Topologie

Une topologie τ sur un ensemble X est un ensemble de parties de X qui vérifie

1. τ est stable par intersection finie.
2. τ est stable par union quelconque.

On dira alors d'un élément de τ qu'il est *ouvert*. Le complémentaire d'un ouvert est par définition un ensemble *fermé*.

Fonction continue

Une fonction $f : X \to Y$ est *continue* de (X, τ) vers (Y, θ) si et seulement si

$$\text{Pour tout } U \in \theta, f^{-1}(U) \in \tau \tag{1}$$

Topologie de Scott

Soit $(D, \leq)$ un dcpo. Une partie $U \subseteq D$ est appellée un *ouvert de Scott* si et seulement si elle vérifie

1. U est clos vers le haut :
$$\text{Pour tous } x, y, \quad \text{Si } x \in U \wedge x \leq y, \text{ alors } y \in U. \tag{2}$$
2. U est inaccessible par le bas :
$$\text{Pour tout } E \text{ dirigée}, \quad \text{Si } \sup E \in U, \text{ alors } E \cap U \neq \emptyset. \tag{3}$$

Fonction Scott-continue

Soit $(X, \leq)$ un ensemble ordonné. Une famille $D \subseteq X$ est dite dirigée si :

- D est non vide ;
- et pour tous $x, y \in D$, x et y ont un majorant dans D.

Une fonction $f : X \to Y$ est Scott-continue si :

- f est monotone ;
- et pour toute famille dirigée D qui admet un sup $\vee D$, la famille $f(D)$ a un sup et $f(\vee D) = \vee f(D)$.

Exercice 1 :

Soit τ une topologie sur un ensemble X.

1. Montrer que τ contient l'ensemble X.
2. Montrer que τ contient l'ensemble $\emptyset$.

Exercice 2 :

(Topologie de Scott)

1. Montrer que la topologie de Scott est une topologie.
2. Montrer qu'un fermé de D est clos par le bas et par suprema de famille dirigée.
3. Montrer que $\downarrow x \triangleq \{y \in D \mid y \leq x\}$ est un fermé de D pour la topologie de Scott.

4. Montrer que les fonctions continues pour la topologie de Scott sont les fonctions Scott-continues.

Exercice 3 :
(Booléens) On considère $\mathbf{Bool}_\perp = \{0, 1, \perp\}$ ordonné tel que avec $x < y$ si et seulement si $x = \perp$ et $y \neq \perp$.

1. Quels sont les ouverts de Scott de $\mathbf{Bool}_\perp$? Les fermés ?
2. Exhiber toutes les fonctions monotones de $\mathbf{Bool}_\perp$ dans $\mathbf{Bool}_\perp$.
3. Soit D un dcpo, et f une fonction monotone de $\mathbf{Bool}_\perp$ dans D. Montrer que f est Scott-continue.
4. Dessiner $\mathbf{Bool}_\perp \times \mathbf{Bool}_\perp$ (ordre produit).
5. Énumérer les fonctions Scott continues f telle que f restreinte à $\{0, 1\}$ définit la fonction booléenne « ou ».
6. En voyant $\perp$ comme « un calcul divergent », donner une interprétation calculatoire de chacun des prolongements à $\mathbf{Bool}_\perp$ de la fonction booléenne « ou ».

Exercice 4 :
(Réels à précision arbitraire) Soit $I = \mathbb{R}$ et $J = \{[x, y] \mid x, y \in I, x \leq y\}$ avec l'ordre $\supseteq$.

1. Montrer que J est un dcpo. Est-ce un treillis ? Complet ?
2. Donner une fonction monotone de J dans $\mathbf{Bool}_\perp$ qui n'est pas Scott-continue.
3. Quels sont les éléments maximaux de J ? Notons M l'ensemble des éléments maximaux.
4. Soit f une fonction continue de J dans $\mathbf{Bool}_\perp$. Montrer que $f^{-1}(\{1\})$ est ouvert.
5. Considérons l'application $I : x \mapsto \{x\}$ qui va de $[0, 1]$ dans J. Montrer que I est continue.

Bonus. Qu'est-ce que la topologie de Scott restreinte à l'ensemble des éléments maximaux ?

6. Montrer que M est connexe. C'est-à-dire qu'il n'existe pas d'ouverts U, V disjoints tous deux non vides tels que
$$U \cap M \uplus V \cap M = M \tag{6}$$
7. Soit g une fonction continue de J dans $\mathbf{Bool}_\perp$ telle que pour tout $x \in I$, $g(\{x\}) \neq \perp$. Montrer que g est constante sur I.
8. Imaginons un langage de programmation qui implémente l'arithmétique réelle de précision arbitraire en utilisant des intervalles. Comment se compotera la fonction d'égalité de ce langage ?

