

Rappel sur les domaines abstraits

Domaines abstraits

Un domaine abstrait permet de représenter une surapproximation d'un ensemble \mathcal{D} de propriétés, aussi appelées invariants, du programme analysé. Il doit également permettre de calculer ces surapproximations.

Un domaine abstrait doit donc spécifier :

- un ensemble $\mathcal{D}^\#$ muni d'une structure de *treillis*, soit :
 - un ordre partiel $\sqsubseteq^\#$;
 - une borne supérieure binaire $\sqcup^\#$;
 - une borne inférieure binaire $\sqcap^\#$;
 - deux extremums \top et \perp ;
- une fonction de *concrétisation* $\gamma : \mathcal{D}^\# \rightarrow \mathcal{D}$, l'ordre abstrait $\sqsubseteq^\#$ devant représenter l'ordre concret \sqsubseteq , cette fonction doit être monotone :

$$\forall x^\#, y^\# \in \mathcal{D}^\#, \quad x^\# \sqsubseteq^\# y^\# \Rightarrow \gamma(x^\#) \sqsubseteq \gamma(y^\#),$$

on notera que cette fonction est purement mathématique, nul besoin de l'implémenter ;

- (*éventuellement*) une fonction d'*abstraction* $\alpha : \mathcal{D} \rightarrow \mathcal{D}^\#$ formant une correspondance de Galois avec γ , mais on n'a pas toujours existence d'une telle fonction ;
- des équivalents abstraits (par exemple $+^\# : (\mathcal{D}^\# \times \mathcal{D}^\#) \rightarrow \mathcal{D}^\#$) des opérations concrètes (par exemple $+$: $(\mathcal{D} \times \mathcal{D}) \rightarrow \mathcal{D}$), ces opérations doivent être des surapproximations *correctes* (sound en anglais) de la version concrète :

$$\forall x^\#, y^\# \in \mathcal{D}^\#, \quad \gamma(x^\#) + \gamma(y^\#) \sqsubseteq \gamma(x^\# +^\# y^\#),$$

on notera que si l'on dispose d'une correspondance de Galois, la meilleure opération abstraite est donnée par $x^\# +^\# y^\# = \alpha(\gamma(x^\#) + \gamma(y^\#))$;

- si le treillis $\mathcal{D}^\#$ possède des chaînes strictement croissantes infinies, il faut un *élargissement* (widening en anglais) ∇ pour garantir la convergence de l'analyse :
 - $\forall x^\#, y^\# \in \mathcal{D}^\#, \quad x^\# \sqcup^\# y^\# \sqsubseteq^\# x^\# \nabla y^\#$;
 - pour toute suite $(x^\#)_{n \in \mathbb{N}}$, la suite croissante

$$\begin{cases} y_0^\# &= x_0^\# \\ y_{i+1}^\# &= y_i^\# \nabla x_{i+1}^\# \end{cases}$$

est stationnaire.

Domaines abstraits numériques non relationnels

Dans notre cas, $(\mathcal{D}, \sqsubseteq) = (\mathcal{P}(\mathbb{Z}), \subseteq)$.