt{rand}(e, e) & \text{rand: nombre aléatoire entre les bornes}
\end{array}
$$

Expressions : ensembles de valeurs

Semantique des expressions: $[\![e]\!]_{\mathrm{E}} : (\mathrm{Var} \to \mathbb{Z}) \to \mathcal{P}(\mathbb{Z})$

$$
\begin{aligned}
[\![v]\!]_{\mathrm{E}}\,(\sigma) &= \{\sigma(v)\} \\
[\![n]\!]_{\mathrm{E}}\,(\sigma) &= \{n\} \\
[\![\mathbf{rand}(n_1, n_2)]\!]_{\mathrm{E}}\,(\sigma) &= \{n \in \mathbb{Z} \mid n_1 \leqslant n \leqslant n_2\} \\
[\![e_1 + e_2]\!]_{\mathrm{E}}\,(\sigma) &= \{n_1 + n_2 \mid n_1 \in [\![e_1]\!]_{\mathrm{E}}\,(\sigma) \wedge n_2 \in [\![e_2]\!]_{\mathrm{E}}\,(\sigma)\} \\
\ldots &
\end{aligned}
$$

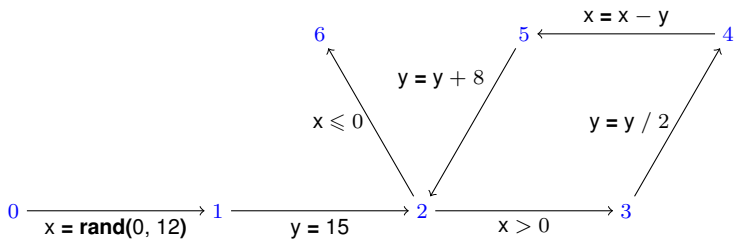
Environnement

L'environnement est la fonction $\sigma : \mathrm{Var} \to \mathbb{Z}$
qui associe chaque variable à une valeur.

Sémantique concrète sur un CFG

La même sémantique peut être décrite sur un graphe de flot de controle:

```
0 x = rand(0, 12);
1 y = 15;
while 2(x > 0) {
    3 y = y / 2;
    4 x = x − y;
    5 y = y + 8;
}6
```

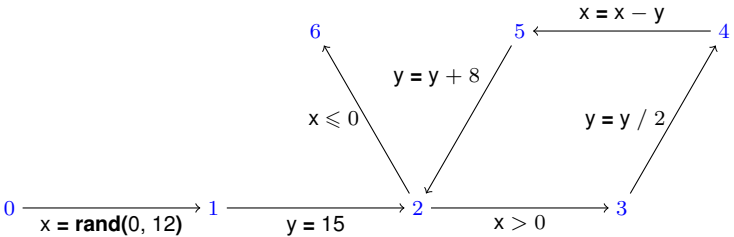


Terminologie

Ce CFG peut être vu comme un système de transitions.

Sémantique concrète et CFG 1/3

La sémantique concrète peut être exprimée sur ce systeme de transition:



- Une **valuation** est une paire (k, σ) avec σ : Var $\to \mathbb{Z}$:
  - Var est l'ensemble fini de d variables numérotées $[0, \ldots, d-1]$

Quelle est la sémantique:

- pour les conditions?
- pour les actions?
- pour le programme?

Sémantique concrète et CFG 2/3

Soit L l'ensemble des noeuds du CFG.

Un arc est de type $L \times commande \times L$ (commande = qqch qui modifie l'état)

Sémantique des commandes: $[\![c]\!]_{\mathrm{C}} : \mathcal{P}(\mathsf{Var} \to \mathbb{Z}) \to \mathcal{P}(\mathsf{Var} \to \mathbb{Z})$

Ensembles de valuation

Attention: Un état est un ensemble de valuations ($\mathcal{P}(\mathsf{Var} \to \mathbb{Z})$).

$$[\![v := e]\!]_{\mathrm{C}}(\Sigma) = \{\sigma[v \mapsto n] \mid \sigma \in \Sigma, n \in [\![e]\!]_{\mathrm{E}}(\sigma)\}$$
$$[\![e > 0]\!]_{\mathrm{C}}(\Sigma) = \{\sigma \mid \sigma \in \Sigma, \exists n \in [\![e]\!]_{\mathrm{E}}(\sigma), n > 0\}$$

Exercice Quelle est la sémantique pour:

- La commande $x := 42 + x$
- Avec l'état initial $\Sigma = \{[x \mapsto 3], [x \mapsto 4]\}$

Sémantique concrète et CFG 3/3

Sémantique des programmes : $[\![(L, A)]\!] : L \to \mathcal{P}(\mathsf{Var} \to \mathbb{Z})$

On associe un **meilleur invariant** (un état) à chaque noeud du CFG.

C'est la plus petite solution (selon l'ordre $\subseteq$) du système:

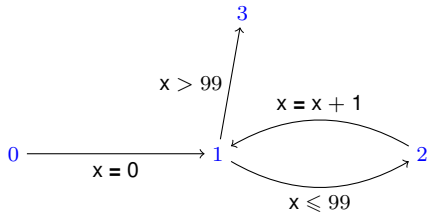
$$\begin{cases} R_0 = \mathsf{Var} \to \mathbb{Z} \\ R_{k'} = \bigcup_{(k,c,k') \in A} [\![c]\!]_{\mathrm{C}} \, (R_k) & k' \neq 0 \end{cases}$$

Théorème

Il existe forcément une solution (théorème de Knaster-Tarski).

Sémantique concrète: un exemple 1/2

```
0x = 0;
while 1(x ⩽ 99) {
    2x = x + 1;
}3
```

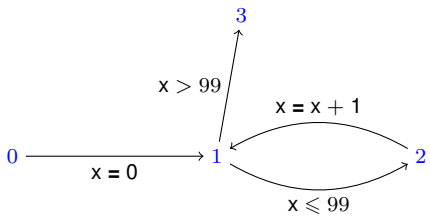


La sémantique du programme ($L \to \mathcal{P}(\text{Var} \to \mathbb{Z})$) :

- $0 \mapsto \{[x \mapsto i], i \in \mathbb{Z}\}$
- **Autres points de contrôle?**

Sémantique concrète: un exemple 2/2

```
0x = 0;
while 1(x ⩽ 99) {
    2x = x + 1;
}3
```



Les équations (R_k est l'état associé au noeud k):

$$\begin{cases} R_0 = \mathsf{Var} \to \mathbb{Z} \\ R_{k'} = \bigcup_{(k,c,k') \in A} [\![c]\!]_{\mathrm{C}} (R_k) \quad k' \neq 0 \end{cases}$$

Écrire les équations

Calculer la sémantique concrète: un algorithme informel

Les équations (R_k est l'état associé au noeud k):

$$\begin{cases} R_0 = \mathsf{Var} \to \mathbb{Z} \\ R_{k'} = \bigcup_{(k,c,k') \in A} [\![c]\!]_{\mathrm{C}}\,(R_k) & k' \neq 0 \end{cases}$$

- début: $i \leftarrow 0$, $R^0 \leftarrow$ "toutes les valuations possibles pour k=0, vide sinon"
- loop: Calculer R^{i+1} à partir de R^i:
  - appliquer $[\![c]\!]_{\mathrm{C}}$ sur les états R^i_k des arcs entrants.
  - faire l'union de ces ensembles pour obtenir $R^{i+1}_{k'}$
- Si $R^{i+1} = R^i$ alors renvoyer cet ensemble, sinon: goto loop.

Terminaison

Ceci ne termine pas en général. Si cela se termine, on obtient la sémantique concrète du programme.

Sémantique abstraite: calcul des invariants

Voici les équations qu'on résout avec notre algorithme itératif:

$$\begin{cases} R_0 = \mathsf{Var} \to \mathbb{Z} \\ R_{k'} = \bigcup_{(k,c,k') \in A} [\![c]\!]_{\mathrm{C}} \left(R_k\right) & k' \neq 0 \end{cases}$$

Il y a trois problèmes à régler :

- **Représenter les états** $R^i(_k)$.
- Calculer $[\![c]\!]_{\mathrm{C}} \left(R^i\right)$, ainsi que les unions.
- Le calcul peut ne pas se terminer. **Donner un exemple!**

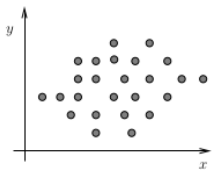
Représenter les états 1/2

Premier problème : **représenter les états** valuations

$$R^{(i)} : (k \to) : \mathcal{P}(\mathsf{Var} \to \mathbb{Z})$$

Observations:

- Les d variables peuvent etre numérotées de 0 à $d-1$
- Dans nos exemples, on attribue le numéro 0 à la variable x, le numéro 1 à la variable y, et ainsi de suite.
- La valeur de toutes les variables : représentée par un vecteur dans $\mathbb{Z}^d$:

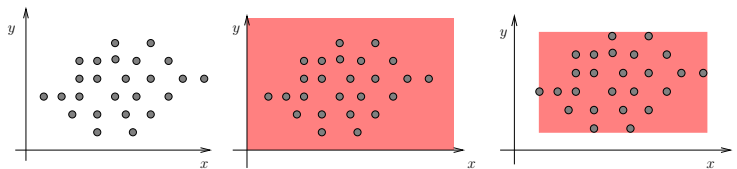


Représenter les états 2/2

Idée: Représenter les valeurs des variables:

$$R_k \in \mathcal{P}(\mathbb{Z}^d)$$

par un **sur-ensemble fini calculable** $R_k^\sharp$:



- Et calculer ces **valeurs abstraites** for à chaque : “x is $\geqslant 0$ at pc=42”

Calculer les relations de transition

Second problèmh : **calculer** les transitions pour les commandes et unions:

$$\bigcup_{(k,c,k')\in A} [\![c]\!]_{\mathrm{C}}\,(R_k) \quad \rightsquigarrow \quad \bigsqcup^{\sharp}_{(k,c,k')\in A} [\![c]\!]^{\sharp}_{\mathrm{C}}\,(R^{\sharp}_k)$$

- Les commandes travaillent sur des valeurs abstraites.
- L'union aussi.

