Paramétricité et indépendance vis-à-vis des représentations
Parametricity and representation independence

Examen partiel du cours MPRI 2-4 / Mid-term exam for MPRI 2-4 course

2011/11/29 — Durée / duration: 2h30

Le but de ce problème est de montrer que si l'on peut donner un type "suffisamment polymorphe" à une fonction, alors on peut deviner à partir du type quel est le comportement de la fonction. Par exemple, si $\emptyset \vdash a : \alpha \to \alpha$, alors a est forcément la fonction identité. De tels résultats s'appellent des propriétés de paramétricités, ou encore des "théorèmes gratuits" comme les appelle Ph. Wadler (1989). En présence d'abstraction de types (types $\exists\alpha.\tau$), le dual des propriétés de paramétricité est l'indépendance vis-à-vis des représentations : des conditions suffisantes pour que deux implémentations différentes du même type abstrait $\exists\alpha.\tau$ soient indistinguables par le reste du programme.

The goal of this exam is to show that if we can give a "polymorphic enough" type to a function, then we can guess the behavior of the function from its type. For instance, if $\emptyset \vdash a : \alpha \to \alpha$, then a must be the identity function. Such results are called parametricity properties or "theorems for free" as in Ph. Wadler (1989). In the presence of type abstraction (types $\exists\alpha.\tau$), the dual of parametricity properties is representation independence: sufficient conditions for two different implementations of the same abstract type $\exists\alpha.\tau$ to be indistinguishable by the rest of the program.

On se place dans le λ-calcul simplement et implicitement typé, étendu avec des constantes entières (type `int`), et muni d'une sémantique en appel par valeur. On rappelle la syntaxe des types τ, des termes a et des valeurs v, ainsi que les règles de typage :

We consider the implicitly-typed simply-typed λ-calculus extended with integer constants (type `int`) and equipped with a call-by-value semantics. We recall the syntax of types τ, terms a, and values v, as well as the typing rules.

$$\tau ::= \alpha \mid \texttt{int} \mid \tau \to \tau \qquad a ::= x \mid N \mid a\ a \mid \lambda x.a \qquad v ::= N \mid \lambda x.a$$

$$\textsc{Int}\ \ \Gamma \vdash N : int \qquad \textsc{Var}\ \ \frac{x : \tau \in \Gamma}{\Gamma \vdash x : \tau} \qquad \textsc{Lam}\ \ \frac{\Gamma, x : \tau_0 \vdash a : \tau}{\Gamma \vdash \lambda x.a : \tau_0 \to \tau} \qquad \textsc{App}\ \ \frac{\Gamma \vdash a_1 : \tau_2 \to \tau_1 \qquad \Gamma \vdash a_2 : \tau_2}{\Gamma \vdash a_1\ a_2 : \tau_1}$$

Préambule / Warm-up

Dans ce préambule, on suppose que le calcul simplement typé est étendu avec une construction $\mu f.\lambda x.a$ pour les fonctions récursives.

In this warm-up section, we assume that the language is extended with a construct $\mu f.\lambda x.a$ for recursive functions.

Question 1

Soit a un terme tel que $\emptyset \vdash a : \alpha$. Montrer que, nécessairement, a diverge, c'est-à-dire que l'évaluation de a conduit forcément à une suite infinie de réductions $a \to a_1 \to a_2 \to \cdots$. Peut-on définir un tel terme a sans utiliser les fonctions récursives ?

Let a be a term such that $\emptyset \vdash a : \alpha$. Show that, necessarily, a diverges, that is, its evaluation must lead to an infinite sequence of reductions $a \to a_1 \to a_2 \to \cdots$. Can such a term a be defined without using recursive functions?

Answer: By way of contradiction, asume that the reduction of a terminates. By subject reduction and progress, it must end with a value v of type α. However, this is not possible, since values are either integers, of type int, or functions, of arrow types $\tau \to \tau'$. Therefore a must diverge.

In the absence of recursive functions, there is no such a because all reductions terminates (the simply-typed λ-calculus is strongly normalizing).

Question 2

Soit a un terme tel que $\emptyset \vdash a : \texttt{int} \to \alpha$. Montrer que a est une fonction qui ne termine jamais : $a\ N$ diverge pour tout argument entier N.

Let a be a term such that $\emptyset \vdash a : \texttt{int} \to \alpha$. Show that a is a nonterminating function: $a\ N$ diverges for any integer argument N.

Answer: Since, for any integer N, we have $\emptyset \vdash a\ N : \alpha$, the application $a\ N$ must diverge, as shown in question 1.

Question 3

Donner un exemple d'un terme a tel que $\emptyset \vdash a : \alpha \to \alpha$ (on donnera seulement le terme, pas sa dérivation de typage). Donner un autre terme de ce type qui se comporte de la même façon. Voyez-vous d'autres termes du même type avec un comportement différent qui n'utilisent pas les fonctions récursives ? qui utilisent les fonctions récursives ?

Give an example of a term a such that $\emptyset \vdash a : \alpha \to \alpha$ (just give the term, without its typing derivation). Give another term of that type with the same behavior. Can you see another term of that type with a different behavior that does not use recursive functions? that uses recursive functions?

Answer: The identity function $a_0 = \lambda x.x$ is the obvious example. Another term with the same behavior is $\lambda x.a_0\ x$. As we shall see below, without recursive definitions, there is no other term of that type with a different behavior. If we allow recursive definitions, there are two other possible behaviors: a term that always loops, and a function that loops whenever applied. An example of the second kind is $a_2 = (\mu f.\lambda x.fx)$; an example of the first kind is $a_2\ a_0$.

