Sémantique des langages de programmation sémantique dénotationelle – Suite

Yves Bertot

Mars 2008

1 Construire de nouveaux ordres partiels complets

Un ordre partiel est un ensemble muni d'une relation qui satisfait certaines propriétés. Lorsque l'on dispose déjà d'un ordre partiel complet, il est possible d'en construire de nouveaux en considérant de nouveaux ensembles: les ensembles de partie, les ensembles de fonctions, etc.

Dans cette leçon, nous allons étudier plusieurs des constructions permettant de construire de nouveaux ordres partiels et nous allons montrer comment ces constructions peuvent s'utiliser pour donner une structure d'ordre partiel complet à l'ensemble des fonctions qui représentent des programmes de notre petit langage impératif.

1.1 Une construction simple: l'ensemble des parties

Si $\mathcal{S}$ est un ensemble arbitraire, alors l'ensemble des parties de $\mathcal{S}$, noté $\mathcal{P}(\mathcal{S})$ est également un ensemble et on peut le munir de la relation d'inclusion. Une partie X de $\mathcal{S}$ est incluse dans une partie Y, noté $X \subset Y$ si tout élément de X est également élément de Y. Cette relation est réflexive, transitive et antisymétrique: deux parties sont égales si elles ont les mêmes éléments. Nous avons bien affaire à un ordre partiel.

Dans cet ordre partiel, tout ne se passe pas comme dans les nombres, naturels, entiers, rationnels, ou réels. En effet, deux nombres x et y arbitraires sont toujours comparables: soit l'on a $x \leq y$, soit l'on a $y \leq x$. En revanche, deux parties X et Y d'un ensemble peuvent ne pas être comparables, au sens où ni l'une ni l'autre n'est incluse dans la restante. Par exemple, si on considère les parties de $\mathcal{Z}$, l'ensemble des entiers relatifs, les ensembles $\{1\}$ et $\{2\}$ sont incomparables.

1.1.1 plus petit élément, plus petit majorant

L'ensemble des parties de $\mathcal{S}$ admet toujours un plus petit élément: l'ensemble vide, noté $\emptyset$. Il existe également un plus grand élément: l'ensemble $\mathcal{S}$ lui même.

Si X et Y sont deux parties de S, alors il existe toujours un plus petit majorant, c'est la réunion de X et Y, notée $X \cup Y$, l'ensemble des éléments de S qui appartiennent soit à X soit à Y. Démontrons-le.

Nous avons $X \subset X \cup Y$ et $Y \subset X \cup Y$ (par définition). Soit Z une partie de $\mathcal{S}$ telle que $X \subset Z$ et $Y \subset Z$. Montrons que $X \cup Y$ est inclus dans Z. Soit $x \in X \cup Y$, montrons que $x \in Z$. par définition, nous avons soit $x \in X$ et comme $X \subset Z$ alors nous avons $x \in Z$, soit $x \in Y$ et comme $Y \subset Z$ alors $x \in Z$. Nous avons $x \in Z$ dans les deux cas, donc $X \cup Y \subset Z$.

1.1.2 complétude

Montrons maintenant que cet ordre est complet. Prenons une suite X_i de parties de $\mathcal{S}$ et montrons que cette suite admet une plus petit majorant. Nous noterons $\bigcup X_i$ l'ensemble défini de la façon suivante:

$$\bigcup X_i = \{y \in \mathcal{S} | \exists i. y \in X_i\}$$

Notons d'abord que si $x \in X_i$ alors, $x \in X_j$, pour tout $j > i$.

Pour tout X_j on a bien $X_j \subset \bigcup X_j$. Soit Z une partie de $\mathcal{S}$ qui est un majorant de $\mathcal{S}$ et soit $x \in \bigcup X_i$. Par définition, il existe un j tel que $x \in X_j$ et $X_j \subset Z$ donc $x \in Z$. donc on a bien $\bigcup X_i \subset Z$. Donc $\bigcup X_i$ est bien un plus petit majorant de la suite X_i. Nous avons déjà vu la semaine dernière que le plus petit majorant d'un ensemble est unique (en vertu de l'antisymétrie de la relation d'ordre). Ici nous avons construit le plus petit majorant d'une suite quelconque de parties, sans imposer que cette suite soit croissante, car la propriété de croissance ne joue aucun rôle.

