Annexe G

Corrigés des exercices du chapitre 8

Exercice 8.1

Proposition G.1 (Réflexivité) *Pour tous environnements E et types de modules M, on a $E \vdash M <: M$.*

Démonstration: par récurrence structurelle sur le type M.

Cas $M = \texttt{sig}\ S_1; \ldots; S_n\ \texttt{end}$. On cherche à obtenir le résultat désiré en appliquant la règle (sub-sig) avec comme injection ρ l'identité. Il suffit donc de montrer

$$E;\ S_1;\ \ldots;\ S_n \vdash S_i <: S_i \tag{1}$$

pour tout $i = 1, \ldots, n$.

Si $S_i = (\texttt{val}\ v : \sigma)$, on a $E;\ S_1;\ \ldots;\ S_n \vdash \sigma \approx \sigma$ (axiome de transitivité sur $\approx$ plus règle (schémas)), d'où (1) par application de la règle (sub-val).

Si $S_i = (\texttt{type}\ t)$, (1) s'ensuit de la règle (sub-abstr-abstr).

Si $S_i = (\texttt{type}\ t = \tau)$, on a $E;\ S_1;\ \ldots;\ S_n \vdash \tau \approx \tau$ par la règle (eq-réflexivité), d'où (1) par la règle (sub-mani-mani).

Si $S_i = (\texttt{module}\ X : M_1)$, on a $E;\ S_1;\ \ldots;\ S_n \vdash M_1 <: M_1$ par application de l'hypothèse de récurrence (M_1 est un sous-terme strict de M). Utilisant la règle (sub-mod), on conclut (1).

D'où le résultat attendu, $E \vdash M <: M$, par application de la règle (8).

Cas $M = \texttt{functor}(X : M_1) \to M_2$. En appliquant l'hypothèse de récurrence à M_1, on obtient

$$E \vdash M_1 <: M_1$$

et en l'appliquant à M_2,

$$E;\ \texttt{module}\ X : M_1 \vdash M_2 <: M_2$$

D'où $E \vdash M <: M$ en appliquant la règle (sub-foncteur). □

Pour prouver la transitivité de $<:$, il faut introduire une relation de sous-typage entre environnements de typage. Un environnement de typage peut être vu comme l'intérieur d'une signature $\texttt{sig} \ldots \texttt{end}$: les deux sont des séquences de spécifications. On dit par conséquent que deux environnements E et A' sont en relation de sous-typage, et on note $\vdash E <: A'$, si $\emptyset \vdash \texttt{sig}\ E\ \texttt{end} <: \texttt{sig}\ A'\ \texttt{end}$; c'est-à-dire, notant $E = S_1; \ldots; S_m$ et $A' = S'_1; \ldots; S'_n$, il existe une injection ρ telle que $E \vdash S_{\rho(i)} <: S'_i$ pour tout $i = 1, \ldots, n$.

L'intérêt de cette notion est que, si $\vdash E <: E'$, tout résultat de typage qui peut être dérivé sous les hypothèses E' peut également être dérivé sous les hypothèses E (hypothèses plus fortes). Plus précisément, on a le lemme suivant :

Proposition G.2 (Sous-typage sur l'environnement) *Supposons* $\vdash E <: E'$.

1. *Si* $E' \vdash \tau \approx \tau'$, *alors* $E \vdash \tau \approx \tau'$.
2. *Si* $E' \vdash \sigma \geq \sigma'$, *alors* $E \vdash \sigma \geq \sigma'$.
3. *Si* $E' \vdash S <: S'$, *alors* $E \vdash S <: S'$.
4. *Si* $E' \vdash M <: M'$, *alors* $E \vdash M <: M'$.

