FAIROUZ TCHIER

SÉMANTIQUES RELATIONNELLES DÉMONIAQUES ET VÉRIFICATION DE BOUCLES NON DÉTERMINISTES

Thèse
présentée
à la Faculté des études supérieures
de l'Université Laval
pour l'obtention
du grade de Philosophiae Doctor (Ph. D.)

Département de mathématiques et de statistique
FACULTÉ DES SCIENCES ET DE GÉNIE
UNIVERSITÉ LAVAL
QUÉBEC

AOÛT 1996

Résumé

Dans cette thèse, nous présentons une sémantique opérationnelle du langage des commandes gardées de Dijkstra. Pour ce faire, nous associons à chaque programme un objet appelé *diagramme relationnel*. Un diagramme relationnel est essentiellement une représentation, dans le formalisme de l'algèbre des relations, d'un système de transitions dont les arcs sont étiquetés par des relations. Nous définissons ensuite la notion de *relation d'entrée/sortie démoniaque* d'un diagramme. Cette démarche permet d'associer à chaque programme (non déterministe) une relation d'entrée/sortie correspondant à sa pire exécution. Nous montrons ensuite que la relation ainsi obtenue est aussi celle qui est assignée par une sémantique dénotationnelle définie dans des articles antérieurs. En d'autres termes, nous montrons l'équivalence de notre sémantique opérationnelle avec une sémantique dénotationnelle relationnelle déjà connue. L'intérêt de cette démonstration réside dans le fait que les définitions dénotationnelles classiques requièrent une bonne dose d'intuition pour être formulées et comprises, alors que l'association d'un diagramme à un programme est tout à fait naturelle.

Comme résultat intermédiaire, nous généralisons à un contexte non déterministe un théorème de Mills connu sous le nom de *règle de vérification de boucle de Mills*, énoncé initialement pour les programmes déterministes. Ce théorème permet de s'assurer qu'une relation donnée est effectivement la sémantique d'une boucle donnée. Cette thèse montre qu'il a bien d'autres usages possibles en l'employant à maintes reprises.

Québec, août 1996

Fairouz Tchier
Étudiante

Jules Desharnais
Directeur de recherche

REMERCIEMENTS

Au terme de ce travail, je tiens à remercier tout d'abord mon directeur de recherche Monsieur Jules Desharnais. Il a toujours fait preuve d'une grande disponibilité et d'une grande patience pour corriger les différents manuscrits de cette thèse. De même, il m'a fourni plusieurs preuves (parmi les plus difficiles) que nous avons simplifiées. J'ai apprécié en lui son esprit scientifique, sa rigueur et son souci de précision. Je remercie également mon codirecteur Monsieur Bernard R. Hodgson pour sa contribution et son encouragement. Des remerciements particuliers vont aux membres du jury, Messieurs Ali Mili, Mourad Debbabi et Brahim Chaib-draa, pour leur précieux travail. Leurs suggestions ont amélioré la version finale de cette thèse.

Je remercie ma famille, et tout particulièrement mes parents Yamina et Said, ainsi que mon frère Dr Nacir, qui a toujours été pour moi un modèle de persévérance.

Je remercie tous mes amis et mes collègues de travail, spécialement Zébida Bahmed, Louise Cloutier, Ridha Khédri et Slim Baltagi.

Finalement, la contribution la plus significative vient sans nul doute de mon époux Djamel et de nos enfants Sarah et Bellal. Ils ont eu à supporter mes nombreuses absences et ont été mon support tout au long de ces années.

Table des matières

Terminologie et notations

Nos démonstrations sont présentées selon le style introduit par W.H.J Feijen dans [32, 34]. En général, une démonstration de l'équation $E_1 = E_2$ est présentée comme suit :

$$
\begin{array}{ll}
& E_1 \\
= & \quad \{ \text{ Justification. } \} \\
& \ldots \\
= & \quad \{ \text{ Justification. } \} \\
& E_2
\end{array}
$$

À la place de l'égalité $=$, tout autre opérateur transitif, comme $\Leftrightarrow$, $\Leftarrow$, $\Rightarrow$, $\subseteq$ et $\leq$, peut-être utilisé.

Nous utilisons les abréviations et les notations suivantes dans le reste de notre travail.

- *ssi* signifie *si et seulement si.*
- L'expression $E := F$ signifie que E est égal à F par définition.
- x, y, z désignent des variables.
- i, j, k désignent des indices.
- f, g, h désignent des fonctions.
- $\mu(f)$ et $\mu(x \mapsto f(x))$ désignent le plus petit point fixe de la fonction f.
- $\nu(f)$ et $\nu(x \mapsto f(x))$ désignent le plus grand point fixe de la fonction f.
- Soient X, Y et Z des ensembles. Si f est une fonction de type $X \to Y$ et g est une fonction de type $Y \to Z$, alors $g \circ f$ est une fonction de type $X \to Z$.
- E, P, Q, R, S, T ... désignent des relations.
- La priorité des opérateurs relationnels (ils sont définis dans le chapitre 2) est, en ordre décroissant : $(\bar{\ }, \breve{\ })$, $(;)$, $(\rhd, \lhd)$, $(\cap)$, $(\cup)$. Les opérateurs à l'intérieur d'une parenthèse ont la même priorité. À partir de la sous-section 2.3.1, le symbole de l'opérateur de composition $(;)$ est supprimé, c.-à-d. que nous écrivons QR pour désigner $Q\,;R$.
- Les opérateurs démoniaques $\Box$, $\sqcup$ et $\sqcap$ (définis dans le chapitre 3) ont respectivement la même priorité que $;$, $\cup$ et $\cap$.
- a, b, c, d, e et s désignent des relations incluses dans l'identité (identités partielles).

- Les expressions quantifiées ont généralement la forme suivante : $(Qx : D : E)$, où Q est un quantificateur, x la variable quantifiée (ou plusieurs variables), D est un prédicat caractérisant le domaine de x et E est le prédicat quantifié. Dans le cas où D est vrai, la forme précédente devient $(Qx : E)$.

Chapitre 1

Introduction

Nous abordons notre travail par une brève introduction historique sur le sujet de cette thèse. Nous décrivons d'abord les classes les plus importantes de sémantique d'un langage de programmation. La notion de sémantique a été traitée par différentes approches dont deux ont un lien avec notre recherche et elles seront décrites brièvement. Comme le non-déterminisme occupe une place considérable dans notre traitement, une description de cette notion s'impose.

La notion de sémantique n'est pas nouvelle ; rappelons ce qu'elle est.

1.1 Qu'est-ce qu'une sémantique ?

Selon Carl. A. Gunter [39], Michel Bréal [17] a introduit le mot *sémantique* dans le but d'étudier comment les mots changent de sens ou de signification. À son tour le mot *sémantique* a changé de sens et il est généralement défini comme l'étude du lien entre les mots et les phrases d'un langage (écrit ou parlé) et leur sens. La plupart des travaux ont été menés dans des domaines linguistiques ainsi que philosophiques qui étudient le sens des phrases du langage naturel. Avec l'introduction de l'informatique, un grand intérêt a été manifesté pour l'étude de la sémantique des langages de programmation.

1.2 Sémantique des langages de programmation

Un programme est caractérisé par au moins deux notions, la *syntaxe* et la *sémantique*. La syntaxe concerne la forme des expressions formant le programme. Pour sa part, la sémantique peut décrire entre autres le résultat de l'évaluation ou de l'exécution d'une expression ou d'un programme syntaxiquement correct et elle peut également décrire la manière de les exécuter ou de les évaluer.

Même dans les langages naturels, il existe une distinction entre la syntaxe et la sémantique. L'expression « thèse rédige je » n'est pas une phrase correcte car elle ne vérifie pas les règles de la grammaire française. Par contre, l'expression « la neige boit l'eau » est syntaxiquement correcte (sujet, verbe et complément) mais, car elle est incorrecte du point de vue sémantique puisqu'elle n'a pas de sens [41].

Citons certaines classes de langages de programmation [27] :

- Impératifs/fonctionnels : caractérisés par la présence de constructions décrivant les ordres donnés à une machine (l'affectation)/les programmes sont des fonctions dont les résultats dépendent des valeurs des arguments.
- Séquentiels/concurrents : les instructions sont exécutées en séquence/le langage admet quelques constructeurs qui permettent d'exécuter des instructions parallèles.
- Déterministes/non déterministes : chaque sortie est déterminée uniquement par l'entrée/pour une entrée correspond au moins une sortie.

La plupart des langages de programmation sont impératifs [60]. Nous considérons des programmes impératifs non déterministes qui terminent. Notre langage de programmation est le langage des commandes gardées de Dijkstra [30], qui permet l'expression du non-déterminisme.

1.3 Différentes sémantiques

Il y a plusieurs manières de définir la sémantique d'un langage de programmation ; chaque définition illustre un aspect particulier de la sémantique du langage et facilite certains raisonnements sur le langage. Nous introduisons brièvement les plus importantes : opérationnelle, dénotationnelle et axiomatique. La sémantique opérationnelle décrit comment un programme (syntaxiquement correct) est interprété comme une suite d'instructions ; les données initiales sont alors transformées séquentiellement pendant l'exécution du programme, instruction par instruction. Une définition opérationnelle de la sémantique ressemble à un interpréteur. L'idée est d'exprimer un mécanisme qui permet de déterminer l'effet de chaque programme. Pour plus de détails, voir [41, 72].

Contrairement à la sémantique opérationnelle, qui tient compte des états intermédiaires lors de l'exécution d'un programme, la sémantique dénotationnelle s'intéresse à la relation d'entrée/sortie calculée par ce programme et ignore les états intermédiaires. Elle associe une dénotation à chaque constructeur d'un langage de programmation. En d'autres termes, elle nous fournit un modèle explicite en associant à chaque constructeur une signification.

La sémantique axiomatique considère la définition des langages de programmation sous une autre perspective ; la sémantique d'un langage est vue comme une théorie des programmes écrits dans ce langage, elle ne définit pas ce que signifie un programme, mais seulement ce qui peut être prouvé à propos de ce programme ; elle exprime la sémantique d'un langage de programmation en associant au langage une théorie mathématique permettant de prouver les propriétés des programmes écrits dans ce langage.

Plusieurs travaux ont abordé la sémantique dénotationnelle, dont ceux de Scott [80, 81, 82] et Strachey [85, 86]. Les aspects théoriques sont présentés dans [54, 58, 65, 76, 92, 93].

En plus de vouloir associer à chaque programme un objet dans un modèle mathématique, parfois il faut une sémantique opérationnelle pour avoir plus d'information sur

l'exécution du programme (temps, mémoire ...). Généralement, pour éviter l'incompatibilité qui peut exister entre la sémantique dénotationnelle et la sémantique opérationnelle, on démontre formellement leur équivalence. Notre travail se situe dans ce champ d'étude. Dans cette perspective, nous donnons une sémantique opérationnelle ainsi qu'une sémantique dénotationnelle et nous démontrons leur équivalence.

1.4 Non-déterminisme

Un programme est déterministe si sa relation d'entrée/sortie est une *fonction*, c'est-à-dire qu'à chaque entrée correspond au plus une sortie. Un programme est non déterministe si sa relation d'entrée/sortie est une *relation*, c'est-à-dire qu'à chaque entrée peut correspondre plus d'une sortie. Le non-déterminisme est une notion très importante en informatique. Selon Sondergaard dans [84], Rabin et Scott [73] ont introduit l'automate fini non déterministe durant les années cinquante. Quant aux travaux qui ont explicitement traité le non-déterminisme dans les langages séquentiels impératifs, ils sont apparus avec McCarthy [59] et Floyd [35]. Un traitement très important du non-déterminisme se trouve dans les travaux de Dijkstra sur les commandes gardées [29, 30]. Dans le langage des commandes gardées de Dijkstra, le non-déterminisme est exprimé par la possibilité qu'il y ait plus d'une garde qui soit vérifiée.

Deux raisons principales peuvent motiver l'usage du non-déterminisme [60] :

- Premièrement, les programmes non déterministes peuvent être utiles pour modéliser le fonctionnement non déterministe du monde réel, comme dans les systèmes réactifs.

- La seconde concerne la volonté de ne pas sur-spécifier : dans certains cas, pour les mêmes données, il est nécessaire de pouvoir exprimer plusieurs déroulements possibles de l'exécution sans préciser quel choix est fait. Si le choix de la branche d'une instruction conditionnelle (par exemple) n'a pas d'importance lorsque les branches conduisent toutes à des résultats acceptables, alors le programmeur n'a pas à choisir explicitement.

Lors de l'exécution d'un programme non déterministe en un état, trois possibilités peuvent survenir : terminaison normale, terminaison anormale (par exemple, lors d'une division par zéro) ou boucle infinie. Le choix non déterministe nous oblige à distinguer deux types de non-déterminisme : le non-déterminisme *angélique* et le non-déterminisme *démoniaque*.

Avec le non-déterminisme angélique, tous les choix sont faits en faveur de la terminaison normale ; s'il y a possibilité que le programme termine normalement, alors la terminaison normale est sûre.

Avec le non-déterminisme démoniaque les choix sont faits en faveur de la non-terminaison ou de la terminaison anormale ; s'il y a possibilité que le programme ne termine pas ou termine anormalement, alors la non-terminaison ou la terminaison anormale est sûre. Ce qui correspond à la *pire exécution* du programme. Selon Sondergaard [84], l'usage des termes *angélique* et *démoniaque* est dû à C. A. R. Hoare.

1.5 Différentes approches

Nombreux sont les chercheurs qui se sont penchés sur l'étude des sémantiques. Par conséquent, un large éventail de logiques, modèles et calculs ont été élaborés. Ces travaux peuvent être regroupés en plusieurs approches : l'approche algébrique, l'approche de Scott avec les domaines de fonctions, l'approche relationnelle, qui sont des approches dénotationnelles, l'approche prédicative, qui est axiomatique, etc.

Dans ce qui suit, nous décrivons les deux approches qui nous intéressent le plus dans cette thèse.

1.5.1 Approche prédicative

L'approche prédicative inclut toutes les approches basées sur l'usage des prédicats. L'approche de Floyd [35] se base sur les assertions inductives. On s'appuie aujourd'hui dans ce domaine sur le travail postérieur de Hoare [43], qui propose un système logique pour prouver les propriétés des fragments de programmes. Les formules bien formées dans ce système sont appelées *formules pré-post* ou *triplets de Hoare*. Elles sont de la forme $\{P\}p\{Q\}$, où P est la précondition, p est le fragment de programme et Q est la postcondition. La notation $\{P\}p\{Q\}$ exprime la correction partielle de p par rapport à P et Q. Dans cette méthode, la terminaison doit être prouvée séparement. Ainsi, la théorie de Hoare est constituée d'axiomes et de règles d'inférence permettant de dériver certaines formules pré-post. Cette approche est nommée *sémantique pré-post*.

Une autre approche, basée sur les plus faibles préconditions, a été développée par Dijkstra [30]. Son but est de développer, à la place d'une théorie logique, un calcul des programmes qui nous permet de raisonner sur des fragments de programmes et sur les assertions associées à l'application des règles de transformation bien formalisées. Une autre différence par rapport à la sémantique pré-post est que cette théorie décrit la correction totale, c'est-à-dire que le programme doit non seulement vérifier la postcondition considérée mais aussi terminer. Les travaux de Dijkstra ont été poursuivis par Back [3, 4], qui a introduit les plus faibles préconditions pour les spécifications. Il permet le non-déterminisme non borné, c'est-à-dire qu'un état initial peut être associé à une infinité d'états finaux possibles. Le calcul de la plus faible précondition a été étendu par de Bakker [23] et Morgan [67]. Le non-déterminisme angélique dans la sémantique de la plus faible précondition a été considéré par Jacobs et Gries [47], Hehner [40], Broy [18], Hoare et He [45] et Morris [68], de même par Gardiner et Morgan [37]. Une approche algébrique de la plus faible précondition a aussi été utilisée par Hesselink [42].

1.5.2 Approche relationnelle

L'idée principale avec cette approche est de considérer que l'abstraction (la signification) d'une instruction est une relation binaire entre les entrées (états du programme) et les sorties (autres états). Pour les instructions déterministes, cette relation est une fonction. Mills [63, 64] et Linger [53] considèrent le cas déterministe où l'abstraction d'un programme est une fonction f. Si un programme est exécuté en un état s appartenant au domaine de la fonction f, alors il termine en un état final $f(s)$. Mills n'a pas considéré

le cas des programmes non déterministes. Mili [61] a remédié à ce problème en considérant les relations binaires au lieu des fonctions, chaque état initial pouvant avoir plus d'une sortie lors d'une exécution normale du programme. De Bakker [21, 22] a utilisé les relations pour définir la sémantique des schémas de programmes non déterministes. Sekerinski [83] a utilisé une approche prédicative avec une interprétation équivalente à celle de Mills et Mili.

Dans [33], R. M. Dijkstra a proposé une sémantique relationnelle des programmes. Nguyen [69] a proposé une approche algébrique relationnelle pour modéliser le langage de programmation de E. W. Dijkstra. Dans [70], Nguyen a fait une comparaison entre le modèle relationnel et le modèle basé sur les transformateurs de prédicats de Dijkstra et il a montré que le calcul démoniaque relationnel et le calcul par des transformateurs de prédicats sont isomorphes. Néanmoins, la majorité des travaux sur la sémantique utilisent l'approche prédicative.

Dans cette thèse, nous adoptons l'approche relationnelle pour plusieurs raisons :

- L'algèbre des relations présente une structure adéquate pour diverses manipulations mathématiques.
- L'algèbre des relations permet un traitement uniforme de la sémantique des programmes et du raffinement des spécifications.
- L'algèbre des relations permet le non-déterminisme et les opérations partielles.
- Les formules relationnelles manipulent les programmes et les spécifications directement, au lieu de manipuler les états contenus dans les relations.
- Le non-déterminisme des relations offre un outil de spécification plus adapté que les fonctions utilisées par Linger et Mills.

1.6 Contributions

Le but principal de cette thèse est de donner une sémantique opérationnelle du langage des commandes gardées de Dijkstra. Pour ce faire, nous associons à chaque programme un objet appelé *diagramme relationnel*. Un diagramme relationnel est essentiellement une représentation, dans le formalisme de l'algèbre des relations, d'un système de transitions dont les arcs sont étiquetés par des relations. Nous définissons ensuite la notion de *relation d'entrée/sortie démoniaque* d'un diagramme. Cette démarche permet d'associer à chaque programme (non déterministe) une relation d'entrée/sortie correspondant à sa pire exécution. Nous montrons ensuite que la relation ainsi obtenue est aussi celle qui est assignée par une sémantique dénotationnelle définie dans des travaux antérieurs [27]. En d'autres termes, nous montrons l'équivalence de notre sémantique opérationnelle avec une sémantique dénotationnelle relationnelle déjà connue [27]. L'intérêt de cette démonstration réside dans le fait que les définitions dénotationnelles classiques requièrent une bonne dose d'intuition pour être formulées et comprises, alors que l'association d'un diagramme à un programme est tout à fait naturelle.

Comme résultat intermédiaire, nous généralisons à un contexte non déterministe un théorème de Mills.

Nous présentons ici les résultats les plus importants de la thèse :

- La règle de vérification de boucle pour les programmes non déterministes. Cette règle qui est une généralisation d'un théorème de Mills, connu sous le nom de *règle de vérification de boucle de Mills* [63, 64]. Ce théorème (voir 4.14) est très utile dans plusieurs situations. Pour la vérification des programmes, ce théorème nous aide à déterminer si une relation donnée est effectivement la sémantique d'une boucle donnée. Dans le contexte de la construction de programmes, le théorème est plus utile dans l'autre direction : si nous avons une spécification (relation) W d'une boucle, nous pouvons trouver intuitivement les abstractions g et B de la condition de boucle et du corps de boucle et utiliser le théorème pour vérifier si ce choix de g et B est correct [89].

- La définition de la *relation d'entrée/sortie démoniaque*. Cette formulation est générale (équation 5.14) ; elle regroupe plusieurs types de diagrammes élémentaires (diagramme atomique, diagramme de séquence, diagramme de choix et diagramme de boucle). Il convient de noter que dans d'autres travaux [90, 91], nous avons présenté des résultats similaires en utilisant les graphes et les matrices.

- La formulation générale de la sémantique opérationnelle démoniaque d'un programme non déterministe (voir 7.9). Cette définition regroupe la séquence, le choix gardé et la boucle.

- La démonstration de l'égalité de la sémantique opérationnelle démoniaque d'un programme et de la sémantique dénotationnelle démoniaque. Notre approche opérationnelle consiste à associer un diagramme relationnel $\mathcal{Q}[\![p]\!]$ à un programme p et à calculer la relation d'entrée/sortie $\mathcal{E}(\mathcal{Q}[\![p]\!])$ du diagramme $\mathcal{Q}[\![p]\!]$. Cette relation $\mathcal{E}(\mathcal{Q}[\![p]\!])$ est définie sur le produit cartésien de l'ensemble des points de contrôle avec l'ensemble des états. Afin d'éliminer les points de contrôle, nous appliquons la fonction $\mathcal{F}$ à la relation $\mathcal{E}(\mathcal{Q}[\![p]\!])$. Finalement, nous obtenons $\mathcal{O}[\![p]\!] := \mathcal{F}(\mathcal{E}(\mathcal{Q}[\![p]\!]))$, qui est égale à $\mathcal{D}[\![p]\!]$, la sémantique dénotationnelle démoniaque du programme p. Autrement dit, nous avons montré que le diagramme de la figure 1.1 (au sens conventionnel du terme) commute.

1.7 Structure de la thèse

Cette thèse est divisée en huit chapitres. Outre ce chapitre qui sert d'introduction à notre recherche, le chapitre 2 présente les fondements mathématiques nécessaires pour notre travail. Le chapitre 3 est dédié à la présentation d'un ordre de raffinement et de la sémantique démoniaque dénotationnelle. Le chapitre 4 est consacré à la généralisation d'un théorème de Mills connu sous le nom de *règle de vérification de boucle*, originalement donné dans un contexte déterministe ; nous le généralisons à un contexte non déterministe. Dans le chapitre 5, nous définissons la notion de diagramme et les différents types

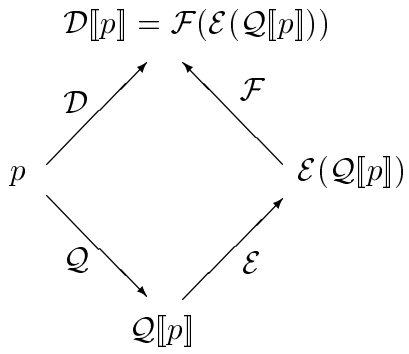


Figure 1.1: $\mathcal{O}[\![p]\!] := \mathcal{F}(\mathcal{E}(\mathcal{Q}[\![p]\!])) = \mathcal{D}[\![p]\!]$

de diagrammes. Ces notions servent à définir la *relation d'entrée/sortie démoniaque* d'un diagramme. Le chapitre 6 est consacré aux diagrammes composés. En utilisant les résultats du chapitre 5, nous y présentons une méthode de calcul de la relation d'entrée/sortie d'un diagramme composé. Dans le chapitre 7, nous définissons la sémantique opérationnelle démoniaque d'un programme non déterministe et nous montrons qu'elle est équivalente à la sémantique dénotationnelle démoniaque de ce programme. Finalement, une conclusion sur ce travail ainsi que des possibilités de travaux futurs sont présentées dans le chapitre 8.

Chapitre 2

Fondements mathématiques

Ce chapitre est consacré à la présentation des concepts mathématiques utilisés tout au long de cette thèse. Dans la première section, nous donnons quelques notions sur la théorie élémentaire des relations. La deuxième section présente certaines structures ordonnées ainsi que quelques résultats sur les points fixes. Le calcul des relations est abordé dans la troisième section, qui introduit également quelques notions relationnelles utiles pour le reste de notre travail.

2.1 Théorie élémentaire des relations

En suivant Alfred Tarski [87], nous distinguons deux niveaux d'abstraction dans l'étude des relations binaires : *la théorie élémentaire des relations* et *le calcul des relations*. Le premier niveau définit les relations comme ensembles (de paires) et le deuxième définit les relations comme objets élémentaires sur lesquels des opérations sont définies et étudiées d'un point de vue algébrique. Dans cette thèse, nous avons besoin des deux niveaux d'abstraction. Le premier nous aide à donner nos exemples et à définir nos spécifications (relations), et le deuxième nous est utile dans nos preuves et formules. Donc, dans ce chapitre nous présentons les deux niveaux d'abstraction mais, comme l'étude des relations n'est pas notre but ici, nous donnons plusieurs propriétés et lois sur les relations sans les démontrer.

Une relation R d'un ensemble X vers un ensemble Y est un sous-ensemble de l'ensemble de toutes les paires (x, y) où $x \in X$ et $y \in Y$. Formellement,

$$R \subseteq X \times Y = \{(x, y) \mid x \in X \text{ et } y \in Y\}.$$

Si $X = Y$, nous disons que R est *homogène* sur X.

(2.1) **Remarque.** Les relations sur des ensembles finis peuvent être représentées par des matrices. Par exemple, la relation $R = \{(a, b), (a, c), (b, d), (c, d), (d, e)\}$ peut être représentée par la matrice suivante :

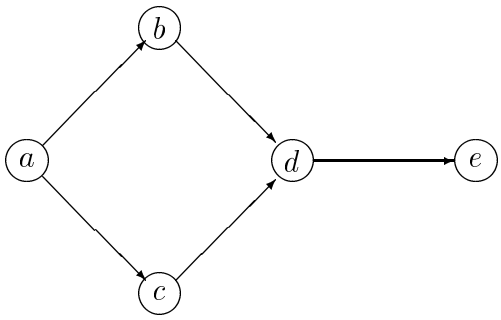


Figure 2.1: Le graphe associé à la relation R

$$R = \begin{array}{c} \\ a \\ b \\ c \\ d \\ e \end{array} \begin{array}{c} \begin{array}{ccccc} a & b & c & d & e \end{array} \\ \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

■

Les graphes et les relations sont aussi étroitement liés. Donnons la définition d'un graphe.

(2.2) **Définition.** Un *graphe* $G = (X, R)$ consiste en un ensemble fini de sommets X et d'une relation $R \subseteq X \times X$. ■

Toute relation finie peut être interprétée comme une représentation d'un graphe et vice-versa. Le graphe 2.1 correspond à la relation R ci-dessus.

Dans la notation matricielle, une entrée 0 correspond à l'absence d'arc entre deux sommets du graphe (l'absence de la paire dans la relation) et une entrée 1 signifie le contraire.

Comme les relations sont des ensembles, elles sont ordonnées par inclusion. La plus petite relation entre les ensembles X et Y est la relation *vide* (dite aussi nulle ou zéro), notée $\emptyset_{XY}$, et la plus grande relation, appelée relation *universelle*, est notée L_{XY}. Une relation particulière définie pour chaque ensemble X est la relation *identité*, notée $I_X := \{(x, x) \mid x \in X\}$. L'ensemble des éléments de X qui ont des images par R est appelé *domaine* de R, noté $\mathrm{dom}(R)$, et celui des images est noté $\mathrm{img}(R)$. Formellement,

$$\mathrm{dom}(R) := \{x \mid (\exists y : (x, y) \in R)\},$$

$$\mathrm{img}(R) := \{y \mid (\exists x : (x, y) \in R)\}.$$

2.1.1 Opérations sur les relations

Les relations sont des ensembles particuliers et, à ce titre, nous pouvons leur appliquer les opérations ensemblistes usuelles, soit l'union ($\cup$), l'intersection ($\cap$) et la complémentation ($\bar{}$). Les relations sont ordonnées par inclusion. De plus, leur structure nous permet de définir d'autres opérateurs qui sont :

(a) L'inverse d'une relation R, noté $R^{\smile}$:

$$R^{\smile} = \{(x, y) | (y, x) \in R\}.$$

(b) Pour $R \subseteq X \times Z$ et $S \subseteq Z \times Y$, nous définissons la composition de R et S, notée $R ; S$, par :

$$R ; S = \{(x, y) \mid (\exists z : z \in Z : (x, z) \in R \text{ et } (z, y) \in S)\}.$$

Remarquons que $R ; S \subseteq X \times Y$.

2.1.2 Propriétés des relations

Dans ce qui suit, nous donnons les définitions de différentes propriétés des relations.

(2.3) **Définition.** Une relation $R \subseteq X \times X$ est :

(a) réflexive ssi $I \subseteq R$, c.-à-d. $(\forall x : (x, x) \in R)$,

(b) transitive ssi $R ; R \subseteq R$, c.-à-d. $(\forall x, y, z : (x, z) \in R \text{ et } (z, y) \in R \Rightarrow (x, y) \in R)$,

(c) symétrique ssi $R \subseteq R^{\smile}$, c.-à-d. $(\forall x, y : (x, y) \in R \Leftrightarrow (y, x) \in R)$,

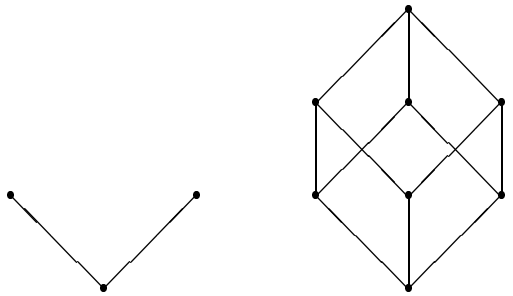
(d) antisymétrique ssi $R \cap R^{\smile} \subseteq I$, c.-à-d. $(\forall x, y : (x, y) \in R \text{ et } (x, y) \in R^{\smile} \Rightarrow x = y)$,

(e) une équivalence ssi R vérifie les propriétés (a), (b) et (c),

(f) un ordre ssi R vérifie les propriétés (a), (b) et (d),

(g) un pré-ordre ssi R vérifie les propriétés (a) et (b). ∎

Le fait de considérer les relations comme ensembles de paires ordonnées est un concept très simple en soi, mais vu l'usage important des relations au cours de notre travail, il est préférable de « typer » une relation $R \subseteq X \times Y$ en rappelant son ensemble de départ X et son ensemble d'arrivée Y en écrivant $R : X \leftrightarrow Y$. Les notations I_X, $\emptyset_{XY}$ et L_{XY} signifient respectivement $I : X \leftrightarrow X$, $\emptyset : X \leftrightarrow Y$ et $L : X \leftrightarrow Y$. Si $R : X \leftrightarrow Y$ est une fonction f, nous écrivons $f : X \to Y$, nous utilisons la notation usuelle $y = f(x)$ au lieu de $(x, y) \in f$. Pour deux fonctions $f : X \to Y$ et $g : Y \to Z$, la fonction composée $g \circ f$ est définie par $(g \circ f)(x) = g(f(x)) = (f ; g)(x)$.



(a) (b)

Figure 2.2: Deux ensembles ordonnés et leurs diagrammes de Hasse

2.2 Structures ordonnées

Soit R une relation d'ordre sur un ensemble X. La paire (X, R) est appelée *ensemble ordonné*. Usuellement « R » est remplacée par le symbole « $\leq$ ». Si X est un ensemble fini, il est parfois instructif de représenter l'ensemble $(X, \leq)$ par un diagramme de Hasse où x est lié à y ssi $x \leq y$ et s'il n'existe aucun élément $z \in X$ avec $x < z < y$, où $x < y$ signifie $x \leq y$ et $x \neq y$. La figure 2.2 présente deux exemples (par convention, les arcs sont orientés de bas en haut). Pour plus de détails voir [20]. Généralement, les éléments extrêmes d'un ensemble ordonné jouent un rôle important dans la structure de celui-ci. Dans ce qui suit, nous présentons leur définition.

(2.4) **Définition.** Soient $(X, \leq)$ un ensemble ordonné et $Y \subseteq X$.

(a) Nous disons que y est un *majorant* de Y ssi

$$(\forall x : x \in Y : x \leq y).$$

Le plus petit des majorants de Y (s'il existe) est appelé la *borne supérieure* ou le *supremum* de Y, et est noté $\bigvee Y$.

(b) Dualement, y est un *minorant* de Y ssi

$$(\forall x : x \in Y : y \leq x).$$

Le plus grand des minorants de Y (s'il existe) est appelé la *borne inférieure* ou l'*infimum* de Y, et est noté $\bigwedge Y$.

Nous n'exigeons pas que y soit dans le sous-ensemble Y. Les bornes supérieures et les bornes inférieures n'existent pas toujours. En particulier, comme tout élément est un majorant de l'ensemble vide, le supremum d'un ensemble vide n'existe que si $(X, \leq)$ admet un plus petit élément.

Un sous-ensemble Y est une *chaîne* s'il est *linéairement ordonné* (ou encore *totalement ordonné*), c'est-à-dire si $x \leq y$ ou $y \leq x$ pour tout $x, y \in Y$. ∎

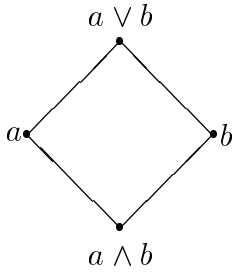


Figure 2.3: Treillis à quatre éléments

2.2.1 Treillis

(2.5) **Définition.** Un *treillis* est un ensemble ordonné dans lequel tout sous-ensemble à deux éléments $\{x, y\}$ admet un supremum, $x \vee y = \bigvee\{x, y\}$ et un infimum $x \wedge y = \bigwedge\{x, y\}$. ∎

La figure 2.3 représente un treillis à quatre éléments.

Soit X un ensemble avec deux opérations binaires $\vee$ et $\wedge$ satisfaisant les propriétés suivantes :

(a) associativité : $(x \vee y) \vee z = x \vee (y \vee z)$ et $(x \wedge y) \wedge z = x \wedge (y \wedge z)$,

(b) commutativité : $x \vee y = y \vee x$ et $x \wedge y = y \wedge x$,

(c) idempotence : $x \vee x = x$ et $x \wedge x = x$,

(d) absorption : $(x \vee y) \wedge x = x$ et $(x \wedge y) \vee x = x$.

Pour tout $x, y \in X$, nous définissons une relation d'ordre $\leq$ sur X par

$$x \leq y \quad \Leftrightarrow \quad x \vee y = y \quad \text{(de manière équivalente } x \leq y \quad \Leftrightarrow \quad x \wedge y = x\text{)}.$$

On montre que $(X, \leq)$ est un treillis. Ainsi, un treillis peut être vu comme un ensemble ordonné $(X, \leq)$ ou une structure algébrique $(X, \vee, \wedge)$.

Dans ce qui suit, nous définissons différents types de treillis.

(2.6) **Définition.** Nous disons que le treillis $(X, \leq)$ est :

- *borné* s'il admet un plus petit élément $\perp$ et un plus grand élément $\top$,
- *complet* si tout sous-ensemble Y (même l'ensemble vide) admet un supremum $\bigvee Y$. Dans ce cas, Y admet aussi un infimum $\bigwedge Y$,

- *complémenté* s'il est borné et si pour chaque $x \in X$ il existe un élément, noté $\overline{x}$ et appelé *complément* de x, tel que $x \vee \overline{x} = \top$ et $x \wedge \overline{x} = \bot$,
- *distributif* si $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ et $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$,
- *booléen* s'il est borné, distributif et complémenté. ∎

Dans un treillis distributif, le complément d'un élément est unique.

