Fonction d'abstraction

Un problème qu'on a déjà vu plusieurs fois maintenant :

Étant donné un ensemble $A \in L^\flat = \mathbb{P}(\mathcal{V}al \cup \{\mathsf{Err}, \mathsf{Wrong}\})$, quelle est sa meilleure abstraction (si elle existe) ?

On pose : $\alpha(A) = \min_{\sqsubseteq^\sharp}\{v \in L^\sharp \mid A \subseteq \gamma(v)\}$ (abstraction).

Note : exige que le côté droit soit bien défini. ($\min_{\sqsubseteq^\sharp} S$ est le plus petit élément de S : $\min_{\sqsubseteq^\sharp} S \in S$ et $\min_{\sqsubseteq^\sharp} S \sqsubseteq^\sharp v$ pour tout $v \in S$.)

Calcul abstrait

Une paire (α, γ) permet de définir une meilleure approximation possible de chaque opération concrète (meilleur = $\subseteq$-minimal) :

$$
\begin{array}{rcl}
a^\sharp & \hat{=} & \alpha\{a\} \\
\text{(par ex.: } 0^\sharp & \hat{=} & \alpha\{0\} = \mathbb{Z}\text{)} \\
v_1 +^\sharp v_2 & \hat{=} & \alpha\{a_1 + a_2 \mid a_1 \in \gamma(v_1), a_2 \in \gamma(v_2)\} \\
-^\sharp v & \hat{=} & \alpha\{-a \mid a \in \gamma(v)\} \\
 & & \ldots
\end{array}
$$

Point `(*3*)` et correction

$1\ /\ 0 \hat{=} \mathsf{Err}$ est abstrait en $+/+\hat{=}+$: c'est correct, car $\mathsf{Err} \in \gamma(+)$. (C'est pourquoi nous avons inclus Err dans les $\gamma(v)$, $v \neq \bot$!)

En général, définissons la sémantique abstraite :

$$
\begin{array}{rcl}
\rho^\sharp \in \mathcal{E}nv^\sharp & \hat{=} & \mathcal{V}ar \to L^\sharp \\
\mathcal{E}[\![\_]\!]^\sharp\_ & : & \mathcal{E}xpr \times \mathcal{E}nv^\sharp \to L^\sharp \\
\mathcal{E}[\![x]\!]^\sharp\rho^\sharp & \hat{=} & \rho^\sharp(x) \\
\mathcal{E}[\![a]\!]^\sharp\rho^\sharp & \hat{=} & a^\sharp \\
\mathcal{E}[\![e_1 \mathbf{+} e_2]\!]^\sharp\rho^\sharp & \hat{=} & \mathcal{E}[\![e_1]\!]^\sharp\rho^\sharp +^\sharp \mathcal{E}[\![e_2]\!]^\sharp\rho^\sharp \quad \ldots
\end{array}
$$

Théorème de correction : si $\rho(x) \in \gamma(\rho^\sharp(x))$ pour tout $x \in \mathcal{V}ar$, alors $\mathcal{E}[\![e]\!]\rho \in \gamma(\mathcal{E}[\![e]\!]^\sharp\rho^\sharp)$ pour tout $e \in \mathcal{E}xpr$.

Démonstration : par récurrence structurelle sur e.

- Si $e = x$, $\mathcal{E}[\![e]\!]\rho = \rho(x) \in \gamma(\rho^\sharp(x)) = \gamma(\mathcal{E}[\![e]\!]^\sharp \rho^\sharp)$.
- Si $e = a$, $\mathcal{E}[\![e]\!]\rho = a$, et $\gamma(\mathcal{E}[\![e]\!]^\sharp \rho^\sharp) = \gamma(a^\sharp) = \gamma(\alpha\{a\})$ contient a …

