TAS : Typage et analyse statique
Master STL, Sorbonne Université

Exemple d'examen (corrigé)

Exercice 1 : Domaine abstrait des entiers booléens

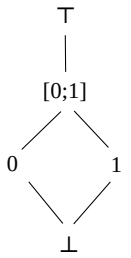
Nous nous intéressons à une abstraction $\mathcal{D}^\sharp$ des ensembles d'entiers $\mathcal{P}(\mathbb{Z})$ qui sera précise sur les valeurs 0 et 1 :

$$\mathcal{D}^\sharp \stackrel{\text{def}}{=} \{\bot, 0, 1, [0;1], \top\}$$

où 0 et 1 représentent les constantes 0 et 1, $[0;1]$ indique un entier entre 0 et 1, et $\top$ un entier arbitraire (non nécessairement dans l'intervalle $[0;1]$).

Question 1.
Donnez l'ordre partiel $\sqsubseteq$ sur $\mathcal{D}^\sharp$ (vous pouvez donner un diagramme de Hasse).
Précisez si $\mathcal{D}^\sharp$ est un treillis et donnez, si c'est le cas, la définition des opérateurs $\sqcup$ et $\sqcap$.

Corrigé.



$\bot \sqsubset 0, 1 \sqsubset [0;1] \sqsubset \top$.
$\mathcal{D}^\sharp$ est bien un treillis, avec un plus petit majorant $\sqcup$ et un plus grand minorant $\sqcap$ définis comme suit :
$\forall x : \bot \sqcup x = x \sqcup \bot = x$; $0 \sqcup 1 = 1 \sqcup 0 = [0;1]$; $\forall x : x \sqcup \top = \top \sqcup x = \top$.
$\forall x : \bot \sqcap x = x \sqcap \bot = \bot$; $0 \sqcap 1 = 1 \sqcap 0 = \bot$; $[0;1] \sqcap 0 = 0 \sqcap [0;1] = 0$; $[0;1] \sqcap 1 = 1 \sqcap [0;1] = 1$; $\forall x : x \sqcap \top = \top \sqcap x = x$.
□

Question 2.
Donnez une correspondance de Galois (α, γ) entre $\mathcal{P}(\mathbb{Z})$ et $\mathcal{D}^\sharp$ (on ne demande pas la preuve qu'il s'agit bien d'une correspondance de Galois).
Donnez les fonctions $\alpha \circ \gamma$ et $\gamma \circ \alpha$. Sont-elles extensives ? réductrices ? l'identité ?

Corrigé.

$$\alpha(x) = \begin{cases} \bot & \text{si } x = \emptyset \\ 0 & \text{si } x = \{0\} \\ 1 & \text{si } x = \{1\} \\ [0;1] & \text{si } x = \{0,1\} \\ \top & \text{sinon} \end{cases} \qquad \begin{array}{l} \gamma(\bot) = \emptyset \\ \gamma(0) = \{0\} \\ \gamma(1) = \{1\} \\ \gamma([0;1] = \{0,1\} \\ \gamma(\top) = \mathbb{Z} \end{array}$$

On en déduit :

$$(\gamma \circ \alpha)(x) = \begin{cases} \gamma(\bot) = \emptyset & \text{si } x = \emptyset \\ \gamma(0) = \{0\} & \text{si } x = \{0\} \\ \gamma(1) = \{1\} & \text{si } x = \{1\} \\ \gamma([0;1] = \{0,1\} & \text{si } x = \{0,1\} \\ \gamma(\top) = \mathbb{Z} & \text{sinon} \end{cases} \qquad \begin{array}{l} (\alpha \circ \gamma)(\bot) = \alpha(\emptyset) = \bot \\ (\alpha \circ \gamma)(0) = \alpha(\{0\}) = 0 \\ (\alpha \circ \gamma)(1) = \alpha(\{1\}) = 1 \\ (\alpha \circ \gamma)([0;1] = \alpha(\{0,1\}) = [0;1] \\ (\alpha \circ \gamma)(\top) = \alpha(\mathbb{Z}) = \top \end{array}$$

$\gamma \circ \alpha$ est extensive, mais ce n'est pas l'identité car $(\gamma \circ \alpha)(\{2\}) = \mathbb{Z} \neq \{2\}$
$\alpha \circ \gamma$ est l'identité.
□

Question 3.
Donnez la meilleur abstraction dans $\mathcal{D}^\sharp$ des opérateurs suivants : l'addition $+$, la multiplication $\times$ et l'union $\cup$ (on ne demande pas la preuve qu'il s'agit bien des meilleurs abstractions).
Précisez, en justifiant votre réponse, si ces opérateurs sont exacts.

