

Examen Programmation I (2020-21)

On insistera sur la correction et la clarté des réponses. Toute affirmation devra être justifiée explicitement, par un théorème du cours, par un numéro de question, par une référence à une règle. Pour tout raisonnement par récurrence, on devra dire sur quoi est effectuée la récurrence. N'inventez pas vos propres notations, et réutilisez les miennes, même si elles ne vous plaisent pas. Je veux une copie au propre, pas un brouillon : pas de rature, pas de questions dans le désordre, notamment. Je corrigerai très probablement toutes les copies en corrigeant d'abord toutes les questions 1 de tout le monde, puis toutes les questions 2, et ainsi de suite : ne comptez pas sur le fait que je me souviens de ce que vous avez écrit dans une question précédente.

Je me réserve le droit de ne pas chercher à comprendre une réponse illisible, insuffisamment claire, ou plus longue ou compliquée que nécessaire.

J'appellerai *fonction* ce qu'on appelle plus communément une application, c'est-à-dire une fonction totale.

1 Prolog

On considère le langage suivant, qui est un sous-ensemble de Prolog. On rappelle la notion de terme, vue en cours dans le cadre du système de typage de ML. L'ensemble $\mathcal{T}(\Sigma, X)$ des termes s, t, u, v, \dots est défini inductivement par : les variables x, y, z, \dots de X sont des termes de $\mathcal{T}(\Sigma, X)$, et les *applications* $f(t_1, \dots, t_n)$ de f (avec f/n dans la signature Σ) à n termes t_1, \dots, t_n de $\mathcal{T}(\Sigma, X)$ sont dans $\mathcal{T}(\Sigma, X)$.

On supposera dans la suite que Σ contient au moins une constante $a/0$. L'ensemble $\mathcal{T}(\Sigma)$ des *termes clos*, défini comme égal à $\mathcal{T}(\Sigma, \emptyset)$, est alors non vide.

Un *atome* A est juste une application $p(t_1, \dots, t_n)$, et p s'appelle le *prédicat* de l'atome. On notera Π l'ensemble des prédicats. Une *clause définie* est une expression de la forme $A :- A_1, \dots, A_m$. où A, A_1, \dots, A_m sont des atomes. (L'entier m peut être nul, auquel cas on écrira juste A : ce genre de clause définie s'appelle un *fait*.) L'atome A forme la *tête* de cette clause définie, et A_1, \dots, A_m est son *corps*.

Un *programme Prolog* est juste une liste finie de clauses définies. On peut lire un programme Prolog de deux façons : soit comme une axiomatisation logique, où une clause définie comme ci-dessus se lira « A_1 et \dots et A_m impliquent logiquement A » ; soit comme un programme exécutable.

Par exemple, le programme Prolog suivant :

```
append(nil,L,L).
append(cons(X,L),L',cons(X,L')) :- append(L,L',L').
```

définit logiquement `append` de sorte que `append(ℓ_1, ℓ_2, ℓ_3)` soit vrai si et seulement si ℓ_3 est la concaténation des listes ℓ_1 et ℓ_2 . (Par convention les fonctions de Σ sont les noms commençant par une minuscule, et les variables commencent par une majuscule.) On peut l'utiliser pour *calculer* la concaténation de listes : si l'on entre le programme Prolog ci-dessus dans, par exemple, SWI-Prolog, et que l'on tape :

```
? append(cons(1,nil), cons(2,cons(3,nil)), Resultat).
```

SWI-Prolog va répondre :

```
yes
```

```
Resultat = cons(1,cons(2,cons(3,nil)))
```

Dans cette partie, on se fixe un programme Prolog P .

On appellera *environnement* ρ toute fonction des variables vers les termes clos. On définit l'application $t\rho$ d'un environnement ρ à un terme t exactement comme pour les substitutions. En général, on manipulera les environnements exactement comme les substitutions.

On notera que $t\rho$ est toujours un terme clos. On étendra la notion d'application de substitutions et d'environnements à tout atome, toute clause, de la façon évidente.

Pour tout $E \in \mathbb{P}(\mathcal{T}(\Sigma))$, définissons un ensemble $T_P(E)$ comme suit. Voici d'abord l'idée intuitive. E est typiquement l'ensemble des atomes clos dont on sait qu'ils sont vrais, parce qu'ils ont été déduits en, disons, k étapes à partir des faits de P . $T_P(E)$ est l'ensemble des atomes clos déduits de ceux de E à l'aide d'une clause définie de P , en une étape ; si E est comme ci-dessus, $T_P(E)$ sera donc l'ensemble des atomes clos déduits en $k+1$ étapes à partir des faits de P . Formellement (et seule cette définition compte pour le raisonnement !) :

$$T_P(E) = \{A\rho \mid \rho \text{ environnement, et il existe une clause définie } (A :- A_1, \dots, A_n) \in P \text{ de tête } A \text{ et telle que } A_1\rho, \dots, A_n\rho \in E\}.$$

On munit $\mathbb{P}(\mathcal{T}(\Sigma))$ de l'ordre \subseteq , ce qui en fait un treillis complet, et donc un dcpo.

Question 1 Montrer que T_P est Scott-continue.

La monotonie est triviale : si $A_1\rho, \dots, A_n\rho \in E$ et $E \subseteq E'$, alors $A_1\rho, \dots, A_n\rho \in E'$.