(2.7) **Définition.** Un élément a d'un treillis X avec un plus petit élément $\bot$, est un *atome*, si $a \neq \bot$ et s'il n'existe aucun élément $x \in X$ tel que $\bot < x < a$. On dit que X est *atomique* si pour tout élément $x \in X$, $x \neq \bot$, il existe un atome a tel que $a \leq x$. ∎

(2.8) **Définition.** Un $\vee$-*demi-treillis* est un ensemble ordonné dans lequel tout sous-ensemble à deux éléments $\{x, y\}$ admet un supremum, $x \vee y = \bigvee\{x, y\}$. Dualement, un $\wedge$-*demi-treillis* est un ensemble ordonné dans lequel tout sous-ensemble à deux éléments $\{x, y\}$ admet un infimum $x \wedge y = \bigwedge\{x, y\}$. Un $\vee$-demi-treillis est complet (supérieurement complet) si tout sous-ensemble non vide Y admet un supremum $\bigvee Y$. Dualement un $\wedge$-demi-treillis est complet (inférieurement complet) si tout sous-ensemble non vide Y admet un infimum $\bigwedge Y$. ∎

2.2.2 Connections de Galois

Il y a plusieurs définitions équivalentes des connections de Galois [2]. Nous choisissons celle qui est proposée par Backhouse *et al.* [10].

(2.9) **Définition.** Soient $(S, \leq_S)$ et $(S', \leq_{S'})$ des ensembles ordonnés. Une paire (f, g) de fonctions, où $f : S \to S'$ et $g : S' \to S$, forme une *connection de Galois* ssi, pour tout $x \in S$ et $y \in S'$,

$$f(x) \leq_{S'} y \Leftrightarrow x \leq_S g(y).$$

∎

2.2.3 Points fixes

Soient $(X, \leq)$ un ensemble ordonné. Une fonction $f : X \to X$ est dite une *endofonction* [10]. Un point fixe de f est un élément $x \in X$ tel que $x = f(x)$. Un *pré-point fixe* de la fonction f est un élément $x \in X$ tel que $f(x) \leq x$. Un *post-point fixe* de la fonction f est un élément $x \in X$ tel que $x \leq f(x)$. Le plus petit point fixe de f, noté $\mu(f)$ (s'il existe), est le plus petit élément de l'ensemble des points fixes de f. Dualement, le plus grand point fixe de f, noté $\nu(f)$ (s'il existe), est le plus grand élément de l'ensemble des points fixes de f. La fonction f est dite *monotone* par rapport à $\leq$ ssi $x \leq x' \Rightarrow f(x) \leq f(x')$. La fonction est dite *antimonotone* par rapport à $\leq$ ssi $x \leq x' \Rightarrow f(x') \leq f(x)$.

En 1928, Knaster a prouvé que toute fonction monotone (par rapport à l'inclusion) sur l'ensemble des sous-ensembles d'un ensemble U admet au moins un point fixe [52]. Tarski a généralisé ce théorème pour un treillis en 1939 (information tirée de [8]). Cette généralisation a été publiée en 1955 [88]. La voici.

(2.10) **Théorème.** *(Knaster-Tarski) Toute endofonction monotone sur un treillis complet admet un plus petit point fixe, qui coïncide avec son plus petit pré-point fixe.* ∎

Le résultat est valable aussi pour le plus grand point fixe $\nu(f)$. Nous présentons dans ce qui suit quelques propriétés des points fixes $\mu(f)$ et $\nu(f)$ (pour plus de détails, voir [8, 20]). Dans le cas où il est nécessaire de donner l'expression de la fonction $f(x)$, nous écrivons $\mu(x \mapsto f(x))$ pour le plus petit point fixe de f et dualement $\nu(x \mapsto f(x))$ pour son plus grand point fixe.

(2.11)
(a) $\mu(f) = \bigwedge\{x \mid f(x) = x\} = \bigwedge\{x \mid f(x) \leq x\}$,
(b) $\nu(f) = \bigvee\{x \mid f(x) = x\} = \bigvee\{x \mid x \leq f(x)\}$,
(c) $\mu(f) \leq \nu(f)$,
(d) $f(y) \leq y \Rightarrow \mu(f) \leq y$,
(e) $y \leq f(y) \Rightarrow y \leq \nu(f)$,
(f) $f(\mu(f)) = \mu(f)$,
(g) $f(\nu(f)) = \nu(f)$.

La comparaison des points fixes des fonctions est parfois très utile pour la comparaison des sémantiques des programmes. La proposition suivante présente quelques résultats dans ce sens.

(2.12) **Proposition.** *Soit $(X, \leq)$ un ensemble ordonné et deux endofonctions f et g. Soit également la relation $\ll$ sur l'ensemble des endofonctions sur X, définie comme suit :*

$$f \ll g \Leftrightarrow (\forall x : x \in X : f(x) \leq g(x)).$$

Nous avons les propriétés suivantes ($+$ est une opération binaire monotone sur X) :

(a) *μ monotone* $f \ll g \Rightarrow \mu(f) \leq \mu(g)$,
(b) *règle de permutation* $\mu(f \circ g) = f(\mu(g \circ f))$,
(c) *règle de la diagonale* $\mu(x \mapsto x + x) = \mu(x \mapsto \mu(y \mapsto x + y))$,
(d) *μ-fusion simple* $f \circ g = g \circ h \Rightarrow \mu(f) = g(\mu(h))$.

L'opérateur ν donnant le plus grand point fixe a des propriétés similaires. ∎

Pour les preuves, voir [8].

(2.13) **Définition.** Soit f une endofonction sur un treillis booléen. La fonction *duale* de f est $f^{\#}(x) := \overline{f(\overline{x})}$. ∎

Le prochain lemme nous présente le lien entre les points fixes d'une fonction sur un treillis booléen et ceux de sa fonction duale.

(2.14) **Lemme.** *Soit f une endofonction sur un treillis booléen et $f^{\#}$ sa fonction duale. Si x est un point fixe de f, alors*

(a) *$\overline{x}$ est un point fixe de $f^{\#}$,*

(b) *$\nu(f^{\#}) = \overline{\mu(f)}$,*

(c) *$\mu(f^{\#}) = \overline{\nu(f)}$.* ∎

Ce lemme est important pour montrer que les propriétés de la proposition 2.12 sont valables aussi pour le plus grand point fixe [8].

2.2.4 Algèbres booléennes

Une *algèbre booléenne* est un treillis booléen $(X, \vee, \wedge, \overline{\ }, \bot, \top)$. Les algèbres booléennes sont les versions algébriques du calcul des ensembles. Le modèle standard de cette structure est la collection de tous les sous-ensembles d'un ensemble X, $(\mathcal{P}(X), \cup, \cap, \overline{\ }, \emptyset, X)$, connue sous le nom de l'ensemble des parties de X. La figure 2.2(b) montre le diagramme de Hasse d'une telle algèbre (où X est un ensemble à 3 éléments). Une *algèbre booléenne atomique complète* est un treillis booléen atomique complet.

Les propriétés suivantes sont vérifiées dans une algèbre booléenne. Pour plus de détails, voir [78].

(2.15) **Théorème.** *Soient x_1, x_2 et y des éléments d'une algèbre booléenne.*

(a) $x_1 \vee x_1 = x_1 \wedge x_1 = x_1$,

(b) $x_1 \wedge x_2 \leq x_i$, $(i = 1, 2)$,

(c) $x_1 \leq x_2 \Rightarrow x_1 \wedge y \leq x_2 \wedge y$,

(d) $y \leq x_1$ et $y \leq x_2 \Leftrightarrow y \leq x_1 \wedge x_2$,

(e) $y \wedge (\bigvee_i x_i) = \bigvee_i y \wedge x_i$,

(f) $x_i \leq x_1 \vee x_2$ $(i = 1, 2)$,

(g) $x_1 \leq y$ et $x_2 \leq y \quad \Leftrightarrow \quad x_1 \vee x_2 \leq y$,

(h) $y \vee (\bigwedge_i x_i) = \bigwedge_i y \vee x_i$,

(i) $x \leq y \quad \Leftrightarrow \quad x \wedge \overline{y} \leq \bot$,

(j) $x_1 \leq x_2 \vee y \quad \Leftrightarrow \quad x_1 \wedge \overline{x_2} \leq y$,

(k) $\overline{\overline{x_1}} = x_1$,

(l) $x_1 \leq x_2 \Leftrightarrow \top \leq \overline{x_1} \vee x_2$,

(m) $x_1 \leq x_2 \Leftrightarrow \overline{x_2} \leq \overline{x_1}$,

(n) $\overline{\bigvee_i x_i} = \bigwedge_i \overline{x_i}$,

(o) $\overline{\bigwedge_i x_i} = \bigvee_i \overline{x_i}$,

(p) $x \vee \bot = x$,

(q) $x \wedge \top = x$. ∎

Pour les besoins de notre travail, nous achevons cette section en présentant les deux propriétés suivantes :

(2.16) Si $x \wedge y = \bot$ alors $(x \leq y \vee z \quad \Leftrightarrow \quad x \leq z)$.

$$
\begin{array}{ll}
& x \leq y \vee z \\
\Rightarrow & \quad \{ \text{ Théorème 2.15(c). } \} \\
& x \wedge x \leq x \wedge (y \vee z) \\
\Rightarrow & \quad \{ \text{ Théorème 2.15(a,e). } \} \\
& x \leq (x \wedge y) \vee (x \wedge z) \\
\Rightarrow & \quad \{ \ x \wedge y = \bot \ (2.15(\text{p,d}). \ \} \\
& x \leq z.
\end{array}
$$

L'autre sens est évident.

La prochaine propriété est connue sous le nom de *règle de l'égalité indirecte*.

(2.17) $x = y \quad \Leftrightarrow \quad (\forall z : z \leq x \Leftrightarrow z \leq y)$.

Sa démonstration est simple. L'implication $\Rightarrow$ est évidente. Dans l'autre direction, prenons $z := x$. De $z \leq x \Rightarrow z \leq y$, nous obtenons $x \leq y$. De même en prenant $z := y$, nous obtenons $y \leq x$. D'où $x = y$, par antisymétrie. ∎

Nous pouvons maintenant définir des structures algébriques abstraites possédant plusieurs propriétés des relations. Elles sont basées sur les algèbres booléennes enrichies par d'autres opérateurs qui sont la composition ; et l'inverse $^\smile$ ainsi qu'un élément particulier I (la relation identité). Nous pourrions continuer à utiliser des symboles différents pour distinguer les structures abstraites des structures concrètes (par exemple, $\vee$ et $\wedge$ versus $\cup$ et $\cap$). Comme cette distinction ne nous est pas utile, nous utiliserons les notations concrètes. Les symboles $\wedge$ et $\vee$ seront utilisés par la suite pour exprimer respectivement la conjonction et la disjonction.

2.3 Calcul des relations

L'origine du calcul des relations remonte au siècle dernier avec les travaux de De Morgan, Dedekind et Schröder, ainsi qu'au début du présent siècle avec ceux de Peirce. Leur étude a été ravivée par les travaux de Chin et Tarski [19, 87]. Pour plus de détails sur l'algèbre des relations, voir [19, 48, 49, 50, 51, 55, 56]. Dans ce qui suit, nous donnons une définition de l'algèbre des relations et des modèles importants des axiomes définissant cette algèbre. La majorité de nos définitions proviennent de [78].

2.3.1 Algèbres de relations

(2.18) **Définition.** Une *algèbre de relations hétérogène abstraite* est une structure algébrique $(\mathcal{R}, \cup, \cap, \bar{}, ^\smile, ;, \emptyset, L, I)$ sur un ensemble non vide $\mathcal{R}$ d'éléments appelés *relations*, et telle que les conditions suivantes sont satisfaites.

(a) Toute relation R dans $\mathcal{R}$ appartient à un sous-ensemble $\mathcal{B}_R$ de l'ensemble $\mathcal{R}$ tel que la structure $(\mathcal{B}_R, \cup, \cap, \bar{}, \emptyset, L)$ est une algèbre booléenne atomique complète.

(b) Toute relation R admet un inverse $R^\smile$.

(c) Étant données deux relations Q et R appartenant à des algèbres booléennes $\mathcal{B}_Q$ et $\mathcal{B}_R$ respectivement, une *composition* associative $Q;R$ est définie. Il existe des identités à droite et à gauche (notées I) pour chaque ensemble $\mathcal{B}_R$ de relations. L'existence d'une composition $Q;R$ implique que $P;R$ est définie pour toutes les relations P dans $\mathcal{B}_Q$. Les compositions $R^\smile;R$ et $R;R^\smile$ sont toujours définies.

(d) La règle de Schröder $P;Q \subseteq R \Leftrightarrow P^\smile;\overline{R} \subseteq \overline{Q} \Leftrightarrow \overline{R};Q^\smile \subseteq \overline{P}$ est toujours valide quand une des trois expressions est définie.

(e) La règle de Tarski est valide : $L;R;L = L$ ssi $R \neq \emptyset$.

Si $R^\smile \in \mathcal{B}_R$, alors R est dite *homogène*. ∎

Par souci de simplification, tous les éléments zéros, universels et identités sont notés respectivement par $\emptyset$, L et I (mais nous pouvons utiliser des indices pour les distinguer si c'est nécessaire).

La priorité des opérateurs relationnels, par ordre décroissant, est comme suit : $^-, ^\smile$, ont la même priorité, ils sont suivis par (;), puis par $\cap$ et, finalement, par $\cup$. La portée des opérateurs $\bigcup_i$ et $\bigcap_i$ s'étend vers la droite aussi loin que le permettent les parenthèses. Dans ce qui suit, le symbole de l'opérateur de composition (;) est supprimé, c.-à-d. que nous écrivons QR pour désigner $Q;R$.

Présentons quelques exemples de modèles vérifiant ces axiomes.

(2.19) **Exemples.**

(a) L'algèbre des relations binaires entre des ensembles différents est une algèbre de relations très importante, car c'est la plus utilisée. Soient $S_1, ..., S_n$ des ensembles.

$$\mathcal{R} := \{R \mid R \subseteq S_i \times S_j, 1 \leq i, j \leq n\},$$

avec les opérateurs relationnels, est une algèbre de relations. Les opérations $\cup$ et $\cap$ entre des relations Q et R sont définies ssi Q et R ont le même type. Une relation est homogène ssi $R : S_i \leftrightarrow S_i$ pour un certain i. La composition QR est définie ssi $Q : S_i \leftrightarrow S_j$ et $R : S_j \leftrightarrow S_k$ pour certains i, j, k.

(b) L'ensemble de toutes les relations binaires homogènes sur un ensemble X, noté $\mathrm{Rel}(X) := (\mathcal{P}(X \times X), \cup, \cap, ^\smile, ^-, ;, \emptyset, X \times X, I_X)$ est une algèbre de relations dite *algèbre pleine* des relations sur X, où $\mathcal{P}(X \times X)$ est l'ensemble de tous les sous-ensembles de $X \times X$.

(c) L'algèbre des matrices booléennes est une autre algèbre de relations importante. Nous donnons comme exemple les matrices dont les entrées sont les valeurs de l'algèbre booléenne $\{0, 1\}$. Pour respecter la convention usuelle, nous utilisons les valeurs booléennes $\{0, 1\}$ au lieu de $\{\emptyset, L\}$. Deux matrices sont compatibles ssi elles ont la même dimension. La composition QR est définie ssi le nombre de

colonnes de Q est égal au nombre de lignes de R. Les matrices homogènes sont les matrices carrées. Voici quelques exemples :

$$I_{2\times 2} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \emptyset_{1\times 2} = \begin{pmatrix} 0 & 0 \end{pmatrix}, \qquad L_{2\times 3} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}^{\smile} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

(d) Un autre modèle est celui de l'algèbre des matrices dont les entrées sont des relations provenant d'une algèbre homogène [78]. Deux matrices ont le même type ssi elles ont la même dimension. La composition QR est définie ssi le nombre de colonnes de Q est égal au nombre de lignes de R. Les matrices homogènes sont les matrices carrées. L'entrée de la matrice R sur la i^{e} ligne et la j^{e} colonne est notée R_{ij}. Les opérations sont définies comme suit :

$$\begin{array}{ll} (R \cup S)_{ij} = R_{ij} \cup S_{ij}, & (\overline{R})_{ij} = \overline{R_{ij}}, \qquad (RS)_{ij} = \bigcup_k R_{ik} S_{kj}, \\ (R \cap S)_{ij} = R_{ij} \cap S_{ij}, & (R^{\smile})_{ij} = (R_{ji})^{\smile}. \end{array} \tag{2.20}$$

Les relations constantes sont définies par :

$$L_{ij} = L, \quad \emptyset_{ij} = \emptyset, \quad I_{ij} = \begin{cases} I & \text{si } i = j \\ \emptyset & \text{sinon.} \end{cases}$$

∎

À partir de la définition 2.18, les règles usuelles du calcul relationnel peuvent être dérivées (voir [14, 19, 78, 79]). Nous en rappelons quelques-unes, incluant certaines lois booléennes exprimées avec la nouvelle notation (comparer avec le théorème 2.15).

(2.21) **Théorème.** *Soient P, Q, R des relations et X un ensemble quelconque d'indices.*

1. $\overline{\bigcup_{i\in X} R_i} = \bigcap_{i\in X} \overline{R_i}$,
2. $\overline{Q \cup R} = \overline{Q} \cap \overline{R}$,
3. $\overline{\bigcap_{i\in X} R_i} = \bigcup_{i\in X} \overline{R_i}$,
4. $\overline{Q \cap R} = \overline{Q} \cup \overline{R}$,
5. $(Q \cap R) \cup \overline{R} = Q \cup \overline{R}$,
6. $P \cap Q \subseteq R \;\Leftrightarrow\; P \subseteq \overline{Q} \cup R$,
7. $Q \subseteq R \;\Leftrightarrow\; \overline{R} \subseteq \overline{Q}$,
8. $Q(\bigcup_{i\in X} R_i) = \bigcup_{i\in X} QR_i$,
9. $P(Q \cup R) = PQ \cup PR$,
10. $(\bigcup_{i\in X} Q_i)R = \bigcup_{i\in X} Q_i R$,
11. $(P \cup Q)R = PR \cup QR$,
12. $Q(\bigcap_{i\in X} R_i) \subseteq \bigcap_{i\in X} QR_i$,
13. $P(Q \cap R) \subseteq PQ \cap PR$,
14. $(\bigcap_{i\in X} Q_i)R \subseteq \bigcap_{i\in X} Q_i R$,
15. $(P \cap Q)R \subseteq PR \cap QR$,
16. $Q \subseteq R \;\Rightarrow\; PQ \subseteq PR$,
17. $P \subseteq Q \;\Rightarrow\; PR \subseteq QR$,
18. $R\emptyset = \emptyset R = \emptyset$,
19. $Q \subseteq R \;\Leftrightarrow\; Q^{\smile} \subseteq R^{\smile}$,

20. $(\bigcup_{i\in X} R_i)^\smile = \bigcup_{i\in X} R_i^\smile$,

21. $(Q \cup R)^\smile = Q^\smile \cup R^\smile$,

22. $(\bigcap_{i\in X} R_i)^\smile = \bigcap_{i\in X} R_i^\smile$,

23. $(Q \cap R)^\smile = Q^\smile \cap R^\smile$,

24. $(QR)^\smile = R^\smile Q^\smile$,

25. $R^{\smile\smile} = R$,

26. $I^\smile = I$,

27. $\overline{R}^\smile = \overline{R^\smile}$,

28. $PQ \cap R \subseteq (P \cap RQ^\smile)(Q \cap P^\smile R)$,

29. $PQ \cap R \subseteq P(Q \cap P^\smile R)$,

30. $PQ \cap R \subseteq (P \cap RQ^\smile)Q$,

31. $LL = L$,

32. $(\bigcap_{i\in X} R_i L)L = \bigcap_{i\in X} R_i L$,

33. $(QL \cap RL)L = QL \cap RL$,

34. $(\bigcup_{i\in X} R_i L)L = \bigcup_{i\in X} R_i L$,

35. $(QL \cup RL)L = QL \cup RL$,

36. $(P \cap QL)R = PR \cap QL$,

37. $(P \cap LQ^\smile)R = P(R \cap QL)$,

38. $QLR = QL \cap LR$,

39. $\overline{RL}L = \overline{RL}$,

40. $R = (I \cap RR^\smile)R$. ∎

Pour les preuves voir [14, 19, 78, 79]

(2.22) **Remarque.** Parfois, au lieu de référer aux lois 8, 9, 10 et 11, nous disons que l'opération ; est distributive. Nous disons aussi que ; est monotone au lieu de référer aux lois 16 et 17. ∎

Dans ce qui suit, nous donnons les définitions de certaines propriétés des relations.

(2.23) **Définition.** Une relation R est :

(a) *déterministe* ssi $R^\smile R \subseteq I$,

(b) *totale* ssi $L = RL$ (équivalent à $I \subseteq RR^\smile$),

(c) une *application* ssi elle est totale et déterministe,

(d) *injective* ssi $R^\smile$ est déterministe (c.-à-d. $RR^\smile \subseteq I$),

(e) *surjective* ssi $R^\smile$ est totale (c.-à-d. $LR = L$, ou encore $I \subseteq R^\smile R$),

(f) une *identité partielle* ssi $R \subseteq I$ (sous-identité),

(g) un *vecteur* ssi $R = RL$ (les vecteurs sont souvent dénotés par la lettre v),

(h) un *point* ssi $R \neq \emptyset$, $R = RL$ et $RR^\smile \subseteq I$. ∎

(2.24) **Remarque.** Si x et y sont deux points différents, alors $x^\smile y = \emptyset$ et $x^\smile x = L$ [78]. ∎

Une *fonction* est une relation déterministe.

Soit v un vecteur ; la relation $v \cap R$ est appelée *prérestriction* de R à v et $v^\smile \cap R$ est appelée *postrestriction* de R à v.

(2.25) **Remarque.** Une autre manière de restreindre une relation consiste à utiliser des identités partielles. Si a est une identité partielle, alors la prérestriction de R à a est aR et la postrestriction de R à a est Ra. ∎

Les vecteurs RL et $R^\smile L$ sont des vecteurs particuliers caractérisant respectivement le domaine et l'image de R. L'ensemble des vecteurs d'un type donné est une algèbre booléenne complète [78].

Dans une algèbre de matrices booléennes, un vecteur est une matrice dont les lignes sont constantes et un point est un vecteur avec une seule ligne non nulle.

Dans une algèbre de relations sur des ensembles, un vecteur de type $X \leftrightarrow Y$ est une relation de la forme $V \times Y$, où $V \subseteq X$. Un vecteur peut aussi être vu comme un ensemble de points ou un prédicat.

(2.26) **Exemple.** Soient $X = \{0, 1, 2\}$ et $V = \{0, 1\}$. Alors

$$v := V \times X = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$$

est un vecteur qui correspond à l'ensemble des points V. L'identité partielle correspondant à v est $a = \{(0,0), (1,1)\}$.

Prenons $R := \{(0,1), (0,2), (2,1)\}$, v et a étant le vecteur et l'identité partielle donnés précédemment.

- La prérestriction de R à v (ou à a) est :

$$v \cap R = aR = \{(0,1), (0,2)\}.$$

- La postrestriction de R à v (ou à a) est :

$$v^\smile \cap R = Ra = \{(0,1), (2,1)\}.$$

- Le domaine de R est

$$RL = \{(0,0), (0,1), (0,2), (2,0), (2,1), (2,2)\}.$$

  Ce vecteur représente le sous-ensemble $\{0, 2\}$.

- La relation $R^\smile L = \{(1,0), (1,1), (1,2), (2,0), (2,1), (2,2)\}$ est le vecteur caractérisant le sous-ensemble $\{1, 2\}$, qui est l'image de R. ∎

Le théorème suivant nous montre l'importance des définitions 2.23.

(2.27) **Théorème.** *Soient P, Q et R des relations et soit X un ensemble d'indices non vide.*

(a) Q *déterministe* $\Rightarrow Q(\bigcap_{i\in X} R_i) = \bigcap_{i\in X} QR_i$

(b) Q *injective* $\Rightarrow (\bigcap_{i\in X} R_i)Q = \bigcap_{i\in X} R_iQ$,

(c) P *déterministe* $\Rightarrow (Q \cap RP^{\smile})P = QP \cap R$,

(d) P *injective* $\Rightarrow P(P^{\smile}Q \cap R) = Q \cap PR$,

(e) Q *totale* $\Leftrightarrow \overline{QR} \subseteq Q\overline{R}$,

(f) Q *déterministe* $\Rightarrow Q\overline{R} = QL \cap \overline{QR}$,

(g) Q *application* $\Rightarrow Q\overline{R} = \overline{QR}$,

(h) Q *surjective* $\Leftrightarrow \overline{RQ} \subseteq \overline{R}Q$,

(i) Q *injective* $\Rightarrow \overline{R}Q = LQ \cap \overline{RQ}$,

(j) Q *déterministe* $\Rightarrow Q\overline{R} \cup \overline{QL} = \overline{QR}$,

(k) Q *injective* $\Rightarrow \overline{R}Q \cup \overline{LQ} = \overline{RQ}$,

(l) Q, R *déterministes* $\Rightarrow QR$ *déterministe,*

(m) Q, R *injectives* $\Rightarrow QR$ *injective*,

(n) Q, R *totales* $\Rightarrow QR$ *totale*,

(o) Q, R *surjectives* $\Rightarrow QR$ *surjective*,

(p) $Q \subseteq R, R$ *déterministe et* $RL \subseteq QL \Rightarrow Q = R$,

(q) $Q \subseteq R, R$ *injective et* $LR \subseteq LQ \Rightarrow Q = R$,

(r) R *déterministe* $\Rightarrow Q \cap R$ *déterministe*,

(s) R *injective* $\Rightarrow Q \cap R$ *injective*,

(t) R *totale* $\Rightarrow Q \cup R$ *totale*,

(u) R *surjective* $\Rightarrow Q \cup R$ *surjective.* ∎

Pour plus de détails voir [24]. Dans ce qui suit, nous présentons quelques propriétés particulières des relations incluses dans l'identité, appelées généralement identités partielles (définition 2.23(f)). L'ensemble des identités partielles est un treillis booléen complet.

Soit R une identité partielle. Nous définissons

(2.28) $R^{\sim} := I \cap \overline{RL}$

le *complément* de R relatif à l'identité ($R^{\sim}$ est une identité partielle). Les identités partielles ont des propriétés simples et utiles. Quelques-unes sont présentées dans le théorème suivant.

(2.29) **Théorème.** *Soient a et b des identités partielles et Q, R des relations.*

(a) $b^\smile = b$,

(b) $b^2 = b$,

(c) $a \cap b = ab = ba$,

(d) $b \cup b^\sim = I$ *et* $b \cap b^\sim = \emptyset$,

(e) $a = I \cap aL$

(f) $Q \cap aR = aQ \cap R$,

(g) $aQ = aL \cap Q$.

Démonstration.

(a) b
$=$ { Théorème 2.21(40). }
$(I \cap bb^\smile)b$
$\subseteq$ { $b \subseteq I$ et $(;)$ monotone. }
$b^\smile$

Par le théorème 2.21(19,25), nous avons $b^\smile = b$.

(b) b
$=$ { Théorème 2.21(40). }
$(I \cap bb^\smile)b$
$\subseteq$ { $b \subseteq I$, partie (a) et $(;)$ monotone. }
b^2
$\subseteq$ { $b \subseteq I$ et $(;)$ monotone. }
b

(c) $a \cap b$
$\subseteq$ { Partie (b) et $(;)$ monotone $\rightarrow a \cap b = (a \cap b)^2 \subseteq ab$. }
ab
$\subseteq$ { $a \subseteq I$, $b \subseteq I$ et $(;)$ monotone. }
$a \cap b$

(d) Par définition du complément (2.28).

(e) $I \cap aL$
$=$ { Théorème 2.27(d). }
$a(a^\smile \cap L)$

$=$ { (a), $a \subseteq L$ et (b). }
a

(f) $Q \cap aR$
$=$ { (e). }
$Q \cap (I \cap aL)R$
$=$ { Théorème 2.21(36). }
$Q \cap R \cap aL$
$=$ { (e) et théorème 2.21(36). }
$aQ \cap R$

(g) aQ
$= aQ \cap L$
$=$ { (f). }
$aL \cap Q$

■

2.3.2 Fermeture transitive réflexive

Dans ce qui suit, nous définissons une opération très utile en informatique, qui permet d'exprimer la sémantique des programmes itératifs.

La *fermeture transitive réflexive* est une opération unaire notée $*$ et définie pour toute relation R par :

(2.30) $R^* = \mu(X \mapsto I \cup RX)$.

L'opération $*$ est donc définie comme un plus petit point fixe ; la monotonicité de $\cup$ et de (;), et le théorème de Knaster-Tarski (2.10) nous garantissent qu'elle est bien définie et qu'elle vérifie $R^* = I \cup RR^*$. On montre également $R^* = I \cup R^*R$. En résumé,

(2.31) $R^* = I \cup RR^* = I \cup R^*R$.

L'opération $*$ a le même ordre de priorité que les opérations unaires $\breve{}$ et $\bar{}$. Nous pouvons aussi définir une opération similaire à $*$, appelée *fermeture transitive*, notée $+$, et définie pour toute relation R par :

(2.32) $R^+ = \mu(X \mapsto R \cup RX)$.

Les opérations $*$ et $+$ sont très étroitement liées :

(2.33) (a) $R^+ = R^*R = RR^* = R \cup RR^*$,
(b) $R^* = I \cup R^+$.

Les opérations $*$ et $+$ ont le même ordre de priorité. L'opération $*$ satisfait aussi

(2.34) $R^* = \bigcup_{i\geq 0} R^i$,

où $R^0 = I$ et $R^{i+1} = RR^i$.

Donnons quelques propriétés de l'opération $*$. Les propriétés de l'opération $+$ sont faciles à déduire à partir des équations 2.33 et des propriétés de $*$. résutlats de Backhouse

(2.35) **Lemme.** *Soient les relations R, Q et X. Nous avons :*

(a) $(R^*)^\smile = (R^\smile)^*$,

(b) $Q \subseteq R \Rightarrow Q^* \subseteq R^*$,

(c) $R^*Q = \mu(X \mapsto Q \cup RX)$,

(d) $(Q \cup R)^* = (R^*Q)^*R^* = (Q^*R)^*Q^*$,

(e) $QR = \emptyset \Rightarrow (Q \cup R)^* = R^*Q^*$,

(f) $RQ = \emptyset$ *et* $QR = \emptyset \Rightarrow (R \cup Q)^* = R^* \cup Q^*$,

(g) $(RQ)^*R = R(QR)^*$.

Démonstration.

(a) Le résultat découle facilement de l'équation 2.34, du théorème 2.21(20) et du fait que $R^{i\smile} = R^{\smile i}$.

(b)
$$\begin{array}{ll} & Q \subseteq R \\ \Rightarrow & \quad \{ \text{ L'opération } (;) \text{ monotone. } \} \\ & QX \subseteq RX \\ \Rightarrow & \quad \{ \text{ Loi booléenne. } \} \\ & I \cup QX \subseteq I \cup RX \\ \Rightarrow & \quad \{ \text{ Proposition 2.12(a). } \} \\ & \mu(X \mapsto I \cup QX) \subseteq \mu(X \mapsto I \cup RX) \\ \Rightarrow & \quad \{ \text{ Équation 2.30. } \} \\ & Q^* \subseteq R^* \end{array}$$

(c) Nous utilisons la proposition 2.12(d). Soient les fonctions f, g et h définies comme suit :

$$f(X) := Q \cup RX, \quad g(X) := XQ, \quad h(X) := I \cup RX.$$

Nous vérifions facilement que

$$f \circ g = g \circ h.$$

$\mu(X \mapsto Q \cup RX)$
$=$ { $f(X) = Q \cup RX$. }
$\mu(f)$
$=$ { $f \circ g = g \circ h$ et proposition 2.12(d). }
$g(\mu(h))$
$=$ { $g(X) = XQ$, $h(X) = I \cup RX$ et équation 2.30. }
R^*Q

(d) $(Q \cup R)^*$
$=$ { Équation 2.30. }
$\mu(X \mapsto I \cup (Q \cup R)X)$
$=$ { Proposition 2.12(c) avec $X + Y = I \cup QX \cup RY$. }
$\mu(X \mapsto \mu(Y \mapsto I \cup QX \cup RY))$
$=$ { Lemme 2.35(c). }
$\mu(X \mapsto R^*(I \cup QX))$
$=$ { Théorème 2.21(9). }
$\mu(X \mapsto R^* \cup R^*QX)$
$=$ { Lemme 2.35(c). }
$(R^*Q)^*R^*$

Par symétrie $(Q \cup R)^* = (Q^*R)^*Q^*$.

(e) $(Q \cup R)^*$
$=$ { Lemme 2.35(d). }
$(Q^*R)^*Q^*$
$=$ { $Q^* = I \cup Q^+$ et théorème 2.21(11). }
$(R \cup Q^+R)^*Q^*$
$=$ { $QR \subseteq \emptyset \Rightarrow Q^+R = \emptyset$. }
R^*Q^*

(f) $(Q \cup R)^*$
$=$ { Lemme 2.35(e). }
Q^*R^*
$=$ { $R^* = I \cup R^+$. }
$(I \cup Q^+)(I \cup R^+)$
$=$ { (;) se distribue sur $\cup$. }
$I \cup Q^+ \cup R^+ \cup Q^+R^+$
$=$ { $R^* = I \cup R^+$, $Q^* = I \cup Q^+$ et $Q^+R = \emptyset$. }
$Q^* \cup R^*$

(g) Nous utilisons la proposition 2.12(b). Soient les fonctions f et g définies comme suit : $f(X) := RX$, $g(X) := I \cup QX$. Nous vérifions facilement que

$$(f \circ g)(X) = R \cup RQX$$

et

$$(g \circ f)(X) = I \cup QRX.$$

Alors,

$$\begin{array}{ll} & (RQ)^*R \\ = & \quad \{ \text{ Lemme 2.35(c) et expression de } f \circ g. \ \} \\ & \mu(f \circ g) \\ = & \quad \{ \text{ Proposition 2.12(b). } \} \\ & f(\mu(g \circ f)) \\ = & \quad \{ \text{ Lemme 2.35(c) et expressions de } f \text{ et } g \circ f. \ \} \\ & R(QR)^* \end{array}$$

■

2.3.3 Produit direct

(2.36) **Définition.** Une paire (π_1, π_2) de relations est appelée *produit direct* [12, 13, 14] ssi :

$$\breve{\pi_1}\pi_1 = I, \qquad \breve{\pi_2}\pi_2 = I, \qquad \breve{\pi_1}\pi_2 = L, \qquad \pi_1\breve{\pi_1} \cap \pi_2\breve{\pi_2} = I.$$

Les relations π_1 et π_2 sont appelées des *projections*. ■

(2.37) **Exemple.** Soient X et Y des ensembles pas nécessairement distincts. Alors la paire (π_1, π_2), avec

$$\pi_1 = \{((x,y),x) \mid x \in X \wedge y \in Y\}, \qquad \pi_2 = \{((x,y),y) \mid x \in X \wedge y \in Y\},$$

est un produit direct, étant donné que :

- $\breve{\pi_1}\pi_1 = \{(x,x) \mid x \in X\} = I_X$,
- $\breve{\pi_2}\pi_2 = \{(y,y) \mid y \in Y\} = I_Y$,
- $\begin{array}{ll} \pi_1\breve{\pi_1} \cap \pi_2\breve{\pi_2} & = \{((x,y),(x,z)) \mid x \in X \wedge y \in Y \wedge z \in Y\} \\ & \quad \cap \{((x,z),(y,z)) \mid x \in X \wedge y \in Y \wedge z \in Y\} \\ & = \{((x,y),(x,y)) \mid x \in X \wedge y \in Y\} \\ & = I_{XY}, \end{array}$
- $\breve{\pi_1}\pi_2 = \{(x,y) \mid x \in X \wedge y \in Y\} = L_{XY}$. ■

(2.38) **Définition.** Soit (π_1, π_2) un produit direct et R_i, $1 \leq i \leq 2$, des relations. Le *produit cartésien* des relations R_i par rapport à (π_1, π_2) est :

$$[R_1, R_2] := \pi_1 R_1 \breve{\pi_1} \cap \pi_2 R_2 \breve{\pi_2}.$$

■

Pour éclaircir cette définition, présentons un exemple simple.

