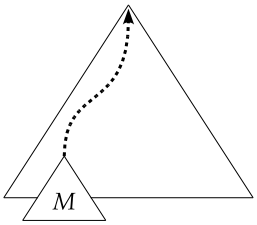
Non-interf´erence

La propriété de non-interférence a été introduite en 1982 par Goguen et Meseguer [16]. En intégrant le concept plus récent de principal, leur définition de cette notion est la suivante : un principal, qui dispose d'un certain ensemble de commandes, n'interfère pas avec un autre principal si les actions du premier n'ont aucun effet visible pour le second.

La non-interférence est une propriété qui s'est révélée particulièrement adaptée aux analyses statiques de flot d'information initiées par Denning et Denning [14, 13]. Intuitivement, ces analyses classent les données en fonction de leur niveau de sécurité. On peut, par exemple, considérer qu'une donnée est soit secrète, soit publique. Un programme peut recevoir en entrée et fournir en sortie des données de différents niveaux. Le but de l'analyse de flot d'information est de déterminer si, en observant les sorties publiques, on peut obtenir une information sur les entrées secrètes. Si tel est le cas, on considère que le programme n'est pas sûr puisqu'il révèle des informations secrètes. Plus concrètement, ces analyses déterminent habituellement si le résultat de l'exécution d'un programme (intuitivement public) révèle des informations sur les données secrètes présentes dans ce programme. On note que la terminaison de l'exécution ou les canaux dits cachés (par exemple le temps d'exécution ou la consommation électrique au cours de l'exécution) ne sont pas pris en compte. Il s'avère que la propriété de sécurité vérifiée par une telle analyse se ramène à la définition de la non-interférence de Goguen-Meseguer. En effet, si on suppose qu'un premier principal peut modifier les entrées secrètes du programme et qu'un deuxième principal n'a accès qu'aux sorties publiques, prouver que le programme est sûr au sens de l'analyse de flot d'information revient à vérifier une propriété de non-interférence. Volpano, Smith et Irvine [42] ont été les premiers à faire ce lien entre les analyses statiques de flot d'information et la non-interférence : le résultat de l'exécution d'un terme bien typé ne révèle pas d'information secrète. La correction de ce système de type est une propriété de non-interférence. Ces résultats ont engendré de nombreux travaux sur les analyses de flot d'information visant à obtenir des systèmes de type pour lesquels tout terme bien typé vérifie la propriété de non-interférence. Volpano et Smith [41] ont poursuivi leurs travaux sur les langages impératifs. Heintze, Riecke, Abadi et Banerjee [22, 1] ont étudié ces analyses dans le cadre de langages fonctionnels dérivés du λ-calcul pur. Simonet et Pottier [37, 39] ont poursuivi l'effort pour traiter Objective Caml, un langage fonctionnel complet, alors que Myers, Nystrom, Zdancewic et Zheng [32] se sont concentrés sur Java. Tous ces travaux portent sur des systèmes de type qui permettent de vérifier statiquement la propriété de non-interférence.

Une autre approche a été initiée par Abadi, Lampson et Lévy [3]. Ces derniers ont proposé une analyse de dépendances dans le contexte du λ-calcul. Les étiquettes du λ-calcul permettent de déterminer si un sous-terme M du terme initial de la réduction contribue au résultat de cette dernière. Cette situation est illustrée par la figure 5.1. Le résultat de cette réduction étant destiné à être public, il ne doit pas dépendre des sous-termes secrets du terme initial. Dans ce cas, les



Est-ce que le résultat de la réduction du terme dépend du sous-terme M ?

FIG. 5.1 – *Non-interférence*

données secrètes n'ont pas interféré dans l'obtention du résultat public de la réduction. Alors que les systèmes de type fournissent une analyse de flot statique, qui nécessite certaines approximations, les étiquettes attachées à un terme indiquent dynamiquement l'information portée par ce dernier. Les travaux de Conchon et Pottier [36] s'inspirent de cette approche. Ils utilisent un langage fonctionnel étiqueté dont les étiquettes, calculées dynamiquement, fournissent une analyse de flot dynamique. En exploitant ce calcul étiqueté, ils proposent un système de type permettant d'assurer statiquement une propriété de non-interférence. Dans ce cas, l'utilisation du calcul étiqueté permet d'obtenir de façon très commode la propriété de non-interférence via une propriété de stabilité. Cependant, en présence de références, cette approche devient plus délicate à cause des effets de bord. L'exemple $\texttt{ifz}\ x\ \texttt{then}\ ()\ \texttt{else}\ y{:=}0$ montre que si, après la réduction de ce terme, la valeur associée à y est non nulle, alors on peut en déduire $x = 0$. En d'autres termes, la non-réduction du sous-terme $y{:=}0$ donne une information sur x.

Dans ce chapitre, l'objectif est d'adapter l'approche d'Abadi et al. à un langage faisant intervenir des références. Dans un premier temps, dans la section 5.1, on étudie la propriété de non-interférence dans le λ-calcul et λ-calcul par valeur. Les valeurs de ces langages ne sont pas des constantes (e.g. des entiers). La définition de la propriété de non-interférence doit être soigneusement adaptée aux valeurs fonctionnelles. Dans le cas du λ-calcul, on établit une relation entre, d'une part la propriété de non-interférence et, d'autre part, les notions de stabilité et de sous-terme critique. Plus précisément, on montre que dans le λ-calcul, un sous-terme interfère si et seulement s'il est critique. Cette équivalence n'est toutefois pas automatique. En particulier, elle n'est pas vraie dans le λ-calcul par valeur. Après avoir étudié la propriété de non-interférence dans le cadre de langages purement fonctionnels, on examine les changements impliqués par la présence d'effets de bord. Dans la section 5.2, on introduit le λ_m-calcul, qui est un λ-calcul muni de δ-règles arithmétiques et conditionnelles et de traits impératifs tels que l'affectation. Ce langage nous permet d'examiner quelques exemples qui permettent de mettre en lumière les difficultés engendrées par la présence d'effets de bord pour la propriété de non-interférence. En plus de l'interférence fonctionnelle déjà observée dans le λ-calcul ou le λ-calcul par valeur, on constate qu'il existe une interférence de mémoire, c'est-à-dire liée à la mémoire. Ainsi, les adresses mémoire peuvent interférer sur le résultat d'une réduction. Et cette interférence s'exerce pendant un certain *intervalle* de temps : entre une écriture et une lecture en mémoire. Dans la section 5.3, on définit le λ_m-calcul étiqueté. Les étiquettes de ce langage visent à exprimer les interférences fonctionnelles et de mémoire. On exploite la propriété d'irréversibilité des chemins pour nommer les adresses avec un nom structurel. Comme pour la propriété de stabilité 1.15 du λ-calcul étiqueté, si un terme se réduit vers une valeur, les étiquettes du λ_m-calcul permettent de déterminer les sous-termes du terme initial qui ont contribué à cette valeur. De plus, les étiquettes permettent aussi d'identifier les intervalles de temps pendant lesquels des adresses de la mémoire ont contribué à cette valeur. Dans la section 5.3.2, on prouve la correction des étiquettes vis-à-vis des intervalles en définissant une réduction contrainte par

un ensemble d'intervalles. Dans la section 5.3.3, on montre que les étiquettes expriment bien une propriété de non-interférence.

5.1 Non-interférence dans le λ-calcul et le λ-calcul par valeur

Si M est un terme dont les différents sous-termes peuvent être publics ou secrets et si M se réduit vers une valeur V, l'enjeu de la non-interférence est de savoir si l'*observation* de cette valeur V, intuitivement publique, donne une information sur un sous-terme secret de M. Dans le cadre du λ-calcul, nous souhaitons examiner cette propriété intuitive en s'inspirant de l'approche des analyses de flot d'information telle que celle développée par Simonet et Pottier [37, 39]. Ces derniers garantissent une propriété de non-interférence en utilisant un typage dans lequel les types ont deux composantes : (1) un type à la ML "classique" (par exemple, le type entier `int`) et (2) un niveau de sécurité qui permet de distinguer les termes secrets des termes publics. La propriété de non-interférence s'énonce informellement de la façon suivante : si le terme M est du type entier public, si x est une variable libre de M dont le type est de niveau secret, si V et V' sont des valeurs de même type que x et si $M\{x\backslash V\}$ et $M\{x\backslash V'\}$ se réduisent vers des entiers n et n', alors ces entiers sont égaux. Ainsi, si la réduction de $M\{x\backslash V\}$ aboutit à une valeur n, cette valeur n ne dépend pas de V et ne fournit donc aucune information sur V. Pour revenir à l'intuition originale de Goguen et Meseguer, un changement d'une valeur secrète V en V' n'a pas d'effet visible du point de vue des valeurs publiques obtenues à l'issue des réductions de $M\{x\backslash V\}$ et $M\{x\backslash V'\}$. Il est important de noter ici que le *canal caché* constitué par l'information selon laquelle la réduction de $M\{x\backslash V\}$ aboutit ou non à une valeur, n'est pas pris en compte. Dans cette section, on s'inspire de la démarche de Simonet et Pottier pour définir une propriété de non-interférence dans le cadre du λ-calcul non typé.

Dans le cadre des travaux de Simonet et Pottier, prouver la non-interférence d'un sous-terme V de M avec le résultat n de la réduction de M, consiste à montrer que si en remplaçant V par une valeur (de même type que V) quelconque V', on obtient une valeur n', alors les valeurs n et n' sont *les mêmes* : on a $n = n'$. On souhaite adapter cette approche de la non-interférence au λ-calcul : si $(C[\,],N)$ est un sous-terme de M et si $M \twoheadrightarrow V$, montrer la non-interférence de N au cours de la réduction menant à V consiste, informellement, à montrer qu'en remplaçant N par N', si $C[N'] \twoheadrightarrow V'$, alors les valeurs V et V' sont *les mêmes*. Le λ-calcul et le λ-calcul par valeur ne contiennent pas de constantes telles que les entiers. Les seules valeurs sont les abstractions. Si la notion de "même valeur" est évidente pour les entiers, cette notion est moins claire dans le cas des abstractions. Pour illustrer ce sujet plus concrètement, on considère l'exemple des réductions des termes $M = (\lambda x.I\lambda y.x)V$ et $M' = (\lambda x.I\lambda y.x)V'$ où $I = V = \lambda z.z$ et $V' = \lambda z.u$.

$$\begin{aligned} \mathcal{R} &: (\lambda x.I\lambda y.x)V \;\to\; I\lambda y.V \;\to\; \lambda y.V \\ \mathcal{R}' &: (\lambda x.I\lambda y.x)V' \to I\lambda y.V' \to \lambda y.V' \end{aligned}$$

Le terme M' est le terme M où la valeur V a été changé en V'. Les valeurs finales des réductions $\mathcal{R}$ et $\mathcal{R}'$ ne sont pas égales. Pourtant, les valeurs V et V' n'ont participé à aucune réduction. Intuitivement, les valeurs $\lambda y.V$ et $\lambda y.V'$ sont identiques à un sous-terme (strict) près. Ces valeurs ont été obtenues de la même façon. Pour distinguer ces valeurs plus clairement, on pourrait utiliser le contexte $C_0[\,] = ([\,]I)I$. On a $C_0[\lambda y.V] \twoheadrightarrow I$ et $C_0[\lambda y.V'] \twoheadrightarrow u$. Ce contexte permet de distinguer ces résultats puisque dans le premier cas, on obtient une valeur, au contraire du deuxième cas. Cependant cette distinction est le fruit d'une interaction entre le contexte $C[\,]$ et les sous-termes V et V'. En d'autres mots, le contexte $C[\,]$ a *interféré* avec V et V'. En revanche, les sous-termes V et V' de M et M' n'interfèrent pas dans les réductions $\mathcal{R}$ et $\mathcal{R}'$. Ceci nous amène à ignorer les

sous-termes stricts des valeurs obtenues et à définir dans ce but la notion d'**observable**.

$$\mathcal{O}(\lambda x.M) = \lambda x.\Omega$$

L'observable d'une abstraction est l'abstraction $\lambda x.\Omega$. Avec cette définition, on peut donner une première tentative de définition de la propriété d'interférence dans le λ-calcul, qui s'inspire de la définition informelle donnée précédemment.

Enoncé 5.1 (Non-interférence) *Le sous-terme $(C[\,],N)$ de M n'interfère pas dans la réduction $M = C[N] \twoheadrightarrow V$ si et seulement si, pour tout N', la réduction $C[N'] \twoheadrightarrow V'$ implique la relation $\mathcal{O}(V) = \mathcal{O}(V')$.*

Un sous-terme n'interfère pas dans une réduction aboutissant à une valeur si, une modification de ce sous-terme ne permet pas d'obtenir une valeur dont l'observable est différent. Comme dans le cas des analyses de flot d'information, on ne tient pas compte ici du canal caché que constitue l'information d'aboutissement vers une valeur. Plus concrètement, on ignore les cas où, en remplaçant N par N' dans M, la réduction n'aboutit pas à une valeur. Ceci se traduit dans la définition de l'interférence par le fait que la convergence de $C[N']$ vers une valeur est une hypothèse. La définition de l'observable d'une valeur et l'énoncé précédent soulèvent toutefois une difficulté : toutes les valeurs, c'est-à-dire toutes les abstractions ont le même observable. Si on adoptait ces définitions, dans l'exemple de la réduction de $M = (\lambda x.I\lambda y.x)V$, on obtiendrait que M n'interfère pas dans la réduction $M \twoheadrightarrow \lambda y.V$. En effet, en remplaçant le sous-terme M par un terme N quelconque et en supposant $N \twoheadrightarrow W$, on a $\mathcal{O}(\lambda y.V) = \mathcal{O}(W) = \lambda y.\Omega$. Intuitivement, les valeurs $\lambda y.V$ et W ne sont pourtant pas les mêmes. La notion d'observable utilisée ici ne capture pas cette intuition. On peut rapprocher cette imprécision des *coïncidences syntaxiques* mentionnées dans la partie 1.3. Dans ce dernier cas, les étiquettes du λ-calcul permettent de distinguer des termes accidentellement identiques. Ainsi, le terme $I(Ix)$ peut se réduire de deux façons différentes vers Ix. Ces termes Ix sont bien syntaxiquement égaux mais ne sont pas intuitivement les mêmes. Dans le cas présent, on exploite aussi les étiquettes du λ-calcul pour pouvoir identifier les valeurs et plus particulièrement leur origine. On se place donc dans le λ-calcul étiqueté et on définit l'observable d'une valeur étiquetée de la façon suivante.

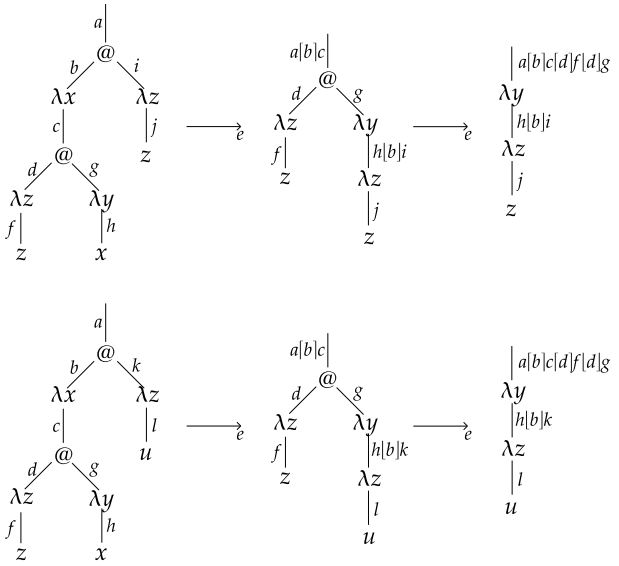
$$\mathcal{O}((\lambda x.M)^\alpha) = (\lambda x.\Omega)^\alpha$$

L'observable d'une abstraction est essentiellement caractérisé par son étiquette de tête. Avec cette définition de l'observable, on définit la propriété de non-interférence dans le λ-calcul étiqueté.

Définition 5.1 (Non-interférence) *Le sous-terme $(C[\,],N)$ du terme M n'interfère pas dans la réduction $M \twoheadrightarrow_e V$ si et seulement si, pour tout terme N', la réduction $C[N'] \twoheadrightarrow_e V'$ implique $\mathcal{O}(V) = \mathcal{O}(V')$.*

Cet énoncé est une adaptation de l'énoncé 5.1. A l'aide de ces nouvelles définitions, on réexamine les exemples mentionnés précédemment. Les réductions de $M = ((\lambda x.((\lambda z.z^f)^d(\lambda y.x^h)^g)^c)^bV)^a$ (où $V = (\lambda z.z^j)^i$) et de $M' = ((\lambda x.((\lambda z.z^f)^d(\lambda y.x^h)^g)^c)^bV')^a$ (où $V' = (\lambda z.u^j)^k$) sont représentées sur la figure 5.2. Conformément à l'intuition, on note que les observables des deux valeurs finales sont bien égaux à $(\lambda y.\Omega)^{a\lceil b\rceil c\lceil d\rceil f\lfloor d\rfloor g}$. Plus généralement, en remplaçant le sous-terme V par un sous-terme quelconque N', on peut montrer que l'observable d'une valeur obtenue est toujours $(\lambda y.\Omega)^{a\lceil b\rceil c\lceil d\rceil f\lfloor d\rfloor g}$. Ceci prouve que le sous-terme V de M n'interfère pas. La nouvelle définition de l'observable capture donc bien la notion de *même valeur* mentionnée dans la définition informelle de la non-interférence que nous avons donnée précédemment.

Dans [36], Conchon et Pottier font le lien entre la propriété de stabilité et la non-interférence en utilisant également un calcul étiqueté inspiré du λ-calcul étiqueté. Pour illustrer ce lien dans le cadre du λ-calcul, il est utile de faire le parallèle entre la définition, étroitement liée à la stabilité,



$M = ((\lambda x.((\lambda z.z^f)^d(\lambda y.x^h)^g)^c)^b V)^a$ où $V = (\lambda z.z^j)^i$
$M' = ((\lambda x.((\lambda z.z^f)^d(\lambda y.x^h)^g)^c)^b V')^a$ où $V' = (\lambda z.u^j)^k$

FIG. 5.2 – *Réductions comparées de M et M'*

de sous-terme *non-critique* et celle de la non-interférence. On considère la réduction $\mathcal{R} : M \twoheadrightarrow_e V$ où $M = C[N]$.

($C[\,]$,N) n'est pas critique ssi, pour tout N', **on a** $C[N'] \twoheadrightarrow_e V'$ **et** $\mathcal{O}(V) = \mathcal{O}(V')$
($C[\,]$,N) n'interfère pas ssi, pour tout N', **si** $C[N'] \twoheadrightarrow_e V'$ **alors** $\mathcal{O}(V) = \mathcal{O}(V')$

Ces définitions ne permettent pas de faire un lien immédiat entre sous-terme critique et sous-terme qui interfère. En revanche, dans le cadre du λ-calcul étiqueté, sous réserve que le terme M initial vérifie l'invariant `INIT`, le résultat 1.16 montre que les termes critiques de M sont ceux dont l'étiquette appartient à l'étiquette de tête de la valeur obtenue. On prouve un résultat similaire, qui permet de caractériser les sous-termes qui interfèrent à l'aide des étiquettes du λ-calcul étiqueté.

Théorème 5.1 (Non-interférence) *On suppose* `INIT`(M) *et* $\mathcal{R} : M \twoheadrightarrow_e V$. *Le sous-terme* ($C[\,]$,$N$) *de M interfère dans $\mathcal{R}$ si et seulement si* $\tau(N) \in |\tau(V)|$.

Preuve : Soit ($C[\,]$,N) un sous-terme de M. Du fait du résultat de stabilité 1.15, on obtient que le préfixe $\mathcal{P}_S(M) = [\![M]\!]_{|\tau(V)|}$ de M vérifie : il existe une valeur V_0 qui est atteinte par la réduction $\mathcal{P}_S(M) \twoheadrightarrow_e V_0$. Du fait du résultat de monotonie 1.13, on obtient $\mathcal{O}(V_0) = \mathcal{O}(V)$. Si $\tau(N) \notin |\tau(V)|$, on a $\mathcal{P}_S(M) = [\![M]\!]_{|\tau(V)|} \preccurlyeq C[\Omega]$. Soit N' un terme quelconque qui vérifie $C[N'] \twoheadrightarrow_e V'$. On obtient $\mathcal{P}_S(M) \preccurlyeq C[\Omega] \preccurlyeq C[N']$ et donc, par monotonie, la réduction $C[N'] \twoheadrightarrow_e V''$ et $V_0 \preccurlyeq V''$. La valeur V'' vérifie bien sûr $\mathcal{O}(V') = \mathcal{O}(V'')$ et $\mathcal{O}(V_0) = \mathcal{O}(V'')$ ce qui prouve que le terme N n'interfère pas dans $\mathcal{R}$. Réciproquement, on suppose que ($C[\,]$,N) n'interfère pas dans $\mathcal{R}$. Soit a une étiquette distincte des étiquettes présentes dans M. Soit N' le terme obtenu à partir de N en changeant l'étiquette de tête en a. Il est clair que $C[N']$ se réduit vers une valeur V'. Par définition de la non-interférence, on obtient $\mathcal{O}(V) = \mathcal{O}(V')$ puis $\tau(V) = \tau(V')$. Comme l'étiquette $\tau(N)$ est absente de $C[N']$, cette étiquette n'appartient pas à $\tau(V')$. On en déduit donc $\tau(N) \notin |\tau(V)|$. □

Si les étiquettes de M sont des lettres distinctes, un sous-terme N de M interfère dans la réduction $M \twoheadrightarrow_e V$ si et seulement si son étiquette est une lettre présente dans l'étiquette de tête de V. On en déduit, en utilisant le résultat 1.16, qu'un sous-terme interfère si et seulement s'il est critique. Pour revenir à la notion de stabilité, on peut adopter un point de vue plus global en définissant le

préfixe d'interférence $\mathcal{P}_I(M)$ d'un terme M qui vérifie $\mathcal{R} : M \twoheadrightarrow_e V$.

$$
\begin{array}{rcll}
\mathcal{P}_I(M) & = & \mathcal{P}_I(M,[\,]) & \\
\mathcal{P}_I(x^\alpha,C[\,]) & = & x^\alpha & \text{si } (C[\,],x^\alpha) \text{ interfère dans } \mathcal{R} \\
\mathcal{P}_I((\lambda x.M)^\alpha,C[\,]) & = & (\lambda x.\mathcal{P}_I(M,C[(\lambda x.[\,])^\alpha]))^\alpha & \text{si } (C[\,],(\lambda x.M)^\alpha) \text{ interfère dans } \mathcal{R} \\
\mathcal{P}_I((MN)^\alpha,C[\,]) & = & (\mathcal{P}_I(M,C[([\,]N)^\alpha])\,\mathcal{P}_I(N,C[(M[\,])^\alpha]))^\alpha & \text{si } (C[\,],(MN)^\alpha) \text{ interfère dans } \mathcal{R} \\
\mathcal{P}_I(M,C[\,]) & = & \Omega & \text{si } (C[\,],M) \text{ n'interfère pas dans } \mathcal{R}
\end{array}
$$

Intuitivement, le préfixe d'interférence de M est un préfixe de M où seuls les sous-termes qui interfèrent sont conservés. On note que cette définition ne dépend pas de la réduction (vers une valeur) considérée. L'introduction du préfixe d'interférence, en conjonction avec le théorème 5.1, permet d'aboutir au résultat suivant.

Théorème 5.2 *Si M vérifie* $\texttt{INIT}(M)$ *et si $M \twoheadrightarrow_e V$, alors les préfixes d'interférence et de stabilité de M coïncident : on a $\mathcal{P}_I(M) = \mathcal{P}_S(M)$.*

Preuve : Ce résultat est une conséquence directe du théorème 5.1 et du résultat 1.16. □

Si les étiquettes de M sont des lettres distinctes, les préfixes d'interférence et de stabilité de M coïncident. Cette propriété permet de faire le lien entre stabilité et non-interférence. Ce lien a été implicitement utilisé dans [36] pour prouver une propriété de non-interférence. Nous verrons dans le paragraphe suivant que cette coïncidence n'est pas systématique.