Les relations logiques / Logical relations

Pour raisonner sur le comportement des termes en fonction de leurs types, nous allons utiliser une puissante construction sémantique appelée *relations logiques*.

To reason on the behaviors of terms as a function of their types, we will use a powerful semantic construction called *logical relations*.

On note *Val* l'ensemble des valeurs closes. Une interprétation des variables de types est une fonction ρ qui associe à chaque variable de types α un ensemble quelconque (possiblement vide ou infini) de paires de valeurs closes :

We write *Val* for the set of closed values. A type variable interpretation is a function ρ that maps every type variable α to a (possibly empty or infinite) set of pairs of closed values:

$$\rho(\alpha) = \{(v_1, v_1'); (v_2, v_2'); \ldots\} \subseteq \mathit{Val} \times \mathit{Val}$$

On définit les deux relations suivantes :

We define the following two relations:

$\rho \vdash a \approx a' : \tau$: les termes a et a' sont reliés au type τ dans l'interprétation ρ
terms a and a' are related at type τ in interpretation ρ

$\rho \vdash v \sim v' : \tau$: les valeurs v et v' sont reliées au type τ dans l'interprétation ρ
values v and v' are related at type τ in interpretation ρ

Ces relations sont définies par les équivalences logiques suivantes :

These relations are defined by the following logical equivalences:

$$\begin{aligned}
\rho \vdash a \approx a' : \tau &\iff \exists v \in \mathit{Val}, \exists v' \in \mathit{Val},\ a \xrightarrow{*} v \wedge a' \xrightarrow{*} v' \wedge \rho \vdash v \sim v' : \tau \\
\rho \vdash v \sim v' : \texttt{int} &\iff v = v' = N \text{ for some integer constant } N \\
\rho \vdash v \sim v' : \alpha &\iff \alpha \in \mathsf{dom}(\rho) \wedge (v, v') \in \rho(\alpha) \\
\rho \vdash v \sim v' : \tau_1 \to \tau_2 &\iff \forall w \in \mathit{Val}, \forall w' \in \mathit{Val},\ \rho \vdash w \sim w' : \tau_1 \Longrightarrow \rho \vdash v\ w \approx v'\ w' : \tau_2
\end{aligned}$$

Autrement dit, deux termes sont reliés si leurs évaluations terminent sur deux valeurs qui sont reliées. Deux valeurs de type `int` sont reliées si ce sont des constantes entières et si elles sont égales. Deux valeurs de type α sont reliées si elles figurent dans l'interprétation $\rho(\alpha)$ de la variable de type. Enfin, deux valeurs d'un type fonctionnel $\tau_1 \to \tau_2$ sont reliées si ce sont des fonctions qui envoient des arguments reliés au type τ_1 sur des résultats reliés au type τ_2.

In other words, two terms are related if their evaluations terminate on two values that are related. Two values of type `int` are related if they are integer constants and they are equal. Two values of type α are related if they belong to the interpretation $\rho(\alpha)$ of the type variable α. Finally, two values of a function type $\tau_1 \to \tau_2$ are related if they are functions that map related arguments (at type τ_1) to related results (at type τ_2).

Question 4

Expliquer (sans démonstration formelle) pourquoi les relations $\rho \vdash a \approx a' : \tau$ et $\rho \vdash v \sim v'$ sont mathématiquement bien définies par les équivalences logiques ci-dessus.

Explain (without a formal proof) why the two relations $\rho \vdash a \approx a' : \tau$ and $\rho \vdash v \approx v'$ are mathematically well-defined by the logical equivalences above.

Answer: The equivalences form a well-founded recursive definition. The definition is in fact by induction on the size of types ($\rho \vdash (\cdot \approx \cdot) : \tau$ depends on $\rho \vdash (\cdot \approx \cdot) : \tau$ which itself depends on $\rho \vdash (\cdot \approx \cdot) : \tau'$ for τ' strictly smaller than τ).

Question 5

Dans cette question, on se donne les opérateurs arithmétiques usuels sur le type `int`. Est-ce que

In this question, we assume given the usual arithmetic operators over type `int`. Is it the case that

$$\emptyset \vdash (\lambda x.\ x + x) \approx (\lambda x.\ x \times 2) : \texttt{int} \to \texttt{int}\ ?$$

(Répondre informellement ; il n'est pas nécessaire de faire une démonstration.) Même question pour

(Informal answer, please; no need for a formal proof.) Same question for

$$\emptyset \vdash (\lambda x.\ x) \approx (\lambda x.\ x + 1) : \texttt{int} \to \texttt{int}\ ?$$

Answer: By definition of logical relations, two functions are related at type `int` $\to$ `int` *iff they return the same integer when applied to the same integer. In the first example, this is the case: the functions $\lambda x.\ x + x$ and $\lambda x.\ x \times 2$ both return the integer $2N$ when applied to the integer N. In the second example, the two functions are not related because they differ when applied to 0, for instance: one returns 0 while the other returns 1.*

Question 6

Montrer que les relations $\approx$ et $\sim$ coincident sur les valeurs : si v et v' sont des valeurs,

Show that the relations $\approx$ et $\sim$ coincide over values: if v and v' are values,

$$\rho \vdash v \approx v' : \tau \iff \rho \vdash v \sim v' : \tau$$

Answer: Since values do not reduce, if v and w are values, $v \xrightarrow{*} w$ if and only if $v = w$. The equivalence follows from the definition of $\approx$.