(2.39) **Exemple.** Soient R_1 et R_2 des relations sur l'ensemble des relatifs $\mathbf{Z}$:

- $R_1 := \{(x, x+1) \mid x \in \mathbf{Z}\}$ et $R_2 := \{(x, x^3) \mid x \in \mathbf{Z}\}$,
- $\pi_1 := \{((x, y), x) \mid x \in \mathbf{Z} \wedge y \in \mathbf{Z}\}$,
- $\pi_2 := \{((x, y), y) \mid x \in \mathbf{Z} \wedge y \in \mathbf{Z}\}$.

Nous avons

$$\begin{aligned}
& [R_1, R_2] \\
= & \quad \{ \text{ Définition 2.36. } \} \\
& \pi_1 R_1 \breve{\pi_1} \cap \pi_2 R_2 \breve{\pi_2} \\
= & \quad \{ \text{ Expressions de } R_1, R_2, \pi_1 \text{ et } \pi_2. \} \\
& \{((x, y), (x+1, z)) \mid x \in \mathbf{Z} \wedge y \in \mathbf{Z} \wedge z \in \mathbf{Z}\} \\
& \cap \{((x, y), (z, y^3)) \mid x \in \mathbf{Z} \wedge y \in \mathbf{Z} \wedge z \in \mathbf{Z}\}, \\
= & \{((x, y), (x+1, y^3)) \mid x \in \mathbf{Z} \wedge y \in \mathbf{Z}\}
\end{aligned}$$

■

Donnons quelques propriétés du produit direct.

(2.40) **Lemme.** *Soient (π_1, π_2) un produit direct et P, Q, R et S des relations.*

(a) $[P, Q] \cap [R, S] = [P \cap R, Q \cap S]$,

(b) $[P, Q] \cup [P, R] = [P, Q \cup R]$,

(c) $P \subseteq R \wedge Q \subseteq S \Rightarrow [P, Q] \subseteq [R, S]$,

(d) $[P, Q]L = [PL, QL]$,

(e) $[P, Q]\pi_1 = \pi_1 P \cap \pi_2 QL$,

(f) $[P, Q]\pi_2 = \pi_1 PL \cap \pi_2 Q$,

(g) $\breve{\pi_1}[P, Q]\pi_1 = P$ *(si* $P \neq \emptyset$*)*,

(h) $\breve{\pi_2}[P, Q]\pi_2 = Q$ *(si* $Q \neq \emptyset$*)*,

(i) $[I, I] = I$,

(j) $[P, Q][R, S] = [PR, QS]$,

(k) $P \subseteq I \Rightarrow [P, Q]^+ = [P, Q^+]$.

Les démonstrations des propriétés (a, c, d, e, f, g, h) se trouvent dans [24] et celle de (j) dans [25]. La propriété (k) découle directement à partir de la définition de + (équations 2.33, 2.34), (j), 2.29(b) et de b. ∎

2.3.4 Somme directe

(2.41) **Définition.** Une paire (σ_1, σ_2) de relations est appelée *somme directe* [12, 13, 24] ssi :

$$\sigma_1\breve{\sigma_1} = I, \qquad \sigma_2\breve{\sigma_2} = I, \qquad \sigma_1\breve{\sigma_2} = \emptyset, \qquad \breve{\sigma_1}\sigma_1 \cup \breve{\sigma_2}\sigma_2 = I.$$

Les relations σ_1 et σ_2 sont appelées des *injections.* ∎

(2.42) **Exemple.** Soient X et Y des ensembles. La paire (σ_1, σ_2)

$$\begin{aligned} \sigma_1 &:= \{(x, (1, x)) \mid x \in X\}, \\ \sigma_2 &:= \{(y, (2, y)) \mid y \in Y\}, \end{aligned}$$

est une somme directe, étant donné que :

- $\sigma_1\breve{\sigma_1} = \{(x, x) \mid x \in X\} = I_X$,
- $\sigma_2\breve{\sigma_2} = \{(y, y) \mid y \in Y\} = I_Y$,
- $\sigma_1\breve{\sigma_2} = \{(x, y) \mid x \in X \wedge y \in Y \wedge (1, x) = (2, y)\} = \emptyset_{XY}$,
- $$\begin{aligned} \breve{\sigma_1}\sigma_1 \cup \breve{\sigma_2}\sigma_2 &= \{((1, x), (1, x)) \mid x \in X\} \cup \{((2, x), (2, x) \mid x \in X)\} \\ &= \{(x, x) \mid x \in X \wedge y \in Y \mid (\exists y : x = (1, y) \vee x = (2, y))\} \\ &= I_{X \uplus Y}. \end{aligned}$$

  La relation $I_{X \uplus Y}$ est l'identité sur l'union disjointe des ensembles X et Y.

∎

La définition qui suit introduit la notion d'union disjointe de deux relations.

(2.43) **Définition.** Soit (σ_1, σ_2) une somme directe. La relation

$$\breve{\sigma_1}R_1\sigma_1 \cup \breve{\sigma_2}R_2\sigma_2$$

est appelée l'*union disjointe* des relations R_1 et R_2 par rapport à (σ_1, σ_2). ∎

2.3.5 Implication relative

Vu l'usage important des expressions de la forme $\overline{Q\overline{R}}$ dans le reste de notre travail, nous définissons l'opérateur suivant :

(2.44) **Définition.** L'opérateur binaire $\triangleright$, appelé *implication relative*, est défini comme suit :

$$Q \triangleright R := \overline{Q\overline{R}}.$$

Cet opérateur admet un opérateur dual (2.13), $\triangleleft$, donné par :

$$Q \triangleleft R := \overline{\overline{Q}R}.$$

∎

Indice mnémonique : le choix du terme « implication relative » est dû au fait que, dans une algèbre concrète, nous avons $xQ \triangleright Ry \Leftrightarrow \forall z : xRz \rightarrow zQy$. Le cas le plus intéressant est celui où l'argument droit est un vecteur RL, c'est-à-dire $Q \triangleright RL$. Si $x.R$ dénote l'ensemble des images de x par R, alors $x \in \mathrm{dom}(Q \triangleright RL) \Leftrightarrow x.Q \subseteq \mathrm{dom}(R)$.

Les propriétés de $\triangleleft$ s'obtiennent par dualisation des propriétés de $\triangleright$. Les opérateurs $\triangleright$ et $\triangleleft$ sont moins prioritaires que $(;)$ mais plus prioritaires que $\cap$ et $\cup$. Dans le lemme suivant nous donnons quelques propriétés vérifiées par les opérateurs $\triangleright$ et $\triangleleft$.

(2.45) **Lemme.** *Soient Q, R des relations et v un vecteur.*

(a) $Q \triangleright RL = (Q \triangleright RL)L$,

(b) $Q \triangleleft RL = (Q \triangleleft RL)L$,

(c) $\overline{Q \triangleright R} = Q\overline{R}$,

(d) $\overline{Q \triangleleft R} = \overline{Q}R$,

(e) $P \triangleright Q \cap P \triangleright R = P \triangleright (Q \cap R)$,

(f) $P \triangleleft R \cap Q \triangleleft R = (P \cap Q) \triangleleft R$,

(g) $P \triangleright R \cap Q \triangleright R = (P \cup Q) \triangleright R$,

(h) $P \triangleleft Q \cap P \triangleleft R = P \triangleleft (Q \cup R)$,

(i) $PQ \triangleright R = P \triangleright (Q \triangleright R)$,

(j) $(v \cap Q) \triangleright R = \overline{v} \cup Q \triangleright R$,

(k) $PQ \cap P \triangleright R = P(Q \cup \overline{R}) \cap P \triangleright R$,

(l) $P \triangleright Q \subseteq PQ \cup \overline{PL}$,

(m) $P \subseteq Q \Rightarrow Q \triangleright R \subseteq P \triangleright R$,

(n) $P \subseteq Q \Rightarrow R \rhd P \subseteq R \rhd Q$,

(o) $(P \rhd Q) \lhd R = P \rhd (Q \lhd R)$.

Nous remarquons que les propriétés (e), (f), (h), (g) et (i) sont similaires aux propriétés des opérateurs logiques $\rightarrow$, $\wedge$ et $\vee$. Par exemple, la propriété (i) correspond à $(P \wedge Q \rightarrow R) \leftrightarrow (P \rightarrow (Q \rightarrow R))$.

Démonstration. (a) et (b) se déduisent facilement du théorème 2.21(39). Les propriétés (c) et (d) découlent directement d'une loi booléenne sur la complémentation. Les propriétés (e), (f), (h) et (g) se déduisent à partir des lois 2.21(2,4,9, 11). Voici les démonstrations des autres propriétés.

(i)
$$\begin{array}{ll} & PQ \rhd R \\ = & \quad \{ \text{ Définition 2.44. } \} \\ & \overline{PQ\overline{R}} \\ = & \quad \{ \text{ Lemme 2.45(c). } \} \\ & \overline{P\overline{Q \rhd R}} \\ = & \quad \{ \text{ Définition 2.44. } \} \\ & P \rhd (Q \rhd R) \end{array}$$

(j)
$$\begin{array}{ll} & (v \cap Q) \rhd R \\ = & \quad \{ \text{ Définition 2.44. } \} \\ & \overline{(v \cap Q)\overline{R}} \\ = & \quad \{ \text{ Théorème 2.21(36, 4) et définition 2.44. } \} \\ & \overline{v} \cup Q \rhd R \end{array}$$

(k)
$$\begin{array}{ll} & PQ \cap P \rhd R \\ = & \quad \{ \text{ Définition 2.44 et } P\overline{R} \cap P \rhd R = \emptyset. \} \\ & (PQ \cup P\overline{R}) \cap P \rhd R \\ = & \quad \{ \text{ Théorème 2.21(9). } \} \\ & P(Q \cup \overline{R}) \cap P \rhd R \end{array}$$

(l)
$$\begin{array}{ll} & PL = P(Q \cup \overline{Q}) \\ \Rightarrow & \quad \{ \text{ Théorème 2.21(9). } \} \\ & PL \subseteq PQ \cup P\overline{Q} \\ \Leftrightarrow & \quad \{ \text{ Théorème 2.21(6) (appliqué deux fois). } \} \\ & P \rhd Q \subseteq PQ \cup \overline{PL} \end{array}$$

(m)
$$\begin{array}{ll} & P \subseteq Q \\ \Rightarrow & \quad \{ \text{ Théorème 2.21(16). } \} \\ & P\overline{R} \subseteq Q\overline{R} \\ \Leftrightarrow & \quad \{ \text{ Théorème 2.21(7). } \} \\ & \overline{Q\overline{R}} \subseteq \overline{P\overline{R}} \\ \Leftrightarrow & \quad \{ \text{ Définition 2.44. } \} \\ & Q \rhd R \subseteq P \rhd R \end{array}$$

(n) Se démontre d'une manière similaire,

(o)
$$\begin{array}{ll} & (P \triangleright Q) \triangleleft R \\ = & \quad \{ \text{ Définition de } \triangleleft \text{ (2.44). } \} \\ & \overline{\overline{P \triangleright Q} R} \\ = & \quad \{ \text{ Lemme 2.45(c). } \} \\ & \overline{P \overline{Q} R} \\ = & \quad \{ \text{ Lemme 2.45(d). } \} \\ & \overline{P \overline{Q \triangleleft R}} \\ = & \quad \{ \text{ Définition de } \triangleright \text{ (2.44). } \} \\ & P \triangleright (Q \triangleleft R). \end{array}$$

■

(2.46) **Remarque.**

- La fonction $X \mapsto X \triangleright R$ est antimonotone en X ; quant à la fonction $X \mapsto R \triangleright X$, elle est monotone en X.
- Les fonctions $f(X) := R^{\smile} X$ et $g(X) := R \triangleright X$ forment une connection de Galois (2.9), comme suit :

  (2.47) $R^{\smile} X \subseteq Y \quad \Leftrightarrow \quad X \subseteq R \triangleright Y.$

  Démonstration.

$$\begin{array}{ll} & X \subseteq R \triangleright Y \\ \Leftrightarrow & \quad \{ \text{ Définition 2.44 et théorème 2.21(7). } \} \\ & R \overline{Y} \subseteq \overline{X} \\ \Leftrightarrow & \quad \{ \text{ Règle de Schröder 2.18(e). } \} \\ & R^{\smile} X \subseteq Y. \end{array}$$

■

2.3.6 Progression finie et partie initiale

Nous présentons maintenant des notions qui permettent de décrire l'ensemble des points qui ne sont pas à l'origine de chemins infinis par une relation R. Ces notions sont la *progression finie* et la *partie initiale* d'une relation.

Dans une algèbre concrète, une relation R est progressivement finie ssi il n'existe aucune chaîne infinie $x_0, x_1, x_2, \ldots$ telle que $(x_i, x_{i+1}) \in R$ pour tout $i \geq 0$; autrement dit, l'ensemble des points qui sont à l'origine de chemins infinis est vide. Le plus petit ensemble de points qui ne sont pas à l'origine de chemins infinis par une relation R est appelé *partie initiale* de R ; celle-ci est formellement définie de la manière suivante :

(2.48) **Définition.** [78] La *partie initiale* d'une relation R, notée $\mathcal{B}(R)$, est donnée par :

$$\mathcal{B}(R) := \bigcap\{x \mid R \triangleright x = x\},$$

où x varie sur l'ensemble des vecteurs (par le théorème 2.21(32,39), $\mathcal{B}(R)$ est donc un vecteur). ∎

(Indice mnémonique : $\mathcal{B}$ pour *boucle* car, dans le contexte de la sémantique des programmes, $\mathcal{B}(R)$ représente l'ensemble des états à partir desquels aucune boucle infinie n'est possible.)

Intuitivement, si x_0 est l'origine d'un certain chemin de longueur infinie par R, alors il en est de même pour tous les prédécesseurs de x_0 ; donc l'ensemble x de ce type de point satisfait $Rx \subseteq x$, et il satisfait aussi $x \subseteq Rx$, car si x_0 est l'origine d'un certain chemin de longueur infinie, alors il en est de même pour tous les successeurs de x_0. Mais, comme nous nous intéressons à l'ensemble de tous les points qui sont à l'origine de chemins infinis, nous prenons $\bigcup\{x \mid x = Rx\}$, qui est égal à $\bigcup\{x \mid x \subseteq Rx\}$ par (2.11(a)). L'ensemble des points qui sont à l'origine de chemins de longueur finie seulement est obtenu en prenant le complément de $\bigcup\{x \mid x = Rx\}$, qui est (lois de De Morgan et lois booléennes) $\bigcap\{x \mid R\overline{x} = \overline{x}\} = \bigcap\{x \mid R \triangleright x = x\}$.

(2.49) **Remarque.** Le vecteur $\mathcal{B}(R)$ est le plus petit point fixe de la fonction $f(x) := R \triangleright x$. Étant donné que cette fonction est monotone et que nos algèbres de relations sont complètes (définition 2.18), le vecteur $\mathcal{B}(R)$ existe, par le théorème 2.10. ∎

Une définition équivalente de $\mathcal{B}(R)$ peut être donnée en quantifiant sur des relations qui ne sont pas nécessairement des vecteurs. Cette définition est :

(2.50) $\mathcal{B}(R) = \bigcap\{X \mid R \triangleright X = X\}$.

Démonstration. Posons $f(X) := R \triangleright X$ et $Q := \mu(f)$. Nous devons montrer $Q = \mathcal{B}(R)$. Puisque $f(\mathcal{B}(R)) = \mathcal{B}(R)$, nous avons $\mu(f) \subseteq \mathcal{B}(R)$ (par 2.11(d)), c'est-à-dire $Q \subseteq \mathcal{B}(R)$. Montrons l'inclusion inverse.

$$\begin{array}{ll} & R \triangleright (Q \triangleleft L) \\ = & \qquad \{ \text{ Lemme 2.45(o). } \} \\ & (R \triangleright Q) \triangleleft L \\ = & \qquad \{ \ Q = f(Q), \text{ c'est-à-dire } Q = R \triangleright Q. \ \} \\ & Q \triangleleft L \end{array}$$

Nous avons donc $f(Q \triangleright L) = Q \triangleright L$, d'où $Q = \mu(f) \subseteq Q \triangleright L$ (par 2.11(d)). D'autre part,

$$\begin{array}{ll} & \overline{Q} \subseteq \overline{Q}L \\ \Leftrightarrow & \overline{\overline{Q}L} \subseteq Q \\ \Leftrightarrow & \qquad \{ \text{ Définition 2.44. } \} \\ & Q \triangleright L \subseteq Q \end{array}$$

Ainsi donc, $Q = Q \triangleright L$, ce qui implique que Q est un vecteur, d'où $Q \in \{x \mid R \triangleright x = x\}$ et, finalement, $\mathcal{B}(R) = \bigcap\{x \mid R \triangleright x = x\} \subseteq Q$. D'où le résultat, c.-à-d. $\mathcal{B}(R)$ est l'intersection de toutes les relations verifiant $R \triangleright X = X$. ∎

(2.51) **Proposition.** *Soit R une relation.*

$$\begin{aligned}(a)\quad \mathcal{B}(R) &= \bigcap\{X \mid R \triangleright X = X\}\\ &= \bigcap\{X \mid R \triangleright X \subseteq X\}\\ &= \bigcap\{X \mid R\overline{X} = \overline{X}\}\\ &= \mu(X \mapsto R \triangleright X)\end{aligned}$$

et

$$\begin{aligned}(b)\quad \overline{\mathcal{B}(R)} &= \bigcup\{X \mid X = RX\}\\ &= \bigcup\{X \mid X \subseteq RX\}\\ &= \nu(X \mapsto RX).\end{aligned}$$

Ces résultats se déduisent facilement des équations 2.11, 2.50, de la définition de $\triangleright$ et de quelques lois booléennes. ∎

Donnons la définition formelle de ce qu'est une relation progressivement finie.

(2.52) **Définition.** Une relation R est dite *progressivement finie* [78] ssi $\mathcal{B}(R) = L$. ∎

En utilisant les résultats de la proposition 2.51, nous avons :

(2.53) R est progressivement finie $\Leftrightarrow$ $\overline{\mathcal{B}(R)} = \emptyset$ $\Leftrightarrow$ $(\forall X : X \subseteq RX \;\Rightarrow\; X = \emptyset)$.

La proposition suivante énonce quelques propriétés des relations progressivement finies et de la partie initiale d'une relation. Les propriétés (a), (b) et (c) se trouvent aussi dans [78]. Les démonstrations de (a) et (c) ci-dessous sont différentes de celles données dans [78].

(2.54) **Proposition.** *Soient Q et R des relations.*

(a) $\mathcal{B}(R) \subseteq R^*\overline{RL}$,

(b) $\bigcup_{i\geq 0} \overline{R^i L} \subseteq \mathcal{B}(R)$,

(c) R *déterministe* $\Rightarrow \mathcal{B}(R) = R^*\overline{RL}$,

(d) $Q \subseteq R \Rightarrow \mathcal{B}(R) \subseteq \mathcal{B}(Q)$,

(e) $R \triangleright \mathcal{B}(R) = \mathcal{B}(R)$ *(équivalent à* $R\overline{\mathcal{B}(R)} = \overline{\mathcal{B}(R)}$*)*,

(f) $\mathcal{B}(R) = \mathcal{B}(R^+)$,

(g) $R^* \triangleright \mathcal{B}(R) = R^+ \triangleright \mathcal{B}(R) = \mathcal{B}(R)$ *(équivalent à* $R^*\overline{\mathcal{B}(R)} = R^+\overline{\mathcal{B}(R)} = \overline{\mathcal{B}(R)}$*)*,

(h) Q *progressivement finie* $\Rightarrow Q \cap R$ *progressivement finie,*

(i) $R \cap \mathcal{B}(R)$ *est progressivement finie.*

Démonstration.

(a)
$$\begin{array}{ll} & \mathcal{B}(R) \\ = & \quad \{ \text{ Proposition 2.51(a). } \} \\ & \mu(X \mapsto R \triangleright X) \\ \subseteq & \quad \{ \text{ Lemme 2.45(l) et proposition 2.12(a). } \} \\ & \mu(X \mapsto RX \cup \overline{RL}) \\ = & \quad \{ \text{ Lemme 2.35(c). } \} \\ & R^*\overline{RL} \end{array}$$

(b) C'est la proposition 6.3.3(i) dans [78].

(c)
$$\begin{array}{ll} & \mathcal{B}(R) \\ = & \quad \{ \text{ Proposition 2.51(a). } \} \\ & \mu(X \mapsto R \triangleright X) \\ = & \quad \{ R \text{ déterministe, théorème 2.27(j) et définition 2.44. } \} \\ & \mu(X \mapsto RX \cup \overline{RL}) \\ = & \quad \{ \text{ Lemme 2.35(c). } \} \\ & R^*\overline{RL} \end{array}$$

(d) Soit X une relation quelconque.

$$\begin{array}{ll} & Q \subseteq R \\ \Rightarrow & \quad \{ \text{ Lemme 2.45(m). } \} \\ & R \triangleright X \subseteq Q \triangleright X \\ \Rightarrow & \quad \{ \text{ Proposition 2.12(a). } \} \\ & \mu(X \mapsto R \triangleright X) \subseteq \mu(X \mapsto Q \triangleright X) \\ \Leftrightarrow & \quad \{ \text{ Proposition 2.51(a). } \} \\ & \mathcal{B}(R) \subseteq \mathcal{B}(Q) \end{array}$$

(e) Par la proposition 2.50(a), $\mathcal{B}(R)$ est la plus petite relation X vérifiant $R \triangleright X = X$ et, par complémentation, nous trouvons l'autre expression.

(f)
$$\begin{array}{ll} & R \subseteq R^+ \\ \Rightarrow & \quad \{ \text{ Proposition 2.54(d). } \} \\ & \mathcal{B}(R^+) \subseteq \mathcal{B}(R) \end{array}$$

D'autre part, soit une relation Y telle que $R^+ \triangleright Y = Y$ (une telle relation existe ; par exemple, on peut prendre $Y = \mathcal{B}(R^+)$).

$$
\begin{array}{ll}
& Y \\
= & \qquad \{\ R^+ \triangleright Y = Y \text{ et équation 2.33(a).}\ \} \\
& RR^* \triangleright Y \\
= & \qquad \{\ \text{Équation 2.33(b) et théorème 2.21(9).}\ \} \\
& (R \cup RR^+) \triangleright Y \\
= & \qquad \{\ \text{Lemme 2.45(g).}\ \} \\
& R \triangleright Y \cap RR^+ \triangleright Y \\
= & \qquad \{\ \text{Lemme 2.45(i).}\ \} \\
& R \triangleright Y \cap R \triangleright (R^+ \triangleright Y) \\
= & \qquad \{\ R^+ \triangleright Y = Y.\ \} \\
& R \triangleright Y
\end{array}
$$

Donc toute relation Y telle que $Y = R^+ \triangleright Y$ vérifie $Y = R \triangleright Y$. Par conséquent, $\bigcap\{X \mid R \triangleright X = X\} \subseteq \bigcap\{X \mid R^+ \triangleright X = X\}$, c'est-à-dire $\mathcal{B}(R) \subseteq \mathcal{B}(R^+)$. D'où le résultat.

(g)
$$
\begin{array}{ll}
& R^* \triangleright \mathcal{B}(R) \\
= & \qquad \{\ \text{Équation 2.33(b)}\ \} \\
& (I \cup R^+) \triangleright \mathcal{B}(R) \\
= & \qquad \{\ \text{Lemme 2.45(g) et } I \triangleright \mathcal{B}(R) = \mathcal{B}(R).\ \} \\
& \mathcal{B}(R) \cap R^+ \triangleright \mathcal{B}(R) \\
= & \qquad \{\ \text{Proposition 2.54(f).}\ \} \\
& \mathcal{B}(R) \cap R^+ \triangleright \mathcal{B}(R^+) \\
= & \qquad \{\ \text{Proposition 2.54(e).}\ \} \\
& \mathcal{B}(R) \cap \mathcal{B}(R^+) \\
= & \qquad \{\ \text{Proposition 2.54(f).}\ \} \\
& \mathcal{B}(R) \\
= & \qquad \{\ \text{Proposition 2.54(f).}\ \} \\
& \mathcal{B}(R^+) \\
= & \qquad \{\ \text{Proposition 2.54(e).}\ \} \\
& R^+ \triangleright \mathcal{B}(R^+) \\
= & \qquad \{\ \text{Proposition 2.54(f).}\ \} \\
& R^+ \triangleright \mathcal{B}(R)
\end{array}
$$

Les autres expressions sont facilement obtenues par complémentation.

(h)
$$
\begin{array}{ll}
& Q \cap R \subseteq Q \\
\Rightarrow & \qquad \{\ \text{Proposition 2.54(d).}\ \} \\
& \mathcal{B}(Q) \subseteq \mathcal{B}(Q \cap R) \\
\Rightarrow & \qquad \{\ \mathcal{B}(Q) = L.\ \}
\end{array}
$$

$\mathcal{B}(Q \cap R) = L$

(i) Nous utilisons l'équation 2.53. Soit X une relation quelconque.

$$
\begin{aligned}
& X \subseteq (R \cap \mathcal{B}(R))X \\
\Leftrightarrow & \qquad \{ \text{ Théorème 2.21(36), } \mathcal{B}(R) \text{ un vecteur par la définition 2.48. } \} \\
& X \subseteq RX \cap \mathcal{B}(R) \\
\Leftrightarrow & X \subseteq RX \text{ et } X \subseteq \mathcal{B}(R) \\
\Rightarrow & \qquad \{ \text{ Équations 2.51(b) et 2.11(b,e). } \} \\
& X \subseteq \overline{\mathcal{B}(R)} \text{ et } X \subseteq \mathcal{B}(R) \\
\Leftrightarrow & X = \emptyset
\end{aligned}
$$

■

Le lemme suivant nous présente certaines propriétés vérifiées par les parties initiales de quelques relations.

(2.55) **Lemme.** *Soient Q et R des relations, (π_1, π_2) un produit direct, π une projection et σ une injection.*

(a) $\mathcal{B}(QR) = Q \triangleright \mathcal{B}(RQ)$,

(b) $\mathcal{B}(\pi R \pi^\smile) = \pi \mathcal{B}(R)$,

(c) $\mathcal{B}(\sigma^\smile R \sigma) = \sigma^\smile \mathcal{B}(R) \cup \overline{\sigma^\smile L}$,

(d) $\mathcal{B}([Q, R]) = [\mathcal{B}(Q), L] \cup [L, \mathcal{B}(R)]$.

Démonstration.

(a) Nous utilisons le lemme 2.12(d). Soient f, g et h des fonctions données comme suit,

$$f(X) := QR \triangleright X, \quad g(X) := Q \triangleright X \quad \text{et} \quad h(X) := RQ \triangleright X.$$

En utilisant la propriété 2.45(i), nous vérifions facilement que

$$(f \circ g)(X) = (g \circ h)(X) = QRQ \triangleright X,$$

d'où

$$
\begin{aligned}
& \mathcal{B}(QR) \\
= & \qquad \{ \text{ Équation 2.51(a) et expression de } f. \} \\
& \mu(f) \\
= & \qquad \{ \text{ Lemme 2.12(d). } \} \\
& g(\mu h) \\
= & \qquad \{ \text{ Équation 2.51(a) et expressions de } g \text{ et } h. \} \\
& Q \triangleright \mathcal{B}(RQ)
\end{aligned}
$$

(b) $\mathcal{B}(\pi R\pi^\smile)$

$=$ { Lemme 2.55(a) avec $Q := \pi$ et $R := R\pi^\smile$. }

$\pi \triangleright \mathcal{B}(R\pi^\smile\pi)$

$=$ { $\pi^\smile\pi = I$, $I \subseteq \pi\pi^\smile$ (définition 2.36), théorème 2.27(g) et définition 2.44. }

$\pi\mathcal{B}(R)$

(c) $\mathcal{B}(\sigma^\smile R\sigma)$

$=$ { Lemme 2.55(a) avec $Q := \sigma^\smile$ et $R := R\sigma$. }

$\sigma^\smile \triangleright \mathcal{B}(R\sigma\sigma^\smile)$

$=$ { $\sigma\sigma^\smile = I$ (définition 2.41). }

$\sigma^\smile \triangleright \mathcal{B}(R)$

$=$ { $\sigma^\smile$ déterministe (définition 2.41), théorème 2.27(j) et définition 2.44. }

$\sigma^\smile\mathcal{B}(R) \cup \overline{\sigma^\smile L}$

■

2.3.7 Lien entre points fixes et progression finie

Dans ce qui suit, nous présentons des résultats sur le plus grand et le plus petit points fixes de la fonction $X \mapsto Q \cup PX$ et les conditions sous lesquelles ces deux points fixes coïncident. Nous attirons particulièrement l'attention sur le théorème 2.57 (à notre avis, ce résultat est très pratique). Les rapports de recherche de Backhouse *et al.* [9, 10] nous ont été très utiles pour cette section.

Le théorème suivant nous donne le lien entre l'unicité d'un point fixe de la fonction $f(X) := Q \cup PX$ et le fait que la relation P soit progressivement finie. Cette fonction servira à donner la sémantique des boucles, d'où son importance et celle de la fonction duale $f^\#(X) := Q \cap P \triangleright X$.

(2.56) **Théorème.** *Soit la fonction $f(X) := Q \cup PX$. Les trois propositions sont équivalentes [9] :*

(a) P est progressivement finie,

(b) La fonction f admet un seul point fixe,

(c) $\nu(f) = \mu(f) = P^*Q$.

Démonstration. Comme la fonction f est monotone et que l'algèbre est complète, par le théorème de Knaster-Tarski (2.10), f admet un plus petit et un plus grand points fixes. Nous en déduisons que si f admet un seul point fixe, le plus petit et le plus grand points fixes coïncident. Ainsi, les propositions (b) et (c) sont équivalentes. Il suffit de prouver l'équivalence (a) $\Leftrightarrow$ (c).

Montrons l'implication $(a) \Rightarrow (c)$. Par le lemme 2.35(c), le plus petit point fixe de f est P^*Q. Par conséquent, il suffit de montrer que si P est progressivement finie, le plus grand point fixe de f est aussi égal à P^*Q, d'où l'unicité. Soit X un point fixe de f ; montrons que $X \subseteq P^*Q$, ce qui est équivalent à $X \cap \overline{P^*Q} = \emptyset$:

$$
\begin{array}{ll}
 & X \cap \overline{P^*Q} \\
= & \qquad \{\ X = Q \cup PX.\ \} \\
 & (Q \cup PX) \cap \overline{P^*Q} \\
= & \qquad \{\ Q \subseteq P^*Q.\ \} \\
 & PX \cap \overline{P^*Q} \\
\subseteq & \qquad \{\ \text{Théorème 2.21(29) (règle de Dedekind).}\ \} \\
 & P(X \cap P^{\smile}\overline{P^*Q}) \\
\subseteq & \qquad \{\ PP^*Q \subseteq P^*Q \Leftrightarrow P^{\smile}\overline{P^*Q} \subseteq \overline{P^*Q}\ \text{(règle de Schröder).}\ \} \\
 & P(X \cap \overline{P^*Q})
\end{array}
$$

Nous venons de prouver que $X \cap \overline{P^*Q} \subseteq P(X \cap \overline{P^*Q})$ et, comme la relation P est progressivement finie, par l'équation 2.53 nous avons $X \cap \overline{P^*Q} = \emptyset$, d'où le résultat. Pour l'implication (c) $\Rightarrow$ (a), il suffit de prouver, par 2.51(b), que $\nu(X \mapsto PX) = \emptyset$. Or, par hypothèse, nous avons $\nu(X \mapsto Q \cup PX) = P^*Q$. Il suffit de prendre $Q = \emptyset$. ∎

Dans le prochain théorème, remarquons que dans le cas où la relation P est progressivement finie ($\mathcal{B}(P) = L$), nous retrouvons les résultats du théorème 2.56.

(2.57) **Théorème.** *Tout point fixe Y de $f(X) := Q \cup PX$ vérifie*

$$P^*Q \subseteq Y \subseteq P^*Q \cup \overline{\mathcal{B}(P)}$$

et P^*Q et $P^*Q \cup \overline{\mathcal{B}(P)}$ sont respectivement le plus petit et le plus grand point fixe de f.

Démonstration. Par le lemme 2.35(c), P^*Q est le plus petit point fixe de f ; donc, $P^*Q \subseteq Y$. Nous prouvons la deuxième inclusion. Montrons d'abord que $P^*Q \cup \overline{\mathcal{B}(P)}$ est un point fixe de f.

$$
\begin{array}{ll}
 & f(P^*Q \cup \overline{\mathcal{B}(P)}) \\
= & \qquad \{\ f(X) = Q \cup PX.\ \} \\
 & Q \cup P(P^*Q \cup \overline{\mathcal{B}(P)}) \\
= & \qquad \{\ \text{Théorème 2.21(9).}\ \} \\
 & Q \cup PP^*Q \cup P\overline{\mathcal{B}(P)} \\
= & \qquad \{\ \text{Théorème 2.21(9), } I \cup PP^* = P^*\text{, proposition 2.54(e).}\ \} \\
 & P^*Q \cup \overline{\mathcal{B}(P)}
\end{array}
$$

Montrons maintenant que tout point fixe Y de f vérifie $Y \subseteq P^*Q \cup \overline{\mathcal{B}(P)}$

$$
\begin{array}{ll}
& Y \\
\subseteq & \qquad \{\ Y = f(Y) = Q \cup PY.\ \} \\
& Q \cup PY \cup \overline{\mathcal{B}(P)} \\
= & \qquad \{\ \text{Théorème 2.21(5).}\ \} \\
& Q \cup PY \cap \mathcal{B}(P) \cup \overline{\mathcal{B}(P)} \\
= & \qquad \{\ \mathcal{B}(P) \text{ est un vecteur, théorème 2.21(36).}\ \} \\
& Q \cup \overline{\mathcal{B}(P)} \cup (P \cap \mathcal{B}(P))Y
\end{array}
$$

En utilisant ce résultat, nous avons

$$
\begin{array}{ll}
& Y \\
\subseteq & \qquad \{\ \text{Loi 2.11(e).}\ \} \\
& \nu(X \mapsto Q \cup \overline{\mathcal{B}(P)} \cup (P \cap \mathcal{B}(P))X) \\
= & \qquad \{\ \text{Théorème 2.54(i) et théorème 2.56.}\ \} \\
& (P \cap \mathcal{B}(P))^*(Q \cup \overline{\mathcal{B}(P)}) \\
\subseteq & \qquad \{\ \text{Monotonicité de } {}^*.\ \} \\
& P^*(Q \cup \overline{\mathcal{B}(P)}) \\
= & \qquad \{\ \text{Théorème 2.21(9).}\ \} \\
& P^*Q \cup P^*\overline{\mathcal{B}(P)} \\
= & \qquad \{\ \text{Proposition 2.54(g).}\ \} \\
& P^*Q \cup \overline{\mathcal{B}(P)}
\end{array}
$$

■

Le prochain corollaire concerne les points fixes de la fonction $g(X) := Q \cap P \triangleright X$.