On examine maintenant la propriété de non-interférence dans le λ-calcul par valeur. De même que précédemment, on se place dans le λ-calcul étiqueté pour avoir une définition de l'observable qui permette d'identifier les valeurs. Dans le λ-calcul étiqueté, une réduction qui contracte des radicaux de la forme $((\lambda x.N)^\alpha V)^\beta$ est une réduction par valeur. Ici, nous n'utilisons pas les étiquettes introduites pour le λ-calcul par valeur dans le chapitre 2. En effet, ces étiquettes ont pour objet de capturer la propriété de stabilité du calcul par valeur. Ici, nous visons la propriété de non-interférence suivante.

Définition 5.2 (Non-interférence) *Le sous-terme $(C[\,],N)$ du terme M n'interfère pas dans la réduction par valeur $M \twoheadrightarrow_e V$ si et seulement si pour tout terme N', le fait que $C[N'] \twoheadrightarrow_e V'$ est une réduction par valeur implique $\mathcal{O}(V) = \mathcal{O}(V')$.*

Cette définition est une adaptation directe de la définition 5.1 dans laquelle on ne considère que des réductions par valeur. Il s'avère que le théorème de non-interférence qui fait le lien entre les étiquettes et la propriété de non-interférence est inchangé.

Théorème 5.3 (Non-interférence) *Soit M un terme tel que* $\texttt{INIT}(M)$ *et $\mathcal{R} : M \twoheadrightarrow_e V$ où $\mathcal{R}$ est une réduction par valeur. Le sous-terme $(C[\,],N)$ de M interfère dans la réduction par valeur $\mathcal{R}$ si et seulement si $\tau(N) \in |\tau(V)|$.*

Preuve : Soit $(C[\,],N)$ un sous-terme de M. Du fait du résultat de stabilité 1.15, on obtient que le préfixe $\mathcal{P}_S(M) = [\![M]\!]_{|\tau(V)|}$ de M vérifie : il existe une valeur V_0 telle que $\mathcal{P}_S(M) \twoheadrightarrow_e V_0$, où, comme nous l'avons vu dans le chapitre 2, cette réduction n'est pas nécessairement par valeur. Comme la réduction menant de M à V peut être vue comme une réduction du λ-calcul étiqueté, en utilisant le résultat de monotonie 1.13, on obtient $\mathcal{O}(V_0) = \mathcal{O}(V)$. Si $\tau(N) \notin |\tau(V)|$, on a $\mathcal{P}_S(M) = [\![M]\!]_{|\tau(V)|} \preccurlyeq C[\Omega]$. Soit N' un terme quelconque qui vérifie $\mathcal{R} : C[N'] \twoheadrightarrow_e V'$ où $\mathcal{R}$ est une réduction par valeur. On obtient $\mathcal{P}_S(M) \preccurlyeq C[\Omega] \preccurlyeq C[N']$ et donc, par monotonie, la réduction $\mathcal{R}' : C[N'] \twoheadrightarrow_e V''$ avec $V_0 \preccurlyeq V''$. La réduction $\mathcal{R}'$ n'est pas nécessairement une réduction par valeur. En revanche, la valeur V'' vérifie $\mathcal{O}(V') = \mathcal{O}(V'')$ et $\mathcal{O}(V_0) = \mathcal{O}(V'')$ ce qui prouve que le terme N n'interfère pas dans $\mathcal{R}$. Réciproquement, on suppose que $(C[\,],N)$ n'interfère pas dans $\mathcal{R}$. Soit a une étiquette distincte des étiquettes présentes dans M. Soit N' le terme obtenu à partir de N en changeant l'étiquette de tête en a. Il est clair que $C[N']$ se réduit par valeur vers une valeur

V'. Par définition de la non-interférence, on obtient $\mathcal{O}(V) = \mathcal{O}(V')$ puis $\tau(V) = \tau(V')$. Comme l'étiquette $\tau(N)$ est absente de $C[N']$, cette étiquette n'appartient pas à $\tau(V')$. On en déduit donc $\tau(N) \notin |\tau(V)|$. □

Comme dans le cas du λ-calcul, si les étiquettes d'un terme M sont des lettres distinctes et si $M \twoheadrightarrow_e V$, un sous-terme interfère si son étiquette est une lettre de $\tau(V)$. De ce fait, les préfixes d'interférence pour le λ-calcul par valeur et pour le λ-calcul classique coïncident. Par conséquent, le préfixe d'interférence pour le λ-calcul par valeur coïncide avec le préfixe de stabilité du λ-calcul. On illustre ces propriétés en prenant l'exemple du terme $((\lambda x.(\lambda y.y^d)^c)^b(\lambda z.z^g)^f)^a$. Ce terme se réduit vers la valeur $V_0 = (\lambda y.y^d)^{a\lceil b\rceil c}$. En vertu du théorème 5.3, le préfixe d'interférence est donc $\mathcal{P}_I(M) = ((\lambda x.(\lambda y.\Omega)^c)^b\Omega)^a$. Dans le cadre du λ-calcul classique, le préfixe de stabilité est le même. Mais en se plaçant dans le λ-calcul par valeur, comme nous l'avons vu dans le chapitre 2, le préfixe de stabilité est en fait $\mathcal{P}_S(M) = ((\lambda x.(\lambda y.\Omega)^c)^b(\lambda z.\Omega)^f)^a$. Dans le λ-calcul par valeur, les préfixes de stabilité et de non-interférence ne coïncident plus ; l'équivalence entre terme critique et terme qui interfère n'est plus vraie. Cette non-coïncidence s'explique simplement en reprenant le parallèle entre les définitions de sous-terme non critique et sous-terme non-interférant mentionné sur la page 111. La non-coïncidence des préfixes de non-interférence et de stabilité pour les réductions par valeur s'explique par l'hypothèse d'obtention d'une valeur à partir du terme $C[N']$. Cette obtention de valeur est garantie dans la définition de sous-terme critique, alors qu'il s'agit d'une hypothèse d'implication dans le cas de la non-interférence. La propriété de stabilité est donc plus forte. Par conséquent, de façon générale, le préfixe de stabilité majore le préfixe de non-interférence.

Dans cette partie, nous avons mis en lumière la relation entre les propriétés de stabilité et d'interférence. Nous avons montré, en particulier, que ces notions coïncident dans le cas du λ-calcul. En revanche, dans le cas du λ-calcul par valeur, la propriété de stabilité est plus forte que la propriété d'interférence car en modifiant un terme non-critique, on obtient bien une valeur alors que si on modifie un terme qui n'interfère pas, l'obtention d'une valeur n'est pas garantie.

5.2 Le λ_m-calcul

Dans cette section, on examine informellement la propriété de non-interférence pour un langage inspiré de Core ML [37, 39] : le λ_m-calcul. Ce langage, fondé sur le λ-calcul présenté dans la section 1.1, dispose en plus de δ-règles pour les opérations arithmétiques et conditionnelles, et de traits impératifs dans le langage afin de pouvoir effectuer des affectations ou des lectures en mémoire. Nous aurions pu traiter dans une section intermédiaire le cas d'un λ-calcul augmenté seulement des δ-règles arithmétiques et conditionnelles. Cependant, comme l'ajout de ces traits fonctionnels ne change pas fondamentalement la situation par rapport au λ-calcul par valeur étudié dans la section 5.1, nous avons préféré ajouter ces δ-règles en même temps que les traits impératifs. Comme nous le verrons par la suite, la présence d'effets de bord change radicalement la nature de la question de la non-interférence.

La syntaxe du langage étudié dans cette section, le λ_m-calcul, est décrite sur la figure 5.3. Pour alléger au maximum les notations de ce chapitre, on se permet de réutiliser certaines notations du λ-calcul ($\mathbf{\Lambda}$,$\mathbf{V}$,...), dans la mesure où le contexte ne laisse aucune ambiguïté. En plus des variables, abstractions et applications du λ-calcul, on ajoute les entiers n, l'addition $M + N$ et le test `ifz` M `then` N `else` P qui porte sur la nullité d'un entier. On ajoute également des traits impératifs. Dans le λ_m-calcul, on dispose d'un ensemble dénombrable d'adresses $\mathbf{M}$. Ces adresses, notées m, représentent les emplacements de la mémoire. Formellement, une mémoire est une application μ définie sur un sous-ensemble fini de $\mathbf{M}$ et qui associe une valeur à chaque adresse de l'ensemble de définition $dom(\mu)$ de μ. Pour une bonne lisibilité, une mémoire μ sera notée

$\mu = \{m_i \mapsto V_i\}_{i \in I}$. Si la mémoire μ étend la mémoire μ' sur l'adresse m, on notera le produit tensoriel correspondant $\mu = (\mu'; m \mapsto V)$. La mémoire vide sera notée $\emptyset$. Pour manipuler la mémoire, quatre nouveaux types de termes sont ajoutés dans la syntaxe du λ_m-calcul. Les *adresses* m sont intuitivement absentes des termes initiaux. Elles sont créées au cours de la réduction par les *références* $\texttt{ref}(M)$. L'*affectation* $M{:=}N$ permet de modifier la valeur associée à une adresse. La *déréférence* $!M$ permet d'accéder à la valeur associée dans la mémoire à une adresse. Le terme *Unit* est ajouté pour les réductions qui ne produisent pas de résultat, par exemple l'affectation. Dans ce calcul, les valeurs sont les abstractions, les entiers, les adresses ou *Unit*.

La réduction $\rightarrow$ du langage est définie sur la figure 5.4. Cette réduction met en relation deux configurations constituées chacune d'un terme et d'une mémoire. La règle (β_m) est reprise du λ-calcul par valeur. L'opération de substitution du λ-calcul est étendue sur les nouveaux termes par la définition de la figure 5.5. Dans le λ_m-calcul, du fait de la définition de la (β_m)-réduction, on ne substitue aux variables que des valeurs. On note que l'ordre d'évaluation est fixé par la règle de contexte (Ctx). Les contextes d'évaluation, définis sur la figure 5.6, imposent une évaluation de gauche à droite sur les applications et les affectations. L'utilisation d'un ordre d'évaluation est dictée par la présence des effets de bord qui rendent le langage non confluent. Par exemple, la réduction de la configuration $((\lambda y.\lambda x.!m)(m{:=}2))(m{:=}0))/(m \mapsto 1)$ peut aboutir à 0, 1 ou 2 selon l'ordre d'évaluation choisi. La δ-règle (Plus) effectue l'addition de deux entiers. Si n est l'entier 0, la réduction de $\texttt{ifz}\ n\ \texttt{then}\ M\ \texttt{else}\ N$ par la δ-règle (Ifz-true) aboutit au terme M. Si le test de nullité échoue, le terme N est obtenu par la règle (Ifz-false). Les règles décrites jusqu'à présent ne modifient pas la mémoire.

La mémoire est modifiée par trois règles. La réduction de la configuration $\texttt{ref}(V)/\mu$ par la règle (Ref) ajoute une nouvelle adresse m à la mémoire μ et retourne cette adresse. Cette adresse est *fraîche* : elle n'appartient pas au domaine de μ. Hormis cette contrainte, le choix de m n'est pas spécifié. La valeur V lui est associée dans la mémoire $(\mu; m \mapsto V)$ obtenue. La réduction d'une configuration $m{:=}V/(\mu; m \mapsto V')$ par la règle (Assign) change la valeur associée par la mémoire à l'adresse m. La nouvelle mémoire associe V à m. Le résultat de la réduction est *Unit*. La réduction d'une déréférence $!m/(\mu; m \mapsto V)$ par la règle (Deref) permet d'accéder à la valeur associée à l'adresse m par la mémoire.

On illustre le langage et les difficultés engendrées pas les effets de bord en étudiant la réduction du terme $M = (\lambda y.(\lambda\_.!y)\ 1)\ \texttt{ref}(0)$ qui est illustrée sur la figure 5.7. Pour représenter la mémoire de façon intuitive, on utilise une bande horizontale pour chaque adresse mémoire. Les opérations d'écriture sont matérialisées par une flèche annotée par E alors que les opérations de lecture sont matérialisées par une flèche annotée par L. La première réduction de M réduit la référence $\texttt{ref}(0)$ ce qui ajoute à la mémoire une nouvelle adresse m_1. Cette dernière est associée en mémoire à la valeur 0. La deuxième réduction est une (β_m)-réduction. L'adresse m_1 est substituée sous la déréférence. La troisième réduction est également une (β_m)-réduction. Comme le corps de l'abstraction contractée ne contient pas la variable liée, l'argument 1 disparaît. On en déduit intuitivement que ce sous-terme n'intervient pas dans le résultat final. La dernière réduction est une déréférence de l'adresse m_1. La valeur associée à m_1 dans la mémoire est lue et donne la valeur finale de la réduction. Deux observations sont retenues de cet exemple : (1) le sous-terme 1 de M n'a pas contribué à la valeur finale. (2) L'adresse m_1 a participé à l'obtention de la valeur finale. Comme on l'a vu dans la section précédente, pour exprimer une propriété de non-interférence sur une réduction, il faut identifier les sous-termes du terme initial qui influencent la valeur finale. Si un sous-terme n'influence pas cette valeur, c'est-à-dire si la modification de ce sous-terme ne change pas l'observable de la valeur finale, alors ce sous-terme n'interfère dans cette valeur. Intuitivement, l'observation (1) nous pousse à émettre l'hypothèse suivante : le sous-terme 1 n'interfère pas dans la réduction $\mathcal{R}$.

Termes	$M,N,P \in \mathbf{\Lambda}$	$::= x$	Variable
		$\mid \lambda x.M$	Abstraction
		$\mid MN$	Application
		$\mid n$	Entier
		$\mid M + N$	Addition
		$\mid \texttt{ifz}\ M\ \texttt{then}\ N\ \texttt{else}\ P$	Branchement
		$\mid \texttt{ref}(M)$	Référence
		$\mid M{:=}N$	Affectation
		$\mid\ !M$	Déréférence
		$\mid m$	Adresse
		$\mid ()$	*Unit*
Valeurs	$V,W \in \mathbf{V}$	$::= \lambda x.M \mid n \mid m \mid ()$	
Mémoire	$\mu \in \mathcal{M}$	$\in\ \mathbf{M} \to \mathbf{V}$	

FIG. 5.3 – *Syntaxe du λ_m-calcul*

(β_m)	$(\lambda x.M)V/\mu \to M\{x\backslash V\}/\mu$
(Plus)	$\dfrac{\mathbf{n} + \mathbf{n'} = \mathbf{n''}}{n + n'/\mu \to n''/\mu}$
(Ifz-true)	$\dfrac{\mathbf{n} = 0}{\texttt{ifz}\ n\ \texttt{then}\ M\ \texttt{else}\ N/\mu \to M/\mu}$
(Ifz-false)	$\dfrac{\mathbf{n} \neq 0}{\texttt{ifz}\ n\ \texttt{then}\ M\ \texttt{else}\ N/\mu \to N/\mu}$
(Ref)	$\dfrac{m \notin dom(\mu)}{\texttt{ref}(V)/\mu \to m/(\mu; m \mapsto V)}$
(Assign)	$m{:=}V/(\mu; m \mapsto V') \to ()/(\mu; m \mapsto V)$
(Deref)	$!m/(\mu; m \mapsto V) \to V/(\mu; m \mapsto V)$
(Ctx)	$\dfrac{R/\mu \to R'/\mu'}{E[R]/\mu \to E[R']/\mu'}$

FIG. 5.4 – *Réduction* $\to$

$$
\begin{aligned}
x\{x\backslash V\} &= V \\
y\{x\backslash V\} &= y \quad \text{si } x \neq y \\
(MN)\{x\backslash V\} &= M\{x\backslash V\}N\{x\backslash V\} \\
(\lambda x.M)\{x\backslash V\} &= \lambda x.M \\
(\lambda y.M)\{x\backslash V\} &= \lambda z.(M\{y \leftarrow z\}\{x\backslash V\}) \quad \text{où } z = \mathsf{Conv}_\alpha(x,y,M,V) \\
\texttt{ref}(M)\{x\backslash V\} &= \texttt{ref}(M\{x\backslash V\}) \\
(!M)\{x\backslash V\} &= !(M\{x\backslash V\}) \\
(M_1{:=}M_2)\{x\backslash V\} &= M_1\{x\backslash V\}{:=}M_2\{x\backslash V\} \\
m\{x\backslash V\} &= m \\
()\{x\backslash V\} &= () \\
\texttt{ifz } M \texttt{ then } N \texttt{ else } P\{x\backslash V\} &= \texttt{ifz } M\{x\backslash V\} \texttt{ then } N\{x\backslash V\} \texttt{ else } P\{x\backslash V\}
\end{aligned}
$$

FIG. 5.5 – *Substitution dans le λ_m-calcul*

$$E[\,] ::= [\,] \mid E[\,]\,N \mid V\,E[\,] \mid E[\,]{:=}N \mid V{:=}E[\,] \mid\, !E[\,] \mid \texttt{ifz } E[\,] \texttt{ then } M \texttt{ else } N$$

FIG. 5.6 – *Les contextes d'évaluation du λ_m-calcul*

On éprouve notre hypothèse en considérant la réduction de $M' = (\lambda y.(\lambda\_.!y)\,\texttt{ref}(1))\,\texttt{ref}(0)$ qui est obtenu à partir du terme M en remplaçant le sous-terme 1 par $\texttt{ref}(1)$. Cette réduction est représentée sur la figure 5.8. La première étape de réduction est similaire à l'exemple précédent. Une adresse m_2 est ajoutée à la mémoire. Le fait que le choix du nom de l'adresse n'est pas spécifié fait que ce nom m_2 est potentiellement différent de m_1. Ensuite, le terme est réduit par (β_m)-réduction qui correspond à la deuxième étape de réduction de $\mathcal{R}$. La troisième réduction ajoute une nouvelle adresse m_3 à la mémoire. Enfin, les deux réductions finales correspondent aux dernières réductions de $\mathcal{R}$. On obtient la même valeur finale 0 ce qui tend à confirmer la non-interférence des sous-termes 1 de M et $\texttt{ref}(1)$ de M', On observe que la réduction $\mathcal{R}'$ ressemble à la réduction $\mathcal{R}$. Seul un pas de réduction causé par le sous-terme $\texttt{ref}(1)$ a été inséré dans $\mathcal{R}'$. Il est clair que les adresses m_1 et m_2 jouent le même rôle dans les deux réductions. Pourtant ces adresses ne portent pas, a priori, le même nom. Ceci illustre bien le fait que le choix du nom d'une adresse n'a pas d'importance, de la même manière que pour le nom de la variable liée par une abstraction. Par une opération similaire à l'α-conversion, on pourrait changer l'adresse m_2 en m_1 dans la réduction $\mathcal{R}$. Nous verrons dans la section suivante qu'on opte pour une solution plus commode : le nom des adresses est choisi

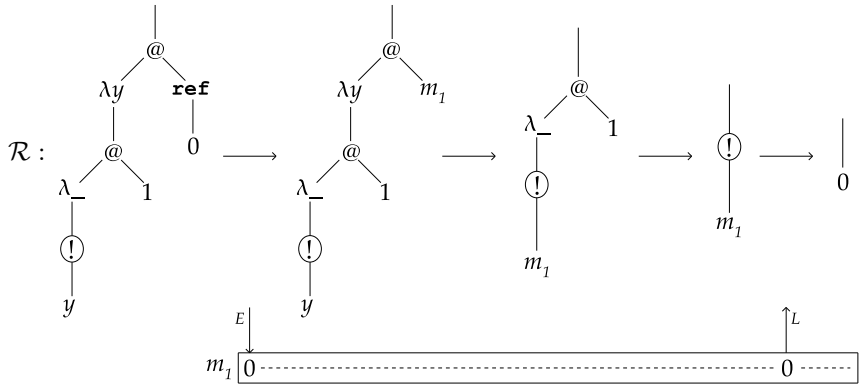


FIG. 5.7 – *Réduction de $M = (\lambda y.(\lambda\_.!y)\,1)\,\texttt{ref}(0)$*

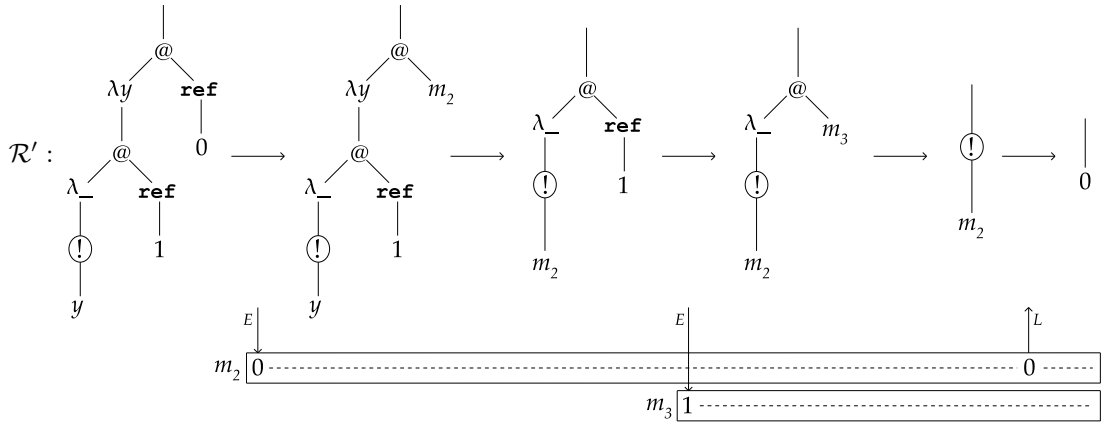


FIG. 5.8 – *Réduction de* $M' = (\lambda y.(\lambda\_.!y)\ \texttt{ref}(1))\ \texttt{ref}(0)$

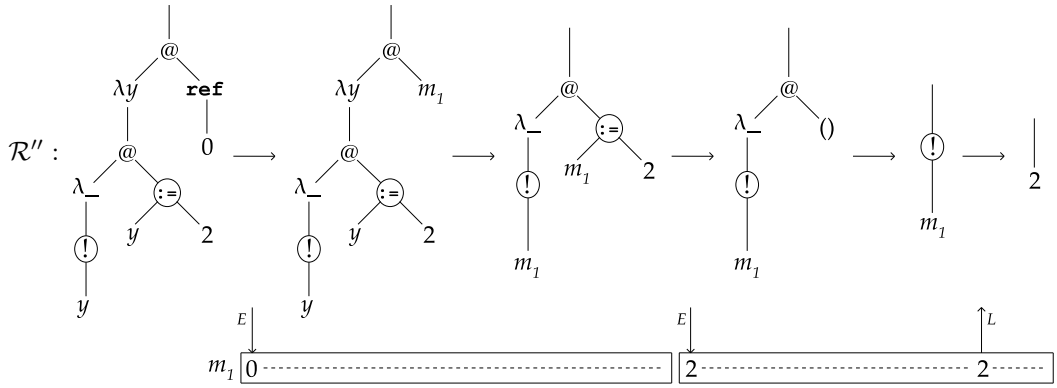
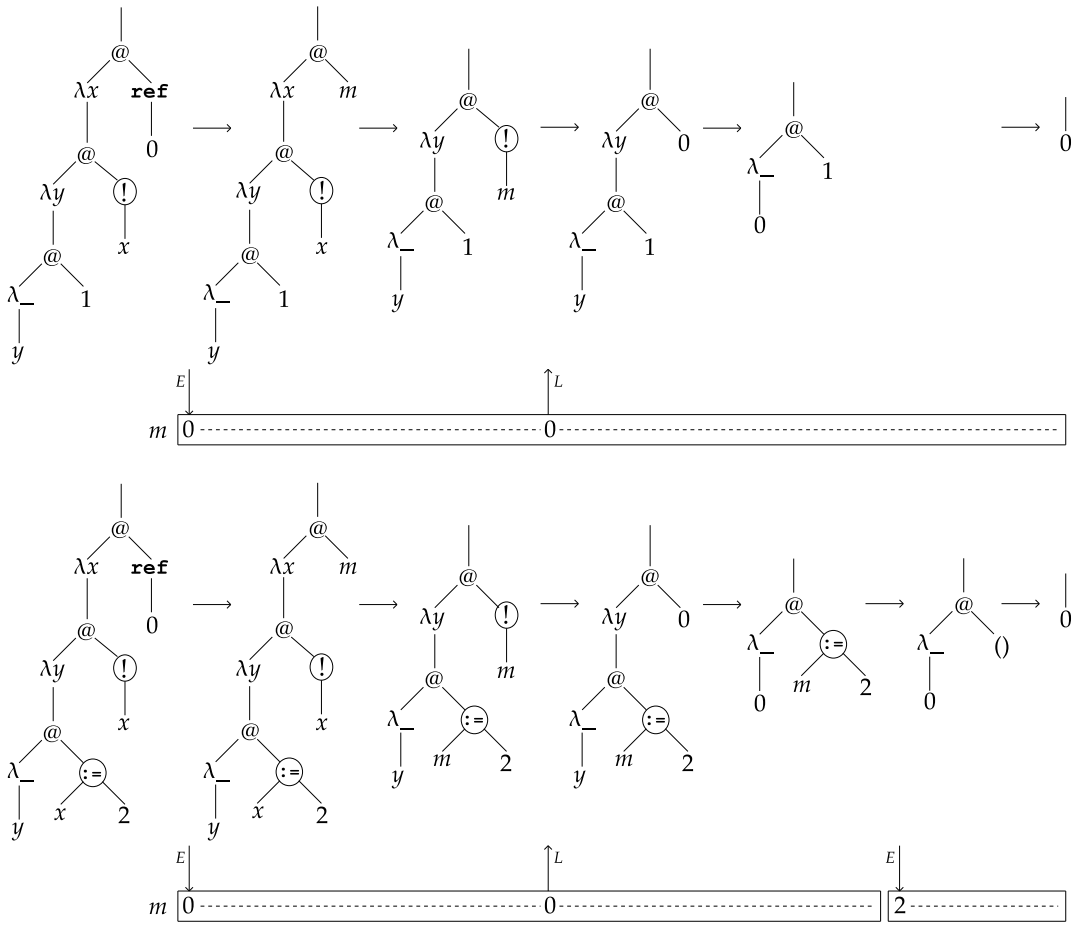


FIG. 5.9 – *Réduction de* $M'' = (\lambda y.(\lambda\_.!y)\ y{:=}2)\ \texttt{ref}(0)$

en fonction de la structure du terme au moment de la réduction (Ref). Comme les termes M et M' sont similaires (en particulier, les chemins qui mènent à la référence réduite $\texttt{ref}(0)$ sont identiques) l'adresse choisie sera la même dans les deux cas. Ceci simplifiera la comparaison entre deux réductions.