Démonstration: on commence par prouver (1) par récurrence sur la dérivation de $E' \vdash \tau \approx \tau'$. Le seul cas intéressant est le cas de base correspondant à l'application de la règle (1) : $E' \vdash t \approx \tau'$ parce que E' contient l'hypothèse $\texttt{type}\ t = \tau'$. Par définition du sous-typage entre environnements, E doit forcément contenir une hypothèse S telle que $E \vdash S <: (\texttt{type}\ t = \tau')$. Il n'y a que deux possibilités : $S = (\texttt{type}\ t = \tau)$ et $E \vdash \tau \approx \tau'$, ou bien $S = (\texttt{type}\ t)$ et $E \vdash t \approx \tau'$. Le second cas nous donne directement la preuve de $E \vdash t \approx \tau'$ désirée. Dans le premier cas, on l'obtient par la dérivation suivante :

$$\dfrac{\dfrac{E = E_1;\ \texttt{type}\ t = \tau;\ E_2}{E \vdash t \approx \tau} \qquad E \vdash \tau \approx \tau'}{E \vdash t \approx \tau'}$$

On prouve ensuite (2) comme corollaire immédiat de (1), puis (3) et (4) simultanément par récurrence structurelle sur M et S. □

Proposition G.3 (Transitivité) *Si* $E \vdash M <: M'$ *et* $E \vdash M' <: M''$, *alors* $E \vdash M <: M''$.

Démonstration: par récurrence structurelle sur les types M, M', M''. Vu les règles (sub-sig) et (sub-foncteur), ces trois types sont ou bien trois signatures, ou bien trois types de foncteurs.

Cas $M = \texttt{sig}\ S_1; \ldots; S_m\ \texttt{end}$ et $M' = \texttt{sig}\ S'_1; \ldots; S'_n\ \texttt{end}$ et $M'' = \texttt{sig}\ S''_1; \ldots; S''_p\ \texttt{end}$. La seule règle ayant pu conclure $E \vdash M <: M'$ et $E \vdash M' <: M''$ est la règle (sub-sig). Ses prémisses sont donc nécessairement vraies. Il existe donc deux injections $\varphi : \{1 \ldots n\} \mapsto \{1 \ldots m\}$ et $\psi : \{1 \ldots p\} \mapsto \{1 \ldots n\}$ telles que

$$E;\ S_1;\ \ldots;\ S_m \vdash S_{\varphi(i)} <: S'_i \quad \text{pour } i = 1, \ldots, n \tag{2}$$

$$E;\ S'_1;\ \ldots;\ S'_n \vdash S'_{\psi(i)} <: S''_i \quad \text{pour } i = 1, \ldots, p \tag{3}$$

Notons $B = E;\ S_1;\ \ldots;\ S_m$ et $B' = E;\ S'_1;\ \ldots;\ S'_n$. Il est facile de voir que $\vdash B <: B'$. Par la proposition G.2, on peut donc prouver (3) sous les hypothèses B au lieu de B' :

$$E;\ S_1;\ \ldots;\ S_n \vdash S'_{\psi(i)} <: S''_i \quad \text{pour } i = 1, \ldots, p \tag{4}$$

Considérons alors $\rho = \varphi \circ \psi$. C'est une injection de $\{1 \ldots p\}$ dans $\{1 \ldots m\}$. Fixons i dans $\{1 \ldots p\}$. Par (2) et (4), nous avons

$$B \vdash S_{\rho(i)} <: S'_{\psi(i)} \qquad \text{et} \qquad B \vdash S'_{\psi(i)} <: S''_i$$

Nous montrons maintenant que $B \vdash S_{\rho(i)} <: S''_i$ en discutant sur la forme de $S_{\rho(i)}$, $S'_{\psi(i)}$ et S''_i. Les cas suivants sont à considérer :