Corrigé.

L'union abstraite $\cup^\sharp$ est égale au plus petit majorant $\sqcup$, donné par diagramme de Hasse de la première question.

$+^\sharp$	$\bot$	0	1	$[0;1]$	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
0	$\bot$	0	1	$[0;1]$	$\top$
1	$\bot$	1	$\top$	$\top$	$\top$
$[0;1]$	$\bot$	$[0;1]$	$\top$	$\top$	$\top$
$\top$	$\bot$	$\top$	$\top$	$\top$	$\top$

$\times^\sharp$	$\bot$	0	1	$[0;1]$	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
0	$\bot$	0	0	0	0
1	$\bot$	0	1	$[0;1]$	$\top$
$[0;1]$	$\bot$	0	$[0;1]$	$[0;1]$	$\top$
$\top$	$\bot$	0	$\top$	$\top$	$\top$

L'union et la multiplication sont exacts.
L'addition n'est pas exacte ; par exemple $\gamma(1 +^\sharp 1) = \gamma(\top) = \mathbb{Z}$, mais $\gamma(1) + \gamma(1) = \{1\} + \{1\} = \{2\}$.
□

Question 4.
Pour analyser l'effet d'une comparaison $\leq$, nous proposons un opérateur concret de raffinement $\leq$: $(\mathcal{P}(\mathbb{Z}) \times \mathcal{P}(\mathbb{Z})) \to (\mathcal{P}(\mathbb{Z}) \times \mathcal{P}(\mathbb{Z}))$ défini par $\leq (X, Y) = (\{\, x \in X \mid \exists y \in Y : x \leq y \,\}, \{\, y \in Y \mid \exists x \in X : x \leq y \,\})$. Étant donnés des ensembles d'entiers X et Y, l'opérateur raffine X et Y pour ne garder que les valeurs $x \in X$ et $y \in Y$ telles que la relation $x \leq y$ puisse être vraie.
Proposez une version abstraite $\leq^\sharp$ $(\mathcal{D}^\sharp \times \mathcal{D}^\sharp) \to (\mathcal{D}^\sharp \times \mathcal{D}^\sharp)$ de cet opérateur.

Corrigé.

$\leq^\sharp$	$\bot$	0	1	$[0;1]$	$\top$
$\bot$	$(\bot, \bot)$	$(\bot, \bot)$	$(\bot, \bot)$	$(\bot, \bot)$	$(\bot, \bot)$
0	$(\bot, \bot)$	$(0, 0)$	$(0, 1)$	$(0, [0;1])$	$(0, \top)$
1	$(\bot, \bot)$	$(\bot, \bot)$	$(1, 1)$	$(1, 1)$	$(1, \top)$
$[0;1]$	$(\bot, \bot)$	$(0, 0)$	$([0;1], 1)$	$([0;1], [0;1])$	$([0;1], \top)$
$\top$	$(\bot, \bot)$	$(\top, 0)$	$(\top, 1)$	$(\top, [0;1])$	$(\top, \top)$

□

Le domaine $\mathcal{D}^\sharp$ est utile en C pour abstraire les entiers susceptibles d'être utilisés comme des booléens. En effet, en C, les booléens sont codés par des entiers, et les opérateurs booléens retournent les entiers 1 et 0 pour dénoter, respectivement, vrai et faux. Par exemple :

— l'opérateur *non logique* `!` retourne 1 si son argument est 0, et 0 si son argument est non-nul ;
— le *et logique* `&&` retourne 0 si un de ses arguments est 0, et 1 si ses deux arguments sont différents de zéro.

Notez que, dans les arguments de `!` et `&&`, toute valeur non nulle est considérée comme vraie, mais le résultat de ces opérateurs retournera toujours 1 pour dénoter vrai.

Question 5.
Donnez la sémantique concrète des opérateurs `!` et `&&`.
Donnez ensuite la sémantique abstraite dans $\mathcal{D}^\sharp$ des opérateurs `!` et `&&`.
Précisez, en justifiant votre réponse, pour chacun des opérateurs abstraits, s'il est optimal et s'il est exact.