A la lumière des conclusions de la section 5.1, on pourrait penser qu'on peut obtenir un préfixe de M dans lequel seuls les sous-termes qui interfèrent, c'est-à-dire participent à l'obtention de la valeur finale, seraient conservés. Tout terme minoré par ce préfixe et qui se réduit vers une valeur, se réduirait, comme M, vers 0. Il s'avère que cette hypothèse est fausse comme le montre la réduction du terme $M'' = (\lambda y.(\lambda\_.!y)\ y{:=}2)\texttt{ref}(0)$ que l'on a obtenu à partir de M en remplaçant le sous-terme 1, supposé ne pas interférer, par $y{:=}2$. Cette réduction est représentée sur la figure 5.9. On observe que les deux premières réductions de $\mathcal{R}''$ sont similaires aux premières réductions de $\mathcal{R}$. La troisième réduction est une affectation $m_1{:=}2$ qui modifie la valeur associée à m_1 en mémoire. Bien entendu, le sous-terme () n'influence pas le résultat puisqu'il disparaît lors de la réduction suivante. En revanche, cette affectation modifie la mémoire ; c'est par ce biais que le résultat final est modifié. A partir de cet instant, les valeurs associées à m_1 dans les mémoires des réductions $\mathcal{R}$ et $\mathcal{R}''$ diffèrent. Au moment de la réduction de la déréférence $!m_1$, cette différence de mémoire entraîne des valeurs finales différentes. Le fait d'avoir remplacé le sous-terme 1 de M par $y{:=}2$ dans M' a donc modifié la valeur finale, sans que le sous-terme () ne soit intervenu. En comparant l'utilisation de m_1 dans $\mathcal{R}$ et $\mathcal{R}''$, on observe que l'écriture et la lecture effectuées au cours de $\mathcal{R}$ se retrouvent bien dans $\mathcal{R}''$. Le problème réside, en réalité, dans le fait qu'une écriture supplémentaire



$$M_1 \;=\; (\lambda y.(\lambda x.(\lambda\_.x)1)!y)\,\texttt{ref}(0)$$
$$M_2 \;=\; (\lambda y.(\lambda x.(\lambda\_.x)(y{:=}2))!y)\,\texttt{ref}(0)$$

FIG. 5.10 – *Réductions comparées de M_1 et M_2*

a lieu entre ces deux instants dans $\mathcal{R}''$. La valeur lue au moment de la déréférence a été modifiée par cette deuxième écriture, ce qui explique les valeurs finales différentes. Intuitivement, l'interférence introduite dans cet exemple n'est pas de la même nature que l'interférence "fonctionnelle" présentée dans la section 5.1 : ici l'interférence n'est pas due à un sous-terme mais à un effet sur une adresse.

On utilise un dernier exemple pour préciser la notion d'interférence sur la mémoire introduite dans l'exemple précédent. Dans cette optique, on compare pas à pas les réductions des termes $M_1 = (\lambda y.(\lambda x.(\lambda\_.x)1)!y)\texttt{ref}(0)$ et $M_2 = (\lambda y.(\lambda x.(\lambda\_.x)(y{:=}2))!y)\texttt{ref}(0)$. Le terme M_2 est le terme M_1 où l'on a remplacé le sous-terme 1 par $y{:=}2$. Ces réductions sont représentées sur la figure 5.10. Les premières réductions de M_1 et M_2 sont similaires. Dans un premier temps, l'adresse m est ajoutée à la mémoire. La valeur 0 lui est associée. Puis une (β_m)-réduction est effectuée : l'adresse m (en argument) est substituée à x. Cette adresse intervient donc dans la déréférence $!m$ et dans l'affectation $m{:=}2$ (dans la réduction de M_2). L'étape suivante consiste à réduire cette déréférence $!m$. La valeur associée à m, à savoir 0 dans les deux cas, est lue. La réduction suivante est, dans les deux cas, une (β_m)-réduction. La cinquième réduction constitue le moment où les deux réductions divergent. Dans la réduction de M_2, l'affectation $m{:=}2$ est réduite, ce qui modifie la valeur associée à m en mémoire. Puis, dans les deux réductions, une (β_m)-réduction permet d'obtenir la valeur finale 0 qui est issue de la lecture de l'adresse m.

La figure 5.10 montre que l'utilisation de l'adresse m est différente dans les deux réductions. Mais ces utilisations différentes n'engendrent pas de différences dans la valeur finale. En effet, la valeur finale 0 est issue de la réduction de la déréférence $!m$. Au moment de cette lecture en mémoire, la valeur associée à m est la même dans les deux réductions. La modification ultérieure, dans la réduction de M_2 ne modifie donc pas le résultat final. Seule la valeur associée à m entre l'écriture initiale et la lecture contribue au résultat. Dans la réduction de M_2, la deuxième écriture a lieu après cette lecture, qui ne perturbe donc pas le résultat. On est donc amené à considérer des *intervalles de temps* pour l'utilisation de la mémoire. Ces intervalles sont délimités par une écriture et une lecture en mémoire. Si on reprend l'exemple de la réduction $\mathcal{R}$, on observe que l'intervalle de m_1 qui contribue à la valeur finale est délimité par l'écriture initiale et la lecture. Au cours de la réduction $\mathcal{R}''$, une écriture a lieu dans cet intervalle, ce qui explique qu'on n'obtienne pas la même valeur finale. Cette notion d'intervalle est donc fondamentale : intuitivement, une adresse n'influence le résultat final que pendant un certain intervalle de temps : entre l'écriture et la lecture d'une valeur qui contribue au résultat final.

Dans le cadre du λ-calcul ou du λ-calcul par valeur, la démarche pour obtenir la propriété de non-interférence pour un terme M donné, consiste à obtenir un préfixe de ce terme dont tous les sous-termes participent au résultat. A contrario, les sous-termes de M qui n'apparaissent pas dans ce préfixe n'influencent pas la valeur finale : ils *n'interfèrent pas*. Dans le cadre présent, ce préfixe ne suffit pas. En plus de l'interférence fonctionnelle déjà étudiée dans la section précédente, il existe, du fait de la présence des effets de bord, une deuxième façon d'interférer : l'interférence sur la mémoire. Comme le montre l'exemple de la réduction $\mathcal{R}''$, une écriture qui intervient au cours d'un intervalle participant à l'obtention de la valeur finale, entraîne une modification de cette dernière. Pour obtenir la non-interférence dans le cadre du λ_m-calcul, il faut donc déterminer, en plus du préfixe mentionné précédemment, les intervalles des adresses qui contribuent au résultat.

5.3 Le λ_m-calcul étiqueté

Dans cette section, nous introduisons le λ_m-calcul étiqueté pour exprimer une propriété de non-interférence. Comme annoncé dans la section précédente, si un terme M se réduit vers une valeur V, les étiquettes du λ_m-calcul doivent permettre de déterminer (1) un préfixe de M qui contient les sous-termes de M qui interfèrent, c'est-à-dire contribuent à l'obtention de V, et (2) l'ensemble des intervalles des adresses qui interfèrent. La syntaxe des termes et des valeurs du λ_m-calcul étiqueté est décrite sur la figure 5.11 : les termes du λ_m-calcul sont munis d'une étiquette. En plus des variables, abstractions et applications du λ-calcul étiqueté, on ajoute les entiers N^α, une addition $(M+N)^\alpha$ et un test à zéro $(\texttt{ifz}\ M\ \texttt{then}\ N\ \texttt{else}\ P)^\alpha$. On retrouve les termes associés à la mémoire. Les adresses m représentent les emplacements de la mémoire, la référence $(\texttt{ref}(M))^\alpha$ permet d'ajouter une nouvelle adresse à la mémoire, l'affectation $(M{:=}N)^\alpha$ permet de modifier la valeur associée à une adresse et la déréférence $(!M)^\alpha$ donne accès à la valeur associée à une adresse. Le terme *Unit* est utilisé pour retourner un résultat vide après une affectation. La syntaxe est également enrichie d'un terme Ω qui représente intuitivement la limite d'un préfixe. Comme dans la section précédente, les valeurs sont les abstractions, les entiers, les adresses ou *Unit*.

Contrairement aux chapitres 1 et 2, dans le λ_m-calcul, le rôle des étiquettes n'est pas d'obtenir une propriété de stabilité. Ici, la propriété visée est la non-interférence. Comme on l'a vu dans la section précédente, dans un langage en appel par valeur comme le λ-calcul par valeur ou le λ_m-calcul, la propriété de non-interférence ne coïncide pas avec la propriété de stabilité. Plus précisément, dans le cas du λ-calcul par valeur, la propriété de non-interférence coïncide avec la propriété de stabilité du λ-calcul général. C'est pourquoi, bien que le λ_m-calcul soit un langage en

Termes	$M,N,P \in \mathbf{\Lambda}$	$::= x^\alpha$	Variable
		$\mid (\lambda x.M)^\alpha$	Abstraction
		$\mid (MN)^\alpha$	Application
		$\mid n^\alpha$	Entier
		$\mid (M+N)^\alpha$	Addition
		$\mid (\texttt{ifz}\ M\ \texttt{then}\ N\ \texttt{else}\ P)^\alpha$	Branchement
		$\mid (\texttt{ref}(M))^\alpha$	Référence
		$\mid (M{:=}N)^\alpha$	Affectation
		$\mid (!M)^\alpha$	Déréférence
		$\mid m^\alpha$	Adresse
		$\mid ()^\alpha$	Unit
		$\mid \Omega$	Préfixe
Valeurs	$V,W \in \mathbf{V}$	$::= (\lambda x.M)^\alpha \mid n^\alpha \mid m^\alpha \mid ()^\alpha$	

FIG. 5.11 – *Syntaxe des termes et des valeurs du λ_m-calcul étiqueté*

appel par valeur, les étiquettes du λ_m-calcul, dont la syntaxe est décrite sur la figure 5.12, sont plus proches des étiquettes du λ-calcul que des étiquettes du λ-calcul par valeur. Comme dans les sections précédentes, une étiquette peut être une lettre a ou une concaténation $\alpha\beta$ de deux étiquettes α et β. Une étiquette peut aussi être une étiquette surlignée $\lceil\alpha\rceil^{\mathtt{x}}$ ou soulignée $\lfloor\alpha\rfloor^{\mathtt{x}}$. Le surlignement (respectivement le soulignement) de α signifie intuitivement que cette étiquette a été créée par le haut (resp. le bas) par la contraction d'un radical de nom α. Cette création est décrite par la *précision* portée en exposant par le surligné ou le souligné : l'étiquette peut être créée par une β-réduction (`b`), par une addition (`p`), par un conditionnel (`i`), par une référence (`c`) ou par une affectation (`w`). Au moment de la contraction d'un terme de la forme $(n^\alpha + n'^\beta)^\gamma$, les origines des termes gauche et droit sont conservées de façon indépendante, dans l'étiquette juxtaposée $\alpha|\beta$. Un *intervalle* $[m,\varphi,\varphi']$ enregistre l'utilisation d'une adresse. Il s'agit d'un triplet constitué de l'adresse impliquée et de deux chemins. Nous montrerons par la suite, dans le théorème 5.4, que la propriété d'irréversibilité des chemins est valable dans le λ_m-calcul étiqueté. Cette propriété implique que certains chemins peuvent être interprétés comme des dates. Ainsi, les chemins φ et φ' correspondent aux dates d'écriture et de lecture de l'adresse m. Un ensemble d'intervalles est appelé *utilisation-mémoire*. Une utilisation-mémoire contient typiquement l'ensemble des intervalles des adresses qui ont contribué au résultat d'une réduction. On utilise la notation $C(B)$ pour obtenir l'ensemble des chemins présents dans une utilisation-mémoire B.

$$C(\{[m_i,\varphi_i,\varphi'_i]\}_{i\in\{1\ldots n\}}) = \bigcup_{i=1}^{n}\{\varphi_i,\varphi'_i\}$$

Les *nœuds* permettent de caractériser la traversée des nœuds sur un parcours d'un chemin issu de la racine. La traversée d'une abstraction est notée avec le nœud λ ; la traversée vers le membre gauche (respectivement droit) d'une application est notée avec le nœud $@_1$ (resp. $@_2$). De même, les nœuds $+_i$ et $:=_i$ sont utilisés pour les chemins qui traversent une addition ou une affectation ($+_1$ et $:=_1$ pour le membre gauche, $+_2$ et $:=_2$ pour le membre droit). Les nœuds `ref` et ! interviendront dans les chemins qui traversent, respectivement, une référence et une déréférence. Dans le cas du branchement, $\texttt{ifz}_1$ est le nœud associé au terme à tester ; $\texttt{ifz}_2$ et $\texttt{ifz}_3$ sont respectivement les nœuds associés au terme de succès et au terme d'échec. Comme précédemment, un chemin est intuitivement la succession des étiquettes et des nœuds rencontrés pendant le parcours depuis la racine vers un nœud de l'arbre de syntaxe associé à un terme. Deux types de chemins sont utilisés. Un chemin-contexte peut être un chemin vide, noté $\bot$, ou une suite alternée d'étiquettes et de

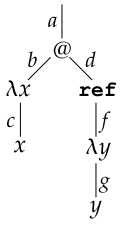
Etiquettes	$\alpha,\beta \in \mathbf{E}$	$::= a$	Lettre
		$\mid \alpha\beta$	Concaténation
		$\mid \lceil\alpha\rceil^{\mathtt{x}}$	Surlignement
		$\mid \lfloor\alpha\rfloor^{\mathtt{x}}$	Soulignement
		$\mid \alpha\vert\beta$	Juxtaposition
		$\mid [m,\varphi,\varphi']$	Intervalle
Précision	$\mathtt{x}$	$::= \mathtt{b} \mid \mathtt{p} \mid \mathtt{i} \mid \mathtt{c} \mid \mathtt{w}$	
Utilisation-mémoire	B	$::= \{[m_i,\varphi_i,\varphi'_i]\}_{i=1\ldots n}$	
Nœud	$\theta \in \mathbf{N}$	$::= \lambda \mid @_i \mid +_i \mid \mathtt{ref} \mid :=_i \mid ! \mid \mathtt{ifz}_j$	$i \in \{1,2\}$ et $j \in \{1,2,3\}$
Chemin-contexte	$\kappa \in \mathbf{K}$	$::= \alpha_1\theta_1\alpha_2\theta_2\ldots\alpha_n\theta_n$	$n \in \mathbb{N}$
Chemin	$m,\varphi,\psi \in \mathbf{\Phi}$	$::= \alpha\theta_1\alpha_1\theta_2\alpha_2\ldots\theta_n\alpha_n$	$n \in \mathbb{N}$

FIG. 5.12 – *Syntaxe des étiquettes et des chemins du λ_m-calcul*

nœuds commençant par une étiquette et finissant par un nœud. Un chemin est une suite alternée commençant et finissant par une étiquette. Comme précédemment, on utilise librement la notation de concaténation pour mettre bout à bout deux suites alternées. Un chemin-contexte correspond à la succession d'étiquettes et de nœuds rencontrés sur le parcours de l'arbre de syntaxe d'un contexte $C[\,]$ menant de la racine au trou de $C[\,]$. Cette correspondance est formalisée par la fonction $\sigma(C[\,])$ qui retourne le chemin-contexte correspondant à $C[\,]$.

$$
\begin{aligned}
\sigma([\,]) &= \bot & \qquad \sigma((C[\,]{:=}N)^\alpha) &= \alpha{:=}_1\sigma(C[\,])\\
\sigma((\lambda x.C[\,])^\alpha) &= \alpha\lambda\sigma(C[\,]) & \qquad \sigma((M{:=}C[\,])^\alpha) &= \alpha{:=}_2\sigma(C[\,])\\
\sigma((C[\,]N)^\alpha) &= \alpha@_1\sigma(C[\,]) & \qquad \sigma((\mathtt{ifz}\ C[\,]\ \mathtt{then}\ N\ \mathtt{else}\ P)^\alpha) &= \alpha\mathtt{ifz}_1\sigma(C[\,])\\
\sigma((MC[\,])^\alpha) &= \alpha@_2\sigma(C[\,]) & \qquad \sigma((\mathtt{ifz}\ M\ \mathtt{then}\ C[\,]\ \mathtt{else}\ P)^\alpha) &= \alpha\mathtt{ifz}_2\sigma(C[\,])\\
\sigma((\mathtt{ref}(C[\,]))^\alpha) &= \alpha\mathtt{ref}\sigma(C[\,]) & \qquad \sigma((\mathtt{ifz}\ M\ \mathtt{then}\ N\ \mathtt{else}\ C[\,])^\alpha) &= \alpha\mathtt{ifz}_3\sigma(C[\,])\\
\sigma((!C[\,])^\alpha) &= \alpha!\sigma(C[\,])
\end{aligned}
$$

Par contraste, un chemin relie la racine à l'étiquette d'un nœud sans contenir le nœud. Nous verrons par la suite qu'une adresse m est, en réalité, un chemin. Certains ensembles sont distingués. On note $\mathbf{\Phi}_\theta$ l'ensemble des chemins qui arrivent sur un nœud θ. Plus formellement, on pose $\mathbf{\Phi}_\theta = \{\varphi \in \mathbf{\Phi} \mid \varphi = \psi\theta\alpha\}$. On définit le prédécesseur $\mathsf{Pre}(\varphi)$ de chemin φ. C'est le plus grand chemin strictement contenu dans φ. Plus formellement, si $\varphi = \varphi'\theta\alpha$, alors $\mathsf{Pre}(\varphi) = \varphi'$. Pour illustrer la notion de chemin, on considère le terme $M = ((\lambda x.x^c)^b(\mathtt{ref}((\lambda y.y^g)^f))^d)^a$ dont le contexte d'évaluation est $E[\,] = ((\lambda x.x^c)^b[\,])^a$.



Le chemin-contexte associé à ce contexte d'évaluation est $\sigma(E[\,]) = a@_2$. Le chemin menant au radical $R = (\mathtt{ref}((\lambda y.y^g)^f))^d$ de M est $\varphi = a@_2d$. Le contexte $C[\,] = (\mathtt{ref}((\lambda y.[\,])^f))^d$ est un contexte de R. Le chemin-contexte associé est $\sigma(C[\,]) = d\mathtt{ref}f\lambda$. De la même manière que les

$$
\begin{array}{rcl@{\qquad}rcl}
\alpha \cdot x^{\beta} & = & x^{\alpha\beta} & \alpha \cdot (\lambda x.M)^{\beta} & = & (\lambda x.M)^{\alpha\beta} \\
\alpha \cdot (MN)^{\beta} & = & (MN)^{\alpha\beta} & \alpha \cdot (N+M)^{\beta} & = & (N+M)^{\alpha\beta} \\
\alpha \cdot n^{\beta} & = & n^{\alpha\beta} & \alpha \cdot (\texttt{ifz}\ M\ \texttt{then}\ N\ \texttt{else}\ P)^{\beta} & = & (\texttt{ifz}\ M\ \texttt{then}\ N\ \texttt{else}\ P)^{\alpha\beta} \\
\alpha \cdot (\texttt{ref}(M))^{\beta} & = & (\texttt{ref}(M))^{\alpha\beta} & \alpha \cdot (M{:=}N)^{\beta} & = & (M{:=}N)^{\alpha\beta} \\
\alpha \cdot (!M)^{\beta} & = & (!M)^{\alpha\beta} & \alpha \cdot ()^{\beta} & = & ()^{\alpha\beta} \\
\alpha \cdot m^{\beta} & = & m^{\alpha\beta} & \alpha \cdot \Omega & = & \Omega
\end{array}
$$

FIG. 5.13 – *Définition de la fonction de concaténation* “ $\cdot$ ”

contextes peuvent s'imbriquer, on utilise la concaténation pour composer les chemins-contextes. Le chemin-contexte associé à $E[C[\,]]$ est $\sigma(E[C[\,]]) = \sigma(E[\,])\sigma(C[\,]) = a@_2d\texttt{ref}f\lambda$. Au moment de la définition des réductions, nous verrons que nous associerons à M *le chemin* $\varphi_0 = a@_2d\texttt{ref}f$ *menant au cœur du radical* R. On remarque en particulier $\mathsf{Pre}(\varphi_0) = \varphi$ et $\psi \in \mathbf{\Phi}_{\texttt{ref}}$. La relation de préfixe sur les chemins qui a été introduite dans la partie 1.3 s'étend de façon élémentaire aux chemins considérés ici.

$$
\begin{array}{l}
\kappa \preceq \kappa' \iff \exists \kappa'' \in \mathbf{K}\ .\ \kappa\kappa'' = \kappa' \\
\kappa \prec \varphi \iff \exists \varphi' \in \mathbf{\Phi}\ .\ \kappa\varphi' = \varphi \\
\varphi \prec \kappa \iff \exists (\kappa',\theta) \in \mathbf{K} \times \mathbf{N}\ .\ \varphi\theta\kappa' = \kappa \\
\varphi \preceq \varphi' \iff \varphi = \varphi' \text{ ou } \exists (\varphi'',\theta) \in \mathbf{\Phi} \times \mathbf{N}\ .\ \varphi\theta\varphi'' = \varphi'
\end{array}
$$

La relation $\preceq$ est un ordre bien fondé sur $\mathbf{K} \cup \mathbf{\Phi}$ dont le plus petit élément est $\bot$.