  …correct si : (1) $A \subseteq \gamma(\alpha(A))$ (cf. transparent suivant).
- Si $e = e_1 \mathbf{+} e_2$,
  $$\begin{aligned} &\gamma(\mathcal{E}[\![e]\!]^\sharp \rho^\sharp) = \gamma(\alpha(\{v_1 + v_2 \mid v_1 \in \gamma(\mathcal{E}[\![e_1]\!]^\sharp \rho^\sharp), v_2 \in \gamma(\mathcal{E}[\![e_2]\!]^\sharp \rho^\sharp)\}) \\ &\supseteq \{v_1 + v_2 \mid v_1 \in \gamma(\mathcal{E}[\![e_1]\!]^\sharp \rho^\sharp), v_2 \in \gamma(\mathcal{E}[\![e_2]\!]^\sharp \rho^\sharp)\} \qquad \text{(par (1))} \\ &\ni \mathcal{E}[\![e_1]\!]\rho + \mathcal{E}[\![e_2]\!]\rho \qquad \text{(par hypothèse de récurrence)} \\ &= \mathcal{E}[\![e]\!]\rho. \end{aligned}$$
- …et similairement pour les autres cas.

Lemme : $\alpha(A) \sqsubseteq^\sharp v \Leftrightarrow A \subseteq \gamma(v)$.

Démonstration: $\alpha(A)$ est un v_0 minimal tel que $A \subseteq \gamma(v_0)$ (a)

$\Rightarrow$ Par hypothèse, $v_0 \sqsubseteq^\sharp v$ (b)

Par (b) et γ monotone, $\gamma(v_0) \subseteq \gamma(v)$ (c)

Par (a) et (c), $A \subseteq \gamma(v)$.

$\Leftarrow$ Par hypothèse, $A \subseteq \gamma(v)$ (d)

Par (d) et la minimalité de v_0 tel que (a), $v_0 \sqsubseteq^\sharp v \ldots$ donc $\alpha(A) \sqsubseteq^\sharp v$.

Corollaire : (1) $A \subseteq \gamma(\alpha(A))$.

Démonstration: $\alpha(A) \sqsubseteq^\sharp \alpha(A)$; utiliser le lemme dans le sens $\Rightarrow$.

Corollaire : (2) $\alpha(\gamma(v)) \sqsubseteq^\sharp v$.

Démonstration: $\gamma(v) \sqsubseteq^\sharp \gamma(v)$; utiliser le lemme dans le sens $\Leftarrow$.

Corollaire : (3) α est monotone.

Dém.: si $A_1 \subseteq A_2$, par (1) $A_1 \subseteq \gamma(\alpha(A_2))$; donc $\alpha(A_1) \sqsubseteq^\sharp \alpha(A_2)$.

Les correspondances de Galois

sont des paires de fonctions (α, γ) :

$$L^\sharp, \sqsubseteq^\sharp \underset{\alpha}{\overset{\gamma}{\rightleftarrows}} L^\flat, \sqsubseteq^\flat$$

(abstrait) (concret)

telles que :

1. α est monotone;
2. γ est monotone;
3. $\alpha(v^\flat) \sqsubseteq^\sharp v^\sharp \Leftrightarrow v^\flat \sqsubseteq^\flat \gamma(v^\sharp)$.

Ex : démontrer (1) $v^\flat \sqsubseteq^\flat \gamma(\alpha(v^\flat))$. **Ex :** démontrer (2) $\alpha(\gamma(v^\sharp)) \sqsubseteq^\sharp v^\sharp$.

