Correction.

Documents autorisés (en particulier le poly).

Exercices

1. On considère le treillis $\mathbb{N} \cup \{+\infty\}$, muni de l'ordre $\leq$ usuel étendu par $n \leq +\infty$ pour tout $n \in \mathbb{N}$, $+\infty \not\leq n$ pour aucun $n \in \mathbb{N}$. Quel est le sup de la partie $\{0, 2, 4, \ldots\} \hat{=} \{2n \mid n \in \mathbb{N}\}$ des entiers pairs ?

   (a) 0 (b) $+\infty$ (c) 42

   (b), qui est le seul majorant des trois possibilités. $+\infty$ est d'autre part le plus petit majorant possible, car aucun majorant de l'ensemble des entiers pairs ne peut être un entier, vu qu'il existe toujours un entier pair supérieur strictement à n'importe quel entier.

2. Donner un exemple de supremum qui n'est pas un maximum (on pourra se fonder sur la question précédente). Justifier.

   $+\infty$ est un supremum, mais n'est pas un maximum de l'ensemble des entiers pairs, dans la question précédente, car $+\infty$ n'est même pas un entier, donc en particulier pas un entier pair.

3. Montrer que dans tout treillis complet $(L, \sqsubseteq, \bigsqcup, \bigsqcap)$, on a :

$$v \sqsubseteq \bigsqcap_{i \in I} v_i \Leftrightarrow \forall i \in I \cdot v \sqsubseteq v_i$$

   Vous pouvez vous inspirer de résultats similaires du cours. (Si vous faites référence à un résultat du cours, donnez le numéro de transparent précis, et l'énoncé du résultat.) On rappelle que $\bigsqcap$ est caractérisé par les propriétés :

(1)	$\forall j \in I \cdot \bigsqcap_{i \in I} v_i \sqsubseteq v_j$	(minorant)
(2)	$\forall v \cdot (\forall j \in I \cdot v \sqsubseteq v_j) \Rightarrow v \sqsubseteq \bigsqcap_{i \in I} v_i$	(plus grand des minorants)

   $\Rightarrow$: si $v \sqsubseteq \bigsqcap_{i \in I} v_i$, alors $v \sqsubseteq v_j$ pour tout j par (1), et ce pour tout j.
   $\Leftarrow$: si $\forall i \in I \cdot v \sqsubseteq v_i$, alors par (2) $v \sqsubseteq \bigsqcap_{i \in I} v_i$.

4. Soit une correspondance de Galois entre deux treillis complets :

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

   (abstrait) (concret)

   On rappelle que ceci signifie que α et γ sont monotones, et que $\alpha(v^\flat) \sqsubseteq^\sharp v^\sharp$ si et seulement si $v^\flat \sqsubseteq^\flat \gamma(v^\sharp)$.

   Montrer que γ *préserve les infs*, c'est-à-dire que :

$$\gamma(\bigsqcap_{i \in I}^{\sharp} v_i^\sharp) = \bigsqcap_{i \in I}^{\flat} \gamma(v_i^\sharp)$$

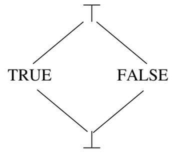
   On pourra encore s'inspirer du cours, et utiliser la question précédente.

   Pour tout v,

$$\begin{array}{rcll} v \sqsubseteq^\flat \gamma(\bigsqcap_{i \in I}^\sharp v_i^\sharp) & \Leftrightarrow & \alpha(v) \sqsubseteq^\sharp \bigsqcap_{i \in I}^\sharp v_i^\sharp & \textit{(Galois)} \\ & \Leftrightarrow & \forall i \in I \cdot \alpha(v) \sqsubseteq^\sharp v_i^\sharp & \textit{(question précédente)} \\ & \Leftrightarrow & \forall i \in I \cdot v \sqsubseteq^\flat \gamma(v_i^\sharp) & \textit{(Galois)} \\ & \Leftrightarrow & v \sqsubseteq^\flat \bigsqcap_{i \in I}^\flat \gamma(v_i^\sharp) & \textit{(question précédente)} \end{array}$$