Corrigé.

$$\texttt{!}(x) = \begin{cases} \emptyset & \text{si } x = \emptyset \\ \{1\} & \text{si } x = \{0\} \\ \{0\} & \text{si } 0 \notin x \\ [0;1] & \text{sinon} \end{cases} \qquad \texttt{\&\&}(x,y) = \begin{cases} \emptyset & \text{si } x = \emptyset \text{ ou } y = \emptyset \\ \{1\} & \text{si } 0 \notin x \text{ et } 0 \notin y \\ \{0\} & \text{si } x = \{0\} \text{ ou } y = \{0\} \\ [0;1] & \text{sinon} \end{cases}$$

$$\texttt{!}^\sharp(x) = \begin{cases} \bot & \text{si } x = \bot \\ 1 & \text{si } x = 0 \\ 0 & \text{si } x = 1 \\ [0;1] & \text{sinon} \end{cases} \qquad \texttt{\&\&}^\sharp(x,y) = \begin{cases} \bot & \text{si } x = \bot \text{ ou } y = \bot \\ 1 & \text{si } x = 1 \text{ et } y = 1 \\ 0 & \text{si } x = 0 \text{ ou } y = 0 \\ [0;1] & \text{sinon} \end{cases}$$

Les deux opérateurs abstraits sont exacts car les images de l'opérateur concret correspondant sont toutes représentables exactement dans l'abstrait. Ils sont donc également optimaux.
□

Question 6.
Soit le domaine $\mathcal{E}^\sharp \stackrel{\text{def}}{=} \{\bot, 0, \neq 0, \top\}$ capable de représenter le fait qu'un entier est nul ou non nul. Donnez l'opérateur de réduction optimal ρ pour définir un produit réduit entre $\mathcal{D}^\sharp$ et $\mathcal{E}^\sharp$.

Corrigé.

ρ	$\bot$	0	$\neq 0$	$\top$
$\bot$	$(\bot, \bot)$	$(\bot, \bot)$	$(\bot, \bot)$	$(\bot, \bot)$
0	$(\bot, \bot)$	$(0, 0)$	$(\bot, \bot)$	$(0, 0)$
1	$(\bot, \bot)$	$(\bot, \bot)$	$(1, \neq 0)$	$(1, \neq 0)$
$[0;1]$	$(\bot, \bot)$	$(0, 0)$	$(1, \neq 0)$	$([0;1], \top)$
$\top$	$(\bot, \bot)$	$(0, 0)$	$(\top, \neq 0)$	$(\top, \top)$

□

Question 7.
Considérons le programme suivant :

1 : $X \leftarrow$ **rand**$(10, 20)$;
2 : $Y \leftarrow$ **rand**$(1, 2)$;
3 : $X \leftarrow X$ `&&` Y;
4 : **assert** $X = 1$

Donnez le résultat de l'analyse du programme aux points 3 et 4 dans le domaine $\mathcal{D}^\sharp$, dans le domaine $\mathcal{E}^\sharp$, et dans le produit réduit de $\mathcal{D}^\sharp$ et $\mathcal{E}^\sharp$.
Précisez, dans chaque cas, si l'assertion est démontrée correcte.

Corrigé.

Avec $\mathcal{D}^\sharp$. En 3 : $X = Y = \top$. En 4 : $X = [0;1]$ et $Y = \top$. L'assertion n'est pas prouvée.
Avec $\mathcal{E}^\sharp$. En 3 : $X = Y = (\neq 0)$. En 4 : $X = Y = (\neq 0)$. L'assertion n'est pas prouvée.
Avec le produit réduit. En 3 : $X = Y = (\top, \neq 0)$. En 4 : $X = \rho([0;1], \neq 0) = (1, \neq 0)$ et $Y = (\neq 0)$. L'assertion est prouvée correcte.
□

Exercice 2 : Boucles repeat until

Dans cet exercice, nous étudions la boucle **repeat** s **until** c, qui est une variante de la boucle **while** vue en cours. La boucle **repeat** s **until** c commence par exécuter son corps s une fois, avant de tester la condition c. Si la condition est vraie, la boucle s'arrête. Si elle est fausse, la boucle exécute à nouveau le corps s, et teste à nouveau la condition c. Tant que la condition est fausse, la boucle continue.