Cette définition est équivalente à la construction précédente de (α, γ) :

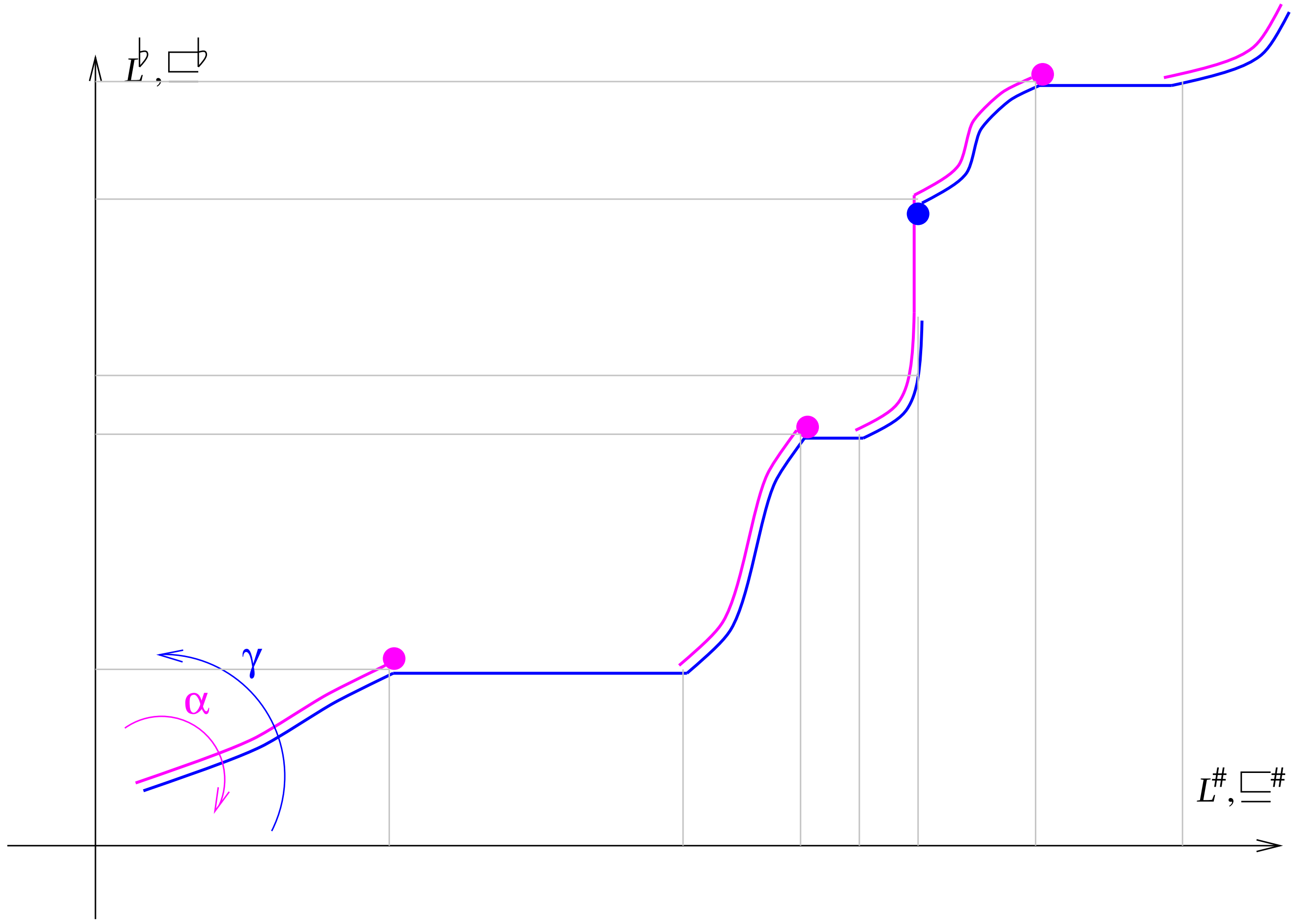
Théorème : $\alpha(v^\flat) = \min_{\sqsubseteq^\sharp}\{v^\sharp \mid v^\flat \sqsubseteq^\flat \gamma(v^\sharp)\}$.
Démonstration : Rappelons que $\min_{\sqsubseteq^\sharp} S$ est caractérisé par : (a) $\min_{\sqsubseteq^\sharp} S \in S$ et (b) $\min_{\sqsubseteq^\sharp} S \sqsubseteq^\sharp v^\sharp$ pour tout $v^\sharp \in S$. Soit $S \hat{=} \{v^\sharp \mid v^\flat \sqsubseteq^\flat \gamma(v^\sharp)\}$. Soit $v_0^\sharp \hat{=} \alpha(v^\flat)$.