Question 7

Soient a, a', b, b' des termes. Démontrer que $\approx$ est stable par l'inverse de la relation de réduction :

Let a, a', b, b' be terms. Prove that $\approx$ is closed under the inverse of the reduction relation:

$$\rho \vdash b \approx b' : \tau \ \wedge \ a \xrightarrow{*} b \ \wedge \ a' \xrightarrow{*} b' \implies \rho \vdash a \approx a' : \tau$$

Answer: By definition of $\approx$, $\rho \vdash b \approx b' : \tau$ implies the existence of values v, v' such that

$$b \xrightarrow{*} v \qquad b' \xrightarrow{*} v' \qquad \rho \vdash v \sim v' : \tau$$

By hypotheses $a \xrightarrow{*} b$ and $a' \xrightarrow{*} b'$ and transivity of $\xrightarrow{*}$, we have $a \xrightarrow{*} v$ and $a' \xrightarrow{*} v'$. The result follows by definition of $\approx$.

Question 8

Soient a, a', b, b' des termes. Démontrer que $\approx$ est stable par application, c'est-à-dire :

Let a, a', b, b' be terms. Prove that $\approx$ is closed under applications, that is:

$$\rho \vdash a \approx a' : \tau_2 \to \tau_1 \ \wedge \ \rho \vdash b \approx b' : \tau_2 \implies \rho \vdash a \ b \approx a' \ b' : \tau_1$$

Answer: Assume $\rho \vdash a \approx a' : \tau_2 \to \tau_1$ and $\rho \vdash b \approx b' : \tau_2$. By definition of $\approx$ there exist values v, v', w, and w' such that:

$$a \xrightarrow{*} v \ \wedge \ a' \xrightarrow{*} v' \ \wedge \ b \xrightarrow{*} w \ \wedge \ b' \xrightarrow{*} w' \ (\textbf{\textit{1}}) \qquad \rho \vdash v \sim v' : \tau_2 \to \tau_1 \ (\textbf{\textit{2}}) \qquad \rho \vdash w \sim w' : \tau_2 \ (\textbf{\textit{3}})$$

*The definition of $\sim$ for function types applied to (2) and (3) implies $\rho \vdash v \ w \approx v' \ w' : \tau_1$ (**4**). This implies $\rho \vdash a \ b \approx a' \ b' : \tau_1$, as expected, since $\approx$ is closed by the inverse of reduction (question 7) and the four reductions (1) imply $a \ b \xrightarrow{*} v \ w$ and $a' \ b' \xrightarrow{*} v' \ w'$.*

Question 9

Nous allons montrer le *lemme fondamental des relations logiques*, dû à R. Statman (1985). Supposons

We now show the *fundamental lemma of logical relations*, due to R. Statman (1985). Assume

$$\Gamma \vdash a : \tau \quad \text{avec/with } \mathsf{dom}(\Gamma) = \{x_1, \ldots, x_n\} \qquad (\mathbf{A})$$

Soit θ and θ' des substitutions des variables x_i par des valeurs closes

Let θ and θ' be substitutions of closed values for the variables x_i

$$\theta = [x_1 \mapsto v_1, \ldots, x_n \mapsto v_n] \qquad \theta' = [x_1 \mapsto v'_1, \ldots, x_n \mapsto v'_n]$$

telles que

such that

$$\forall i \in= \{1, \ldots, n\}, \quad \rho \vdash \theta x_i \sim \theta' x_i : \Gamma(x_i) \tag{B}$$

Démontrer que

$$\rho \vdash \theta a \approx \theta' a : \tau \tag{C}$$

Autrement dit, pour tout terme bien typé a, si l'on remplace ses variables libres par deux jeux de valeurs reliées, on obtient deux termes reliés. Indication : on procédera par récurrence sur la dérivation de $\Gamma \vdash a : \tau$ et par cas sur a.

Prove that

In other words, for every well-typed term a, if we replace its free variables by two sets of related values, we obtain two related terms. Hint: proceed by induction over the typing derivation of $\Gamma \vdash a : \tau$ and by case analysis over a.

Answer: We assume (A) and (B) and show (C) by induction on the typing derivation of (A), then by case analysis on the last rule applied (or equivalently on the shape of a).

Case INT; a is N. *By inversion of typing, a is N and τ must be* ***int****. Hence, the conclusion (C) is $\rho \vdash N \approx N : int$, which follows from question 6 and the definition of $\sim$ at type* ***int****.*

Case VAR; a is x. *By inversion of typing, x and must be some x_i in $\mathsf{dom}(\Gamma)$ and τ must be τ_i. Hence, the conclusion (C) is $\rho \vdash \theta x_i \approx \theta' x_i : \tau_i$, which follows from question 6 and (B).*

Case LAM; a is $\lambda x.a_1$. *We may assume,* w.l.o.g., *that x does not appear free in Γ (**1**). By inversion of typing, τ is of the form $\tau_0 \to \tau_1$ with $\Gamma, x : \tau_0 \vdash a_1 : \tau_1$ (**2**). The conclusion (C) is $\rho \vdash \theta(\lambda x.a_1) \approx \theta'(\lambda x.a_1) : \tau_0 \to \tau_1$,* i.e. *$\rho \vdash \lambda x.\theta a_1 \approx \lambda x.\theta' a_1 : \tau_0 \to \tau_1$, thanks to (1). Since both terms are values, by question 6 it suffices to show $\rho \vdash \lambda x.\theta a_1 \sim \lambda x.\theta' a_1 : \tau_0 \to \tau_1$.*