La continuité est plus difficile. On a $\bigcup_{i \in I} T_P(E_i) \subseteq T_P(\bigcup_{i \in I} E_i)$ par monotonie.

Réciproquement, si $E = \bigcup_{i \in I} E_i$ (dirigée), on veut montrer que tout atome $A\theta_0$ dans $T_P(E)$ est dans un $T_P(E_i)$. Mais $A\theta_0$ est obtenu à partir d'une clause définie avec $A_1\theta_0$ dans E donc dans un E_{i_1} , $A_2\theta_0$ dans E donc dans un E_{i_2} , \dots , $A_n\theta_0$ est dans E donc dans un E_{i_n} . Il n'y a qu'un nombre fini de $E_{i_1}, E_{i_2}, \dots, E_{i_n}$. Comme la famille est dirigée, il y a un E_i qui les contient tous ; donc $A\theta_0$ est dans $T_P(E_i)$.

Question 2 Pourquoi le plus petit point fixe de T_P existe-t-il ?

Théorème de Kleene : plus petit point fixe d'une fonction continue sur un dcpo pointé (\emptyset est le plus petit élément).

Ou bien Knaster-Tarski : plus petit point fixe d'une fonction monotone sur un treillis complet. (Mais c'est moins utile pour la suite.)

On notera $\text{lfp}(T_P)$ le plus petit point fixe de T_P . C'est, intuitivement, l'ensemble des atomes clos *vrais* dans l'interprétation logique de P . C'est aussi, de façon plus banale, la sémantique dénotationnelle du programme Prolog P .

Etant donné un *but*, c'est-à-dire un atome B , pas nécessairement clos, précédé du symbole ? (comme ? `append(cons(1,nil), cons(2,cons(3,nil)))`, `Resultat`), avec une variable `Resultat`, Prolog va chercher des valeurs des variables dans B rendant B vrai. Formellement, Prolog va chercher s'il existe un environnement ρ tel que $B\rho \in \text{lfp}(T_P)$ (et en retourner un, restreint aux variables de B , s'il en existe un).

On note $\text{mgu}(A \doteq B)$ l'unificateur le plus général (le mgu) de l'équation $A \doteq B$. On a vu la notion en cours pour des équations entre termes. Ici il s'agit d'équations entre atomes : l'extension aux atomes est triviale.

Question 3 Supposons qu'aucune variable n'apparaisse à la fois dans l'atome B et dans le programme P . On notera aussi $\text{vars}(B)$ l'ensemble des variables apparaissant dans B , et de même $\text{vars}(P)$, etc.

Montrer que si $B\rho \in \text{lfp}(T_P)$, alors : (i) il existe une clause définie $A :- A_1, A_2, \dots, A_n$ dans P telle que l'équation $B \doteq A$ soit unifiable ; (ii) en posant $\theta = \text{mgu}(B \doteq A)$, $B\rho$ s'écrit $B\theta\rho'$ pour un certain environnement ρ' ; (iii) $A_1\theta\rho', \dots, A_n\theta\rho'$ sont tous dans $\text{lfp}(T_P)$.

$B\rho$ s'écrit $A\theta_0$ pour une certaine clause comme dans la définition de T_P , car il est dans $\text{lfp}(T_P) = T_P(\text{lfp}(T_P))$. Comme B et P (donc A) n'ont aucune variable en commun, la substitution θ' obtenue comme l'union de $\theta_0|_{\text{vars}(A)}$ et de $\rho|_{\text{vars}(P)}$ existe, et $B\theta' = B\rho = A\theta_0 = A\theta'$. Donc θ' unifie $B \doteq A$, ce qui établit (i). Par définition du mgu, θ est plus générale que θ' , i.e., $\theta = \theta\rho'$ pour une substitution ρ' . Donc $B\rho = B\theta\rho'$, et l'on peut ensuite étendre ρ' arbitrairement à toutes les variables hors de $\text{vars}(B)$ (ce qui est possible car il existe des termes clos ! et il en existe par notre hypothèse qu'il existe au moins une constante a/0), ce qui établit (ii). De plus, tous les $A_i\theta\rho'$ ($= A_i\theta_0$) sont dans $\text{lfp}(T_P)$, ce qui établit (iii).

Pour une clause définie C de P et un atome B , on appellera *renommage de C loin de B* une clause de la forme $C\rho$, où ρ est un renommage (une substitution qui envoie les variables vers des variables, et qui est injective sur l'ensemble des variables libres de C), de sorte qu'il n'y ait aucune variable en commun entre $C\rho$ et B .

On définit une sémantique opérationnelle de Prolog comme suit. Une configuration C de cette sémantique est un multi-ensemble fini de buts. L'unique règle, dite de *résolution*, est :

$$C \cup \{?B\} \xrightarrow{\theta} C\theta \cup \{?A_1\theta, \dots, ?A_n\theta\}$$

où $A :- A_1, A_2, \dots, A_n$ est un renommage d'une clause définie dans P loin de B , et $\theta = \text{mgu}(B \doteq A)$. (Oui, la sémantique est non déterministe : on ne précise pas comment choisir le but $?B$ dans la configuration.) Noter qu'on a pris soin d'étiqueter la transition par le mgu θ : ce sera parfois pratique dans la suite. On notera $C \longrightarrow C'$ pour dire que $C \xrightarrow{\theta} C'$ pour une certaine substitution θ , si elle n'est pas importante. Ceci permet de définir la clôture réflexive-transitive \longrightarrow^* , notamment.