(a): $\alpha(v^\flat) \sqsubseteq^\sharp v_0^\sharp$, donc $v^\flat \sqsubseteq^\flat \gamma(v_0^\sharp)$ (par 3.), donc $v_0^\sharp \in \{v^\sharp \mid v^\flat \sqsubseteq^\flat \gamma(v^\sharp)\}$, donc $v_0^\sharp \in S$.

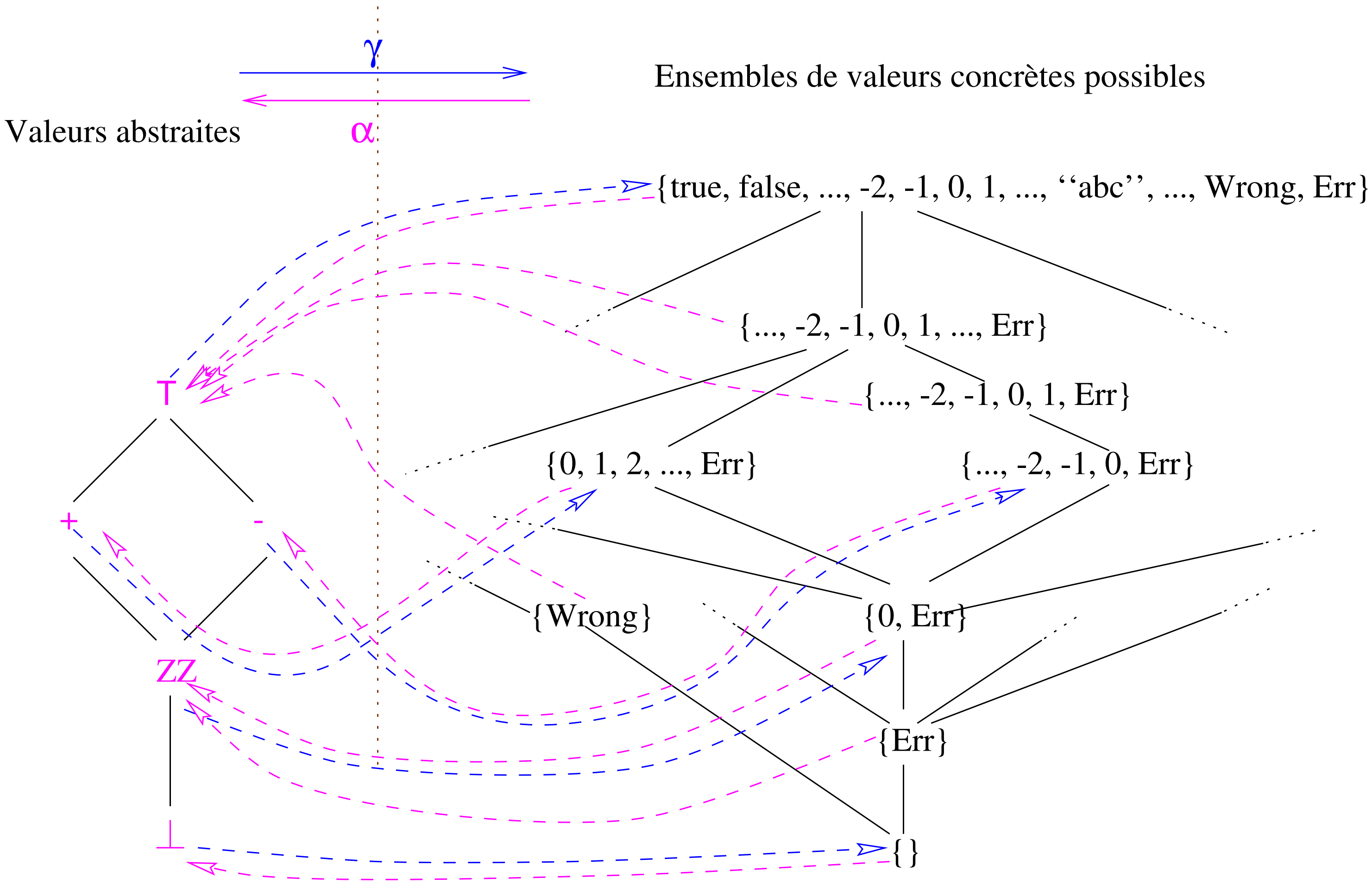
(b): Pour tout $v^\sharp \in S$, $v^\flat \sqsubseteq^\flat \gamma(v^\sharp)$, donc $\alpha(v^\flat) \sqsubseteq^\sharp v^\sharp$ (par 3.), donc $v_0^\sharp \sqsubseteq^\sharp v^\sharp$.