(2.58) **Corollaire.** *Tout point fixe Y de $g(X) := Q \cap P \triangleright X$ vérifie*

$$P^* \triangleright Q \cap \mathcal{B}(P) \subseteq Y \subseteq P^* \triangleright Q$$

$P^* \triangleright Q \cap \mathcal{B}(P)$ et $P^* \triangleright Q$ sont respectivement le plus petit et le plus grand point fixe de g.

Démonstration. Il est facile de vérifier que g est la fonction duale (définition 2.13) de $f(X) := \overline{Q} \cup PX$. Par le lemme 2.14, $\overline{Y}$ est un point fixe de f. Par le théorème 2.57, $\overline{Y}$ vérifie

$$P^*\overline{Q} \subseteq \overline{Y} \subseteq P^*\overline{Q} \cup \overline{\mathcal{B}(P)}.$$

En appliquant les lois de De Morgan, ceci est équivalent à

$$\overline{P^*\overline{Q}} \cap \mathcal{B}(P) \subseteq Y \subseteq \overline{P^*\overline{Q}}.$$

Finalement, en utilisant la définition 2.44,

$$P^* \triangleright Q \cap \mathcal{B}(P) \subseteq Y \subseteq P^* \triangleright Q.$$

■

Remarquons que si la relation P est progressivement finie, la fonction g admet un seul point fixe égal à $P^* \triangleright Q$.

Nous achevons cette section par un lemme qui nous donne la partie initiale de l'union de deux relations.

(2.59) **Lemme.** *Soient Q et R deux relations.*

$$\mathcal{B}(Q \cup R) = (R^*Q)^* \triangleright \mathcal{B}(R) \cap \mathcal{B}(R^*Q).$$

Démonstration.

$$\begin{array}{ll} & \mathcal{B}(Q \cup R) \\ = & \qquad \{ \text{ Équation 2.51(a). } \} \\ & \mu(X \mapsto (Q \cup R) \triangleright X) \\ = & \qquad \{ \text{ Lemme 2.45(g). } \} \\ & \mu(X \mapsto Q \triangleright X \cap R \triangleright X) \\ = & \qquad \{ \text{ Proposition 2.12(c) avec } X + Y = Q \triangleright X \cap R \triangleright Y. \} \\ & \mu(X \mapsto \mu(Y \mapsto Q \triangleright X \cap R \triangleright Y)) \\ = & \qquad \{ \text{ Corollaire 2.58. } \} \\ & \mu(X \mapsto R^* \triangleright (Q \triangleright X) \cap \mathcal{B}(R)) \\ = & \qquad \{ \text{ Lemme 2.45(i). } \} \\ & \mu(X \mapsto R^*Q \triangleright X \cap \mathcal{B}(R)) \\ = & \qquad \{ \text{ Corollaire 2.58. } \} \\ & (R^*Q)^* \triangleright \mathcal{B}(R) \cap \mathcal{B}(R^*Q). \end{array}$$

■

2.4 Conclusion

Nous avons présenté dans ce chapitre notre outil mathématique qui est l'algèbre des relations. Nous avons établi un lien entre les points fixes de la fonction $f(X) := Q \cup PX$, la progression finie et la partie initiale. Ce lien nous a conduit à des résultats intéressants sur les points fixes de certaines fonctions (théorème 2.57 et corrolaire 2.58). Nous avons défini et donné des propriétés d'un opérateur binaire $\triangleright$ (2.44). Dans les chapitres suivants, l'opérateur d'implication relative $\triangleright$ permet de simplifier les preuves et de les améliorer en réduisant l'usage de l'opérateur de complémentation. Pour éviter l'utilisation exagérée de ce dernier, Backhouse et *al.* recommandent l'usage des résidus. L'implication relative et l'opération de résiduation à gauche sont très semblables ; en effet, $Q \triangleright R = Q^\smile \backslash R$. Pour notre application, l'emploi de l'implication relative plutôt que du résidu donne la possibilité de diminuer le nombre d'inverses ($^\smile$).

Chapitre 3

Raffinement et sémantique démoniaques

Le but de ce chapitre est de définir la sémantique dénotationnelle démoniaque [6, 7, 14, 27, 69, 70, 83] des programmes séquentiels. Nous considérons des programmes impératifs. Notre langage de programmation est le langage des commandes gardées de Dijkstra [30], qui permet l'expression du non-déterminisme. La sémantique d'un programme p est définie comme étant la relation d'entrée/sortie calculée par le programme. Cette relation est aussi appelée l'*abstraction relationnelle* du programme p. Un élément s de l'espace (ensemble) sur lequel est calculée cette relation est appelé *état*. Si l'exécution du programme p débute en s, on dit que s est un *état initial*, ou encore une *entrée*. Si p termine en s', on dit que s' est un *état final* ou encore une *sortie* du programme p. Lors d'une exécution d'un programme, trois possibilités peuvent survenir :

- terminaison normale ;
- terminaison anormale ;
- boucle infinie.

Lors de l'exécution d'un programme non déterministe en un état initial, les trois possibilités précédentes peuvent survenir pour ce même état. Nous nous intéressons à la sémantique du programme p en supposant sa pire exécution, c'est-à-dire en supposant que s'il y a possibilité que le programme ne termine pas normalement, alors il ne termine pas normalement. Cette sémantique est appelée *sémantique démoniaque*. La notion de sémantique démoniaque des programmes séquentiels n'est pas nouvelle : elle est connue au moins depuis les travaux de Dijkstra [30] sur son langage de commandes gardées. Récemment, un grand intérêt a été manifesté pour une sémantique démoniaque relationnelle des programmes séquentiels [33, 57, 69, 70]. La sémantique démoniaque est exprimée en fonction d'opérateurs, dits *démoniaques*, induits par un ordre de raffinement [11, 12, 13, 14, 16, 26, 28, 62]. Dans la section suivante, nous présentons cet ordre de raffinement. Dans la section 3.2, nous donnons la sémantique démoniaque des constructeurs suivants : affectation, séquence, choix gardé et boucle. Les notions de terminaison normale, terminaison anormale ainsi que celle de sémantique démoniaque seront présentées plus en détail dans le chapitre 5.

3.1 Un ordre de raffinement démoniaque

Dans [16], Boudriga *et al.* ont étudié un ordre de raffinement introduit initialement dans [62]. L'ensemble des relations (considérées comme spécifications) muni de cet ordre est un demi-treillis. Des notions similaires ont été définies dans un contexte de transformateurs de prédicats par Back [5, 7], Morgan et Robinson [66], et Morris [68]. Dans ce qui suit, nous donnons la définition de notre ordre de raffinement.

Si une relation R est vue comme étant la spécification du comportement observable (entrées/sorties) d'un programme p, alors on dit que p *raffine* R (ou que p est correct par rapport à R) si :

- pour toute entrée s dans le domaine de R, s' est une sortie possible de p seulement si $(s, s') \in R$, et
- p produit une sortie pour chaque entrée du domaine de la relation R [61].

Ceci peut être défini comme suit :

(3.1) **Définition.** Nous disons qu'une relation Q *raffine* [62] une relation R, ce qui sera noté $Q \sqsubseteq R$, ssi

$$RL \subseteq QL \text{ et } Q \cap RL \subseteq R$$

■

En d'autres termes, Q raffine R quand le domaine de R est inclus dans le domaine de Q et la prérestriction de Q au domaine de R est incluse dans R.

(3.2) **Exemples.**

- Nos premiers exemples sont des éléments d'une algèbre concrète (voir section 2.1). Tout d'abord,

  $$\{(0,0),(0,1),(1,0),(2,1)\} \sqsubseteq \{(0,0),(0,1),(0,2),(1,0),(1,1)\}.$$

  Il est facile de vérifier que les deux conditions de la définition (3.1) sont satisfaites. Ce n'est toutefois pas le cas pour les relations suivantes :

  $$\{(0,0),(0,1),(2,1)\} \not\sqsubseteq \{(0,0),(0,1),(0,2),(1,0),(1,1)\},$$

  car la condition sur les domaines n'est pas vérifiée, et de même

  $$\{(0,0),(1,0),(2,1)\} \not\sqsubseteq \{(0,0),(0,1),(0,2),(1,0),(2,0)\},$$

  étant donné que la prérestriction de la relation de gauche au domaine de la relation de droite n'est pas incluse dans cette dernière.

- Prenons maintenant des exemples dans l'algèbre des matrices booléennes (voir section 2.1).

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} \sqsubseteq \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

mais

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \not\sqsubseteq \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 1 & 1 \end{pmatrix} \not\sqsubseteq \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 1 & 1 \end{pmatrix}.$$

■

(3.3) **Théorème.** *La relation $\sqsubseteq$ est un ordre partiel.*

La démonstration de ce théorème ainsi que celles des prochains résultats dans ce chapitre se trouvent dans [26]. ■

Cet ordre de raffinement ($\sqsubseteq$) induit une structure de demi-treillis, appelé *demi-treillis démoniaque*, sur lequel sont définis des opérateurs dits *démoniaques*.

3.1.1 Opérateurs démoniaques

Dans cette sous-section, nous allons présenter les opérateurs démoniaques ainsi que quelques-unes de leurs propriétés. Pour plus de détails voir [12, 13, 16, 26].

(3.4) **Théorème.** *Soit $\mathcal{R}$ une algèbre de relations. Pour toute relation $R \in \mathcal{R}$, $(\mathcal{B}_R, \sqsubseteq)$ est un $\sqcup$-demi-treillis complet supérieurement, avec $\emptyset$ comme plus grand élément.*

Soit une famille de relations $\{R_i \mid i \in X\}$, où X est un ensemble d'indices, telle que pour tout $i \in X$, $R_i \in \mathcal{B}_R$, pour une certaine relation $R \in \mathcal{B}_R$.

- *La borne supérieure (supremum) des relations $\{R_i | i \in X\}$ est :*

$$\bigsqcup_{i \in X} R_i = (\bigcup_{i \in X} R_i) \cap (\bigcap_{i \in X} R_i L).$$

Nous avons

$$(\bigsqcup_{i \in X} R_i)L = \bigcap_{i \in X} R_i L.$$

- *La borne inférieure (infimum) des relations $\{R_i | i \in X\}$ existe ssi*

$$L \subseteq (\bigcap_{i \in X} R_i \cup \overline{R_i L})L.$$

Quand c'est le cas,

$$\bigsqcap_{i \in X} R_i = (\bigcap_{i \in X} R_i \cup \overline{R_i L}) \cap (\bigcup_{i \in X} R_i L),$$

où $\sqcap$ dénote l'infimum par rapport à $\sqsubseteq$; nous avons aussi

$$(\bigsqcap_{i \in X} R_i)L = \bigcup_{i \in X} R_i L.$$

■

Pour la démonstration voir [26].

Afin d'éclaircir les idées, prenons deux relations Q et R [16] :

- Leur supremum est

$$Q \sqcup R = (Q \cup R) \cap QL \cap RL \tag{3.5}$$

et il satisfait

$$(Q \sqcup R)L = QL \cap RL.$$

Donc, $Q \sqcup R$ est exactement l'expression relationnelle de l'*union démoniaque* telle que définie par Berghammer dans [12, 13] (ceci explique le qualificatif *démoniaque* du $\sqcup$-demi-treillis $(\mathcal{B}_R, \sqsubseteq)$). Considérons

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \sqcup \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Cette opération correspond au choix démoniaque non déterministe, étant donné que la possibilité d'échec (troisième ligne de la première matrice ou première ligne de la deuxième matrice) apparaît dans le résultat, tandis que pour la ligne du milieu, le résultat est l'union usuelle car il n'y a pas de possibilité d'échec.

- Leur infimum, s'il existe, est

$$\begin{aligned} Q \sqcap R &= (Q \cup \overline{QL}) \cap (R \cup \overline{RL}) \cap (QL \cup RL) \\ &= Q \cap R \cup Q \cap \overline{RL} \cup \overline{QL} \cap R, \end{aligned} \tag{3.6}$$

et il satisfait

$$(Q \sqcap R)L = QL \cup RL.$$

L'opérateur $\sqcap$ est appelé *intersection démoniaque*. Pour que $Q \sqcap R$ existe, il faut que $L \subseteq ((Q \cup \overline{QL}) \cap (R \cup \overline{RL}))L$. Cette condition est équivalente à $QL \cap RL \subseteq (Q \cap R)L$, qui peut être interprétée comme suit : pour chaque élément dans l'intersection de leurs domaines, Q et R doivent avoir au moins une image commune. Par exemple, considérons

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \sqcap \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix};$$

sur l'intersection de leurs domaines (la deuxième ligne), les deux matrices ont une image commune (la deuxième colonne), ce qui nous garantit l'existence de l'intersection démoniaque. Ce n'est toutefois pas le cas pour les matrices suivantes

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \text{ et } \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix},$$

étant donné que les matrices ont des résultats contradictoires sur l'intersection de leurs domaines. Nous assignons à $\sqcup$ et $\sqcap$ les mêmes priorités que celles de $\cup$ et $\cap$ (respectivement).

Dans ce qui suit, nous donnons quelques exemples ainsi que certains détails concernant les notions précédentes.

- La figure 3.1 présente l'algèbre homogène de toutes les matrices booléennes 2×2, ordonnée par $\sqsubseteq$.
- La figure 3.2 présente la structure d'une algèbre de relations homogène ordonnée par $\sqsubseteq$ (voir [77, 78]) qui n'est pas l'ensemble de toutes les matrices 3×3.
- La figure 3.3 illustre la structure générale de $(\mathcal{B}_R, \sqsubseteq)$ pour toute relation $R \in \mathcal{R}_{\sqsubseteq}$.

Nous attirons particulièrement l'attention sur les observations suivantes [16, 26].

- L'élément maximal est la relation $\emptyset$ et les relations totales qu'il n'est plus possible de raffiner sont les éléments minimaux ; dans la figure 3.1, les applications sont les éléments minimaux, mais la figure 3.2 montre que ce n'est pas toujours le cas dans une algèbre de relations arbitraire.
- Il est facile de montrer que dans le cas des vecteurs, $u \sqsubseteq v \Leftrightarrow v \subseteq u$. Mais, pour toute relation $R \in \mathcal{R}_{\sqsubseteq}$, l'ensemble des vecteurs de $\mathcal{B}_R$ est un sous-treillis complet de $(\mathcal{B}_R, \subseteq)$ [78, 79] ; donc, le treillis booléen des vecteurs est aussi un sous-treillis (inversé) de $(\mathcal{B}_R, \sqsubseteq)$. Nous remarquons que les vecteurs atomiques (par rapport à $\subseteq$) sont les prédécesseurs de la relation $\emptyset$.
- Finalement, pour des relations totales Q et R, $Q \sqsubseteq R \Leftrightarrow Q \subseteq R$; donc, dans ce cas-là, le raffinement est le même que l'inclusion (dans les figures présentées, les relations totales sont celles qui sont sous L).

Dans ce qui suit, nous donnons la définition de la composition démoniaque [12, 13, 14].

(3.7) **Définition.** La *composition démoniaque* des relations Q et R est

$$Q \mathbin{▫} R = QR \cap Q \triangleright RL.$$

■

L'opération $▫$ a la même priorité que (;).

- Dans une algèbre concrète de relations sur des ensembles, une paire (s, t) appartient à $Q ▫ R$ ssi elle appartient à QR et s'il n'existe aucune possibilité d'atteindre, à partir de s, par Q, un élément s' n'appartenant pas au domaine de R. Par exemple, soient les relations $Q := \{(1,1), (1,2), (3,3)\}$ et $R := \{(2,1), (3,2), (3,3)\}$. Nous trouvons que $Q ▫ R = \{(3,2), (3,3)\}$; la paire $(1,1)$, qui appartient à QR, n'appartient pas à $Q ▫ R$, car $(1,1) \in Q$ et 1 n'appartient pas au domaine de R.

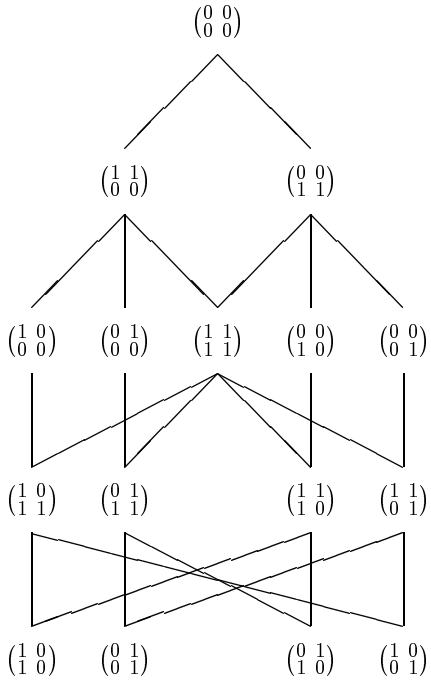


Figure 3.1: Algèbre de relations ordonnée par $\sqsubseteq$

- En utilisant les matrices, cet exemple se traduit comme suit :

$$\begin{pmatrix}1&1&0\\0&0&0\\0&0&1\end{pmatrix}\begin{pmatrix}0&0&0\\1&0&0\\0&1&1\end{pmatrix}=\begin{pmatrix}1&0&0\\0&0&0\\0&1&1\end{pmatrix}\text{ mais }\begin{pmatrix}1&1&0\\0&0&0\\0&0&1\end{pmatrix}\mathbin{▫}\begin{pmatrix}0&0&0\\1&0&0\\0&1&1\end{pmatrix}=\begin{pmatrix}0&0&0\\0&0&0\\0&1&1\end{pmatrix}.$$

  La première ligne de la matrice résultant de la composition (;) ne s'annule pas, car la première ligne de la matrice gauche peut conduire à une valeur qui est dans le domaine de la matrice droite (précisément, la deuxième ligne) ; mais la deuxième ligne de la composition démoniaque de ces deux matrices est nulle, car la première ligne de la matrice gauche peut mener à l'extérieur du domaine de la matrice droite (la première ligne).

3.1.2 Propriétés des opérateurs démoniaques

Les opérateurs démoniaques $\sqcap, \sqcup$ et $▫$ possèdent des propriétés similaires à celles de $\cap, \cup$ et (;), à condition que les intersections démoniaques soient définies. Donnons-en quelques-unes.

(3.8) **Théorème.** *Soient P, Q et R des relations. Alors,*

(a) $P \sqcap (Q \sqcup R) = (P \sqcap Q) \sqcup (P \sqcap R)$,

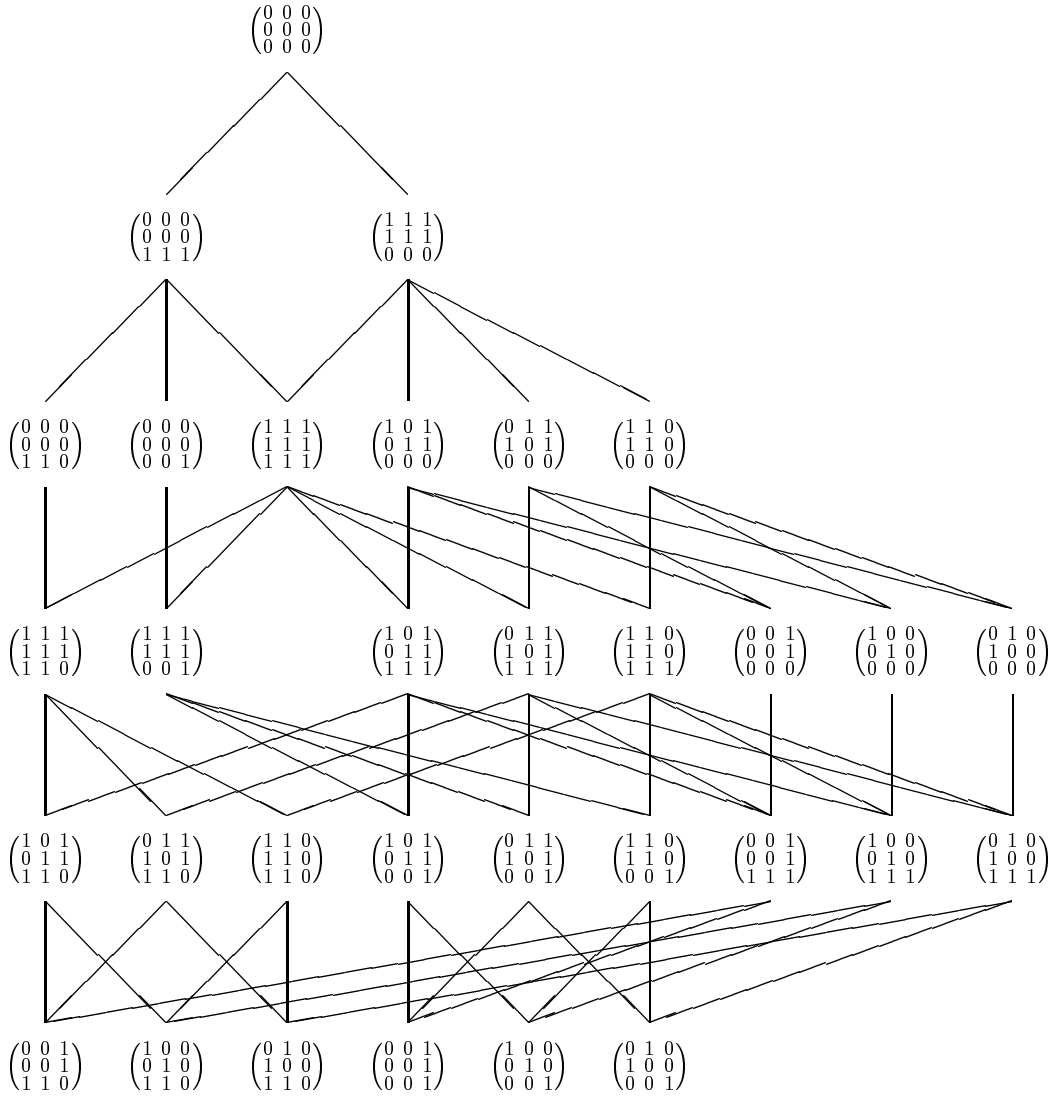


Figure 3.2: Une algèbre de relations ordonnée par $\sqsubseteq$

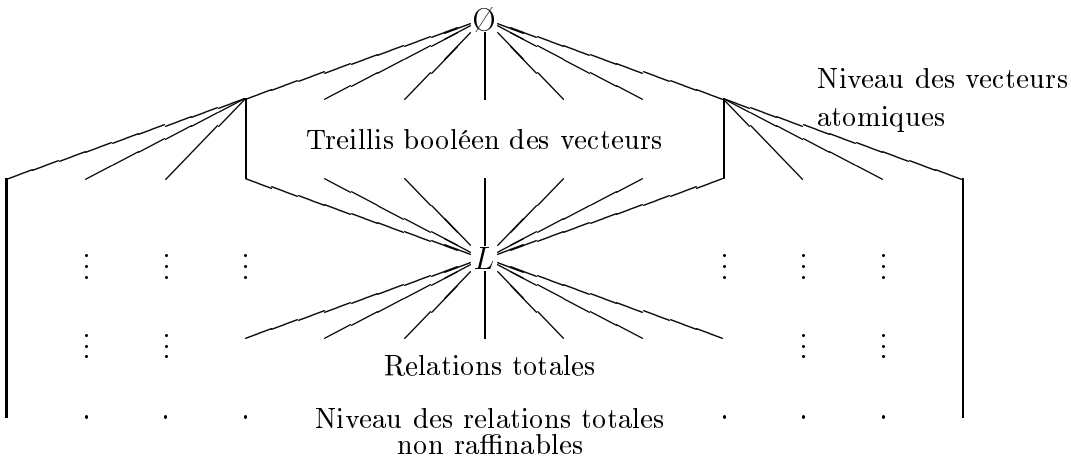


Figure 3.3: Structure générale du demi-treillis ordonné par $\sqsubseteq$

(b) $P \sqcup (Q \sqcap R) = (P \sqcup Q) \sqcap (P \sqcup R)$,

(c) $R \circ I = I \circ R = R$,

(d) $Q \sqsubseteq R \Rightarrow P \circ Q \sqsubseteq P \circ R$,

(e) $P \sqsubseteq Q \Rightarrow P \circ R \sqsubseteq Q \circ R$,

(f) $P \circ (Q \sqcup R) = P \circ Q \sqcup P \circ R$,

(g) $(P \sqcup Q) \circ R = P \circ R \sqcup Q \circ R$,

(h) $P \circ (Q \sqcap R) \sqsubseteq P \circ Q \sqcap P \circ R$,

(i) $P \circ (Q \circ R) = (P \circ Q) \circ R$,

(j) $(P \sqcap Q) \circ R \sqsubseteq P \circ R \sqcap Q \circ R$. ∎

Présentons quelques cas particuliers.

(3.9) **Proposition.**

(a) Q *déterministe* $\Rightarrow Q \circ R = QR$,

(b) P *déterministe* $\Rightarrow P \circ (Q \sqcap R) = PQ \sqcap PR$,

(c) R *totale* $\Rightarrow Q \circ R = QR$,

(d) $PL \cap QL = \emptyset \Rightarrow (P \cup Q) \circ R = P \circ R \cup Q \circ R$,

(e) $PL \cap QL = \emptyset \Rightarrow P \sqcap Q = P \cup Q$.

Démonstration. Nous faisons les démonstrations de (b), (d) et (e), les autres se trouvant dans [26].

(b) $P \mathbin{\triangledown} (Q \sqcap R)$
$= \quad$ { Proposition 3.9(a) et définition de $\sqcap$ (3.6). }
$P(Q \cap R \cup Q \cap \overline{RL} \cup R \cap \overline{QL})$
$= \quad$ { Théorème 2.21(9). }
$P(Q \cap R) \cup P(Q \cap \overline{RL}) \cup P(R \cap \overline{QL})$
$= \quad$ { Théorème 2.27(a). }
$PQ \cap PR \cup PQ \cap P\overline{RL} \cup PR \cap P\overline{QL}$
$= \quad$ { Théorème 2.27(f). }
$PQ \cap PR \cup PQ \cap PL \cap \overline{PRL} \cup PR \cap PL \cap \overline{PQL}$
$= \quad$ { Définition de $\sqcap$ (3.6) et $PQ \cap PL = PQ$, $PR \cap PL = PR$. }
$PQ \sqcap PR$

(d) $(P \cup Q) \mathbin{\triangledown} R$
$= \quad$ { Définition de $\mathbin{\triangledown}$ (3.7). }
$(P \cup Q)R \cap (P \cup Q) \triangleright RL$
$= \quad$ { Lemme 2.45(g). }
$(P \cup Q)R \cap P \triangleright RL \cap Q \triangleright RL$
$= \quad$ { Théorème 2.21(11). }
$PR \cap P \triangleright RL \cap Q \triangleright RL \cup QR \cap P \triangleright RL \cap Q \triangleright RL$
$= \quad$ { $PR \cap Q\overline{RL} \subseteq PL \cap QL = \emptyset \Rightarrow PR \subseteq Q \triangleright RL$; de même, $QR \subseteq P \triangleright RL$. }
$PR \cap P \triangleright RL \cup QR \cap Q \triangleright RL$
$= \quad$ { Définition de $\mathbin{\triangledown}$ (3.7). }
$P \mathbin{\triangledown} R \cup Q \mathbin{\triangledown} R$

(e) $P \sqcap Q$
$= \quad$ { Définition de $\sqcap$ (3.6). }
$P \cap Q \cup P \cap \overline{QL} \cup Q \cap \overline{PL}$
$= \quad$ { $PL \cap QL = \emptyset \Leftrightarrow PL \subseteq \overline{QL}$, donc $P \subseteq \overline{QL}$; de même, $Q \subseteq \overline{PL}$; finalement, $P \cap Q \cup P = P$. }
$P \cup Q$

■

Nous concluons cette section en présentant des résultats concernant les opérateurs démoniaques et les vecteurs.

(3.10) **Lemme.** *Soient Q, R des relations et u, v des vecteurs. Pourvu que les diverses occurrences de $\sqcap$ soient définies, nous avons*

(a) $v \cap (Q \sqcup R) = (v \cap Q) \sqcup (v \cap R)$,

(b) $(v \cap Q) \mathbin{\triangledown} R = v \cap Q \mathbin{\triangledown} R$,

(c) $R \mathbin{\triangledown} v = RL \cap R \triangleright v$,

(d) $Q \mathbin{\triangledown} (v \cap R) = Q \mathbin{\triangledown} v \cap Q \mathbin{\triangledown} R$, *[36, 83]*

(e) $v \cap (Q \sqcap R) = (v \cap Q) \sqcap (v \cap R)$,

(f) $Q \sqsubseteq R \Leftrightarrow v \cap Q \sqsubseteq v \cap R \wedge \overline{v} \cap Q \sqsubseteq \overline{v} \cap R$,

(g) $R \sqsubseteq v \cap R$,

(h) $v \cap Q \sqsubseteq R \;\Rightarrow\; Q \sqsubseteq R$.

Démonstration.

(a)
$v \cap (Q \sqcup R)$
$=$ { Théorème 2.21(36). }
$(v \cap I)(Q \sqcup R)$
$=$ { $v \cap I$ est déterministe et proposition 3.9(a). }
$(v \cap I) \triangleleft (Q \sqcup R)$
$=$ { Théorème 3.8(f) ($\triangleleft$ se distribue sur $\sqcup$). }
$(v \cap I) \triangleleft Q \sqcup (v \cap I) \triangleleft R$
$=$ { $v \cap I$ est déterministe et proposition 3.9(a). }
$(v \cap Q) \sqcup (v \cap R)$

Donc, $\cap$ se distribue sur $\sqcup$ si l'un de ses opérandes est un vecteur.

(b)
$(v \cap Q) \triangleleft R$
$=$ { Définition de $\triangleleft$ (3.7). }
$(v \cap Q)R \cap (v \cap Q) \triangleright RL$
$=$ { $v = vL$, théorème 2.21(36) et lemme 2.45(j). }
$v \cap QR \cap (\overline{v} \cup Q \triangleright RL)$
$=$ { Définition de $\triangleleft$ (3.7) et $v \cap \overline{v} = \emptyset$. }
$v \cap (Q \triangleleft R)$

Donc, la propriété 2.21(36) est valable même dans le cas où nous avons $\triangleleft$ au lieu de $(;)$.

(c)
$R \triangleleft v$
$=$ { Définition de $\triangleleft$ (3.7). }
$Rv \cap R \triangleright v$
$=$ { Théorème 2.21(9) et $R\overline{v} \cap R \triangleright v = \emptyset$. }
$R(v \cup \overline{v}) \cap R \triangleright v$
$=$ { $v \cup \overline{v} = L$. }
$RL \cap R \triangleright v$

(d)
$Q \triangleleft (v \cap R)$
$=$ { Définition de $\triangleleft$ (3.7). }
$Q(v \cap R) \cap Q \triangleright (v \cap R)L$
$=$ { $v = vL$, théorème 2.21(36), lemme 2.45(e) et $Q \triangleright v \cap Q\overline{v} = \emptyset$. }
$Q(v \cap R \cup \overline{v}) \cap Q \triangleright v \cap Q \triangleright RL$
$=$ { Théorème 2.21(5). }
$Q(R \cup \overline{v}) \cap Q \triangleright v \cap Q \triangleright RL$

$=$ { Théorème 2.21(9), $QR \subseteq QL$ et $Q\overline{v} \cap Q \triangleright v = \emptyset$. }
$QL \cap Q \triangleright v \cap QR \cap Q \triangleright RL$
$=$ { Définition de $\square$ (3.7) et proposition 3.10(c). }
$Q \square v \cap Q \square R$

Donc, $\square$ se distribue à droite sur $\cap$ dans le cas où l'un des termes de l'intersection est un vecteur.

(e) $v \cap (Q \sqcap R)$
$=$ { Théorème 2.21(36). }
$(v \cap I)(Q \sqcap R)$
$=$ { Proposition 3.9(a). }
$(v \cap I) \square (Q \sqcap R)$
$=$ { Proposition 3.9(b). }
$(v \cap I)Q \sqcap (v \cap I)R$
$=$ { Théorème 2.21(36). }
$(v \cap Q) \sqcap (v \cap R)$

(f) $Q \sqsubseteq R$
$\Leftrightarrow$ { Définition de $\sqsubseteq$ (3.1). }
$Q \cap RL \subseteq R \ \wedge \ RL \subseteq QL$
$\Leftrightarrow$ { Pour tout vecteur v et relations Q, R, $Q \subseteq R \Leftrightarrow v \cap Q \subseteq v \cap R \ \wedge \ \overline{v} \cap Q \subseteq \overline{v} \cap R$. }
$v \cap Q \cap RL \subseteq v \cap R \ \wedge \ v \cap RL \subseteq v \cap QL$
$\wedge \ \overline{v} \cap Q \cap RL \subseteq \overline{v} \cap R \ \wedge \ \overline{v} \cap RL \subseteq \overline{v} \cap QL$
$\Leftrightarrow$ { v et $\overline{v}$ étant des vecteurs, le théorème 2.21(36) donne $(v \cap R)L = v \cap RL$ et $(\overline{v} \cap R)L = \overline{v} \cap RL$. }
$\Leftrightarrow v \cap Q \cap (v \cap R)L \subseteq v \cap R \ \wedge \ (v \cap R)L \subseteq (v \cap Q)L$
$\wedge \ \overline{v} \cap Q \cap (\overline{v} \cap R)L \subseteq \overline{v} \cap R \ \wedge \ (\overline{v} \cap R)L \subseteq (\overline{v} \cap Q)L$
$=$ { Définition 3.1. }
$v \cap Q \sqsubseteq v \cap R \ \wedge \ \overline{v} \cap Q \sqsubseteq \overline{v} \cap R$

(g) À partir de la définition de $\sqsubseteq$ (3.1) et 2.21(36),

$$R \sqsubseteq v \cap R \ \Leftrightarrow \ (v \cap R)L \subseteq RL \ \wedge \ R \cap v \cap RL \subseteq v \cap R \ \Leftrightarrow \ \text{vrai}.$$

(h) Par (g), $Q \sqsubseteq v \cap Q \sqsubseteq R \Rightarrow Q \sqsubseteq R$. ∎

La remarque suivante est utile pour le reste de notre tarvail.

(3.11) **Remarque.** Soit la fonction $f(X) := Q \cup P \square X$, avec $PL \cap QL = \emptyset$. Alors,

- f a au moins un point fixe car elle est $\subseteq$-monotone et le treillis ordonné par $\subseteq$ est complet.
- f est $\sqsubseteq$-monotone. En effet, si X et Y sont deux relations telles que $X \sqsubseteq Y$, nous avons

$$
\begin{array}{ll}
& X \sqsubseteq Y \\
\Rightarrow & \quad \{ \text{ Théorème 3.8(e). } \} \\
& P \circ X \sqsubseteq P \circ Y \\
\Rightarrow & \quad \{ \circ \text{ monotone par rapport à } \sqsubseteq. \} \\
& Q \sqcap P \circ X \sqsubseteq Q \sqcap P \circ Y \\
\Leftrightarrow & \quad \{ \text{ Proposition 3.9(e) (car } PL \cap QL = \emptyset). \} \\
& Q \cup P \circ X \sqsubseteq Q \cup P \circ Y
\end{array}
$$

Ce qui implique que $\bigsqcup\{X \mid X = f(X)\}$ est le plus grand point fixe par rapport à $\sqsubseteq$ de f (2.11(b)), c'est-à-dire $\nu \Leftrightarrow \sqsubseteq (f)$.

