# Excursión Matemática: Iteración y *least fixed points.* Aplicación a la semántica de `while`

## 1 Conjuntos parcialmente ordenados completos y con un menor elemento (*cpo with bottom*)

1. Un **orden parcial**(*po*) $(A, \sqsubseteq)$ es un par formado por un conjunto $A$ y una relación binaria en $A$ que denotamos $\sqsubseteq$ que es reflexiva, transitiva y antisimétrica.

2. Dado un orden parcial $(A, \sqsubseteq)$ y un subconjunto $X \subseteq A$, se dice que un elemento $a \in A$ es una **cota superior** de $X$ síi $x \sqsubseteq a$ para cualquier $x \in X$. Dicho elemento se denomina **supremo** (*lub*) de $X$ síi $a$ es una cota superior de $X$ y además $a \sqsubseteq b$ si $b$ es también una cota superior de $X$.

   Como consecuencia, el supremo de un $X$, si existe, es único (¿porqué?) y se denota por $\bigsqcup X$.

3. Un orden parcial $(A, \sqsubseteq)$ es **completo** (*cpo*) si toda cadena de elementos del conjunto A: $a_0 \sqsubseteq a_1 \sqsubseteq \ldots \sqsubseteq a_n \sqsubseteq \ldots$ tiene supremo que denotaremos $\bigsqcup_n a_n$. Si además tiene un menor elemento (es decir un elemento $\bot \in A$ tal que $\bot \sqsubseteq a$ para todo $a \in A$) se dirá que es un **orden parcial completo com mínimo** (*cpo with bottom*).

## 2 Puntos fijos de funciones entre órdenes parciales completos con mínimo

1. Dados dos ordenes parciales completos con mínimo [1] $(D, \sqsubseteq_D)$ y $(E, \sqsubseteq_E)$, una función $f : D \to E$ se dice que es **continua** síi

   - siempre que $d \sqsubseteq_D d'$ entonces $f(d) \sqsubseteq_E f(d')$ (monótona) y
   - para cualquier cadena $d_0 \sqsubseteq_D d_1 \sqsubseteq_D \ldots \sqsubseteq_D d_n \sqsubseteq_D \ldots$ en $D$ se tiene que[2] $\bigsqcup_n f(d_n) = f(\bigsqcup_n d_n)$.

2. **Teorema**: *Si $(D, \sqsubseteq)$ es un orden parcial completo con mínimo y $f : D \to D$ es continua, entonces existe un menor punto fijo de $f$ (que denotaremos $f^{fix}$) y su valor es:*

$$f^{fix} = \bigsqcup_n f^n(\bot)$$

   **Demostración**: Tenemos que probar dos cosas: en primer lugar que tal elemento (cuya existencia está garantizada por ser $\bot \sqsubseteq f(\bot) \sqsubseteq f^2(\bot) \sqsubseteq \ldots \sqsubseteq f^n(\bot) \sqsubseteq \ldots$ una cadena (¿porqué?) y por ser $(D, \sqsubseteq)$ un orden parcial completo con mínimo) es efectivamente un punto fijo, es decir, que se cumple $f(f^{fix}) = f^{fix}$ y que nuestro $f^{fix}$ está relacionado por $\sqsubseteq$ con cualquier otro punto fijo de $f$, es decir que cualquier $d \in D$ tal que $f(d) = d$ deberá cumplir que $f^{fix} \sqsubseteq d$.

   Para probar lo primero hacemos un simple cálculo:

   $f(f^{fix}) = f(\bigsqcup_n f^n(\bot)) = \bigsqcup_n f(f^n(\bot)) = \bigsqcup_n f^{n+1}(\bot) = \bot \sqcup \bigsqcup_n f^n(\bot) = \bigsqcup_n f^n(\bot) = f^{fix}$.

   Y para lo segundo, si $f(d) = d$, como tiene que cumplirse que $\bot \sqsubseteq d$, entonces por el carácter monótono de $f$ se tendrá que $f^n(\bot) \sqsubseteq f^n(d) = d$ para cualquier $n$ de modo que el supremo de todos los $f^n(\bot)$ (o sea $f^{fix}$) cumplirá, efectivamente que $f^{fix} \sqsubseteq d$ tal como habíamos dicho.

[1] como hay dos órdenes parciales involucarados tenemos que distinguir el orden del primero y del segundo, por eso usamos un subfijo en el símbolo de la relación de orden.