Ex : démontrer que réciproquement, $\gamma(v^\sharp) = \max_{\sqsubseteq^\flat}\{v^\flat \mid \alpha(v^\flat) \sqsubseteq^\sharp v^\sharp\}$.

Une correspondance de Galois est *presque* une bijection



Exemple de correspondance de Galois



Ex: sur quels autres treillis donnés dans le cours peut-on mettre une correspondance de Galois ?

Ex: décrire explicitement le α du treillis du transparent 41.

Ex: en déduire les tables de calcul de $+^\sharp$, $-^\sharp$, etc., dans le treillis abstrait du transparent 41.

Tables de sémantique concrète :

+	Wrong	Err	$n_2 \in \mathbb{Z}$	$s_2 \in \mathcal{S}tring$	autres
Wrong	Wrong	Err	Wrong	Wrong	Wrong
Err	Wrong	Err	Err	Err	Err
$n_1 \in \mathbb{Z}$	Wrong	Err	$n_1 + n_2$	Wrong	Wrong
$s_1 \in \mathcal{S}tring$	Wrong	Err	Wrong	concat(s_1, s_2)	Wrong
autres	Wrong	Err	Wrong	Wrong	Wrong

-	Wrong	Err	$n \in \mathbb{Z}$	autres
	Wrong	Err	$-n$	Wrong

$*$	Wrong	Err	$n_2 \in \mathbb{Z}$	autres
Wrong	Wrong	Err	Wrong	Wrong
Err	Wrong	Err	Err	Err
$n_1 \in \mathbb{Z}$	Wrong	Err	$n_1 \times n_2$	Wrong
autres	Wrong	Err	Wrong	Wrong

$/$	Wrong	Err	$n_2 \in \mathbb{Z}$	autres
Wrong	Wrong	Err	Wrong	Wrong
Err	Wrong	Err	Err	Err
$n_1 \in \mathbb{Z}$	Wrong	Err	$\begin{cases} \lfloor n_1 / n_2 \rfloor & (n_2 \neq 0) \\ \mathsf{Err} & (n_2 = 0) \end{cases}$	Wrong
autres	Wrong	Err	Wrong	Wrong

=	Wrong	Err	$n_2 \in \mathbb{Z}$	$s_2 \in \mathcal{S}tring$	$b_2 \in \mathbb{B}$
Wrong	Wrong	Err	Wrong	Wrong	Wrong
Err	Wrong	Err	Err	Err	Err
$n_1 \in \mathbb{Z}$	Wrong	Err	$\begin{cases} \texttt{true}\ (n_1 = n_2) \\ \texttt{false}(n_1 \neq n_2) \end{cases}$	Wrong	Wrong
$s_1 \in \mathcal{S}tring$	Wrong	Err	Wrong	$\begin{cases} \texttt{true}\ (s_1 = s_2) \\ \texttt{false}(s_1 \neq s_2) \end{cases}$	Wrong
$b_1 \in \mathbb{B}$	Wrong	Err	Wrong	Wrong	$\begin{cases} \texttt{true}\ (b_1 = b_2) \\ \texttt{false}(b_1 \neq b_2) \end{cases}$

