Rappel sur les domaines abstraits

Domaines abstraits

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

Un domaine abstrait doit donc spécifier :

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

  $$\forall x^\sharp, y^\sharp \in \mathscr{D}^\sharp, \quad x^\sharp \sqsubseteq^\sharp y^\sharp \;\Rightarrow\; \gamma\left(x^\sharp\right) \sqsubseteq \gamma\left(y^\sharp\right),$$

  on notera que cette fonction est purement mathématique, nul besoin de l'implémenter ;
- (*éventuellement*) une fonction d'*abstraction* $\alpha : \mathscr{D} \to \mathscr{D}^\sharp$ formant une correspondance de Galois avec γ, mais on n'a pas toujours existence d'une telle fonction ;
- des équivalents abstraits (par exemple $+^\sharp : \left(\mathscr{D}^\sharp \times \mathscr{D}^\sharp\right) \to \mathscr{D}^\sharp$) des opérations concrètes (par exemple $+ : (\mathscr{D} \times \mathscr{D}) \to \mathscr{D}$), ces opérations doivent être des surapproximations *correctes* (sound en anglais) de la version concrète :

  $$\forall x^\sharp, y^\sharp \in \mathscr{D}^\sharp, \quad \gamma\left(x^\sharp\right) + \gamma\left(y^\sharp\right) \;\sqsubseteq\; \gamma\left(x^\sharp +^\sharp y^\sharp\right),$$

  on notera que si l'on dispose d'une correspondance de Galois, la meilleure opération abstraite est donnée par $x^\sharp +^\sharp y^\sharp = \alpha\left(\gamma\left(x^\sharp\right) + \gamma\left(y^\sharp\right)\right)$;
- si le treillis $\mathscr{D}^\sharp$ possède des chaînes strictement croissantes infinies, il faut un *élargissement* (widening en anglais) $\triangledown$ pour garantir la convergence de l'analyse :
  - $\forall x^\sharp, y^\sharp \in \mathscr{D}^\sharp, \quad x^\sharp \sqcup^\sharp y^\sharp \;\sqsubseteq^\sharp\; x^\sharp \triangledown y^\sharp$;
  - pour toute suite $\left(x^\sharp\right)_{n\in\mathbb{N}}$, la suite croissante

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

    est stationnaire.

Domaines abstraits numériques non relationnels

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