   Si on prend $v \hat{=} \gamma(\bigsqcap_{i \in I}^\sharp v_i^\sharp)$, l'inégalité du haut est évidente, et on en déduit $\gamma(\bigsqcap_{i \in I}^\sharp v_i^\sharp) \sqsubseteq^\flat \bigsqcap_{i \in I}^\flat \gamma(v_i^\sharp)$. Si on prend $v \hat{=} \bigsqcap_{i \in I}^\flat \gamma(v_i^\sharp)$, l'inégalité du bas est évidente, et on en déduit celle du haut, soit $\bigsqcap_{i \in I}^\flat \gamma(v_i^\sharp) \sqsubseteq^\flat \gamma(\bigsqcap_{i \in I}^\sharp v_i^\sharp)$. D'où le résultat.

5. On choisit comme treillis abstrait $L^\sharp \hat{=} \{\top, \text{TRUE}, \text{FALSE}, \bot\}$ avec $\bot \sqsubseteq^\sharp$ TRUE $\sqsubseteq^\sharp \top$, $\bot \sqsubseteq^\sharp$ FALSE $\sqsubseteq^\sharp \top$ et TRUE et FALSE incomparables :



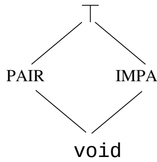
On définit $\gamma(\top) \hat{=} \{\text{true}, \text{false}, Err\}$, $\gamma(\text{TRUE}) \hat{=} \{\text{true}, Err\}$, $\gamma(\text{FALSE}) \hat{=} \{\text{false}, Err\}$, $\gamma(\bot) \hat{=} \emptyset$. Utiliser la question précédente pour montrer qu'on ne peut pas trouver de fonction $\alpha : \mathbb{P}\{\text{true}, \text{false}, Err\}, \subseteq \longrightarrow L^\sharp, \sqsubseteq^\sharp$ telle que α, γ soit une correspondance de Galois. Proposer une modification (légère) de $L^\sharp$ ou de γ permettant de trouver un tel α.

S'il y en avait une, par la question précédente on aurait $\gamma(\text{TRUE} \sqcap^\sharp \text{FALSE}) = \gamma(\text{TRUE}) \cap \gamma(\text{FALSE})$, soit $\gamma(\bot) = \{\text{true}, Err\} \cap \{\text{false}, Err\}$, c'est-à-dire $\emptyset = \{Err\}$, ce qui est impossible.

On peut par exemple prendre $\gamma(\bot) \hat{=} \{Err\}$ au lieu de $\emptyset$, ou bien ajouter un élément VOID à $L^\sharp$ tel que $\gamma(\text{VOID}) \hat{=} \{Err\}$.

Problème

On cherche à déterminer la parité des entiers utilisés dans un programme, et de là des propriétés qui vont en se compliquant. On reprend le mini-langage du cours, et on consière le treillis $L_2^\sharp, \sqsubseteq_2^\sharp$:



et une concrétisation γ_2 :

$v^\sharp$	$\gamma_2(v^\sharp)$
`void`	$\{Err, Wrong, Err_{init}\}$
PAIR	$\{2n \mid n \in \mathbb{Z}\} \cup \{Err, Wrong, Err_{init}\} = \{\ldots, -4, -2, 0, 2, 4, \ldots, Err, Wrong, Err_{init}\}$
IMPAIR	$\{2n+1 \mid n \in \mathbb{Z}\} \cup \{Err, Wrong, Err_{init}\} = \{\ldots, -3, -1, 1, 3, 5, \ldots, Err, Wrong, Err_{init}\}$
$\top$	$\mathcal{V}al \cup \{Err, Wrong, Err_{init}\}$

où l'on rappelle que $\mathcal{V}al = \mathbb{Z} \cup \mathbb{B} \cup String$.