$S_{\rho(i)}$	$S'_{\psi(i)}$	S''_i	
`val` $v : \sigma$	`val` $v : \sigma'$	`val` $v : \sigma''$	On a $B \vdash \sigma \geq \sigma'$ et $B \vdash \sigma' \geq \sigma''$, d'où $B \vdash \sigma \geq \sigma''$ car $\geq$ est transitive, et le résultat attendu par la règle (sub-val).
_	_	`type` t	Trivial par (sub-mani-abstr) ou (sub-abstr-abstr).
`type` t	`type` t	`type` $t = \tau''$	De (4) il vient $B \vdash t \approx \tau''$, d'où le résultat par la règle (sub-abstr-mani).
`type` t	`type` $t = \tau'$	`type` $t = \tau''$	De (4) il vient $B \vdash t \approx \tau'$ et $B \vdash \tau' \approx \tau''$, d'où $B \vdash t \approx \tau''$ par transitivité de $\approx$ et le résultat par la règle (sub-abstr-mani).
`type` $t = \tau$	`type` t	`type` $t = \tau''$	On a $B \vdash t \approx \tau''$, et d'autre part $B \vdash t \approx \tau$ trivialement puisque B contient l'hypothèse `type` $t = \tau$. D'où le résultat par transitivité de $\approx$ et la règle (sub-mani-mani).
`type` $t = \tau$	`type` $t = \tau'$	`type` $t = \tau''$	Transitivité de $\approx$ et règle (sub-mani-mani).
`module` $X : M_1$	`module` $X : M'_1$	`module` $X : M''_1$	On a $B \vdash M_1 <: M'_1$ et $B \vdash M'_1 <: M''_1$. Les types M_1, M'_1, M''_1 étant sous-termes stricts de M, M', M'' respectivement, on peut appliquer l'hypothèse de récurrence, obtenant $B \vdash M_1 <: M''_1$ et le résultat attendu via la règle (sub-mod).

Ayant ainsi montré $B \vdash S_{\rho(i)} <: S''_i$ pour tout $i = 1, \ldots, p$, nous pouvons conclure

$$E \vdash \texttt{sig } S_1; \ldots; S_m \texttt{ end} <: \texttt{sig } S''_1; \ldots; S''_p \texttt{ end}$$

par la règle (sub-sig) ; c'est le résultat attendu.

Cas $M = \texttt{functor}(X : P) \rightarrow Q$ et $M' = \texttt{functor}(X : P') \rightarrow Q'$ et $M'' = \texttt{functor}(X : P'') \rightarrow Q''$. La seule règle ayant pu conclure $E \vdash M <: M'$ et $E \vdash M' <: M''$ est la règle (sub-foncteur). On a donc :

$$E \vdash P' <: P \qquad E; \texttt{module } X : P' \vdash Q <: Q' \qquad E \vdash P'' <: P' \qquad E; \texttt{module } X : P'' \vdash Q' <: Q''$$

On a clairement $\vdash (E; \texttt{module } X : P'') <: (E; \texttt{module } X : P')$, d'où par la proposition G.2,

$$E; \texttt{module } X : P'' \vdash Q' <: Q''$$

Appliquant deux fois l'hypothèse de récurrence, on obtient des preuves de

$$E \vdash P'' <: P \qquad E; \texttt{module } X : P'' \vdash Q <: Q''$$

D'où le résultat attendu par application de la règle (sub-foncteur). □

Exercice 8.2 On définit le prédicat $E \vdash S_1 \approx S_2$ par les règles d'inférence suivantes :

$$\frac{\rho \text{ permutation de } \{1 \ldots n\} \qquad E; S_1; \ldots; S_n \vdash S_{\rho(i)} \approx S'_i \text{ pour } i = 1, \ldots, n}{E \vdash (\mathtt{sig}\ S_1; \ldots; S_n\ \mathtt{end}) \approx (\mathtt{sig}\ S'_1; \ldots; S'_n\ \mathtt{end})} \qquad \frac{E \vdash \sigma \approx \sigma'}{E \vdash (\mathtt{val}\ v : \sigma) \approx (\mathtt{val}\ v : \sigma')}$$

$$E \vdash (\mathtt{type}\ t) \approx (\mathtt{type}\ t) \qquad \frac{E \vdash \tau \approx t}{E \vdash (\mathtt{type}\ t = \tau) \approx (\mathtt{type}\ t)} \qquad \frac{E \vdash \tau \approx \tau'}{E \vdash (\mathtt{type}\ t = \tau) \approx (\mathtt{type}\ t = \tau')}$$

$$\frac{E \vdash \tau \approx t}{E \vdash (\mathtt{type}\ t) \approx (\mathtt{type}\ t = \tau)} \qquad \frac{E \vdash M \approx M'}{E \vdash (\mathtt{module}\ X : M) \approx (\mathtt{module}\ X : M')}$$

$$\frac{E \vdash P_1 \approx P_2 \qquad E; \mathtt{module}\ X : P_2 \vdash R_1 \approx R_2}{E \vdash (\mathtt{functor}\ (X : P_1) \to R_1) \approx (\mathtt{functor}\ (X : P_2) \to R_2)}$$