▶ Il faut remplacer notre sémantique concrete $[\![]\!]_{\mathrm{C}}$ par une **sémantique abstraite** $[\![]\!]^{\sharp}_{\mathrm{C}}$ et donner une **union abstraite** compatible.

Algorithme de l'interprétation abstraite

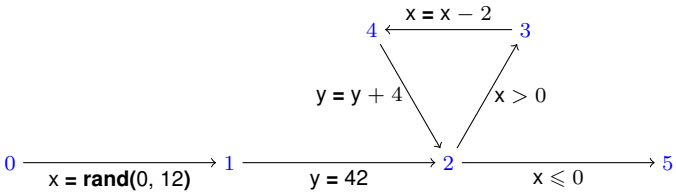
Algorithme (haut niveau):

- Écrire les équations correspondantes à la sémantique abstraite
- Interpréter le programme depuis le début, mais **de manière abstraite**:
  - Calculer un élement de valeur abstraite pour chaque noeud:
  - Toujours faire l'union (join) avec l'ancienne valeur.
- Arreter lorsqu'il n'y a plus de changement (pour tous les points de controle).

credit exemples, P. Roux (Onera)

Exemple de calcul d'un point-fixe abstrait (Signes) 1/2

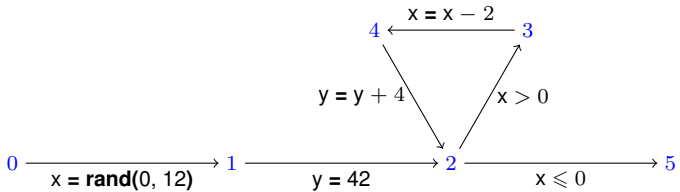
```
0 x = rand(0, 12)
1 y = 42;
while 2 (x > 0) {
    3 x = x − 2;
    4 y = y + 4;
}5
```



- **Objectif**: propager le **Signe** pour chaque variable, avec les notations $\geqslant 0$, $\leqslant 0$, $\top$ (peut être positif ou negatif), $\bot$ (aucune info disponible pour l'instant).

Exemple de calcul d'un point-fixe abstrait (Signes) 2/2

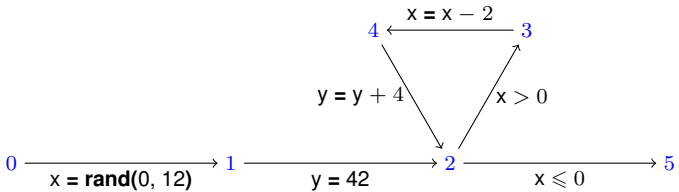
```
0x = rand(0, 12);1y = 42;
while 2(x > 0) {
    3x = x − 2;
    4y = y + 4;
}5
```



$$
\begin{aligned}
R_0^{\sharp\, i+1} &= \top_{\mathrm{nr}} \\
R_1^{\sharp\, i+1} &= R_0^{\sharp\, i+1}\,[x \mapsto \geqslant 0] \\
R_2^{\sharp\, i+1} &= R_1^{\sharp\, i+1}\,[y \mapsto \geqslant 0] \sqcup^{\sharp}_{\mathrm{nr}} \\
&\qquad R_4^{\sharp\, i}\left[y \mapsto R_4^{\sharp\, i}(y) +^{\sharp} (\geqslant 0)\right] \\
R_3^{\sharp\, i+1} &= R_2^{\sharp\, i+1}\left[x \mapsto R_2^{\sharp\, i+1}(x) \sqcap^{\sharp} \geqslant 0\right] \\
R_4^{\sharp\, i+1} &= R_3^{\sharp\, i+1}\left[x \mapsto R_3^{\sharp\, i+1}(x) -^{\sharp} (\geqslant 0)\right] \\
R_5^{\sharp\, i+1} &= R_2^{\sharp\, i+1}\left[x \mapsto R_2^{\sharp\, i+1} \sqcap^{\sharp} \leqslant 0\right]
\end{aligned}
$$

Exemple de calcul d'un point-fixe abstrait (Signes) 2/2

$_0$x = **rand**(0, 12);$_1$y = 42;
while $_2$(x $>$ 0) **{**
  $_3$x = x $-$ 2;
  $_4$y = y $+$ 4;
}$_5$

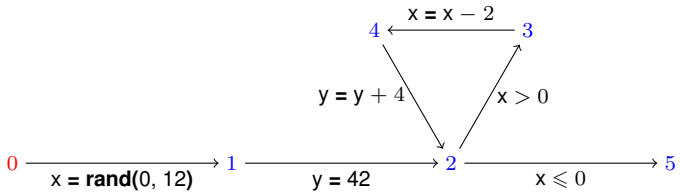


$$
\begin{aligned}
R_0^{\sharp\, i+1} &= \top_{\mathrm{nr}} \\
R_1^{\sharp\, i+1} &= R_0^{\sharp\, i+1}\,[x \mapsto \geqslant 0] \\
R_2^{\sharp\, i+1} &= R_1^{\sharp\, i+1}\,[y \mapsto \geqslant 0] \sqcup^{\sharp}_{\mathrm{nr}} \\
&\quad\ R_4^{\sharp\, i}\left[y \mapsto R_4^{\sharp\, i}(y) +^{\sharp} (\geqslant 0)\right] \\
R_3^{\sharp\, i+1} &= R_2^{\sharp\, i+1}\left[x \mapsto R_2^{\sharp\, i+1}(x) \sqcap^{\sharp} \geqslant 0\right] \\
R_4^{\sharp\, i+1} &= R_3^{\sharp\, i+1}\left[x \mapsto R_3^{\sharp\, i+1}(x) -^{\sharp} (\geqslant 0)\right] \\
R_5^{\sharp\, i+1} &= R_2^{\sharp\, i+1}\left[x \mapsto R_2^{\sharp\, i+1} \sqcap^{\sharp} \leqslant 0\right]
\end{aligned}
$$

k	$R_k^{\sharp\, 0}$	$R_k^{\sharp\, 1}$	$R_k^{\sharp\, 2}$	$R_k^{\sharp\, 3}$
0	$(\bot, \bot)$			
1	$(\bot, \bot)$			
2	$(\bot, \bot)$			
3	$(\bot, \bot)$			
4	$(\bot, \bot)$			
5	$(\bot, \bot)$			

Exemple de calcul d'un point-fixe abstrait (Signes) 2/2

```
0x = rand(0, 12);1y = 42;
while 2(x > 0) {
    3x = x − 2;
    4y = y + 4;
}5
```

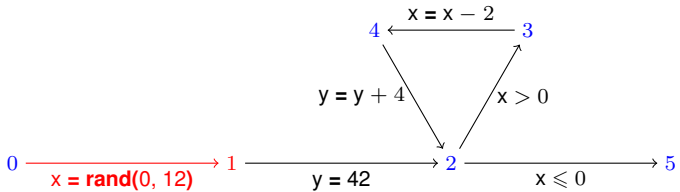


$$
\begin{aligned}
R_0^{\sharp\,i+1} &= \top_{\mathrm{nr}} \\
R_1^{\sharp\,i+1} &= R_0^{\sharp\,i+1}\,[x \mapsto \geqslant 0] \\
R_2^{\sharp\,i+1} &= R_1^{\sharp\,i+1}\,[y \mapsto \geqslant 0] \sqcup_{\mathrm{nr}}^{\sharp} \\
&\qquad R_4^{\sharp\,i}\left[y \mapsto R_4^{\sharp\,i}(y) +^{\sharp} (\geqslant 0)\right] \\
R_3^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1}(x) \sqcap^{\sharp} \geqslant 0\right] \\
R_4^{\sharp\,i+1} &= R_3^{\sharp\,i+1}\left[x \mapsto R_3^{\sharp\,i+1}(x) -^{\sharp} (\geqslant 0)\right] \\
R_5^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1} \sqcap^{\sharp} \leqslant 0\right]
\end{aligned}
$$

k	$R_k^{\sharp\,0}$	$R_k^{\sharp\,1}$	$R_k^{\sharp\,2}$	$R_k^{\sharp\,3}$
0	$(\bot, \bot)$	$(\top, \top)$		
1	$(\bot, \bot)$			
2	$(\bot, \bot)$			
3	$(\bot, \bot)$			
4	$(\bot, \bot)$			
5	$(\bot, \bot)$			

Exemple de calcul d'un point-fixe abstrait (Signes) 2/2

```
0x = rand(0, 12);1y = 42;
while 2(x > 0) {
    3x = x − 2;
    4y = y + 4;
}5
```

