Analyse de boucles

TAS : Typage et analyse statique
M2, Master STL INSTA, Sorbonne Université

Antoine Miné

Année 2021–2022

Cours 10
11 mars 2022

Plan du cours

Suite des sémantiques abstraites,
avec application à l'analyse numérique non-relationnelle.

- analyse des boucles :
  - principe des itérations avec accélération de la convergence ;
  - application à l'analyse d'intervalles.

$\Longrightarrow$ nous obtenons un analyseur **effectif**
pour des propriétés numériques non-triviales !

- conseils d'implantation pour le projet.

Analyse de boucles

Boucles et invariants

Rappel : sémantique concrète des boucles

Calcul de : $\mathsf{S}[\![\, \textbf{while}\ c\ \textbf{do}\ s \,]\!]\, R$

- $\mathsf{S}[\![\, \textbf{while}\ c\ \textbf{do}\ s \,]\!]\, R = \mathsf{C}[\![\, \neg c \,]\!]\, I$
- où I est un invariant de boucle inductif,
  l'ensemble des environnements accessibles
  à chaque itération de la boucle, au point : **while** • c **do** s.

I est la plus petite solution de l'équation :
$I = F(I)$ où $F(X) = R \cup \mathsf{S}[\![\, s \,]\!]\, (\mathsf{C}[\![\, c \,]\!]\, X)$.

Justification :

- $R \subseteq I$ — cas de la première itération de la boucle
- $\mathsf{S}[\![\, s \,]\!]\, (\mathsf{C}[\![\, c \,]\!]\, I) \subseteq I$ — stabilité par une itération de boucle
- I minimal. — meilleur invariant

Preuve d'existence :

F est croissante dans le treillis complet $(\mathcal{P}(\mathcal{E}), \subseteq, \emptyset, \mathcal{E}, \cup, \cap)$

$\Longrightarrow$ F a un plus petit point fixe $\text{lfp}\ F \stackrel{\text{def}}{=} \min \{\, I \mid F(I) = I \,\}$
de plus : $\text{lfp}\ F = \min \{\, I \mid F(I) \subseteq I \,\}$ (plus petit post point fixe)
c'est le Théorème de Tarksi

Rappel : interprétation par itération

$I = \text{lfp } F$ où $F(X) = R \cup \mathsf{S}[\![\, s \,]\!]\,(\mathsf{C}[\![\, c \,]\!]\, X)$
or F est continue dans le CPO $(\mathcal{P}(\mathcal{E}), \subseteq, \cup)$
$\Longrightarrow$ nous pouvons aussi appliquer le théorème de Kleene :

$$\text{lfp } F = \cup_{n \in \mathbb{N}} F^n(\emptyset)$$

I est la limite d'une séquence d'itérations (la séquence peut être infinie).

Intuition :

- $F^0(\emptyset) = \emptyset$
- $F^1(\emptyset) = R$
  environnements avant d'entrer dans la boucle
- $F^2(\emptyset) = R \cup \mathsf{S}[\![\, s \,]\!]\,(\mathsf{C}[\![\, c \,]\!]\, R)$
  environnements après zéro ou une itération de boucle
- $F^n(\emptyset)$: environnements après au plus $n-1$ itérations de la boucle
  juste avant de tester la condition de sortie,
  pour déterminer si une $n-$ième itération est nécessaire
- $\cup_{n \in \mathbb{N}} F^n(\emptyset)$ est bien l'invariant de boucle

$\Longrightarrow$ méthode constructive de calcul du meilleur invariant.

Exemple d'itération concrète

$$\begin{array}{l} V \leftarrow 0; \\ \textbf{while } V < 10 \textbf{ do} \\ \quad V \leftarrow V + 2 \\ \textbf{done} \end{array}$$

$\mathsf{S}[\![\, \textbf{while } V < 10 \textbf{ do } V \leftarrow V + 2 \,]\!]\, R = \mathsf{C}[\![\, V \geq 10 \,]\!]\, (\cup_{n \in \mathbb{N}} F^n(\emptyset))$

où $F(S) \stackrel{\text{def}}{=} \{0\} \cup \{\, V + 2 \mid V \in S \wedge V < 10 \,\}$:

n	$F^n(\emptyset)$
0	$\emptyset$
1	$\{0\}$
2	$\{0, 2\}$
3	$\{0, 2, 4\}$
4	$\{0, 2, 4, 6\}$
5	$\{0, 2, 4, 6, 8\}$
6	$\{0, 2, 4, 6, 8, 10\}$
7	$\{0, 2, 4, 6, 8, 10\}$

si $F^n(\emptyset) = F^{n+1}(\emptyset)$
alors $\forall i \geq n$: $F^i(\emptyset) = F^n(\emptyset)$

Nous trouvons donc :
$\cup_{n \in \mathbb{N}} F^n(\emptyset) = \{0, 2, 4, 6, 8, 10\} = \mathrm{lfp}\, F$

puis $\mathsf{S}[\![\, \textbf{while } V < 10 \textbf{ do } V \leftarrow V + 2 \,]\!]\, R = \{10\}$

Note : pour simplifier les notations, nous avons assimilé $\mathcal{P}(\{V\} \to \mathbb{Z})$ à $\mathcal{P}(\mathbb{Z})$.