*Let v and v' be such that $\rho \vdash v \sim v' : \tau_0$ (**3**). We now show that $\rho \vdash (\lambda x.\theta a_1)\ v \approx (\lambda x.\theta' a_1)\ v' : \tau_1$. Since $\approx$ is closed by the inverse of reduction (question 7), it suffices to show $\rho \vdash [x \mapsto v](\theta a_1) \sim [x \mapsto v'](\theta' a_1) : \tau_1$ (**4**). Let θ_1 be $[x \mapsto v]\theta$ and θ'_1 be $[x \mapsto v']\theta$. (Notice that, the images of θ_1 are closed, the it can be written indifferently as $[x \mapsto v]\theta$ or $\theta[x \mapsto v]$—and similarly for θ'_1.) By induction hypothesis applied to the derivation of (2) with (3), and (B), we have $\rho \vdash \theta_1 a_1 \approx \theta'_1 a_1 : \tau_1$, which is equal to (4).*

Case APP; a is $a_1\ a_2$. *By inversion of typing, τ must be of the form $\tau_2 \to \tau_1$ and such that $\Gamma \vdash a_1 : \tau_2 \to \tau_1$ and $\Gamma \vdash a_2 : \tau_2$. Applying the induction hypothesis applied twice to the typing derivations a_1 and a_2, we obtain $\rho \vdash \theta a_1 \approx \theta' a_1 : \tau_2 \to \tau_1$ and $\rho \vdash \theta a_2 \approx \theta' a_2 : \tau_2$. This implies $\rho \vdash (\theta a_1)\ (\theta a_2) \approx (\theta' a_1)\ (\theta' a_2) : \tau$, since $\approx$ is closed by application (question 8), which is equal to $\rho \vdash \theta(a_1\ a_2) \approx \theta'(a_1\ a_2) : \tau$,* i.e. *the conclusion (C).*

Question 10

Comme corollaire du lemme fondamental, donner une nouvelle preuve de normalisation forte pour le λ-calcul simplement typé :

As a corollary of the fundamental lemma, give a new proof of strong normalization for simply-typed λ-calculus:

$$\emptyset \vdash a : \tau \implies \exists v \in \mathit{Val},\ a \xrightarrow{*} v$$

Answer: Assume $\emptyset \vdash a : \tau$. The fundamental lemma implies $\emptyset \vdash a \approx a : \tau$, which by definition of $\approx$ implies, in particular, that there exists a value v such that $a \xrightarrow{*} v$.

Question 11

Nous étendons le langage avec un destructeur unaire `succ` de type $int \to int$, et avec la δ-réduction :

We now extend the language with a unary destructor `succ` of type $int \to int$ and δ-reduction:

$$\texttt{succ}\ N \to N + 1$$

Montrer que le lemme fondamental des relations logiques est préservé. (Décrire et détailler uniquement le nouveau cas à ajouter dans la preuve de la question 9.)

Show that the fundamental lemma of logical relation is preserved. (Show and detail only the case that must be added to the proof of question 9.)

Answer: A new case of expression appears in the case for constants:

Case a is `succ`. *By inversion of typing, the type τ must be $int \to int$. The conclusion (C) becomes $\rho \vdash \texttt{succ} \approx \texttt{succ} : int \to int$, that is, by question 6, $\rho \vdash \texttt{succ} \sim \texttt{succ} : int \to int$. For any value v and v' such that $\rho \vdash v \sim v' : int$, we must show that $\rho \vdash \texttt{succ}\ v \approx \texttt{succ}\ v' : int$ (**1**). By definition of $\sim$, v and v' must be the same integer N. Therefore, `succ` v and `succ` v' reduce to the same integer $N+1$, which is related to itself at type `int`. Hence, (1) holds.*

Théorèmes gratuits ! / Theorems for free!

Question 12

Soit a un terme tel que

Let a be a term such that

$$\emptyset \vdash a : \alpha \to \alpha$$

En utilisant le lemme fondamental, montrer que a se comporte comme la fonction identité $\lambda x.x$:

Using the fundamental lemma, show that a behaves like the identity function $\lambda x.x$:

$$\forall v \in \mathit{Val},\ a\ v \xrightarrow{*} v$$

Indication : étant donnée une valeur v, interpréter α par l'ensemble $\rho(\alpha) = \{(v, v)\}$.

Hint: given a value v, interpret α by the set $\rho(\alpha) = \{(v, v)\}$.

*Answer: Asume $\emptyset \vdash a : \alpha \to \alpha$ (**1**). Let $v \in Val$. Let ρ be $\alpha \mapsto \{(v, v)\}$. The fundamental lemma implies $\rho \vdash a \approx a : \alpha \to \alpha$. Moreover, by construction of ρ and question 6, we have $\rho \vdash v \approx v$. It follows that $\rho \vdash a\ v \approx a\ v : \alpha$ by question 8. This means that there exists a value v' such that $a\ v \xrightarrow{*} v'$ and $\rho \vdash v' \sim v'$. By definition of $\sim$ at type α, $(v', v') \in \rho(a)$. The only possible choice for v' is v. In conclusion, we have shown $a\ v \xrightarrow{*} v$. This holds for any $v \in Val$.*

Question 13

Soit a un terme tel que

Let a be a term such that

$$\emptyset \vdash a : \alpha \to \alpha \to \alpha$$

Donner deux exemples de termes a qui ont ce type et se comportent différemment. Puis montrer que tout terme a de ce type se comporte comme l'un de ces deux exemples. Plus précisément, en utilisant le lemme fondamental, prouver que

Give two possible terms a that have this type. Then, show that any term a with that type behaves like one of these two examples. More precisely, using the fundamental lemma, prove that

$$(\forall v_1, v_2 \in \mathit{Val},\ a\ v_1\ v_2 \xrightarrow{*} v_1) \quad \vee \quad (\forall v_1, v_2 \in \mathit{Val},\ a\ v_1\ v_2 \xrightarrow{*} v_2)$$

Indication : étant donné deux valeurs v_1, v_2, interpréter α par l'ensemble $\rho(\alpha) = \{(1, v_1); (2, v_2)\}$, montrer que $\rho \vdash a\ 1\ 2 \approx a\ v_1\ v_2 : \alpha$, et conclure.