Dans le λ_m-calcul étiqueté, on adapte la définition de la mémoire, afin de déterminer les dates d'écriture et de lecture des adresses.

$$\text{Mémoire} \qquad \mu \in \Phi \rightarrow \mathbf{\Phi} \times \mathbf{V} \qquad \Phi \subseteq \mathbf{\Phi} \text{ et } \Phi \text{ fini}$$

Comme annoncé précédemment, les adresses sont, dans le λ_m-calcul étiqueté, des chemins. Une mémoire est une fonction finie qui associe à une adresse $m \in \Phi$, un couple (φ,V) constitué d'un chemin φ et d'une valeur V. Cette dernière est bien entendu la valeur associée en mémoire à m. Le chemin φ correspond à la date d'écriture de V en mémoire. Comme pour le λ_m-calcul, pour une bonne lisibilité, une mémoire μ peut s'écrire $\mu = \{m_i \mapsto (\varphi_i,V_i)\}_{i\in I}$ ou bien $\mu = \{m_i \overset{\varphi_i}{\longmapsto} V_i\}_{i\in I}$. Si μ est définie sur $\Phi \cup \{m\}$ avec $\mu(m) = (\varphi,V)$ et si sa restriction sur Φ est μ_0, alors on pourra écrire μ sous la forme du produit tensoriel $\mu = (\mu_0; m \overset{\varphi}{\longmapsto} V)$. La mémoire vide sera notée $\emptyset$. Une *configuration* est un couple constitué d'un terme M et d'une mémoire μ. Intuitivement, cette dernière contient les valeurs associées aux adresses présentes dans M. Cette configuration est notée M/μ.

La réduction étiquetée du λ_m-calcul est décrite sur la figure 5.14. Pour alléger les notations, nous utilisons le même symbole que pour la réduction sans étiquettes. La réduction $\rightarrow$ est définie à l'aide de la réduction $\overset{\kappa}{\rightarrow}$ pour laquelle κ est le chemin-contexte associé au contexte du radical. Les définitions de ces réductions s'appuient sur les définitions de la fonction “ $\cdot$ ” de concaténation (sur la figure 5.16), de l'étiquette de tête τ (sur la figure 5.13) et de la substitution (sur la figure 5.15). La fonction $|\alpha|$ qui fournit les lettres présentes dans l'étiquette α est adaptée simplement du λ-calcul étiqueté ; sa définition est donnée sur la figure 5.17.

Comme annoncé précédemment, la réduction étiquetée du λ_m-calcul vise la propriété de non-interférence et non la stabilité. De ce fait, bien que la stratégie d'évaluation choisie pour le λ_m-calcul soit en appel par valeur, la réduction $\rightarrow$ s'inspire davantage de la réduction étiquetée du λ-calcul

$$(\beta_{me}) \qquad ((\lambda x.M)^\alpha V)^\beta/\mu \xrightarrow{\kappa} \beta \cdot \lceil\alpha\rceil^{\mathtt{b}} \cdot M\{x\backslash\lfloor\alpha\rfloor^{\mathtt{b}} \cdot V\}/\mu$$

$$(\mathrm{Plus}_e) \qquad \frac{\mathbf{n_1} + \mathbf{n_1} = \mathbf{n}}{(n_1^\alpha + n_2^\beta)^\gamma/\mu \xrightarrow{\kappa} n^{\gamma\lceil\alpha|\beta\rceil^{\mathtt{p}}}/\mu}$$

$$(\text{Ifz-true}_e) \qquad \frac{\mathbf{n} = 0}{(\mathtt{ifz}\ n^\alpha\ \mathtt{then}\ M\ \mathtt{else}\ N)^\beta/\mu \xrightarrow{\kappa} \beta \cdot \lceil\alpha\rceil^{\mathtt{i}} \cdot M/\mu}$$

$$(\text{Ifz-false}_e) \qquad \frac{\mathbf{n} \neq 0}{(\mathtt{ifz}\ n^\alpha\ \mathtt{then}\ M\ \mathtt{else}\ N)^\beta/\mu \xrightarrow{\kappa} \beta \cdot \lceil\alpha\rceil^{\mathtt{i}} \cdot N/\mu}$$

$$(\mathrm{Ref}_e) \qquad \frac{m = \kappa\beta \qquad \alpha = \tau(V) \qquad \varphi = \kappa\beta\mathtt{ref}\alpha}{(\mathtt{ref}(V))^\beta/\mu \xrightarrow{\kappa} m^{\lceil\beta\rceil^{\mathtt{c}}}/(\mu; m \overset{\varphi}{\longmapsto} V)}$$

$$(\mathrm{Assign}_e) \qquad \frac{\varphi' = \kappa\beta{:=_1}\alpha}{(m^\alpha{:=}V)^\beta/(\mu; m \overset{\varphi}{\longmapsto} V') \xrightarrow{\kappa} ()^{\lceil\beta\rceil^{\mathtt{w}}}/(\mu; m \overset{\varphi'}{\longmapsto} V)}$$

$$(\mathrm{Deref}_e) \qquad \frac{\varphi' = \kappa\beta!\alpha}{(!m^\alpha)^\beta/(\mu; m \overset{\varphi}{\longmapsto} V) \xrightarrow{\kappa} \beta \cdot [m,\varphi,\varphi'] \cdot V/(\mu; m \overset{\varphi}{\longmapsto} V)}$$

$$(\mathrm{Ctx}_e) \qquad \frac{R/\mu \xrightarrow{\sigma(E[\,])} R'/\mu'}{E[R]/\mu \to E[R']/\mu'}$$

FIG. 5.14 – *Réductions* $\to$ *et* $\xrightarrow{\kappa}$ $(\kappa \in \mathbf{K})$

$$\begin{aligned}
x^\alpha\{x\backslash V\} &= \alpha \cdot V \\
y^\alpha\{x\backslash V\} &= y^\alpha \\
n^\alpha\{x\backslash V\} &= n^\alpha \\
(\lambda x.M)^\alpha\{x\backslash V\} &= (\lambda x.M)^\alpha \\
(\lambda y.M)^\beta\{x\backslash V\} &= (\lambda z.M\{y \leftarrow z\}\{x\backslash V\})^\beta \text{ où } z = \mathsf{Conv}_\alpha(x,y,M,V) \\
(MN)^\alpha\{x\backslash V\} &= (M\{x\backslash V\}N\{x\backslash V\})^\alpha \\
(\mathtt{ref}(M))^\alpha\{x\backslash V\} &= (\mathtt{ref}(M\{x\backslash V\}))^\alpha \\
!(M)^\alpha\{x\backslash V\} &= (M\{x\backslash N\})^\alpha \\
(M_1{:=}M_2)^\alpha\{x\backslash V\} &= (M_1\{x\backslash V\}M_2\{x\backslash V\})^\alpha \\
m^\alpha\{x\backslash V\} &= m^\alpha \\
()^\alpha\{x\backslash V\} &= ()^\alpha \\
(\mathtt{ifz}\ M\ \mathtt{then}\ N\ \mathtt{else}\ P)^\alpha\{x\backslash V\} &= (\mathtt{ifz}\ M\{x\backslash V\}\ \mathtt{then}\ N\{x\backslash V\}\ \mathtt{else}\ P\{x\backslash V\})^\alpha
\end{aligned}$$

FIG. 5.15 – *Définition de la substitution par une valeur*

$$\begin{aligned}
\tau(x^\alpha) &= \alpha & \tau((\lambda x.M)^\alpha) &= \alpha \\
\tau((MN)^\alpha) &= \alpha & \tau((N+M)^\alpha) &= \alpha \\
\tau(n^\alpha) &= \alpha & \tau((\mathtt{ifz}\ M\ \mathtt{then}\ N\ \mathtt{else}\ P)^\alpha) &= \alpha \\
\tau((\mathtt{ref}(M))^\alpha) &= \alpha & \tau((M{:=}N)^\alpha) &= \alpha \\
\tau((!M)^\alpha) &= \alpha & \tau(()^\alpha) &= \alpha \\
\tau(m^\alpha) &= \alpha
\end{aligned}$$

FIG. 5.16 – *Définition de la fonction* τ *d'étiquette de tête*

$$\begin{aligned}
|a| &= \{a\} & |\lfloor\alpha\rfloor^{\mathtt{x}}| &= |\alpha| & |\lceil\alpha\rceil^{\mathtt{x}}| &= |\alpha| \\
|\alpha\beta| &= |\alpha| \cup |\beta| & |[m,\varphi,\varphi']| &= |m| \cup |\varphi| \cup |\varphi'| & |\alpha|\beta| &= |\alpha| \cup |\beta| \\
& & |\varphi\theta\alpha| &= |\varphi| \cup |\alpha|
\end{aligned}$$

FIG. 5.17 – *Lettres présentes dans une étiquette ou un chemin*

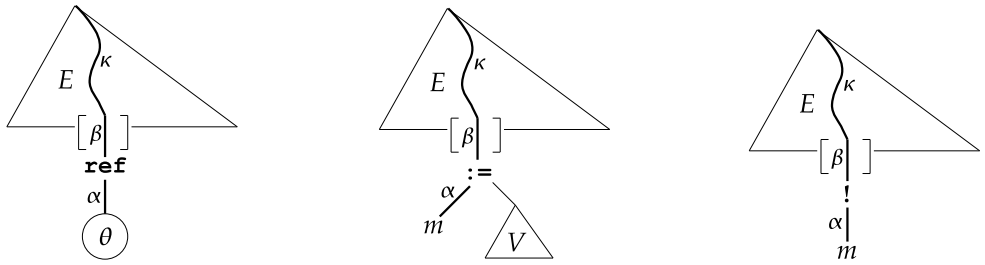
$$E[\,] := [\,] \mid (E[\,]N)^{\alpha} \mid (V\,E[\,])^{\alpha} \mid (E[\,]{:=}N)^{\alpha} \mid (V{:=}E[\,])^{\alpha} \mid (!E[\,])^{\alpha} \mid (\texttt{ifz}\ E[\,]\ \texttt{then}\ M\ \texttt{else}\ N)^{\alpha}$$

FIG. 5.18 – *Contexte d'évaluation du λ_m-calcul étiqueté*

que celle du λ-calcul par valeur. De ce fait, l'étiquette de tête de la valeur intervenant dans la β_{me}-réduction n'intervient pas dans cette réduction. Cette étiquette sera visible dans le résultat final uniquement si la valeur V est effectivement utilisée. Dans le cas de la règle (Plus_e), les deux entiers interviennent effectivement dans le résultat. C'est pourquoi les étiquettes, qui représentent les histoires de ces entiers, sont *juxtaposées* dans le résultat. Pour les règles (Ifz-true_e) et (Ifz-false_e), une étiquette $\lceil\alpha\rceil^{\mathtt{i}}$ est créée pour enregistrer l'histoire de l'entier qui a commandé la δ-règle conditionnelle. La règle (Ctx_e) permet d'imposer l'ordre d'évaluation qui correspond aux contextes d'évaluation décrits sur la figure 5.18. Parmi les chemins des termes, certains seront plus particulièrement utilisés dans la suite de la section. Si $M = E[R]$ et $M/\mu \to M'/\mu'$, le **chemin menant au radical contracté** entre M et M' est défini par $\varphi_r = \sigma(E[\,])\tau(R)$.

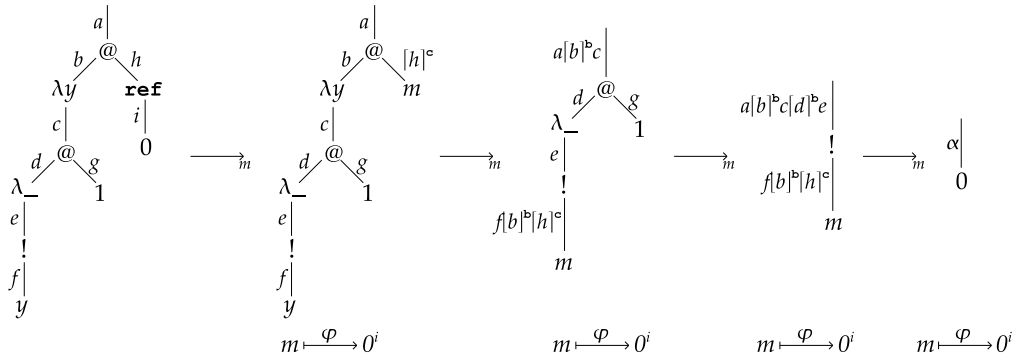
Dans les règles de réductions qui manipulent la mémoire, en plus d'identifier les sous-termes qui participent au résultat, les étiquettes enregistrent les intervalles associés aux adresses. La règle (Ref_e) réduit le terme $(\texttt{ref}(V))^{\alpha}$ et ajoute une nouvelle adresse m à la mémoire μ. L'adresse choisie $m = \kappa\beta$ correspond au chemin menant au radical. Ce choix est *structurel* : il ne dépend que du terme à réduire. Ce choix est aussi *correct* : comme on le montrera plus tard dans le théorème 5.4, cette adresse n'appartient pas au domaine de la mémoire (sous certaines hypothèses raisonnables). L'adresse m retournée est étiquetée par $\lceil\beta\rceil^{\mathtt{c}}$. En effet, le sous-terme m ne dépend pas de la mémoire, ni de la valeur V. Les sous-termes qui ont contribué à obtenir cette adresse sont donc les mêmes que ceux qui ont contribué à obtenir le radical $(\texttt{ref}(V))^{\beta}$. La valeur V et le chemin $\varphi = \kappa\beta\texttt{ref}\alpha$ sont associés à m en mémoire. En ce qui concerne l'interférence de la mémoire, deux informations doivent être enregistrées dans le cas de cette réduction : (1) l'étiquette α qui permet d'identifier l'ensemble des sous-termes ayant contribué à créer le radical qui effectue l'écriture (interférence fonctionnelle) et (2) la date de l'écriture de V dans l'adresse m (interférence de la mémoire). Comme on l'a vu dans la section 1.3, le chemin $\kappa\beta$ menant au radical peut être considéré comme une date, puisque, du fait de la propriété d'irréversibilité des chemins, ce chemin ne peut réapparaître dans la suite de la réduction. Par conséquent, le chemin φ peut aussi être considéré comme une date. Ce chemin est une façon concise de garder les deux informations à enregistrer. Ce chemin donne accès à l'étiquette α et au chemin menant au radical par $\mathsf{Pre}(\varphi) = \kappa\beta$. Dans le cas de cette réduction, l'étiquette α enregistre à la fois les sous-termes ayant contribué à obtenir la valeur V mais aussi les sous-termes ayant contribué à l'obtention du radical. En conséquence, cette étiquette est gardée à la fois dans le chemin φ associé à m en mémoire et dans l'étiquette de tête de V. On pourrait sans doute se contenter du chemin $\kappa\beta$ à la place de φ. Nous avons préféré utiliser φ par souci d'uniformité avec les réductions (Assign_e) et (Deref_e) présentées ci-dessous.

La règle (Assign_e) réduit l'affectation $(m^{\alpha}{:=}V)^{\beta}$. Le terme *Unit* retourné est étiqueté par $\lceil\beta\rceil^{\mathtt{w}}$. En effet, le résultat de l'affectation ne dépend ni de m ni de V. Les sous-termes qui ont contribué à obtenir () sont bien les mêmes que ceux qui ont contribué à obtenir le radical $(m^{\alpha}{:=}V)^{\beta}$. La valeur V et le chemin $\varphi = \kappa\beta{:=}_1\alpha$ sont associés en mémoire à l'adresse m. Comme pour la règle (Ref_e), deux informations concernant l'interférence mémoire doivent être enregistrées dans le cas de cette réduction : (1) l'étiquette α qui permet d'identifier l'ensemble des sous-termes ayant contribué à créer le radical qui effectue l'écriture (interférence fonctionnelle) et (2) la date de l'écriture de V dans l'adresse m (interférence de la mémoire). Comme précédemment, le chemin φ, qui peut être considéré comme une date, est une façon concise de garder les deux informations à enregistrer. Ce



Cas (Ref) : $\varphi = \kappa\beta\mathtt{ref}\alpha$ Cas (Assign) : $\varphi = \kappa\beta{:=}_1\alpha$ Cas (Deref) : $\varphi = \kappa\beta!\alpha$

FIG. 5.19 – *Chemin menant au cœur du radical pour* $\kappa = \sigma(E[\,])$



$$
\begin{aligned}
m &= a@_2h\\
\varphi &= a@_2h\mathtt{ref}i\\
\varphi' &= a\lceil b\rceil^{\mathtt{b}}c\lceil d\rceil^{\mathtt{b}}e!f\lfloor b\rfloor^{\mathtt{b}}\lceil h\rceil^{\mathtt{c}}\\
\alpha &= a\lceil b\rceil^{\mathtt{b}}c\lceil d\rceil^{\mathtt{b}}e[m,\varphi,\varphi']i
\end{aligned}
$$

FIG. 5.20 – *Réduction de* $M = ((\lambda y.((\lambda\_.(!y^f)^e)^d)^c\ 1^g)^b\ (\mathtt{ref}(0^i))^h)^a$

chemin donne accès à l'étiquette α et au chemin menant au radical par $\mathsf{Pre}(\varphi) = \kappa\beta$.

La règle (Deref$_e$) réduit la déréférence $(!m^\alpha)^\beta$ et lit la valeur associée à l'adresse m en mémoire. Cette valeur dépend de l'utilisation de l'adresse m pendant l'intervalle entre la dernière écriture et cette lecture. L'étiquette intervalle $[m,\varphi,\varphi']$ est donc concaténée en tête de la valeur retournée. Le chemin φ est la dernière date d'écriture enregistrée en mémoire. Comme précédemment, le chemin φ' enregistre une double information : (1) l'étiquette α qui permet d'identifier l'ensemble des sous-termes ayant contribué à créer le radical qui effectue l'écriture (interférence fonctionnelle) et (2) la date de lecture de l'adresse m (interférence de la mémoire). Les chemins introduits dans les règles qui manipulent la mémoire sont appelés *chemins menant au cœur du radical* et sont illustrés sur la figure 5.19.

On illustre plus concrètement ces règles de réduction en reprenant l'exemple du terme suivant.

$$M = ((\lambda y.((\lambda\_.(!y^f)^e)^d)^c\ 1^g)^b\ (\mathtt{ref}(0^i))^h)^a$$

Comme dans les sections précédentes, l'étiquette de tête permet d'obtenir un ensemble de lettres $A = \{a,b,c,d,e,f,h,i\}$. De cet ensemble, on déduit le préfixe P des sous-termes de M qui interfèrent dans la valeur : on a $P = ((\lambda y.((\lambda\_.(!y^f)^e)^d)^c\ \Omega)^b\ (\mathtt{ref}(0^i))^h)^a$. Mais cette étiquette de tête donne aussi l'utilisation-mémoire de la réduction : $B = \{[m,\varphi,\varphi']\}$. Dans la suite de cette partie, on montre

que tout terme préfixé par P qui se réduit *en respectant* B vers une valeur se réduit nécessairement vers 0^α.

5.3.1 Propriétés de la réduction étiquetée

De la définition des règles de réduction, on tire une première remarque sur les chemins associés aux adresses dans la mémoire.

Remarque 5.1 *On considère la réduction $M_0/\mu_0 \to M_1/\mu_1 \to \ldots \to M_n/\mu_n$. Pour i tel que $1 \leq i \leq n$, le chemin menant au radical contracté entre M_{i-1} et M_i est noté φ_r^i. Si $m \in dom(\mu_n)$ et $\mu_n(m) = (\varphi,V)$, deux cas sont possibles.*

1. *$m \in dom(\mu_0)$ et pour tout i tel que $0 \leq i \leq n$, on a $\mu_i(m) = (\varphi,V)$.*
2. *Il existe un indice j tel que $\varphi_r^j = \mathsf{Pre}(\varphi)$, φ est un chemin de M_{j-1} et pour tout i tel que $j \leq i \leq n$, on a $\mu_i(m) = (\varphi,V)$.*

Un chemin est associé en mémoire à une adresse au moment de l'ajout ou d'une affectation d'une adresse. De ce fait, si une adresse m appartient au domaine d'une mémoire issue d'une réduction, alors les scenarii pouvant aboutir à cette situation se classent en deux catégories. (1) L'adresse est présente dans la mémoire initiale et elle n'a pas été modifiée au cours du calcul. (2) L'adresse a été créée et/ou modifiée au cours de la réduction. Dans ce cas, si $\mu(m) = (\varphi,V)$, φ est le chemin menant au cœur du radical de (Ref) ou (Assign) impliqué dans la dernière modification. Et l'adresse m n'est plus modifiée jusqu'à la configuration finale.

Les intervalles jouent un rôle particulier parmi les étiquettes. On utilise les notations $T(M/\mu)$, $T(M)$, $T(\mu)$, $T(\alpha)$ et $T(\varphi)$ pour obtenir l'ensemble des intervalles, respectivement, d'une configuration, d'un terme, d'une mémoire, d'une étiquette et d'un chemin. Cette notation est formellement définie de la façon suivante.

$$
\begin{array}{rcl@{\qquad}rcl}
T(x^\alpha) & = & T(\alpha) & T((\lambda x.M)^\alpha) & = & T(M) \cup T(\alpha) \\
T((MN)^\alpha) & = & T(M) \cup T(N) \cup T(\alpha) & T(n^\alpha) & = & T(\alpha) \\
T((M+N)^\alpha) & = & T(M) \cup T(N) \cup T(\alpha) & T(()^\alpha) & = & T(\alpha) \\
T((\mathtt{ref}(M))^\alpha) & = & T(M) \cup T(\alpha) & T((!M)^\alpha) & = & T(M) \cup T(\alpha) \\
T((M{:=}N)^\alpha) & = & T(M) \cup T(N) \cup T(\alpha) & T(m^\alpha) & = & T(m) \cup T(\alpha) \\
T((\mathtt{ifz}\ M\ \mathtt{then}\ N\ \mathtt{else}\ P)^\alpha) & = & T(M) \cup T(N) \cup T(P) \cup T(\alpha) & T(\Omega) & = & \emptyset \\
\multicolumn{3}{r@{\qquad}}{} & & & \\
T(\{m_i \overset{\varphi_i}{\longmapsto} V_i\}_{i \in I}) & = & \bigcup_{i \in I}(T(\varphi_i) \cup T(V_i)) & T(M/\mu) & = & T(M) \cup T(\mu) \\
\multicolumn{3}{r@{\qquad}}{} & & & \\
T(\mathtt{a}) & = & \emptyset & T(\alpha\beta) & = & T(\alpha) \cup T(\beta) \\
T(\lceil\alpha\rceil^{\mathtt{x}}) & = & T(\alpha) & T(\lfloor\alpha\rfloor^{\mathtt{x}}) & = & T(\alpha) \\
T([m,\varphi,\varphi']) & = & \{[m,\varphi,\varphi']\} \cup T(m) \cup T(\varphi) \cup T(\varphi') & T(\alpha|\beta) & = & T(\alpha) \cup T(\beta) \\
\multicolumn{3}{r@{\qquad}}{} & & & \\
T(\varphi\theta\alpha) & = & T(\varphi) \cup T(\alpha) & & &
\end{array}
$$

Cette notation permet d'introduire une deuxième remarque élémentaire portant sur les intervalles.