Itération dans le domaine des intervalles

$V \leftarrow 0;$
while $V < 10$ **do**
$\quad V \leftarrow V + 2$
done

Principe :

remplacer $\cup_{n\in\mathbb{N}} F^n(\emptyset)$

où $F(X) = R \cup \mathsf{S}[\![s]\!](\mathsf{C}[\![c]\!] X)$

par $\dot\cup_{n\in\mathbb{N}} F^{\sharp n}(\dot\perp)$

où $F^\sharp(X^\sharp) = R^\sharp \cup^\sharp \mathsf{S}^\sharp[\![s]\!](\mathsf{C}^\sharp[\![c]\!] X^\sharp)$

en assimilant $\mathbb{V} \to \mathcal{D}^\sharp$ à un intervalle dans $\mathcal{D}^\sharp$, nous avons :

$\mathsf{C}^\sharp[\![V < 10]\!]\,[a,b] = [a, \min(9,b)]$

$\mathsf{S}^\sharp[\![V \leftarrow V + 2]\!]\,[a,b] = [a+2, b+2]$

e.g. :

$F^\sharp([0,10]) = [0,0] \cup^\sharp [0+2, \min(9,10)+2] = [0,11] = F^\sharp([0,11])$

n	$F^{\sharp n}(\dot\perp)$
0	$\perp$
1	$[0,0]$
2	$[0,2]$
3	$[0,4]$
4	$[0,6]$
5	$[0,8]$
6	$[0,10]$
7	$[0,11]$
8	$[0,11]$

Dans cet exemple :

- $[0,11]$ est correct mais approximatif (pas d'information de parité) ;
- le résultat est optimal pour les intervalles ;
- les itérés convergent en temps fini.

$\Longrightarrow$ est-ce toujours le cas ?

Itération abstraite : justification et limitation ⁂

Correction pour tout domaine abstrait $\mathcal{E}^\sharp$

Si $F^\sharp$ est une abstraction sûre de F
alors $\cup^\sharp_{n\in\mathbb{N}}\ F^{\sharp n}(\dot\perp)$ est une abstraction sûre de $\cup_{n\in\mathbb{N}}\ F^n(\emptyset)$, i.e. :

$$\cup_{n\in\mathbb{N}}\ F^n(\emptyset) \subseteq \gamma(\cup^\sharp_{n\in\mathbb{N}}\ F^{\sharp n}(\dot\perp))$$

Justification : par récurrence

- $\emptyset \subseteq \gamma(\dot\perp)$;
- si $F^n(\emptyset) \subseteq \gamma(F^{\sharp n}(\dot\perp))$, alors

$$\begin{array}{rcll} F(F^n(\emptyset)) & \subseteq & F(\gamma(F^{\sharp n}(\dot\perp))) & \text{(car } F \text{ est croissante)} \\ & \subseteq & \gamma(F^\sharp(F^{\sharp n}(\dot\perp))) & \text{(car } F^\sharp \text{ est une abstraction sûre de } F\text{)} \end{array}$$

  donc $\forall n$: $F^n(\emptyset) \subseteq \gamma(F^{\sharp n}(\dot\perp))$, et donc $\cup_{n\in\mathbb{N}}\ F^n(\emptyset) \subseteq \cup_{n\in\mathbb{N}}\ \gamma(F^{\sharp n}(\dot\perp))$
- si $\cup^\sharp$ est une abstraction sûre de $\cup$, alors de plus :
  $\cup_{n\in\mathbb{N}}\ F^n(\emptyset) \subseteq \cup_{n\in\mathbb{N}}\ \gamma(F^{\sharp n}(\emptyset)) \subseteq \gamma(\cup^\sharp_{n\in\mathbb{N}}\ F^{\sharp n}(\emptyset))$

Limitation :
Utiliser ce résultat suppose que $\cup^\sharp_{n\in\mathbb{N}}\ F^{\sharp n}(\dot\perp)$ existe dans $\mathcal{E}^\sharp$;
ce n'est pas toujours le cas (certains domaines abstraits ne sont pas des CPOs)
$\Longrightarrow$ nous verrons plus loin une preuve de correction plus puissante...

Non-terminaison de l'itération de sémantique concrète

$U \leftarrow 0$; $V \leftarrow 0$;
while $\textbf{rand}(0,1) = 0$ **do**
  if $U < 10$ **then** $U \leftarrow U + 1$
  else $V \leftarrow V + 1$
done

n	$F^n(\emptyset) \in \mathcal{P}(\{U,V\} \to \mathbb{Z})$
0	$\emptyset$
1	$\{(0,0)\}$
2	$\{(0,0),(1,0)\}$
	$\ldots$
11	$\{(0,0),(1,0),\ldots,(9,0),(10,0)\}$
12	$\{(0,0),(1,0),\ldots,(0,0),(10,0),(10,1)\}$
13	$\{(0,0),(1,0),\ldots,(0,0),(10,0),(10,1),(10,2)\}$
	$\ldots$

$\cup_{n\in\mathbb{N}} F^n(\emptyset) = \{\,(x,0)\,|\,x\in[0,10]\,\} \cup \{\,(10,y)\,|\,y\in\mathbb{N}\,\}$

La limite existe, mais est l'union d'un nombre infini d'itérés !

