1 Forme générale d'une définition d'ensemble par induction (d'une définition inductive d'ensemble).

On suppose donnés des ensembles pré-existants $B_1, \ldots, B_t$.

Une définition inductive est donnée par un ensemble de <u>*constructeurs*</u> $c_1, \ldots, c_k$.

À chaque c_i est associé un tuple $(a^i_1, \ldots, a^i_{n_i})$ d'*arguments*, avec, pour chaque j, soit $a^i_j = B_{m_{i,j}}$ (avec $1 \leq m_{i,j} \leq t$), soit $a^i_j = \textbf{rec}$.

rec est un "mot réservé", qui désigne les endroits où la définition est récursive.

Exemple, notations : définition inductive de `com`.

- ensembles pré-existants : $B_1 = \mathcal{V}$, $B_2 =$ `aexpr`, ensemble des expressions arithmétiques, $B_3 =$ `bexpr`, ensemble des expressions booléennes.

- constructeurs, avec leurs arguments :

		nom usuel du constructeur
c_1	(B_1, B_2)	`assgn`
c_2	$(\textbf{rec}, \textbf{rec})$	`seq`
c_3	$(B_3, \textbf{rec}, \textbf{rec})$	`ifte`
c_4	$(B_3, \textbf{rec})$	`while`
c_5	$\emptyset$	`skip`

Rq : les constructeurs $c_1, \ldots, c_k$ sont souvent associés à une grammaire (comme pour la définition de la syntaxe de Imp vue en cours).

Les constructeurs $c_1, \ldots, c_k$ déterminent une fonction $f_{c_1,\ldots,c_k}$, que l'on va noter simplement f, définie par

$$f(A) = \bigcup_{1\leq i\leq k} \left\{ c_i(u_1, \ldots, u_{n_i}),\ \text{avec} \quad \begin{array}{l} u_j \in B_{m_{i,j}} \text{ si } a^i_j = B_{m_{i,j}} \\ u_j \in A \text{ si } a^i_j = \textbf{rec} \end{array} \right\}$$

Lemme : f est une fonction croissante.
Preuve. Laissée en exercice.

On peut alors appliquer le théorème de Knaster-Tarski, qui nous fournit deux choses :

1. L'existence du plus petit point fixe de f, que l'on appelle généralement l'ensemble défini inductivement par les $c_1, \ldots, c_k$.

   Notons cet ensemble E.

2. Le principe de preuve par induction (structurelle) sur E, pour prouver un énoncé de la forme

$$\forall x \in E, P(x)$$

   (on dit que P est un *prédicat* sur E).

Faire une preuve par induction structurelle sur $x \in E$ revient à appliquer Knaster-Tarski, et à montrer $f(A) \subseteq A$, où $A = \{x \in E, P(x) \text{ est vrai}\}$ (alors on saura que A est un pré-point fixe de f, donc, par Knaster-Tarski, que $E \subseteq A$, et ainsi $E = A$, puisque $A \subseteq E$).

Explicitons ce que signifie montrer $f(A) \subseteq A$: on doit établir $\forall i = 1, \ldots, k.\, F_i$, où F_i est une propriété qui exprime que l'appartenance à A est préservée par le constructeur c_i.

Plus précisément,

$$F_i = \forall x_1 \in a^i_1, \forall x_2 \in a^i_2, \ldots, \forall x_{n_i} \in a^i_{n_i}, \left(H^i_1 \wedge \cdots \wedge H^i_{n_i}\right) \Rightarrow P(c_i(x_1, \ldots, x_{n_i}))$$

où $H^i_j = P(x_j)$ si $a^i_j = \textbf{rec}$, et $H^i_j = \top$ (la formule "vrai") sinon.

Intuitivement, on a le droit de supposer $P(x_j)$ pour tous les arguments tels que $a^i_j = \mathbf{rec}$.
Retour sur l'exemple. Le principe d'induction associé à la définition des commandes est le suivant : pour montrer $\forall x \in \mathtt{com}, P(x)$, on doit établir

$$\begin{array}{ll}
\underbrace{(\forall x_1 \in B_1, \forall x_2 \in B_2, P(c_1(x_1,x_2)))}_{F_1} & \texttt{(assgn)} \\
\wedge \quad \underbrace{(\forall x_1 \in \mathtt{com}, \forall x_2 \in \mathtt{com}, (P(x_1) \wedge P(x_2)) \Rightarrow P(c_2(x_1,x_2)))}_{F_2} & \texttt{(seq)} \\
\wedge \quad \underbrace{(\forall x_1 \in B_3, \forall x_2 \in \mathtt{com}, \forall x_3 \in \mathtt{com}, (P(x_2) \wedge P(x_3)) \Rightarrow P(c_3(x_1,x_2,x_3)))}_{F_3} & \texttt{(ite)} \\
\wedge \quad \underbrace{\forall x_1 \in B_3, \forall x_2 \in \mathtt{com}, P(x_2) \Rightarrow P(c_4(x_1,x_2))}_{F_4} & \texttt{(while)} \\
\wedge \quad \underbrace{P(c_5)}_{F_5} & \texttt{(skip)}
\end{array}$$

NB : ci-dessus, on a simplifié les $\top \wedge \mathcal{F}$ en $\mathcal{F}$, et $\top \Rightarrow \mathcal{F}$ en $\mathcal{F}$.