Remarque 5.2 *On suppose $M_0/\mu_0 \to M_1/\mu_1 \to \ldots \to M_n/\mu_n$. Pour i tel que $1 \leq i \leq n$, le chemin menant au radical contracté entre M_{i-1} et M_i est noté φ_r^i. Si $[m,\varphi,\varphi'] \in T(M_n/\mu_n)$, trois cas sont possibles :*

1. *$[m,\varphi,\varphi'] \in T(M_0/\mu_0)$*
2. *L'adresse m vérifie $m \in dom(\mu_0)$ et $\mu_0(m) = (\varphi,V)$ et il existe un indice $i \in \{1 \ldots n\}$ tel que $\varphi_r^i = \mathsf{Pre}(\varphi')$, φ' est un chemin de M_{i-1}, $\varphi' \in \mathbf{\Phi}_!$ et pour tout j tel que $0 \leq j \leq i$, on a $\mu_j(m) = (\varphi,V)$.*
3. *Il existe deux indices i et i' et une valeur V tels que :*

(a) Le chemin φ est un chemin de M_{i-1} qui appartient à $\mathbf{\Phi}_{\mathtt{ref}} \cup \mathbf{\Phi}_{:=}$ et vérifie $\varphi_r^i = \mathsf{Pre}(\varphi)$. De plus, si $\varphi \in \mathbf{\Phi}_{\mathtt{ref}}$, alors $\varphi_r^i = m$. Et si $\varphi \in \mathbf{\Phi}_{:=}$, alors le chemin φ mène, dans M_{i-1}, à l'adresse m.

(b) Le chemin φ' est un chemin de $M_{i'-1}$ qui appartient à $\mathbf{\Phi}_!$ et qui vérifie $\varphi_r^{i'} = \mathsf{Pre}(\varphi')$. Dans $M_{i'-1}$, le chemin φ' mène à m.

(c) Si j vérifie $i \leq j \leq i'$, alors on a $\mu_j(m) = (\varphi,V)$.

Cette remarque, tirée d'une inspection des règles de réduction, énonce les trois origines possibles d'un intervalle présent dans une configuration issue d'une réduction. (1) Il peut provenir de la configuration initiale. (2) Il peut être créé par une déréférence d'une adresse déjà présente dans la configuration initiale. Dans ce cas, le chemin φ' est le chemin menant au cœur d'un radical contracté par la règle (Deref) au cours de la réduction. On en déduit $\varphi' \in \mathbf{\Phi}_!$. (3) L'intervalle peut être créé par une déréférence d'une adresse qui a été modifiée au cours de la réduction. Dans ce cas, φ est le chemin menant au cœur du radical contracté au moment de l'écriture de m. Deux règles de réduction peuvent modifier une référence : (i) si m est modifiée par (Ref), alors $\varphi \in \mathbf{\Phi}_{\mathtt{ref}}$; (ii) si m est modifiée par (Assign), alors $\varphi \in \mathbf{\Phi}_{:=}$ est le chemin qui mène à l'adresse m. Comme dans le cas précédent, φ' est un chemin menant au cœur d'un radical contracté par la règle (Deref) au cours de la réduction. On en déduit $\varphi' \in \mathbf{\Phi}_!$. Comme nous le remarquions plus tôt, l'adresse m n'est pas modifiée entre la date d'écriture φ et la date de lecture φ'.

Comme annoncé précédemment, le langage que nous avons introduit exploite la propriété d'irréversibilité évoquée dans la section 1.3. Cette propriété est conservée dans le cadre présent.

Théorème 5.4 (Irréversibilité) *On suppose $M_0/\mu_0 \to M_1/\mu_1 \to \ldots \to M_n/\mu_n$. Pour i tel que $1 \leq i \leq n$, le chemin menant au radical contracté entre M_{i-1} et M_i est noté φ_r^i. Si $i \leq j$, le chemin φ_r^i ne préfixe aucun chemin de M_j.*

Preuve : On prouve ce résultat de la même façon que pour le théorème 1.2. On utilise en particulier le lemme 5.1 mentionné ci-dessous et qui correspond au lemme 1.2. □

A chaque étape de réduction, le chemin menant au radical disparaît, et ne peut pas réapparaître dans un terme de la suite de la réduction. Cette propriété, qui est bien entendu fausse en l'absence d'étiquettes, exploite la relation $\preceq$ sur les étiquettes que l'on a introduite dans la partie 1.3 et qu'on adapte ci-dessous à la syntaxe des étiquettes du λ_m-calcul.

$\alpha \preceq \alpha$	
$\alpha \preceq \beta$	si $\alpha \preceq \gamma$ et $\gamma \preceq \beta$
$\alpha \preceq \alpha_1\alpha_2$	si $\alpha \preceq \alpha_i$ pour $i \in \{1,2\}$
$\alpha \preceq \lceil\alpha\rceil^{\mathtt{x}}$	pour $\mathtt{x} \in \{\mathtt{b},\mathtt{p},\mathtt{i},\mathtt{c},\mathtt{w}\}$
$\alpha \preceq \lfloor\alpha\rfloor^{\mathtt{x}}$	pour $\mathtt{x} \in \{\mathtt{b},\mathtt{p},\mathtt{i},\mathtt{c},\mathtt{w}\}$
$\alpha \preceq \alpha_1\vert\alpha_2$	si $\alpha \preceq \alpha_i$ pour $i \in \{1,2\}$
$\alpha \preceq [m,\varphi,\varphi']$	si $\alpha \preceq m$ ou $\alpha \preceq \varphi$ ou $\alpha \preceq \varphi'$
$\alpha \preceq \alpha_0\theta_1\alpha_1\cdots\theta_n\alpha_n$	si $\alpha \preceq \alpha_i$ pour $i \in \{0,n\}$

La relation $\preceq$ est un ordre bien fondé sur les étiquettes et les chemins. La relation d'ordre stricte associée $\prec$ est exploitée dans le lemme suivant qui est la propriété essentielle sur laquelle repose le théorème d'irréversibilité.

Lemme 5.1 *1. Si $R/\mu \xrightarrow{\kappa} R'/\mu'$, alors on a $\tau(R) \prec \tau(R')$.*
2. Si $M/\mu \xrightarrow{\kappa} M'/\mu'$, alors on a $\tau(M) \preceq \tau(M')$.

Preuve : Ce résultat se prouve en inspectant les différentes règles de réduction. □

L'étiquette de tête d'un terme réduit contient l'étiquette du terme avant réduction. Si le terme considéré est le radical, alors l'étiquette de tête du contractum contient strictement l'étiquette de tête du radical.

Un corollaire du théorème d'irréversibilité est la correction du choix des adresses. Pour prouver et exploiter ce résultat par la suite, on définit l'invariant suivant.

Invariant 5.1 *La configuration M/μ vérifie l'invariant $\mathcal{L}$, ce que l'on note $\mathcal{L}(M,\mu)$, si et seulement si pour toute réduction $M/\mu \twoheadrightarrow E[(\mathtt{ref}(V))^\alpha]/\mu'$ on a $\sigma(E[\,])\alpha \notin dom(\mu')$.*

Cet invariant signifie qu'au moment de la création d'une adresse, l'adresse choisie est bien *fraîche*, c'est-à-dire qu'elle n'appartient pas au domaine de la mémoire.

Corollaire 5.1 (Correction du choix des adresses) *Pour tout terme M, on a $\mathcal{L}(M,\emptyset)$.*

En partant d'une mémoire initiale vide, à chaque application de la règle (Ref), l'adresse choisie est bien *fraîche* puisqu'elle n'appartient pas au domaine de la mémoire. L'adresse choisie ne dépend que du chemin menant à la racine. Cette technique est intéressante pour deux raisons. D'une part, elle résout le problème de non-reproductibilité des réductions que nous avons évoqué précédemment. D'autre part, cette technique est aussi utile pour comparer les réductions de deux termes M_1 et M_2 qui ne diffèrent que sur un ensemble de sous-termes. Pour surmonter ce problème, Pottier et Simonet ajoutent au langage une construction spécifique $\langle N_1|N_2\rangle$. Avec cette construction, M_1 et M_2 sont codés dans un seul terme et les sous-termes communs de M_1 et M_2 sont factorisés. De ce fait, les adresses créées en dehors des crochets sont partagées par les deux termes. Dans le λ_m-calcul, le choix de l'adresse utilisé offre une solution, de notre point de vue, plus simple : si un radical $(\mathtt{ref}(V))^\beta$ est contracté dans une partie commune à M_1 et M_2, le chemin menant à ce radical est le même dans les deux cas, ce qui signifie que dans les deux réductions, l'adresse créée aura le même nom. On peut donc comparer directement les deux réductions.

L'utilisation du théorème d'irréversibilité et de la remarque 5.2 fournit la propriété suivante sur les intervalles créés au cours d'une réduction.

Lemme 5.2 *On considère la réduction $\mathcal{R} : M_0/\emptyset \to M_1/\mu_1 \to \ldots \to M_n/\mu_n$ où $T(M_0/\emptyset) = \emptyset$. Pour $1 \leq i \leq n$, on appelle φ_r^i le chemin menant au radical contracté entre M_{i-1} et M_i. On pose $\Phi_n = C(T(M_n/\mu_n))$.*

1. *Si φ est un chemin de Φ_n, alors il existe un unique indice i tel que $\varphi_r^i = \mathsf{Pre}(\varphi)$.*
2. *Pour i tel que $1 \leq i \leq n$, il existe au plus un chemin φ de Φ_n qui vérifie $\varphi_r^i = \mathsf{Pre}(\varphi)$.*

Preuve : On montre successivement les deux points.

1. Si $\varphi \in \Phi_n$, la remarque 5.2 permet d'obtenir l'existence d'un indice i tel que $\varphi_r^i = \mathsf{Pre}(\varphi)$. S'il existe un deuxième indice j tel que $1 \leq j \leq n$ et $\varphi_r^j = \mathsf{Pre}(\varphi)$, alors, en utilisant le théorème 5.4, on obtient $i = j$. D'où l'unicité de l'indice.
2. Soient φ et φ' deux chemins de Φ_n qui vérifient $\varphi_r^i = \mathsf{Pre}(\varphi)$ et $\varphi_r^i = \mathsf{Pre}(\varphi')$. En utilisant la remarque 5.2, on obtient un indice j tel que $1 \leq j \leq n$ tel que $\varphi_r^j = \mathsf{Pre}(\varphi)$ et φ est un chemin de M_{j-1}. De même, on obtient un indice j' tel que $1 \leq j' \leq n$, $\varphi_r^{j'} = \mathsf{Pre}(\varphi')$ et φ' est un chemin de $M_{j'-1}$. En utilisant le théorème 5.4, on obtient $j = j' = i$. Les chemins φ et φ' sont donc des chemins d'un même terme qui vérifient $\varphi_r^i = \mathsf{Pre}(\varphi) = \mathsf{Pre}(\varphi')$. On en déduit donc $\varphi = \varphi'$. □

Au cours d'une réduction $\mathcal{R}$ partant d'une configuration sans intervalle et de mémoire vide, pour tout chemin φ présent dans un intervalle de la configuration finale, il correspond un unique chemin menant à un radical R contracté au cours de $\mathcal{R}$; plus précisément φ mène au cœur de R. Inversement, un chemin menant à un radical φ_r^i ne peut être associé par Pre qu'à au plus un chemin de $C(T(M_n/\mu_n))$. Ce résultat prouve que les chemins menant au cœur d'un radical sont liés de façon injective avec les chemins menant aux radicaux. Ceci signifie que, comme ces derniers, on peut les utiliser comme des *dates* de la réduction.

$$(\beta_{\mathrm{B}}) \qquad ((\lambda x.M)^{\alpha}V)^{\beta}/\mu/\Phi \xrightarrow{\kappa}_B \beta \cdot \lceil\alpha\rceil^{\mathtt{b}} \cdot M\{x \backslash \lfloor\alpha\rfloor^{\mathtt{b}} \cdot V\}/\mu/\Phi$$

$$(\mathrm{Plus}_{\mathrm{B}}) \qquad \frac{\mathbf{n_1} + \mathbf{n_2} = \mathbf{n}}{(n_1^{\alpha} + n_2^{\beta})^{\gamma}/\mu/\Phi \xrightarrow{\kappa}_B n^{\gamma\lceil\alpha|\beta\rceil^{\mathtt{p}}}/\mu/\Phi}$$

$$(\text{Ifz-true}_{\mathrm{B}}) \qquad \frac{\mathbf{n} = 0}{(\mathtt{ifz}\ n^{\alpha}\ \mathtt{then}\ M\ \mathtt{else}\ N)^{\beta}/\mu/\Phi \xrightarrow{\kappa}_B \beta \cdot \lceil\alpha\rceil^{\mathtt{i}} \cdot M/\mu/\Phi}$$

$$(\text{Ifz-false}_{\mathrm{B}}) \qquad \frac{\mathbf{n} \neq 0}{(\mathtt{ifz}\ n^{\alpha}\ \mathtt{then}\ M\ \mathtt{else}\ N)^{\beta}/\mu/\Phi \xrightarrow{\kappa}_B \beta \cdot \lceil\alpha\rceil^{\mathtt{i}} \cdot N/\mu/\Phi}$$

$$(\mathrm{Ref}^{o}_{\mathrm{B}}) \qquad \frac{\varphi = \kappa\beta\mathtt{ref}\alpha \qquad B(m,\varphi) = \emptyset \qquad m = \kappa\beta \qquad \alpha = \tau(V)}{(\mathtt{ref}(V))^{\beta}/\mu/\Phi \xrightarrow{\kappa}_B m^{\lceil\beta\rceil^{\mathtt{c}}}/(\mu; m \overset{\varphi}{\longmapsto} V)/\Phi}$$

$$(\mathrm{Ref}^{i}_{\mathrm{B}}) \qquad \frac{\varphi = \kappa\beta\mathtt{ref}\alpha \qquad B(m,\varphi) \neq \emptyset \qquad m = \kappa\beta \qquad \alpha = \tau(V)}{(\mathtt{ref}(V))^{\beta}/\mu/\Phi \xrightarrow{\kappa}_B m^{\lceil\beta\rceil^{\mathtt{c}}}/(\mu; m \overset{\varphi}{\longmapsto} V)/\Phi \cup \{\varphi\}}$$

$$(\mathrm{Deref}^{o}_{\mathrm{B}}) \qquad \frac{\varphi' = \kappa\beta!\alpha \qquad [m,\varphi,\varphi'] \notin B}{(!m^{\alpha})^{\beta}/(\mu; m \overset{\varphi}{\longmapsto} V)/\Phi \xrightarrow{\kappa}_B \beta \cdot [m,\varphi,\varphi'] \cdot V/(\mu; m \overset{\varphi}{\longmapsto} V)/\Phi}$$

$$(\mathrm{Deref}^{i}_{\mathrm{B}}) \qquad \frac{\varphi' = \kappa\beta!\alpha \qquad [m,\varphi,\varphi'] \text{ est } (B,\Phi)\text{-actif}}{(!m^{\alpha})^{\beta}/(\mu; m \overset{\varphi}{\longmapsto} V)/\Phi \xrightarrow{\kappa}_B \beta \cdot [m,\varphi,\varphi'] \cdot V/(\mu; m \overset{\varphi}{\longmapsto} V)/\Phi \cup \{\varphi'\}}$$

$$(\mathrm{Assign}^{o}_{\mathrm{B}}) \qquad \frac{\begin{array}{c}\forall t \in B(m,\varphi)\ .\ t \text{ est } (B,\Phi)\text{-inactif} \\ \varphi' = \kappa\beta{:=_1}\alpha \qquad B(m,\varphi') = \emptyset\end{array}}{(m^{\alpha}{:=}V)^{\beta}/(\mu; m \overset{\varphi}{\longmapsto} V')/\Phi \xrightarrow{\kappa}_B ()^{\lceil\beta\rceil^{\mathtt{w}}}/(\mu; m \overset{\varphi'}{\longmapsto} V)/\Phi}$$

$$(\mathrm{Assign}^{i}_{\mathrm{B}}) \qquad \frac{\begin{array}{c}\forall t \in B(m,\varphi)\ .\ t \text{ est } (B,\Phi)\text{-inactif} \\ \varphi' = \kappa\beta{:=_1}\alpha \qquad B(m,\varphi') \neq \emptyset\end{array}}{(m^{\alpha}{:=}V)^{\beta}/(\mu; m \overset{\varphi}{\longmapsto} V')/\Phi \xrightarrow{\kappa}_B ()^{\lceil\beta\rceil^{\mathtt{w}}}/(\mu; m \overset{\varphi'}{\longmapsto} V)/\Phi \cup \{\varphi'\}}$$

$$(\mathrm{Ctx}_{\mathrm{B}}) \qquad \frac{M/\mu/\Phi \xrightarrow{\sigma([\,])}_B M'/\mu'/\Phi'}{E[M]/\mu/\Phi \rightarrow_B E[M']/\mu'/\Phi'}$$

FIG. 5.21 – *Réduction* $\rightarrow_B$ *et* $\xrightarrow{\kappa}_B$ $(\kappa \in \mathbf{K})$

5.3.2 Réduction respectant une utilisation-mémoire

On montre dans cette section que les étiquettes employées dans le λ_m-calcul donnent une information correcte de l'utilisation de la mémoire. Pour ce faire, on définit une nouvelle réduction $\rightarrow_B$ paramétrée par une utilisation-mémoire B. Cette réduction impose la conformité de l'utilisation des adresses vis-à-vis des intervalles présents dans B. Intuitivement, si $[m,\varphi,\varphi'] \in B$ et si la date φ est passée, alors l'adresse m appartient au domaine de la mémoire. Et toute modification de la valeur associée à m est interdite tant que la date φ' n'est pas passée.

Plus concrètement, la réduction $\rightarrow_B$ porte sur des configurations étendues $M/\mu/\Phi$ constituées d'un terme M, d'une mémoire μ et d'un ensemble de chemin Φ appelé *passé*. Cet ensemble Φ contient les chemins de B qui sont intervenus précédemment dans la réduction. En reprenant l'analogie temporelle, cet ensemble contient effectivement les dates d'écriture et de lecture d'adresses qui sont déjà passées. Les chemins de B qui n'apparaissent pas dans Φ peuvent être interprétés comme des dates futures. On définit la notion d'**intervalle** (B,Φ)***-actif*** qui sera utilisée par la suite : $[m,\varphi,\varphi']$ est (B,Φ)-actif si et seulement si $[m,\varphi,\varphi'] \in B$, $\varphi \in \Phi$ et $\varphi' \notin \Phi$. Si un intervalle n'est pas (B,Φ)-actif, il est (B,Φ)-inactif. Par souci de concision, on utilise dans les règles de réduction la notation suivante : $B(m,\varphi) = \{[m,\varphi,\varphi'] \in B\}$. Les règles de réductions de $\rightarrow_B$ et $\xrightarrow{\kappa}_B$ sont données par la figure 5.21. Les réductions (β_{B}), $(\mathrm{Plus}_{\mathrm{B}})$, $(\mathrm{Ifz}_{\mathrm{B}})$ et $(\mathrm{Ctx}_{\mathrm{B}})$ sont inchangées : elles ne modi-

fient pas le passé Φ. L'ensemble B contient les intervalles qui décrivent les utilisations de certaines adresses. La réduction $\xrightarrow{\kappa}_B$ contraint au respect de ces utilisations. Plus concrètement, en reprenant l'analogie temporelle évoquée précédemment, si $[m,\varphi,\varphi'] \in B$, l'adresse m est protégée entre les dates φ et φ'. Si $[m,\varphi,\varphi']$ est (B,Φ)-actif, c'est-à-dire si $\varphi \in \Phi$ et $\varphi' \notin \Phi$, l'adresse m ne peut subir une affectation. Cette protection est assurée par la condition "$\forall t \in B(m,\varphi).t$ est (B,Φ)-inactif" des règles ($\text{Assign}^i_{\text{B}}$) et ($\text{Assign}^o_{\text{B}}$). Par ailleurs, pour chacun des termes faisant intervenir la mémoire, il existe deux règles de réduction qui traitent séparément les cas $B(m,\varphi) = \emptyset$ et $B(m,\varphi) \neq \emptyset$. Plaçons-nous dans le cas d'une référence $(\texttt{ref}(V))^\beta$. Si $B(m,\varphi) \neq \emptyset$, alors le chemin φ qui mène au cœur du radical intervient dans un intervalle $t = [m,\varphi,\varphi']$ de B. La règle (Ref^i_{B}) s'applique. Ce chemin est ajouté au passé Φ. La date de début de protection de m est donc passée. En d'autres termes, l'intervalle t devient (B,Φ)-actif et l'adresse m ne peut donc plus être modifiée avant que le chemin φ' n'apparaisse. Si $B(m,\varphi) = \emptyset$, aucune adresse n'est protégée à partir de la date φ. Cette date n'est donc pas une date d'intérêt : elle n'est pas ajoutée à Φ. Le cas de l'affectation est similaire au cas de la référence. Considérons le cas de la déréférence. Comme précédemment, si $[m,\varphi,\varphi'] \notin B$, alors la date φ' ne libère aucune adresse. Le passage de cette date n'a donc pas d'effet. La règle ($\text{Deref}^o_{\text{B}}$) n'ajoute donc pas φ' à Φ. Si $[m,\varphi,\varphi'] \in B$, le chemin φ' correspond à une date de fin de protection de l'adresse m. Cette date est donc ajoutée par la règle ($\text{Deref}^i_{\text{B}}$) à Φ et l'intervalle $[m,\varphi,\varphi']$ devient inactif. On dira que M/μ se réduit vers N/ν en respectant B si et seulement si $M/\mu/\emptyset \xrightarrow{\kappa}\!\!\!\!\rightarrow_B N/\nu/\Phi$.

Intuitivement, la définition des règles de calcul qui font intervenir la mémoire est telle que seuls les chemins présents dans B sont ajoutés au passé. Cette *spécialisation* des règles vis-à-vis de B a pour conséquence de doubler les règles pour la référence, l'affectation et la déréférence. On aurait pu éviter cette complexité en ajoutant systématiquement les chemins au passé, en ne faisant pas la distinction de l'appartenance du chemin dans B. La raison de ce choix, a priori plus complexe, est que nous souhaitons comparer les réductions de deux termes : si on reprend l'exemple utilisé précédemment, nous voulons comparer les réductions $\mathcal{R}$ et $\mathcal{R}'$. Cette dernière réduction produit un effet de bord supplémentaire par rapport à $\mathcal{R}$, en créant une adresse m_2. Si nous avions décidé d'ajouter systématiquement tous les chemins associés aux opérations sur la mémoire au passé, les passés associés aux réductions $\mathcal{R}$ et $\mathcal{R}'$ auraient divergé. Ceci aurait rendu la comparaison des réductions moins aisée. Par contraste, nous avons choisi de n'ajouter au passé que des chemins significatifs, c'est-à-dire des chemins correspondant aux intervalles présents dans B. Ce choix simplifie la synchronisation entre les réductions $\mathcal{R}$ et $\mathcal{R}'$ car les passés de ces réductions sont comparables.

On utilise un invariant pour formaliser certaines intuitions sur les intervalles que nous avons évoquées précédemment.

Invariant 5.2 *L'ensemble B vérifie l'invariant $\mathcal{B}$, ce que l'on note $\mathcal{B}(B)$, si et seulement si les propriétés suivantes sont vérifiées :*

1. *Si $[m,\varphi,\varphi'] \in B$, alors $\varphi \in \mathbf{\Phi}_{\texttt{ref}} \cup \mathbf{\Phi}_{:=}$ et $\varphi' \in \mathbf{\Phi}_!$.*
2. *Si $[m,\varphi,\psi] \in B$ et $[m',\varphi,\psi'] \in B$, alors $m = m'$.*
3. *Si $[m,\varphi,\psi] \in B$ et $[m',\varphi',\psi] \in B$, alors $m = m'$ et $\varphi = \varphi'$.*

Le premier point de l'invariant indique qu'une date d'écriture d'un intervalle est nécessairement un chemin dont le dernier nœud est une référence ou une affectation. De même, la date de lecture est nécessairement un chemin dont le dernier nœud est une déréférence. Ce point exprime bien l'interprétation des intervalles donnée précédemment : φ (respectivement φ') est un chemin menant au cœur d'un radical de référence ou d'affectation (resp. déréférence). Le deuxième point indique que le premier chemin d'un intervalle est lié de façon injective avec l'adresse de l'intervalle. Le troisième point indique que le deuxième chemin est lié de façon injective avec le premier chemin et

l'adresse de l'intervalle. Ces deux derniers points formalisent l'intuition selon laquelle un chemin menant au cœur d'un radical correspond de façon univoque à une date du calcul. Comme une date ne peut pas survenir deux fois, un chemin ne peut pas être lié à deux adresses différentes.