Non-terminaison de l'itération dans les intervalles

$U \leftarrow 0$; $V \leftarrow 0$;
while rand$(0,1) = 0$ **do**
  if $U < 10$ **then** $U \leftarrow U + 1$
  else $V \leftarrow V + 1$
done

n	$F^{\sharp n}(\dot{\perp}) \in \{U, V\} \to \mathcal{D}^\sharp$
0	$(\perp, \perp)$
1	$([0,0],[0,0])$
2	$([0,1],[0,0])$
	$\dots$
11	$([0,10],[0,0])$
12	$([0,10],[0,1])$
13	$([0,10],[0,2])$
	$\dots$

Analyse dans le domaine des intervalles :

$\cup^\sharp_{n\in\mathbb{N}} F^{\sharp n}(\dot{\perp}) = ([0,10],[0,+\infty])$

La limite abstraite existe,
mais c'est l'union d'un nombre infini d'itérés
$\Longrightarrow \cup^\sharp_{n\in\mathbb{N}} F^{\sharp n}(\dot{\perp})$ n'est pas calculable.

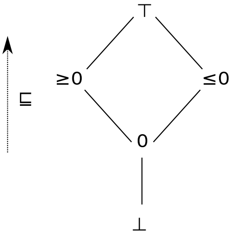
Terminaison de l'itération dans un domaine de hauteur finie

$U \leftarrow 0;\ V \leftarrow 0;$
while rand$(0,1) = 0$ **do**
  if $U < 10$ **then** $U \leftarrow U + 1$
  else $V \leftarrow V + 1$
done

n	$F^{\sharp n}(\dot\perp) \in \{U,V\} \to \mathcal{D}^\sharp$
0	$(\perp,\perp)$
1	$(0,0)$
2	$(\geq 0, 0)$
3	$(\geq 0, \geq 0)$
4	$(\geq 0, \geq 0)$

$\cup^\sharp_{n\in\mathbb{N}} F^{\sharp n}(\dot\perp) = (\geq 0, \geq 0)$

Analyse dans le domaine des signes :



Le domaine a une hauteur finie : pas de chaîne croissante infinie.
Toutes les itérations croissantes convergent en temps fini ;

$\Longrightarrow$ l'analyse est toujours calculable dans un domaine de hauteur finie.

Accélération de la convergence

Intuition : accélération de la convergence

$V \leftarrow 10;$
while $V \leq 100$ **do**
  $V \leftarrow V + 2$
done

Principe : relâcher les bornes non stables à l'infini

Sans accélération :

n	$F^{\sharp n}(\dot{\perp})$
0	$\perp$
1	$[10, 10]$
2	$[10, 12]$
3	$[10, 14]$
...	...
47	$[10, 102]$
48	$[10, 102]$

Avec accélération :

n	$F^{\sharp n}(\dot{\perp})$
0	$\perp$
1	$[10, 10]$
2	$[10, \infty]$
3	$[10, \infty]$

rappel : $F^\sharp(X^\sharp) = R^\sharp \cup^\sharp S^\sharp[\![s]\!] (C^\sharp[\![c]\!] X^\sharp)$

$\Longrightarrow$ convergence vers un résultat moins précis, mais plus rapidement !

Opérateur d'élargissement

Accélérer la convergence par extrapolation entre itérés successifs.

Élargissement : $\triangledown : (\mathcal{E}^\sharp \times \mathcal{E}^\sharp) \to \mathcal{E}^\sharp$ *widening*

- opérateur binaire $X^\sharp \triangledown Y^\sharp \in \mathcal{E}^\sharp$;
- sur-approximation de l'union :
  $\gamma(X^\sharp) \cup \gamma(Y^\sharp) \subseteq \gamma(X^\sharp \triangledown Y^\sharp)$
- pour toute séquence $Y_0^\sharp, Y_1^\sharp, \ldots, Y_n^\sharp, \ldots$

$$\text{la séquence } \begin{cases} X_0^\sharp = Y_0^\sharp \\ X_1^\sharp = X_0^\sharp \triangledown Y_1^\sharp \\ \ldots \\ X_n^\sharp = X_{n-1}^\sharp \triangledown Y_n^\sharp \\ \ldots \end{cases}$$

converge en temps fini : $\exists N : \forall n \geq N : X_n^\sharp = X_N^\sharp$.

Élargissement standard dans les intervalles

Élargissement d'intervalles : $\triangledown : (\mathcal{D}^\sharp \times \mathcal{D}^\sharp) \to \mathcal{D}^\sharp$

$$\forall I \in \mathcal{D}^\sharp : \bot \triangledown I = I \triangledown \bot = I$$

$$[a, b] \triangledown [c, d] \stackrel{\text{def}}{=} \left[\begin{cases} a & \text{si } a \le c \\ -\infty & \text{si } c < a \end{cases}, \begin{cases} b & \text{si } b \ge d \\ +\infty & \text{si } d > b \end{cases} \right]$$

- une borne inférieure non stable est mise à $-\infty$;
- une borne supérieure non stable est mise à $+\infty$;
- une fois à $-\infty$ ou $+\infty$, les bornes sont nécessairement stables !