On appellera *instance* d'un but $?A$ tout atome clos de la forme $A\rho$, où ρ est un environnement. On appellera $A\rho$ plus précisément une ρ -instance de A lorsqu'on veut mentionner ρ explicitement.

Question 4 Montrer que la règle de résolution est correcte, au sens où, pour tout environnement ρ , si toutes les ρ -instances du côté droit $C\theta \cup \{?A_1\theta, \dots, ?A_n\theta\}$ sont dans $\text{lfp}(T_P)$, alors toutes les $\theta\rho$ -instances du côté gauche $C \cup \{?B\}$ sont aussi dans $\text{lfp}(T_P)$.

Pour les buts de C (gauche; $C\theta$ à droite), c'est évident. Sinon, on a $A_i\theta\rho$ dans $\text{lfp}(T_P)$ donc $B\theta\rho$ est dans $T_P(\text{lfp}(T_P)) = \text{lfp}(T_P)$.

Question 5 En déduire que la sémantique opérationnelle de Prolog est correcte : si $\{?B\} \longrightarrow^* \emptyset$, et plus précisément si $\{?B\} = C_0 \xrightarrow{\theta_1} C_1 \xrightarrow{\theta_2} \dots \xrightarrow{\theta_m} C_m = \emptyset$, alors il existe une substitution θ telle que, pour tout environnement ρ , $B\theta\rho$ est dans $\text{lfp}(T_P)$. On construira θ explicitement.

Dans ce cas, Prolog répond **yes** suivi de la restriction de θ à $\text{vars}(B)$.

On a $\{?B\} = C_0 \xrightarrow{\theta_1} C_1 \xrightarrow{\theta_2} \dots \xrightarrow{\theta_m} C_m = \emptyset$ où on a décoré chaque flèche des mgus calculés. Par la question précédente, et une récurrence facile sur m si l'on souhaite être formel, $B\theta\rho$ est dans $\text{lfp}(T_P)$ pour tout ρ , si l'on pose $\theta = \theta_1\theta_2\dots\theta_m$.

Question 6 En adaptant la **Question 3**, montrer que la sémantique opérationnelle de Prolog est aussi adéquate : si $B\rho$ est une instance de $?B$ dans $\text{lfp}(T_P)$, alors $\{?B\} \longrightarrow^* \emptyset$. On montrera plus précisément que si $B\rho$ est une instance de $?B$ dans $\text{lfp}(T_P)$, alors il existe un nombre fini d'étapes $\{?B\} = C_0 \xrightarrow{\theta_1} C_1 \xrightarrow{\theta_2} \dots \xrightarrow{\theta_m} C_m = \emptyset$ et un environnement ρ' tel que $\rho = \theta_1\theta_2\dots\theta_m\rho'$.

Erratum : tel que ρ et $\theta_1\theta_2\dots\theta_m\rho'$ coïncident sur les variables libres de B .

Pour tenir compte de l'erratum, on pose ρ_0 la restriction de ρ aux variables libres de B , et l'on va montrer qu'il existe une substitution ρ'_0 telle que $\rho_0 = \theta_1\theta_2\dots\theta_m\rho'_0$. On peut se restreindre à ce que le domaine de ρ'_0 soit l'ensemble des variables libres dans $B\theta_1\theta_2\dots\theta_m$, auquel cas ρ'_0 envoie toutes les variables de son domaine vers des termes clos. On peut alors définir ρ' comme n'importe quel environnement coïncidant avec ρ'_0 sur cet ensemble (ce qui est possible car il existe au moins une constante, donc au moins un terme clos).

Pour tout ensemble fini C_0 de buts, écrivons $C_0\rho_0$ pour l'ensemble des ρ_0 -instances de buts de C_0 .

On montre plus généralement que si $C_0\rho_0$ est inclus dans $\text{lfp}(T_P)$, pour C_0 fini, alors on a une suite $C_0 \xrightarrow{\theta_1} C_1 \xrightarrow{\theta_2} \dots \xrightarrow{\theta_m} C_m = \emptyset$ et une substitution ρ'_0 telles que ρ_0 et $\theta_1\theta_2\dots\theta_m\rho'_0$ coïncident sur les variables libres de C_0 , où les σ_i sont des renommages de clauses de P .

On a $\text{lfp}(T_P) = \bigcup_{n \in \mathbb{N}} T_P^n(\emptyset)$, en utilisant le théorème de Kleene, et donc tout élément appartient à $T_P^m(\emptyset)$ pour un certain m . Appelons rang d'un but dans $\text{lfp}(T_P)$ le plus petit entier m tel que ce but est dans $T_P^m(\emptyset)$.

On procède par récurrence sur (n, m) , ordonné lexicographiquement, où m est le plus grand rang d'un but de C_0 et n est le nombre de buts de rang m dans C_0 (par exemple; ce faisant, on résout d'abord les sous-buts de rang le plus grand; si $C_0 = \emptyset$, on conviendra que $n = m = 0$; sinon, on note qu'on aura toujours $n \neq 0$, et aussi $m = 0$ car le rang d'un but ne vaut jamais 0, sinon il serait dans $T_P^0(\emptyset) = \emptyset$.) Il y a bien d'autres façons de faire cette récurrence, et chaque mesure selon laquelle on fait une récurrence mènera à une stratégie de résolution différente.