Dans la section suivante, nous donnons la sémantique dénotationnelle démoniaque des constructeurs suivants : l'affectation, la séquence, le choix gardé et la boucle.

3.2 Sémantique dénotationnelle démoniaque

La sémantique démoniaque d'un programme p non déterministe est donnée par une relation $\mathcal{D}[\![p]\!]$, où $\mathcal{D}$ est une fonction de l'ensemble des programmes $\mathcal{P}$ vers une certaine algèbre de relations (voir 2.18). Comme nous nous intéressons à des programmes impératifs, cette algèbre est généralement une algèbre complète de la forme $\mathrm{Rel}(X)$ (exemple 2.19(b)). Les constructeurs considérés sont l'affectation, la séquence, le choix gardé et la boucle. Tout au long de notre travail, nous supposons que les algèbres sont complètes, afin de pouvoir traiter le cas de la boucle. Nous allons d'abord présenter brièvement la syntaxe avant d'introduire notre sémantique dénotationnelle.

3.2.1 Syntaxe

Nous utilisons les termes *programmes* et *instructions* de manière interchangeable. En réalité, se sont donc des fragments de programmes qui sont considérés. Chaque programme contient un certain nombre de variables $x_0, \ldots, x_n$. Nous ne précisons pas la syntaxe des expressions admissibles. Lorsqu'un programme concret est utilisé dans la thèse, les variables et leur type sont indiqués dans le texte qui précède le programme. C'est pour cette raison que la syntaxe des déclarations n'est pas présentée. Soit i une instruction.

- affectation

  $$x_i := f(x),$$

  où $f(x)$ est une expression qui dépend de x_0, …, x_n.

- séquence

  $$i_1; i_2,$$

  où i_1 et i_2 sont des instructions.

- choix gardé

$$\textbf{if } c_1 \to i_1 [] \ c_2 \to i_2 \textbf{ fi},$$

où chaque c_i est une expression booléenne appelée *garde* et où i_1 et i_2 sont des instructions. Ceci peut se généraliser au cas d'un nombre arbitraire de gardes.

- boucle

$$\textbf{do } c \to i \textbf{ od},$$

où c est une expression booléenne (la garde) et i une instruction.

3.2.2 Sémantique

Nous allons maintenant, donner la sémantique dénotationnelle démoniaque de chacun de nos constructeurs. Il convient de noter que ces résultats sont tirés de [27].

(3.12) **Remarque.** Dans nos exemples, nous utilisons les ensembles pour définir les espaces des programmes. L'espace d'un programme est déterminé par les variables du programme et leur type. Ainsi, les ensembles qui nous intéressent correspondent à des produits cartésiens d'ensembles prédéfinis.

Soit R une relation définie sur un ensemble X qui est le produit cartésien des ensembles $X_0, \ldots, X_n$. Un élément $x \in X$ a la forme $x = (x_0, \ldots, x_n)$, où $x_i \in X_i$, donc la notation (x, x') n'est qu'une abréviation de $((x_0, \ldots, x_n), (x'_0, \ldots, x'_n))$. ∎

Débutons par le cas de base, celui de l'affectation.

- **Affectation**

Supposons que $x_0, \ldots, x_n$ sont les variables du programme et qu'elles prennent leurs valeurs dans $X_0, \ldots, X_n$, respectivement, et que f est une certaine fonction exécutable. La sémantique démoniaque de l'affectation

$$x_i := f(x),$$

où $0 \leq i \leq n$, $x = (x_0, \ldots, x_n)$ et $x' = (x'_0, \ldots, x'_n)$, est la relation

$$\mathcal{D}[\![x_i := f(x)]\!] := \{(x, x') \mid (\forall j : 0 \leq j \leq n : x_j \in X_j \wedge x'_j \in X_j) \wedge x'_i = f(x) \\ \wedge (\forall j : 0 \leq j \leq n \wedge j \neq i : x'_j = x_j)\}. \tag{3.13}$$

- **Séquence**

La sémantique démoniaque de la séquence $p; q$ des programmes p et q est

$$\mathcal{D}[\![p; q]\!] := \mathcal{D}[\![p]\!] \diamond \mathcal{D}[\![q]\!]. \tag{3.14}$$

- **Choix gardé**

La sémantique démoniaque du choix gardé $\textbf{if } g_1 \to p_1 [] \ g_2 \to p_2 \textbf{ fi}$ est

$$(3.15)\quad \begin{aligned}\mathcal{D}[\![\ \textbf{if}\ g_1 \to p_1 [\!]\ g_2 \to p_2\ \textbf{fi}\ ]\!] := \quad & \mathcal{G}[\![g_1]\!] \circ \mathcal{G}[\![g_2]\!]^{\sim} \circ \mathcal{D}[\![p_1]\!] \\ & \sqcap\ \mathcal{G}[\![g_1]\!]^{\sim} \circ \mathcal{G}[\![g_2]\!] \circ \mathcal{D}[\![p_2]\!] \\ & \sqcap\ \mathcal{G}[\![g_1]\!] \circ \mathcal{G}[\![g_2]\!] \circ (\mathcal{D}[\![p_1]\!] \sqcup \mathcal{D}[\![p_2]\!]),\end{aligned}$$

où $\mathcal{G}[\![g_i]\!]$ est la sémantique de la garde g_i, $i = 1, 2$. La relation $\mathcal{G}[\![g_i]\!]$ est une identité partielle dont le domaine satisfait la condition de la garde. Notons que $\mathcal{G}$ s'applique à des expressions booléennes alors que $\mathcal{D}$ s'applique à des instructions et que pour cette raison que nous utilisons deux symboles différents.

Comme les relations $\mathcal{G}[\![g_i]\!]$ sont des identités partielles, en appliquant la proposition 3.9(a,e), l'expression (3.15) est exprimée avec des opérateurs angéliques comme suit :

$$(3.16)\quad \begin{aligned}\mathcal{D}[\![\textbf{if}\ g_1 \to p_1 [\!]\ g_2 \to p_2\ \textbf{fi}]\!] = \quad & \mathcal{G}[\![g_1]\!]\mathcal{G}[\![g_2]\!]^{\sim}\mathcal{D}[\![p_1]\!]\ \cup\ \mathcal{G}[\![g_1]\!]^{\sim}\mathcal{G}[\![g_2]\!]\mathcal{D}[\![p_2]\!] \\ & \cup\ \mathcal{G}[\![g_1]\!]\mathcal{G}[\![g_2]\!](\mathcal{D}[\![p_1]\!] \sqcup \mathcal{D}[\![p_2]\!]).\end{aligned}$$

Cette expression se comprend intuitivement comme suit :

Si g_1 est vraie et g_2 fausse, exécuter p_1 ; si g_1 est fausse et g_2 vraie, exécuter p_2 ; si les deux gardes sont vraies, alors faire un choix démoniaque entre p_1 et p_2 ($\sqcup$).

Dans le cas où les gardes sont mutuellement exclusives, en appliquant les lois 3.9(a,e) et 2.29(c,d), l'équation 3.15 se réduit à :

$$\mathcal{D}[\![\textbf{if}\ g_1 \to p_1 [\!]\ g_2 \to p_2\ \textbf{fi}]\!] = \mathcal{G}[\![g_1]\!] \circ \mathcal{D}[\![p_1]\!] \sqcap \mathcal{G}[\![g_2]\!] \circ \mathcal{D}[\![p_2]\!].$$

Dans le cas d'un nombre arbitraire de gardes, nous avons

$$(3.17)\quad \mathcal{D}[\![\textbf{if}\ [\!]_{i=1}^{n} g_i \to p_i\ \textbf{fi}]\!] := \bigsqcap_X g_X \circ g_{\widetilde{X}} \circ p_X,$$

où

- $n \geq 0$,
- $\emptyset \neq X \subseteq \{0, \ldots, n\}$
- $\overline{X}$ est le complément de X par rapport à $\{1, \ldots, n \Leftrightarrow 1\}$,
- g_X est la composition démoniaque des identités partielles $\mathcal{G}(g_i)$, pour $i \in X$,
- $g_{\widetilde{X}}$ est la composition démoniaque des identités partielles $\mathcal{G}(g_i)^{\sim}$, pour $i \in \overline{X}$ (comme $\mathcal{G}(g_i)$ et $\mathcal{G}(g_i)^{\sim}$ sont des identités partielles, l'ordre de composition n'est pas important par 2.29(c)) ; pour $\overline{X} = \emptyset$, nous définissons $g_{\widetilde{X}}^{\sim} = I$,
- $p_X = \bigsqcup_{i \in X} \mathcal{D}[\![p_i]\!]$.

Pour $n = 2$, nous retrouvons l'équation (3.15).

- **Boucle**

  Le dernier cas que nous traitons est celui de la boucle $W := \mathbf{do}\ g \to p\ \mathbf{od}$, où g est la condition (garde) de boucle et p est le corps de boucle.

  La sémantique démoniaque de cette boucle W est le plus grand point fixe par rapport à $\sqsubseteq$ de la fonction sémantique $W_d(X) := \mathcal{G}[\![g]\!]^{\sim} \sqcap \mathcal{G}[\![g]\!] \circ \mathcal{D}[\![p]\!] \circ X$ (l'indice d nous rappelle *d*émoniaque), où $\mathcal{G}[\![g]\!]$ est la sémantique de la garde g ; comme pour le choix gardé, $\mathcal{G}[\![g]\!]$ est une identité partielle dont le domaine satisfait la condition de la garde. Formellement,

  $$\mathcal{D}[\![W]\!] = \bigsqcup\{X \mid X = \mathcal{G}[\![g]\!]^{\sim} \sqcap \mathcal{G}[\![g]\!] \circ \mathcal{D}[\![p]\!] \circ X\}. \tag{3.18}$$

  Comme les domaines des deux facteurs de $\sqcap$ sont disjoints, que les gardes sont des identités partielles (donc déterministes) et que $\circ$ est associative, nous avons, par 3.9(a,e),

  $$W_d(X) = \mathcal{G}[\![g]\!]^{\sim} \cup (\mathcal{G}[\![g]\!]\mathcal{D}[\![p]\!]) \circ X, \tag{3.19}$$

  qui est une forme plus familière de la définition d'une boucle. Par la proposition 2.11(b), nous avons aussi $\mathcal{D}[\![W]\!] = \bigsqcup\{X \mid X \sqsubseteq W_d(X)\}$. Par la remarque 3.11, $\mathcal{D}[\![W]\!]$ existe et elle est bien définie. L'expression 3.18 est la sémantique démoniaque de la boucle donnée dans des travaux antérieurs [1, 28]. Le fait de choisir le plus grand point fixe (par rapport à $\sqsubseteq$) signifie que c'est le point fixe avec le plus petit domaine qui est choisi, ce qui est conforme au point de vue démoniaque. D'autres définitions similaires de la sémantique démoniaque de la boucle se trouvent dans [69, 83].

Remarquons que pour les instructions (affectation, séquence, choix gardé et boucle), la sémantique de chaque instruction a été donnée directement sur la base d'une compréhension intuitive du comportement de l'instruction considérée. Celle de la boucle, c'est-à-dire $\mathcal{D}[\![W]\!]$, est le plus grand point fixe d'une certaine fonction. On peut montrer son existence mais il est difficile de le calculer directement. Pour résoudre ce problème, lorsque la boucle est déterministe, il est possible d'utiliser un théorème connu sous le nom de *règle de vérification de boucle de Mills* [63, 64]. Nous avons généralisé ce théorème à un contexte non déterministe. Cette généralisation fait l'objet du prochain chapitre.

(3.20) **Remarque.** Dans les chapitres suivants, pour éviter l'usage assez lourd des fonctions sémantiques $\mathcal{D}$ et $\mathcal{G}$ de ce chapitre, les programmes seront notés en style `verbatim` et leur sémantique en style mathématique. Par exemple, prenons le programme **do** `g` $\to$ `B` **od** ; la sémantique de la condition de boucle `g` sera dénotée par g et la sémantique du corps de boucle `B` par B.

3.3 Conclusion

Dans ce chapitre, nous avons présenté la notion d'ordre de raffinement ainsi que les opérateurs induits par cet ordre. Nous avons aussi donné les définitions sémantiques des instructions affectation, séquence, choix et boucle. Ces définitions ont été tirées de [27]. Des exemples seront donnés dans le chapitre suivant. En considérant le diagramme de la figure 1.1, nous avons établi la partie qui concerne la fonction $\mathcal{D}$.

Chapitre 4

Règle de vérification de boucles

En général, il n'existe aucune méthode formelle pour calculer la sémantique d'une boucle directement à partir du programme. Il est clair qu'un calcul direct à partir de l'équation (3.18) est difficile ou même impossible (si c'était possible on aurait une solution au problème de l'arrêt). Si une relation candidate est donnée, il est plus facile de vérifier si cette relation est effectivement une solution, c'est-à-dire si elle est la sémantique de la boucle en question. Il existe une méthode générale pour faire cette vérification. Cette méthode est appelée *la règle de vérification de boucle de Mills* [63, 64]. Cette règle a été donnée dans un contexte déterministe. Dans ce chapitre, nous en donnons une généralisation ; nous considérons un programme non déterministe et nous supposons sa pire exécution (voir section 1.4). Dans la première section nous présentons le théorème de Mills dans un contexte déterministe, c'est-à-dire dans le cas où la sémantique du corps de boucle ainsi que la relation candidate sont des fonctions. Nous terminons cette section par un exemple d'application simple, mais qui illustre bien l'utilité de ce théorème. Avant de donner notre généralisation, nous présentons des résultats préliminaires sur les points fixes. L'application principale de cette généralisation, aux fins de cette thèse, sera donnée dans le chapitre 5.

4.1 Cas des boucles déterministes

Dans l'approche de Mills, la sémantique W d'une boucle déterministe **do** g $\to$ B **od** est donnée comme le plus petit point fixe (par rapport à l'inclusion) de la fonction

$$f_a(X) := g^\sim \cup gBX, \tag{4.1}$$

où l'identité partielle g est la sémantique de la condition de boucle g et la relation B est la sémantique du corps de boucle B. La boucle **do** g $\to$ B **od** est dite déterministe si B est déterministe. Parce que la relation B est déterministe, nous pouvons montrer que la définition de Mills est équivalente à celle donnée au chapitre précédent (équation 3.18). Comme nous considérons une algèbre de relations complète (tel qu'indiqué à la section 3.2) et que la fonction f_a est monotone (par rapport à $\subseteq$), par le théorème 2.10 le plus petit point fixe W de f_a existe et $W = (gB)^* g^\sim$.

Donnons le théorème de Mills [63, 64] et sa démonstration. Notre démonstration est différente de celle de Mills ; elle est plus simple et plus directe.

4.1.1 Théorème de Mills pour les programmes déterministes

(4.2) **Théorème.** *(Règle de vérification de boucle de Mills [63, 64].) Soient R et B des fonctions et W le plus petit point fixe (par rapport à $\subseteq$) de la fonction f_a (équation 4.1).*

Alors, $R = W$ ssi les conditions suivantes sont satisfaites :

$$\begin{array}{ll} (a) & R = f_a(R), \\ (b) & RL \subseteq WL. \end{array}$$

Démonstration.

($\Rightarrow$) : évident.

($\Leftarrow$) : Par l'hypothèse (a), la relation R est un point fixe de la fonction f_a et comme W est le plus petit point fixe de f_a, alors $W \subseteq R$. Nous avons donc $W \subseteq R$ et $RL \subseteq WL$. Par le théorème 2.27(p), nous obtenons $R = W$. ∎

L'hypothèse que R soit une fonction n'est pas une restriction. En effet, on peut montrer que si B est une fonction, alors W est une fonction.

Nous présentons un exemple simple mais qui illustre bien l'utilisation de ce théorème.

(4.3) **Exemple.** Considérons la boucle suivante :

$$\textbf{do } \texttt{b} > 0 \to \texttt{b} := \texttt{b} \Leftrightarrow 1 \ ; \ \texttt{c} := \texttt{c} \times \texttt{a} \textbf{ od}.$$

où les trois variables `a`, `b` et `c` sont des variables sur l'ensemble $\mathbf{N}$ des nombres naturels $\{0, 1, 2, \ldots\}$.

En utilisant la notion de sémantique donnée dans le chapitre 3, nous avons les résultats suivants :

- La relation donnant la sémantique du corps de boucle est :

  $$B = \{((a,b,c),(a',b',c')) \mid a,b,c,a',b',c' \in \mathbf{N} \wedge a' = a \wedge b' = b \Leftrightarrow 1 \wedge c' = ca\},$$

  que nous abrégeons par :

  $$B = \{a' = a \wedge b' = b \Leftrightarrow 1 \wedge c' = ca\},$$

  et de même pour toutes les autres relations qui vont suivre. Remarquons que B est déterministe.

- L'identité partielle décrivant la condition de boucle est

  $$g = \{b > 0 \wedge a' = a \wedge b' = b \wedge c' = c\},$$

  et donc,

  $$g^{\sim} = \{b \leq 0 \wedge a' = a \wedge b' = b \wedge c' = c\}.$$

- La sémantique de la boucle est donnée par la relation W qui est le plus petit point fixe de f_a (équation 4.1).

Maintenant, donnons notre relation candidate

$$R = \{a' = a \wedge b' = 0 \wedge c' = ca^b\}.$$

Remarquons que R est déterministe. Notre but est de montrer que R est la sémantique de la boucle ci-dessus. Nous devons vérifier les conditions (a) et (b) du théorème 4.2. Commençons par la condition (a).

$$\begin{array}{ll}
& f_a(R) \\
= & \qquad \{ \text{ Équation 4.1. } \} \\
& g^\sim \cup gBR \\
= & \qquad \{ \text{ Substitution de } g, B, R \text{ et composition de } g \text{ et } B. \} \\
& g^\sim \cup \{b > 0 \wedge a' = a \wedge b' = b \Leftrightarrow 1 \wedge c' = ca\}\{a' = a \wedge b' = 0 \wedge c' = ca^b\} \\
= & \qquad \{ \text{ Définition de la composition. } \} \\
& g^\sim \cup \{\exists a'', b'', c'' : b > 0 \wedge a'' = a \wedge b'' = b \Leftrightarrow 1 \wedge c'' = ca \\
& \qquad\qquad \wedge\ a' = a'' \wedge b' = 0 \wedge c' = c''a''^{b''}\} \\
= & \qquad \{ \text{ Substituant } g^\sim \text{ par sa valeur, éliminant le quantificateur et } caa^{b-1} = ca^b. \\
& \qquad \} \\
& \{b \leq 0 \wedge a' = a \wedge b' = b \wedge c' = c\} \cup \{b > 0 \wedge a' = a \wedge b' = 0 \wedge c' = ca^b\} \\
= & \qquad \{ \text{ Sur } \mathbf{N},\ b \leq 0 \ \Leftrightarrow\ b = 0, \text{ et } b^0 = 1. \} \\
& \{b = 0 \wedge a' = a \wedge b' = 0 \wedge c' = ca^b\} \cup \{b > 0 \wedge a' = a \wedge b' = 0 \wedge c' = ca^b\} \\
= & \{b \geq 0 \wedge a' = a \wedge b' = 0 \wedge c' = ca^b\} \\
= & \qquad \{ \ (\forall b : b \in \mathbf{N} : b \geq 0). \ \} \\
& \{a' = a \wedge b' = 0 \wedge c' = ca^b\} \\
= & R
\end{array}$$

Donc, la condition (a) est vérifiée.

Pour la condition (b), l'argument est le suivant [63, 64]. La relation W est totale, puisque tout entier n satisfaisant la condition g est dans le domaine de la relation $gB = \{b > 0 \wedge a' = a \wedge b' = b \Leftrightarrow 1 \wedge c' = ca\}$ et qu'il n' y a aucune suite infinie par gB (en répétant l'application de gB l'entier naturel b se réduit à 0, et aucun état de la forme $(a, 0, c)$ n'est dans le domaine de gB). Donc, $RL \subseteq L = WL$. Il s'agit d'un argument informel qui pourrait être formalisé ; pour un exemple, voir 4.15. ∎

4.2 Cas des boucles non déterministes

Le problème de la section précédente se pose aussi dans le cas non déterministe déjà indiqué, c'est-à-dire prouver qu'une relation W est la relation calculée par un programme itératif non déterministe **do** g $\rightarrow$ B **od** en supposant sa pire exécution. En utilisant les notions données dans le chapitre 3, ceci revient à vérifier si la relation W est effectivement le plus grand point fixe de la fonction

(4.4) $f_d(X) := g^\sim \cup (gB) \boxdot X,$

dans le demi-treillis démoniaque (voir équation 3.19). Ce qui est équivalent à montrer l'équation suivante :

(4.5) $W = \bigsqcup\{X | X \sqsubseteq g^\sim \cup (gB) \boxdot X\}.$

Considérons le cas général suivant :

(4.6) $W = \bigsqcup\{X | X \sqsubseteq Q \cup P \boxdot X\},$

avec $PL \cap QL = \emptyset$. Pour retrouver notre cas particulier, il suffit de prendre $P := gB$ et $Q := g^\sim$.

4.2.1 Résultats préliminaires

Introduisons les abréviations suivantes :

(4.7) **Abréviation.** Soient P et Q des relations telles que $PL \cap QL = \emptyset$. Les abréviations w_d, w_a, w_L et $\mathcal{A}(P,Q)$ sont définies comme suit (x est un vecteur) :

$$w_d(X) := Q \cup P \boxdot X, \qquad w_a(X) := Q \cup PX,$$
$$w_L(x) := QL \cup P \boxdot x, \qquad \mathcal{A}(P,Q) := P^* \triangleright (PL \cup QL).$$

■

(Indice mnémonique : les indices a et d rappellent *a*ngélique et *d*émoniaque, respectivement ; l'indice L rappelle que w_L est obtenu à partir de w_d par composition avec L. La raison du choix de $\mathcal{A}$ sera donnée dans le chapitre suivant.)

Le lemme suivant fait le lien entre les points fixes de w_L et de w_d (abréviation 4.7).

(4.8) **Remarque.** Dans le cas où $P := gB$ et $Q := g^\sim$, nous avons $w_d(X) = f_d(X)$ et $w_a(X) = f_a(X)$ (voir 4.1, 4.4).

(4.9) **Lemme.** *Si Y est un point fixe de w_d alors YL est un point fixe de w_L.*

Démonstration. Supposons que $w_d(Y) = Y$.

$$\begin{array}{ll} & w_L(YL) \\ = & \quad \{ \text{ Définition de } w_L \text{ (4.7). } \} \\ & QL \cup P \boxdot (YL) \\ = & \quad \{ \text{ Proposition 3.9(c). } \} \\ & QL \cup P \boxdot (Y \boxdot L) \\ = & \quad \{ \text{ Théorème 3.8(i), proposition 3.9(c) et théorème 2.21(11). } \} \\ & (Q \cup P \boxdot Y)L \\ = & \quad \{ \text{ Définition de } w_d \text{ (4.7) et } w_d(Y) = Y. \} \\ & YL \end{array}$$

■

Dans ce qui suit, nous donnons les bornes des points fixes de w_L et nous montrons que ces bornes sont des points fixes de w_L.

(4.10) **Théorème.** *Si Y est un point fixe de w_d, alors*

1. $\mathcal{A}(P,Q) \cap \mathcal{B}(P) \subseteq YL \subseteq \mathcal{A}(P,Q)$,
2. $\mathcal{A}(P,Q) \cap \mathcal{B}(P)$ *et* $\mathcal{A}(P,Q)$ *sont des points fixes de* w_L.

Démonstration.

1. Par le lemme 4.9, YL est un point fixe de w_L. Montrons d'abord que $w_L(x) = (PL \cup QL) \cap P \triangleright x$, où x est un vecteur.

   $$\begin{array}{ll} & w_L(x) \\ = & \quad \{ \text{ Abréviation 4.7. } \} \\ & QL \cup P \,\square\, x \\ = & \quad \{ \; QL \subseteq \overline{PL} \subseteq P \triangleright x \text{ et lemme 3.10(c). } \} \\ & QL \cap P \triangleright x \cup PL \cap P \triangleright x \\ = & \quad \{ \text{ Loi booléenne. } \} \\ & (QL \cup PL) \cap P \triangleright x \end{array}$$

2. Donc YL est un point fixe de $w_L(x) = (PL \cup QL) \cap P \triangleright x$. En remplaçant $Q := PL \cup QL$ dans le corollaire 2.58, nous trouvons

   $$P^* \triangleright (PL \cup QL) \cap \mathcal{B}(P) \subseteq YL \subseteq P^* \triangleright (PL \cup QL);$$

   en utilisant l'abréviation 4.7, nous obtenons

   $$\mathcal{A}(P,Q) \cap \mathcal{B}(P) \subseteq YL \subseteq \mathcal{A}(P,Q).$$

3. Par le corollaire 2.58, nous déduisons que $\mathcal{A}(P,Q) \cap \mathcal{B}(P)$ et $\mathcal{A}(P,Q)$ sont des points fixes de w_L. ∎

Le lemme suivant montre que l'intersection d'un point fixe de w_d et d'un point fixe de w_L est un point fixe de w_d.

(4.11) **Lemme.** *Soient Y un point fixe de w_d et y un point fixe de w_L (abréviation 4.7). La relation $y \cap Y$ est un point fixe de w_d.*

Démonstration.

$$
\begin{aligned}
& w_d(y \cap Y) \\
= \; & Q \cup P \,\square\, (y \cap Y) \\
= \; & \qquad \{ \text{ Lemme 3.10(d). } \} \\
& Q \cup P \,\square\, y \cap P \,\square\, Y \\
= \; & \qquad \{ \text{ Lois booléennes, } P \,\square\, Y \subseteq PL \text{ et } PL \cap QL = \emptyset. \} \\
& (QL \cup P \,\square\, y) \cap (Q \cup P \,\square\, Y) \\
= \; & \qquad \{ \; y = w_L(y) \text{ et } Y = w_d(Y). \; \} \\
& y \cap Y
\end{aligned}
$$

■

Le théorème suivant nous donne une caractérisation du domaine du plus grand point fixe de la fonction w_d (par rapport à $\sqsubseteq$). Ce domaine est l'ensemble des points à partir desquels la terminaison est garantie (il n'y a aucune boucle infinie ou échec).

(4.12) **Théorème.** *Soit W le plus grand point fixe de w_d (abréviation 4.7) par rapport à $\sqsubseteq$. Nous avons*

$$WL = \mathcal{A}(P, Q) \cap \mathcal{B}(P).$$

Démonstration.

(a) Par le théorème 4.10, $\mathcal{A}(P, Q) \cap \mathcal{B}(P)$ est un point fixe de w_L et vérifie

$$\mathcal{A}(P, Q) \cap \mathcal{B}(P) \subseteq WL.$$

(b) Par (a) et le lemme 4.11, $\mathcal{A}(P, Q) \cap \mathcal{B}(P) \cap W$ est un point fixe de w_d. Par la proposition 3.10(g), $W \sqsubseteq \mathcal{A}(P, Q) \cap \mathcal{B}(P) \cap W$. Mais W est le plus grand point fixe (par rapport à $\sqsubseteq$) de w_d, donc

$$W = \mathcal{A}(P, Q) \cap \mathcal{B}(P) \cap W.$$

(c) À partir de (b) et du théorème 2.21(33,36) (étant donné que $\mathcal{A}(P, Q)$ et $\mathcal{B}(P)$ sont des vecteurs), $WL = \mathcal{A}(P, Q) \cap \mathcal{B}(P) \cap WL$, ce qui est équivalent à

$$WL \subseteq \mathcal{A}(P, Q) \cap \mathcal{B}(P).$$

Le résultat découle de (a) et (c). ■

Le lemme suivant nous donne une condition suffisante pour que deux points fixes de w_d coïncident.

(4.13) **Lemme.** *Si Y et Y' sont deux points fixes de w_d (abréviation 4.7) tels que $YL = Y'L$ et $YL \cap P$ est progressivement finie, alors $Y = Y'$.*

Démonstration. Soit $v := YL \ \ (= Y'L)$.

$$
\begin{array}{ll}
& Y \\
= & \qquad \{\ Y \subseteq v,\ Q \subseteq \overline{PL} \text{ et } Y = w_d(Y).\ \} \\
& v \cap (Q \cap \overline{PL} \cup P \,\square\, Y) \\
= & \qquad \{\ \text{Loi booléenne, définition de } \square \ (3.7) \text{ et } v = YL.\ \} \\
& v \cap Q \cap \overline{PL} \cup v \cap PY \cap P \triangleright v \\
= & \qquad \{\ \text{Théorème 2.21(36) et } Q \subseteq \overline{PL}.\ \} \\
& v \cap Q \cup (v \cap P \cap P \triangleright v)Y
\end{array}
$$

Donc, Y est un point fixe de $g(X) := v \cap Q \cup (v \cap P \cap P \triangleright v)X$ Par symétrie, Y' est aussi un point fixe de g. Par hypothèse, $v \cap P$ est progressivement finie, donc, par la proposition 2.54(h), $v \cap P \cap P \triangleright v$ est aussi progressivement finie. Par le théorème 2.56 nous concluons que g a un point fixe unique, c'est-à-dire $Y = Y'$. ∎

La section suivante présente la généralisation de la règle de Mills annoncée au début du chapitre.

4.2.2 Règle de vérification de boucles non déterministes

Tchier et Desharnais [89] ont donné une caractérisation, dans un contexte non déterminste, du plus grand point fixe W (par rapport à $\sqsubseteq$) de w_d (abréviation 4.7). Ils ont montré qu'il est uniquement caractérisé par les conditions (a) et (b) du théorème suivant, c'est-à-dire que W est un point fixe de w_d et que toutes les exécutions en un point du domaine de W sont finies (pas de boucle infinie à partir de ce point-là). Sekerinski [83] a aussi montré une partie de ce théorème (la direction $\Leftarrow$).

(4.14) **Théorème.** *Une relation W est le plus grand point fixe, par rapport à $\sqsubseteq$, de la fonction w_d (abréviation 4.7) ssi les conditions suivantes sont vérifiées :*

$$
\begin{array}{ll}
(a) & W = w_d(W), \\
(b) & WL \subseteq \mathcal{B}(P).
\end{array}
$$

Démonstration.

($\Rightarrow$) : Comme W est un point fixe de w_d alors, (a) est vérifié. Par le théorème 4.12, $WL = \mathcal{A}(P,Q) \cap \mathcal{B}(P)$, donc (b) est évident.

($\Leftarrow$) : Par l'hypothèse (a), W est un point fixe de w_d. Donc, par le théorème 4.10, $\mathcal{A}(P,Q) \cap \mathcal{B}(P) \subseteq WL \subseteq \mathcal{A}(P,Q)$. Mais, par l'hypothèse (b), $WL \subseteq \mathcal{B}(P)$, donc $\mathcal{A}(P,Q) \cap \mathcal{B}(P) \subseteq WL \subseteq \mathcal{A}(P,Q) \cap \mathcal{B}(P)$, c'est-à-dire $WL = \mathcal{A}(P,Q) \cap \mathcal{B}(P)$, d'où $WL \cap P = \mathcal{A}(P,Q) \cap \mathcal{B}(P) \cap P$; par la proposition 2.54(i,h), $WL \cap P$ est donc

progressivement finie. Soit W' le plus grand point fixe (par rapport à $\sqsubseteq$) de w_d ; par le théorème 4.12, $W'L = \mathcal{A}(P,Q) \cap \mathcal{B}(P) = WL$. Donc, par le lemme 4.13, $W = W'$. ∎

Ce théorème peut être utilisé pour vérifier si la relation R de l'exemple 4.3 est la sémantique de la boucle du même exemple. Comme B est une fonction, il en est de même de gB, donc $(gB) \triangledown R = gBR$ (voir 3.9(a)), ce qui implique que $g^\sim \cup (gB) \triangledown R = g^\sim \cup gBR$, c'est-à-dire $f_d(R) = f_a(R) = R$ (comme nous avons montré dans l'exemple 4.3) ; donc la condition (a) est vérifiée (remarque 4.8).

Pour la condition (b), nous donnons un argument informel semblable à celui qui a été donné dans l'exemple 4.3. Comme il n'y a aucune suite infinie par gB (en répétant l'application de gB l'entier naturel b se réduit à 0, et aucun état de la forme $(a, 0, c)$ n'est dans le domaine de gB), gB est progressivement finie, c'est-à-dire $\mathcal{B}(gB) = L$; ce qui implique $RL \subseteq L = \mathcal{B}(gB) = \mathcal{B}(P)$ (remarque 4.8). Cet argument informel pourrait être formalisé. ∎

L'exemple suivant est simple, mais il illustre bien les différents cas qui peuvent survenir lors d'une exécution d'un programme non déterministe [27, 89].

(4.15) **Exemple.** Considérons la boucle suivante où l'unique variable `n` appartient à l'ensemble **Z** des entiers.

```
do n > 0 → if  n = 1 → n := 1   ▯  n = 1 → n := ⇔3
           ▯  n = 3 → n := 2   ▯  n = 3 → n := ⇔1
           ▯  n ≥ 4 → n := ⇔4
           fi
od
```

- Remarquons que tous les entiers $n > 0$ tels que $n \bmod 4 = 1$ peuvent conduire à la terminaison avec un état final $n' = \Leftrightarrow 3$, mais peuvent aussi conduire à une boucle infinie à travers l'état $n = 1$; donc ces valeurs de n n'appartiennent pas au domaine de la relation W donnant la sémantique de la boucle.

- Remarquons aussi que tous les entiers $n > 0$ tels que $n \bmod 4 = 3$ peuvent conduire à la terminaison avec un état final $n' = \Leftrightarrow 1$, mais aussi à la valeur $n = 2$, pour laquelle le corps de boucle n'est pas défini (par la sémantique de **if fi** 3.17) ; ces entiers naturels n ne peuvent pas appartenir au domaine de W. Puisqu'ils mènent aussi à $n = 2$, tous les entiers $n > 0$ tels que $n \bmod 4 = 2$ n'appartiennent pas au domaine de W.

En utilisant la notion de sémantique définie dans le chapitre 3, nous avons les résultats suivants.

- La sémantique de la condition de boucle est

(4.16) $g = \{n > 0 \wedge n' = n\} \quad (g^\sim = \{n \leq 0 \wedge n' = n\})$.

- La sémantique du corps de boucle est :

$$\begin{aligned}(4.17)\quad B = \;& \{n = 1 \wedge n' = n\} \triangleright (\{n' = 1\} \sqcup \{n' = \Leftrightarrow 3\}) \\ & \sqcap \{n = 3 \wedge n' = n\} \triangleright (\{n' = 2\} \sqcup \{n' = \Leftrightarrow 1\}) \\ & \sqcap \{n \geq 4 \wedge n' = n\} \triangleright \{n' = n \Leftrightarrow 4\}.\end{aligned}$$

En appliquant les propriétés 3.8(f) et 3.9(a), cette expression peut être simplifiée comme suit :

$$\begin{aligned}(4.18)\quad B = \;& (\{n = 1 \wedge n' = 1\} \sqcup \{n = 1 \wedge n' = \Leftrightarrow 3\}) \\ & \sqcap (\{n = 3 \wedge n' = 2\} \sqcup \{n = 3 \wedge n' = \Leftrightarrow 1\}) \\ & \sqcap \{n \geq 4 \ \wedge n' = n \Leftrightarrow 4\}).\end{aligned}$$

De même, en utilisant les lois 3.8(f) et 3.9(a,b), il est facile de voir que $g \triangleright B = gB = B$. Montrons maintenant que

$$(4.19)\quad W := \{n \leq 0 \wedge n' = n \vee n > 0 \wedge n \bmod 4 = 0 \wedge n' = 0\}$$

est l'abstraction (sémantique) de la boucle. Par 3.9(e), W est égale à :

$$W = \{n \leq 0 \wedge n' = n\} \sqcap \{n > 0 \wedge n \bmod 4 = 0 \wedge n' = 0\}.$$

Nous devons vérifier que W satisfait les conditions (a) et (b) du théorème 4.14, c'est-à-dire $w_d(W) = W$ et $WL \subseteq \mathcal{B}(gB)$ (remarque 4.8).