[2] nótese que al ser $f$ monótona, los elementos $f(d_0), f(d_1) \ldots f(d_n), \ldots$ forman también una cadena.

## 3 Nuestro caso

1. consideremos el conjunto de todas las funciones parciales del conjunto de estados $\Sigma$ en sí mismo: $\Sigma \rightharpoonup \Sigma$ y en él definimos el orden parcial definido por

$$\phi \sqsubseteq \psi$$

sii $dom(\phi) \subseteq dom(\psi)$ y $\forall \sigma \in dom(\phi),\ \phi(\sigma) = \psi(\sigma)$, es decir, si la segunda está definida en todos los estados donde lo está la primera y en esos estados coinciden. Tenemos así un *cpo with bottom* pues efectivamente hay una función parcial que está relacionada (diremos simplemente que es "menor o igual que") con todas y que no es otra que la función vacía cuyo dominio es el conjunto $\emptyset$ y que representaremos simplemente $\emptyset$. Además es completo pues cualquier cadena de funciones parciales:

$$\phi_0 \sqsubseteq \phi_1 \sqsubseteq \dots \phi_n \sqsubseteq \dots$$

tiene como supremo la función parcial cuyo dominio es la reunión de los dominio de todas ellas y que en un estado toma el valor que toma alguna de ellas. Este valor no depende de la que tomemos (¿porqué?). De ahora en adelante, para simplificar, en lugar de escribir $\phi \sqsubseteq \psi$ y $\bigsqcup_n \phi_n$ pondremos $\phi \subseteq \psi$ y $\bigcup_n \phi_n$ respectivamente para representar el orden y el supremo.

2. **Notaciones útiles**:
   - Si $\sigma$ es un estado y $c$ es un programa que termina ejecutado en el estado $\sigma$, entonces escribiremos simplemente $\sigma^c$ en lugar de $\mathcal{C}[\![c]\!](\sigma)$.
   - En lugar de $\mathcal{B}[\![b]\!]\sigma = \texttt{true}$ escribiremos $\sigma \models b$ y analogamente en lugar de $\mathcal{B}[\![b]\!]\sigma = \texttt{false}$ pondremos $\sigma \models \neg b$

3. Si $b$ es una expresión booleana y $c$ es un programa, vamos a ver que la función $\Gamma_{b,c} : (\Sigma \rightharpoonup \Sigma) \to (\Sigma \rightharpoonup \Sigma)$ definida por[3]

$$\Gamma(\phi)\sigma = \begin{cases} \phi(\sigma^c) & \text{si } \sigma \models b \\ \sigma & \text{si } \sigma \models \neg b \end{cases}$$

es **continua** y por lo tanto, en virtud del resultado general anterior, poseerá un menor punto fijo.

   (a) (Monotonía) Hay que ver que si $\phi \subseteq \psi$ entonces $\Gamma(\phi) \subseteq \Gamma(\psi)$. Para ello tomamos un estado cualquiera $\sigma$ en el que $\Gamma(\phi)$ esté definida y hay que ver que entonces $\Gamma(\psi)$ también lo está y que valen lo mismo. Una tal $\sigma$ o cumple $\sigma \models \neg b$ (en cuyo caso ambas funciones valen $\sigma$) ó $\sigma \models b$ y por lo tanto:

$$\Gamma(\phi)\sigma = \phi(\sigma^c) = \psi(\sigma^c) = \Gamma(\psi)\sigma.$$

   (b) (Conserva supremos) Dada una cadena $\phi_0 \subseteq \phi_1 \subseteq \dots \phi_n \subseteq \dots$ hay que probar que

$$\bigcup_n (\Gamma(\phi_n)) = \Gamma(\bigcup_n \phi_n)$$

pero si $\sigma$ es un estado en el que está definido el lado izquierdo, existirá un $k$ tal que $(\bigcup_n (\Gamma(\phi_n)))(\sigma) = \Gamma(\phi_k)\sigma$ valor que dependerá de si $\sigma \models \neg b$ o bien $\sigma \models b$. En el primer caso dará $\sigma$ que es también el resultado del lado derecho; y en el segundo dará $\phi_k(\sigma^c)$ y el lado derecho $(\bigcup_n \phi_n)(\sigma^c)$ que son el mismo (¿porqué?).