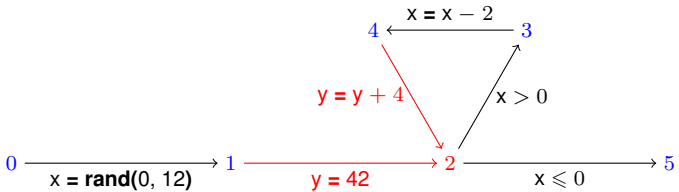


$$
\begin{aligned}
R_0^{\sharp\, i+1} &= \top_{\mathrm{nr}} \\
R_1^{\sharp\, i+1} &= R_0^{\sharp\, i+1}\,[x \mapsto \geqslant 0] \\
R_2^{\sharp\, i+1} &= R_1^{\sharp\, i+1}\,[y \mapsto \geqslant 0] \sqcup_{\mathrm{nr}}^{\sharp} \\
&\qquad R_4^{\sharp\, i}\left[y \mapsto R_4^{\sharp\, i}(y) +^{\sharp} (\geqslant 0)\right] \\
R_3^{\sharp\, i+1} &= R_2^{\sharp\, i+1}\left[x \mapsto R_2^{\sharp\, i+1}(x) \sqcap^{\sharp} \geqslant 0\right] \\
R_4^{\sharp\, i+1} &= R_3^{\sharp\, i+1}\left[x \mapsto R_3^{\sharp\, i+1}(x) -^{\sharp} (\geqslant 0)\right] \\
R_5^{\sharp\, i+1} &= R_2^{\sharp\, i+1}\left[x \mapsto R_2^{\sharp\, i+1} \sqcap^{\sharp} \leqslant 0\right]
\end{aligned}
$$

k	$R_k^{\sharp\, 0}$	$R_k^{\sharp\, 1}$	$R_k^{\sharp\, 2}$	$R_k^{\sharp\, 3}$
0	$(\bot, \bot)$	$(\top, \top)$		
1	$(\bot, \bot)$	$(\geqslant 0, \top)$		
2	$(\bot, \bot)$			
3	$(\bot, \bot)$			
4	$(\bot, \bot)$			
5	$(\bot, \bot)$			

Exemple de calcul d'un point-fixe abstrait (Signes) 2/2

$_0$x = **rand**(0, 12);$_1$y = 42;
while $_2$(x > 0) **{**
  $_3$x = x − 2;
  $_4$y = y + 4;
}$_5$



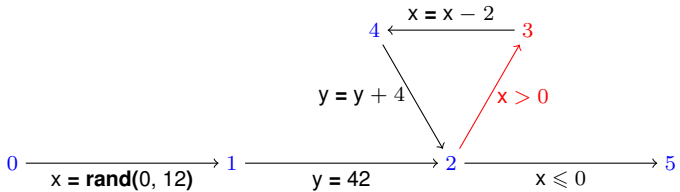
$$
\begin{aligned}
R_0^{\sharp\,i+1} &= \top_{\mathrm{nr}} \\
R_1^{\sharp\,i+1} &= R_0^{\sharp\,i+1}\,[x \mapsto \geqslant 0] \\
R_2^{\sharp\,i+1} &= R_1^{\sharp\,i+1}\,[y \mapsto \geqslant 0] \sqcup^{\sharp}_{\mathrm{nr}} \\
&\quad\; R_4^{\sharp\,i}\left[y \mapsto R_4^{\sharp\,i}(y) +^{\sharp} (\geqslant 0)\right] \\
R_3^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1}(x) \sqcap^{\sharp} \geqslant 0\right] \\
R_4^{\sharp\,i+1} &= R_3^{\sharp\,i+1}\left[x \mapsto R_3^{\sharp\,i+1}(x) -^{\sharp} (\geqslant 0)\right] \\
R_5^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1} \sqcap^{\sharp} \leqslant 0\right]
\end{aligned}
$$

k	$R_k^{\sharp\,0}$	$R_k^{\sharp\,1}$	$R_k^{\sharp\,2}$	$R_k^{\sharp\,3}$
0	$(\bot, \bot)$	$(\top, \top)$		
1	$(\bot, \bot)$	$(\geqslant 0, \top)$		
2	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$		
3	$(\bot, \bot)$			
4	$(\bot, \bot)$			
5	$(\bot, \bot)$			

$$(\geqslant 0, \geqslant 0) \sqcup^{\sharp}_{\mathrm{nr}} (\bot, \bot)$$

Exemple de calcul d'un point-fixe abstrait (Signes) 2/2

$_0$x = **rand**(0, 12);$_1$y = 42;
while $_2$(x > 0) **{**
  $_3$x = x − 2;
  $_4$y = y + 4;
}$_5$

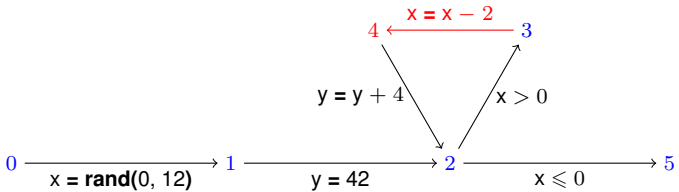


$$
\begin{aligned}
R_0^{\sharp\,i+1} &= \top_{\mathrm{nr}} \\
R_1^{\sharp\,i+1} &= R_0^{\sharp\,i+1}\,[x \mapsto \geqslant 0] \\
R_2^{\sharp\,i+1} &= R_1^{\sharp\,i+1}\,[y \mapsto \geqslant 0] \sqcup^{\sharp}_{\mathrm{nr}} \\
&\qquad R_4^{\sharp\,i}\left[y \mapsto R_4^{\sharp\,i}(y) +^{\sharp} (\geqslant 0)\right] \\
R_3^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1}(x) \sqcap^{\sharp} \geqslant 0\right] \\
R_4^{\sharp\,i+1} &= R_3^{\sharp\,i+1}\left[x \mapsto R_3^{\sharp\,i+1}(x) -^{\sharp} (\geqslant 0)\right] \\
R_5^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1} \sqcap^{\sharp} \leqslant 0\right]
\end{aligned}
$$

k	$R_k^{\sharp\,0}$	$R_k^{\sharp\,1}$	$R_k^{\sharp\,2}$	$R_k^{\sharp\,3}$
0	$(\bot, \bot)$	$(\top, \top)$		
1	$(\bot, \bot)$	$(\geqslant 0, \top)$		
2	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$		
3	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$		
4	$(\bot, \bot)$			
5	$(\bot, \bot)$			

Exemple de calcul d'un point-fixe abstrait (Signes) 2/2

$_0$x = **rand**(0, 12);$_1$y = 42;
while $_2$(x $>$ 0) **{**
  $_3$x = x $-$ 2;
  $_4$y = y $+$ 4;
}$_5$

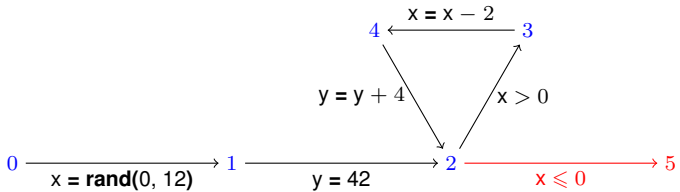


$$
\begin{aligned}
R_0^{\sharp\,i+1} &= \top_{\mathrm{nr}} \\
R_1^{\sharp\,i+1} &= R_0^{\sharp\,i+1}\,[x \mapsto \geqslant 0] \\
R_2^{\sharp\,i+1} &= R_1^{\sharp\,i+1}\,[y \mapsto \geqslant 0] \sqcup^{\sharp}_{\mathrm{nr}} \\
&\quad\ R_4^{\sharp\,i}\left[y \mapsto R_4^{\sharp\,i}(y) +^{\sharp} (\geqslant 0)\right] \\
R_3^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1}(x) \sqcap^{\sharp} \geqslant 0\right] \\
R_4^{\sharp\,i+1} &= R_3^{\sharp\,i+1}\left[x \mapsto R_3^{\sharp\,i+1}(x) -^{\sharp} (\geqslant 0)\right] \\
R_5^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1} \sqcap^{\sharp} \leqslant 0\right]
\end{aligned}
$$

k	$R_k^{\sharp\,0}$	$R_k^{\sharp\,1}$	$R_k^{\sharp\,2}$	$R_k^{\sharp\,3}$
0	$(\bot, \bot)$	$(\top, \top)$		
1	$(\bot, \bot)$	$(\geqslant 0, \top)$		
2	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$		
3	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$		
4	$(\bot, \bot)$	$(\top, \geqslant 0)$		
5	$(\bot, \bot)$			

Exemple de calcul d'un point-fixe abstrait (Signes) 2/2

$_0$x = **rand**(0, 12);$_1$y = 42;
while $_2$(x > 0) **{**
  $_3$x = x − 2;
  $_4$y = y + 4;
}$_5$