Notons que

$$(4.20)\quad W = g^{\sim} \sqcap \{n > 0 \wedge n \bmod 4 = 0 \wedge n' = 0\}.$$

Donc, pour montrer (a), il suffit de prouver que

$$(4.21)\quad B \triangleright W = \{n > 0 \wedge n \bmod 4 = 0 \wedge n' = 0\},$$

étant donné que

$$\begin{aligned}& B \triangleright W = \{n > 0 \wedge n \bmod 4 = 0 \wedge n' = 0\} \\ \Rightarrow \quad & \{\ B = g \triangleright B.\ \} \\ & g^{\sim} \sqcap g \triangleright B \triangleright W = g^{\sim} \sqcap \{n > 0 \wedge n \bmod 4 = 0 \wedge n' = 0\} \\ \Rightarrow \quad & \{\ \text{Équations 3.9(e), abréviation 4.7 avec } P := gB \text{ et } Q := g^{\sim}, \text{ et équation 4.20.}\ \} \\ & w_d(W) = W\end{aligned}$$

Montrons donc l'équation 4.21.

$$\begin{aligned}& B \triangleright W \\ = \quad & \{\ \text{Équations 4.18.}\ \} \\ & (\{n = 1 \wedge n' = 1\} \sqcup \{n = 1 \wedge n' = \Leftrightarrow 3\}) \\ & \sqcap (\{n = 3 \wedge n' = 2\} \sqcup \{n = 3 \wedge n' = \Leftrightarrow 1\})\end{aligned}$$

$$
\begin{array}{ll}
& \sqcap \{n \geq 4 \wedge n' = n \Leftrightarrow 4\}) \triangleleft W \\
= & \qquad \{ \text{ Proposition 3.9(d,e). } \} \\
& (\{n = 1 \wedge n' = 1\} \sqcup \{n = 1 \wedge n' = \Leftrightarrow 3\}) \triangleleft W \\
& \sqcap (\{n = 3 \wedge n' = 2\} \sqcup \{n = 3 \wedge n' = \Leftrightarrow 1\}) \triangleleft W \\
& \sqcap \{n \geq 4 \wedge n' = n \Leftrightarrow 4\} \triangleleft W \\
= & \qquad \{ \triangleleft \text{ se distribue sur } \sqcup. \} \\
& (\{n = 1 \wedge n' = 1\} \triangleleft W \sqcup \{n = 1 \wedge n' = \Leftrightarrow 3\} \triangleleft W) \\
& \sqcap (\{n = 3 \wedge n' = 2\} \triangleleft W \sqcup \{n = 3 \wedge n' = \Leftrightarrow 1\} \triangleleft W) \\
& \sqcap \{n \geq 4 \wedge n' = n \Leftrightarrow 4\} \triangleleft W \\
= & \qquad \{ \text{ Proposition 3.9(a) et expression de } W. \} \\
& (\emptyset \sqcup \{n = 1 \wedge n' = \Leftrightarrow 3\}) \sqcap (\emptyset \sqcup \{n = 3 \wedge n' = \Leftrightarrow 1\}) \\
& \sqcap \{n > 0 \wedge n \bmod 4 = 0 \wedge n' = 0\} \\
= & \qquad \{ \emptyset \text{ est le supremum du demi-treillis démoniaque. } \} \\
& \emptyset \sqcap \emptyset \sqcap \{n > 0 \wedge n \bmod 4 = 0 \wedge n' = 0\} \\
= & \qquad \{ \emptyset \text{ est le supremum du demi-treillis démoniaque. } \} \\
& \{n > 0 \wedge n \bmod 4 = 0 \wedge n' = 0\}
\end{array}
$$

Ceci montre la partie (a) du théorème. La partie (b) peut être établie informellement en remarquant que le domaine de W est

$$\{n \leq 0 \vee n \bmod 4 = 0\}, \tag{4.22}$$

et qu'il n'existe aucune suite infinie par gB pour tout n dans le domaine de la relation W ; en d'autres termes, $WL \subseteq \mathcal{B}(gB)$.

Une méthode intéressante pour prouver que $WL \subseteq \mathcal{B}(gB)$ est de calculer $\mathcal{B}(gB)$. Mais, étant donné que $\mathcal{B}(gB)$ caractérise le domaine de terminaison garantie de la boucle associée, il n'existe aucune méthode systématique pour calculer cette partie initiale (ceci permettrait de résoudre le problème de l'arrêt). Pour démontrer la terminaison de la boucle à partir de chaque état du domaine de W, les démonstrations classiques basées sur les fonctions variantes ou les ensembles bien fondés peuvent être données. Mais des arguments formels basés sur la définition de la partie initiale (sous-section 2.3.6) peuvent être aussi utilisés.

Nous utilisons l'un de ces arguments. Pour $k \geq 0$, soit $v_k := \{n \leq 0 \vee n \leq 4k \wedge n \bmod 4 = 0\}$. Aussi, soit $h(X) := gB \triangleright X$.

Nous pouvons vérifier facilement que le domaine de W (équation 4.22) est égal à $\bigcup_{k \geq 0} v_k$.

Montrons brièvement par induction que pour tout $k \geq 0$, $v_k \subseteq h^{k+1}(\emptyset)$, où, comme d'habitude, $h^0(X) := X$ et $h^{k+1}(X) := h(h^k(X))$.

Pour $k = 0$, $v_0 = \{n \leq 0\}$ et $h(\emptyset) = \overline{gBL}$. Remarquons que $v_0 = \overline{gL}$ (voir 4.16), ce qui implique que $v_0 \subseteq h(\emptyset)$ (car $\overline{gL} \subseteq \overline{gBL}$). Maintenant, supposons que $v_k \subseteq h^{k+1}(\emptyset)$; par (2.45(n)), $gB \triangleright v_k \subseteq gB \triangleright h^{k+1}(\emptyset)$. En calculant $B\overline{v_k}$, nous trouvons que $B\overline{v_k} \subseteq \overline{v_{k+1}}$. Comme $B = gB$, alors $gB\overline{v_k} \subseteq \overline{v_{k+1}}$, qui est équivalent à $v_{k+1} \subseteq gB \triangleright v_k$ (complémentation

et 2.44). En utilisant la définition de la fonction h, nous obtenons $v_{k+1} \subseteq h^{k+2}(\emptyset)$. Donc, pour tout $k \geq 0$, $v_k \subseteq h^{k+1}(\emptyset)$.

En utilisant des lois de la théorie des treillis [20], nous avons :

$$
\begin{array}{ll}
 & WL \\
= & \bigcup_{k\geq 0} v_k \\
\subseteq & \qquad \{\ v_k \subseteq h^{k+1}(\emptyset).\ \} \\
 & \bigcup_{k\geq 0} h^{k+1}(\emptyset) \\
\subseteq & \qquad \{\ \text{Loi booléenne.}\ \} \\
 & \bigcup_{k\geq 0} h^{k}(\emptyset) \\
\subseteq & \qquad \{\ h \text{ monotone et propriété du plus petit point fixe (voir [20]).}\ \} \\
 & \bigcap\{X \mid h(X) = X\} \\
= & \qquad \{\ \text{Définition 2.50 et } h(X) = gB \triangleright X.\ \} \\
 & \mathcal{B}(gB)
\end{array}
$$

■

4.3 Conclusion

Dans ce chapitre nous avons présenté une règle de vérification de boucles non déterministes, qui est une généralisation d'un théorème de Mills connu sous le nom de *règle de vérification de boucle de Mills* [63, 64], ainsi que des exemples pour illustrer l'utilisation de ce théorème. Le théorème que nous venons de prouver est très utile dans plusieurs domaines ; pour la vérification des programmes, si nous avons une condition de boucle et un corps de boucle, le théorème 4.14 nous aide à vérifier si une relation quelconque W est effectivement la sémantique de la boucle en question. Dans le contexte de la construction de programme, le théorème est aussi utile : si nous avons une spécification (relation) W d'une boucle, nous pouvons trouver intuitivement les abstractions g et B de la condition de boucle et du corps de boucle et utiliser le théorème 4.14 pour vérifier si ce choix de g et B est correct. Dans les chapitres suivants, ce théorème va nous servir généralement pour vérifier si une relation donnée est le plus grand point fixe d'une fonction f qui a la forme $f(X) := Q \cup P \triangleright X$ avec $PL \cap QL = \emptyset$.

Chapitre 5

Diagrammes élémentaires

Dans ce chapitre nous définissons d'abord les *diagrammes* et nous donnons une description informelle de leur exécution. Le but de cette description informelle est de fournir des indices qui aident à saisir l'intuition qui se cache derrière les définitions formelles. En partant de ces notions, nous montrons que nous pouvons extraire de ces diagrammes une relation binaire d'entrée/sortie en considérant leur pire exécution, c'est-à-dire en supposant que s'il y a possibilité que le diagramme ne termine pas normalement, alors il ne termine pas normalement ; c'est la *relation d'entrée/sortie démoniaque*. Dans la section 5.1, nous distinguons deux types de diagrammes ; les diagrammes *élémentaires* et les diagrammes *composés*. Dans la sous-section 5.1.2, nous donnons formellement les expressions relationnelles qui décrivent la *terminaison normale*, la *terminaison anormale* et les *boucles infinies* d'un diagramme. Dans la section 5.2, nous donnons une définition formelle de la relation d'entrée/sortie démoniaque d'un diagramme. Cette définition regroupe plusieurs types de diagrammes (*diagramme atomique*, *diagramme de séquence*, *diagramme de choix*, *diagramme de boucle* et les *diagrammes composés*). Dans la section 5.3, nous appliquons notre définition pour calculer la relation d'entrée/sortie des diagrammes élémentaires. Les diagrammes composés seront traités dans le chapitre suivant.

5.1 Diagrammes relationnels

Les graphes sont souvent utilisés pour représenter les programmes et les machines de Turing [15]. Ces graphes sont généralement composés de sommets connectés par des arcs orientés. Les sommets représentent les points de contrôle et les arcs représentent les changements d'état. Plusieurs travaux ont utilisé les graphes [35, 38, 46, 74, 75], où ils sont introduits et définis pour des objectifs différents en connection avec la description des algorithmes et des programmes considérés. Dans un formalisme relationnel, un graphe est basé sur des concepts relationnels : une relation de représentation du graphe, un ensemble de sommets, un sommet initial et un sommet final. En utilisant une approche semblable à celle que nous venons de décrire, nous définissons un *diagramme* comme étant un quadruplet formé d'une relation, d'un ensemble d'identités partielles deux à deux disjointes, qui ont un rôle semblable à celui des sommets dans un graphe et aussi de deux identités partielles particulières qui caractérisent l'entrée et la sortie du diagramme. Notre

approche est semblable à celle de Schmidt et Ströhlein [78], qui définissent un programme relationnel comme étant un quintuplet formé d'un graphe de situation, un graphe de contrôle, un homomorphisme relationnel, une relation d'entrée et une relation de sortie (pour plus de détails voir le chapitre 10 dans [78]). Schmidt et Ströhlein ont utilisé ces notions pour traiter la correction totale et la correction partielle des programmes. Dans ce qui suit, nous donnons la définition formelle d'un *diagramme*.

(5.1) **Définition.** Soit $\mathcal{R}$ une algèbre de relations homogène complète. Un quadruplet $\mathcal{P} = (P, C, e, s)$ est un *diagramme* sur $\mathcal{R}$ si

- P est une relation de $\mathcal{R}$, appelée la *relation associée* au diagramme $\mathcal{P}$,
- C un ensemble dont les éléments sont des identités partielles (définition 2.23(f)) deux à deux disjointes, vérifiant la condition $(\bigcup C)P(\bigcup C) = P$,
- e et s sont des identités partielles ($e, s \in C$) appelées respectivement la *relation d'entrée* et la *relation de sortie* du diagramme $\mathcal{P}$. ∎

Bien que nous ne nous servons pas des matrices et des graphes dans notre traitement formel (déjà utilisés dans nos travaux antérieurs [28, 90]), nous les utilisons dans nos explications informelles et intuitives. L'usage des matrices et des graphes justifie bien le terme *diagramme*.

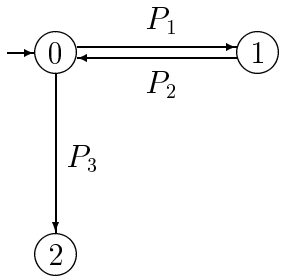
Donnons un exemple qui illustre cette définition.

(5.2) **Exemple.** Considérons la boucle :

$$\textbf{do } \mathtt{n} > 0 \to \mathtt{n} := \mathtt{n} \Leftrightarrow 100 \textbf{ od},$$

où n prend ses valeurs sur l'ensemble des naturels $\mathbf{N}$, qui est l'ensemble des états.

En suivant une approche semblable à celle de Schmidt et Ströhlein [78], ce programme peut être représenté par le graphe suivant :



Le sommet 0 est le point d'entrée et le sommet 2 est le point de sortie. Chaque arc est étiqueté par une relation sur $\{0, 1, 2\} \times \mathbf{N}$ calculée par le programme entre les sommets reliés par cet arc. Ces relations sont :

- $P_1 = \{((0, n), (1, n')) \mid n > 0 \wedge n' = n\}$,

- $P_2 := \{((1,n),(0,n')) \mid n \in \mathbf{N} \wedge n' = n \Leftrightarrow 100\}$,
- $P_3 = \{((0,n),(2,n')) \mid n \leq 0 \wedge n' = n\}$.

Par exemple, la relation sur $\{0,1,2\} \times \mathbf{N}$ calculée par le corps de boucle entre les points 1 et 0 est P_2.

La matrice de représentation de ce graphe est :

$$P_M = \begin{array}{c} \\ 0 \\ 1 \\ 2 \end{array} \begin{array}{c} \begin{array}{ccc} 0 & 1 & 2 \end{array} \\ \begin{pmatrix} \emptyset & P_1 & P_3 \\ P_2 & \emptyset & \emptyset \\ \emptyset & \emptyset & \emptyset \end{pmatrix} \end{array}$$

Nous donnons les relations caractérisant notre diagramme $\mathcal{P} = (P, C, e, s)$.

- La relation associée à ce diagramme est $P = P_1 \cup P_2 \cup P_3$. Donc, P est une relation de type $\{0,1,2\} \times \mathbf{N} \leftrightarrow \{0,1,2\} \times \mathbf{N}$.
- $C = \{e, a, s\}$ où $e = \{((0,n),(0,n')) \mid n' = n\}$, $a = \{((1,n),(1,n')) \mid n' = n\}$ et $s = \{((2,n),(2,n')) \mid n' = n\}$.
- On peut facilement vérifier que e, a, s sont de type $\{0,1,2\} \times \mathbf{N} \leftrightarrow \{0,1,2\} \times \mathbf{N}$, qu'elles sont des identités partielles deux à deux disjointes et qu'elles vérifient $(e \cup a \cup s)P(e \cup a \cup s) = P$. ∎

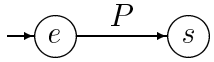
5.1.1 Différents types de diagrammes

Dans notre traitement, nous distinguons deux types de diagrammes ; les diagrammes *élémentaires* et les diagrammes *composés*. Dans cette section, nous allons les définir.

Pour étiqueter le sommet initial et le sommet final d'un graphe, nous utiliserons les lettres e et s plutôt que des entiers naturels comme à l'exemple précédent.

(5.3) **Définition.** Un diagramme $\mathcal{P} = (P, C, e, s)$ est dit *atomique* si $P = ePs$. ∎

Le graphe et la relation associés à ce diagramme sont :



et

$$P = \begin{array}{c} \\ e \\ s \end{array} \begin{array}{c} \begin{array}{cc} e & s \end{array} \\ \begin{pmatrix} \emptyset & P \\ \emptyset & \emptyset \end{pmatrix} \end{array}.$$

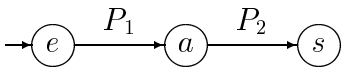
Un diagramme atomique consiste en une seule étape atomique (ne peut pas être décomposée), c'est-à-dire que la transition entre le point d'entrée et le point de sortie se fait en une seule étape (il y a une seule entrée différente de $\emptyset$ dans la matrice). Le diagramme de l'exemple (5.2) n'est pas atomique.

(5.4) **Définition.** Un diagramme $\mathcal{P} = (P, C, e, s)$ est un *diagramme de séquence* si

$$P = P_1 \cup P_2, \quad \{e, a, s\} \subseteq C, \quad P_1 = eP_1a \quad \text{et} \quad P_2 = aP_2s.$$

■

Ce diagramme peut être représenté par le graphe et la matrice suivants :

(5.5) 

et $P = \begin{array}{c} \\ e \\ a \\ s \end{array} \begin{array}{c} \begin{array}{ccc} e & a & s \end{array} \\ \begin{pmatrix} \emptyset & P_1 & \emptyset \\ \emptyset & \emptyset & P_2 \\ \emptyset & \emptyset & \emptyset \end{pmatrix} \end{array}$.

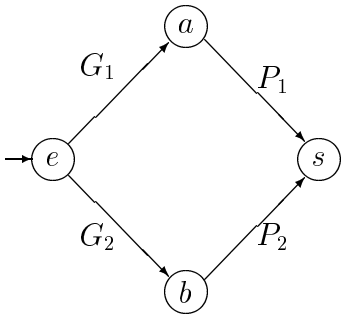
Le graphe ainsi que la matrice illustrent bien l'usage du terme « séquence ». Remarquons qu'un diagramme de séquence est la séquence de deux diagrammes atomiques tels que la relation de sortie du premier est égale à la relation d'entrée du deuxième.

(5.6) **Définition.** Un diagramme $\mathcal{P} = (P, C, e, s)$ est un *diagramme de choix* si

$$P = G_1 \cup P_1 \cup G_2 \cup P_2, \quad \{e, a, b, s\} \subseteq C, \quad G_1 = eG_1a, \quad P_1 = aP_1s,$$
$$G_2 = eG_2b \text{ et } P_2 = bP_2s.$$

■

Le graphe et la relation associés à ce diagramme sont :

(5.7) 

et $P = \begin{array}{c} \\ e \\ a \\ b \\ s \end{array} \begin{array}{c} \begin{array}{cccc} e & a & b & s \end{array} \\ \begin{pmatrix} \emptyset & G_1 & G_2 & \emptyset \\ \emptyset & \emptyset & \emptyset & P_1 \\ \emptyset & \emptyset & \emptyset & P_2 \\ \emptyset & \emptyset & \emptyset & \emptyset \end{pmatrix} \end{array}$.

Dans un diagramme de choix, le calcul entre le point d'entrée et le point de sortie est fait d'une façon non déterministe en deux branches différentes et chacune d'elles est constituée de deux étapes atomiques. Notons que si $G_2 = P_2 = b = \emptyset$ (ou le cas symétrique), alors $\mathcal{P}$ se transforme en un diagramme de séquence.

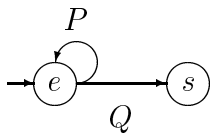
(5.8) **Définition.** Un diagramme $\mathcal{W} = (W, C, e, s)$ est un *diagramme de boucle* si

$$W = P \cup Q, \quad P = ePe, \quad Q = eQs \quad \text{et} \quad PL \cap QL = \emptyset.$$

■

Dans un diagramme de boucle, P est appliquée jusqu'à ce que Q puisse être appliquée.

Le graphe et la matrice représentant le diagramme de boucle $\mathcal{P}$ sont :

(5.9) 

et $P = \begin{array}{c} \\ e \\ s \end{array} \begin{array}{c} \begin{array}{cc} e & s \end{array} \\ \begin{pmatrix} P & Q \\ \emptyset & \emptyset \end{pmatrix} \end{array}$.

(5.10) **Définition.** Un diagramme est dit *élémentaire* s'il est un diagramme atomique ou un diagramme de séquence, de choix ou de boucle. Un diagramme est dit *composé* s'il n'est pas élémentaire. ∎

5.1.2 Exécution d'un diagramme

Nous allons décrire l'*exécution d'un diagramme* en un état et par la suite nous donnons quelques notions liées à cette exécution, soit la *terminaison normale*, la *terminaison anormale* et les *boucles infinies*. Soit $\mathcal{P} = (P, C, e, s)$ un diagramme, où P, e et s sont de type $S \leftrightarrow S$ où S est un ensemble quelconque. Soit i un élément dans le domaine de e (c'est-à-dire $(i, i) \in e$). Nous allons décrire une exécution du diagramme $\mathcal{P}$ en i. Le but de cette notion d'exécution est de fournir des indices qui aident à saisir l'intuition qui se cache derrière les définitions formelles subséquentes.

- On applique la relation P à i itérativement (on itère P), jusqu'à ce qu'on aboutisse à un état i' qui n'est pas dans le domaine de P (si P est non déterministe alors on fait un choix non déterministe), c'est-à dire (i, i') appartient à la postrestriction de la relation P^* à $\overline{PL}$, d'où $(i, i') \in e(P^* \cap \overline{PL}^{\sim})$. Si i' est un état final, c'est-à-dire $(i', i') \in s$, ce qui implique que $(i, i') \in e(P^* \cap \overline{PL}^{\sim})s$, nous disons alors que l'exécution du diagramme se *termine normalement*. Ce qui correspond à une *exécution angélique* du diagramme $\mathcal{P}$ en i.

- Si P est non déterministe, i peut avoir plusieurs images par le terme $e(P^* \cap \overline{PL}^{\sim})$. S'il existe parmi ces images un état qui conduit en dehors des points de sortie $(i \in e(P^* \cap \overline{PL}^{\sim})\overline{sL})$, i n'est alors pas considéré. On dit que le diagramme *termine anormalement*.

- Si on applique P à i (on itère P) et s'il existe un chemin infini à partir de i, on dit alors qu'il y a une boucle infinie d'origine i.

Les deux derniers cas correspondent à une *exécution démoniaque* du diagramme $\mathcal{P}$ en i.

Donnons les expressions relationnelles qui formalisent les cas précédents (terminaison normale, terminaison anormale et boucle infinie). Ces notions sont tirées de [78].

(5.11) **Définition.** Soit un diagramme $\mathcal{P} = (P, C, e, s)$. Nous appelons

(a) P^* l'*action*,
(b) $T := P^* \cap \overline{PL}^{\sim}$ l'*action de terminaison*,
(c) $E := eTs$ l'*effet*.

∎

- L'action d'un diagramme est la relation joignant un état initial i avec tous ceux qui peuvent apparaître dans une suite de calculs débutant en i.
- L'action de terminaison est la relation joignant deux états i, i' tels qu'il y a un chemin de i à i' (le terme P^* dans T) et que i' ne peut être traité par le diagramme (le terme $\overline{PL}^\smile$ dans T).
- L'effet du diagramme est la relation entre les états initiaux et les états finaux, sans tenir compte du chemin suivi.

Comme un diagramme est caractérisé par des notions relationnelles, il arrive que la relation associée au diagramme soit déterministe. Dans ce qui suit, nous donnons la définition de diagramme *déterministe* ainsi que celle de *sous-diagramme*.

(5.12) **Définition.**

- Un diagramme $\mathcal{P} = (P, C, e, s)$ est dit *déterministe* ssi P est déterministe.
- Un diagramme $\mathcal{P}_1 = (P_1, C, e_1, s_1)$ est un *sous-diagramme* du diagramme $\mathcal{P} = (P, C, e, s)$ ssi $P_1 \subseteq P$. ∎

Un sous-diagramme est un diagramme dont la relation associée est incluse dans celle du diagramme principal. Durant l'exécution du diagramme principal, le sous-diagramme est aussi exécuté. Le contrôle entre par le point d'entrée e_1 à $\mathcal{P}_1$ et sort par s_1. Le diagramme $\mathcal{P}_1$ ne communique aucune information au diagramme $\mathcal{P}$ par l'intermédiaire des points internes du diagramme $\mathcal{P}_1$.

Il arrive qu'on ait $s \subseteq \overline{PL}$, ce qui permet de simplifier l'expression de l'effet. On dit dans ce cas que s est terminal. C'est le cas des différents types de diagrammes présentés jusqu'ici. Si la relation associée à un diagramme est déterministe, alors l'effet de ce diagramme l'est aussi, comme le montre la proposition suivante.

(5.13) **Proposition.** *Soit $\mathcal{P} = (P, C, e, s)$ un diagramme et E l'effet de ce diagramme. Nous avons [78] :*

$$\begin{array}{lllll} (a) & s \subseteq \overline{PL} & \Rightarrow & E = eP^*s, \\ (b) & \mathcal{P} \textit{ déterministe} & \Rightarrow & E \textit{ déterministe.} \end{array}$$

Démonstration.

$$\begin{array}{ll} (a) & E \\ = & \quad \{ \text{ Définition 5.11(c). } \} \\ & eTs \\ = & \quad \{ \text{ Définition 5.11(b). } \} \\ & e(P^* \cap \overline{PL}^\smile)s \\ = & \quad \{ \text{ Théorème 2.21(37). } \} \\ & eP^*(s \cap \overline{PL}) \\ = & \quad \{ \text{ Hypothèse } s \subseteq \overline{PL}. \} \\ & eP^*s \end{array}$$

(b) $E^{\smile}E$

$=$ { Définition 5.11(c), théorème 2.21(24) et $R \subseteq I \Rightarrow R^{\smile} = R$. }

$sT^{\smile}eeTs$

$\subseteq$ { $e \subseteq I$, $s \subseteq I$ et (;) monotone. }

$T^{\smile}T$

$=$ { Définition 5.11(b) et théorème 2.21(23,25). }

$(P^{*\smile} \cap \overline{PL})(P^* \cap \overline{PL}^{\smile})$

$=$ { Théorème 2.21(36). }

$P^{*\smile}P^* \cap \overline{PL}^{\smile} \cap \overline{PL}$

$\subseteq$ { Proposition 2.4.2.(ii) dans [78] : si P est déterministe alors $P^{*\smile}P^* = P^{*\smile} \cup P^*$. Aussi $P^* = I \cup P^+ \subseteq I \cup PL$ et $P^{*\smile} \subseteq I \cup (PL)^{\smile}$. }

$(I \cup (PL)^{\smile} \cup PL) \cap \overline{PL}^{\smile} \cap \overline{PL}$

$\subseteq$ { Lois booléennes. }

I

∎

Nous partons de ces notions pour définir la *relation d'entrée/sortie démoniaque* d'un diagramme.

5.2 Relation d'entrée/sortie démoniaque

Nous avons vu dans la section 5.1.2 que lors d'une exécution d'un diagramme en un état initial, trois cas peuvent survenir : la terminaison normale, la terminaison anormale et les boucles infinies. Comme notre but est de définir formellement la relation d'entrée/sortie d'un diagramme en supposant sa pire exécution, nous devons tenir compte de ces trois cas en même temps. Donnons d'abord les expressions relationnelles qui formalisent respectivement ces notions : la terminaison normale, la terminaison anormale et les boucles infinies. Soit

$$\mathcal{P} = (P, C, e, s)$$

un diagramme.

(a) Le terme $e(P^* \cap \overline{PL}^{\smile})s$ est la relation joignant deux états i, i' tels que i' ne peut être traité par le diagramme (le terme $\overline{PL}^{\smile}$), il y a un chemin de i à i' (le terme P^*) et i' est un point de sortie. Donc, le terme eTs (définition 5.11(b,c)) représente l'ensemble des exécutions débutant au point d'entrée (e) et menant aux points de sortie (s). C'est ce que nous appelons la *relation d'entrée/sortie angélique* du diagramme $\mathcal{P}$ ou l'effet du diagramme (s'il y a possibilité que l'exécution du diagramme se termine, alors la terminaison est garantie).

(b) Nous avons vu au début de la sous-section 5.1.2 que le vecteur $(P^* \cap \overline{PL}^{\smile})\overline{sL}$ représente l'ensemble des états à partir desquels l'exécution peut se terminer en dehors des points de sortie. En utilisant les propriétés 2.21(37,2), ce vecteur

est égal à $P^*\overline{PL \cup sL}$. En considérant le complément de ce vecteur et l'abréviation 4.7, on voit que le vecteur $e\mathcal{A}(P,s)$ représente l'ensemble des états initiaux à partir desquels l'exécution ne peut mener à une terminaison anormale. En utilisant l'expression $T = P^* \cap \overline{PL}^{\smile}$ (5.11(b)) et l'abréviation 4.7, on obtient $e\mathcal{A}(P,s) = e(T \triangleright sL)$. Indice mnémonique : maintenant nous sommes en mesure de justifier notre choix du symbole $\mathcal{A}$ (abréviation 4.7) ; $\mathcal{A}$ pour *a*normale, car ce vecteur représente les états à partir desquels aucune terminaison anormale n'est possible.

(c) Nous avons vu (définition 2.48) que le terme qui traite les boucles infinies est la partie initiale. Le vecteur $e\mathcal{B}(P)$ élimine les états initiaux qui peuvent mener à une boucle infinie, c'est-à-dire que le domaine de $e\mathcal{B}(P)$ contient des états initiaux qui ne peuvent conduire à une boucle infinie.

Donc, en considérant les trois cas précédents en même temps, nous sommes sûrs que nous avons considéré la pire exécution du diagramme ; s'il y a possibilité que le diagramme ne termine pas normalement, alors il ne termine pas normalement. Le terme $eTs \cap e\mathcal{A}(P,s) \cap e\mathcal{B}(P)$ est appelée la *relation d'entrée/sortie démoniaque* du diagramme $\mathcal{P}$. Il convient de noter que, même si Schmidt et Ströhlein n'ont pas défini cette relation, c'était assez naturel de le faire à partir des concepts présentés dans leur livre [78].

Par la suite, sauf avis contraire, l'expression « relation d'entrée/sortie » désigne la relation d'entrée/sortie démoniaque. Nous allons traiter l'arc concernant la fonction $\mathcal{E}$ dans la figure 1.1.

Nous nous restreignons aux mêmes hypothèses que celles du chapitre 3, c'est-à-dire que nous considérons une algèbre concrète complète de la forme $\mathrm{Rel}(X)$ (exemple 2.19). La relation d'entrée/sortie d'un diagramme $\mathcal{P}$ est donnée par une relation $\mathcal{E}(\mathcal{P})$ où $\mathcal{E}$ est une fonction de l'ensemble des diagrammes vers cette algèbre de relations, qui associe à chaque diagramme $\mathcal{P}$ la relation $\mathcal{E}(\mathcal{P})$ donnée par :

$$\mathcal{E}(\mathcal{P}) := eTs \cap e(T \triangleright sL) \cap e\mathcal{B}(P), \tag{5.14}$$

avec $T := P^* \cap \overline{PL}^{\smile}$. Cette expression est équivalente à

$$\mathcal{E}(\mathcal{P}) = eTs \cap eT \triangleright sL \cap e\mathcal{B}(P), \tag{5.15}$$

puisque

$$\begin{array}{ll}
 & \mathcal{E}(\mathcal{P}) \\
= & \qquad \{ \text{ Équation 5.14. } \} \\
 & eTs \cap e(T \triangleright sL) \cap e\mathcal{B}(P) \\
= & \qquad \{ \text{ Définition 2.44. } \} \\
 & eTs \cap e\overline{T\overline{sL}} \cap e\mathcal{B}(P) \\
= & \qquad \{ \text{ Théorème 2.27(f) et } e \text{ déterministe. } \} \\
 & eTs \cap eL \cap \overline{eT\overline{sL}} \cap e\mathcal{B}(P) \\
= & \qquad \{ \ eTs \subseteq eL \text{ et définition 2.44. } \} \\
 & eTs \cap eT \triangleright sL \cap e\mathcal{B}(P)
\end{array}$$

L'expression suivante est une expression alternative de $\mathcal{E}(\mathcal{P})$:

$$\mathcal{E}(\mathcal{P}) := e \,▫\, (T \cap \mathcal{B}(P)) \,▫\, s. \tag{5.16}$$

En effet,

$$\begin{aligned}
&\mathcal{E}(\mathcal{P}) \\
=& \quad \{ \text{ Équation 5.14. } \} \\
&eTs \cap e(T \triangleright sL) \cap e\mathcal{B}(P) \\
=& \quad \{ e \text{ déterministe et théorème 2.27(a). } \} \\
&e(Ts \cap T \triangleright sL \cap \mathcal{B}(P)) \\
=& \quad \{ \text{ Définition 3.7 et proposition 3.9(a). } \} \\
&e \,▫\, (T \,▫\, s \cap \mathcal{B}(P)) \\
=& \quad \{ \text{ Lemme 3.10(b) } (\mathcal{B}(P) \text{ est un vecteur par la définition 2.48). } \} \\
&e \,▫\, (T \cap \mathcal{B}(P)) \,▫\, s
\end{aligned}$$

Nous avons également

$$\mathcal{E}(\mathcal{P}) = eP^*(s \cap \overline{PL}) \cap eP^* \triangleright (PL \cup sL) \cap e\mathcal{B}(P), \tag{5.17}$$

comme le montre la démonstration suivante :

$$\begin{aligned}
&\mathcal{E}(\mathcal{P}) \\
=& \quad \{ \text{ Équation 5.15. } \} \\
&eTs \cap eT \triangleright sL \cap e\mathcal{B}(P) \\
=& \quad \{ \text{ Expression de } T \text{ (définition 5.11(b)) et définition 2.44. } \} \\
&e(P^* \cap \overline{PL}^{\smile})s \cap \overline{e(P^* \cap \overline{PL}^{\smile})\overline{sL}} \cap e\mathcal{B}(P) \\
=& \quad \{ \text{ Théorème 2.21(37) et loi de De Morgan. } \} \\
&eP^*(s \cap \overline{PL}) \cap \overline{eP^*\overline{PL \cup sL}} \cap e\mathcal{B}(P) \\
=& \quad \{ \text{ Définition 2.44. } \} \\
&eP^*(s \cap \overline{PL}) \cap eP^* \triangleright (PL \cup sL) \cap e\mathcal{B}(P)
\end{aligned}$$

5.3 Relation d'entrée/sortie des diagrammes

Comme nous considérons des diagrammes dont tous les points de sortie sont terminaux (il n'est pas possible, à partir d'un point de sortie, d'atteindre un autre point en appliquant P), c'est-à-dire

$$s \subseteq \overline{PL},$$

l'équation 5.17 se réduit à :

$$\mathcal{E}(\mathcal{P}) = eP^*s \cap eP^* \triangleright (PL \cup sL) \cap e\mathcal{B}(P). \tag{5.18}$$

Dans cette section, nous utilisons cette forme. Vu l'usage exhaustif des propriétés des identités partielles (théorème 2.29) dans nos calculs, ainsi que le fait que les éléments de l'ensemble C sont deux à deux disjoints, nous omettons parfois de mentionner ces propriétés.