Hint: for two given values v_1, v_2, interpret α by the set $\rho(\alpha) = \{(1, v_1); (2, v_2)\}$, show that $\rho \vdash a\ 1\ 2 \approx a\ v_1\ v_2 : \alpha$, and conclude.

Answer: The two examples are $a = \lambda x.\lambda y.x$ and $a = \lambda x.\lambda y.y$.

Take $\rho(\alpha) = \{(1, v_1); (2, v_2)\}$. By construction, $\rho \vdash 1 \approx v_1 : \alpha$ and $\rho \vdash 2 \approx v_2 : \alpha$. By the fundamental lemma, $\rho \vdash a \approx a : \alpha \to \alpha \to \alpha$. Applying question 8 twice, it follows that $\rho \vdash a\ 1\ 2 \approx a\ v_1\ v_2 : \alpha$. Let w and w' be the values of $a\ 1\ 2$ and $a\ v_1\ v_2$. By definition of $\approx$, we have $\rho \vdash w \sim w' : \alpha$, that is, $(w, w') \in \rho(\alpha)$. There are only two possible choices: $w = 1$ and $w' = v_1$, or $w = 2$ and $w' = v_2$. Only one of these choices is possible since the semantics of our language is deterministic, and therefore $a\ 1\ 2$ cannot evaluate both to 1 and to 2.

We can now conclude. Either $a\ 1\ 2$ evaluates to 1 and the proof above shows that $a\ v_1\ v_2$ evaluates to v_1 for any values v_1, v_2. Or $a\ 1\ 2$ evaluates to 2 and the proof above shows that $a\ v_1\ v_2$ evaluates to v_2 for any values v_1, v_2.

Question 14

Soit a un terme tel que

Let a be a term such that

$$\emptyset \vdash a : (\alpha \to \alpha) \to (\alpha \to \alpha)$$

Montrer que le seul comportement possible pour a est de composer son argument avec lui-même n fois, pour un n indépendant de son argument :

Show that the only possible behavior for a is to compose its functional argument with itself n times, for an n that is independent of the argument:

$$a \equiv \lambda g.\lambda x.x \ \vee\ a \equiv \lambda g.\lambda x.g\ x \ \vee\ a \equiv \lambda g.\lambda x.g\ (g\ x) \ \vee\ \ldots \ \vee\ a \equiv \lambda g.\lambda x.g^n x \ \vee\ \ldots$$

Plus formellement, pour une valeur $v : \tau$ et une fonction $g : \tau \to \tau$ données, on définit la suite $(v_i)_{i \in \mathbb{N}}$ des valeurs des itérés de g par :

More formally: given a value $v : \tau$ and a function $g : \tau \to \tau$, define the sequence $(v_i)_{i \in \mathbb{N}}$ of the value of the iterates of g by:

$$v_0 = v \qquad \forall i,\ \ g\ v_i \xrightarrow{*} v_{i+1}$$

Construire une interprétation ρ telle que :

Construct an interpretation ρ such that:

$$\rho \vdash a\ \texttt{succ}\ 0 \approx a\ g\ v : \alpha$$

En déduire qu'il existe un entier n, indépendant de g et v, tel que

Deduce that there exists an integer n, independent of g and v, such that

$$a\ g\ v \xrightarrow{*} v_n$$

Answer: Take the interpretation $\rho(\alpha) = \{(0, v_0); (1, v_1); \ldots; (n, v_n); \ldots\}$. By construction, we have $\rho \vdash 0 \approx v : \alpha$ since $v = v_0$. But we also have $\rho \vdash \texttt{succ} \approx g : \alpha \to \alpha$. Indeed, consider two argument values w, w' such that $\rho \vdash w \sim w' : \alpha$. By construction of ρ, there exists an integer i such that $w = i$ and $w' = v_i$. Then, $\texttt{succ}\ i$ reduces to $i + 1$, and $g\ v_i$ reduces to v_{i+1} by definition of the sequence $(v_i)_{i \in \mathbb{N}}$. These two results are related at type α by ρ, as required.

Using the fundamental lemma and question 8 twice, we therefore have $\rho \vdash a\ \texttt{succ}\ 0 \approx a\ g\ v : \alpha$. This implies the existence of values w, w' such that

$$a\ \texttt{succ}\ 0 \xrightarrow{*} w \qquad\qquad a\ g\ v \xrightarrow{*} w' \qquad\qquad \rho \vdash w \sim w' : \alpha$$

By construction of ρ, w must be an integer n and w' must be v_n. Moreover, the integer n is the (unique) value of $a\ \texttt{succ}\ 0$ and is independent from g and v.