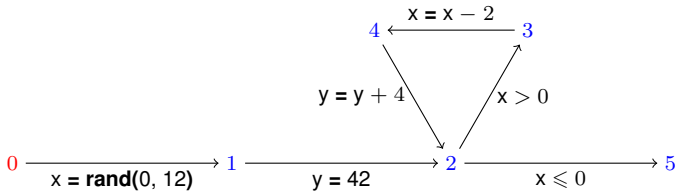


$$
\begin{aligned}
R_0^{\sharp\,i+1} &= \top_{\mathrm{nr}} \\
R_1^{\sharp\,i+1} &= R_0^{\sharp\,i+1}\,[x \mapsto \geqslant 0] \\
R_2^{\sharp\,i+1} &= R_1^{\sharp\,i+1}\,[y \mapsto \geqslant 0] \sqcup^{\sharp}_{\mathrm{nr}} \\
&\qquad R_4^{\sharp\,i}\left[y \mapsto R_4^{\sharp\,i}(y) +^{\sharp} (\geqslant 0)\right] \\
R_3^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1}(x) \sqcap^{\sharp} \geqslant 0\right] \\
R_4^{\sharp\,i+1} &= R_3^{\sharp\,i+1}\left[x \mapsto R_3^{\sharp\,i+1}(x) -^{\sharp} (\geqslant 0)\right] \\
R_5^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1} \sqcap^{\sharp} \leqslant 0\right]
\end{aligned}
$$

k	$R_k^{\sharp\,0}$	$R_k^{\sharp\,1}$	$R_k^{\sharp\,2}$	$R_k^{\sharp\,3}$
0	$(\bot, \bot)$	$(\top, \top)$		
1	$(\bot, \bot)$	$(\geqslant 0, \top)$		
2	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$		
3	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$		
4	$(\bot, \bot)$	$(\top, \geqslant 0)$		
5	$(\bot, \bot)$	$(0, \geqslant 0)$		

Exemple de calcul d'un point-fixe abstrait (Signes) 2/2

$_0$x = **rand**(0, 12);$_1$y = 42;
while $_2$(x > 0) **{**
  $_3$x = x − 2;
  $_4$y = y + 4;
}$_5$

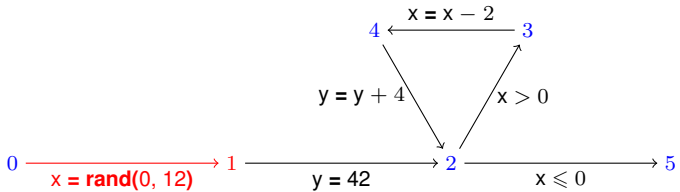


$$
\begin{aligned}
R_0^{\sharp\,i+1} &= \top_{\mathrm{nr}} \\
R_1^{\sharp\,i+1} &= R_0^{\sharp\,i+1}\,[x \mapsto \geqslant 0] \\
R_2^{\sharp\,i+1} &= R_1^{\sharp\,i+1}\,[y \mapsto \geqslant 0] \sqcup^{\sharp}_{\mathrm{nr}} \\
&\qquad R_4^{\sharp\,i}\left[y \mapsto R_4^{\sharp\,i}(y) +^{\sharp} (\geqslant 0)\right] \\
R_3^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1}(x) \sqcap^{\sharp} \geqslant 0\right] \\
R_4^{\sharp\,i+1} &= R_3^{\sharp\,i+1}\left[x \mapsto R_3^{\sharp\,i+1}(x) -^{\sharp} (\geqslant 0)\right] \\
R_5^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1} \sqcap^{\sharp} \leqslant 0\right]
\end{aligned}
$$

k	$R_k^{\sharp\,0}$	$R_k^{\sharp\,1}$	$R_k^{\sharp\,2}$	$R_k^{\sharp\,3}$
0	$(\bot, \bot)$	$(\top, \top)$	$(\top, \top)$	
1	$(\bot, \bot)$	$(\geqslant 0, \top)$		
2	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$		
3	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$		
4	$(\bot, \bot)$	$(\top, \geqslant 0)$		
5	$(\bot, \bot)$	$(0, \geqslant 0)$		

Exemple de calcul d'un point-fixe abstrait (Signes) 2/2

```
0x = rand(0, 12);1y = 42;
while 2(x > 0) {
    3x = x − 2;
    4y = y + 4;
}5
```

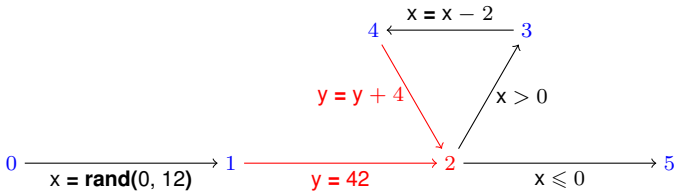


$$
\begin{aligned}
R_0^{\sharp\,i+1} &= \top_{\text{nr}} \\
R_1^{\sharp\,i+1} &= R_0^{\sharp\,i+1}\,[x \mapsto \geqslant 0] \\
R_2^{\sharp\,i+1} &= R_1^{\sharp\,i+1}\,[y \mapsto \geqslant 0] \sqcup^{\sharp}_{\text{nr}} \\
&\qquad R_4^{\sharp\,i}\left[y \mapsto R_4^{\sharp\,i}(y) +^{\sharp} (\geqslant 0)\right] \\
R_3^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1}(x) \sqcap^{\sharp} \geqslant 0\right] \\
R_4^{\sharp\,i+1} &= R_3^{\sharp\,i+1}\left[x \mapsto R_3^{\sharp\,i+1}(x) -^{\sharp} (\geqslant 0)\right] \\
R_5^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1} \sqcap^{\sharp} \leqslant 0\right]
\end{aligned}
$$

k	$R_k^{\sharp\,0}$	$R_k^{\sharp\,1}$	$R_k^{\sharp\,2}$	$R_k^{\sharp\,3}$
0	$(\bot, \bot)$	$(\top, \top)$	$(\top, \top)$	
1	$(\bot, \bot)$	$(\geqslant 0, \top)$	$(\geqslant 0, \top)$	
2	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$		
3	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$		
4	$(\bot, \bot)$	$(\top, \geqslant 0)$		
5	$(\bot, \bot)$	$(0, \geqslant 0)$		

Exemple de calcul d'un point-fixe abstrait (Signes) 2/2

```
0x = rand(0, 12);1y = 42;
while 2(x > 0) {
    3x = x − 2;
    4y = y + 4;
}5
```



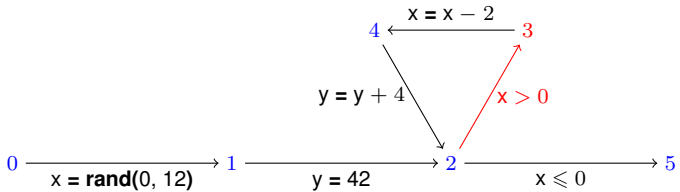
$$
\begin{aligned}
R_0^{\sharp\, i+1} &= \top_{\text{nr}} \\
R_1^{\sharp\, i+1} &= R_0^{\sharp\, i+1}\,[x \mapsto \geqslant 0] \\
R_2^{\sharp\, i+1} &= R_1^{\sharp\, i+1}\,[y \mapsto \geqslant 0] \sqcup^\sharp_{\text{nr}} \\
&\quad\ R_4^{\sharp\, i}\left[y \mapsto R_4^{\sharp\, i}(y) +^\sharp (\geqslant 0)\right] \\
R_3^{\sharp\, i+1} &= R_2^{\sharp\, i+1}\left[x \mapsto R_2^{\sharp\, i+1}(x) \sqcap^\sharp \geqslant 0\right] \\
R_4^{\sharp\, i+1} &= R_3^{\sharp\, i+1}\left[x \mapsto R_3^{\sharp\, i+1}(x) -^\sharp (\geqslant 0)\right] \\
R_5^{\sharp\, i+1} &= R_2^{\sharp\, i+1}\left[x \mapsto R_2^{\sharp\, i+1} \sqcap^\sharp \leqslant 0\right]
\end{aligned}
$$

k	$R_k^{\sharp\, 0}$	$R_k^{\sharp\, 1}$	$R_k^{\sharp\, 2}$	$R_k^{\sharp\, 3}$
0	$(\bot, \bot)$	$(\top, \top)$	$(\top, \top)$	
1	$(\bot, \bot)$	$(\geqslant 0, \top)$	$(\geqslant 0, \top)$	
2	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$	$(\top, \geqslant 0)$	
3	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$		
4	$(\bot, \bot)$	$(\top, \geqslant 0)$		
5	$(\bot, \bot)$	$(0, \geqslant 0)$		

$$(\geqslant 0, \geqslant 0) \sqcup^\sharp_{\text{nr}} (\top, \geqslant 0)$$

Exemple de calcul d'un point-fixe abstrait (Signes) 2/2

```
0x = rand(0, 12);1y = 42;
while 2(x > 0) {
    3x = x − 2;
    4y = y + 4;
}5
```

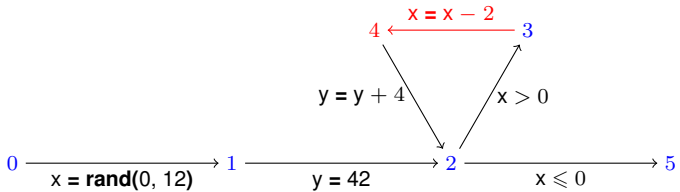


$$
\begin{aligned}
R_0^{\sharp\,i+1} &= \top_{\mathrm{nr}} \\
R_1^{\sharp\,i+1} &= R_0^{\sharp\,i+1}\,[x \mapsto \geqslant 0] \\
R_2^{\sharp\,i+1} &= R_1^{\sharp\,i+1}\,[y \mapsto \geqslant 0] \sqcup^\sharp_{\mathrm{nr}} \\
&\quad\; R_4^{\sharp\,i}\left[y \mapsto R_4^{\sharp\,i}(y) +^\sharp (\geqslant 0)\right] \\
R_3^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1}(x) \sqcap^\sharp \geqslant 0\right] \\
R_4^{\sharp\,i+1} &= R_3^{\sharp\,i+1}\left[x \mapsto R_3^{\sharp\,i+1}(x) -^\sharp (\geqslant 0)\right] \\
R_5^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1} \sqcap^\sharp \leqslant 0\right]
\end{aligned}
$$

k	$R_k^{\sharp\,0}$	$R_k^{\sharp\,1}$	$R_k^{\sharp\,2}$	$R_k^{\sharp\,3}$
0	$(\bot, \bot)$	$(\top, \top)$	$(\top, \top)$	
1	$(\bot, \bot)$	$(\geqslant 0, \top)$	$(\geqslant 0, \top)$	
2	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$	$(\top, \geqslant 0)$	
3	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$	$(\geqslant 0, \geqslant 0)$	
4	$(\bot, \bot)$	$(\top, \geqslant 0)$		
5	$(\bot, \bot)$	$(0, \geqslant 0)$		