5.3.1 Diagramme atomique

Nous commençons par le calcul de la relation d'entrée/sortie d'un diagramme atomique (5.3) $\mathcal{P}$. Nous rappelons que dans ce cas, nous avons

(5.19) $\mathcal{P} = (P, C, e, s)$ où $P = ePs$.

Montrons d'abord que

(5.20) $eP^* = e \cup P$.

$$
\begin{array}{ll}
& eP^* \\
= & \qquad \{ \text{ Équation 2.34. } \} \\
& e(I \cup P \cup P^2P^*) \\
= & \qquad \{ \text{ (;) se distribue sur } \cup,\ P^2 = \emptyset \text{ (car } P = ePs,\ es = \emptyset) \text{ et } eP = P. \ \} \\
& e \cup P
\end{array}
$$

Vu que (;) se distribue sur ($\cup$), que $es = \emptyset$ et que $Ps = P$, nous obtenons

(5.21) $eP^*s = P$.

Ceci est la relation d'entrée/sortie angélique du diagramme atomique donné ci-dessus.

Calculons maintenant le terme $eP^* \triangleright (PL \cup sL)$. Dans le but de simplifier et de réduire les calculs, nous utilisons la règle de l'égalité indirecte (2.17) et la propriété sur les connections de Galois (2.47) vérifiées par l'opérateur $\triangleright$.

Soit X une relation arbitraire. Alors,

$$
\begin{array}{ll}
& X \subseteq eP^* \triangleright (PL \cup sL) \\
\Leftrightarrow & \qquad \{ \text{ Équation 2.47. } \} \\
& (eP^*)^\smile X \subseteq PL \cup sL \\
\Leftrightarrow & \qquad \{ \text{ Équation 5.20. } \} \\
& (e \cup P)^\smile X \subseteq PL \cup sL \\
\Leftrightarrow & \qquad \{ \text{ Théorème 2.21(11,21) et } P = Ps = eP. \ \} \\
& e^\smile X \cup (Ps)^\smile X \subseteq ePL \cup sL \\
\Leftrightarrow & \qquad \{ \text{ Théorème 2.21(24). } \} \\
& e^\smile X \cup sP^\smile X \subseteq ePL \cup sL \\
\Leftrightarrow & \qquad \{ \text{ Propriété 2.16 et } e^\smile = e. \ \} \\
& e^\smile X \subseteq ePL \quad \wedge \quad sP^\smile X \subseteq sL \\
\Leftrightarrow & \qquad \{ \text{ Équation 2.47, } eP = P \text{ et } sP^\smile X \subseteq sL. \ \} \\
& X \subseteq e \triangleright PL
\end{array}
$$

En appliquant la propriété 2.17, nous concluons que :

(5.22) $eP^* \triangleright (PL \cup sL) = e \triangleright PL$.

Étant donné que le diagramme est atomique et qu'il n'y a pas de boucle, alors P est progressivement finie, c'est-à-dire $\mathcal{B}(P) = L$. Calculons quand même $\mathcal{B}(P)$ afin d'illustrer la méthode.

Il est facile de vérifier que $P^n = \emptyset$ pour $n \geq 2$ (le plus long chemin dans le graphe associé à un diagramme atomique est de longueur 1).

$$
\begin{array}{ll}
& L \\
= & \qquad \{\ P^n = \emptyset \text{ pour } n \geq 2.\ \} \\
& \bigcup_n \overline{P^n} L \\
\subseteq & \qquad \{\ \text{Proposition 2.54(b).}\ \} \\
& \mathcal{B}(P)
\end{array}
$$

d'où

$$e\mathcal{B}(P) = eL. \tag{5.23}$$

En faisant l'intersection des trois termes 5.21, 5.22, 5.23 et en utilisant l'expression de $\mathcal{E}(\mathcal{P})$ (équation 5.18), nous obtenons :

$$
\begin{array}{ll}
& \mathcal{E}(\mathcal{P}) \\
= & \qquad \{\ \text{Équations 5.18, 5.21, 5.22 et 5.23.}\ \} \\
& P \cap e \triangleright PL \cap eL \\
= & \qquad \{\ \text{Définition 2.44, théorème 2.27(f) et } P = eP.\ \} \\
& P \cap PL \\
= & P
\end{array}
$$

Comme l'exécution du diagramme conduit nécessairement à un état de s (car $P = Ps$) et qu'il n' y a pas de boucle infinie, alors la terminaison est garantie. En d'autres termes, il n'est pas surprenant que la relation d'entrée/sortie démoniaque soit égale à la relation d'entrée/sortie angélique qui n'est autre que la relation P. ∎

Dans la sous-section suivante, nous calculons les relations d'entrée/sortie des autres diagrammes élémentaires. Nous débutons par le diagramme de choix et nous montrons par après que la relation d'entrée/sortie d'un diagramme de séquence est un cas particulier de celle du diagramme de choix.

5.3.2 Diagramme de choix

Soit le diagramme de choix (5.6) $\mathcal{P} = (P, C, e, s)$, où

$$P = G_1 \cup P_1 \cup G_2 \cup P_2,\quad \{e, a, b, s\} \subseteq C,\quad G_1 = eG_1a,\quad G_2 = eG_2b,\quad P_1 = aP_1s \text{ et } P_2 = bP_2s. \tag{5.24}$$

En utilisant la distributivité de $(;)$ sur $\cup$, le fait que les identités partielles (a, b, e et s) sont deux à deux disjointes ainsi que l'équation 5.24, il est facile de déduire que

(5.25) $eP = G_1 \cup G_2, \quad P^2 = G_1P_1 \cup G_2P_2, \quad \text{et } P^3 = \emptyset.$

En utilisant ces résultats, montrons que

(5.26) $eP^* = e \cup G_1 \cup G_2 \cup G_1P_1 \cup G_2P_2.$

$$
\begin{array}{ll}
& eP^* \\
= & \qquad \{ \text{ Équation 2.34 et } (;) \text{ se distribue sur } \cup. \} \\
& e \cup eP \cup eP^2 \cup eP^3P^* \\
= & \qquad \{ \text{ Équation 5.25. } \} \\
& e \cup G_1 \cup G_2 \cup G_1P_1 \cup G_2P_2
\end{array}
$$

Calculons la relation d'entrée/sortie angélique du diagramme $\mathcal{P}$, c'est-à-dire l'expression eP^*s.

$$
\begin{array}{ll}
& eP^*s \\
= & \qquad \{ \text{ Équation 5.26. } \} \\
& (e \cup G_1 \cup G_2 \cup G_1P_1 \cup G_2P_2)s \\
= & \qquad \{ (;) \text{ se distribue sur } \cup \text{ et équation 5.24. } \} \\
& es \cup G_1as \cup G_2bs \cup G_1P_1s \cup G_2P_2s \\
= & \qquad \{ \text{ Équation 5.24 } (e, a, s, b \text{ deux à deux disjointes}). \} \\
& G_1P_1 \cup G_2P_2
\end{array}
$$

donc,

(5.27) $eP^*s = G_1P_1 \cup G_2P_2.$

Ceci est la relation d'entrée/sortie angélique d'un diagramme de choix. L'exécution du diagramme se termine en un état si au moins une des deux branches conduit en cet état.

Notre but est de trouver la relation d'entrée/sortie démoniaque $\mathcal{E}(\mathcal{P})$ (équation 5.18) du diagramme $\mathcal{P}$ (équation 5.24).

Calculons maintenant le terme $eP^* \triangleright (PL \cup sL)$. Nous utilisons la règle de l'égalité indirecte (2.17) et la propriété sur les connections de Galois vérifiées par l'opérateur ($\triangleright$) (2.47).

Soit X une relation arbitraire :

$$
\begin{array}{ll}
& X \subseteq eP^* \triangleright (PL \cup sL) \\
\Leftrightarrow & \qquad \{ \text{ Équation 2.47. } \} \\
& (eP^*)^\smile X \subseteq PL \cup sL \\
\Leftrightarrow & \qquad \{ \text{ Équations 5.24 et 5.26. } \} \\
& (e \cup G_1a \cup G_2b \cup G_1P_1s \cup G_2P_2s)^\smile X \subseteq PL \cup sL \\
\Leftrightarrow & \qquad \{ \text{ Théorème 2.21(10,20,24) et équation 5.24. } \}
\end{array}
$$

$$
\begin{array}{ll}
& e^{\smile}X \cup aG_1^{\smile}X \cup bG_2^{\smile}X \cup s(G_1P_1 \cup G_2P_2)^{\smile}X \subseteq eG_1L \cup eG_2L \cup aP_1L \cup bP_2L \cup sL \\
\Leftrightarrow & \quad \{\ e^{\smile} = e, \text{ propriété 2.16 et } s(G_1P_1 \cup G_2P_2)^{\smile}X \subseteq sL.\ \} \\
& e^{\smile}X \subseteq eG_1L \cup eG_2L \ \ \wedge \ \ aG_1^{\smile}X \subseteq aP_1L \ \ \wedge \ \ bG_2^{\smile}X \subseteq bP_2L \\
\Leftrightarrow & \quad \{\ \text{Équation 5.24 et loi booléenne.}\ \} \\
& e^{\smile}X \subseteq G_1L \cup G_2L \ \ \wedge \ \ G_1^{\smile}X \subseteq P_1L \ \ \wedge \ \ G_2^{\smile}X \subseteq P_2L \\
\Leftrightarrow & \quad \{\ \text{Équation 2.47.}\ \} \\
& X \subseteq e \rhd (G_1L \cup G_2L) \ \ \wedge \ \ X \subseteq G_1 \rhd P_1L \ \ \wedge \ \ X \subseteq G_2 \rhd P_2L \\
\Leftrightarrow & \quad \{\ \text{Loi booléenne.}\ \} \\
& X \subseteq e \rhd (G_1L \cup G_2L) \cap G_1 \rhd P_1L \cap G_2 \rhd P_2L
\end{array}
$$

Donc, en utilisant la propriété 2.17, nous obtenons

$$eP^* \rhd (PL \cup sL) = e \rhd (G_1L \cup G_2L) \cap G_1 \rhd P_1L \cap G_2 \rhd P_2L. \tag{5.28}$$

En utilisant le même raisonnement que celui utilisé pour le cas du diagramme atomique, nous obtenons :

$$e\mathcal{B}(P) = eL. \tag{5.29}$$

De ce qui précède, nous pouvons déduire

$$\mathcal{E}(\mathcal{P}) = (G_1P_1 \cup G_2P_2) \cap G_1 \rhd P_1L \cap G_2 \rhd P_2L. \tag{5.30}$$

En effet,

$$
\begin{array}{ll}
& \mathcal{E}(\mathcal{P}) \\
= & \quad \{\ \text{Équations 5.18, 5.27, 5.28 et 5.29.}\ \} \\
& (G_1P_1 \cup G_2P_2) \cap e \rhd (G_1L \cup G_2L) \cap G_1 \rhd P_1L \cap G_2 \rhd P_2L \cap eL \\
= & \quad \{\ \text{Théorème 2.27(f), } eG_1 = G_1 \text{ et } eG_2 = G_2.\ \} \\
& (G_1P_1 \cup G_2P_2) \cap (G_1L \cup G_2L) \cap G_1 \rhd P_1L \cap G_2 \rhd P_2L \\
= & \quad \{\ \text{Lois booléennes et } G_1P_1 \cup G_2P_2 \subseteq G_1L \cup G_2L.\ \} \\
& (G_1P_1 \cup G_2P_2) \cap G_1 \rhd P_1L \cap G_2 \rhd P_2L
\end{array}
$$

Comme le nom l'indique (relation d'entrée/sortie démoniaque), nous souhaitons autant que possible l'usage des opérateurs démoniaques. Donc, l'équation 5.30 devient

$$\mathcal{E}(\mathcal{P}) = G_1 \triangleleft P_1 \cap G_2 \rhd P_2L \cup G_2 \triangleleft P_2 \cap G_1 \rhd P_1L, \tag{5.31}$$

puisque

$$
\begin{array}{ll}
& \mathcal{E}(\mathcal{P}) \\
= & \quad \{\ \text{Équation 5.30.}\ \} \\
& (G_1P_1 \cup G_2P_2) \cap G_1 \rhd P_1L \cap G_2 \rhd P_2L \\
= & \quad \{\ \text{Lois booléennes.}\ \} \\
& G_1P_1 \cap G_1 \rhd P_1L \cap G_2 \rhd P_2L \cup G_2P_2 \cap G_2 \rhd P_2L \cap G_1 \rhd P_1L \\
= & \quad \{\ \text{Définition de } \triangleleft \ (3.7).\ \} \\
& G_1 \triangleleft P_1 \cap G_2 \rhd P_2L \cup G_2 \triangleleft P_2 \cap G_1 \rhd P_1L
\end{array}
$$

■

Dans ce qui suit, nous considérons quelques cas particuliers de cette expression, qui correspondent à ce que nous trouvons dans la pratique.

(5.32) **Proposition.** *Soit le diagramme $\mathcal{P} = (P, C, e, s)$ vérifiant l'équation 5.24.*

(a) Si les domaines des relations G_1 et G_2 sont égaux ($G_1 L = G_2 L$), alors

$$\mathcal{E}(\mathcal{P}) = G_1 \circ P_1 \sqcup G_2 \circ P_2.$$

(b) Si les relations G_1 et G_2 ont des domaines disjoints ($G_1 L \cap G_2 L = \emptyset$), alors

$$\mathcal{E}(\mathcal{P}) = G_1 \circ P_1 \cup G_2 \circ P_2 = G_1 \circ P_1 \sqcap G_2 \circ P_2.$$

(c) Dans le cas où les relations G_1 et G_2 sont déterministes, alors

$$\mathcal{E}(\mathcal{P}) = G_1 P_1 \cap \overline{G_2 L} \cup G_2 P_2 \cap \overline{G_1 L} \cup (G_1 P_1 \sqcup G_2 P_2).$$

(d) Si les relations G_1 et G_2 sont des identités partielles ($G_1 \subseteq I$ et $G_2 \subseteq I$), alors

$$\mathcal{E}(\mathcal{P}) = G_2^{\sim} \circ G_1 \circ P_1 \sqcap G_1^{\sim} \circ G_2 \circ P_2 \sqcap G_1 \circ G_2 \circ (P_1 \sqcup P_2).$$

(e) Si les relations G_1 et G_2 sont égales à l'identité ($G_1 = G_2 = I$), alors

$$\mathcal{E}(\mathcal{P}) = P_1 \sqcup P_2.$$

Démonstration.

(a) Supposons que $G_1 L = G_2 L$.

$$\begin{array}{ll} & \mathcal{E}(\mathcal{P}) \\ = & \qquad \{ \text{ Équation 5.31. } \} \\ & G_1 \circ P_1 \cap G_2 \triangleright P_2 L \cup G_2 \circ P_2 \cap G_1 \triangleright P_1 L \\ = & \qquad \{ \ G_i \circ P_i \subseteq G_i L,\ i = 1, 2 \text{ et } G_1 L = G_2 L. \ \} \\ & G_1 \circ P_1 \cap G_2 L \cap G_2 \triangleright P_2 L \cup G_2 \circ P_2 \cap G_1 L \cap G_1 \triangleright P_1 L \\ = & \qquad \{ \text{ Lemme 3.10(c). } \} \\ & G_1 \circ P_1 \cap G_2 \circ (P_2 L) \cup G_2 \circ P_2 \cap G_1 \circ (P_1 L) \\ = & \qquad \{ \text{ Proposition 3.9(c) et théorème 3.8(h). } \} \\ & G_1 \circ P_1 \cap (G_2 \circ P_2) L \cup G_2 \circ P_2 \cap (G_1 \circ P_1) L \\ = & \qquad \{ \text{ Définition de } \sqcup \text{ (3.5). } \} \\ & G_1 \circ P_1 \sqcup G_2 \circ P_2 \end{array}$$

C'est le cas du choix non déterministe démoniaque. Si au moins une des relations (G_1 ou G_2) conduit à un échec, alors comme nous considérons le pire cas, l'échec se reflète dans le résultat.

(b) Supposons que $G_1 L \cap G_2 L = \emptyset$.

$$
\begin{array}{ll}
& \mathcal{E}(\mathcal{P}) \\
= & \qquad \{ \text{ Équation 5.31. } \} \\
& G_1 \triangleleft P_1 \cap G_2 \triangleright P_2 L \cup G_2 \triangleleft P_2 \cap G_1 \triangleright P_1 L \\
= & \qquad \{ \ G_1 \triangleleft P_1 \subseteq G_1 L \subseteq \overline{G_2 L} \subseteq G_2 \triangleright P_2 L \text{ et de même } G_2 \triangleleft P_2 \subseteq G_1 \triangleright P_1 L. \\
& \qquad \} \\
& G_1 \triangleleft P_1 \cup G_2 \triangleleft P_2 \\
= & \qquad \{ \text{ Proposition 3.9(e). } \} \\
& G_1 \triangleleft P_1 \sqcap G_2 \triangleleft P_2
\end{array}
$$

C'est l'alternative exclusive démoniaque ; si les domaines des relations G_1 et G_2 sont disjoints, alors on fait un choix angélique entre $G_1 \triangleleft P_1$ et $G_2 \triangleleft P_2$.

(c) Supposons que G_1 et G_2 sont déterministes.

$$
\begin{array}{ll}
& \mathcal{E}(\mathcal{P}) \\
= & \qquad \{ \text{ Équation 5.31. } \} \\
& G_1 \triangleleft P_1 \cap G_2 \triangleright P_2 L \cup G_2 \triangleleft P_2 \cap G_1 \triangleright P_1 L \\
= & \qquad \{ \text{ Proposition 3.9(a) et théorème 2.27(j). } \} \\
& G_1 P_1 \cap (\overline{G_2 L} \cup G_2 P_2 L) \cup G_2 P_2 \cap (\overline{G_1 L} \cup G_1 P_1 L) \\
= & \qquad \{ \text{ Loi booléenne. } \} \\
& G_1 P_1 \cap \overline{G_2 L} \cup G_1 P_1 \cap G_2 P_2 L \cup G_2 P_2 \cap \overline{G_1 L} \cup G_2 P_2 \cap G_1 P_1 L \\
= & \qquad \{ \text{ Définition de } \sqcup \text{ (3.5). } \} \\
& G_1 P_1 \cap \overline{G_2 L} \ \cup \ G_2 P_2 \cap \overline{G_1 L} \ \cup (G_1 P_1 \sqcup G_2 P_2)
\end{array}
$$

Ceci peut être interprété comme suit : si un état est dans le domaine de G_1 et qu'il n'est pas dans le domaine de G_2, alors on applique $G_1 \triangleleft P_1$ et de même pour le cas symétrique. Si l'état est dans l'intersection des domaines de G_1 et G_2, on fait un choix démoniaque entre $G_1 \triangleleft P_1$ et $G_2 \triangleleft P_2$.

(d) Supposons que les relations G_1 et G_2 sont des identités partielles.

$$
\begin{array}{ll}
& \mathcal{E}(\mathcal{P}) \\
= & \qquad \{ \text{ Résultat (c). } \} \\
& G_1 P_1 \cap \overline{G_2 L} \ \cup \ G_2 P_2 \cap \overline{G_1 L} \ \cup \ (G_1 P_1 \sqcup G_2 P_2) \\
= & \qquad \{ \text{ Définition de } \sqcup \text{ (équation 3.5). } \} \\
& G_1 P_1 \cap \overline{G_2 L} \ \cup \ G_2 P_2 \cap \overline{G_1 L} \ \cup \ (G_1 P_1 \cap G_2 L \sqcup G_2 P_2 \cap G_1 L) \\
= & \qquad \{ \text{ Théorème 2.21(36). } \} \\
& (I \cap \overline{G_2 L}) G_1 P_1 \ \cup \ (I \cap \overline{G_1 L}) G_2 P_2 \ \cup \ ((I \cap G_2 L) G_1 P_1 \sqcup (I \cap G_1 L) G_2 P_2) \\
= & \qquad \{ \text{ Équation 2.28. } \}
\end{array}
$$

$$
\begin{aligned}
& G_2^{\sim} G_1 P_1 \ \cup\ G_1^{\sim} G_2 P_2 \ \cup\ (G_2 G_1 P_1 \sqcup G_1 G_2 P_2) \\
= & \qquad \{ \text{ Théorème 2.29(c). } \} \\
& G_2^{\sim} G_1 P_1 \ \cup\ G_1^{\sim} G_2 P_2 \ \cup\ (G_1 G_2 P_1 \sqcup G_1 G_2 P_2) \\
= & \qquad \{ \text{ Proposition 3.9(a). } \} \\
& G_2^{\sim} \triangleleft G_1 \triangleleft P_1 \ \cup\ G_1^{\sim} \triangleleft G_2 \triangleleft P_2 \ \cup\ (G_1 \triangleleft G_2 \triangleleft P_1 \sqcup G_1 \triangleleft G_2 \triangleleft P_2) \\
= & \qquad \{ \ \triangleleft \text{ se distribue sur } \sqcup. \ \} \\
& G_2^{\sim} \triangleleft G_1 \triangleleft P_1 \ \cup\ G_1^{\sim} \triangleleft G_2 \triangleleft P_2 \ \cup\ G_1 \triangleleft G_2 \triangleleft (P_1 \sqcup P_2)
\end{aligned}
$$

Cette expression est semblable à la précédente et elle signifie la même chose, sauf qu'ici les relations G_1 et G_2 sont des identités partielles et correspondent davantage au cas des commandes gardées de Dijkstra [30]. C'est la forme la plus familière et celle qu'on rencontre le plus en pratique.

(e) Il suffit de remplaçer G_1 et G_2 par I dans l'équation 5.31 ou dans le résultat (a).

Nous pouvons penser que le choix non déterministe entre P_1 et P_2 peut être exprimé par $P_1 \cup P_2$. Mais, pour un état initial donné, si P_1 ou P_2 conduit à un échec, alors, comme nous considérons le pire cas, l'échec se reflète dans le résultat, c'est-à-dire que l'état initial considéré n'est pas dans le domaine du résultat. Il s'agit donc d'un choix démoniaque. ∎

5.3.3 Diagramme de séquence

Soit le diagramme de séquence (5.4) $\mathcal{P} = (P, C, e, s)$, où

$$P = G_1 \cup P_1, \quad \{e, a, s\} \subseteq C, \quad G_1 = eG_1a, \quad \text{et} \quad P_1 = aP_1s.$$

Remarquons que ce diagramme est un cas particulier du diagramme de choix 5.6, en prenant $G_2 = P_2 = b = \emptyset$. En remplaçant G_2 et P_2 par $\emptyset$ dans l'équation 5.31, nous obtenons :

(5.33) $\quad \mathcal{E}(\mathcal{P}) = G_1 \triangleleft P_1.$

Ceci est la relation d'entrée/sortie du diagramme de séquence $\mathcal{P}$.

5.3.4 Diagramme de boucle

Enfin, nous exposons le cas du diagramme de boucle. Considérons le diagramme de boucle (5.8) $\mathcal{W} = (W, C, e, s)$, où

(5.34) $\quad W = P \cup Q, \quad P = ePe, \quad Q = eQs \quad \text{et} \quad PL \cap QL = \emptyset.$

Comme nous allons le voir par la suite, contrairement aux autres cas, la relation W n'est pas nécessairement progressivement finie. Calculons la relation eW^*.

$$
\begin{array}{ll}
& eW^* \\
= & \qquad \{\ W = P \cup Q.\ \} \\
& e(P \cup Q)^* \\
= & \qquad \{\ QP = \emptyset \text{ (équation 5.34, } es = \emptyset) \text{ et lemme 2.35(e).}\ \} \\
& eP^*Q^* \\
= & \qquad \{\ \text{Équation 2.34 et } Q^2 = \emptyset \text{ (car } Q = eQs \text{ et } se = \emptyset).\ \} \\
& eP^*(I \cup Q) \\
= & \qquad \{\ \text{Théorème 2.21(9) et } eP^*Q = P^*Q \text{ (car } eQs = Q \text{ et } eP = P).\ \} \\
& eP^* \cup P^*Q
\end{array}
$$

d'où

(5.35) $eW^* = eP^* \cup P^*Q.$

Étant donné que (;) se distribue sur $\cup$, que $es = \emptyset$, $Q = Qs$ et que $eP^* = eP^*e$ (car $P = ePe$), nous avons,

(5.36) $eW^*s = P^*Q.$

Ceci est la relation d'entrée/sortie angélique du diagramme de boucle. Cette expression signifie que P est exécutée jusqu'à ce que Q puisse être exécutée.

Dans ce qui suit, nous calculons les autres termes de l'expression $\mathcal{E}(\mathcal{W})$ (équation 5.18 avec $P := W$). Pour le calcul du terme $eW^* \triangleright (WL \cup sL)$, nous appliquons la même méthode que celle utilisée pour les cas précédents.

Appliquons la loi de l'égalité indirecte (2.17). Soit X une relation quelconque.

$$
\begin{array}{ll}
& X \subseteq eW^* \triangleright (WL \cup sL) \\
\Leftrightarrow & \qquad \{\ \text{Équation 2.47.}\ \} \\
& (eW^*)^\smile X \subseteq WL \cup sL \\
\Leftrightarrow & \qquad \{\ \text{Équation 5.35, } P = eP,\ Q = eQ,\ W = P \cup Q \text{ et (;) se distribue sur } \cup.\ \} \\
& (eP^* \cup P^*Q)^\smile X \subseteq ePL \cup eQL \cup sL \\
\Leftrightarrow & \qquad \{\ \text{Théorème 2.21(11,21,24) et } P^*Q = P^*Qs.\ \} \\
& (eP^*)^\smile X \cup s(P^*Q)^\smile X \subseteq e(PL \cup QL) \cup sL \\
\Leftrightarrow & \qquad \{\ \text{Équation 2.16 et } (eP^*)^\smile = (eP^*e)^\smile \subseteq eL.\ \} \\
& (eP^*)^\smile X \subseteq e(PL \cup QL) \quad \wedge \quad s(P^*Q)^\smile X \subseteq sL \\
\Leftrightarrow & \qquad \{\ s(P^*Q)^\smile X \subseteq sL \text{ et } e(PL \cup QL) = PL \cup QL.\ \} \\
& (eP^*)^\smile X \subseteq PL \cup QL \\
\Leftrightarrow & \qquad \{\ \text{Équation 2.47.}\ \} \\
& X \subseteq eP^* \triangleright (PL \cup QL)
\end{array}
$$

Par la loi 2.17, nous obtenons $eW^* \triangleright (WL \cup sL) = eP^* \triangleright (PL \cup QL)$. En appliquant le lemme 2.45(i) et l'abréviation 4.7, nous obtenons

(5.37) $eW^* \triangleright (WL \cup sL) = e \triangleright \mathcal{A}(P, Q)$.

Calculons le troisième terme de $\mathcal{E}(\mathcal{W})$ (équation 5.18 avec $P := W$), c'est-à-dire $e\mathcal{B}(W)$.

$$
\begin{array}{ll}
& \mathcal{B}(W) \\
= & \qquad \{\ W = P \cup Q.\ \} \\
& \mathcal{B}(P \cup Q) \\
= & \qquad \{\ \text{Lemme 2.59.}\ \} \\
& ((Q^*P)^* \triangleright \mathcal{B}(Q) \cap \mathcal{B}(Q^*P)) \\
= & \qquad \{\ Q^*P = P\ (se = \emptyset, \text{ équation 2.31 et } (;) \text{ se distribue sur } \cup).\ \} \\
& P^* \triangleright \mathcal{B}(Q) \cap \mathcal{B}(P) \\
= & \qquad \{\ \mathcal{B}(Q) = L \text{ car } Q^n = \emptyset \text{ pour } n \geq 2, \text{ proposition 2.54(b) et } P^* \triangleright L = L.\ \} \\
& \mathcal{B}(P)
\end{array}
$$

d'où

(5.38) $e\mathcal{B}(W) = e\mathcal{B}(P)$.

Nous obtenons donc

(5.39) $\mathcal{E}(\mathcal{W}) = P^*Q \cap \mathcal{A}(P, Q) \cap \mathcal{B}(P)$.

En effet,

$$
\begin{array}{ll}
& \mathcal{E}(\mathcal{W}) \\
= & \qquad \{\ \text{Équations 5.18, 5.36, 5.37, 5.38 et } e\mathcal{B}(P) \subseteq eL.\ \} \\
& P^*Q \cap e \triangleright \mathcal{A}(P, Q) \cap eL \cap e\mathcal{B}(P) \\
= & \qquad \{\ \text{Théorème 2.27(f).}\ \} \\
& P^*Q \cap e\mathcal{A}(P, Q) \cap e\mathcal{B}(P) \\
= & \qquad \{\ P^*Q = eP^*Q\ (\text{théorème 2.29(e)}).\ \} \\
& P^*Q \cap \mathcal{A}(P, Q) \cap \mathcal{B}(P)
\end{array}
$$

Cette expression est la relation d'entrée/sortie du diagramme de boucle 5.34, obtenue en appliquant la définition 5.18. ∎

Dans la section suivante, nous allons donner une application du théorème de Mills généralisé. Nous allons montrer que la relation d'entrée/sortie du diagramme de boucle, donnée par l'équation 5.39, est le plus grand point fixe de la fonction $w_d(X) := Q \cup P \triangleleft X$ dans le demi-treillis démoniaque.

5.4 Application du théorème de Mills

Nous voulons montrer que la relation $B := P^*Q \cap \mathcal{A}(P,Q) \cap \mathcal{B}(P)$ (équation 5.39) est le plus grand point fixe par rapport à $\sqsubseteq$ de $w_d(X) := Q \cup P \,\square\, X$. Utilisons le théorème de Mills généralisé (4.14) pour prouver

(5.40) $P^*Q \cap \mathcal{A}(P,Q) \cap \mathcal{B}(P) = \bigsqcup\{X | X \sqsubseteq Q \cup P \,\square\, X\}$.

Avant de prouver l'équation 5.40, démontrons les deux lemmes suivants.

(5.41) **Lemme.** *Soient P, Q et R des relations quelconques. Elles satisfont l'égalité*

$$R \,\square\, (P^*(Q \cap \overline{PL}) \cap \mathcal{A}(P,Q) \cap \mathcal{B}(P)) = RP^*(Q \cap \overline{PL}) \cap R \triangleright (\mathcal{A}(P,Q) \cap \mathcal{B}(P)).$$

Démonstration.

$$\begin{array}{ll}
& R \,\square\, (P^*(Q \cap \overline{PL}) \cap \mathcal{A}(P,Q) \cap \mathcal{B}(P)) \\
= & \qquad \{ \text{ Lemme 3.10(d). } \} \\
& R \,\square\, (P^*(Q \cap \overline{PL})) \cap R \,\square\, \mathcal{A}(P,Q) \cap R \,\square\, \mathcal{B}(P) \\
= & \qquad \{ \text{ Définition 3.7, théorème 2.21(36) et lemme 3.10(c). } \} \\
& RP^*(Q \cap \overline{PL}) \cap R \triangleright P^*(QL \cap \overline{PL}) \cap R \triangleright \mathcal{A}(P,Q) \cap R \triangleright \mathcal{B}(P) \cap RL \\
= & \qquad \{ \text{ Lemme 2.45(e), } RP^*(Q \cap \overline{PL}) \subseteq RL \text{, loi booléenne et } P^*(\overline{PL} \cap \overline{QL}) \cap \\
& \qquad \mathcal{A}(P,Q) = \emptyset \text{ (voir abréviation 4.7). } \} \\
& RP^*(Q \cap \overline{PL}) \cap R \triangleright ((P^*(QL \cap \overline{PL}) \cup P^*(\overline{PL} \cap \overline{QL})) \cap \mathcal{A}(P,Q) \cap \mathcal{B}(P)) \\
= & \qquad \{ \text{ (;) se distribue sur } \cup \text{ et loi booléenne. } \} \\
& RP^*(Q \cap \overline{PL}) \cap R \triangleright (P^*(\overline{PL} \cap (QL \cup \overline{QL})) \cap \mathcal{A}(P,Q) \cap \mathcal{B}(P)) \\
= & \qquad \{ \text{ Lois booléennes et } QL \cup \overline{QL} = L. \} \\
& RP^*(Q \cap \overline{PL}) \cap R \triangleright (P^*\overline{PL} \cap \mathcal{A}(P,Q) \cap \mathcal{B}(P)) \\
= & \qquad \{ \text{ Proposition 2.54(a). } \} \\
& RP^*(Q \cap \overline{PL}) \cap R \triangleright (\mathcal{A}(P,Q) \cap \mathcal{B}(P))
\end{array}$$

∎

Le lemme suivant regroupe quelques propriétés vérifiées par les vecteurs $\mathcal{A}(P,Q)$ (abréviation 4.7) et $\mathcal{B}(P)$.

(5.42) **Lemme.** *Soient P et Q des relations telles que $PL \cap QL = \emptyset$.*

(a) $PL \cap P \triangleright (\mathcal{A}(P,Q) \cap \mathcal{B}(P)) = PL \cap \mathcal{A}(P,Q) \cap \mathcal{B}(P)$,

(b) $Q \subseteq \mathcal{A}(P,Q) \cap \mathcal{B}(P)$.

Démonstration.

$$
\begin{array}{lll}
\text{(a)} & PL \cap P \triangleright (\mathcal{A}(P,Q) \cap \mathcal{B}(P)) & \\
= & & \{\ PL \subseteq PL \cup QL.\ \} \\
& PL \cap (PL \cup QL) \cap P \triangleright (\mathcal{A}(P,Q) \cap \mathcal{B}(P)) & \\
= & & \{\ \text{Théorème 4.10(2) (nous utilisons l'expression } w_L(x) = (PL \cup QL) \cap \\
& & \quad P \triangleright x \text{ donnée au début de la démonstration du théorème 4.10(2)).}\ \} \\
& PL \cap \mathcal{A}(P,Q) \cap \mathcal{B}(P) &
\end{array}
$$

$$
\begin{array}{lll}
\text{(b)} & Q \subseteq QL \cup PL \cap P \triangleright X & \\
\Rightarrow & & \{\ \text{Proposition 2.12(a) et } \mu(X \mapsto Q) = Q.\ \} \\
& Q \subseteq \mu(X \mapsto QL \cup PL \cap P \triangleright X) & \\
\Rightarrow & & \{\ PL \cap QL = \emptyset \text{ et } \overline{PL} \subseteq P \triangleright X.\ \} \\
& Q \subseteq \mu(X \mapsto (PL \cup QL) \cap P \triangleright X) & \\
\Rightarrow & & \{\ \text{Corollaire 2.58 et abréviation 4.7.}\ \} \\
& Q \subseteq \mathcal{A}(P,Q) \cap \mathcal{B}(P) &
\end{array}
$$

■

Maintenant, nous sommes prêts à démontrer l'équation 5.40.