Bien entendu, cet invariant n'est pas vrai en général puisque les éléments de B peuvent être arbitraires. Cependant, cet invariant est vrai si les éléments de B ont été créés par un calcul, comme le montre le résultat suivant.

Lemme 5.3 *Soit M un terme tel que $T(M) = \emptyset$. Si $M/\emptyset \twoheadrightarrow V/\nu$ et $B = T(V/\nu)$ alors $\mathcal{B}(B)$.*

Preuve : Le premier point de $\mathcal{B}$ est obtenu directement à l'aide de la remarque 5.2. La réduction de M à M' peut s'écrire $M/\emptyset = M_0/\emptyset \to M_1/\mu_1 \to \ldots \to M_n/\mu_n = M'/\mu'$. Pour $i \in \{1 \ldots n\}$, on note φ_r^i le chemin menant au radical contracté entre M_{i-1} et M_i. On suppose $[m,\varphi,\psi] \in B$. Comme $T(M) = \emptyset$, on obtient, en utilisant la remarque 5.2, deux indices i et j tels que $\varphi = \mathsf{Pre}(\varphi_r^i)$, φ est un chemin de M_{i-1}, $\psi = \mathsf{Pre}(\varphi_r^j)$, ψ est un chemin de M_{j-1} et pour tout $l \in \{i \ldots j\}$, on a $\mu_l(m) = (\varphi,V)$. Si $[m',\varphi,\psi'] \in B$, on obtient de même un indice i' tel que $\varphi = \mathsf{Pre}(\varphi_r^{i'})$ et φ est un chemin de $M_{i'-1}$. En utilisant le lemme 5.4, on obtient $i = i'$. Deux cas sont possibles.

- Si $\varphi \in \mathbf{\Phi}_{\mathtt{ref}}$, la remarque 5.2 implique que $\varphi_r^i = m = m'$.
- Si $\varphi_r^i \in \mathbf{\Phi}_{:=}$, la remarque 5.2 implique que φ est un chemin de M_{i-1} qui mène à la fois à m et m'. De là, on obtient $m = m'$.

Le deuxième point de l'invariant est donc prouvé. Si $[m',\varphi',\psi] \in B$, on obtient, en utilisant la remarque 5.2, deux indices i' et j' tels que $\varphi' = \mathsf{Pre}(\varphi_r^{i'})$, φ' est un chemin de $M_{i'-1}$, $\psi = \mathsf{Pre}(\varphi_r^{j'})$, ψ est un chemin de $M_{j'-1}$ et pour tout $l \in \{i' \ldots j'\}$, on a $\mu_l(m) = (\varphi',V')$. En utilisant le lemme 5.4, on obtient $j = j'$. De là, on obtient $\varphi = \varphi'$. En utilisant le point précédent, on en déduit $m = m'$. □

Si la mémoire de la configuration initiale est vide et si le terme initial ne contient pas d'intervalle, alors les intervalles présents dans le terme final ont été calculés au cours de la réduction. Cette utilisation-mémoire vérifie l'invariant $\mathcal{B}$.

On montre maintenant le résultat central de cette section : les étiquettes du λ_m-calcul donnent une information correcte de l'utilisation de la mémoire. Ce résultat s'énonce formellement de la façon suivante.

Lemme 5.4 *Soit M un terme tel que $T(M) = \emptyset$. Si $M/\emptyset \twoheadrightarrow V/\nu$ et $B = T(\tau(V))$, alors $M/\emptyset/\emptyset \twoheadrightarrow_B V/\nu/C(B)$.*

Preuve : La réduction de M à V peut s'écrire : $M/\emptyset = M_0/\emptyset \to M_1/\mu_1 \to \ldots \to M_n/\mu_n = V/\nu$. L'utilisation du lemme 5.3 prouve $\mathcal{B}(B)$. Pour $i \in \{1 \ldots n\}$, on note φ_r^i le chemin menant au radical contracté entre M_{i-1} et M_i. On définit récursivement les ensembles $\{L_i\}_{i\in\{0\ldots n\}}$ de la façon suivante.

- $L_0 = \emptyset$
- Pour $i \in \{1 \ldots n\}$, $L_i = L_{i-1} \cup \{\varphi \in C(B) \mid \varphi_r^i = \mathsf{Pre}(\varphi)\}$.

La propriété $\mathcal{P}(i)$ est définie de la façon suivante : la propriété $\mathcal{P}(i)$ est vraie si et seulement si $M_0/\emptyset/\emptyset \to_B M_1/\mu_1/\Phi_1 \to_B \ldots \to_B M_i/\mu_i/\Phi_i$ et $\forall j \leq i.\Phi_j = L_j$. On montre par récurrence cette propriété pour $i \in \{0 \ldots n\}$. Cette propriété est trivialement vraie pour $i = 0$. On suppose $\mathcal{P}(i)$. On procède par cas sur la réduction entre M_i et M_{i+1}.

1. Si $M_i = E[(\mathtt{ref}(W))^\beta]$, la réduction considérée est $M_i/\mu_i \to E[\lceil\beta\rceil^{\mathtt{b}}.m]/\mu_{i+1}$ où μ_{i+1} vérifie $\mu_{i+1} = (\mu_i; m \overset{\varphi_0}{\longmapsto} W)$ avec $\alpha = \tau(W)$, $\varphi_0 = \varphi_r^{i+1}\mathtt{ref}\alpha$, et $m = \varphi_r^{i+1}$. Deux cas sont à considérer.
   (a) Si $B(m,\varphi_0) = \emptyset$. Soit ψ un chemin de $C(B)$ qui vérifie $\varphi_r^{i+1} = \mathsf{Pre}(\psi)$. En utilisant le lemme 5.2, on obtient $\psi = \varphi_0$, ce qui contredit $B(m,\varphi_0) = \emptyset$. On en déduit $L_{i+1} = L_i$. En utilisant $\mathcal{P}(i)$, on obtient donc $M_i/\mu_i/\Phi_i \to_B M_{i+1}/\mu_{i+1}/\Phi_{i+1}$ avec $L_{i+1} = \Phi_{i+1}$.

(b) Si $B(m,\varphi_0) \neq \emptyset$, alors on a $\Phi_{i+1} = \Phi_i \cup \{\varphi_0\}$. Soit ψ un chemin de $C(B)$ tel que $\varphi_r^{i+1} = \mathsf{Pre}(\psi)$. De la même façon que précédemment, on montre $\psi = \varphi_0$. De là, on a $L_{i+1} = L_i \cup \{\varphi_0\}$. En utilisant $\mathcal{P}(i)$, on obtient donc $M_i/\mu_i/\Phi_i \rightarrow_B M_{i+1}/\mu_{i+1}/\Phi_{i+1}$ avec $L_{i+1} = \Phi_{i+1}$.

2. Si $M_i = E[(m^\alpha{:=}W)^\beta]$, la réduction considérée est $M_i/\mu_i \rightarrow E[()^{\lceil\beta\rceil^\varpi}]/\mu_{i+1}$ où on utilise les notations $\varphi_1 = \varphi_r^{i+1}{:=}_1\alpha$, $\mu_i = (\nu; m \overset{\varphi_0}{\longmapsto} W_0)$ et $\mu_{i+1} = (\nu; m \overset{\varphi_1}{\longmapsto} W)$. Soit $[m,\varphi_0,\psi]$ un intervalle de $B(m,\varphi_0)$. On veut montrer que $[m,\varphi_0,\psi]$ est (B,Φ_i)-inactif. Comme la mémoire initiale est vide et $T(M_0/0) = \emptyset$, en utilisant la remarque 5.2, on obtient deux indices i_1 et i_2 tels que $\varphi_r^{i_1} = \mathsf{Pre}(\varphi_0)$, $\varphi_r^{i_2} = \mathsf{Pre}(\psi)$ et pour tout $j \in \{i_1,\ldots,i_2\}$, on a $\mu_j(m) = (\varphi_0,W_0')$. De même, comme la mémoire initiale est vide, en utilisant la remarque 5.1, on obtient un indice i_0 tel que $\varphi_r^{i_0} = \mathsf{Pre}(\varphi_0)$ et pour tout $j \in \{i_0,\ldots,i\}$, on a $\mu_j(m) = (\varphi_0,W_0)$. L'égalité $\varphi_r^{i_0} = \varphi_r^{i_1}$ implique, d'après le théorème 5.4, l'égalité $i_0 = i_1$ et donc $W_0' = W_0$. Comme $\mu_{i+1}(m) \neq (\varphi_0,W_0)$, on en déduit $i_2 \leq i$. Comme $\varphi_r^{i_2} = \mathsf{Pre}(\psi)$, par définition de L_{i_2}, on a $\psi \in L_{i_2} \subseteq L_i$. Par hypothèse de récurrence $\mathcal{P}(i)$, on obtient $\psi \in \Phi_i$. L'intervalle $[m,\varphi_0,\psi]$ est donc (B,Φ_i)-inactif. Deux cas sont maintenant à considérer.

(a) Si $B(m,\varphi_1) = \emptyset$, alors $\Phi_{i+1} = \Phi_i$. Soit ψ un chemin de $C(B)$ qui vérifie $\varphi_r^{i+1} = \mathsf{Pre}(\psi)$. En utilisant le lemme 5.2, on obtient $\psi = \varphi_1$, ce qui contredit $B(m,\varphi_1) = \emptyset$. On en déduit $L_{i+1} = L_i$. En utilisant $\mathcal{P}(i)$, on obtient donc $M_i/\mu_i/\Phi_i \rightarrow_B M_{i+1}/\mu_{i+1}/\Phi_{i+1}$ avec $L_{i+1} = \Phi_{i+1}$.

(b) Si $B(m,\varphi_1) \neq \emptyset$, alors $\Phi_{i+1} = \Phi_i \cup \{\varphi_1\}$. Soit $\psi \in C(B)$ tel que $\varphi_r^{i+1} = \mathsf{Pre}(\psi)$. De la même façon que précédemment, on montre $\psi = \varphi_1$. De là, on a $L_{i+1} = L_i \cup \{\varphi_1\}$. En utilisant $\mathcal{P}(i)$, on obtient donc $M_i/\mu_i/\Phi_i \rightarrow_B M_{i+1}/\mu_{i+1}/\Phi_{i+1}$ avec $L_{i+1} = \Phi_{i+1}$.

3. Si $M_i = E[(!m^\alpha)^\beta]$, la réduction considérée est $M_i/\mu_i \rightarrow_B E[\beta \cdot [m,\varphi_0,\varphi_1] \cdot V_0]/\mu_{i+1}$ avec $\varphi_1 = \varphi_r^{i+1}\mathtt{ref}\alpha$, $\mu_i = (\nu; m \overset{\varphi_0}{\longmapsto} W_0)$ et $\mu_{i+1} = \mu_i$. Deux cas sont à considérer.

(a) Si $[m,\varphi_0,\varphi_1] \notin B$, alors $\Phi_{i+1} = \Phi_i$. Soit ψ un chemin de $C(B)$ qui vérifie $\varphi_r^{i+1} = \mathsf{Pre}(\psi)$. En utilisant le lemme 5.2, on obtient $\psi = \varphi_1$. Comme $\varphi_1 \in \mathbf{\Phi}_!$, φ_1 est présent dans B dans un intervalle de la forme $[m',\psi',\varphi_1]$. L'invariant $\mathcal{B}(B)$ donne alors $m' = m$ et $\psi' = \varphi_0$ ce qui apporte une contradiction à l'hypothèse $[m,\varphi_0,\varphi_1] \notin B$. On en déduit $L_{i+1} = L_1$. En utilisant $\mathcal{P}(i)$, on obtient donc $M_i/\mu_i/\Phi_i \rightarrow_B M_{i+1}/\mu_{i+1}/\Phi_{i+1}$ avec $L_{i+1} = \Phi_{i+1}$.

(b) Si $[m,\varphi_0,\varphi_1] \in B$, alors $\Phi_{i+1} = \Phi_i \cup \{\varphi_1\}$. Soit ψ un chemin de $C(B)$ qui vérifie $\varphi_r^{i+1} = \mathsf{Pre}(\psi)$. Comme dans le cas précédent, on obtient $\psi = \varphi_1$. De là, on obtient $L_{i+1} = L_i \cup \{\varphi_1\}$. En utilisant $\mathcal{P}(i)$, on obtient donc $M_i/\mu_i/\Phi_i \rightarrow_B M_{i+1}/\mu_{i+1}/\Phi_{i+1}$ avec $L_{i+1} = \Phi_{i+1}$.

4. Les autres cas sont élémentaires. □

Si une réduction aboutit à une valeur V dont tous les intervalles ont été calculés, alors la même configuration initiale se réduit vers la même configuration finale en respectant les intervalles présents dans l'étiquette de tête de V. On en déduit que les étiquettes donnent une information suffisante sur l'utilisation de la mémoire. Ce résultat de cohérence justifie la dénomination de "réduction respectant une utilisation-mémoire".

5.3.3 Non-interférence

Nous nous penchons dans cette section sur la dernière phase du raisonnement qui aboutit au théorème de non-interférence. On considère ici une configuration $M/\emptyset$ qui se réduit vers une valeur V. Comme dans les parties précédentes consacrées à la propriété de stabilité, on obtient, dans un premier temps, un préfixe P de M à partir de l'étiquette de tête de V. Cette étiquette fournit aussi une utilisation-mémoire $B = T(\tau(V))$. Dans un second temps, on considère un terme N préfixé

par P. On montre que si N se réduit vers V' en *respectant l'utilisation-mémoire* B, alors V et V' admettent un préfixe commun, non réduit à Ω. Ceci implique que les observables de V et V' sont égaux. La définition de l'observable d'une valeur étend la définition introduite dans le section précédente.

$$\begin{array}{rlrl} \mathcal{O}((\lambda x.M)^\alpha) &= (\lambda x.\Omega)^\alpha & \mathcal{O}(n^\alpha) &= n^\alpha \\ \mathcal{O}(m^\alpha) &= m^\alpha & \mathcal{O}(()^\alpha) &= ()^\alpha \end{array}$$

On note que les observables d'une valeur qui n'est pas une abstraction est égale à la valeur. On s'inspire de la définition de la non-interférence introduite dans le cadre du λ-calcul pour adapter cette définition au λ_m-calcul.

Définition 5.3 (Non-interférence) *On suppose $\mathcal{R} : M/\emptyset \twoheadrightarrow V/\mu$ et $B = T(\tau(V))$. Le sous-terme $(C[\,],N)$ du terme M n'interfère pas dans $\mathcal{R}$ si et seulement si, pour tout terme N', la réduction $C[N']/\emptyset/\emptyset \twoheadrightarrow_B V'/\mu/\Phi$ implique la relation $\mathcal{O}(V) = \mathcal{O}(V')$.*

Comme nous l'avons vu au moment de l'étude des exemples de la section 5.2, dans un calcul muni d'effet de bord, les interférences liées à l'utilisation de la mémoire s'ajoutent aux interférences fonctionnelles déjà présentes dans le λ-calcul ou le λ-calcul par valeur. La définition de la non-interférence tient compte de ces deux composantes. Comme dans le λ-calcul, la non-interférence fonctionnelle est capturée par le relation $\mathcal{O}(V) = \mathcal{O}(V')$. Le fait de ne considérer que des réductions qui respectent B permet de prendre en ligne de compte la non-interférence sur la mémoire.

Dans les sections précédentes, on obtenait le préfixe de stabilité de M en effaçant dans M les sous-termes dont l'étiquette de tête contenait des lettres absentes de $A = |\tau(V)|$. Ici, en plus de considérer cet ensemble de lettres, on utilise aussi les intervalles de $B = T(\tau(V))$. Le préfixe de M est obtenu par la fonction $[\![\cdot]\!]_B^A$ qui est définie de la façon suivante.

$$\begin{array}{rcll} [\![\Omega]\!]_B^A &=& \Omega & \\ [\![M]\!]_B^A &=& \Omega \quad \text{où } \tau(M) = \alpha & \text{si } |\alpha| \not\subseteq A \text{ ou } T(\alpha) \not\subseteq B \\ \left.\begin{array}{r} [\![x^\alpha]\!]_B^A \\ [\![(\lambda x.M)^\alpha]\!]_B^A \\ [\![(MN)^\alpha]\!]_B^A \\ [\![()^\alpha]\!]_B^A \\ [\![n^\alpha]\!]_B^A \\ [\![(M+N)^\alpha]\!]_B^A \\ [\![(\mathtt{ref}(M))^\alpha]\!]_B^A \\ [\![(M{:=}N)^\alpha]\!]_B^A \\ [\![(!M)^\alpha]\!]_B^A \\ [\![m^\alpha]\!]_B^A \\ [\![(\mathtt{ifz}\ M\ \mathtt{then}\ N\ \mathtt{else}\ P)^\alpha]\!]_B^A \end{array}\right. & \left.\begin{array}{l} = x^\alpha \\ = (\lambda x.[\![M]\!]_B^A)^\alpha \\ = ([\![M]\!]_B^A\ [\![N]\!]_B^A)^\alpha \\ = () \\ = n^\alpha \\ = ([\![M]\!]_B^A + [\![N]\!]_B^A)^\alpha \\ = (\mathtt{ref}([\![M]\!]_B^A))^\alpha \\ = ([\![M]\!]_B^A{:=}[\![N]\!]_B^A)^\alpha \\ = (!M)^\alpha \\ = m^\alpha \\ = (\mathtt{ifz}\ [\![M]\!]_B^A\ \mathtt{then}\ [\![N]\!]_B^A\ \mathtt{else}\ [\![P]\!]_B^A)^\alpha \end{array}\right. & \text{si } |\alpha| \subseteq A \text{ et } T(\alpha) \subseteq B \end{array}$$

L'effacement d'un sous-terme M dépend de son étiquette de tête α. M est effacé non seulement si α contient des lettres qui sont absentes de A, mais aussi si α contient un triplet absent de B. Par la suite, une étiquette α qui vérifie $|\alpha| \subseteq A$ et $T(\alpha) \subseteq B$ sera dite (A,B)**-compatible**. Pour comparer deux termes, on étend de façon naturelle la relation de préfixe utilisée dans les sections

précédentes.

$$
\begin{array}{rcll}
M & \preccurlyeq & M' & \text{si } M \equiv M' \\
M & \preccurlyeq & M' & \text{si } M \preccurlyeq M'' \text{ et } M'' \preccurlyeq M' \\
\Omega & \preccurlyeq & M & \\
(\lambda x.M)^\alpha & \preccurlyeq & (\lambda x.M')^\alpha & \text{si } M \preccurlyeq M' \\
(MN)^\alpha & \preccurlyeq & (M'N')^\alpha & \text{si } M \preccurlyeq M' \text{ et } N \preccurlyeq N' \\
(M+N)^\alpha & \preccurlyeq & (M'+N')^\alpha & \text{si } M \preccurlyeq M' \text{ et } N \preccurlyeq N' \\
(\mathtt{ref}(M))^\alpha & \preccurlyeq & (\mathtt{ref}(M'))^\alpha & \text{si } M \preccurlyeq M' \\
(M{:=}N)^\alpha & \preccurlyeq & (M'{:=}N')^\alpha & \text{si } M \preccurlyeq M' \text{ et } N \preccurlyeq N' \\
(!M)^\alpha & \preccurlyeq & (!M')^\alpha & \text{si } M \preccurlyeq M' \\
(\mathtt{ifz}\ M\ \mathtt{then}\ N\ \mathtt{else}\ P)^\alpha & \preccurlyeq & (\mathtt{ifz}\ M'\ \mathtt{then}\ N'\ \mathtt{else}\ P')^\alpha & \text{si } M \preccurlyeq M' \text{ et } N \preccurlyeq N' \text{ et } P \preccurlyeq P'
\end{array}
$$

L'opération $[\![\cdot]\!]^A_B$ vérifie des propriétés syntaxiques similaires à celles vérifiées par les fonctions d'effacement considérées dans les sections précédentes.

Lemme 5.5 *1. Si $M \preccurlyeq N$, alors on a $\alpha \cdot M \preccurlyeq \alpha \cdot N$.*
2. Si $M \preccurlyeq N$ et $V \preccurlyeq W$, alors $M\{x\backslash V\} \preccurlyeq N\{x\backslash W\}$.

Preuve : On montre successivement ces propriétés.

1. Ce point se montre de façon élémentaire par cas sur M.
2. On procède par induction sur la structure de M.
   (a) Si $M = \Omega$, alors on a $M\{x\backslash V\} = \Omega$ et le résultat est élémentaire.
   (b) Si $M = x^\alpha$, alors on a $N = x^\alpha$. De là, on obtient les relations $M\{x\backslash V\} = \alpha \cdot V$ et $N\{x\backslash W\} = \alpha \cdot W$. On conclut par le point précédent.
   (c) Si $M = (\lambda y.M')^\alpha$, alors on a $N = (\lambda y.N')^\alpha$ avec $M' \preccurlyeq N'$. De là, on obtient les relations $M\{x\backslash V\} = (\lambda y.M'\{x\backslash V\})^\alpha$ et $N\{x\backslash W\} = (\lambda y.N'\{x\backslash W\})^\alpha$. On conclut par hypothèse d'induction.
   (d) Les autres cas sont similaires aux cas précédents. □

La relation de préfixe est compatible avec les opérations de concaténation et de substitution (à gauche et à droite). On examine ensuite les propriétés élémentaires de la fonction d'effacement.

Lemme 5.6 *1. Si $|\alpha| \subseteq A$, alors $\alpha \cdot [\![M]\!]^A_B = [\![\alpha \cdot M]\!]^A_B$*
2. $[\![M]\!]^A_B\{x\backslash[\![N]\!]^A_B\} = [\![M\{x\backslash N\}]\!]^A_B$

Preuve : On montre successivement ces propriétés.

1. Ce point se montre de façon élémentaire par cas sur M.
2. On procède par induction sur la structure de M.
   (a) Si $M = \Omega$, l'égalité est triviale.
   (b) Si $\tau(M)$ n'est pas (A,B)-compatible, alors $[\![M]\!]^A_B = \Omega$ et l'étiquette $\tau(M\{x\backslash N\})$ n'est pas (A,B)-compatible. On a donc $[\![M\{x\backslash N\}]\!]^A_B = \Omega$.
   (c) Si $\tau(M)$ est (A,B)-compatible, on procède par cas.
      i. Si $M = x^\alpha$, alors $[\![M]\!]^A_B = x^\alpha$ et $[\![M]\!]^A_B\{x\backslash[\![N]\!]^A_B\} = \alpha \cdot [\![N]\!]^A_B$. Par ailleurs, on a $[\![M\{x\backslash N\}]\!]^A_B = [\![\alpha \cdot N]\!]^A_B$. On conclut par le lemme 5.5.
      ii. Si $M = (\lambda y.M')^\alpha$, alors on obtient la relation $[\![M]\!]^A_B = (\lambda y.[\![M']\!]^A_B)^\alpha$. De là, on obtient $[\![M\{x\backslash N\}]\!]^A_B = (\lambda y.[\![M']\!]^A_B\{x\backslash N\})^\alpha$. On conclut par hypothèse d'induction.
      iii. Les autres cas sont similaires aux précédents. □

Le premier point indique que si α est une étiquette (A,B)-compatible, la fonction de concaténation avec α commute avec la fonction préfixe $[\![\cdot]\!]^A_B$. Le deuxième point indique que la fonction préfixe commute avec la fonction de substitution.