Exercice 8.3 Informellement, toute signature qui ne contient pas de spécification de type abstrait possède toujours une signature équivalente (au sens de l'exercice 8.2) dans laquelle il n'y a pas de dépendances entre les composantes. On l'obtient en expansant de manière répétée les égalités sur les types manifestes dans le reste de la signature. Par exemple, si on part de la signature

```
module type S =
  sig
    type t = int
    type u = t
    module X : sig val v : u end
  end
```

et qu'on remplace chaque utilisation de `u` par `t`, puis chaque utilisation de `t` par `int`, on obtient la signature non-dépendante équivalente

```
  sig
    type t = int
    type u = int
    module X : sig val v : int end
  end
```

D'autre part, si un chemin p a une signature M, on peut toujours lui attribuer la signature M/p (règle de renforcement), dans laquelle toute les spécifications de types sont manifestes.

En combinant les deux remarques, l'idée est donc de remplacer chaque utilisation des règles de projections non restreintes (eq-projection), (val-projection) et (mod-projection) par une étape de renforcement (mod-renforcement), une étape de sous-typage vers un type non dépendant équivalent (mod-sub), une projection restreinte (eq-projection'), (val-projection'), (mod-projection'), et enfin une étape d'équivalence de type ou de sous-typage (equiv), (mod-sub) pour revenir au type initialement obtenu comme conclusion de (eq-projection), (val-projection), (mod-projection). Faisons le cas (val-projection) plus en détails. Considérons une occurrence de

$$\frac{E \vdash p : \mathtt{sig}\ S_1^*;\ \mathtt{val}\ v : \sigma;\ S_2^*\ \mathtt{end} \qquad \tau \leq \sigma\{z \leftarrow p.z \mid z \text{ lié dans } S_1^*\}}{E \vdash p.v : \tau}$$

dans une dérivation. Notons $M = \texttt{sig}\ S_1^*;\ \texttt{val}\ v : \sigma;\ S_2^*\ \texttt{end}$ et M' la signature non dépendante équivalente à M/p. Par construction, M' est de la forme $\texttt{sig}\ S_1'^*;\ \texttt{val}\ v : \sigma';\ S_2'^*\ \texttt{end}$. On peut donc construire la dérivation suivante :

$$\dfrac{\dfrac{\dfrac{\dfrac{E \vdash p : M}{E \vdash p : M/p} \qquad E \vdash M/p <: M'}{E \vdash p : M'} \qquad \mathcal{L}(\sigma') \cap \mathcal{B}(S_1'^*) = \emptyset \qquad \tau' \leq \sigma'}{E \vdash p.v : \tau'} \qquad E \vdash \tau' \approx \tau}{E \vdash p.v : \tau}$$

Il reste bien sûr à montrer que $E \vdash \tau' \approx \tau$. Ceci découle de $E \vdash \sigma' \approx \sigma$, qui est conséquence des lemmes suivants :

1. Si $E \vdash p : M$, alors $E \vdash M \approx M/p$.
2. L'équivalence entre types de modules est transitive. D'où $E \vdash M \approx M'$.
3. Si $E \vdash (\texttt{sig}\ S_1^*;\ \texttt{val}\ v : \sigma;\ S_2^*\ \texttt{end}) <: (\texttt{sig}\ S_1'^*;\ \texttt{val}\ v : \sigma';\ S_2'^*\ \texttt{end})$, alors

$$E \vdash \sigma\{z \leftarrow p.z \mid z \text{ lié dans } S_1^*\} \approx \sigma'\{z \leftarrow p.z \mid z \text{ lié dans } S_1'^*\}$$