Cas de base $n = m = 0$, donc C_0 est vide, et le résultat est trivial : on prend $\rho'_0 \stackrel{\text{def}}{=} \rho_0$. Sinon, soit $?B$ un but tel que $B\rho$ est de rang maximal m dans C_0 . Soit $C \stackrel{\text{def}}{=} C_0 \setminus \{?B\}$. Alors : (i) il existe un renommage $A\sigma_1 :- A_1\sigma_1, A_2\sigma_1, \dots, A_n\sigma_1$, loin

non seulement de B mais même de tous les buts de C_0 , d'une clause définie $A :- A_1, A_2, \dots, A_n$. dans P telle que $B \doteq A\sigma_1$ soit unifiable; (ii) en posant $\theta_1 = \text{mgu}(B \doteq A\sigma_1)$, ρ_0 est une instance de θ_1 , donc s'écrit $\theta_1\rho_1$ pour une certaine substitution ρ_1 ; (iii) $A_1\sigma_1\theta_1\rho_1, \dots, A_n\sigma_1\theta_1\rho_1$ sont tous dans $T_P^{m-1}(\emptyset)$ (et $m \geq 1$). La différence avec la question **Question 3** est le (iii), où l'on demande à être dans $T_P^{m-1}(\emptyset)$ plutôt que dans $\text{lfp}(T_P)$, ce qui est plus précis; et que de plus on demande à $A :- A_1, A_2, \dots, A_n$. d'être un renommage loin de B d'une clause de P , plutôt qu'une clause de P directement.

Alors $C_0 \xrightarrow{\theta_1} C_1 \stackrel{\text{def}}{=} C\theta_1 \cup \{?A_1\sigma_1\theta_1, \dots, ?A_n\sigma_1\theta_1\}$. Comme $\theta_1\rho_1 = \rho_0$, on a $C_1\rho_1 = C\rho_0 \cup \{?A_1\sigma_1\theta_1\rho_1, \dots, ?A_n\sigma_1\theta_1\rho_1\}$, où les n derniers buts sont de rang au plus $m-1$, et $C\rho_0$ a au moins un but de rang m de moins que $C_0\rho_0$; et s'il n'en a aucun, alors le rang maximal de $C_1\rho_1$ est d'au plus $m-1$. On peut donc appliquer l'hypothèse de récurrence, et trouver un nombre fini d'étapes $C_1 \xrightarrow{\theta_2} C_2 \xrightarrow{\theta_3} \dots \xrightarrow{\theta_m} C_m = \emptyset$ et une substitution ρ'_0 telles que $\rho_1 = \theta_2 \dots \theta_m \rho'_0$. On conclut en utilisant le fait que $\theta_1\rho_1 = \rho_0$.

2 Boules formelles

Le but de cette section est de montrer que les dcpos interviennent naturellement en mathématiques, pas seulement en informatique. Soit X un espace métrique, dont la distance sera notée d . Autrement dit, d est une fonction de X^2 dans \mathbb{R}_+ telle que, pour tous $x, y, z \in X$:

- $d(x, y) = 0$ si et seulement si $x = y$;
- $d(x, y) = d(y, x)$;
- $d(x, z) \leq d(x, y) + d(y, z)$ (inégalité triangulaire).

Il se trouve que les notions suivantes ne sont plus au programme des classes préparatoires, définissons-les donc. Soit $(x_n)_{n \in \mathbb{N}}$ une suite de points dans X . On dit qu'un point x_∞ de X est une *limite* de cette suite si et seulement si pour tout $\epsilon > 0$, il existe un $n_0 \in \mathbb{N}$ tel que pour tout $n \geq n_0$, $d(x_n, x_\infty) \leq \epsilon$. (On dira, pour abrégé : « pour tout $\epsilon > 0$, pour tout n assez grand, $d(x_n, x_\infty) \leq \epsilon$ ».) La limite, si elle existe, est alors unique, et on dit aussi que la suite *converge* vers sa limite ou *est convergente*. La suite est *de Cauchy* si et seulement si pour tout $\epsilon > 0$, il existe un $n_0 \in \mathbb{N}$ tel que pour tous $i, j \geq n_0$, $d(x_i, x_j) \leq \epsilon$. Toute suite convergente est de Cauchy. Un espace dans lequel toute suite de Cauchy est convergente et appelé un espace métrique *complet*. \mathbb{R} , muni de sa distance usuelle, est un espace métrique complet; \mathbb{Q} , en revanche, non.

Passons à notre sujet. Au lieu de vous faire démontrer la totalité des résultats, je vous demanderai d'en démontrer une partie, et je vous donnerai une idée des arguments manquants.

Une *boule formelle* est un couple (x, r) où $x \in X$ et $r \in \mathbb{R}_+$. On peut imaginer qu'il s'agisse de la spécification de la boule fermée de centre x et de rayon r , mais l'analogie, quoiqu'utile, aura ses limites.

On pose $\mathbf{B}(X)$ l'ensemble de toutes les boules formelles, et on définit la relation \sqsubseteq par $(x, r) \sqsubseteq (y, s)$ si et seulement si $d(x, y) \leq r - s$. (On notera au passage que ceci implique $r \geq s$.) Il s'agit toujours d'une relation d'ordre. Cela ne saute pas forcément aux yeux, et je vous incite à vous familiariser avec cette notion en démontrant que \sqsubseteq est transitive d'abord, antisymétrique ensuite.