Élargissement point à point sur $\mathcal{E}^\sharp$: $\dot{\triangledown} : (\mathcal{E}^\sharp \times \mathcal{E}^\sharp) \to \mathcal{E}^\sharp$

Dans le cas de plusieurs variables $\mathcal{E}^\sharp \stackrel{\text{def}}{=} \mathbb{V} \to \mathcal{D}^\sharp$,
chaque variable est extrapolée de manière indépendante :

$$X^\sharp \mathbin{\dot{\triangledown}} Y^\sharp \stackrel{\text{def}}{=} \lambda V \in \mathbb{V}. X^\sharp(V) \triangledown Y^\sharp(V)$$

Application : itération avec élargissement

Limite concrète :

Nous pouvons interpréter $\cup_{n\in\mathbb{N}} F^n(\emptyset)$ comme la limite de la séquence :

$$\begin{cases} X_0 & \stackrel{\text{def}}{=} & \emptyset \\ X_{n+1} & \stackrel{\text{def}}{=} & X_n \cup F(X_n) \end{cases}$$

(cela permet d'exposer les deux éléments sur lesquels faire l'extrapolation : X_n et $F(X_n)$)

Limite abstraite :

Dans l'abstrait, nous calculons :

$$\begin{cases} X_0^\sharp & \stackrel{\text{def}}{=} & \perp \\ X_{n+1}^\sharp & \stackrel{\text{def}}{=} & X_n^\sharp \triangledown F^\sharp(X_n^\sharp) \end{cases}$$

jusqu'à avoir $X_{n+1}^\sharp = X_n^\sharp$.

Correction et terminaison ⁂

$$\begin{cases} X_0^\sharp & \stackrel{\text{def}}{=} & \dot\bot \\ X_{n+1}^\sharp & \stackrel{\text{def}}{=} & X_n^\sharp \triangledown F^\sharp(X_n^\sharp) \end{cases}$$

Terminaison : $\exists N: X_{N+1}^\sharp = X_N^\sharp$

Preuve : par l'absurde

Sinon, $X_0^\sharp, X_1^\sharp, \ldots, X_n^\sharp, \ldots$ serait une séquence infinie de la forme $X_0^\sharp = Y_0^\sharp$, $X_{n+1}^\sharp = X_n^\sharp \triangledown Y_{n+1}^\sharp$, où $Y_0^\sharp = \dot\bot$, $Y_{n+1}^\sharp = F^\sharp(X_n^\sharp)$.

Ceci serait contraire à la définition de $\triangledown$.

Correction : $\text{lfp}\, F \subseteq \gamma(X_N^\sharp)$

Preuve :

Par le théorème de Tarski, $\text{lfp}\, F = \min \{ I \mid F(I) \subseteq I \}$.

Il suffit donc de prouver que $\gamma(X_N^\sharp)$ est un post point fixe de F :

$$\begin{array}{lcll} F(\gamma(X_N^\sharp)) & \subseteq & \gamma(F^\sharp(X_N^\sharp)) & \text{(sûreté de } F^\sharp\text{)} \\ & \subseteq & \gamma(X_N^\sharp) \cup \gamma(F^\sharp(X_N^\sharp)) & \\ & \subseteq & \gamma(X_N^\sharp \triangledown F^\sharp(X_N^\sharp)) & \text{(sûreté de } \triangledown\text{)} \\ & = & \gamma(X_{N+1}^\sharp) & \text{(définition de } X_{N_1}^\sharp\text{)} \\ & = & \gamma(X_N^\sharp) & \text{(car } X_{N+1}^\sharp = X_N^\sharp\text{)} \end{array}$$

Note : la preuve ne suppose pas l'existence de $\cup^\sharp_{n\in\mathbb{N}} F^{\sharp n}(\dot\bot)$!

Exemple d'itération avec élargissement

$U \leftarrow 0;\ V \leftarrow 0;$
while rand$(0,1) = 0$ **do**
  if $U < 10$ **then** $U \leftarrow U + 1$
  else $V \leftarrow V + 1$
done

n	$X_0^\sharp = \dot{\bot},\ X_{n+1}^\sharp = X_n^\sharp \triangledown F(X_n^\sharp)$				
0					$(\bot, \bot)$
1	$(\bot, \bot)$	$\triangledown$	$([0,0],[0,0])$	$=$	$([0,0],[0,0])$
2	$([0,0],[0,0])$	$\triangledown$	$([0,1],[0,0])$	$=$	$([0,+\infty],[0,0])$
3	$([0,+\infty],[0,0])$	$\triangledown$	$([0,+\infty],[0,1])$	$=$	$([0,+\infty],[0,+\infty])$
4	$([0,+\infty],[0,+\infty])$	$\triangledown$	$([0,+\infty],[0,+\infty])$	$=$	$([0,+\infty],[0,+\infty])$

Convergence en au plus $2|\mathbb{V}|$ itérations (nombre de bornes à stabiliser).