Indépendance vis-à-vis des représentations / Representation Independence

Nous étendons maintenant le langage avec des types existentiels primitifs. Afin de changer le minimum à la présentation précédente, nous gardons le style implicitement typé et nous choisissons une présentation où Γ n'introduit pas les variables de types. Le langage est étendu comme suit :

We now extend the language with primitive existential types. In order to change as litle as possible to the previous setting, we keep the implicitly typed style and we choose a presentation where type variables are not introduced in Γ. The language is extended as follows:

$$\tau ::= \ldots \mid \exists\alpha.\tau \qquad a ::= \ldots \mid \mathsf{pack}\ a \mid \mathsf{let}\ x = \mathsf{unpack}\ a\ \mathsf{in}\ a \qquad v ::= \ldots \mid \mathsf{pack}\ v$$

$$\frac{\Gamma \vdash a : [\alpha \mapsto \tau_0]\tau}{\Gamma \vdash \mathsf{pack}\ a : \exists\alpha.\tau} \qquad \frac{\Gamma \vdash a_0 : \exists\alpha.\tau_0 \qquad \Gamma, x : \tau_0 \ \vdash a : \tau \qquad \alpha \notin \mathit{ftv}(\Gamma, \tau)}{\Gamma \vdash \mathsf{let}\ x = \mathsf{unpack}\ a_0\ \mathsf{in}\ a : \tau}$$

$$\mathsf{let}\ x = \mathsf{unpack}\ (\mathsf{pack}\ v)\ \mathsf{in}\ a \to [x \mapsto v]a$$

Les contextes d'évaluation sont étendus de la façon habituelle.

Evaluation contexts are extended as usual.

Nous étendons la définition des relations logiques pour les valeurs de type existentiel comme suit :

We now extend the logical relation for the case of existential types as follows:

$$\rho \vdash v \sim v' : \exists\alpha.\tau \iff \exists w, w' \in \mathit{Val},\ \exists R \subseteq \mathit{Val} \times \mathit{Val},\ \wedge \begin{cases} v = \mathsf{pack}\ w \wedge v' = \mathsf{pack}\ w' \\ \rho, (\alpha \mapsto R) \vdash w \sim w' : \tau \end{cases}$$

Autrement dit, deux valeurs empaquetées sont reliées au type $\exists\alpha.\tau$ si et seulement si leurs valeurs dépaquetées sont reliées au type τ dans une extension de l'interprétation en α pour une relation R quelconque.

In other words, two packed values are related at type $\exists\alpha.\tau$ if and only the unpacked values are related at type τ in an extension of the interpretation on α with some relation R.

On note

We write

$$\mathcal{R}_\rho(\tau) = \{(v, v') \mid \rho \vdash v \sim v' : \tau\}$$

On admettra le *lemme de substitution* suivant :

We shall admit the following *substitution lemma*:

$$\rho, \alpha \mapsto \mathcal{R}_\rho(\tau_0) \vdash a \approx a' : \tau \iff \rho \vdash a \approx a' : [\alpha \mapsto \tau_0]\tau$$

Question 15

Montrer que le lemme fondamental est encore valide avec les types existentiels : détailler dans la preuve de la question 9 les nouveaux cas correspondants aux nouvelles constructions du langage.

The statement of the fundamental lemma is unchanged. Show that the proof of the lemma can be extended: in the proof of question 9, write the new cases for the new language constructs).

Answer: We reuse the notations of question 9. The hypotheses are (A) and (B). The conclusion (C) is shown by structural induction on the term a. We just need to two new cases:

Case Pack; a is $\mathsf{pack}\ a'$. *By inversion of typing applied to (A), τ is of the form $\exists\alpha.\tau'$ and $\Gamma \vdash a' : [\alpha \mapsto \tau_0]\tau'$ for some type τ'_0. The induction hypothesis applied to the derivation of a' implies that $\rho \vdash \theta a' \approx \theta' a' : [\alpha \mapsto \tau_0]\tau'$. the* substitution lemma *implies that $\rho, \alpha \mapsto \mathcal{R}_\rho(\tau_0) \vdash \theta a' \approx \theta' a' : \tau'$. Therefore, there exist values v and v' such that $\theta a' \xrightarrow{*} v$ and $\theta' a' \to v'$ (**1**) and $\rho, \alpha \mapsto \mathcal{R}_\rho(\tau_0) \vdash v \sim$*

$v' : \tau'$. This last relation implies $\rho \vdash \mathsf{pack}\ v \sim \mathsf{pack}\ v' : \exists\alpha.\tau'$ (2) by definition of $\sim$ for existential types. Since substitution commutes with $\mathsf{pack}\ \cdot$, the reduction sequences (1) imply $\theta a = \theta(\mathsf{pack}\ a') = \mathsf{pack}\ (\theta a') \xrightarrow{*} \mathsf{pack}\ v$ and, similarly, $\theta' a \xrightarrow{*} \mathsf{pack}\ v'$. This and (2), implies the conclusion (C).