Question 1.
On suppose que $R \in \mathcal{P}(\mathcal{V} \to \mathbb{Z})$ est un ensemble d'environnements, sur un ensemble $\mathcal{V}$ de variables à valeur entière.
Donnez la sémantique concrète $\mathsf{S}[\![\,\textbf{repeat}\ s\ \textbf{until}\ c\,]\!]\,R \in \mathcal{P}(\mathcal{V} \to \mathbb{Z})$ de la boucle à l'aide d'un point fixe.
Donnez la formule exprimant les itérés de point-fixe, ainsi qu'une interprétation de ces itérés en terme d'exécution du programme.

Corrigé.

$\mathsf{S}[\![\,\textbf{repeat}\ s\ \textbf{until}\ c\,]\!]\,R = \mathsf{C}[\![\,c\,]\!]\,I$
où $I = \mathrm{lfp}\,F$
et $F(X) = \mathsf{S}[\![\,s\,]\!]\,R \cup \mathsf{S}[\![\,s\,]\!]\,(\mathsf{C}[\![\,\neg c\,]\!]\,X)$.
Par le théorème de point fixe de Tarski $I = \cup_n F^n(\emptyset)$.
À la première itération, $F^0(\emptyset) = \mathsf{S}[\![\,s\,]\!]\,R$ est l'état après exactement une exécution du corps.
Puis, $F^1(\emptyset) = \mathsf{S}[\![\,s\,]\!]\,R \cup (\mathsf{S}[\![\,s\,]\!] \circ \mathsf{C}[\![\,\neg c\,]\!] \circ \mathsf{S}[\![\,s\,]\!])R$ est l'état après une ou deux exécutions du corps.
De manière générale, $F^n(\emptyset)$ est l'état après au moins une et au plus $n+1$ exécutions du corps.
$I = \cup_n F^n(\emptyset)$ est donc l'état après un nombre d'exécutions du corps supérieur ou égal à 1.
$\mathsf{C}[\![\,c\,]\!]\,I$ est l'état quand on sort de la boucle par une condition vraie après un nombre d'exécutions du corps supérieur ou égal à 1. C'est donc la sémantique recherchée.
□

Question 2.
Considérons le programme suivant :

$X \leftarrow 0$;
$Y \leftarrow 0$;
repeat
    $X \leftarrow X + \textbf{rand}(1, 2)$;
    $Y \leftarrow Y + 1$
until $X \geq 3$

Donnez les itérés de calcul de point-fixe de ce programme dans la sémantique concrète jusqu'à la limite.
Donnez également l'état concret juste après être sorti de la boucle.

Corrigé.

Juste avant la boucle, l'état concret est $R = \{(X \mapsto 0, Y \mapsto 0)\}$.
$F^0(\emptyset) = \{\,(X \mapsto x, Y \mapsto 1) \mid 1 \leq x \leq 2\,\}$.
$F^1(\emptyset) = \{\,(X \mapsto x, Y \mapsto 1) \mid 1 \leq x \leq 2\,\} \cup \{\,(X \mapsto x, Y \mapsto 2) \mid 2 \leq x \leq 4\,\}$
$F^2(\emptyset) = \{\,(X \mapsto x, Y \mapsto 1) \mid 1 \leq x \leq 2\,\} \cup \{\,(X \mapsto x, Y \mapsto 2) \mid 2 \leq x \leq 4\,\} \cup \{\,(X \mapsto x, Y \mapsto 3) \mid 3 \leq x \leq 4\,\}$
$F^3(\emptyset) = F^2(\emptyset)$
Le point fixe est donc $\mathrm{lfp}\,F = F^2(\emptyset)$.
En sortie de boucle, on a : $\{\,(X \mapsto x, Y \mapsto y) \mid 3 \leq x \leq 4 \wedge 2 \leq y \leq 3\,\}$.
□

Question 3.
Nous considérons maintenant l'analyse dans le domaine des intervalles avec l'élargissement standard.

Donnez les itérations du calcul de point-fixe dans l'abstrait, l'invariant de boucle trouvé par le domaine des intervalles et l'état abstrait quand le programme est sorti de la boucle.

Corrigé.

Juste avant la boucle, l'état abstrait est $R^\sharp = (X \mapsto [0;0], Y \mapsto [0;0])$.
Le premier itéré est : $X_1^\sharp = F^{\sharp 0}(\bot) = (X \mapsto [1;2], Y \mapsto [1;1])$.
Puis $F^\sharp(X_1^\sharp) = (X \mapsto [1;4], Y \mapsto [1;2])$.
L'élargissement donne $X_2^\sharp = X_1^\sharp \triangledown F^\sharp(X_1^\sharp) = (X \mapsto [1;+\infty], Y \mapsto [1;+\infty])$, qui est stable.
En sortie de boucle, on trouve : $(X \mapsto [3;+\infty], Y \mapsto [1;+\infty])$.
□

Question 4.
Montrez qu'avec un élargissement retardé dans le domaine des intervalles, il est possible de retrouver pour X une information aussi précise que celle de la sémantique concrète.
Cette technique permet-elle d'améliorer la précision sur Y ? Justifiez votre réponse.