Exemple de calcul d'un point-fixe abstrait (Signes) 2/2

$_0$x = **rand**(0, 12);$_1$y = 42;
while $_2$(x > 0) **{**
  $_3$x = x − 2;
  $_4$y = y + 4;
}$_5$

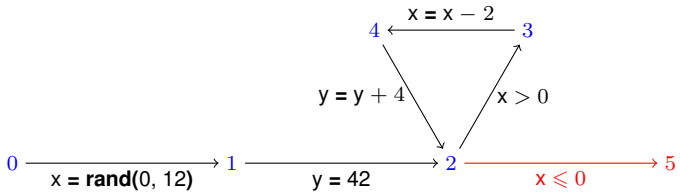


$$
\begin{aligned}
R_0^{\sharp\,i+1} &= \top_{\mathrm{nr}} \\
R_1^{\sharp\,i+1} &= R_0^{\sharp\,i+1}\,[x \mapsto \geqslant 0] \\
R_2^{\sharp\,i+1} &= R_1^{\sharp\,i+1}\,[y \mapsto \geqslant 0] \sqcup^{\sharp}_{\mathrm{nr}} \\
&\qquad R_4^{\sharp\,i}\left[y \mapsto R_4^{\sharp\,i}(y) +^{\sharp} (\geqslant 0)\right] \\
R_3^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1}(x) \sqcap^{\sharp} \geqslant 0\right] \\
R_4^{\sharp\,i+1} &= R_3^{\sharp\,i+1}\left[x \mapsto R_3^{\sharp\,i+1}(x) -^{\sharp} (\geqslant 0)\right] \\
R_5^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1} \sqcap^{\sharp} \leqslant 0\right]
\end{aligned}
$$

k	$R_k^{\sharp\,0}$	$R_k^{\sharp\,1}$	$R_k^{\sharp\,2}$	$R_k^{\sharp\,3}$
0	$(\bot, \bot)$	$(\top, \top)$	$(\top, \top)$	
1	$(\bot, \bot)$	$(\geqslant 0, \top)$	$(\geqslant 0, \top)$	
2	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$	$(\top, \geqslant 0)$	
3	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$	$(\geqslant 0, \geqslant 0)$	
4	$(\bot, \bot)$	$(\top, \geqslant 0)$	$(\top, \geqslant 0)$	
5	$(\bot, \bot)$	$(0, \geqslant 0)$		

Exemple de calcul d'un point-fixe abstrait (Signes) 2/2

$_0$x = **rand**(0, 12);$_1$y = 42;
while $_2$(x > 0) **{**
  $_3$x = x − 2;
  $_4$y = y + 4;
}$_5$

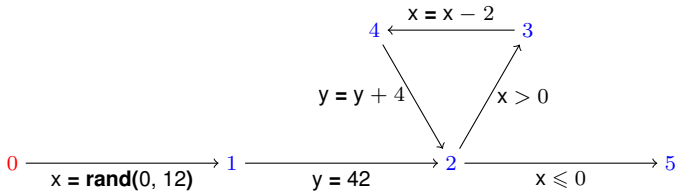


$$
\begin{aligned}
R_0^{\sharp\,i+1} &= \top_{\mathrm{nr}} \\
R_1^{\sharp\,i+1} &= R_0^{\sharp\,i+1}\,[x \mapsto \geqslant 0] \\
R_2^{\sharp\,i+1} &= R_1^{\sharp\,i+1}\,[y \mapsto \geqslant 0] \sqcup^\sharp_{\mathrm{nr}} \\
&\quad\; R_4^{\sharp\,i}\left[y \mapsto R_4^{\sharp\,i}(y) +^\sharp (\geqslant 0)\right] \\
R_3^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1}(x) \sqcap^\sharp \geqslant 0\right] \\
R_4^{\sharp\,i+1} &= R_3^{\sharp\,i+1}\left[x \mapsto R_3^{\sharp\,i+1}(x) -^\sharp (\geqslant 0)\right] \\
R_5^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1} \sqcap^\sharp \leqslant 0\right]
\end{aligned}
$$

k	$R_k^{\sharp\,0}$	$R_k^{\sharp\,1}$	$R_k^{\sharp\,2}$	$R_k^{\sharp\,3}$
0	$(\bot, \bot)$	$(\top, \top)$	$(\top, \top)$	
1	$(\bot, \bot)$	$(\geqslant 0, \top)$	$(\geqslant 0, \top)$	
2	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$	$(\top, \geqslant 0)$	
3	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$	$(\geqslant 0, \geqslant 0)$	
4	$(\bot, \bot)$	$(\top, \geqslant 0)$	$(\top, \geqslant 0)$	
5	$(\bot, \bot)$	$(0, \geqslant 0)$	$(\leqslant 0, \geqslant 0)$	

Exemple de calcul d'un point-fixe abstrait (Signes) 2/2

$_0$x = **rand**(0, 12);$_1$y = 42;
while $_2$(x > 0) **{**
  $_3$x = x − 2;
  $_4$y = y + 4;
}$_5$

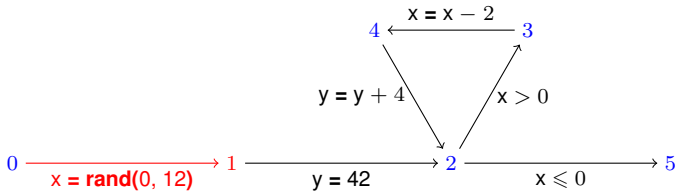


$$
\begin{aligned}
R_0^{\sharp\,i+1} &= \top_{\mathrm{nr}} \\
R_1^{\sharp\,i+1} &= R_0^{\sharp\,i+1}\,[x \mapsto \geqslant 0] \\
R_2^{\sharp\,i+1} &= R_1^{\sharp\,i+1}\,[y \mapsto \geqslant 0] \sqcup^{\sharp}_{\mathrm{nr}} \\
&\qquad R_4^{\sharp\,i}\left[y \mapsto R_4^{\sharp\,i}(y) +^{\sharp} (\geqslant 0)\right] \\
R_3^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1}(x) \sqcap^{\sharp} \geqslant 0\right] \\
R_4^{\sharp\,i+1} &= R_3^{\sharp\,i+1}\left[x \mapsto R_3^{\sharp\,i+1}(x) -^{\sharp} (\geqslant 0)\right] \\
R_5^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1} \sqcap^{\sharp} \leqslant 0\right]
\end{aligned}
$$

k	$R_k^{\sharp\,0}$	$R_k^{\sharp\,1}$	$R_k^{\sharp\,2}$	$R_k^{\sharp\,3}$
0	$(\bot, \bot)$	$(\top, \top)$	$(\top, \top)$	$(\top, \top)$
1	$(\bot, \bot)$	$(\geqslant 0, \top)$	$(\geqslant 0, \top)$	
2	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$	$(\top, \geqslant 0)$	
3	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$	$(\geqslant 0, \geqslant 0)$	
4	$(\bot, \bot)$	$(\top, \geqslant 0)$	$(\top, \geqslant 0)$	
5	$(\bot, \bot)$	$(0, \geqslant 0)$	$(\leqslant 0, \geqslant 0)$	

Exemple de calcul d'un point-fixe abstrait (Signes) 2/2

```
0x = rand(0, 12);1y = 42;
while 2(x > 0) {
    3x = x − 2;
    4y = y + 4;
}5
```

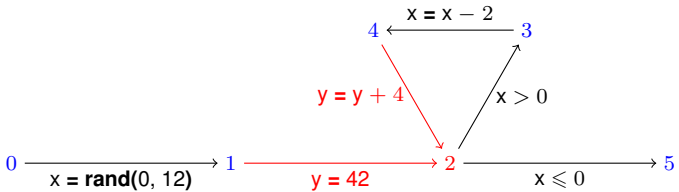


$$
\begin{aligned}
R_0^{\sharp\,i+1} &= \top_{\mathrm{nr}} \\
R_1^{\sharp\,i+1} &= R_0^{\sharp\,i+1}\,[x \mapsto \geqslant 0] \\
R_2^{\sharp\,i+1} &= R_1^{\sharp\,i+1}\,[y \mapsto \geqslant 0] \sqcup^{\sharp}_{\mathrm{nr}} \\
&\qquad R_4^{\sharp\,i}\left[y \mapsto R_4^{\sharp\,i}(y) +^{\sharp} (\geqslant 0)\right] \\
R_3^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1}(x) \sqcap^{\sharp} \geqslant 0\right] \\
R_4^{\sharp\,i+1} &= R_3^{\sharp\,i+1}\left[x \mapsto R_3^{\sharp\,i+1}(x) -^{\sharp} (\geqslant 0)\right] \\
R_5^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1} \sqcap^{\sharp} \leqslant 0\right]
\end{aligned}
$$

k	$R_k^{\sharp\,0}$	$R_k^{\sharp\,1}$	$R_k^{\sharp\,2}$	$R_k^{\sharp\,3}$
0	$(\bot, \bot)$	$(\top, \top)$	$(\top, \top)$	$(\top, \top)$
1	$(\bot, \bot)$	$(\geqslant 0, \top)$	$(\geqslant 0, \top)$	$(\geqslant 0, \top)$
2	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$	$(\top, \geqslant 0)$	
3	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$	$(\geqslant 0, \geqslant 0)$	
4	$(\bot, \bot)$	$(\top, \geqslant 0)$	$(\top, \geqslant 0)$	
5	$(\bot, \bot)$	$(0, \geqslant 0)$	$(\leqslant 0, \geqslant 0)$	