Case UNPACK; *a is $\mathsf{let}\ x = \mathsf{unpack}\ a_1\ \mathsf{in}\ a_2$. We may assume* w.l.o.g. *that $x \notin \mathsf{dom}(\Gamma)$. By inversion of typing applied to (A), we have $\Gamma \vdash a_1 : \exists\alpha.\tau_1$ and $\Gamma, x; \tau_1 \vdash a_2 : \tau$ where $\alpha \notin ftv(\Gamma, \tau)$. By induction hypothesis applied to the derivation of a_1 we have $\rho \vdash \theta a_1 \approx \theta' a_1 : \exists\alpha.\tau_1$ By definition of $\approx$ and $\sim$, there exist v_1 and v_1' such that $\theta a_1 \xrightarrow{*} \mathsf{pack}\ v_1$ and $\theta' a_1 \xrightarrow{*} \mathsf{pack}\ v_1'$; and a relation R such that $\rho, \alpha \mapsto R \vdash v_1 \approx v_1 : \tau_1$.*

Let θ_1 be $[\alpha \mapsto v_1]\theta$ and θ_1' be $[\alpha \mapsto v_1']\theta'$. By preservation of typing, we have $\Gamma \vdash v_1 : \tau_1$ and $\Gamma \vdash v_1' : \tau_1$. Therefore we can apply the induction hypothesis to the derivation of a_2 with θ_1 and θ_1'. Thus gives $\rho \vdash \theta_1 a_2 \approx \theta_1' a_2 : \tau$, i.e., *$\rho \vdash [x \mapsto v_1](\theta a_2) \approx [x \mapsto v_1'](\theta' a_2) : \tau$ (3). Observe that θa is $\mathsf{let}\ x = \mathsf{unpack}\ \theta a_1\ \mathsf{in}\ \theta a_2$ and reduces to $[x \mapsto v_1](\theta a_2)$; and similarly when replacing θ by θ'. This and (3) and question 7 proves the conclusion (C).*

Comme nous l'avons vu en cours, les types existentiels permettent de modéliser les types de données abstraits. Par exemple, on s'intéresse à un type abstrait α ressemblant aux booléens et muni d'une constante `true` de type α, d'une fonction `not` de type $\alpha \to \alpha$ représentant la négation, et d'une fonction `istrue` de type $\alpha \to$ `bool`. L'interface de ce type abstrait peut être décrite par le type existentiel

As mentioned in the lectures, existential types model abstract data types. For instance, consider an abstract data type α that looks like booleans and is equipped of a constant `true` of type α, of a function `not` with type $\alpha \to \alpha$ representing boolean negation, and of a function `istrue` of type $\alpha \to$ `bool`. The interface of this abstract data type can be described by the existential type

$$\tau_{abool} = \exists\alpha.(\alpha \times (\alpha \to \alpha) \times (\alpha \to \texttt{bool}))$$

Voici deux implémentations de ce type abstrait. L'une représente le type α par des booléens concrets, l'autre le représente par des entiers avec la convention "entier pair = `true`" et "entier impair = `false`".

Here are two implementations of this abstract type. The first implementation represents type α by concrete booleans; the other, by integers, with the convention that "even integer = `true`" and "odd integer = `false`".

$$\begin{aligned} abool_1 : \tau_{abool} &= \mathsf{pack}\ (\texttt{true}, \texttt{not}, \lambda x.x) \\ abool_2 : \tau_{abool} &= \mathsf{pack}\ (0, \texttt{succ}, \lambda x.(x \bmod 2 = 0)) \end{aligned}$$

Le principe d'indépendance vis-à-vis des représentations, énoncé par J. C. Reynolds en 1983, dit qu'il doit être possible de remplacer une implémentation d'un type abstrait par une autre sans changer le comportement d'aucun programme bien typé utilisant ce type abstrait. Ainsi, dans l'exemple ci-dessus, $abool_1$ et $abool_2$ sont indistinguables par tout programme bien typé, alors même que ces deux paquetages implémentent le type abstrait par des types concrets `bool` et `int` qui ne sont pas isomorphes.

The principle of representation independence, due to J.C. Reynolds in 1983, states that it must be possible to replace an implementation of an abstract data type by another implementation, without changing the behavior of any well-typed program that uses this abstract data type. For instance, in the example above, $abool_1$ and $abool_2$ are indistinguishable by any well-typed program, even though those two packages implement the abstract type by concrete types `bool` and `int` that are not isomorphic.

Question 16

Soit $\exists\alpha.\tau$ l'interface d'un type de données abstrait et $\mathsf{pack}\ a_1, \mathsf{pack}\ a_2$ deux implémentations de cette interface :

Let $\exists\alpha.\tau$ be the interface of an abstract data type and $\mathsf{pack}\ a_1, \mathsf{pack}\ a_2$ be two implementations of this interface:

$$\emptyset \vdash \mathsf{pack}\ a_1 : \exists\alpha.\tau \qquad\qquad \emptyset \vdash \mathsf{pack}\ a_2 : \exists\alpha.\tau$$

Soit p un programme "client" paramétré par une implémentation de notre type de données abstrait, c'est-à-dire un terme tel que

Let p be a "client program" parameterized over an implementation of our abstract data type, that is, a term such that

$$\emptyset \vdash p : \exists\alpha.\tau \to \texttt{int}$$

Donner une condition suffisante sur les termes a_1 et a_2 qui garantit que, pour tout programme client p, les termes $p\ (\mathsf{pack}\ a_1)$ et $p\ (\mathsf{pack}\ a_2)$ s'évaluent à l'identique :

Give a sufficient condition over the terms a_1 and a_2 that guarantees that for any client program p, the terms $p\ (\mathsf{pack}\ a_1)$ and $p\ (\mathsf{pack}\ a_2)$ evaluate identically:

$$\forall p, N, \quad p\ (\mathsf{pack}\ a_1) \xrightarrow{*} N \iff p\ (\mathsf{pack}\ a_2) \xrightarrow{*} N$$