Question 7 Soit D une famille dirigée de boules formelles. On pose $r_\infty \stackrel{\text{def}}{=} \inf\{r \mid (x, r) \in D\}$. Justifier les affirmations suivantes :

- (a) Pour tout $n \in \mathbb{N}$, il existe une boule formelle (x'_n, r'_n) dans D telle que $r'_n \leq r_\infty + 1/2^n$.
- (b) On peut trouver une suite croissante d'éléments (x_n, r_n) de D tels que $r_n \leq r_\infty + 1/2^n$ pour tout $n \in \mathbb{N}$.
- (c) Les majorants (y, s) de D sont exactement les majorants de la suite $\{(x_n, r_n) \mid n \in \mathbb{N}\}$.

(a) L'ordre sur \mathbb{R}_+ est total. Si (a) échouait, il existerait un $n \in \mathbb{N}$ tel que pour tout $(x, r) \in D$, $r > r_\infty + 1/2^n$. Alors l'inf de ces r vaudrait au moins $r_\infty + 1/2^n$, ce qui contredirait la définition de r_∞ .

(b) On la construit par récurrence sur n . Pour $n = 0$, on prend $x_0 \stackrel{\text{def}}{=} x'_0$, $r_0 \stackrel{\text{def}}{=} r'_0$. Dans le cas de récurrence, on dispose de (x_{n-1}, r_{n-1}) par hypothèse de récurrence et de (x'_n, r'_n) par (a). Comme D est dirigée, il existe un élément (x_n, r_n) de D plus grand ou égal à ces deux derniers. En particulier, $(x_{n-1}, r_{n-1}) \sqsubseteq (x_n, r_n)$, ce qui assurera la croissance; et $(x'_n, r'_n) \sqsubseteq (x_n, r_n)$, ce qui implique $r_n \leq r'_n \leq r_\infty + 1/2^n$.

(c) Tout majorant de D est aussi un majorant de la suite, car cette suite est incluse dans D . Réciproquement, soit (y, s) un majorant de la suite : $(x_n, r_n) \sqsubseteq (y, s)$, c'est-à-dire $d(x_n, y) \leq r_n - s$ pour tout $n \in \mathbb{N}$.

Soit $(x, r) \in D$. Comme D est dirigée, (x, r) et (x_n, r_n) ont un majorant (z_n, t_n) dans D . Donc $d(x, z_n) \leq r - t_n$ et $d(x_n, z_n) \leq r_n - t_n$.

Par l'inégalité triangulaire, $d(x, y) \leq d(x, z_n) + d(z_n, x_n) + d(x_n, y) \leq (r - t_n) + (r_n - t_n) + (r_n - s) = r + 2r_n - 2t_n - s$.

Mais comme $d(x_n, z_n) \leq r_n - t_n$, on a $r_n \geq t_n$. On a aussi $r_n \leq r_\infty + 1/2^n$ par définition de la suite, et aussi $t_n \geq r_\infty$ par définition de r_∞ . Donc $r_\infty \leq t_n, r_n \leq r_\infty + 1/2^n$. On en déduit que $d(x, y) \leq r - s + 2/2^n$.

Ceci étant vrai pour tout $n \in \mathbb{N}$, $d(x, y) \leq r - s$, donc $(x, r) \sqsubseteq (y, s)$.

On aura besoin du fait suivant, que vous n'aurez pas à démontrer. Vous pouvez, et devez, le citer explicitement à tout moment où il vous sera utile. De même pour les autres faits qui seront énoncés plus loin.

Fait 1 Soit X un espace métrique, de distance d . Pour toute suite croissante (x_n, r_n) , $n \in \mathbb{N}$, dans $\mathbf{B}(X)$, $(x_n)_{n \in \mathbb{N}}$ est une suite de Cauchy dans X .

Démonstration. Soit $r_\infty \stackrel{\text{def}}{=} \inf_{n \in \mathbb{N}} r_n$. La suite $(r_n)_{n \in \mathbb{N}}$ est décroissante. Fixons $\epsilon > 0$. On a alors $r_n \leq r_\infty + \epsilon$ pour n assez grand, disons $n \geq n_0$. Pour tous $i, j \geq n_0$, disons $i \leq j$ par symétrie, on a donc $(x_i, r_i) \sqsubseteq (x_j, r_j)$ donc $d(x_i, x_j) \leq r_i - r_j \leq r_i - r_\infty \leq \epsilon$. \square

Question 8 Montrer que pour toute suite croissante (x_n, r_n) , $n \in \mathbb{N}$, dans $\mathbf{B}(X)$, si $(x_n)_{n \in \mathbb{N}}$ converge vers un point x_∞ de X , alors (x_∞, r_∞) est la borne supérieure de la famille $(x_n, r_n)_{n \in \mathbb{N}}$ dans $\mathbf{B}(X)$, où $r_\infty \stackrel{\text{def}}{=} \inf_{n \in \mathbb{N}} r_n$.