Note : boucles imbriquées

$U \leftarrow 0$; $V \leftarrow 0$;
while $\bullet$ $U < 100$ **do**
    while $\bullet$ $V < U$ **do** $V \leftarrow V + 1$ **done**;
    $U \leftarrow U + 1$; $V \leftarrow 0$
done

à $\bullet$: $n = 0, ; (\bot, \bot)$ $n = 1,\ ([0,0],[0,0])$ $n = 2,\ ([0,+\infty],[0,0])$

a $\bullet$:

n	
0	$(\bot,\bot)$

n	
0	$(\bot,\bot)$
1	$([0,0],[0,0])$

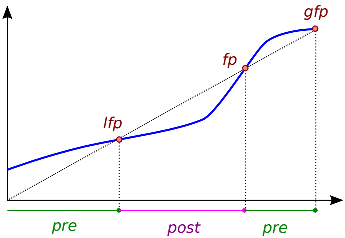
n	
0	$(\bot,\bot)$
1	$([0,+\infty],[0,0])$
2	$([0,+\infty],[0,+\infty])$

La sémantique concrète des boucles imbriquées est formée de point fixes imbriqués.

La sémantique abstraite génère des itérations imbriquées.

Pour chaque itération avec $\triangledown$ de la boucle externe, une séquence complète d'itération avec $\triangledown$ de la boucle interne est calculée !

Raisonnement inductif et élargissement : intuition ⁂



Invariant inductifs :

- $\text{lfp } F$ est le plus petit invariant ;
- $\text{lfp } F \subseteq I \implies I$ est un invariant ;
- $F(I) \subseteq I \implies I$ est un invariant inductif $\implies I$ est aussi un invariant (Tarksi) ;
- $F^\sharp(I^\sharp) \sqsubseteq I^\sharp \implies I^\sharp$ est un invariant inductif **prouvable dans l'abstrait**.

Généralités sur le raisonnement inductif :

- induction = généralisation à partir d'un petit ensemble d'observations ;
  e.g., si la borne supérieure croît, elle est probablement non-bornée ;
  processus cognitif important !
- $\neq$ induction en mathématiques, qui est *déductive* par nature
  (application d'un axiome d'induction)
- en logique philosophique, le raisonnement inductif n'est pas fiable
  (puisqu'il généralise à partir d'un nombre fini d'exemples)
- mais, en interprétation abstraite, l'élargissement $\triangledown$ effectue un raisonnement inductif toujours sûr !

Itérations avancées

Principe

L'utilisation d'un élargissement $\triangledown$ permet d'obtenir une itération :

- qui termine toujours ;
- avec un nombre d'itérations indépendant des constates du programme ;
  (e.g., l'analyse de **while** $N < 100$ **do** $V \leftarrow V + 1$ **done** ne dépend pas du choix de 100)
- mais qui est souvent imprécise.

De nombreux travaux visent à améliorer la précision du calcul.

Quelques idées d'amélioration :

- définir un opérateur $\triangledown$ plus précis :
- appliquer $\triangledown$ moins souvent ;
- faire une analyse par cas pour certaines itérations de la boucle ;
- raffiner le résultat *a posteriori*.

Comparaison des signes et des intervalles : exemple

$V \leftarrow 100;$
while • $V > 0$ **do**
  $V \leftarrow V - 1$
done

n	signes	intervalles
0	$\perp$	$\perp$
1	> 0	$[100, 100]$
2	≥ 0	$[-\infty, 100]$

Comparaison de l'analyse :

- dans les signes stricts, sans élargissement ;
  nous utilisons des signes améliorés, avec signes stricts : $\{\perp, 0, > 0, < 0, \geq 0, \leq 0, \top\}$
- dans les intervalles, avec élargissement.

Le domaine des intervalles est strictement plus expressif ;
pourtant, l'analyse d'intervalles ne trouve pas $V \geq 0$,
qui est trouvé par une analyse de signe !

Explication :

la borne inférieure, non stable, est élargie à $-\infty$,
pourtant, la borne 0, non testée, est bien stable !

Solution : élargissement avec étages

$V \leftarrow 100;$
while • $V > 0$ **do**
  $V \leftarrow V - 1$
done

Analyse avec élargissement étagé $\triangledown_{\{0\}}$

n	intervalles
0	$\perp$
1	$[100, 100]$
2	$[0, 100]$

Solution : élargissement avec étages $\triangledown_T$, plus précis.

Étant donné un ensemble $T \subseteq \mathbb{Z}$ fini, contenant $-\infty$, $+\infty$:

$[a, b] \triangledown_T [c, d] \stackrel{\text{def}}{=}$

$$\left[\begin{cases} a & \text{si } a \le c \\ \max \{ t \in T \mid t \le c \} & \text{si } c < a \end{cases}, \begin{cases} b & \text{si } b \ge d \\ \min \{ t \in T \mid t \ge d \} & d > b \end{cases} \right]$$

- teste si les valeurs de T sont des bornes stables ;
  (dans notre exemple, on trouve $[\max \{ c \in T \mid c \le 0 \}, 100]$)
- termine toujours, car T est fini (au pire, on obtient $-\infty$ ou $+\infty$).

Choix des étages

Comment choisir T ?