1. Décrire explicitement l'abstraction $\alpha_2 : \mathbb{P}(\mathcal{V}al \cup \{Err, Wrong, Err_{init}\}), \subseteq \longrightarrow L_2^\sharp, \sqsubseteq_2^\sharp$. Autrement dit, que vaut $\alpha_2(A)$, pour chaque partie A de $\mathcal{V}al \cup \{Err, Wrong, Err_{init}\}$? Distinguer quatre cas (au moins).

   Par définition, $\alpha_2(A) = \min_{\sqsubseteq_2^\sharp}\{v^\sharp \in L_2^\sharp \mid A \subseteq \gamma_2^\sharp(v^\sharp)\}$.

   Si A ne contient que des erreurs, autrement dit $A \subseteq \{Err, Err_{init}, Wrong\}$, alors $A \subseteq \gamma_2^\sharp(v^\sharp)$ pour tout $v^\sharp$, donc $\alpha_2(A) =$ `void`.

   Si A contient au moins une valeur non entière (un booléen, une chaîne), alors $A \subseteq \gamma_2^\sharp(v^\sharp)$ implique $v^\sharp \sqsupseteq_2^\sharp \top$, donc $\alpha_2(A) = \top$.

   Sinon, A ne contient que des erreurs et des entiers, et au moins un entier. Si les seuls entiers de A sont pairs, alors $\alpha_2(A) =$ PAIR, si les seuls entiers de A sont impairs, alors $\alpha_2(A) =$ IMPAIR; sinon, $\alpha_2(A) = \top$.

2. Compléter les tables de calcul de l'addition et de la division :

$+^\sharp$	`void`	PAIR	IMPAIR	$\top$
`void`	`void`	`void`	`void`	?
PAIR	?	?	?	$\top$
IMPAIR	?	?	?	$\top$
$\top$	?	$\top$	$\top$	$\top$

$/^\sharp$	`void`	PAIR	IMPAIR	$\top$
`void`	`void`	`void`	`void`	?
PAIR	?	?	?	$\top$
IMPAIR	?	?	?	$\top$
$\top$	?	$\top$	$\top$	$\top$

On rappelle que la sémantique concrète de $/$ est la partie entière du quotient : $4/2 = 2$, $2/2 = 1$, mais $4/3 = 1$ et $2/3 = 0$.

$+^\sharp$	`void`	PAIR	IMPAIR	$\top$
`void`	`void`	`void`	`void`	`void`
PAIR	`void`	PAIR	IMPAIR	$\top$
IMPAIR	`void`	IMPAIR	PAIR	$\top$
$\top$	`void`	$\top$	$\top$	$\top$

$/^\sharp$	`void`	PAIR	IMPAIR	$\top$
`void`	`void`	`void`	`void`	`void`
PAIR	`void`	$\top$	$\top$	$\top$
IMPAIR	`void`	$\top$	$\top$	$\top$
$\top$	`void`	$\top$	$\top$	$\top$

Noter en particulier que $\text{PAIR}/^\sharp\text{PAIR} = \top$ *car* $\gamma_2(\text{PAIR}/^\sharp\text{PAIR})$ *doit contenir notamment* $4/2 = 2$ *et* $2/2 = 1$*, donc* $\text{PAIR}/^\sharp\text{PAIR} \sqsupseteq_2^\sharp \text{PAIR} \sqcup_2^\sharp \text{IMPAIR} = \top$*. On perd ici de la précision de façon un peu idiote. Si on ajoutait un élément* Int *au treillis* $L_2^\sharp$ *dont le* γ_2 *serait* $\mathbb{Z} \cup \{Err, Err_{init}, Wrong\}$*, on obtiendrait au moins que* $\text{PAIR}/^\sharp\text{PAIR} = Int$*. Même remarque pour les autres entrées.*

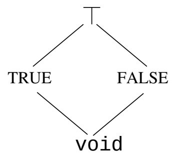
3. A-t-on besoin d'utiliser un élargissement pour garantir la terminaison de l'analyses statique avant sur ce treillis ? Pourquoi ? Si oui, proposer un élargissement.