1.2 Espaces de fonctions partielles

Si $\mathcal{S}_1$ et $\mathcal{S}_2$ sont deux ensembles arbitraires, les fonctions partielles de $\mathcal{S}_1$ et $\mathcal{S}_2$ sont représentées par les parties de $\mathcal{S}_1 \times \mathcal{S}_2$ qui ont la propriété suivante:

$$X \text{ est une fonction} \Leftrightarrow \forall (x_1, y_1), (x_2, y_2) \in X x_1 = x_2 \Rightarrow y_1 = y_2$$

Puisque les fonctions sont les parties d'un ensemble, on peut également munir l'ensemble des fonctions partielles de l'ordre d'inclusion. Ainsi, nous savons d'emblée qu'il s'agit bien d'un ensemble partiel.

En pratique, si f et g sont des fonctions partielles et $f \subset g$, nous saurons que g est définie partout où f l'est et que $f(x) = g(x)$.

1.2.1 Complétude

Si nous considérons une suite croissante (pour l'ordre d'inclusion) de fonctions X_i, cette suite est aussi une suite croissante de sous-ensembles de $\mathcal{S}_1 \times \mathcal{S}_2$. Cette suite de sous-ensembles admet un plus petit majorant, $\bigcup X_i$ mais ce plus petit majorant peut-il être une fonction?

Soient (x, y) et (x, y') deux éléments de $\bigcup X_i$, pouvons-nous prouver que $y = y'$?

Si (x, y) est élément de $\bigcup X_i$ alors il existe un j tel que $(x, y) \in X_j$. De même, nous pouvons également trouver un k tel que $(x, y') \in X_k$. Sans perdre de généralité, nous pouvons supposer que $j < k$. Par transitivité, nous savons que $X_j \subset X_k$, donc (x, y) et (x, y') sont éléments de X_k, ce dont nous pouvons déduire que $y = y'$.

Nous pouvons donc déduire que $\bigcup X_i$ est également une fonction. C'est le plus petit majorant pour l'ordre d'inclusion, que nous appellerons maintenant l'ordre naturel sur les fonctions partielles.

1.3 Transposition d'un ordre vers les fonctions partielles

Si $\mathcal{S}_2$ est un ensemble muni d'une structure d'ordre partiel $\sqsubseteq$, il existe un autre moyen de munir l'ensemble des fonctions de $\mathcal{S}_1$ vers $\mathcal{S}_2$ d'une structure d'ordre partiel, que nous noterons (dans cette section) $\sqsubseteq'$.

Premièrement, si f est une fonction partielle de $\mathcal{S}_1$ vers $\mathcal{S}_2$, nous noterons $Dom(f)$ l'ensemble $\{x \in \mathcal{S}_1 | \exists y(x, y) \in f\}$ ($Dom(f)$ est le *domaine* de f).

Si f et g sont deux fonctions partielles de $\mathcal{S}_1$ et $\mathcal{S}_2$, nous dirons que $f \sqsubseteq' g$ si et seulement si:

1. $Dom(f) \subset Dom(g)$
2. $\forall x \in Dom(f).\ f(x) \sqsubseteq g(x)$ (cette comparaison a un sens dès que $f(x)$ est défini, puisque $Dom(f) \subset Dom(g)$).