Corrigé.

En retardant une fois, nous avons $X_2^\sharp = X_1^\sharp \cup^\sharp F^\sharp(X_1^\sharp) = (X \mapsto [1;4], Y \mapsto [1;2])$.
Puis, $F(X_2^\sharp) = (X \mapsto [1;4], Y \mapsto [1;3])$.
Un élargissement donne $X_2^\sharp \triangledown F(X_2^\sharp) = (X \mapsto [1;4], Y \mapsto [1;+\infty])$.
Et en sortie de boucle, $X \mapsto [3;4]$, ce qui est le même résultat que dans le concret.
Par contre, on aura toujours $Y \mapsto [1;+\infty]$ quel que soit le nombre de déroulements, car la borne supérieure de Y est toujours incrémentée de 1 par le corps de la boucle.
□

Question 5.
Proposez une solution pour améliorer la valeur de Y à la fin de l'analyse, en justifiant votre réponse.

Corrigé.

Plusieurs solutions sont envisageables (une seule était demandée) :

1. un déroulement de boucles,
2. un partitionnement d'état vis à vis de la valeur de Y,
3. l'utilisation du domaine des polyèdres à la place du domaine des intervalles.

Pour le déroulement de boucles, on obtient les itérés $X_1^\sharp = F^{\sharp 0}(\bot) = (X \mapsto [1;2], Y \mapsto [1;1])$, $X_2^\sharp = F^\sharp(X_1^\sharp) = (X \mapsto [2;4], Y \mapsto [2;2])$, $X_3^\sharp = F^\sharp(X_1^\sharp) = (X \mapsto [3;4], Y \mapsto [3;3])$, et $X_i^\sharp = \bot$ après.
Appliquer la condition de sortie sur $X_1^\sharp$, $X_2^\sharp$ et $X_3^\sharp$ donnera, respectivement, $\bot$, $(X \mapsto [3;4], Y \mapsto [2;2])$ et $(X \mapsto [3;4], Y \mapsto [3;3])$.
L'union de ces informations donne $(X \mapsto [3;4], Y \mapsto [2;3])$.

Le partitionnement d'état sur la valeur de Y donne un résultat similaire à celui du déroulement de boucles. En effet, chaque état $X_1^\sharp$, $X_2^\sharp$ et $X_3^\sharp$ corresponds également à une valeur de Y différente.

Dans le domaine des polyèdres, on obtiendrait comme premier itéré $X_1^\sharp = (1 \leq X \leq 2 \wedge Y = 1)$.
Puis, $F^\sharp(X_1^\sharp) = (1 \leq X \leq 2 \wedge Y = 1) \cup^\sharp (2 \leq X \leq 4 \wedge Y = 2) = (Y \leq X \leq 2Y \wedge 1 \leq Y \leq 2)$.
On retarde l'élargissement en définissant $X_2^\sharp = X_1^\sharp \cup^\sharp F^\sharp(X_1^\sharp) = F^\sharp(X_1^\sharp)$.
Alors, $F^\sharp(X_2^\sharp) = (1 \leq X \leq 2 \wedge Y = 1) \cup^\sharp (Y \leq X \leq 2Y \wedge X \leq 4 \wedge 2 \leq Y \leq 3) = (Y \leq X \leq 2Y \wedge X \leq 4 \wedge 1 \leq Y \leq 3)$.
On retarde encore l'élargissement en définissant $X_3^\sharp = X_2^\sharp \cup^\sharp F^\sharp(X_2^\sharp) = F^\sharp(X_2^\sharp)$.
Enfin $F^\sharp(X_3^\sharp) = X_3^\sharp$, et on trouve un point fixe.
En sortie de boucle, la condition $X \geq 3$ donne $(Y \leq X \leq 2Y \wedge 3 \leq X \leq 4 \wedge 2 \leq Y \leq 3)$, qui est équivalente à $(3 \leq X \leq 4 \wedge 2 \leq Y \leq 3)$.
□