- $0 \in T$ permet d'être au moins aussi précis que les signes ;
- inclure les constantes apparaissant dans le programme ;
- inclure les tailles de tableau (± 1) ;
  (utile pour vérifier les dépassements de tableau)
- utiliser une séquence géométrique : $T = \{\, \pm 2^i \mid i \in [0, 31] \,\} \cup \{\pm\infty\}$.
  (pour prouver l'absence de dépassement de capacité, il suffit que T soit suffisamment dense)

Note : ⋆⋆⋆ points fixes stables et instables

Que se passe-t-il si T ne contient pas exactement la borne la plus précise ?

```
V ← 100;
while rand(0, 1) = 0 do
    V ← V − 1;
    if V < 0 then V ← 0
done
```

Cas stable.
$[t, 100]$ est un point fixe pour tout $t \le 0$.
Il suffit d'avoir $-\infty \ne t \le 0$ fini dans T pour trouver une borne t finie.
L'optimal n'est atteint que si $0 \in T$.

```
V ← 100;
while rand(0, 1) = 0 do
    V ← V − 1;
    if V = −1 then V ← 0
done
```

Cas instable.
$[t, 100]$ est un point fixe uniquement pour $t = 0$.
Il faut avoir $0 \in T$ pour trouver une borne finie, sinon, on trouve toujours $[-\infty, 100]$.

Élargissement retardé

```
V ← 0;
while rand(0,1) = 0 do
    if V = 0 then V ← 1;
    ...
done
```

V n'est incrémenté qu'une seule fois, de 0 à 1.

Problème :

$\triangledown$ trouvera V non stable, et le placera à $[0, +\infty] \Longrightarrow$ perte de précision
(en effet, $[0, 0] \triangledown [0, 1] = [0, +\infty]$)

Solution : **retarder** l'élargissement d'une (ou plusieurs) itération(s) :

$$X_{n+1} \stackrel{\text{def}}{=} \begin{cases} F^\sharp(X_n^\sharp) & \text{si } n < N \\ X_n^\sharp \triangledown F^\sharp(X_n^\sharp) & \text{si } n \geq N \end{cases}$$

(rappel : $F^\sharp(X^\sharp) = R^\sharp \cup^\sharp \mathsf{S}^\sharp[\![s]\!] (\mathsf{C}^\sharp[\![c]\!] X^\sharp)$)

(dans notre exemple, avec $N = 1$, $X_1^\sharp = [0, 0] \cup^\sharp [1, 1] = [0, 1]$, $X_2^\sharp = [0, 1] \triangledown [0, 1] = [0, 1] = X_1^\sharp$)

Il est nécessaire de reprendre les itérations avec $\triangledown$ après un nombre fini d'itérations pour assurer la convergence en temps fini !

Déroulement de boucles : problème

$U \leftarrow$ **rand**$(-\infty, +\infty)$; $V \leftarrow 1$;
while rand$(0, 1) = 0$ **do**
  if $V = 1$ **then** $V \leftarrow 0$; $U \leftarrow 0$;
  $U \leftarrow U + 1$
  assert $U \neq 0$
done

Au début de la boucle, U n'est pas initialisé (modélisé par $[-\infty, +\infty]$) ;
U est initialisé pendant le premier tour de boucle, puis il est incrémenté
$\Longrightarrow U \geq 0$ quand *stat* est exécuté

Imprécision :

L'invariant de boucle le plus précis est :

$$(V = 1 \wedge U \in [-\infty, +\infty]) \vee (V = 0 \wedge U \geq 0)$$

Dans les intervalles, non-relationnels, nous ne pouvons exprimer que :

$V \in [0, 1] \wedge U \in [-\infty, +\infty]$!

$\Longrightarrow$ échec de l'assertion

Une solution serait d'utiliser un domaine plus précis, capable de représenter des disjonctions.
Nous verrons un tel domaine plus loin dans le cours.
Dans le transparent suivant, nous proposons une solution plus simple à ce problème.

Déroulement de boucles : sémantique concrète

Solution : déroulement de boucle

Analyser les N premières itérations de la boucle séparément
puis calculer un point fixe rassemblant les itérations après N.

Dans le concret :

Pour $\mathsf{S}[\![\, \textbf{while } c \textbf{ do } s \,]\!]\, R$:

- $X_0 \stackrel{\text{def}}{=} R$ (environnements d'entrée)
- $\forall i \leq N$: $X_i \stackrel{\text{def}}{=} \mathsf{S}[\![\, s \,]\!]\, (\mathsf{C}[\![\, c \,]\!]\, X_{i-1})$ (N déroulements)
- $\forall i > N$: $X_i \stackrel{\text{def}}{=} X_N \cup \mathsf{S}[\![\, s \,]\!]\, (\mathsf{C}[\![\, c \,]\!]\, X_{i-1})$ (itérés de point fixe à partir de N)
  $X_\omega \stackrel{\text{def}}{=} \cup_{i \geq N}\ X_i$ (limite du point fixe)

On peut réécrire la sémantique de la boucle comme :

$$\mathsf{S}[\![\, \textbf{while } c \textbf{ do } s \,]\!]\, R = (\cup_{i<N}\ \mathsf{C}[\![\, \neg c \,]\!]\, X_i) \cup \mathsf{C}[\![\, \neg c \,]\!]\, X_\omega$$

(pensez à rassembler, avec $\cup$, les déroulements $< N$ et le point fixe en sortie de boucle !)

dans le concret, c'est strictement équivalent car $\mathsf{S}[\![\, \cdot \,]\!]$ et $\mathsf{C}[\![\, \cdot \,]\!]$ commutent avec $\cup$...
dans l'abstrait, cela sera plus précis car on appliquera ∇ sur moins d'itérés,
et l'union $\cup$ est retardée après le calcul du point fixe et l'application de la condition de sortie