1.3.1 Propriétés d'ordre partiel

Montrons que la relation $\sqsubseteq'$ est bien réflexive, transitive et antisymétrique.

réflexive. On a bien $Dom(f) \subset Dom(f)$, et pour tout $x \in Dom(f)$, $f(x) \sqsubseteq f(x)$.

transitive. Supposons $f \sqsubseteq' g$ et $g \sqsubseteq' h$, nous avons donc $Dom(f) \subset Dom(g) \subset Dom(h)$, ce dont nous pouvons déduire $Dom(f) \subset Dom(h)$. Maintenant, pour tout $x \in Dom(f)$, nous avons $f(x) \sqsubseteq g(x) \sqsubseteq h(x)$ ce dont nous pouvons déduire $f(x) \sqsubseteq h(x)$. Nous pouvons conclure $f \sqsubseteq' h$.

antisymétrique. Supposons $f \sqsubseteq' g$ et $g \sqsubseteq' f$. On a alors $Dom(f) \subset Dom(g) \subset Dom(f)$, ce dont nous pouvons déduire $Dom(f) = Dom(g)$. De plus, pour tout $x \in Dom(f)$, nous avons $f(x) \sqsubseteq g(x) \sqsubseteq f(x)$, ce dont nous pouvons déduire $f(x) = g(x)$. Nous pouvons en conclure que $f = g$.

1.3.2 Complétude

Supposons ici que $(\mathcal{S}_2, \sqsubseteq)$ forme un ordre partiel complet. Que pouvons nous dire de $(\mathcal{S}_1 \to \mathcal{S}_2, \sqsubseteq')$?

Considérons une suite croissante pour l'ordre $\sqsubseteq'$, la suite $Dom(f_i)$ constitue elle même une suite croissante (pour l'ordre d'inclusion) de sous-ensembles de $\mathcal{S}_1$. Nous connaissons déjà le plus petit majorant de cette suite $\bigcup Dom(f_i)$.

Soit $x \in \bigcup Dom(f_i)$. Il existe un k tel que

$$x \in Dom(f_k)$$

Supposons en outre que k est le plus petit entier tel que $x \in Dom(f_k)$, de sorte que nous avons:

$$x \in Dom(f_k) \wedge \forall j.\ j < k \Rightarrow f_j(x) \text{ n'est pas définie}$$

Nous pouvons construire la suite $y_i \in \mathcal{S}_2$ définie par $y_i = f_{k+i}(x)$. Puisque la suite f_i est croissante pour l'ordre $\sqsubseteq'$, la suite y_i est croissante pour l'ordre $\sqsubseteq$. Notons $f(x)$ le plus petit majorant de cette suite. Montrons que la fonction f ainsi définie est en fait le plus petit majorant de la suite f_i.

Par construction, f est un majorant de toutes les fonctions f_i. En effet, pour tout i, on a bien $Dom(f_i) \subset \bigcup Dom(f_i) = Dom(f)$, et pour tout $x \in Dom(f_i)$, on a $f_i(x) \sqsubseteq f(x)$ par définition de $f(x)$ comme plus petit majorant de la suite $f_j(x)$ donc majorant de $f_i(x)$, en particulier.

Soit maintenant g une fonction majorant la suite f_i. Soit x un élément de $Dom(f)$. Par construction, $Dom(f) = \bigcup(f_i)$, donc il existe un j tel que $x \in Dom(f_j)$, mais comme $f_j \sqsubseteq g$, on a également $Dom(f_j) \subset Dom(g)$ et donc $x \in Dom(g)$. Si g est un majorant de la suite f_j en particulier, $g(x)$ est un majorant de la suite $f_{k+i}(x)$ où k est le plus petit entier tel que $f_k(x)$ est défini. donc $g(x)$ est un majorant de $f(x)$ puis que $f(x)$ est le plus petit majorant de la suite $f_{k+i}(x)$. Ceci permet de conclure que f est le plus petit majorant de la suite f_i.

Le couple $(\mathcal{S}_1 \to \mathcal{S}_2, \sqsubseteq')$ est donc bien un ordre partiel complet, dès que le couple $(\mathcal{S}_2, \sqsubseteq)$ est un ordre partiel complet.