Answer: It suffices that $p\ (\mathsf{pack}\ a_1)$ and $p\ (\mathsf{pack}\ a_2)$ are related at type $\mathtt{int}$:

$$\emptyset \vdash p\ (\mathsf{pack}\ a_1) \approx p\ (\mathsf{pack}\ a_2) : \mathtt{int}$$

Since p is related to itself by the fundamental lemma, it suffices that

$$\emptyset \vdash \mathsf{pack}\ a_1 \approx \mathsf{pack}\ a_2 : \exists\alpha.\tau$$

Let v_1 and v_2 be the values of a_1 and a_2, respectively. By definition of logical relations at existential types, the sufficient condition is that there exists an interpretation R for the type variable α such that

$$\alpha \mapsto R \vdash v_1 \sim v_2 : \tau$$

Question 17

Est-ce que votre condition suffisante est vraie pour les deux implémentations $abool_1$ et $abool_2$ du type abstrait τ_{abool} ? On admettra que le lemme fondamental reste vrai si on étend les relations logiques aux types `bool` et triplets de la manière évidente :

Does your sufficient condition hold for the two implementation $abool_1$ et $abool_2$ of the abstract type τ_{abool}? You can admit that the fundamental lemma still holds if we extend logical relations at types `bool` and triples in the obvious way:

$$\begin{aligned}
\rho \vdash v \sim v' : \texttt{bool} &\iff v = v' = \texttt{true} \vee v = v' = \texttt{false} \\
\rho \vdash v \sim v' : \tau_1 \times \tau_2 \times \tau_3 &\iff \exists v_1, v_2, v_3, v_1', v_2', v_3'. \\
&\quad v = (v_1, v_2, v_3) \wedge v' = (v_1', v_2', v_3) \wedge\ \forall i \in \{1,2,3\},\ \rho \vdash v_i \sim v_i' : \tau_i
\end{aligned}$$

Answer: The answer is yes, using the following interpretation R of α:

$$R = \{(\mathtt{true}, 0); (\mathtt{false}, 1); (\mathtt{true}, 2); (\mathtt{false}, 3); \ldots\} = \{(b, n) \mid b \text{ is the parity of } n\}$$

It suffices to check that the components of the two triplets are properly related:

- $\alpha \mapsto R \vdash \mathtt{true} \sim 0 : \alpha$ *by construction of R.*
- $\alpha \mapsto R \vdash \mathtt{not} \sim \mathtt{succ} : \alpha \to \alpha$. *If we apply these two functions to arguments that are related at type α, the arguments are a boolean b and an integer n, with b being the parity of n. The results, then, are $\mathtt{not}\ b$ and $n+1$, and they are related at type α because $\mathtt{not}\ b$ is the parity of $n+1$.*
- $\alpha \mapsto R \vdash \lambda x.x \sim \lambda x.(x \bmod 2 = 0) : \alpha \to \mathtt{bool}$. *If we apply these two functions to arguments that are related at type α, the arguments are a boolean b and an integer n, with b being the parity of n. The results are, then, identical since $n \bmod 2 = 0$ if and only if n is even, that is, $b = \mathtt{true}$.*

Types universels / Universal types

Question 18

Nous étendons maintenant le langage avec des types polymorphes de première class $\forall\alpha.\tau$ comme dans le Système F. Proposer une extension de la définition des relations logiques pour le cas des types polymorphes.

We now extend the language with first-class polymorphic types $\forall\alpha.\tau$ as in System F. Propose an extension of the definition of logical relations for the case of polymorphic types.

Answer: The case for universal types is:

$$\rho \vdash v \sim v' : \forall\alpha.\tau \iff \forall R \subseteq \mathit{Val} \times \mathit{Val},\ \rho, (\alpha \mapsto R) \vdash v \sim v' : \tau$$

In other words, two values are related at type $\forall\alpha.\tau$ if and only if they are related at type τ in any extension of the interpretation on α.

Remark: The fundamental lemma still holds for universal types. It suffices to add the two new cases:

Case Gen. By inversion of typing applied to (A), τ must be of the form $\forall\alpha.\tau$ with $\alpha \notin \mathit{ftv}(\Gamma)$ such that $\Gamma \vdash a : \tau'$ (**1**) holds. Let ρ' be $\rho, \alpha \mapsto R$ for an arbitrary relation R. By induction hypothesis applied to the derivation of (1), we have $\rho' \vdash \theta a : \theta' a : \tau'$. Hence, there are values v and v' such that $\theta a \xrightarrow{*} v$ and $\theta' a \xrightarrow{*} v'$ (**2**) and $\rho' \vdash v \sim v' : \tau'$. Since v does not depend on R, we have actually shown, $\forall R \subseteq \mathit{Val} \times \mathit{Val},\ \rho, (\alpha \mapsto R) \vdash v \sim v' : \tau$, *i.e.* $\rho \vdash v \sim v' : \forall\alpha.\tau'$. This with (2) implies (C).

Case Inst. By inversion of typing applied to (A), τ must be of the form $[\alpha \mapsto \tau_0]\tau'$ (**3**) where $\Gamma \vdash a : \forall\alpha.\tau'$. By induction hypothesis applied to the derivation of this judgment, we have $\rho \vdash \theta a : \theta' a : \forall\alpha.\tau'$. Hence, we have $\rho, \alpha \mapsto R \vdash \theta a : \theta' a : \tau'$. for any relation R, and in particular for $\mathcal{R}_\rho(\tau_0)$. By the subtitution lemma, we have $\rho \vdash \theta a : \theta' a : [\alpha \mapsto \tau_0]\tau'$, which by (3) is (C).