- Majorant. On doit montrer que pour tout $n \in \mathbb{N}$, $d(x_n, x_\infty) \leq r_n - r_\infty$. Or $d(x_n, x_m) \leq r_n - r_m$ pour tout $m \geq n$. Pour tout $\epsilon > 0$, on peut choisir m suffisamment grand de sorte que $d(x_m, x_\infty) \leq \epsilon$, par définition de x_∞ comme

limite des x_m . Par l'inégalité triangulaire, on a donc que pour m suffisamment grand, $d(x_n, x_\infty) \leq d(x_n, x_m) + d(x_m, x_\infty) \leq r_n - r_m + \epsilon \leq r_n - r_\infty + \epsilon$ (car $r_m \geq r_\infty$). Comme $\epsilon > 0$ est arbitraire, on obtient que $d(x_n, x_\infty) \leq r_n - r_\infty$, donc $(x_n, r_n) \sqsubseteq (x_\infty, r_\infty)$.

- Le plus petit. Soit (y, s) un autre majorant de $(x_n, r_n)_{n \in \mathbb{N}}$, c'est-à-dire $d(x_n, y) \leq r_n - s$ pour tout $n \in \mathbb{N}$. On souhaite démontrer que $(x_\infty, r_\infty) \sqsubseteq (y, s)$, c'est-à-dire que $d(x_\infty, y) \leq r_\infty - s$. Par l'inégalité triangulaire, $d(x_\infty, y) \leq d(x_\infty, x_n) + d(x_n, y) \leq d(x_\infty, x_n) + r_n - s$. Pour tout $\epsilon > 0$, par définition de x_∞ comme limite, on aura $d(x_\infty, x_n) \leq \epsilon$ pour tout n assez grand. On aura aussi $r_n \leq r_\infty + \epsilon$ dès que n sera assez grand. Donc, pour n assez grand, $d(x_\infty, y) \leq r_\infty - s + 2\epsilon$. Comme $\epsilon > 0$ est arbitraire, $d(x_\infty, y) \leq r_\infty - s$, cqfd.

Voici deux nouveaux faits utiles, dont je vous donne aussi les démonstrations.

Fait 2 Soit X un espace métrique, de distance d . De toute suite de Cauchy $(x_n)_{n \in \mathbb{N}}$ dans X on peut extraire une sous-suite $(x_{n_k})_{k \in \mathbb{N}}$ (i.e., $n_0 < n_1 < \dots < n_k < \dots$) telle que $(x_{n_k}, 1/2^k)_{k \in \mathbb{N}}$ soit une famille dirigée, et en fait une suite croissante, dans $\mathbf{B}(X)$.

Démonstration. On construit n_k par récurrence sur k . Comme $(x_n)_{n \in \mathbb{N}}$ est de Cauchy, il existe un entier n_0 tel que pour tous $i, j \geq n_0$, $d(x_i, x_j) \leq 1/2^1$.

Il existe ensuite un entier n_1 tel que pour tous $i, j \geq n_1$, $d(x_i, x_j) \leq 1/2^2$, et on peut choisir $n_1 > n_0$.

De proche en proche (c'est-à-dire, formellement, par une récurrence sur k), on trouve $n_k > n_{k-1}, \dots, n_0$ tel que pour tous $i, j \geq n_k$, $d(x_i, x_j) \leq 1/2^{k+1}$.

En particulier, pour tout $k \geq 1$, $d(x_{n_{k-1}}, x_{n_k}) \leq 1/2^k$. Or $1/2^k = 1/2^{k-1} - 1/2^k$, donc $(x_{n_{k-1}}, 1/2^{k-1}) \sqsubseteq (x_{n_k}, 1/2^k)$. \square .

Fait 3 Soit X un espace métrique, de distance d . Pour toute suite de Cauchy $(x_n)_{n \in \mathbb{N}}$ dans X , s'il en existe une sous-suite $(x_{n_k})_{k \in \mathbb{N}}$ qui converge vers une limite x_∞ , alors $(x_n)_{n \in \mathbb{N}}$ elle-même converge vers x_∞ .

Démonstration. Pour tout $\epsilon > 0$, en utilisant que $(x_n)_{n \in \mathbb{N}}$ est de Cauchy, on a $d(x_n, x_m) \leq \epsilon/2$ pour tous n, m assez grands, disons plus grands que n_0 . Comme $(x_{n_k})_{k \in \mathbb{N}}$ converge vers x_∞ , on a aussi $d(x_{n_k}, x_\infty) \leq \epsilon/2$ pour k assez grand, disons plus grand que k_0 . On choisit un tel k plus grand que k_0 de sorte que n_k soit plus grand que n_0 . En posant $m \stackrel{\text{def}}{=} n_k$, pour tout n plus grand que n_0 , on a alors $d(x_n, x_\infty) \leq d(x_n, x_{n_k}) + d(x_{n_k}, x_\infty) \leq \epsilon/2 + \epsilon/2 = \epsilon$. \square

Question 9 Montrer que si $(x_n, r_n)_{n \in \mathbb{N}}$ est une suite croissante dans $\mathbf{B}(X)$ et si $\inf_{n \in \mathbb{N}} r_n = 0$, alors la famille $(x_n, r_n)_{n \in \mathbb{N}}$ a au plus un majorant ; que s'il existe, il est de la forme $(x_\infty, 0)$, et que x_∞ est alors une (la) limite de $(x_n)_{n \in \mathbb{N}}$ dans X .