Exemple de calcul d'un point-fixe abstrait (Signes) 2/2

```
0x = rand(0, 12);1y = 42;
while 2(x > 0) {
    3x = x − 2;
    4y = y + 4;
}5
```



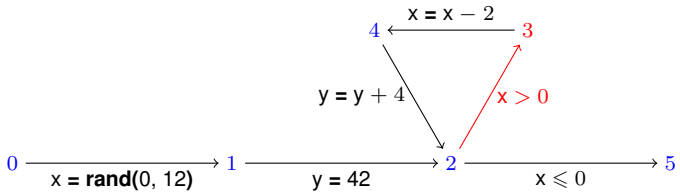
$$
\begin{aligned}
R_0^{\sharp\,i+1} &= \top_{\mathrm{nr}} \\
R_1^{\sharp\,i+1} &= R_0^{\sharp\,i+1}\,[x \mapsto \geqslant 0] \\
R_2^{\sharp\,i+1} &= R_1^{\sharp\,i+1}\,[y \mapsto \geqslant 0] \sqcup^{\sharp}_{\mathrm{nr}} \\
&\quad\; R_4^{\sharp\,i}\left[y \mapsto R_4^{\sharp\,i}(y) +^{\sharp} (\geqslant 0)\right] \\
R_3^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1}(x) \sqcap^{\sharp} \geqslant 0\right] \\
R_4^{\sharp\,i+1} &= R_3^{\sharp\,i+1}\left[x \mapsto R_3^{\sharp\,i+1}(x) -^{\sharp} (\geqslant 0)\right] \\
R_5^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1} \sqcap^{\sharp} \leqslant 0\right]
\end{aligned}
$$

k	$R_k^{\sharp\,0}$	$R_k^{\sharp\,1}$	$R_k^{\sharp\,2}$	$R_k^{\sharp\,3}$
0	$(\bot, \bot)$	$(\top, \top)$	$(\top, \top)$	$(\top, \top)$
1	$(\bot, \bot)$	$(\geqslant 0, \top)$	$(\geqslant 0, \top)$	$(\geqslant 0, \top)$
2	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$	$(\top, \geqslant 0)$	$(\top, \geqslant 0)$
3	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$	$(\geqslant 0, \geqslant 0)$	
4	$(\bot, \bot)$	$(\top, \geqslant 0)$	$(\top, \geqslant 0)$	
5	$(\bot, \bot)$	$(0, \geqslant 0)$	$(\leqslant 0, \geqslant 0)$	

$$(\geqslant 0, \geqslant 0) \sqcup^{\sharp}_{\mathrm{nr}} (\top, \geqslant 0)$$

Exemple de calcul d'un point-fixe abstrait (Signes) 2/2

$_0$x = **rand**(0, 12);$_1$y = 42;
while $_2$(x > 0) **{**
  $_3$x = x − 2;
  $_4$y = y + 4;
}$_5$

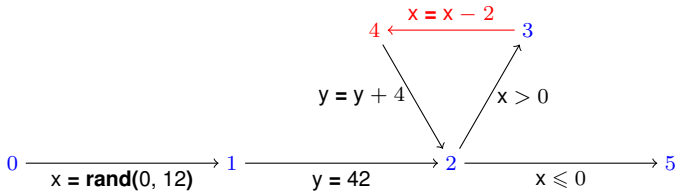


$$
\begin{aligned}
R_0^{\sharp\,i+1} &= \top_{\mathrm{nr}} \\
R_1^{\sharp\,i+1} &= R_0^{\sharp\,i+1}\,[x \mapsto \geqslant 0] \\
R_2^{\sharp\,i+1} &= R_1^{\sharp\,i+1}\,[y \mapsto \geqslant 0] \sqcup^{\sharp}_{\mathrm{nr}} \\
&\qquad R_4^{\sharp\,i}\left[y \mapsto R_4^{\sharp\,i}(y) +^{\sharp} (\geqslant 0)\right] \\
R_3^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1}(x) \sqcap^{\sharp} \geqslant 0\right] \\
R_4^{\sharp\,i+1} &= R_3^{\sharp\,i+1}\left[x \mapsto R_3^{\sharp\,i+1}(x) -^{\sharp} (\geqslant 0)\right] \\
R_5^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1} \sqcap^{\sharp} \leqslant 0\right]
\end{aligned}
$$

k	$R_k^{\sharp\,0}$	$R_k^{\sharp\,1}$	$R_k^{\sharp\,2}$	$R_k^{\sharp\,3}$
0	$(\bot, \bot)$	$(\top, \top)$	$(\top, \top)$	$(\top, \top)$
1	$(\bot, \bot)$	$(\geqslant 0, \top)$	$(\geqslant 0, \top)$	$(\geqslant 0, \top)$
2	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$	$(\top, \geqslant 0)$	$(\top, \geqslant 0)$
3	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$	$(\geqslant 0, \geqslant 0)$	$(\geqslant 0, \geqslant 0)$
4	$(\bot, \bot)$	$(\top, \geqslant 0)$	$(\top, \geqslant 0)$	
5	$(\bot, \bot)$	$(0, \geqslant 0)$	$(\leqslant 0, \geqslant 0)$	

Exemple de calcul d'un point-fixe abstrait (Signes) 2/2

```
0x = rand(0, 12);1y = 42;
while 2(x > 0) {
    3x = x − 2;
    4y = y + 4;
}5
```

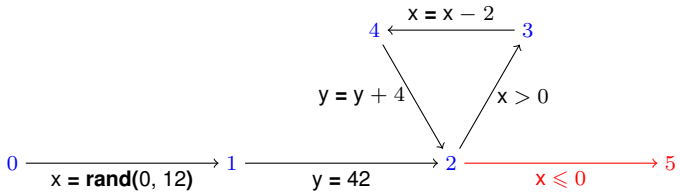


$$
\begin{aligned}
R_0^{\sharp\,i+1} &= \top_{\text{nr}} \\
R_1^{\sharp\,i+1} &= R_0^{\sharp\,i+1}\,[x \mapsto \geqslant 0] \\
R_2^{\sharp\,i+1} &= R_1^{\sharp\,i+1}\,[y \mapsto \geqslant 0] \sqcup^{\sharp}_{\text{nr}} \\
&\qquad R_4^{\sharp\,i}\left[y \mapsto R_4^{\sharp\,i}(y) +^{\sharp} (\geqslant 0)\right] \\
R_3^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1}(x) \sqcap^{\sharp} \geqslant 0\right] \\
R_4^{\sharp\,i+1} &= R_3^{\sharp\,i+1}\left[x \mapsto R_3^{\sharp\,i+1}(x) -^{\sharp} (\geqslant 0)\right] \\
R_5^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1} \sqcap^{\sharp} \leqslant 0\right]
\end{aligned}
$$

k	$R_k^{\sharp\,0}$	$R_k^{\sharp\,1}$	$R_k^{\sharp\,2}$	$R_k^{\sharp\,3}$
0	$(\bot, \bot)$	$(\top, \top)$	$(\top, \top)$	$(\top, \top)$
1	$(\bot, \bot)$	$(\geqslant 0, \top)$	$(\geqslant 0, \top)$	$(\geqslant 0, \top)$
2	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$	$(\top, \geqslant 0)$	$(\top, \geqslant 0)$
3	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$	$(\geqslant 0, \geqslant 0)$	$(\geqslant 0, \geqslant 0)$
4	$(\bot, \bot)$	$(\top, \geqslant 0)$	$(\top, \geqslant 0)$	$(\top, \geqslant 0)$
5	$(\bot, \bot)$	$(0, \geqslant 0)$	$(\leqslant 0, \geqslant 0)$	

Exemple de calcul d'un point-fixe abstrait (Signes) 2/2

```
0x = rand(0, 12);1y = 42;
while 2(x > 0) {
    3x = x − 2;
    4y = y + 4;
}5
```