2 Applications à la sémantique dénotationnelle

Notre objectif est de trouver la fonction $\mathcal{I}[\![while(e,i)]\!]$ lorsque e et i sont des fonctions arbitraires. Nous avons montré que cette fonction devait vérifier l'équation suivante:

$$\mathcal{I}[\![while(e,i)]\!] = \lambda\sigma.\ \text{si } \mathcal{A}[\![e]\!](\sigma) = true \text{ alors } \mathcal{I}[\![while(e,i)]\!] \circ \mathcal{I}[\![i]\!](\sigma) \text{ sinon } \sigma$$

En d'autres termes, $\mathcal{I}[\![while(e,i)]\!]$ doit vérifier l'équation

$$\mathcal{I}[\![while(e,i)]\!] = \Gamma(\mathcal{I}[\![while(e,i)]\!])$$

où Γ est donné par la définition suivante:

$$\Gamma = \lambda f.\lambda\sigma.\ \text{si } \mathcal{A}[\![e]\!](\sigma) = true \text{ alors } f \circ \mathcal{I}[\![i]\!](\sigma) \text{ sinon } \sigma$$

Existe-t-il une fonction telle que $f = \Gamma(f)$? Si Γ était une fonction arbitraire dans un ensemble quelconque, ce ne serait pas sûr. Mais ici, nous savons que Γ est une fonction de l'ordre partiel complet des fonctions partielles dans lui-même. Cette fonction est elle croissante? Nous allons le voir tout de suite.

Soient f et g deux fonctions de l'ensemble $state \rightarrow state$ dans lui-même[1]. Notons $\sqsubseteq$ l'ordre naturel entre les fonctions partielles et supposons $f \sqsubseteq g$. Ceci signifie que pour tout $\sigma \in state$, si $f(\sigma)$ est défini, alors $g(\sigma)$ est défini et $g(\sigma) = f(\sigma)$. Pouvons nous comparer $\Gamma(f)$ et $\Gamma(g)$?

Notons $f' = \Gamma(f)$ et $g' = \Gamma(g)$ prenons un $\sigma \in state$ tel que $f'(\sigma)$ est défini. Par définition de f' et Γ, nous savons qu'alors $\mathcal{A}[\![e]\!](\sigma)$ est défini, et nous pouvons avoir deux cas:

1. Si $\mathcal{A}[\![e]\!](\sigma) = false$ alors on a les égalités suivantes:

$$f'(\sigma) = \Gamma(f)(\sigma) = \sigma = \Gamma(g)(\sigma) = g'(\sigma)$$

2. Si $\mathcal{A}[\![e]\!](\sigma) = true$ alors on sait que $\mathcal{I}[\![i]\!](\sigma)$ est défini et que $f(\mathcal{I}[\![i]\!](sigma))$ est défini. Puisque $f \sqsubseteq g$ on sait également que $g(\mathcal{I}[\![i]\!](sigma))$ est défini et

$$g(\mathcal{I}[\![i]\!](sigma)) = f(\mathcal{I}[\![i]\!](sigma))$$

   On en déduit que $g'(\sigma)$ est défini et $g'(\sigma) = f'(\sigma)$.

Dans les deux cas, on a obtenu que $g'(\sigma)$ est défini et $g'(\sigma) = f'(\sigma)$. Ceci montre que $\Gamma(f) \sqsubseteq \Gamma(g)$, donc Γ est croissante.

La fonction Γ est-elle continue? Pour le savoir, considérons une suite de fonctions f_i, où toutes les fonction f_i sont des fonctions de $state \rightarrow state$ et où $f_i \sqsubseteq f_{i+1}$, notons $f = \sqcup f_i$ le plus petit majorant de cette suite et notons $f' = \sqcup \Gamma(f_i)$.