Soit (x_∞, r_∞) un majorant de cette famille. Comme $(x_n, r_n) \sqsubseteq (x_\infty, r_\infty)$ pour tout $n \in \mathbb{N}$, en particulier $r_n \geq r_\infty$ pour tout $n \in \mathbb{N}$, donc $r_\infty = 0$, en prenant l'inf sur n . Si x_∞ n'est pas une limite de $(x_n)_{n \in \mathbb{N}}$ dans X , par définition il existe un $\epsilon > 0$ tel que pour tout $n \in \mathbb{N}$, il existe $m \geq n$ tel que $d(x_m, x_\infty) > \epsilon$. Comme $\inf_{n \in \mathbb{N}} r_n = 0$, on peut choisir n suffisamment grand de sorte que $r_n < \epsilon$, et alors $r_m \leq r_n < \epsilon$ pour tout $m \geq n$. On en déduit que $d(x_m, x_\infty) > r_m$, donc que (x_m, r_m) n'est pas inférieur ou égal à $(x_\infty, 0)$: contradiction.

Question 10 En déduire que $\mathbf{B}(X)$ est un dcpo si et seulement si X est un espace métrique complet.

Si X est complet, soit D une famille dirigée de $\mathbf{B}(X, d)$. On construit la sous-suite croissante (x_n, r_n) comme à la **Question 7**. Par le **Fait 1**, $(x_n)_{n \in \mathbb{N}}$ est une suite de Cauchy, et a donc une limite x_∞ . La **Question 8** nous permet d'affirmer que (x_∞, r_∞) est le plus petit des majorants de $\{(x_n, r_n) \mid n \in \mathbb{N}\}$, et donc aussi de D , puisque les deux familles ont les mêmes majorants par la **Question 7 (c)**.

Réciproquement, si $\mathbf{B}(X)$ est un dcpo, on considère une suite de Cauchy $(x_n)_{n \in \mathbb{N}}$ quelconque dans X . Par le **Fait 2**, elle a une sous-suite $(x_{n_k})_{k \in \mathbb{N}}$ telle que $(x_{n_k}, 1/2^k)_{k \in \mathbb{N}}$ soit une famille dirigée dans $\mathbf{B}(X)$. Cette famille a donc une borne supérieure (x_∞, r_∞) . Par la **Question 9**, $r_\infty = 0$ et x_∞ est la limite de $(x_{n_k})_{k \in \mathbb{N}}$ dans X .

Par le **Fait 1**, $(x_{n_k})_{k \in \mathbb{N}}$ est de Cauchy. Ceci nous permet d'utiliser le **Fait 3**, et de conclure que x_∞ est aussi la limite de $(x_n)_{n \in \mathbb{N}}$.

Donc X est complet.

De cela, on peut déduire des théorèmes de point fixe intéressants. Par exemple, si X est un espace métrique complet et f est une fonction α -lipschitzienne de X dans X (i.e., $d(f(x), f(y)) \leq \alpha \cdot d(x, y)$ pour tous $x, y \in X$) avec $0 \leq \alpha < 1$, on peut vérifier que la fonction $\mathbf{B}_\alpha f: \mathbf{B}(X) \rightarrow \mathbf{B}(X)$ qui à (x, r) associe $(f(x), \alpha r)$ est Scott-continue. Si x est n'importe quel point de X , en posant $r \stackrel{\text{def}}{=} d(x, f(x))/(1 - \alpha)$, on peut vérifier que la suite des points $(\mathbf{B}_\alpha f)^n(x, r)$, $n \in \mathbb{N}$, est croissante dans $\mathbf{B}(X)$. Par la **Question 10**, elle aura une borne supérieure, qui est nécessairement un point fixe de $\mathbf{B}_\alpha f$. Or les seuls points fixes de $\mathbf{B}_\alpha f$ sont les boules formelles de la forme $(x, 0)$ où x est un point fixe de f . On retrouve ainsi le théorème du point fixe de Banach... par une démonstration bien plus compliquée que la démonstration usuelle.

Voici un théorème beaucoup plus fin. On aura besoin du *théorème de Bourbaki-Witt*, que certains d'entre vous ont vu en cours de mathématiques discrètes. Il énonce que, pour tout ensemble ordonné inductif P (par exemple, un dcpo), pour toute fonction $f: P \rightarrow P$ inflationnaire (c'est-à-dire telle que $p \leq f(p)$ pour tout $p \in P$; f n'est pas nécessairement croissante), pour tout $p_0 \in P$, f a un point fixe p tel que $p_0 \leq p$.

Un *potentiel* sur X est une fonction $\pi: X \rightarrow \mathbb{R}_+$ semi-continue inférieurement, c'est-à-dire telle que pour toute suite $(x_n)_{n \in \mathbb{N}}$ qui a une limite x_∞ dans X , pour tout $\epsilon > 0$, on a $\pi(x_n) \geq \pi(x_\infty) - \epsilon$ pour tout n assez grand.

Question 11 Soit X un espace métrique complet non vide, $f: X \rightarrow X$ une fonction quelconque (pas nécessairement lipschitzienne, continue, ou rien) de X dans X , et π un potentiel tel que pour tout $x \in X$, $d(x, f(x)) \leq \pi(x) - \pi(f(x))$. Montrer qu'alors f a un point fixe. C'est le *théorème de Caristi*. À titre d'indication, montrer que $Z \stackrel{\text{def}}{=} \{(x, r) \in \mathbf{B}(X) \mid r \geq \pi(x)\}$ est un dcpo dans l'ordre \sqsubseteq . Si vous ne voyez pas à quoi ça sert, vous avez peut-être raté un point subtil de la démonstration. Vous devriez être capable de montrer que pour tout point x_0 de X , il existe même un tel point fixe de f à distance au plus $\pi(x_0)$ de x_0 .