Déroulement de boucles : analyse abstraite

$U \leftarrow$ **rand**$(-\infty, +\infty)$; $V \leftarrow 1$;
while rand$(0,1) = 0$ **do**
  if $V = 1$ **then** $V \leftarrow 0$; $U \leftarrow 0$ **endif**;
  $U \leftarrow U + 1$
  assert $U \neq 0$
done

Dans l'abstrait :

- $\forall i \leq N$: $X_i^\sharp \stackrel{\text{def}}{=} \mathsf{S}^\sharp[\![s]\!] (\mathsf{C}^\sharp[\![c]\!] X_{i-1}^\sharp)$ (N déroulements abstraits)
- $\forall i > N$: $X_i^\sharp \stackrel{\text{def}}{=} X_{i-1}^\sharp \,\triangledown\, (X_N^\sharp \cup^\sharp \mathsf{S}[\![s]\!] (\mathsf{C}^\sharp[\![c]\!] X_{i-1}^\sharp))$ (itérés abstraits avec $\triangledown$)
  jusqu'à avoir $X_{\delta+1}^\sharp = X_\delta^\sharp$ (limite des itérés)
- $\mathsf{S}^\sharp[\![$ **while** c **do** $s]\!]\, R \stackrel{\text{def}}{=} (\cup_{i<N}^\sharp \mathsf{C}^\sharp[\![\neg c]\!] X_i^\sharp) \cup^\sharp \mathsf{C}^\sharp[\![\neg c]\!] X_\delta^\sharp$

  (rassemblement des itérés en sortie de boucle)

Dans l'exemple, pour $N = 1$:
$X_0^\sharp = [U \mapsto [-\infty, +\infty], V \mapsto [1,1]]$
$X_1^\sharp = [U \mapsto [1,1], V \mapsto [0,0]]$
$X_2^\sharp = [U \mapsto [1, +\infty], V \mapsto [0,0]] = X_3^\sharp$
(ne pas confondre avec l'élargissement retardé, incapable de faire une analyse par cas !)

Itérations décroissantes

$$V \leftarrow 0;$$
$$\textbf{while } V \leq 50 \textbf{ do } V \leftarrow V + 1 \textbf{ done}$$

Imprécision

Dans cet exemple, nous trouvons $V \in [0, +\infty]$ comme invariant de boucle, mais l'invariant de boucle le plus précis est $V \in [0, 51]$.

Solution : itérations décroissantes de raffinement

Remarque, nous cherchons un point fixe $X_N^\sharp = F^\sharp(X_N^\sharp)$

mais nous avons en réalité un point fixe $X_N^\sharp = X_N^\sharp \triangledown F^\sharp(X_N^\sharp)\ldots$

Il est possible que $F^\sharp(X_N^\sharp) \sqsubset X_N^\sharp$

dans ce cas, $F^\sharp(X_N^\sharp)$ est un invariant plus précis que $X_N^\sharp$.

$\Longrightarrow$ après stabilisation de $X_{n+1}^\sharp = X_n^\sharp \triangledown F^\sharp(X_n^\sharp)$
calculer $X_{n>N}^\sharp = F^\sharp(X_{n-1}^\sharp)$ sans élargissement, tant que $X_n^\sharp$ décroît !

Itérations décroissantes : exemple

$V \leftarrow 0;$
while $V \leq 50$ **do** $V \leftarrow V + 1$ **done**

$$F^\sharp(X^\sharp) \stackrel{\text{def}}{=} [0,0] \,\dot\cup^\sharp\, \mathsf{S}^\sharp[\![\, V \leftarrow V+1 \,]\!]\,(\mathsf{C}^\sharp[\![\, V \leq 50 \,]\!]\, X^\sharp)$$

- $X^\sharp_N \stackrel{\text{def}}{=} \;= [0, +\infty]$ (limite des itérations avec élargissement)
- $X^\sharp_{N+1} = F^\sharp(X^\sharp_N) = [0,0] \cup^\sharp ([0,50] +^\sharp [1,1]) = [0,0] \cup^\sharp [1,51] = [0,51]$
- $X^\sharp_{N+2} = F^\sharp(X^\sharp_{N+1}) = [0,51] = X^\sharp_{N+1}$

$\Longrightarrow$ dans ce cas, nous trouvons l'invariant le plus précis exprimable dans les intervalles !

En sortie de boucle, nous avons : $\mathsf{C}^\sharp[\![\, V > 50 \,]\!]\,[0,51] = [51,51]$.

Itérations décroissantes : correction et terminaison

Correction :

Nous avons vu que, comme $F^\sharp(X_N^\sharp) \sqsubseteq X_N^\sharp$, alors $F(\gamma(X_N^\sharp)) \subseteq \gamma(X_N^\sharp)$ et donc $\mathrm{lfp}\, F \subseteq \gamma(X_N^\sharp)$.
Nous calculons $X_{N+n}^\sharp = F^{\sharp\, n}(X_N^\sharp)$.
Par monotonie de F, $F^n(\mathrm{lfp}\, F) \subseteq F^n(\gamma(X_N^\sharp))$.
Par définition de lfp, $\mathrm{lfp}\, F = F^n(\mathrm{lfp}\, F)$.
Par sûreté de $F^\sharp$, il vient $F^n(\gamma(X_N^\sharp)) \subseteq \gamma(F^{\sharp\, n}(X_N^\sharp))$.
Donc $\mathrm{lfp}\, F \subseteq \gamma(F^{\sharp\, n}(X_N^\sharp))$.