Sémantique et vérification

Imp

On donne une version de Imp possédant non seulement des expressions arithmétiques, mais aussi des expressions booléennes.

$$\begin{aligned}
e &:= x \mid 0 \mid 1 \mid e + e \mid -e \mid e \times e \\
b &:= (e \sim e) \mid e \leq e \mid \neg b \mid b \wedge b \\
c &:= \mathbf{skip} \mid \mathbf{while}\ b\ \mathbf{do}\ c \mid x := e \mid \mathbf{if}\ b\ \mathbf{then}\ c\ \mathbf{else}\ c
\end{aligned}$$

Formules arithmétiques au premier ordre

Voici la construction des formules au premier ordre que nous autoriserons, leur ensemble est noté $\mathsf{FO}[0, 1, +, \times, \leq]$. Dans la suite i est une variable logique à valeur entière.

$$t := x \mid 0 \mid 1 \mid t + t \mid -t \mid t \times t \mid i$$
$$\phi := (t \sim t) \mid t \leq t \mid \neg\phi \mid \phi \wedge \phi \mid \exists i.\phi$$

Exercice 5 :

1. Donner une sémantique dénotationnelle aux expressions booléeenes.
2. Donner une sémantique aux formules logiques. On écrira $\rho \models^I \phi$ quand la formule ϕ est validée dans l'environnement ρ pour les variables de programme et I pour les variables logiques.
3. En remarquant que la syntaxe des expressions booléennes de Imp est un sous ensemble de la syntaxe des formules, on peut se demander si les deux sémantiques coïncident. Démontrer que pour tout I, $\rho \models^I b \iff [\![b]\!]_\rho \neq 0$.
4. Montrer que l'on peut supposer que $x < y$ est une expression booléeenne valide.
5. Pourquoi introduire des variables logiques ?

Triplets de Hoare

On appelle triplet de Hoare $\{\phi\}\ c\ \{\psi\}$. On dit que ce triplet est *valide* sous I, ce qui est noté $\models^I \{\phi\}\ c\ \{\psi\}$ quand

$$\forall \rho, \rho \models^I \phi \wedge [\![c]\!]_\rho \neq \bot \implies [\![c]\!]_\rho \models^I \psi$$

Une autre manière de présenter cela est d'étendre la sémantique des formules en posant $\bot \models^I \phi$ quelque soit la formule ϕ et l'environnement σ.
On notera $\models \{\phi\}\ c\ \{\psi\}$ quand pour tout I on a $\models^I \{\phi\}\ c\ \{\psi\}$.

Axiomatique de Hoare

On donne des règles de Hoare pour toutes les constructions excepté le while.

$$\frac{}{\{\phi\}\ \textbf{skip}\ \{\phi\}} \qquad \frac{\{\phi \wedge b\}\ c_1\ \{\psi\} \qquad \{\phi \wedge \neg b\}\ c_2\ \{\psi\}}{\{\phi\}\ \textbf{if}\ b\ \textbf{then}\ c_1\ \textbf{else}\ c_2\ \{\psi\}}$$

$$\frac{}{\{\phi[x := e]\}\ x := e\ \{\phi\}} \qquad \frac{\phi \implies \phi' \qquad \{\phi'\}\ c\ \{\psi'\} \qquad \psi' \implies \psi}{\{\phi\}\ c\ \{\psi\}}$$

Exercice 6 :

(Hoare sur un langage jouet)

1. Montrer que pour tout ρ, I, pour tout u, v termes et x variable

$$\rho \models^I \phi[x \mapsto u] \iff \rho[x \mapsto [\![u]\!]_\rho] \models^I \phi$$

2. Montrer que tout triplet de Hoare est valide. C'est-à-dire que le système est correct.
3. Proposer une règle pour le while. Montrer que celle-ci est correcte.
4. À l'aide de ce système axiomatique, prouver le triplet suivant

$$\{x \sim 0 \land y \sim 0 \land z \sim 0 \land n \geq 0\}\ c\ \{x \sim n^3\} \tag{8}$$

Où

$$c \triangleq \textbf{while}\ z < 3n\ \textbf{do}\ z := z + 3; y := y + 2z - 3; x := x + y - z + 1$$

Plus faible précondition libérale

On note $\mathsf{wlp}^I\,(c, \phi) \triangleq \{\rho \mid [\![c]\!]_\rho \models^I \phi\}$.

Exercice 7 :

(Plus faible précondition libérale)

1. Soit I une interprétation des variables logiques. Pour tout programme c sans boucle while et formule ψ, construire une formule $\phi_{c,\psi}$ telle que $\rho \models^I \phi_{c,\psi}$ si et seulement si $\rho \in \mathsf{wlp}^I\,(c, \psi)$.
2. Soit ϕ une formule définissant $\mathsf{wlp}^I\,(\textbf{while}\ b\ \textbf{do}\ c, \psi)$. Donnez une équation $\models^I \phi \iff \phi'$ où ϕ' est une formule faisant intervenir ϕ.
3. À l'aide de disjonctions et conjonctions infinies, écrire deux solutions à cette équation.
4. Laquelle correspond à ϕ ?

Exercice 8 :

(Complétude) On admet qu'il existe une formule exprimant la plus faible précondition libérale pour la boucle while.

1. Montrer que l'axiomatique définie est complète. C'est-à-dire, prouver que pour tout triplet valide $\models \{\phi\}\ c\ \{\psi\}$ il existe une dérivation de $\{\phi\}\ c\ \{\psi\}$. *Indication : On pourra commencer par le démontrer pour les plus faibles préconditions libérales.*
2. Que dire d'un système S de preuve sur les triplets de Hoare qui est correct et vérifiable ?
3. Pourquoi la logique de Hoare est-elle malgré tout complète ?
4. On admet que les plus faibles préconditions libérales sont calculables. En déduire que le problème suivant n'est pas récursivement énnumérable.

   Entrée Une formule close $\phi \in \mathsf{FO}[0, 1, +, \times, \leq]$

   Sortie Est-ce que ϕ est valide ?