On montre l'indication. Soit D une famille dirigée dans Z . Par la **Question 7**, il existe une suite croissante d'éléments (x_n, r_n) de D qui a les mêmes majorants, donc le même sup. Ce sup (x_∞, r_∞) existe dans $\mathbf{B}(X)$, par la **Question 10**. De plus, r_∞ est l'inf des rayons des boules formelles de D et x_∞ est la limite de $(x_n)_{n \in \mathbb{N}}$. Si (x_∞, r_∞) n'était pas dans Z , on aurait $r_\infty < \pi(x_\infty)$. Posons $\epsilon > 0$ inférieur à

$1/2(\pi(x_\infty) - r_\infty)$. Par semi-continuité inférieure, on aurait $\pi(x_n) \geq \pi(x_\infty) - \epsilon$ pour n assez grand, donc $r_n \geq \pi(x_n) \geq \pi(x_\infty) - \epsilon > r_\infty + \epsilon$, pour tout n assez grand. Mais ceci impliquerait que $\inf_{n \in \mathbb{N}} r_n$ (qui vaut r_∞) serait supérieur ou égal à $r_\infty + \epsilon$, ce qui est impossible.

Ceci démontre que le supremum (x_∞, r_∞) de D dans $\mathbf{B}(X)$ est dans Z , mais il faut encore arguer du fait qu'il s'agit du supremum de D dans Z , autrement dit du plus petit des majorants de D dans Z . C'est un majorant de D dans Z , car l'ordre sur Z est \sqsubseteq , restreint à Z . Pour tout majorant (y, s) de D dans Z , (y, s) est aussi un majorant de D dans $\mathbf{B}(X)$, donc $(x_\infty, r_\infty) \sqsubseteq (y, s)$, et l'on conclut. (Plus généralement, si P est un dcpo et Q est un sous-ensemble de P clos par suprema pris dans P , alors Q est un dcpo. Mais il se peut que Q soit un dcpo sans que Q soit clos par les suprema pris dans P . Par exemple, si $P = \mathbb{P}(\mathbb{R})$ ordonné par inclusion et Q est l'ensemble des fermés de \mathbb{R} , aussi ordonné par inclusion, Q est un dcpo, et même un treillis complet, dans lequel le sup est l'adhérence de l'union, qui ne coïncide que rarement avec l'union.)

Pour tout $(x, r) \in Z$, posons $f'(x, r) \stackrel{\text{def}}{=} (f(x), r - \pi(x) + \pi(f(x)))$. La raison d'être de Z est que $f'(x, r)$ soit bien une boule formelle, autrement dit que $r - \pi(x) + \pi(f(x)) \geq 0$: et en effet, comme (x, r) est dans Z , $r - \pi(x) \geq 0$. En fait, $f'(x, r)$ est même dans Z , ce qui sera conséquence du fait que f' est inflationnaire sur Z (paragraphe suivant), ou directement : $r - \pi(x) + \pi(f(x)) \geq \pi(f(x))$ car $r - \pi(x) \geq 0$, puisque (x, r) est dans Z .

On montre que f' est inflationnaire sur Z , et pour cela on doit montrer que pour tout $(x, r) \in Z$, $(x, r) \sqsubseteq (f'(x, r))$, c'est-à-dire $d(x, f(x)) \leq \pi(x) - \pi(f(x)) \dots$ et c'est justement l'hypothèse qui est faite.

Par le théorème de Bourbaki-Witt, f' a un point fixe dans Z . En fait, au-dessus de chaque point (x_0, r_0) de Z (qui existe car X est non vide), f' a un point fixe (x, r) . Dire que c'est un point fixe revient à dire que $f(x) = x$ (et $r - \pi(x) + \pi(f(x)) = r$, ce qui est automatique), ce qui nous permet de conclure.

En fait, nous avons montré un résultat plus fort : (x, r) est plus grand ou égal à (x_0, r_0) , c'est-à-dire que $d(x_0, x) \leq r_0 - r$. En particulier, $d(x_0, x) \leq r_0$. Or x_0 est arbitraire dans X , et r_0 est arbitraire parmi les réels positifs ou nuls tels que $r_0 \geq \pi(x_0)$. On a donc montré que pour tout point x_0 de Z , f a un point fixe x qui est à distance au plus $\pi(x_0)$ de x_0 .

On pouvait aussi définir $f'(x, r)$ comme $(f(x), \pi(f(x)))$. Comme π est à valeur dans \mathbb{R}_+ , c'est bien un élément de $\mathbf{B}(X)$. De plus, il est dans Z , trivialement, et ce même si (x, r) n'est pas dans Z . On montre que cette nouvelle fonction f' est inflationnaire sur Z , c'est-à-dire que $(x, r) \sqsubseteq (f'(x, r))$ pour tout $(x, r) \in Z$: ceci revient à vérifier que $d(x, f(x)) \leq r - \pi(f(x))$ lorsque $r \geq \pi(x)$; mais $d(x, f(x)) \leq \pi(x) - \pi(f(x))$ (par hypothèse) $\leq r - \pi(f(x))$.