[3] escribiremos simplemente $\Gamma$ en lugar de $\Gamma_{b,c}$ cuando no haya confusión

4. Habiendo comprobado la continuidad de $\Gamma$ podemos dar ya una fórmula para calcular su menor punto fijo que será justamente la semántica denotacional buscada para nuestro `while` $b$ `do` $c$:

$$\mathcal{C}[\![\texttt{while } b \texttt{ do } c]\!] = \Gamma^{fix} = \bigcup_n \Gamma^n(\emptyset)$$

5. Lo primero que observamos es que nuestra $\Gamma^{fix}$ se convierte en una función recursiva definida por:

$$\Gamma^{fix}(\sigma) = \Gamma(\Gamma^{fix})(\sigma) = \begin{cases} \Gamma^{fix}(\sigma^c) & \text{si } \sigma \models b \\ \sigma & \text{si } \sigma \models \neg b \end{cases}$$

Si $\Gamma^{fix}$ está definida en $\sigma$ y $\sigma \models b$ habrá un **primer** $n > 0$ (¿porqué?) tal que $\sigma^{(c^n)} \models \neg b$ Entonces

$$\Gamma^{fix}(\sigma) = \Gamma^{fix}(\sigma^c) = \Gamma^{fix}(\sigma^{(c^2)}) = \cdots = \Gamma^{fix}(\sigma^{(c^{n-1})}) = \Gamma^{fix}(\sigma^{(c^n)}) = \sigma^{(c^n)}$$

Si llamamos $D_0 = \emptyset$ abreviemos también $D_1 = \{\sigma \in \Sigma \mid \sigma \models \neg b\}$ De esta forma es fácil representar los dominios de las sucesivas potencias $\Gamma^n(\emptyset)$ que nos ayudará a comprender su significado:

| | |
|---|---|
| $\Gamma^0(\emptyset) = \emptyset$ | $D_0$ |
| $\Gamma(\emptyset)(\sigma) = \begin{cases} \emptyset(\sigma^c) & \text{si } \sigma \models b \\ \sigma & \text{si } \sigma \models \neg b \end{cases}$ | $D_1$ |
| $\Gamma^2(\emptyset)(\sigma) = \begin{cases} \Gamma(\emptyset)(\sigma^c) & \text{si } \sigma \models b \\ \sigma & \text{si } \sigma \models \neg b \end{cases}$ | $D_2 = D_1 \cup \{\sigma \in \Sigma \mid \sigma \models b \ \& \ \sigma^c \models \neg b\}$ |
| $\Gamma^3(\emptyset)(\sigma) = \begin{cases} \Gamma^2(\emptyset)(\sigma^c) & \text{si } \sigma \models b \\ \sigma & \text{si } \sigma \models \neg b \end{cases}$ | $D_3 = D_2 \cup \{\sigma \in \Sigma \mid \sigma \models b \ \& \ \sigma^c \models b \ \& \ \sigma^{(c^2)} \models \neg b\}$ |
| $\vdots$ | $\vdots$ |
| $\Gamma^{n+1}(\emptyset)(\sigma) = \begin{cases} \Gamma^n(\emptyset)(\sigma^c) & \text{si } \sigma \models b \\ \sigma & \text{si } \sigma \models \neg b \end{cases}$ | $D_{n+1} = D_n \cup \{\sigma \in \Sigma \mid \sigma \models b \ \& \ \sigma^c \models b \ \& \ \sigma^{(c^2)} \models b \ \vdots \ \& \ \sigma^{(c^{n-1})} \models b \ \& \ \sigma^{(c^n)} \models \neg b\}$ |

Resumiendo,

$$\Gamma^{fix}(\sigma) \quad = \quad \Gamma^n(\emptyset)(\sigma) = \sigma^{c^n}$$

significa que si se ejecuta `while` $b$ `do` $c$ en el estado $\sigma$ el programa termina en el estado $\sigma'$ despues de, a lo sumo $n$ ejecuciones del bucle $c$ y además $\sigma'$ no satisface el test $b$.

6. **Ejercicio**: Consideremos el programa `while x>1 do (y:=x*y;x:=x-1)`. Calcular su semántica denotacional siguiendo el método anterior.

   Se trata pues de calcular ${\Gamma_{b,c}}^{fix}$ donde $b$ es `x>1` y $c$ es `y:=x*y;x:=x-1`.