   Non, on n'en a pas besoin, car $L_2^\sharp$ *a la condition de chaîne croissante, et l'analyse termine toute seule.*

4. L'intérêt du treillis de parité est que le test $e_1 = e_2$ doit nécessairement échouer si e_1 est pair et e_2 impair, ou réciproquement. Que vaut $\text{PAIR} =^\sharp \text{IMPAIR}$ dans ce treillis, où $=^\sharp$ est la meilleure approximation de l'égalité $=$? (La sémantique concrète de $=$ est supposée retourner `true` sur deux valeurs égales, `false` sur deux valeurs différentes du même type, $Wrong$ sur deux valeurs de types différents.)

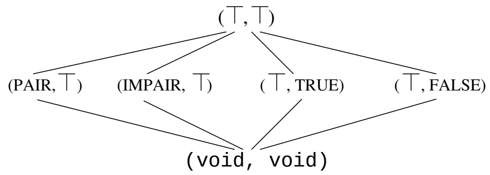
   Nécessairement, $\text{PAIR} =^\sharp \text{IMPAIR} = \alpha_2\{v_1 = v_2 \mid v_1 \in \gamma_2(\text{PAIR}), v_2 \in \gamma_2(\text{IMPAIR})\} = \alpha_2\{v_1 = v_2 \mid v_1 \in \{\ldots, -4, -2, 0, 2, 4, \ldots, Err, Wrong, Err_{init}\}, v_2 \in \{\ldots, -3, -1, 1, 3, 5, \ldots, Err, Wrong, Err_{init}\}\} = \alpha_2\{\texttt{false}, Err, Err_{init}, Wrong\}$*, donc* $\text{PAIR} =^\sharp \text{IMPAIR}$ *vaut* $\top$*. Le treillis* $L_2^\sharp$ *seul n'est donc pas suffisamment.*

5. On considère le treillis des constantes booléennes $L_{\mathbb{B}}^\sharp, \sqsubseteq_{\mathbb{B}}^\sharp$:



   où $\gamma_{\mathbb{B}}(\top) = \mathcal{V}al \cup \{Err, Err_{init}, Wrong\}$, $\gamma_{\mathbb{B}}(\text{TRUE}) = \{\texttt{true}, Err, Err_{init}, Wrong\}$, $\gamma_{\mathbb{B}}(\text{FALSE}) = \{\texttt{false}, Err, Err_{init}, Wrong\}$, $\gamma_{\mathbb{B}}(\bot) = \{Err, Err_{init}, Wrong\}$.

   Dessiner le produit réduit de $L_2^\sharp$ avec $L_{\mathbb{B}}^\sharp$. Montrer qu'on peut définir l'égalité abstraite $=^\sharp$ de façon plus précise dans ce produit réduit que dans $L_2^\sharp$ seul, en particulier telle que $\text{PAIR} =^\sharp \text{IMPAIR}$ est strictement plus précis que $(\top, \top)$.



   En effet, $\alpha(\gamma(\text{PAIR}, \text{TRUE})) = \alpha(\{\ldots, -4, -2, 0, 2, 4, \ldots, Err, Err_{init}, Wrong\} \cap \{\texttt{true}, Err, Err_{init}, Wrong\}) = \alpha(\{Err, Err_{init}, Wrong\}) = \alpha(\gamma(\texttt{void}, \texttt{void})))$ *et de même pour* $(\text{PAIR}, \text{FALSE})$*,* $(\text{IMPAIR}, \text{TRUE})$*,* $(\text{IMPAIR}, \text{FALSE})$*. D'autre part,* $\alpha(\gamma(x, \texttt{void})) = \alpha(\gamma(\texttt{void}, y)) = \alpha\{\{Err, Err_{init}, Wrong\}) = \alpha(\gamma(\texttt{void}, \texttt{void})))$ *pour tous* x*,* y*. Donc les seuls éléments du produit réduit sont ceux du diagramme ci-dessus.*