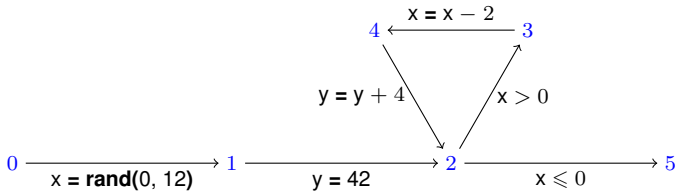


$$
\begin{aligned}
R_0^{\sharp\, i+1} &= \top_{\mathrm{nr}} \\
R_1^{\sharp\, i+1} &= R_0^{\sharp\, i+1}\,[x \mapsto \geqslant 0] \\
R_2^{\sharp\, i+1} &= R_1^{\sharp\, i+1}\,[y \mapsto \geqslant 0] \sqcup^{\sharp}_{\mathrm{nr}} \\
&\qquad R_4^{\sharp\, i}\left[y \mapsto R_4^{\sharp\, i}(y) +^{\sharp} (\geqslant 0)\right] \\
R_3^{\sharp\, i+1} &= R_2^{\sharp\, i+1}\left[x \mapsto R_2^{\sharp\, i+1}(x) \sqcap^{\sharp} \geqslant 0\right] \\
R_4^{\sharp\, i+1} &= R_3^{\sharp\, i+1}\left[x \mapsto R_3^{\sharp\, i+1}(x) -^{\sharp} (\geqslant 0)\right] \\
R_5^{\sharp\, i+1} &= R_2^{\sharp\, i+1}\left[x \mapsto R_2^{\sharp\, i+1} \sqcap^{\sharp} \leqslant 0\right]
\end{aligned}
$$

k	$R_k^{\sharp\, 0}$	$R_k^{\sharp\, 1}$	$R_k^{\sharp\, 2}$	$R_k^{\sharp\, 3}$
0	$(\bot, \bot)$	$(\top, \top)$	$(\top, \top)$	$(\top, \top)$
1	$(\bot, \bot)$	$(\geqslant 0, \top)$	$(\geqslant 0, \top)$	$(\geqslant 0, \top)$
2	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$	$(\top, \geqslant 0)$	$(\top, \geqslant 0)$
3	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$	$(\geqslant 0, \geqslant 0)$	$(\geqslant 0, \geqslant 0)$
4	$(\bot, \bot)$	$(\top, \geqslant 0)$	$(\top, \geqslant 0)$	$(\top, \geqslant 0)$
5	$(\bot, \bot)$	$(0, \geqslant 0)$	$(\leqslant 0, \geqslant 0)$	$(\leqslant 0, \geqslant 0)$

Exemple de calcul d'un point-fixe abstrait (Signes) 2/2

$_0$x = **rand**(0, 12);$_1$y = 42;
while $_2$(x > 0) **{**
  $_3$x = x − 2;
  $_4$y = y + 4;
}$_5$



$$
\begin{aligned}
R_0^{\sharp\,i+1} &= \top_{\mathrm{nr}} \\
R_1^{\sharp\,i+1} &= R_0^{\sharp\,i+1}\,[x \mapsto \geqslant 0] \\
R_2^{\sharp\,i+1} &= R_1^{\sharp\,i+1}\,[y \mapsto \geqslant 0] \sqcup^{\sharp}_{\mathrm{nr}} \\
&\qquad R_4^{\sharp\,i}\left[y \mapsto R_4^{\sharp\,i}(y) +^{\sharp} (\geqslant 0)\right] \\
R_3^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1}(x) \sqcap^{\sharp} \geqslant 0\right] \\
R_4^{\sharp\,i+1} &= R_3^{\sharp\,i+1}\left[x \mapsto R_3^{\sharp\,i+1}(x) -^{\sharp} (\geqslant 0)\right] \\
R_5^{\sharp\,i+1} &= R_2^{\sharp\,i+1}\left[x \mapsto R_2^{\sharp\,i+1} \sqcap^{\sharp} \leqslant 0\right]
\end{aligned}
$$

k	$R_k^{\sharp\,0}$	$R_k^{\sharp\,1}$	$R_k^{\sharp\,2}$	$R_k^{\sharp\,3}$
0	$(\bot, \bot)$	$(\top, \top)$	$(\top, \top)$	$(\top, \top)$
1	$(\bot, \bot)$	$(\geqslant 0, \top)$	$(\geqslant 0, \top)$	$(\geqslant 0, \top)$
2	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$	$(\top, \geqslant 0)$	$(\top, \geqslant 0)$
3	$(\bot, \bot)$	$(\geqslant 0, \geqslant 0)$	$(\geqslant 0, \geqslant 0)$	$(\geqslant 0, \geqslant 0)$
4	$(\bot, \bot)$	$(\top, \geqslant 0)$	$(\top, \geqslant 0)$	$(\top, \geqslant 0)$
5	$(\bot, \bot)$	$(0, \geqslant 0)$	$(\leqslant 0, \geqslant 0)$	$(\leqslant 0, \geqslant 0)$

Point-fixe atteint!

Conclusion de la section

Idée principale: Abstraction

Abstraire les ensembles de valuations permet d'avoir une analyse decidable

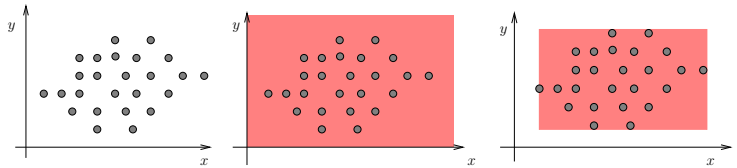
Comment construire la sémantique abstraite:

- de manière correcte?
- de manière a garantir la terminaison **par construction**?

▶ Il faut un peu plus de formalisation.

Représenter les états

~~Représenter~~ Abstraire un état: $R_k \in \mathcal{D}$ par un a **sur-ensemble fini calculable** $R_k^\sharp \in \mathcal{D}^\sharp$:



Domaine abstrait: notations

Definition (domaine abstrait $\mathcal{D}^\sharp$)

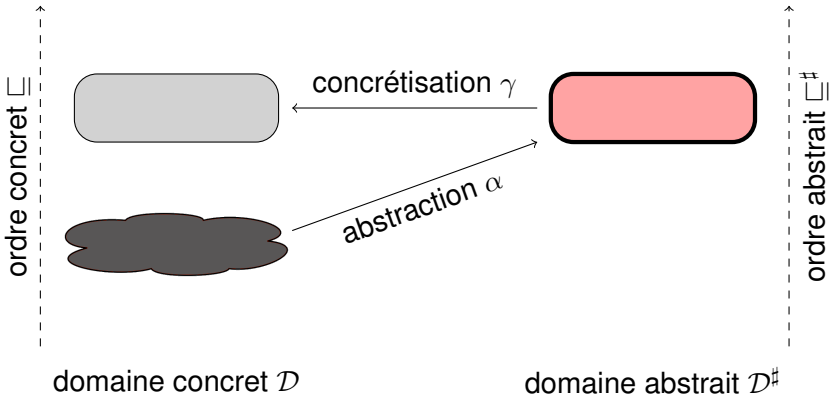
Un domaine abstrait définit:

- un ensemble $\mathcal{D}^\sharp$ d'élements abstraits;
- des opérations abstraites $[\![]\!]^\sharp$ correspondantes aux opérations concretes $[\![]\!]$.

Definition (abstraction α, concrétisation γ)

- Une fonction d'abstraction α qui fait correspondre chaque état concret R_k à un objet abstrait $R_k^\sharp$, approximant R.
- Une fonction de concrétisation γ qui fait correspondre chaque état abstrait $R_k^\sharp$ au plus grand état concret R_k dont il est l'approximation.

Concrete vs Abstract: digest



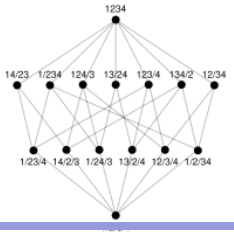
Du treillis au domaine abstrait 1/2

Definition (Treillis)

Un **treillis** est un ensemble partiellement ordonné ($\sqsubseteq$) pour lequel chaque paire d'élements (x, y) a:

- un sup: $x \sqcup y$, aussi appelé union, ou join (abstrait).
- un inf: $x \sqcap y$, aussi appelé intersection, ou meet (abstrait).

Il peut être représenté par un diagramme de Hasse:



Treillis des partitions d'un ensemble de 4 élements

From User:ed_g2s, Personal Work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=318292

Du treillis au domaine abstrait 2/2

1. Construire (α, γ), une correspondance de Galois du domaine concret $\mathcal{D}$ ($\subseteq$, $\cap$, $\emptyset$, $\mathbb{Z}^d$) vers le domaine abstrait $\mathcal{D}^\sharp$ (un treillis: $\sqsubseteq^\sharp, \sqcap^\sharp, \bot, \top$).
2. Construire les fonctions de transfert abstraites (qui doivent être **sures**).