Une fois établie la conjonction des 5 propriétés ci-dessus, on déduit, par Knaster-Tarski, $\forall x \in \mathtt{com}, P(x)$.

2 Définitions inductives de relations

NB : on parle ici de *relations*, ou de *prédicats*, n-aires.
Encore plus que pour la partie précédente, les notes qui sont présentées proposent une description du cas général pour le traitement des définitions et preuves par induction, mais tout n'est pas complètement formalisé. Ceci afin de préserver un minimum de lisibilité, tout en essayant de faire passer les idées générales.
On se donne

- des ensembles préexistants $B_1, \ldots, B_t$
- des prédicats (inductifs) préexistants $\pi_1, \ldots, \pi_p$
  Chaque π_h porte sur un tuple dans $B_{j^h_1} \times \cdots \times B_{j^h_{q_h}}$.

On définit par induction un nouveau prédicat $\boldsymbol{\rho}$, portant sur un tuple dans $B_{i_1} \times \cdots \times B_{i_n}$, en se donnant k règles d'inférence $\mathrm{r}_1, \ldots, \mathrm{r}_\mathrm{k}$.

Pour $1 \leq i \leq k$, la règle $\mathrm{r_i}$

(*nota:* "tout" devrait dépendre de i ci-dessous, on omet cette dépendance pour ne pas trop alourdir)

- a pour metavariables $\{z_1, \ldots, z_w\}$
- est de la forme $\dfrac{H_1 \cdots H_m}{C}\ SC$, avec
  - C est la conclusion, de la forme $\boldsymbol{\rho}(t_1, \ldots, t_n)$, où les t_j peuvent dépendre des $z_1, \ldots, z_w$
  - SC est une condition d'application ("side condition"), éventuellement vide, ne mentionnant ni $\boldsymbol{\rho}$ ni les π_h
  - chaque H_ℓ est une prémisse (ou *hypothèse*) pouvant être
    * soit de la forme $\boldsymbol{\rho}(u_1, \ldots, u_n)$, les u_j pouvant dépendre des $z_1, \ldots, z_w$
    * soit de la forme $\pi_{h_\ell}(u_1, \ldots, u_{q_{h_\ell}})$, les u_j pouvant dépendre des $z_1, \ldots, z_w$

Fonction croissante associée. Aux $\mathrm{r}_1, \ldots, \mathrm{r}_\mathrm{k}$ est associée une fonction f : si A est un ensemble de dérivations dont la conclusion est de la forme $\boldsymbol{\rho}(t_1, \ldots, t_n)$, avec $t_j \in B_{i_j}$, alors $f(A) = f_1(A) \cup \cdots \cup f_k(A)$, chaque f_i étant associée à r_i de la manière suivante :

$$f_i(A) = \left\{ \frac{\delta_1 \cdots \delta_m}{\boldsymbol{\rho}(t_1, \ldots, t_n)}, SC \text{ est vérifiée} \right\} \ ,$$

avec la convention que $\delta_\ell : \boldsymbol{\rho}(u_1, \ldots, u_n) \in A$ lorsque H_ℓ est de la forme $\boldsymbol{\rho}(u_1, \ldots, u_n)$, et δ_ℓ est une dérivation de $\pi_{h_\ell}(u_1, \ldots, u_{q_h})$ sinon.

On remarque que f est croissante.

NB : aucune prémisse n'est de la forme $\neg\boldsymbol{\rho}(\ldots)$. Sinon, f ne serait pas croissante.

La fonction f induit, par Knaster-Tarski, son plus petit point fixe, qui est un ensemble de dérivations dont la conclusion est de la forme $\boldsymbol{\rho}(t_1, \ldots, t_n)$. On a pour habitude de noter simplement $\boldsymbol{\rho}(t_1, \ldots, t_n)$ pour dire qu'il existe une dérivation de ce jugement dans l'ensemble qu'on vient de définir.

Preuve par induction sur la dérivation. Supposons que l'on veuille montrer une propriété de la forme

$$\forall y_1, \ldots, y_n.\ \boldsymbol{\rho}(y_1, \ldots, y_n) \implies P(y_1, \ldots, y_n) \ .$$

On peut appliquer Knaster-Tarski, et montrer que $f(A) \subseteq A$, où

$$A \quad = \quad \{(s_1, \ldots, s_n).\ \boldsymbol{\rho}(s_1, \ldots, s_n) \wedge P(s_1, \ldots, s_n)\} \ .$$

Pour ce faire, il y a autant de cas à traiter que de règles d'inférence. Dans le cas de la règle r_i,

- on se donne les metavariables $z_1, \ldots, z_w$
- on suppose SC
- on suppose $\pi_{h_\ell}(u_1, \ldots, u_{q_{h_\ell}})$ pour toutes les prémisses H_ℓ ayant cette forme
- on suppose $\boldsymbol{\rho}(u_1, \ldots, u_n) \wedge P(u_1, \ldots, u_n)$ pour toutes les prémisses de la forme $\boldsymbol{\rho}(\ldots)$

…et on doit montrer $P(t_1, \ldots, t_n)$ (la conclusion de la règle r_i).

NB : on devrait en principe démontrer $\boldsymbol{\rho}(t_1, \ldots, t_n) \wedge P(t_1, \ldots, t_n)$, mais la première partie de cette conjonction découle directement par application de r_i.