Nous nous intéressons maintenant aux deux interprétations que nous avons données d'un intervalle (B,Φ)-actif dans une configuration $M/\mu/\Phi$. (1) L'adresse d'un intervalle (B,Φ)-actif appartient bien au domaine de la mémoire. (2) La valeur associée en mémoire à une adresse d'un intervalle (B,Φ)-actif ne peut être modifiée. Nous énonçons formellement la première interprétation sous la forme de l'invariant suivant.

Invariant 5.3 *Le triplet (μ,Φ,B) vérifie l'invariant $\mathcal{J}$, ce que l'on note $\mathcal{J}(\mu,\Phi,B)$, si et seulement si pour tout triplet $[m,\varphi,\varphi']$ qui est (B,Φ)-actif, on a $m \in dom(\mu)$.*

Cet invariant assure la cohérence entre la mémoire μ, le passé Φ et l'utilisation-mémoire B. Dans le résultat suivant, on montre à la fois que si B vérifie la propriété de régularité $\mathcal{B}$, alors l'invariant $\mathcal{J}$ est préservé et la deuxième interprétation d'un intervalle (B,Φ)-actif est vérifiée.

Lemme 5.7 *Soient B une utilisation-mémoire et M/μ une configuration qui vérifient $\mathcal{B}(B)$ et $\mathcal{L}(M,\mu)$. Si $M/\mu/\Phi \to_B M'/\mu'/\Phi'$ et $\mathcal{J}(\mu,\Phi,B)$, alors $\mathcal{J}(\mu',\Phi',B)$ et si $[m,\varphi,\varphi']$ est (B,Φ)-actif alors $\mu(m) = \mu'(m)$.*

Preuve : Dans la suite de cette preuve, l'hypothèse $\mathcal{J}(\mu,\Phi,B)$ est notée $\mathcal{J}_0$. Le terme M est de la forme $M = E[R]$. On note $\kappa = \sigma(E[\,])$ et φ_r est le chemin menant au radical contracté $\varphi_r = \kappa\tau(R)$. On procède par cas sur la réduction.

1. Si $M = E[(\mathtt{ref}(V))^\beta]$, on a $M/\mu/\Phi \to_B E[m_0^{\lceil\beta\rceil^c}]/(\mu; m_0 \overset{\psi_0}{\longmapsto} V)/\Phi'$ avec $\varphi_r = \kappa\beta$, $m_0 = \varphi_r$ et $\psi_0 = \varphi_r\mathtt{ref}\tau(V)$. Par $\mathcal{L}(M,\mu)$, on obtient $m_0 \notin dom(\mu)$. Deux cas sont à considérer.
   (a) Si $B(m_0,\psi_0) = \emptyset$, alors $\Phi = \Phi'$. Soit $[m,\varphi,\varphi']$ un intervalle (B,Φ)-actif : on a $\varphi \in \Phi$ et $\varphi' \notin \Phi$. De là, on obtient, par $\mathcal{J}_0$, $m \in dom(\mu)$. Ceci implique, d'une part $m \in dom(\mu')$, et d'autre part $m \neq m_0$ et $\mu'(m_0) = \mu(m)$.
   (b) Si $B(m_0,\psi_0) \neq \emptyset$, on a $\Phi' = \Phi \cup \{\psi_0\}$. Soit $[m,\varphi,\varphi']$ un intervalle (B,Φ')-actif : on a $\varphi \in \Phi'$ et $\varphi' \notin \Phi'$. Deux cas sont à considérer :
      – Si $\varphi \in \Phi$, alors $[m,\varphi,\varphi']$ est (B,Φ)-actif. De là, par $\mathcal{J}_0$, on obtient $m \in dom(\mu)$. Ceci implique, d'une part $m \in dom(\mu')$, et d'autre part $m \neq m_0$ et $\mu(m) = \mu'(m)$.
      – Si $\varphi = \psi_0$, comme $B(m_0,\psi_0) \neq \emptyset$, en utilisant l'hypothèse $\mathcal{B}(B)$, on obtient $m = m_0$. De là, $m \in dom(\mu')$.
2. Si $M = E[(m_0^\alpha{:=}V)^\beta]$, on a la réduction $M/\mu/\Phi \to_B E[()^{\lceil\beta\rceil^{\mathtt{w}}}]/\mu'/\Phi'$ avec les notations $\mu = (\mu_0; m_0 \overset{\psi_0}{\longmapsto} V_0)$, $\mu' = (\mu_0; m_0 \overset{\psi_1}{\longmapsto} V)$ et $\psi_1 = \varphi_r{:=}_1\alpha$. Soit $[m,\varphi,\varphi']$ un intervalle qui est (B,Φ')-actif. Deux cas sont à considérer.
   (a) Si $B(m_0,\psi_1) = \emptyset$, alors $\Phi' = \Phi$. De ce fait, $[m,\varphi,\varphi']$ est (B,Φ)-actif. Du fait de la réduction de l'affectation, tout intervalle de $B(m_0,\psi_0)$ est (B,Φ)-inactif. En utilisant $\mathcal{J}_0$, on obtient $m \in dom(\mu) - \{m_0\}$. Ceci implique $m \in dom(\mu')$ et $\mu'(m) = \mu(m)$.
   (b) Si $B(m_0,\psi_1) \neq \emptyset$, on a $\Phi' = \Phi \cup \{\psi_1\}$. Deux cas sont à considérer.
      – Si $\varphi \in \Phi$, alors $[m,\varphi,\varphi']$ est (B,Φ)-actif. De même que précédemment, on obtient $m \in dom(\mu) - \{m_0\}$, ce qui implique $m \in dom(\mu')$ et $\mu'(m) = \mu(m)$.
      – Si $\varphi = \psi_1$, en utilisant l'hypothèse $\mathcal{B}(B)$, on obtient $m = m_0$. De là, on a bien $m_0 \in dom(\mu')$.
3. Si $M = E[(!m_0^\alpha)^\beta]$, on a $M/\mu/\Phi \to_B E[\beta \cdot [m_0,\psi_0,\psi_1] \cdot V]/\mu/\Phi'$ avec $\mu = (\mu_0; m_0 \overset{\psi_0}{\longmapsto} V)$ et $\psi_1 = \varphi_r!\alpha$. En utilisant l'hypothèse $\mathcal{B}(B)$, on montre que dans tous les cas, un intervalle (B,Φ')-actif est nécessairement (B,Φ)-actif, ce qui permet de conclure comme dans les cas précédents.
4. Dans les autres cas, on a $\mu' = \mu$ et $\Phi = \Phi'$, ce qui permet de conclure directement. □

Si m est une adresse impliquée dans un intervalle $[m,\varphi,\varphi']$ (B,Φ)-actif, alors le contenu associé en mémoire à m ne peut être modifié tant que l'intervalle demeure (B,Φ)-actif, c'est-à-dire qu'un

radical de chemin φ' n'a pas été contracté. Si cette contraction a lieu, φ' appartient au passé et $[m,\varphi,\varphi']$ devient inactif. Une adresse active devient donc inactive avant d'être modifiée.

Les chemins présents dans un passé Φ sont, a priori, arbitraires. Mais du fait de la spécialisation vis-à-vis de B des règles de réduction, on observe que les chemins ajoutés à Φ au cours d'une réduction ne peuvent être que des chemins présents dans B. Le résultat suivant exploite cette remarque.

Lemme 5.8 *On suppose $M/\mu/\Phi \to_B M'/\mu'/\Phi'$. Soit φ_r le chemin menant au radical contracté entre M et M'. Si φ_r ne préfixe aucun chemin de $C(B) - \Phi$, alors $\Phi = \Phi'$.*

Preuve : Par l'absurde, on suppose $\Phi \neq \Phi'$. Dans tous les cas de figure, on a $\Phi' = \Phi \cup \{\varphi\}$ où $\varphi \in C(B) - \Phi$ et $\varphi_r = \mathsf{Pre}(\varphi) \prec \varphi =$. Ceci contredit l'hypothèse du lemme. □

Intuitivement, les chemins de B sont les étapes importantes de l'utilisation de la mémoire ; ce sont les étapes qui participent à l'obtention de la valeur finale. Le passé enregistre les étapes importantes de B qui sont survenues. Si pour une réduction, le chemin menant au radical contracté ne préfixe pas un chemin de B qui n'est pas déjà passé, cela signifie que cette réduction n'est pas une de ces étapes importantes. Le passé est donc inchangé.

Pour montrer la propriété de non-interférence, on veut comparer les réductions de deux termes qui aboutissent à deux valeurs et montrer que ces valeurs sont liées l'une à l'autre. Pour cela, on introduit l'invariant suivant dont on montrera la conservation par $\to_B$.

Invariant 5.4 *Soit B une utilisation-mémoire. Un quintuplet (M,μ,Φ,N,ν) vérifie l'invariant $\mathcal{I}_B$, ce que l'on note $\mathcal{I}_B(M,\mu,\Phi,N,\nu)$, si et seulement si*

(I1) $M/\mu/\Phi \twoheadrightarrow_B V/\mu'/\Phi'$ *avec* $A = |\tau(V)|$ *et* $B = T(\tau(V))$.

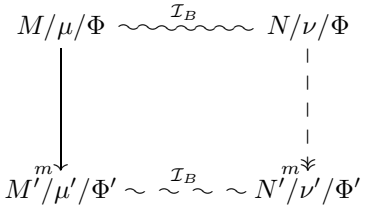
(I2) $N/\nu/\Phi \twoheadrightarrow_B W/\nu'/\Phi''$

(I3) $[\![M]\!]_B^A \preccurlyeq N$

(I4) Si $[m,\varphi,\varphi']$ *est* (B,Φ)*-actif, alors on a (a)* $m \in dom(\mu)$ *et* $m \in dom(\nu)$,
(b) $\mu(m) = (\varphi,V_1)$ *et* $\nu(m) = (\varphi,W_1)$,
(c) $[\![V_1]\!]_B^A \preccurlyeq W_1$.

Cet invariant porte sur deux configurations synchronisées (i.e. dont les passés sont égaux) $M/\mu/\Phi$ et $N/\nu/\Phi$ et se décompose en quatre points. Le point (I1) indique que la configuration étendue $M/\mu/\Phi$ se réduit vers une valeur. De cette étiquette de tête, on tire l'ensemble de lettres A et l'utilisation-mémoire B. Le point (I2) indique, de même, que la configuration étendue $N/\nu/\Phi$ se réduit aussi vers une valeur. Le point (I3) relie les termes M et N : le préfixe de M obtenu à partir de A et B est également un préfixe de N. De façon duale, le point (I4) relie les mémoires μ et ν. Toutes les adresses impliquées dans un intervalle (B,Φ)-actif appartiennent au domaine de μ et ν et les valeurs qui leur sont associées sont reliées de la même manière que pour le point (I3). Cet invariant est conservé par réduction.

Lemme 5.9 *Soit B un ensemble tel que $\mathcal{B}(B)$. On considère la réduction $M/\mu/\Phi \to_B M'/\mu'/\Phi'$ où le chemin menant au radical contracté est nommé φ_r. Si on a $\mathcal{I}_B(M,\mu,\Phi,N,\nu)$ et si φ_r ne préfixe aucun élément de $C(B) - \Phi'$, alors il existe une réduction $N/\nu/\Phi \twoheadrightarrow_B N'/\nu'/\Phi'$ qui vérifie $\mathcal{I}_B(M',\mu',\Phi',N',\nu')$.*



Si la configuration étendue $M/\mu/\Phi$ se réduit en une étape vers $M'/\mu'/\Phi'$, alors il existe une configuration étendue issue de $N/\nu/\Phi$ qui est *synchronisée* avec $M'/\mu'/\Phi'$ et qui vérifie l'invariant $\mathcal{I}_B$ avec cette dernière. On note que des conditions supplémentaires sur B sur le chemin menant au radical sont ajoutées aux hypothèses.

Preuve : Dans la suite de cette preuve, l'invariant $\mathcal{I}_B(M,\mu,\Phi,N,\nu)$ sera noté $\mathcal{I}_0$; l'hypothèse selon laquelle φ_r ne préfixe aucun élément de $C(B) - \Phi'$ est notée $\mathcal{K}_0$. On remarque que $\mathcal{I}_0$ implique $\mathcal{J}(\mu,\Phi,B)$ et $\mathcal{J}(\nu,\Phi,B)$; ces propriétés sont respectivement notées $\mathcal{J}_0$ et $\mathcal{J}'_0$. Soient R le radical contracté entre M et M' et $E[\,]$ son contexte d'évaluation dans M. On a $M = E[R]$. En posant $\kappa = \sigma(E[\,])$, on a $R/\mu/\Phi \xrightarrow{\kappa}_B R'/\mu'/\Phi'$ et $M' = E[R']$. On note $\beta = \tau(R)$; le chemin menant au radical contracté est donc $\varphi_r = \kappa\beta$. On note que, par définition de B, si $\varphi \in C(B)$, alors $|\varphi| \subseteq A$. On procède par cas.

1. Si $|\varphi_r| \not\subseteq A$, on a d'une part $[\![M]\!]^A_B = [\![M']\!]^A_B \preccurlyeq N$ et d'autre part, le chemin φ_r menant au radical R ne préfixe aucun chemin de $C(B)$. Par conséquent, en utilisant le lemme 5.8, on obtient $\Phi' = \Phi$. On veut montrer $\mathcal{I}_B(M',\mu',\Phi,N,\nu)$. Les points (I1), (I2) et (I3) sont vérifiés. Soit $[m_0,\varphi,\varphi']$ un intervalle (B,Φ)-actif. Par $\mathcal{I}_0$, on a $m_0 \in dom(\nu)$, $m_0 \in dom(\mu)$, $\mu(m_0) = (\varphi,V_0)$ et et $\nu(m_0) = (\varphi,W_0)$ avec $[\![V_0]\!]^A_B \preccurlyeq W_0$. En utilisant le lemme 5.7 avec $\mathcal{J}_0$, on obtient $m_0 \in dom(\mu')$ et $\mu'(m_0) = \mu(m_0)$. Le point (I4) est donc aussi vérifié.
2. Si $|\varphi_r| \subseteq A$, alors $[\![E[\,]]\!]^A_B$ est un contexte. On pose $[\![E[\,]]\!]^A_B = E_0[\,]$. On a $[\![M]\!]^A_B = E_0[[\![R]\!]^A_B]$ et $[\![M']\!]^A_B = E_0[[\![R']\!]^A_B]$. Comme, par $\mathcal{I}_0$, on a $[\![M]\!]^A_B \preccurlyeq N$, il existe un contexte $E_1[\,]$ tel que $E_0[\,] \preccurlyeq E_1[\,]$, $N = E_1[N_1]$ et $[\![R]\!]^A_B \preccurlyeq N_1$. On procède par cas sur la réduction.
   (a) Si $R = ((\lambda x.M_1)^\alpha V_1)^\beta$, on a $R/\mu/\Phi \xrightarrow{\kappa}_B \beta\cdot\lceil\alpha\rceil^{\mathtt{b}} \cdot M_1\{x\backslash\lfloor\alpha\rfloor^{\mathtt{b}} \cdot V_1\}/\mu/\Phi$. On considère les cas suivants.
      i. Si $|\alpha| \not\subseteq A$, on a $[\![M']\!]^A_B = E_0[\Omega] \preccurlyeq E_0[[\![R]\!]^A_B] = [\![M]\!]^A_B \preccurlyeq N$. De là, on obtient $\mathcal{I}_B(M',\mu,\Phi,N,\nu)$.
      ii. Si $|\alpha| \subseteq A$, on a $[\![M]\!]^A_B = E_0[((\lambda x.[\![M_1]\!]^A_B)^\alpha [\![V_1]\!]^A_B)^\beta]$ et $N = E_1[((\lambda x.N_2)^\alpha N_3)^\beta]$ avec $[\![M_1]\!]^A_B \preccurlyeq N_2$ et $[\![V_1]\!]^A_B \preccurlyeq N_3$. Comme N se réduit vers une valeur, on a nécessairement $N/\nu/\Phi \twoheadrightarrow_B N'/\nu'/\Phi_1$ où $N' = E_1[((\lambda x.N_2)^\alpha W_1)^\beta]$. Les chemins menant aux radicaux contractés entre N et N' sont préfixés par φ_r. Par hypothèse, le chemin φ_r ne préfixe aucun chemin de $C(B) - \Phi$. Par conséquent, en utilisant itérativement le lemme 5.8, on obtient la relation $\Phi_1 = \Phi$. On a donc la réduction $N/\nu/\Phi \twoheadrightarrow_B N'/\nu'/\Phi \to_B N''/\nu'/\Phi$ où $N'' = E_1[\beta\cdot\lceil\alpha\rceil^{\mathtt{b}}\cdot N_2\{x\backslash\lfloor\alpha\rfloor^{\mathtt{b}}.W_1\}]$. On veut montrer $\mathcal{I}_B(M',\mu,\Phi,N'',\nu')$. Les points (I1) et (I2) sont vérifiés. Pour le point (I3), deux cas sont à envisager.
         – Si $|\tau(V_1)| \not\subseteq A$, alors $[\![V_1]\!]^A_B = \Omega \preccurlyeq W_1$. En utilisant le lemme 5.6, on obtient $[\![\beta\cdot\lceil\alpha\rceil^{\mathtt{b}}.M_1\{x\backslash\lfloor\alpha\rfloor^{\mathtt{b}}\cdot V_1\}]\!]^A_B \preccurlyeq \beta\cdot\lceil\alpha\rceil^{\mathtt{b}}\cdot N_2\{x\backslash\lfloor\alpha\rfloor^{\mathtt{b}}.W_1\}$ ce qui permet de conclure $[\![M']\!]^A_B \preccurlyeq N''$.
         – Si $|\tau(V_1)| = |\gamma| \subseteq A$, alors $[\![V_1]\!]^A_B$ est une valeur qui vérifie $[\![V_1]\!]^A_B \preccurlyeq N_3$. Par conséquent, N_3 est une valeur. On en déduit donc $N_3 = W_1$ et $[\![V_1]\!]^A_B \preccurlyeq W_1$. En utilisant le lemme 5.6, on obtient bien $[\![M']\!]^A_B \preccurlyeq N''$.

      Soit $[m_0,\varphi,\varphi']$ un intervalle (B,Φ)-actif. En utilisant le lemme 5.7 avec $\mathcal{J}_0$ et $\mathcal{J}'_0$, on obtient $m_0 \in dom(\mu')$ et $m_0 \in dom(\nu')$ avec $\mu'(m_0) = \mu(m_0)$ et $\nu'(m_0) = \nu(m_0)$. Par $\mathcal{I}_0$, on a $\mu(m_0) = (\varphi,V_0)$ et $\nu(m_0) = (\varphi,W_0)$ avec $[\![V_0]\!]^A_B \preccurlyeq W_0$. Le point (I4) est donc aussi vérifié.
   (b) Si $R = (\mathtt{ref}(V_1))^\beta$, on pose $\alpha = \tau(V_1)$, $m = \varphi_r = \kappa\beta$ et $\varphi_0 = \varphi_r\mathtt{ref}\alpha$. La contraction considérée est $R/\mu/\Phi \xrightarrow{\kappa}_B m^{\lceil\beta\rceil^{\mathtt{c}}}/\mu'/\Phi'$ où $\mu' = (\mu; m \xmapsto{\varphi_0} V_1)$. On considère les cas suivants.

i. Si $B(m,\varphi_0) = \emptyset$, alors on a $\Phi' = \Phi$. De là, on obtient $[\![M]\!]^A_B = E_0[(\mathtt{ref}([\![V_1]\!]^A_B))^\beta]$ et $N = E_1[(\mathtt{ref}(N_2))^\beta]$ avec $[\![V_1]\!]^A_B \preccurlyeq N_2$. Comme N se réduit vers une valeur, on a nécessairement $N/\nu/\Phi \twoheadrightarrow_B N'/\nu'/\Phi_1$ où $N' = E_1[m^{\lceil\beta\rceil^c}]$. Les chemins menant aux radicaux contractés entre N et N' sont préfixés par φ_r. Par hypothèse, φ_r ne préfixe aucun chemin de $C(B) - \Phi' = C(B) - \Phi$. Par conséquent, en utilisant itérativement le lemme 5.8, on obtient $\Phi_1 = \Phi$. On veut montrer $\mathcal{I}_B(M',\mu',\Phi,N',\nu')$. Les points (I1), (I2) et (I3) sont vérifiés. Soit $[m_0,\varphi,\varphi']$ un intervalle (B,Φ)-actif. En utilisant le lemme 5.7 avec $\mathcal{J}_0$ et $\mathcal{J}'_0$, on obtient $m_0 \in dom(\mu')$ et $m_0 \in dom(\nu')$ avec $\mu'(m_0) = \mu(m_0)$ et $\nu'(m_0) = \nu(m_0)$. Par $\mathcal{I}_0$, on obtient $\mu(m_0) = (\varphi,V_0)$ et $\nu(m_0) = (\varphi,W_0)$ avec $[\![V_0]\!]^A_B \preccurlyeq W_0$. Le point (I4) est donc aussi vérifié.

ii. Si $B(m,\varphi_0) \neq \emptyset$, alors on a $\Phi' = \Phi \cup \{\varphi_0\}$. Comme $\varphi_0 = \kappa\beta\mathtt{ref}\alpha \in C(B)$, on en déduit $|\alpha| \subseteq A$. De là, on a $[\![M]\!]^A_B = E_0[(\mathtt{ref}([\![V_1]\!]^A_B))^\beta]$ et $N = E_1[(\mathtt{ref}(W_1))^\beta]$ où W_1 est une valeur qui vérifie $[\![V_1]\!]^A_B \preccurlyeq W_1$ et $\tau(W_1) = \alpha$. On a donc la réduction $N/\nu/\Phi \to_B N'/\nu'/\Phi'$ où $N' = E_1[m^{\lceil\beta\rceil^c}]$ et $\nu' = (\nu; m \overset{\varphi_0}{\longmapsto} W_1)$. On veut montrer $\mathcal{I}_B(M',\mu',\Phi,N',\nu')$. Les points (I1), (I2) et (I3) sont vérifiés. Soit $[m_0,\varphi,\varphi']$ un intervalle (B,Φ')-actif : on a $\varphi \in \Phi' = \Phi \cup \{\varphi_0\}$ et $\varphi' \notin \Phi'$. Deux cas sont à considérer.

– Si $\varphi \in \Phi$, alors l'intervalle $[m_0,\varphi,\varphi']$ est (B,Φ)-actif. Par conséquent, en utilisant le lemme 5.7 avec $\mathcal{J}_0$ et $\mathcal{J}'_0$, on obtient $m_0 \in dom(\mu')$ et $m_0 \in dom(\nu')$ avec $\mu(m_0) = \mu'(m_0)$ et $\nu(m_0) = \nu'(m_0)$. Par $\mathcal{I}_0$, on a $\mu(m_0) = (\varphi,V_2) = \mu'(m_0)$ et $\nu(m_0) = (\varphi,W_2) = \nu'(m_0)$ avec $[\![V_2]\!]^A_B \preccurlyeq W_2$.

– Si $\varphi = \varphi_0$, alors, du fait de l'invariant $\mathcal{B}$, on a $m_0 = m$. On obtient donc $\mu'(m) = (\varphi_0,V_1)$ et $\nu'(m) = (\varphi_0,W_1)$.

Le point (I4) est donc aussi vérifié.