`not`	Wrong	Err	$b \in \mathbb{B}$	autres
	Wrong	Err	$\neg b$	Wrong

Ex: montrer que dans ce treillis, on a ZZ $\times^\sharp v =$ ZZ dès que void $\sqsubset^\sharp v \sqsubseteq^\sharp$ Int. (Et si $v =$ void ? et si $v = \bot$?) Montrer que si on avait choisi γ(ZZ)$\hat{=}\{0\}$, ce ne serait pas correct.

Ex: que vaut $\mathrm{NZ} /^\sharp \mathrm{NZ}$ dans ce treillis ? Pourquoi ne vaut-il pas NZ ?

Ex: montrer que si on modifiait ce treillis abstrait en supprimant l'élément `void` (tout en gardant $\gamma(\bot) \hat{=} \{\}$), il n'existerait pas de α faisant de (α, γ) une correspondance de Galois.

Ex: Implémenter les opérations sur ce nouveau treillis.

Wrong **et sûreté du typage**

Dans le treillis du transparent 41 :

Théorème : si $\rho(x) \in \gamma(\rho^\sharp(x))$ pour tout $x \in \mathcal{V}ar$ et $\mathcal{E}[\![e]\!]^\sharp \rho^\sharp \neq \top$, alors $\mathcal{E}[\![e]\!]\rho \neq$ Wrong.
"Toute expression de type $\neq \top$ ne provoque pas d'erreur de type (valeur Wrong) à l'exécution."

On peut alors supprimer tous les tests de types dans e : *soft typing*.

Discipline de type à la ML : on refuse toute expression de type $\top$;
alors plus aucun test de type à l'exécution n'est nécessaire.

Une application typique : le *bytecode verifier* Java

… utilise un treillis un peu plus compliqué. Les valeurs abstraites sont $\top$ plus les $(\tau_1, \ldots, \tau_{nvars}, m, \tau'_1, \ldots, \tau'_m)$, où :

- $\tau_1, \ldots, \tau_{nvars}$ = types des $nvars$ *variables locales*;
- $0 \leq m \leq maxstack$ est la profondeur courante de la *pile*;
- $\tau'_1, \ldots, \tau'_m$ sont les types des entrées courantes de la pile.

$$\begin{array}{rcl} \tau & ::= & \top \mid \bot \mid \texttt{int} \mid \texttt{bool} \mid \texttt{char} \mid \texttt{string} \mid \texttt{float} \mid \texttt{double} \\ & \mid & \texttt{array}(dim, \tau) \quad \text{(tableaux)} \quad \mid C \quad \text{(classes)} \end{array}$$

Ordre $C \sqsubseteq^\sharp C'$ si C sous-classe de C' + $\tau \sqsubseteq^\sharp \top$ + $\texttt{array}(dim, \tau) \sqsubseteq^\sharp \texttt{array}(dim', \tau')$ si $dim = dim'$ et $\tau \sqsubseteq^\sharp \tau'$.

En résumé :

- concrétisation γ : sémantique des valeurs abstraites, sous forme de propriétés concrètes;
- abstraction α : donne la valeur abstraite la plus précise représentant une propriété concrète donnée;
- $\rightarrow$ correspondance de Galois (α, γ) permettant de calculer des versions abstraites $f^\sharp$ de toute fonction concrète $f^\flat$ par : $f^\sharp(v) \hat{=} \alpha(f^\flat(\gamma(v)))$.

  Ce procédé de définition est automatiquement correct.

Ceci règle la sémantique des expressions, la prochaine fois nous verrons comment traiter les commandes.