Definition (Correspondance de Galois)

(α, γ) est une correspondance de Galois ssi $\forall x \in \mathcal{D}, x \subseteq \gamma(\alpha(x))$

Definition (Sûreté)

- sûreté de l'ordre abstrait: $\forall x^\sharp, y^\sharp \in \mathcal{D}^\sharp, \quad x^\sharp \sqsubseteq^\sharp y^\sharp \Rightarrow \gamma(x^\sharp) \subseteq \gamma(y^\sharp)$
- sûreté des opérations abstraites: $f(x) \subseteq \gamma(f^\sharp(\alpha(x)))$

Quelques exemples d'abstractions

Pour des valeurs numériques, on peut:

- Abstraire $\mathcal{P}(\text{Var} \to \mathbb{Z})$ en $\text{Var} \to \mathcal{P}(\mathbb{Z})$ puis $\mathcal{P}(\mathbb{Z})$ en $\mathcal{D}^\sharp$
  - non relationel: les valeurs de x et y sont indépendantes
  - exemples: signes, constantes, intervales.
- Abstraire $\mathcal{P}(\text{Var} \to \mathbb{Z})$ directement en $\mathcal{D}^\sharp$
  - relationel: certaines combinaisons de x et y sont impossibles
  - $+$ plus précis
  - $-$ plus compliqué, plus coûteux...
  - Octagones, polyèdres

Notion de sûreté

Definition (Sûreté de l'analyse / de la sémantique)

La sémantique abstraite est une **sur-approximation sûre** de la sémantique concrète, ssi $\forall k \in L$, on a: $R_k \subseteq \gamma\left(R_k^\sharp\right)$

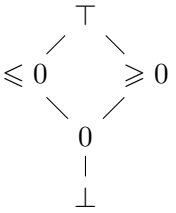
Domaine non-relationel (nr): une construction simple

Abstraire $\mathcal{P}(\mathsf{Var} \to \mathbb{Z})$ en $\mathsf{Var} \to \mathcal{P}(\mathbb{Z})$ puis $\mathcal{P}(\mathbb{Z})$ en $\mathcal{D}^\sharp$

C'est-à-dire abstraire chaque variable indépendamment:

- $\mathcal{D}^\sharp_{\text{nr}} = \mathsf{Var} \to \mathcal{D}^\sharp$
- $x^\sharp \sqsubseteq^\sharp_{\text{nr}} y^\sharp$ quand $\forall v \in \mathsf{Var}$, $x^\sharp(v) \sqsubseteq^\sharp y^\sharp(v)$
- $\gamma_{\text{nr}}\left(x^\sharp\right) = \left\{\rho \in (\mathsf{Var} \to \mathbb{Z}) \mid \forall v \in \mathsf{Var}, \sigma(v) \in \gamma\left(x^\sharp(v)\right)\right\}$
- $\alpha_{\text{nr}}(x) = v \mapsto \alpha\left(\{\rho(v) \mid \sigma \in x\}\right)$
- $\top_{\text{nr}} = v \mapsto \top$
- $\bot_{\text{nr}} = v \mapsto \bot$
- $x^\sharp \sqcup^\sharp_{\text{nr}} y^\sharp = v \mapsto x^\sharp(v) \sqcup^\sharp y^\sharp(v)$
- $x^\sharp \sqcap^\sharp_{\text{nr}} y^\sharp = v \mapsto x^\sharp(v) \sqcap^\sharp y^\sharp(v)$

Signes 1/4: abstraction d'une variable



$$\alpha(S) = \begin{cases} \top & \text{quand } \exists s, s' \in S, s < 0, s' > 0 \\ \leqslant 0 & \text{quand } \forall s \in S, s \leqslant 0 \wedge \exists s \in S, s < 0 \\ \geqslant 0 & \text{quand } \forall s \in S, s \geqslant 0 \wedge \exists s \in S, s > 0 \\ 0 & \text{quand } S = \{0\} \\ \bot & \text{quand } S = \emptyset \end{cases}$$

$$\begin{aligned} \gamma(\top) &= \mathbb{Z} \\ \gamma(\leqslant 0) &=]\!]-\infty, 0]\!] \\ \gamma(\geqslant 0) &= [\![0, +\infty[\![\\ \gamma(0) &= \{0\} \\ \gamma(\bot) &= \emptyset \end{aligned}$$

Abstraction d'un ensemble de valeurs pour une seule variable

Propriétés:

- **Sûreté de $\sqsubseteq$?** Prouver que $x^\sharp \sqsubseteq^\sharp y^\sharp \Rightarrow \gamma(x^\sharp) \subseteq \gamma(y^\sharp)$
- **Galois?** Prouver que $\gamma(\alpha(X)) \subseteq X$

Signes 2/4: abstraction de toutes les variables

- **Abstraction**: rappel: $\alpha_{\mathrm{nr}}(x) = v \mapsto \alpha\left(\{\sigma(v) \mid \sigma \in x\}\right)$

  Exemple: $x = \{(1,2),(2,3),(-1,7)\}$ $\alpha_{\mathrm{nr}}(x) =$**?**

- **Intersection (meet)**: rappel $x^\sharp \sqcap^\sharp_{\mathrm{nr}} y^\sharp = v \mapsto x^\sharp(v) \sqcap^\sharp y^\sharp(v)$. Exemple

  $x^\sharp = (\geqslant 0, 0), y^\sharp = (\top, \geqslant 0)$, $x^\sharp \sqcap^\sharp_{\mathrm{nr}} y^\sharp =$**?**

- **Essayez pour $\sqcup$ et $\sqsubseteq$**

Sémantique des expressions pour les domaines non-relationels

Sémantique des expressions: $[\![e]\!]^\sharp_{\mathrm{E}} : (\mathsf{Var} \to \mathcal{D}^\sharp) \to \mathcal{D}^\sharp$

$$
\begin{aligned}
[\![v]\!]^\sharp_{\mathrm{E}}(\rho) &= \rho(v) \\
[\![n]\!]^\sharp_{\mathrm{E}}(\rho) &= n^\sharp \\
[\![\textbf{rand}(n_1, n_2)]\!]^\sharp_{\mathrm{E}}(\rho) &= \textbf{rand}^\sharp(n_1, n_2) \\
[\![e_1 + e_2]\!]^\sharp_{\mathrm{E}}(\rho) &= [\![e_1]\!]^\sharp_{\mathrm{E}} +^\sharp [\![e_2]\!]^\sharp_{\mathrm{E}} \\
&\dots
\end{aligned}
$$

Sémantique des expressions pour les domaines non-relationels

Sémantique des expressions: $[\![e]\!]^\sharp_{\mathrm{E}} : (\mathsf{Var} \to \mathcal{D}^\sharp) \to \mathcal{D}^\sharp$

$$
\begin{aligned}
[\![v]\!]^\sharp_{\mathrm{E}}(\rho) &= \rho(v) \\
[\![n]\!]^\sharp_{\mathrm{E}}(\rho) &= n^\sharp \\
[\![\mathbf{rand}(n_1, n_2)]\!]^\sharp_{\mathrm{E}}(\rho) &= \mathbf{rand}^\sharp(n_1, n_2) \\
[\![e_1 + e_2]\!]^\sharp_{\mathrm{E}}(\rho) &= [\![e_1]\!]^\sharp_{\mathrm{E}} +^\sharp [\![e_2]\!]^\sharp_{\mathrm{E}} \\
&\dots
\end{aligned}
$$

Remarque

C'est tout à fait calculable.

Signes 3/4: définir les opérations arithmétiques abstraites

- $n^\sharp = \alpha(\{n\}) \begin{cases} \leqslant 0 & \text{si } n < 0 \\ \geqslant 0 & \text{si } n > 0 \\ 0 & \text{si } n = 0 \end{cases}$
- $\textbf{rand}^\sharp(n_1, n_2) = \alpha([\![n_1, n_2]\!]) = \begin{cases} \bot & \text{si } n_1 > n_2 \\ 0 & \text{si } n_1 = n_2 = 0 \\ \leqslant 0 & \text{sinon si } n_2 \leqslant 0 \\ \geqslant 0 & \text{sinon si } n_1 \geqslant 0 \\ \top & \text{sinon} \end{cases}$

Signes 3/4: définir les opérations arithmétiques abstraites (suite)

- $x^\sharp +^\sharp y^\sharp = \alpha\left(\{x + y \mid x \in \gamma(x^\sharp), y \in \gamma(y^\sharp)\}\right) =$

$+^\sharp$	$\top$	$\leqslant 0$	$\geqslant 0$	0	$\bot$
$\top$	$\top$	$\top$	$\top$	$\top$	$\bot$
$\leqslant 0$	$\top$	$\leqslant 0$	$\top$	$\leqslant 0$	$\bot$
$\geqslant 0$	$\top$	$\top$	$\geqslant 0$	$\geqslant 0$	$\bot$
0	$\top$	$\leqslant 0$	$\geqslant 0$	0	$\bot$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$

- **Definir** $-^\sharp$

Signes 4/4: définir les commandes abstraites

Sémantique des commandes: $[\![c]\!]^\sharp_{\mathrm{C}} : (\mathsf{Var} \to \mathcal{D}^\sharp) \to (\mathsf{Var} \to \mathcal{D}^\sharp)$

$$[\![v = e]\!]^\sharp_{\mathrm{C}}(\sigma) = \sigma\left[v \mapsto [\![e]\!]^\sharp_{\mathrm{E}}(\sigma)\right]$$
$$[\![e > 0]\!]^\sharp_{\mathrm{C}}(\sigma) = \sigma\left[e \mapsto \sigma(e) \sqcap^\sharp \alpha([\![1, +\infty[\![)\right]$$
$$\ldots$$

Que vaut $[\![x > 0]\!]^\sharp_{\mathrm{C}}(x \mapsto \top)$?

Remarque

C'est toujours parfaitement calculable.

Sémantique abstraite d'un programme (rappel)

Rappel : c'est la plus petite solution (selon l'ordre $\sqsubseteq^\sharp_{\mathrm{nr}}$) du système d'équations:

$$\begin{cases} R^\sharp_0 = \mathsf{Var} \to \top \\ R^\sharp_{k'} = \bigsqcup_{(k,c,k')\in A}{}^{\sharp_{\mathrm{nr}}} [\![c]\!]^\sharp_{\mathrm{C}}\,(R^\sharp_k) \qquad\qquad k' \neq 0 \end{cases}$$

qu'on calcule comme ceci:

1. On part de $R^{\sharp}{}^0 := L \to \bot_{\mathrm{nr}}$;
2. On calcule $R^{\sharp}{}^{i+1}$ à partir du précédent $R^{\sharp}{}^i$;
3. On revient à l'étape 2 jusqu'a aboutir à un point-fixe.

- Terminaison? Sûreté ?