Terminaison :

- la séquence décroissante $X_{n>N}^\sharp = F^\sharp(X_n^\sharp)$ peut être infinie ;
  ($[0, +\infty] \supseteq [1, +\infty] \supseteq [2, +\infty] \supseteq \cdots$)
- tous les itérés $X_{n>N}^\sharp = F^\sharp(X_n^\sharp)$ sont des invariants corrects
  $\Longrightarrow$ nous pouvons arrêter le raffinement à tout instant ;
- un opérateur de rétrécissement $\triangle$ permet de forcer la convergence en temps fini :

  $X_{n>N}^\sharp \stackrel{\text{def}}{=} X_{n-1}^\sharp \triangle F^\sharp(X_{n-1}^\sharp)$ où

  $$[a, b] \triangle [c, d] \stackrel{\text{def}}{=} \left[\begin{cases} c & \text{si } a = -\infty \\ a & \text{sinon} \end{cases}, \begin{cases} d & \text{if } b = +\infty \\ b & \text{sinon} \end{cases} \right]$$

  (seules les bornes à l'infini sont raffinées)

Remarque : non-croissance de l'élargissement ⁂

Exemple : considérons encore $stat \stackrel{\text{def}}{=}$ **while** $V \leq 50$ **do** $V \leftarrow V + 1$ **done**

nous avons $\quad S^\sharp[\![\, stat \,]\!]\, R^\sharp \;=\; C^\sharp[\![\, V > 50 \,]\!]\, (\lim \lambda X^\sharp . X^\sharp \mathbin{\dot\triangledown} F^\sharp(R^\sharp, X^\sharp))$

où $\quad F^\sharp(R^\sharp, X^\sharp) \stackrel{\text{def}}{=} R^\sharp \mathbin{\dot\cup^\sharp} S^\sharp[\![\, V \leftarrow V + 1 \,]\!]\, (C^\sharp[\![\, V \leq 50 \,]\!]\, X^\sharp)$

$\triangledown$ n'est pas croissant vis à vis de son argument de gauche :

e.g., $[0,0] \triangledown [0,51] = [0,+\infty]$, mais $[0,51] \triangledown [0,51] = [0,51]$

- si $R^\sharp = [0,0]$, les itérés de $F^\sharp$ sont : $\perp$, $[0,0]$, $[0,+\infty]$

  $[0,0] \triangledown F^\sharp([0,0],[0,0]) = [0,0] \triangledown ([0,0] \cup^\sharp [1,1]) = [0,0] \triangledown [0,1] = [0,+\infty]$

  $\Longrightarrow S^\sharp[\![\, stat \,]\!]\, ([0,0]) = [51,+\infty]$

- si $R^\sharp = [0,51]$, les itérés de $F^\sharp$ sont : $\perp$, $[0,51]$, $[0,51]$

  $[0,51] \triangledown F^\sharp([0,51],[0,51]) = [0,51] \triangledown ([0,0] \cup^\sharp [1,51]) = [0,51] \triangledown [0,51] = [0,51]$

  $\Longrightarrow S^\sharp[\![\, stat \,]\!]\, ([0,51]) = [51,51]$

$\Longrightarrow S^\sharp[\![\, stat \,]\!]$ n'est pas croissant

Ceci intervient en particulier dans le cas de boucles imbriquées :
la boucle externe itère $X^\sharp_{n+1} = X^\sharp_n \triangledown F^\sharp(X^\sharp_{n+1})$
où $F^\sharp$ n'est pas croissante car elle continent un élargissement.

Cela ne pose pas de problème : l'élargissement de la boucle externe garanti la sûreté et la terminaison même si $F^\sharp$ n'est pas croissante !
La seule hypothèse importante de croissance est celle de F, i.e. : dans le concret.

Conseils d'implantation OCaml pour le projet

Itérateur

L'interprète fourni contient un itérateur de boucles très simple, sans accélération.

interpreter/interpreter.ml

```
let rec eval_stat (a:t) ((s,ext):stat ext) : t = match s with
   | AST_while (e,s) ->
        (* simple fixpoint *)
        let rec fix (f:t -> t) (x:t) : t =
          let fx = f x in
          if D.subset fx x then fx
          else fix f fx
        in
        (* function to accumulate one more loop iteration:
           F(X(n+1)) = X(0) U body(F(X(n))
           we apply the loop body and add back the initial abstract state
         *)
        let f x = D.join a (eval_stat (filter x e true) s) in
        (* compute fixpoint from the initial state (i.e., a loop invariant) *)
        let inv = fix f a in
        (* and then filter by exit condition *)
        filter inv e false
```

`fix f fx` correspond à $X^\sharp_{n+1} = F^\sharp(X^\sharp_n)$,

il faudra le changer en $X^\sharp_{n+1} = X^\sharp_n \triangledown F^\sharp(X^\sharp_n)$...

puis ajouter le délai sur $\triangledown$, le déroulement de boucles, etc.

(Note : retourner `fx` quand `D.subseteq fx x` correspond à une itération décroissante)