Montrons que $f' \sqsubseteq \Gamma(f)$. Considérons un état σ tel que $f'(\sigma)$ soit défini. Par définition de l'ordre naturel sur les fonctions partielles, il existe un j tel que $\Gamma(f_j)(\sigma)$ est défini et $f'(\sigma) = \Gamma(f_j)(\sigma)$. Mais ceci n'est possible que si l'une des deux affirmations suivantes est satisfaite:

1. $\mathcal{A}[\![e]\!](\sigma) = false$ et $\Gamma(f_j)(\sigma) = (\sigma)$ et on aurait $\Gamma(g)(\sigma) = (\sigma)$ pour tout g, donc en particuler $\Gamma(f)(\sigma) = (\sigma)$.

2. $\mathcal{A}[\![e]\!](\sigma) = true$ et alors f_j est définie en $\mathcal{I}[\![i]\!](\sigma)$, mais par définition de f, f est également définie en $\mathcal{I}[\![i]\!](\sigma)$ et l'on a pour tout $j' > j$

$$f_{j'}(\mathcal{I}[\![i]\!](\sigma)) \sqsubseteq f(\mathcal{I}[\![i]\!](\sigma))$$

   donc $f(\mathcal{I}[\![i]\!](\sigma))$ est un majorant de la suite des $f_j(\mathcal{I}[\![i]\!](\sigma))$. Comme $f'(\mathcal{I}[\![i]\!](\sigma))$ est le plus petit des majorants on a bien:

$$f'(\sigma) \sqsubseteq \Gamma(f)(\sigma).$$

[1] l'ensemble state est lui-même l'ensemble $V \rightarrow int$ l'ensemble des fonctions partielles des variables vers les valeurs entières.

Ceci montre que $\Gamma(f)$ est définie partout où f' est définie et $\Gamma(f)(\sigma) = f'(\sigma)$.

Pour montrer que $\Gamma(f) \sqsubseteq f'$ il faut maintenant montrer que f' est définie partout où $\Gamma(f)$ l'est. Soit σ un état tel que $\Gamma(f)(\sigma)$ est défini. Par définition de Γ, nous avons encore deux cas possibles:

1. $\mathcal{A}[\![e]\!](\sigma) = false$ et $\Gamma(g)$ est définie pour tout g, en particulier $\Gamma(f_j)(\sigma)$ pour un j quelconque et $f'(\sigma)$ est nécessairement définie puisque f' majore $\Gamma(f_j)$.

2. $\mathcal{A}[\![e]\!](\sigma) = true$ et alors f est définie en $\mathcal{I}[\![i]\!](\sigma)$. Par définition du plus petit majorant pour l'ordre naturel des fonctions partielles, il existe un j tel que f_j soit définie en $\mathcal{I}[\![i]\!](\sigma)$. Par définition de Γ, $\Gamma(f_j)$ est donc défini en σ. Puisque f' est un majorant de $\Gamma(f_j)$, on obtient nécessairement que f' est définie en σ.

Nous avons montré que $f'(\sigma)$ est défini dans les deux cas. Nous devons maintenant montrer que $\Gamma(f)(\sigma) \sqsubseteq f'(\sigma)$ lorsque cette valeur est définie. C'est trivial si $\mathcal{B}[\![e]\!](\sigma) = false$, puisqu'alors les deux valeurs sont définies. dans l'autre cas, si $\Gamma(f)(\sigma)$ est définie, c'est que f est définie en $\mathcal{I}[\![i]\!](\sigma)$, et comme f est le plus petit des majorants f_i, $f(\mathcal{I}[\![i]\!](\sigma))$ est le plus petit des majorants des $f_i(\mathcal{I}[\![i]\!](\sigma))$ et donc plus petit que $\sqcup\Gamma(f_i)(\sigma) = f'(\sigma))$.

Des deux comparaisons nous obtenons bien que $\Gamma(f) = f'$, la fonction Γ est continue. Cette fonction admet un point fixe et ce point fixe est le plus petit majorant de la suite:

$$\emptyset, \Gamma(\emptyset), \Gamma(\Gamma(\emptyset)), \ldots \Gamma^k(\emptyset), \ldots$$

où $\emptyset$ est la fonction qui n'est définie nulle part.