(c) Si $R = (m^\alpha{:=}V_1)^\beta$, alors on pose $\varphi_1 = \varphi_r{:=}_1\alpha$. La contraction considérée dans ce cas est $R/\mu/\Phi \xrightarrow{\kappa}_B ()^{\lceil\beta\rceil^u}/\mu'/\Phi'$ où on pose $\mu = (\mu_0; m \overset{\varphi_0}{\longmapsto} V_0)$ et $\mu' = (\mu_0; m \overset{\varphi_1}{\longmapsto} V_1)$. On examine les cas suivants.

i. Si $B(m,\varphi_1) = \emptyset$, alors on a $\Phi' = \Phi$. De là, on obtient $[\![M]\!]^A_B = E_0[([\![m^\alpha]\!]^A_B{:=}[\![V_1]\!]^A_B)^\beta]$ et $N = E_1[(N_1{:=}N_2)^\beta]$ avec $[\![m^\alpha]\!]^A_B \preccurlyeq N_1$ et $[\![V_1]\!]^A_B \preccurlyeq N_2$. Comme N se réduit vers une valeur, on a $N/\nu/\Phi \xrightarrow{\kappa}\!\!\!\!\twoheadrightarrow_B N'/\nu'/\Phi_1$ avec $N' = E_1[()^{\lceil\beta\rceil^u}]$. Les chemins menant aux radicaux contractés entre N et N' sont préfixés par φ_r. Par hypothèse, ce dernier ne préfixe aucun chemin de $C(B) - \Phi' = C(B) - \Phi$. Par conséquent, en utilisant itérativement le lemme 5.8, on obtient $\Phi = \Phi_1$. On veut montrer $\mathcal{I}_B(M',\mu',\Phi,N',\nu')$. Les points (I1), (I2) et (I3) sont vérifiés. Soit $[m_0,\varphi,\varphi']$ un intervalle (B,Φ)-actif. Par $\mathcal{I}_0$, on a $\mu(m_0) = (\varphi,V_2)$ et $\nu(m_0) = (\varphi,W_2)$ avec $[\![V_2]\!]^A_B \preccurlyeq W_2$. En utilisant le lemme 5.7 avec $\mathcal{J}_0$ et $\mathcal{J}'_0$, on obtient $m_0 \in dom(\mu')$ et $m_0 \in dom(\nu')$ avec $\mu'(m_0) = \mu(m_0)$ et $\nu'(m_0) = \nu(m_0)$. Le point (I4) est donc aussi vérifié.

ii. Si $B(m,\varphi_1) \neq \emptyset$, alors on a $\Phi' = \Phi \cup \{\varphi_1\}$. Comme $\varphi_1 = \varphi_r{:=}_1\alpha \in C(B)$, on obtient $|\alpha| \subseteq A$. De là, on a $[\![M]\!]^A_B = E_0[(m^\alpha{:=}[\![V_1]\!]^A_B)^\beta]$ et $N = E_1[(m^\alpha{:=}N_2)^\beta]$ avec $[\![V_1]\!]^A_B \preccurlyeq N_2$. Comme N se réduit vers une valeur, on a $N/\nu/\Phi \xrightarrow{\kappa}\!\!\!\!\twoheadrightarrow_B N'/\nu'/\Phi_1$ avec $N' = E_1[(m^\alpha{:=}W_1)^\beta]$. Soit ψ un chemin menant à un radical contracté entre N et N'. Ce chemin est nécessairement de la forme $\psi = \varphi_r{:=}_2\psi'$. Ce chemin est préfixé par φ_r. Comme, par hypothèse, φ_r ne préfixe aucun chemin de $C(B) - \Phi'$, de même ψ ne préfixe aucun chemin de $C(B) - \Phi'$. Comme $C(B) - \Phi = (C(B) - \Phi') \cup \{\varphi_1\}$ et $\varphi_1 = \varphi_r{:=}_1\alpha$, on en déduit que ψ ne préfixe aucun chemin de $C(B) - \Phi$. Par conséquent, en utilisant itérativement le lemme 5.8, on obtient $\Phi_1 = \Phi$. De là, on obtient la réduction : $E_1[(m^\alpha{:=}W_1)^\beta]/\nu'/\Phi \xrightarrow{\kappa}_B N'/\nu''/\Phi'$ avec $N' = E_1[()^{\lceil\beta\rceil^u}]$.

On veut montrer $\mathcal{I}_B(M',\mu',\Phi',N',\nu'')$. Les points (I1), (I2) et (I3) sont vérifiés. Soit $[m_0,\varphi,\varphi']$ un intervalle (B,Φ)-actif. Deux cas sont à considérer.

- Si $\varphi \in \Phi$, alors $[m_0,\varphi,\varphi']$ est (B,Φ)-actif. Par $\mathcal{I}_0$, on a $\mu(m_0) = (\varphi,V_2)$ et $\nu(m_0) = (\varphi,W_2)$ avec $[\![V_2]\!]_B^A \preccurlyeq W_2$. En utilisant le lemme 5.7 avec les hypothèses $\mathcal{J}_0$ et $\mathcal{J}_0'$, on obtient $m_0 \in dom(\mu')$ et $m_0 \in dom(\nu'')$ avec $\mu(m_0) = \mu'(m_0)$ et $\nu(m_0) = \nu''(m_0)$.
- Si $\varphi = \varphi_1$, alors, du fait de l'invariant $\mathcal{B}$, on a $m_0 = m$. On obtient donc $\mu'(m) = (\varphi_1,V_1)$ et $\nu''(m) = (\varphi_1,W_1)$.

Le point (I4) est donc aussi vérifié.

(d) Si $R = (!m^\alpha)^\beta$, alors on pose $\varphi_1 = \varphi_r!\alpha$. La contraction considérée dans ce cas est $R/\mu/\Phi \xrightarrow{\kappa}_B \beta\cdot[m,\varphi_0,\varphi_1]\cdot V_0/\mu/\Phi'$ où $\mu = (\mu_0; m \overset{\varphi_0}{\longmapsto} V_0)$. On considère les cas suivants.

i. Si $[m,\varphi_0,\varphi_1] \notin B$, on a $\Phi' = \Phi$ et $[\![M']\!]_B^A = E_0[\Omega] \preccurlyeq [\![M]\!]_B^A \preccurlyeq N$. On obtient donc immédiatement $\mathcal{I}_B(M',\mu,\Phi,N,\nu)$.

ii. Si $[m,\varphi_0,\varphi_1] \in B$, alors cet intervalle est (B,Φ)-actif et $\Phi' = \Phi\cup\{\varphi_1\}$ et $|\alpha| \subseteq A$. De là, on a $[\![M]\!]_B^A = E_0[(!m^\alpha)^\beta]$ et $N = E_1[(!m^\alpha)^\beta]$. Comme l'intervalle $[m,\varphi_0,\varphi_1]$ est (B,Φ)-actif, en utilisant $\mathcal{I}_0$, on a $m \in dom(\nu)$ avec $\nu(m) = (\varphi_0,W_0)$ et $[\![V_0]\!]_B^A \preccurlyeq W_0$. On obtient donc la réduction $N/\nu/\Phi \xrightarrow{\kappa}_B N'/\nu/\Phi'$ où $N' = E_1[\beta\cdot[m,\varphi_0,\varphi_1].W_0]$. On veut montrer $\mathcal{I}_B(M',\mu,\Phi',N',\nu)$. Les points (I1) et (I2) sont vérifiés. Comme $[\![V_0]\!]_B^A \preccurlyeq W_0$, on obtient le point (I3) en utilisant le lemme 5.6. Soit $[m_0,\varphi,\varphi']$ un intervalle (B,Φ')-actif : on a $\varphi \in \Phi'$ et $\varphi' \notin \Phi'$. Deux cas sont à considérer.

- Si $\varphi \in \Phi$, alors $[m_0,\varphi,\varphi']$ est (B,Φ)-actif. Par $\mathcal{I}_0$, on a $\mu(m_0) = (\varphi,V_1) = \mu'(m_0)$ et $\nu(m_0) = (\varphi,W_1) = \nu'(m_0)$ avec $[\![V_1]\!]_B^A \preccurlyeq W_1$. En utilisant le lemme 5.7 avec $\mathcal{J}_0$ et $\mathcal{J}_0'$, on obtient $m_0 \in dom(\mu')$ et $m_0 \in dom(\nu')$ avec $\mu(m_0) = \mu'(m_0)$ et $\nu(m_0) = \nu'(m_0)$.
- Le cas $\varphi = \varphi_1$ est exclu par l'invariant $\mathcal{B}$ car $[m_0,\varphi,\varphi'] \in B$ et $[m,\varphi_0,\varphi_1] \in B$.

Le point (I4) est donc aussi vérifié.

(e) Si $R = (\texttt{ifz}\ 0^\alpha\ \texttt{then}\ M_1\ \texttt{else}\ M_2)^\beta$, alors la contraction considérée dans ce cas est $R/\mu/\Phi \xrightarrow{\kappa}_B \beta\cdot\lceil\alpha\rceil^{\mathtt{i}}\cdot M_1/\mu/\Phi$. On examine les cas suivants.

i. Si $|\alpha| \not\subseteq A$, on a $[\![M']\!]_B^A = E_0[\Omega] \preccurlyeq N$. On obtient donc $\mathcal{I}_B(M',\mu,\Phi,N,\nu)$.

ii. Si $|\alpha| \subseteq A$, alors on a $[\![M]\!]_B^A = E_0[(\texttt{ifz}\ 0^\alpha\ \texttt{then}\ [\![M_1]\!]_B^A\ \texttt{else}\ [\![M_2]\!]_B^A)^\beta]$. De là, on obtient $N = E_1[(\texttt{ifz}\ 0^\alpha\ \texttt{then}\ N_1\ \texttt{else}\ N_2)^\beta]$ où $[\![M_1]\!]_B^A \preccurlyeq N_1$. Par conséquent, on a $N/\nu/\Phi \xrightarrow{\kappa}_B N'/\nu/\Phi$ avec $N' = E_1[\beta\cdot\lceil\alpha\rceil^{\mathtt{i}}\cdot N_1]$. On veut montrer $\mathcal{I}_B(M',\mu,\Phi,N',\nu)$. Les points (I1), (I2) et (I4) sont vérifiés. On obtient le point (I3) en utilisant le lemme 5.6.

(f) Les autres cas sont similaires aux cas précédents. □

Ce résultat permet d'obtenir le lemme suivant qui constitue le résultat de base du théorème de non-interférence.

Lemme 5.10 *Soit M un terme tel que $T(M) = \emptyset$. On suppose $M/\emptyset \twoheadrightarrow V/\mu$. Soient $A = |\tau(V)|$ et $B = T(\tau(V))$. Si le terme N vérifie $[\![M]\!]_B^A \preccurlyeq N$ et $N/\emptyset/\emptyset \twoheadrightarrow_B W/\nu/\Phi$, alors $[\![V]\!]_B^A \preccurlyeq W$.*

Preuve : En utilisant le lemme 5.3 on obtient $\mathcal{B}(B)$. Avec le lemme 5.4, on obtient la réduction $M/\emptyset/\emptyset \twoheadrightarrow_B V/\mu/C(B)$. Cette réduction peut s'écrire de la façon suivante

$$M/\emptyset/\emptyset = M_0/\mu_0/\Phi_0 \to_B M_1/\mu_1/\Phi_1 \to_B \ldots \to_B M_n/\mu_n/\Phi_n = V/\mu/C(B)$$

Pour $i \in \{1\ldots n\}$, on nomme φ^i le chemin menant au radical contracté entre M_{i-1} et M_i. Soit $j \in \{1\ldots n-1\}$; on veut montrer que φ_j ne préfixe aucun chemin de $C(B) - \Phi_j$. Par l'absurde,

soit $\psi \in C(B) - \Phi_j$ tel que $\varphi_j \preceq \psi$. Comme ψ appartient au passé final, il existe un indice k tel que $j < k \leq n$ tel que $\varphi^k = \mathsf{Pre}(\psi)$. Par conséquent, ceci implique $\varphi^j \preceq \varphi^k$ ce qui contredit le théorème 5.4. Par conséquent, φ_j ne préfixe aucun chemin de $C(B) - \Phi_j$. De là, en utilisant itérativement le lemme 5.9, on obtient $\mathcal{I}_B(V,\mu,C(B),W,\nu)$ et donc $[\![V]\!]_B^A \preccurlyeq W$. □

De la valeur obtenue de la réduction de M, on obtient un préfixe P de M. Si un terme est préfixé par P et se réduit vers une valeur W, en respectant l'utilisation-mémoire de V, alors V et W admettent un préfixe commun non réduit à Ω. Si on se place dans le cas particulier où V est un entier n^α, on obtient $W = n^\alpha = V$. Dans ce cas, l'observation du résultat ne donne aucune information sur les sous-termes de M qui sont effacés dans P. On exploite ce résultat dans le théorème de non-interférence.

Théorème 5.5 (Non-interférence) *Soit M un terme tel que $\mathtt{INIT}(M)$ et $\mathcal{R} : M/\emptyset \twoheadrightarrow V/\mu$. Le sous-terme $(C[\,],N)$ de M interfère dans $\mathcal{R}$ si et seulement si $\tau(N) \in |\tau(V)|$.*

Preuve : En utilisant le lemme 5.10, on obtient que si $\tau(N) \notin |\tau(\alpha)|$, alors N n'interfère pas. Réciproquement, si N n'interfère pas, on peut le remplacer par N' qui est le terme N où l'on a changé l'étiquette de tête pour une lettre qui n'intervient pas dans M. Il est clair que $C[N']/\emptyset/\emptyset$ se réduit vers une valeur V' en respectant $T(\tau(V))$. Par définition de la non-interférence, on a $\tau(V) = \tau(V')$ ce qui implique $\tau(N) \notin |\tau(V)|$. □

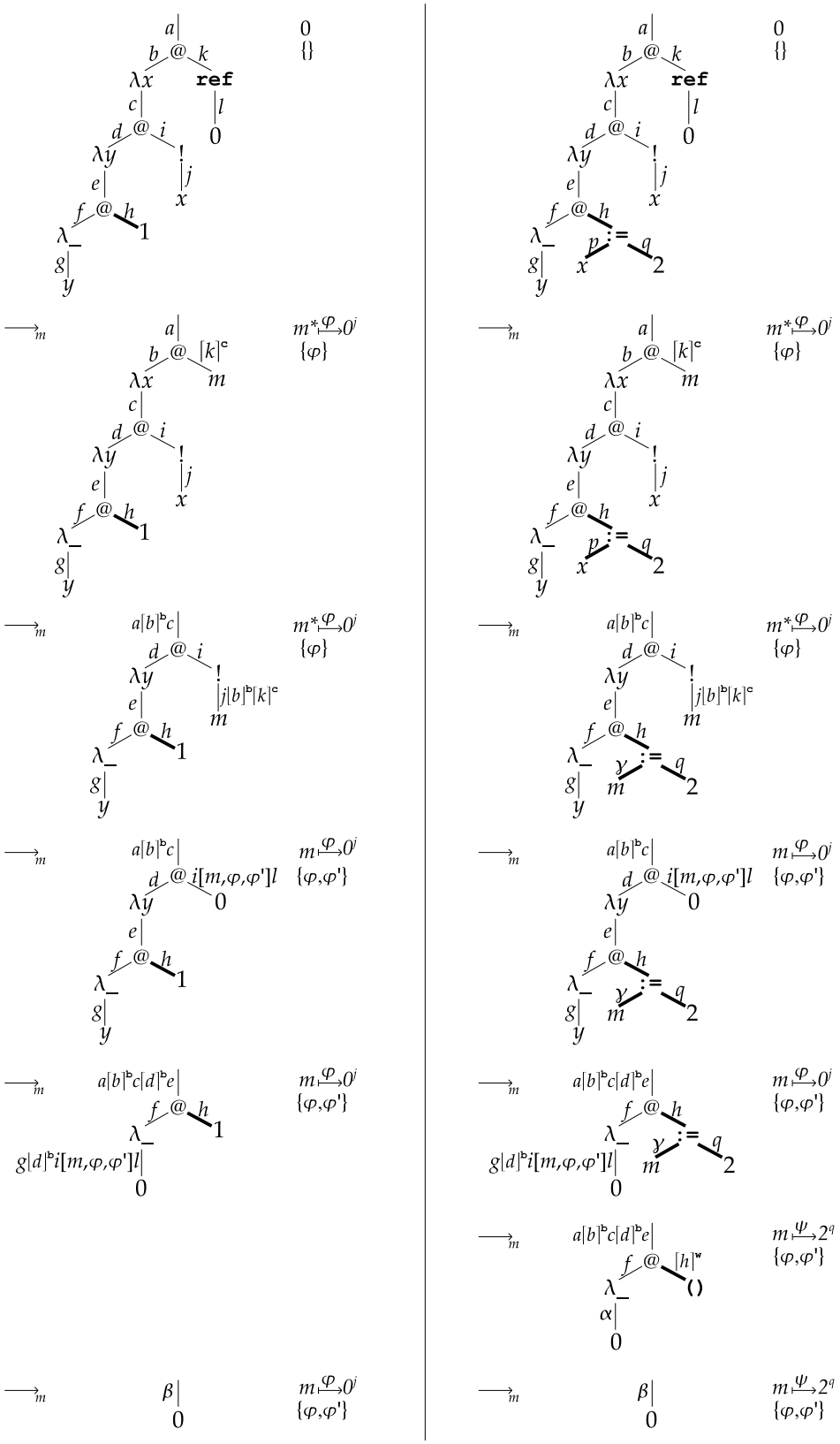
Si les étiquettes de M sont des lettres distinctes, un sous-terme N de M interfère, au sens de la définition 5.3, dans la réduction $M/\emptyset \twoheadrightarrow_e V/\mu$ si et seulement si son étiquette est une lettre présente dans l'étiquette de tête de V. Pour illustrer cette propriété de non-interférence, on reprend les réductions $\mathcal{R}_1$ et $\mathcal{R}_2$ citées en exemple dans la section 5.3. Ces termes, une fois étiquetés, sont :

$$M_1 = ((\lambda x.((\lambda y.((\lambda\_.y^g)^f 1^h)^e)^d(!x^j)^i)^c)^b(\mathtt{ref}(0^l))^k)^a$$
$$M_2 = ((\lambda x.((\lambda y.((\lambda\_.y^g)^f(x^p{:=}2^q)^h)^e)^d(!x^j)^i)^c)^b(\mathtt{ref}(0^l))^k)^a$$

Les réductions de ces termes sont illustrées sur la figure 5.22. Cette figure est composée de deux colonnes. Dans la première colonne, on trouve la réduction de M_1. Dans la colonne de droite, on trouve la réduction de M_2. Les parties non communes aux deux colonnes sont signalées en gras. Le préfixe obtenu avec $[\![\,]\!]_B^A$ à partir du terme de la colonne de gauche correspond à la partie non grasse, c'est-à-dire à la partie commune entre les termes des deux réduction. Ceci est bien conforme au lemme 5.9. De même, lorsque l'adresse m est active (ce qui est mentionné par une étoile), la valeur associée à m est égale dans les réductions de M_1 et M_2.

Si on applique l'analyse statique de Pottier et Simonet [37, 39] sur M_2, en supposant que 2^q est secret, alors on obtient que le résultat de la réduction est secret. En effet, cette analyse statique attribue à chaque adresse un niveau de sécurité qui correspond au niveau de sécurité des valeurs qui sont associées à l'adresse au cours de la réduction. Comme 2^q est affecté à m, alors le niveau de sécurité de m est secret. En réalité, deux valeurs sont successivement associées à m dans la mémoire. Tout d'abord, l'adresse est initialisée avec la valeur publique 0^l. Puis, la valeur secrète 2^q est affecté à m. Mais seule la première valeur contribue au résultat, qui devrait donc être considéré comme public. Bien entendu, une analyse statique nécessite certaines approximations pour être décidable. Si le système présenté ici ne fournit pas une analyse statique, il offre, en revanche, une base théorique pour raisonner sur une telle analyse.

Dans ce chapitre nous avons successivement examiné la propriété de non-interférence dans le λ-calcul, dans le λ-calcul par valeur et dans un λ-calcul muni de traits impératifs. Pour aborder ce problème, on s'inspire de l'approche des analyses statiques de flot d'information : si la réduction du terme M aboutit sur une valeur V, on souhaite savoir si l'observation de la valeur V (intuitivement publique) permet d'obtenir une information sur certains sous-termes (intuitivement secrets) de M. Les étiquettes du λ-calcul s'avèrent être un outil précieux puisque ces étiquettes fournissent



$$\begin{aligned}
\beta &= a\lceil a\rceil^{\mathtt{b}} c\lceil d\rceil^{\mathtt{b}} e\lceil f\rceil^{\mathtt{b}} g\lfloor d\rfloor^{\mathtt{b}} i[m,\varphi,\varphi']l & \gamma &= p\lfloor b\rfloor^{\mathtt{b}}\lceil k\rceil^{\mathtt{c}} \\
m &= a@_2 k & \psi &= a\lceil b\rceil^{\mathtt{b}} c\lceil d\rceil^{\mathtt{b}} e@_2 h{:=_1}\gamma \\
\varphi &= a@_2 k\,\mathtt{ref}\,l & \varphi' &= a\lceil b\rceil^{\mathtt{b}} c@_2 i!j\lfloor b\rfloor^{\mathtt{b}}\lceil k\rceil^{\mathtt{c}}
\end{aligned}$$

FIG. 5.22 – *Réduction des termes M_1 et M_2*

intuitivement une analyse dynamique de dépendance des termes vis-à-vis des sous-termes du terme initial. Dans le cas du λ-calcul et du λ-calcul par valeur, l'étiquette de tête de V permet d'obtenir le préfixe X des sous-termes de M dont V dépend. Ces sous-termes interfèrent dans V. A contrario, les sous-termes qui sont effacés dans X n'interfèrent pas dans V puisque cette valeur ne donne aucune information sur ces sous-termes. Nous avons remarqué au passage que les préfixes d'interférence et de stabilité coïncident dans le cas du λ-calcul. En revanche, dans le λ-calcul par valeur, le préfixe d'interférence est inclus dans le préfixe de stabilité. Nous avons expliqué cette inclusion par les différences entre les définitions de sous-terme non-critique et de sous-terme qui n'interfère pas. Si M se réduit vers une valeur, un sous-terme $(C[\,],N)$ de M n'est pas critique si en changeant N pour N', on obtient une valeur de même observable. Par contraste, ce sous-terme n'interfère pas si, en changeant N pour N' *et* dans le cas où $C[N']$ se réduit vers une valeur, l'observable de cette valeur est inchangé.

Les étiquettes du λ-calcul permettent d'obtenir simplement la propriété de non-interférence, dans le cas de ces langages fonctionnels. En présence de traits impératifs tels que l'affectation ou la déréférence, un nouveau type d'interférence vient se combiner à l'interférence fonctionnelle présente dans le λ-calcul et le λ-calcul par valeur. Pour étudier ce phénomène, on introduit le λ_m-calcul et le λ_m-calcul étiqueté. Au cours de la réduction $M/\emptyset \twoheadrightarrow V/\mu$, des écritures et des lectures en mémoire ont lieu. Certaines adresses de la mémoire peuvent interférer dans V. Plus précisément, une adresse peut contribuer à V pendant certains intervalles de temps : entre une écriture et une lecture. Si un effet de bord vient interférer entre cette écriture et cette lecture, la valeur lue est modifiée, ce qui entraîne la modification de la valeur finale. A l'interférence "fonctionnelle" vient s'ajouter une interférence sur la mémoire. Les étiquettes du λ_m-calcul étiqueté permettent d'identifier à la fois les sous-termes qui interfèrent (interférence fonctionnelle) et les intervalles actifs des adresses qui interfèrent (interférence de la mémoire). Les étiquettes du λ_m-calcul permettent d'étendre l'approche initiée par Abadi et al. dans [3]. Une comparaison formelle entre notre approche très théorique et l'approche pragmatique des analyses de flot d'information telles que Flow Caml pourrait être très fructueuse.