Maintenant, la table de $=^\sharp$ sur le produit réduit est :

$=^\sharp$	$(\top,\top)$	$(\text{PAIR},\top)$	$(\text{IMPAIR},\top)$	$(\top,\text{TRUE})$	$(\top,\text{FALSE})$	$(\texttt{void},\texttt{void})$
$(\top,\top)$	$(\top,\top)$	$(\top,\top)$	$(\top,\top)$	$(\top,\top)$	$(\top,\top)$	$(\texttt{void},\texttt{void})$
$(\text{PAIR},\top)$	$-$	$(\top,\top)$	$(\top,\text{FALSE})$	$(\texttt{void},\texttt{void})$	$(\texttt{void},\texttt{void})$	$(\texttt{void},\texttt{void})$
$(\text{IMPAIR},\top)$	$-$	$-$	$(\top,\top)$	$(\texttt{void},\texttt{void})$	$(\texttt{void},\texttt{void})$	$(\texttt{void},\texttt{void})$
$(\top,\text{TRUE})$	$-$	$-$	$-$	$(\top,\text{TRUE})$	$(\top,\text{FALSE})$	$(\texttt{void},\texttt{void})$
$(\top,\text{FALSE})$	$-$	$-$	$-$	$-$	$(\top,\text{TRUE})$	$(\texttt{void},\texttt{void})$
$(\texttt{void},\texttt{void})$	$-$	$-$	$-$	$-$	$-$	$(\texttt{void},\texttt{void})$

où les $-$ notent des entrées redondantes par symétrie.

En particulier, $(\text{PAIR},\top) =^\sharp (\text{IMPAIR},\top)$ *vaut* $(\top,\text{FALSE})$*, autrement dit (et conformément à l'intuition) un nombre pair est bien reconnu comme ne pouvant jamais être égal à un nombre impair.*

6. On veut améliorer la précision de l'analyse, et la combiner avec une analyse d'intervalles sur les entiers. Un élément de notre treillis final est donc dans le produit réduit $L^\sharp$ de $L_2^\sharp \times L_{\mathbb{B}}^\sharp \times L_{itv}^\sharp$, où $L_{itv}^\sharp$ est le treillis des intervalles du cours (valeurs $[\![a,b]\!]$ avec $a,b \in \mathbb{Z} \cup \{-\infty,+\infty\}$, plus $\top$). A-t-on besoin d'un élargissement ici pour garantir la terminaison des analyses ? Si oui, en proposer un.

   (Question bonus.)

   Oui, il existe des chaînes infinies. Par exemple, $(\text{PAIR},\top,[\![0,0]\!])$, $(\text{PAIR},\top,[\![0,2]\!])$, $\ldots$, $(\text{PAIR},\top,[\![0,2k]\!])$, $\ldots$, *est une chaîne strictement croissante dans le produit réduit. (À vous de montrer que ce sont bien des éléments du produit réduit !)*

   Si ∇ est l'élargissement du cours sur les intervalles, alors on définit l'élargissement ∇' sur les éléments de $L^\sharp$ par : $(v_1,w_1,I_1)\nabla'(v_2,w_2,I_2) = (v_1 \sqcap_2^\sharp v_2, w_1 \sqcap_{\mathbb{B}}^\sharp w_2, I_1 \nabla I_2)$ … *sauf que ça n'est pas forcément à valeurs dans $L^\sharp$. On pose donc* $(v_1,w_1,I_1)\nabla''(v_2,w_2,I_2) = \alpha(\gamma((v_1,w_1,I_1)\nabla'(v_2,w_2,I_2)))$*, où (α,γ) est la correspondance de Galois sur le produit.*

   Il n'est pas facile de montrer qu'en général un élargissement défini comme cela a la propriété que toute $x_{n+1} = x_n \nabla'' x'_n$ est stationnaire. (Je pense même qu'il y a des contre-exemples, quoique je n'aie pas cherché.) C'est par contre vrai pour l'élargissement considéré. Je vous laisse chercher la raison, c'est assez compliqué …