(5.43) **Théorème.** *Soient P et Q des relations telles que $PL \cap QL = \emptyset$. La relation $P^*Q \cap \mathcal{A}(P,Q) \cap \mathcal{B}(P)$ (abréviation 4.7) est le plus grand point fixe de $w_d(X) := Q \cup P \triangleright\!\!\triangleleft X$ (par rapport à $\sqsubseteq$).*

Démonstration. Nous utilisons le théorème 4.14. La condition (b) du théorème 4.14 est évidente. Il nous reste à montrer la condition (a), c'est-à-dire que $P^*Q \cap \mathcal{A}(P,Q) \cap \mathcal{B}(P)$ est un point fixe de w_d.

$$
\begin{array}{lll}
& w_d(P^*Q \cap \mathcal{A}(P,Q) \cap \mathcal{B}(P)) & \\
= & & \{\ w_d(X) = Q \cup P \triangleright\!\!\triangleleft X.\ \} \\
& Q \cup P \triangleright\!\!\triangleleft (P^*Q \cap \mathcal{A}(P,Q) \cap \mathcal{B}(P)) & \\
= & & \{\ \text{Lemme 5.41 avec } Q \cap \overline{PL} = Q \text{ et } PP^*Q \subseteq PL.\ \} \\
& Q \cup PP^*Q \cap P \triangleright (\mathcal{A}(P,Q) \cap \mathcal{B}(P)) \cap PL & \\
= & & \{\ \text{Lemme 5.42(a,b).}\ \} \\
& Q \cap \mathcal{A}(P,Q) \cap \mathcal{B}(P) \cup PP^*Q \cap PL \cap \mathcal{A}(P,Q) \cap \mathcal{B}(P) & \\
= & & \{\ \text{Lois booléennes et } PP^*Q \subseteq PL.\ \} \\
& (Q \cup PP^*Q) \cap \mathcal{A}(P,Q) \cap \mathcal{B}(P) & \\
= & & \{\ \text{Théorème 2.21(11) et équation 2.31.}\ \} \\
& P^*Q \cap \mathcal{A}(P,Q) \cap \mathcal{B}(P) &
\end{array}
$$

■

5.5 Conclusion

Dans ce chapitre nous avons donné la définition des diagrammes ainsi qu'une description informelle de leur exécution. En partant de ces notions, nous avons défini la relation d'entrée/sortie démoniaque d'un diagramme (équation 5.15) qui regroupe différents types de diagrammes. Nous avons appliqué cette définition générale pour calculer les relations d'entrée/sortie des diagrammes élémentaires. Notons que la relation d'entrée/sortie du diagramme de séquence et celle du diagramme de choix ne nous sont pas nouvelles : elles sont équivalentes (en omettant quelques détails que nous allons régler dans le chapitre 7) aux sémantiques dénotationnelles démoniaques de la séquence et du choix gardé (déja présentées dans le chapitre 3). Pour, le diagramme de boucle, nous avons appliqué le théorème de Mills généralisé (4.14) pour prouver que la relation d'entrée/sortie (5.39) du diagramme de boucle est le plus grand point fixe par rapport à $\sqsubseteq$ de la fonction $w_d(X) := Q \cup P \,\square\, X$ dans le demi-treillis démoniaque.

Chapitre 6

Diagrammes composés

Dans le chapitre 5, nous avons montré comment calculer la relation d'entrée/sortie démoniaque des diagrammes élémentaires. Dans ce chapitre, nous considérons le cas des diagrammes composés. Ces derniers sont les diagrammes constitués à partir d'autres diagrammes (les constructeurs sont : la séquence, le choix et la boucle).

Supposons que nous avons un diagramme composé $\mathcal{R} = (\bigcup_{i=1}^{n} P_i, C, e, s)$ construit à partir de sous-diagrammes élémentaires (5.12(b)) $\mathcal{P}_i = (P_i, C_i, e_i, s_i)$. Au lieu de calculer la relation d'entrée/sortie $\mathcal{E}(\mathcal{R})$ du diagramme $\mathcal{R}$ directement en appliquant l'équation 5.15, ce qui est un travail très laborieux, nous allons prouver que cette relation $\mathcal{E}(\mathcal{R})$ est égale à la relation d'entrée/sortie du diagramme obtenu à partir du diagramme $\mathcal{R}$ en remplaçant chaque sous-diagramme $\mathcal{P}_i$ par sa relation d'entrée/sortie $\mathcal{E}(\mathcal{P}_i)$.

Le processus continue jusqu'à l'obtention des diagrammes élémentaires auxquels nous appliquons les résultats du chapitre 5. Donnons un exemple.

(6.1) **Exemple.** Soit un diagramme $\mathcal{R} = (R, C, e, s)$ constitué de deux sous-diagrammes $\mathcal{P}_1 = (P_1, C, e, c)$ et $\mathcal{P}_2 = (P_2, C, c, s)$, comme illustré par la figure 6.1. Les sous-diagrammes $\mathcal{P}_1$ et $\mathcal{P}_2$ peuvent eux-mêmes être des diagrammes composés.

Au lieu de calculer directement la relation d'entrée/sortie $\mathcal{E}(\mathcal{R})$ du diagramme $\mathcal{R}$ en appliquant l'équation (5.15), nous voulons montrer que

$$\mathcal{E}(\mathcal{R}) = \mathcal{E}(\mathcal{R}'),$$

avec

$$\mathcal{R}' = (\mathcal{E}(\mathcal{P}_1) \cup \mathcal{E}(\mathcal{P}_2), C, e, s), \quad C = \{e, c, s\}, \quad \mathcal{E}(\mathcal{P}_1) = e\mathcal{E}(\mathcal{P}_1)c, \quad \mathcal{E}(\mathcal{P}_2) = c\mathcal{E}(\mathcal{P}_2)s.$$

Par la définition 5.4, $\mathcal{R}'$ est un diagramme de séquence (voir le graphe de la figure 6.2). En appliquant l'équation 5.33 au diagramme $\mathcal{R}'$, nous obtenons $\mathcal{E}(\mathcal{R}') = \mathcal{E}(\mathcal{P}_1) \,▫\, \mathcal{E}(\mathcal{P}_2)$ et nous en déduisons donc

(6.2) $$\mathcal{E}(\mathcal{R}) = \mathcal{E}(\mathcal{P}_1) \,▫\, \mathcal{E}(\mathcal{P}_2).$$

■

Il est clair que derrière ce résultat (équation 6.2) se cache tout un traitement formel préliminaire. Nous devons aussi considérer les autres types de diagrammes, c'est-à-dire le

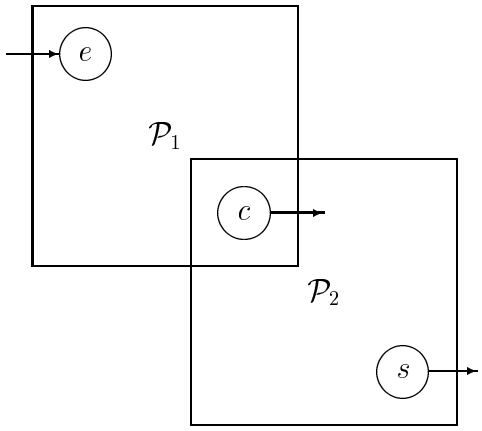


Figure 6.1: Diagramme composé de deux sous-diagrammes

diagramme de choix et le diagramme de boucle. Au lieu de traiter chaque cas séparément, nous allons donner un résultat général qui regroupe tous ces cas.

Nous nous restreignons aux hypothèses suivantes que nous allons expliquer ci-dessous.

(6.3) **Hypothèses.** Soit un diagramme $\mathcal{R} = (R, C, e, s)$, dans lequel nous identifions un sous-diagramme $\mathcal{P} = (P, C_P, a, c)$ (figure 6.3) tel que :

$$R = P \cup Q, \qquad C_P = \{a, b, c\},$$
$$C = \{a, b, c, d\}, \qquad e \subseteq a \cup c \cup d,$$
$$P = (a \cup b)P(a \cup b \cup c), \qquad s \subseteq c \cup d. \quad \blacksquare$$
$$Q = (c \cup d)Q(a \cup c \cup d),$$

Notre but est de décomposer la relation R de manière à mettre en évidence un sous-diagramme $\mathcal{P}$ du diagramme $\mathcal{R}$.

Les points d'entrée de $\mathcal{P}$ sont représentés par a, les points de sortie par c et les points qui ne sont ni points d'entrée ni points de sortie, que nous appelons points internes, sont représentés par b. Nous imposons que ces trois éléments soient deux à deux disjoints, c'est-à-dire $a \cap b = c \cap a = c \cap b = \emptyset$, ainsi que $c \subseteq \overline{PL}$ (c'est-à-dire $cP = \emptyset$) qui signifie que c est terminal. Cette restriction imposée à a, b et c n'est pas majeure car les diagrammes de la sous-section 5.1.1 (atomique, séquence, choix et boucle) satisfont tous ces conditions. L'identité partielle d représente les points de $\mathcal{R}$ autres que ceux de a, b, c, d'où $dP = \emptyset$, $Pd = \emptyset$ et $d \cap a = d \cap b = d \cap c = \emptyset$. En considérant ces conditions et le fait que P est la relation associée du sous-diagramme $\mathcal{P}$, nous avons $P = (a \cup b)P(a \cup b \cup c)$.

Nous supposons que les points internes de $\mathcal{P}$ ne peuvent servir à passer le contrôle de P à Q ou de Q à P, ce qui donne $bQ = Qb = \emptyset$.

Nous supposons aussi que les points de a servent d'entrée à P seulement, ce qui donne $aQ = \emptyset$. En regroupant, nous obtenons : $Q = (c \cup d)Q(a \cup c \cup d)$.

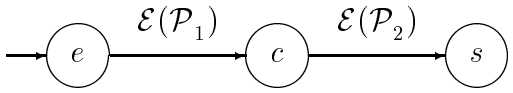


Figure 6.2: Le diagramme de séquence $\mathcal{R}'$

De même, l'entrée dans $\mathcal{R}$ ne peut se faire par b, d'où $e \subseteq a \cup c \cup d$. Finalement, les points de sortie du diagramme principal $\mathcal{R}$ doivent être des points de sortie des sous-diagrammes, d'où $s \cap a = s \cap b = \emptyset$, ce qui implique que $s \subseteq c \cup d$.

La relation Q représente l'union des relations associées aux sous-diagrammes de $\mathcal{R}$ autres que $\mathcal{P}$.

Sur la base de ces hypothèses, les matrices R et P associées respectivement aux diagrammes $\mathcal{R}$ et $\mathcal{P}$ peuvent être représentées comme suit :

$$R = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{pmatrix} P_1 & P_2 & P_3 & \emptyset \\ P_4 & P_5 & P_6 & \emptyset \\ Q_1 & \emptyset & Q_2 & Q_3 \\ Q_4 & \emptyset & Q_5 & Q_6 \end{pmatrix} \end{array}, \qquad P = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{pmatrix} P_1 & P_2 & P_3 & \emptyset \\ P_4 & P_5 & P_6 & \emptyset \\ \emptyset & \emptyset & \emptyset & \emptyset \\ \emptyset & \emptyset & \emptyset & \emptyset \end{pmatrix} \end{array}.$$

(6.4) **Remarque.** Tout diagramme $\mathcal{R} = (\bigcup_{i=1}^{n} P_i, C, e, s)$ construit à partir des sous-diagrammes $\mathcal{P}_i = (P_i, C, e_i, s_i)$ peut être ramené aux hypothèses 6.3 en identifiant un sous-diagramme $\mathcal{P}_k = (P_k, C_k, e_k, s_k)$, où $1 \leq k \leq n$, et en posant

$P := P_k$,
$Q := \bigcup_{i=1}^{n} P_i$, avec $i \neq k$,
$a := e_k$,
$b := (\bigcup C_k) \cap \overline{e_k \cup s_k}$,
$c := s_k$,
$d := (\bigcup_{i=1}^{n} C_i) \cap \overline{\bigcup C_k}$,
$e := e$. ∎

Présentons maintenant le résultat principal de ce chapitre.

(6.5) **Théorème.** *Soient* $\mathcal{R} := (R, C, e, s)$ *et* $\mathcal{P} := (P, C, a, c)$ *vérifiant les hypothèses (6.3). On a*

$$\mathcal{E}(\mathcal{R}) = \mathcal{E}(\mathcal{R}'),$$

où

$$\mathcal{R}' := (\mathcal{E}(\mathcal{P}) \cup Q, C, e, s).$$

∎

Les sections 6.1 et 6.2 sont consacrées à la démonstration du théorème 6.5.

Ceci signifie que la relation d'entrée/sortie du diagramme $\mathcal{R} = (P \cup Q, C, e, s)$ est égale à la relation d'entrée/sortie du diagramme $(\mathcal{E}(\mathcal{P}) \cup Q, C, e, s)$; la relation associée au

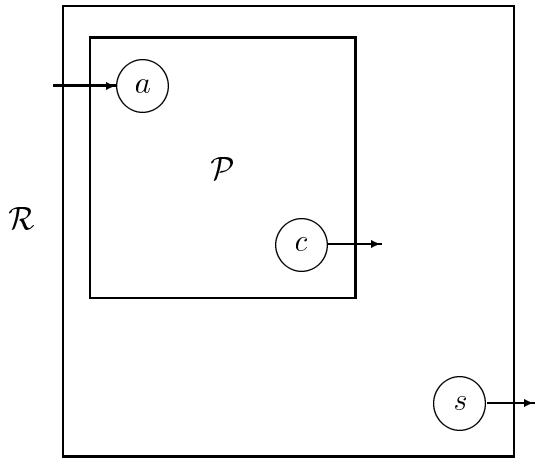


Figure 6.3: Diagramme composé quelconque

diagramme $\mathcal{P}$ a été remplacée par la relation d'entrée/sortie de ce dernier (voir la matrice ci-dessous). Notons que le diagramme $(\mathcal{E}(\mathcal{P}), \{a, c\}, a, c)$ est un diagramme atomique.

$$R' = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{pmatrix} \emptyset & \emptyset & \mathcal{E}(\mathcal{P}) & \emptyset \\ \emptyset & \emptyset & \emptyset & \emptyset \\ Q_1 & \emptyset & Q_2 & Q_3 \\ Q_4 & \emptyset & Q_5 & Q_6 \end{pmatrix} \end{array}$$

Pour prouver ce résultat (théorème 6.5), nous avons besoin de présenter des résultats préliminaires. Ces résultats font l'objet de la section ci-après.

6.1 Résultats préliminaires

Avant de démontrer le théorème 6.5, nous allons établir les liens existant entre les différents termes des expressions $\mathcal{E}(\mathcal{P})$ et $\mathcal{E}(\mathcal{R})$, c'est-à-dire P^*, R^*, $\mathcal{A}(P, c)$ et $\mathcal{A}(R, s)$ ainsi que les parties initiales $\mathcal{B}(P)$ et $\mathcal{B}(R)$. Ces propriétés seront présentées sous forme de lemmes. Nous donnons des explications informelles et intuitives de quelques-unes de ces propriétés.

(6.6) **Lemme.** *Soient P, Q et s les relations données dans les hypothèses 6.3.*

(a) $PR^* = P^+(a \cup b) \cup P^+cR^*$,

(b) $P^+(a \cup b) \triangleright (RL \cup sL) = P \triangleright \mathcal{A}(P, c)$,

(c) $P \triangleright \mathcal{A}(R, s) = P \triangleright \mathcal{A}(P, c) \cap P^+c \triangleright \mathcal{A}(R, s)$.

Démonstration.

(a)
$$
\begin{aligned}
& PR^* \\
= & \quad \{\ R = P \cup Q \text{ et lemme 2.35(d,g).}\ \} \\
& PP^*(QP^*)^* \\
= & \quad \{\ \text{Équation 2.33(a) et } P^+ = P^+(a \cup b \cup c) \text{ (hypothèses 6.3).}\ \} \\
& P^+(a \cup b \cup c)(QP^*)^* \\
= & \quad \{\ \text{Théorème 2.21(9,11) et équation 2.33(b).}\ \} \\
& P^+(a \cup b)(I \cup (QP^*)^+) \cup P^+c(QP^*)^* \\
= & \quad \{\ \text{Théorème 2.21(9).}\ \} \\
& P^+(a \cup b) \cup P^+(a \cup b)(QP^*)^+ \cup P^+c(QP^*)^* \\
= & \quad \{\ (a \cup b)Q = \emptyset,\ cP = \emptyset \text{ et équation 2.33(b).}\ \} \\
& P^+(a \cup b) \cup P^+cP^*(QP^*)^* \\
= & \quad \{\ R = P \cup Q \text{ et lemme 2.35(d,g).}\ \} \\
& P^+(a \cup b) \cup P^+cR^*
\end{aligned}
$$

Un chemin d'un état i à un autre état i' par R, où i est un état du domaine de P, peut s'arrêter en a ou en b (donc à l'intérieur du diagramme $\mathcal{P}$) ou bien il peut continuer jusqu'à c et passer par la suite au diagramme $\mathcal{R}$.

(b)
$$
\begin{aligned}
& (a \cup b) \triangleright (RL \cup sL) \\
= & \quad \{\ \text{Théorème 2.27(j) et définition 2.44.}\ \} \\
& \overline{(a \cup b)L} \cup (a \cup b)(RL \cup sL) \\
= & \quad \{\ (a \cup b)s = \emptyset,\ R = P \cup Q,\ (a \cup b)Q = \emptyset \text{ et } (a \cup b)PL = PL \\
& \quad \text{(hypothèses 6.3).}\ \} \\
& \overline{(a \cup b)L} \cup (a \cup b)PL \\
= & \quad \{\ \text{Théorème 2.27(j) et définition 2.44.}\ \} \\
& (a \cup b) \triangleright PL \\
= & \quad \{\ PL \subseteq \overline{cL} \ (cP = \emptyset \text{ et règle de Schröder}) \text{ et lois booléennes.}\ \} \\
& (a \cup b) \triangleright (\overline{cL} \cap (PL \cup cL)) \\
= & \quad \{\ \text{Lemme 2.45(e).}\ \} \\
& (a \cup b) \triangleright \overline{cL} \cap (a \cup b) \triangleright (PL \cup cL) \\
= & \quad \{\ \text{Définition 2.44 et } (a \cup b)c = \emptyset.\ \} \\
& (a \cup b) \triangleright (PL \cup cL) \\
= & \quad \{\ c\overline{cL} = \emptyset, \text{ d'où } c \triangleright (PL \cup cL) = L.\ \} \\
& (a \cup b) \triangleright (PL \cup cL) \cap c \triangleright (PL \cup cL) \\
= & \quad \{\ \text{Lemme 2.45(g).}\ \} \\
& (a \cup b \cup c) \triangleright (PL \cup cL)
\end{aligned}
$$

Ainsi, nous avons prouvé que $(a \cup b) \triangleright (RL \cup sL) = (a \cup b \cup c) \triangleright (PL \cup cL)$, ce qui implique que $P^+ \triangleright ((a \cup b) \triangleright (RL \cup sL)) = P^+ \triangleright ((a \cup b \cup c) \triangleright (PL \cup cL))$. Par le lemme

2.45(i), ceci est équivalent à $P^+(a \cup b) \triangleright (RL \cup sL) = P^+(a \cup b \cup c) \triangleright (PL \cup cL)$. En appliquant la définition 2.44, le fait que $P^+(a \cup b \cup c) = P^+$, $P^+ = PP^*$, le lemme 2.45(i) ainsi que l'abréviation 4.7, nous obtenons $P^+(a \cup b) \triangleright (RL \cup sL) = P \triangleright \mathcal{A}(P, c)$.

(c)
$$
\begin{aligned}
& P \triangleright \mathcal{A}(R, s) \\
= & \quad \{ \text{ Définition 2.44, abréviation 4.7 et lemme 2.45(i). } \} \\
& PR^* \triangleright (RL \cup sL) \\
= & \quad \{ \text{ Lemme 6.6(a). } \} \\
& (P^+(a \cup b) \cup P^+cR^*) \triangleright (RL \cup sL) \\
= & \quad \{ \text{ Lemme 2.45(i,h) et abréviation 4.7. } \} \\
& P^+(a \cup b) \triangleright (RL \cup sL) \cap P^+c \triangleright \mathcal{A}(R, s) \\
= & \quad \{ \text{ Lemme 6.6(b). } \} \\
& P \triangleright \mathcal{A}(P, c) \cap P^+c \triangleright \mathcal{A}(R, s)
\end{aligned}
$$

Rappelons que le vecteur $\mathcal{A}(R, s)$ représente les états à partir desquels aucune terminaison anormale par R n'est possible. La loi que nous venons de démontrer se lit facilement après l'avoir complémentée : $P\overline{\mathcal{A}(R, s)} = P\overline{\mathcal{A}(P, c)} \cup P^+c\overline{\mathcal{A}(R, s)}$. Elle exprime alors le fait qu'une transition par P peut mener à une terminaison anormale par R si et seulement si elle mène, soit à une terminaison anormale par P, soit à une terminaison normale (avec sortie par c) suivie d'une terminaison anormale par R. ∎

Dans le corollaire suivant nous allons montrer que la relation d'entrée/sortie d'un diagramme est le plus grand point fixe par rapport à $\sqsubseteq$ d'une certaine fonction.

(6.7) **Corollaire.** *Soit le diagramme* $\mathcal{R} = (R, C, e, s)$.

$$\mathcal{E}(\mathcal{R}) = e\nu_{\sqsubseteq}(f),$$

où $f(X) := s \cap \overline{RL} \cup R \triangleleft X$.

Démonstration.

$$
\begin{aligned}
& \mathcal{E}(\mathcal{R}) \\
= & \quad \{ \text{ Équation 5.17. } \} \\
& eR^*(s \cap \overline{RL}) \cap eR^* \triangleright (RL \cup sL) \cap e\mathcal{B}(R) \\
= & \quad \{ \text{ Théorème 2.27(a,f), définition 2.44 et abréviation 4.7. } \} \\
& e(R^*(s \cap \overline{RL}) \cap \mathcal{A}(R, s) \cap \mathcal{B}(R))
\end{aligned}
$$

Par le théorème 5.43 nous avons

(6.8) $$P^*Q \cap \mathcal{A}(P, Q) \cap \mathcal{B}(P) = \nu_{\sqsubseteq}(X \mapsto P \cup Q \triangleleft X),$$

avec $PL \cap QL = \emptyset$. Remarquons que par le théorème 2.21(5,36) nous avons

$$R^* \triangleright (RL \cup sL) = R^* \triangleright (RL \cup (s \cap \overline{RL})L).$$

Par conséquent, en posant $P := R$ et $Q := s \cap \overline{RL}$ dans l'équation 6.8, nous déduisons que $\mathcal{E}(\mathcal{R}) = e\nu_{\sqsubseteq}(f)$. ∎

Nous allons utiliser ce corollaire pour exprimer les relations $\mathcal{E}(\mathcal{R})$ et $\mathcal{E}(\mathcal{P})$ comme les plus grands points fixes par rapport à $\sqsubseteq$ des fonctions suivantes :

(6.9) (a) $f_R(X) := s \cap \overline{RL} \cup R \square X$,
(b) $f_P(X) := c \cap \overline{PL} \cup P \square X$.

Soient également

(6.10) (a) $S_R := R^*(s \cap \overline{RL}) \cap \mathcal{A}(R, s) \cap \mathcal{B}(R)$,
(b) $S_P := P^*(c \cap \overline{PL}) \cap \mathcal{A}(P, c) \cap \mathcal{B}(P)$.

En utilisant les notations ci-dessus et le corollaire 6.7, nous avons

(6.11) $\mathcal{E}(\mathcal{R}) = eS_R$ et $S_R = \nu_{\sqsubseteq}(f_R)$.

Donc, eS_R est la relation d'entrée/sortie du diagramme $\mathcal{R}$.

En considérant le fait que $c \subseteq \overline{PL}$, la fonction f_P et la relation S_P deviennent

(6.12) $f_P(X) := c \cup P \square X$ et $S_P := P^*c \cap \mathcal{A}(P, c) \cap \mathcal{B}(P)$.

En utilisant les notations données dans l'équation 6.12 et le corollaire 6.7, nous obtenons

(6.13) $\mathcal{E}(\mathcal{P}) = aS_P$ et $S_P = \nu_{\sqsubseteq}(f_P)$.

Donc, aS_P est la relation d'entrée/sortie du diagramme $\mathcal{P}$.

Comme les relations P et R sont des relations quelconques, nous devons tenir compte aussi des propriétés vérifiées par les parties initiales de ces relations. En voici quelques-unes.

(6.14) **Lemme.** *Les relations c, P, Q et S_P données par les hypothèses 6.3 et l'équation 6.12 satisfont les propriétés suivantes :*

(a) $P \triangleright \mathcal{B}(R) = \mathcal{B}(P) \cap P^+c \triangleright \mathcal{B}(R)$,

(b) $\mathcal{B}(R) \subseteq \mathcal{B}(P \square S_P \cup Q)$.

Démonstration.

(a)
$$
\begin{aligned}
& P \triangleright \mathcal{B}(R) \\
= & \quad \{\ R = P \cup Q \text{ et lemme 2.59.}\ \} \\
& P \triangleright ((P^*Q)^* \triangleright \mathcal{B}(P) \cap \mathcal{B}(P^*Q)) \\
= & \quad \{\ \text{Lemme 2.45(e,i) et équation 2.31.}\ \} \\
& P(I \cup P^*Q(P^*Q)^*) \triangleright \mathcal{B}(P) \cap P \triangleright \mathcal{B}(P^*Q) \\
= & \quad \{\ \text{Lemme 2.45(g,i), (;) se distribue sur } \cup \text{ et proposition 2.54(e,g).}\ \} \\
& P^+ \triangleright \mathcal{B}(P) \cap PP^*Q(P^*Q)^* \triangleright \mathcal{B}(P) \cap PP^*Q \triangleright \mathcal{B}(P^*Q) \\
= & \quad \{\ cP = \emptyset \text{ et } PQ = PcQ \text{ donc } PP^*Q = P^+cP^*Q, \text{ et équation 2.33.}\ \} \\
& P^+ \triangleright \mathcal{B}(P) \cap P^+c(P^*Q)^+ \triangleright \mathcal{B}(P) \cap P^+cP^*Q \triangleright \mathcal{B}(P^*Q) \\
= & \quad \{\ \text{Lemme 2.45(i,m) } (P^+c \subseteq P^+).\ \} \\
& P^+ \triangleright \mathcal{B}(P) \cap P^+c \triangleright \mathcal{B}(P) \cap P^+c \triangleright ((P^*Q)^+ \triangleright \mathcal{B}(P)) \cap P^+c \triangleright (P^*Q \triangleright \mathcal{B}(P^*Q)) \\
= & \quad \{\ \text{Proposition 2.54(e,g).}\ \} \\
& \mathcal{B}(P) \cap P^+c \triangleright (\mathcal{B}(P) \cap (P^*Q)^+ \triangleright \mathcal{B}(P) \cap \mathcal{B}(P^*Q)) \\
= & \quad \{\ \mathcal{B}(P) = I \triangleright \mathcal{B}(P), \text{ lemme 2.45(g) et équation 2.33(b).}\ \} \\
& \mathcal{B}(P) \cap P^+c \triangleright ((P^*Q)^* \triangleright \mathcal{B}(P) \cap \mathcal{B}(P^*Q)) \\
= & \quad \{\ R = P \cup Q \text{ et lemme 2.59.}\ \} \\
& \mathcal{B}(P) \cap P^+c \triangleright \mathcal{B}(R)
\end{aligned}
$$

En considérant la définition de $\triangleright$ (2.44), nous obtenons, en complémentant les termes extrêmes de cette dérivation, l'équation $P\overline{\mathcal{B}(R)} = \overline{\mathcal{B}(P)} \cup P^+c\overline{\mathcal{B}(R)}$. Rappelons que $\overline{\mathcal{B}(R)}$ est le vecteur qui caractérise l'ensemble des états à partir desquels une boucle infinie par R est possible. L'équation signifie donc qu'un état i a une image par P qui mène à une boucle infinie par R si et seulement si i mène à une boucle infinie par P ou si i mène d'abord à un état i' en sortie de P (c'est-à-dire que $(i, i') \in P^+c$) et que cet état i' mène à une boucle infinie par R.

(b)
$$
\begin{aligned}
& P \square S_P \cup Q \\
= & \quad \{\ \text{Équation 6.12.}\ \} \\
& P \square (P^*c \cap (\mathcal{A}(P,c) \cap \mathcal{B}(P)) \cup Q \\
= & \quad \{\ \text{Lemme 5.41, } c \subseteq \overline{PL} \text{ et équation 2.33(a).}\ \} \\
& P^+c \cap P \triangleright (\mathcal{A}(P,c) \cap \mathcal{B}(P)) \cup Q \\
\subseteq & \quad \{\ \text{Loi booléenne, } c \subseteq I \text{ et } Q \subseteq Q^+.\ \} \\
& P^+ \cup Q^+ \\
\subseteq & \quad \{\ P \subseteq R,\ Q \subseteq R \text{ et } + \text{ monotone.}\ \} \\
& R^+
\end{aligned}
$$

En utilisant la proposition 2.54(d,f), nous obtenons $\mathcal{B}(R) \subseteq \mathcal{B}(P \square S_P \cup Q)$. ∎

(6.15) **Lemme.** *Les relations P, S_P et S_R données par les hypothèses 6.3 et les équations 6.10(a) et 6.12 satisfont les propriétés suivantes :*

(a) $P \triangleleft S_R = P \triangleleft S_P \triangleleft S_R$,

(b) $S_P \triangleleft (a \cup c \cup d) = S_P$,

(c) $Q \triangleleft (a \cup c \cup d) = Q$,

Démonstration.

(a) $P \triangleleft S_R$

$=$ { Équation 6.10(a). }

$P \triangleleft (R^*(s \cap \overline{RL}) \cap \mathcal{A}(R,s) \cap \mathcal{B}(R))$

$=$ { Lemme 5.41 et lemme 2.45(e). }

$PR^*(s \cap \overline{RL}) \cap P \triangleright \mathcal{A}(R,s) \cap P \triangleright \mathcal{B}(R)$

$=$ { Lemme 6.6(a) et $(;)$ se distribue sur $\cup$. }

$(P^+(a \cup b)(s \cap \overline{RL}) \cup P^+cR^*(s \cap \overline{RL})) \cap P \triangleright \mathcal{A}(R,s) \cap P \triangleright \mathcal{B}(R)$

$=$ { $(a \cup b)(s \cap \overline{RL}) = \emptyset$, lemmes 6.6(c) et 6.14(a). }

$P^+cR^*(s \cap \overline{RL}) \cap P \triangleright \mathcal{A}(P,c) \cap P^+c \triangleright \mathcal{A}(R,s) \cap \mathcal{B}(P) \cap P^+c \triangleright \mathcal{B}(R)$

$=$ { Lemme 2.45(e) et lemme 5.41. }

$P^+c \triangleleft (R^*(s \cap \overline{RL}) \cap \mathcal{A}(R,s) \cap \mathcal{B}(R)) \cap P \triangleright \mathcal{A}(P,c) \cap \mathcal{B}(P)$

$=$ { Équation 6.10(a). }

$P^+c \triangleleft S_R \cap P \triangleright \mathcal{A}(P,c) \cap \mathcal{B}(P)$

$=$ { Lemme 3.10(b). }

$(P^+c \cap P \triangleright \mathcal{A}(P,c) \cap \mathcal{B}(P)) \triangleleft S_R$

$=$ { Équation 2.33(a) et proposition 2.54(e). }

$(PP^*c \cap P \triangleright \mathcal{A}(P,c) \cap P \triangleright \mathcal{B}(P)) \triangleleft S_R$

$=$ { Lemme 2.45(e), $c \subseteq \overline{PL}$ et lemme 5.41. }

$P \triangleleft (P^*c \cap \mathcal{A}(P,c) \cap \mathcal{B}(P)) \triangleleft S_R$

$=$ { Équation 6.12. }

$P \triangleleft S_P \triangleleft S_R$

Donc, une transition par P suivie de l'exécution totale du diagramme $\mathcal{R}$ est égale à une transition par P suivie de l'exécution complète du diagramme $\mathcal{P}$ suivie de l'exécution du diagramme $\mathcal{R}$.

(b) $S_P \triangleleft (a \cup c \cup d)$

$=$ { Équation 6.12. }

$(P^*c \cap \mathcal{A}(P,c) \cap \mathcal{B}(P)) \triangleleft (a \cup c \cup d)$

$=$ { Lemme 3.10(b). }

$(P^*c) \triangleleft (a \cup c \cup d) \cap \mathcal{A}(P,c) \cap \mathcal{B}(P)$

$=$ { Définition 3.7. }

$(P^*c)(a \cup c \cup d) \cap P^*c \triangleright (a \cup c \cup d)L \cap \mathcal{A}(P,c) \cap \mathcal{B}(P))$

$=$ { $ca = cd = \emptyset$, $cc = c$ et lemme 2.45(i). }
$P^*c \cap P^* \triangleright (c \triangleright (a \cup c \cup d)L) \cap \mathcal{A}(P,c) \cap \mathcal{B}(P))$
$=$ { $c \triangleright (a \cup c \cup d)L = L$ et $P^* \triangleright L = L$. }
$P^*c \cap \mathcal{A}(P,c) \cap \mathcal{B}(P)$
$=$ { Équation 6.12. }
S_P

(c) $Q \mathbin{▫} (a \cup c \cup d)$
$=$ { Définition 3.7. }
$Q(a \cup c \cup d) \cap Q \triangleright (a \cup c \cup d)L$
$=$ { $Q(a \cup c \cup d) = Q$, hypothèses 6.3 et lemme 2.45(i). }
$Q \cap Q \triangleright ((a \cup c \cup d) \triangleright (a \cup c \cup d)L)$
$=$ { $ca = cd = \emptyset$, $cc = c$ et $(a \cup c \cup d) \triangleright (a \cup c \cup d)L = L$. }
$Q \cap Q \triangleright L$
$=$ { $Q \triangleright L = L$ et loi booléenne. }
Q

∎

6.2 Démonstration du théorème de réduction

Rappelons que notre but est de prouver le théorème 6.5 ; nous devons donc montrer que la relation d'entrée/sortie $\mathcal{E}(\mathcal{R})$ du diagramme $\mathcal{R}$ est égale à la relation d'entrée/sortie $\mathcal{E}(\mathcal{R}')$ du diagramme $\mathcal{R}' = (aS_P \cup Q, C, e, s)$ (c'est-à-dire que $\mathcal{P}$ a été remplacé par sa relation d'entrée/sortie aS_P (6.13)). En appliquant le corollaire 6.7, on voit que $\mathcal{E}(\mathcal{R}') = e\nu_{\sqsubseteq}(f_r)$, où

(6.16) $f_r(X) := s \cap \overline{(aS_P \cup Q)L} \cup (aS_P \cup Q) \mathbin{▫} X,$

(l'indice r rappelle *r*éduit, étant donné que le diagramme $\mathcal{P}$ a été réduit à sa relation d'entrée/sortie aS_P). Par l'équation 6.11, $\mathcal{E}(\mathcal{R}) = e\nu_{\sqsubseteq}(f_r)$. Il faut donc montrer l'équation suivante :

(6.17) $e\nu_{\sqsubseteq}(f_R) = e\nu_{\sqsubseteq}(f_r).$

Montrons que

(6.18) $f_r(X) = s \cap \overline{QL} \cup (aP \mathbin{▫} S_P \cup Q) \mathbin{▫} X.$

$f_r(X)$
$=$ { Équation 6.16 et loi de De Morgan. }
$s \cap \overline{aS_PL} \cap \overline{QL} \cup (aS_P \cup Q) \mathbin{▫} X$
$=$ { $s \subseteq \overline{aL} \subseteq \overline{aS_PL}$, $aS_P = ac \cup aP \mathbin{▫} S_P$ (car $S_P = f_P(S_P)$ par 6.13) et $ac = \emptyset$. }
$s \cap \overline{QL} \cup (aP \mathbin{▫} S_P \cup Q) \mathbin{▫} X$

Avant de montrer l'équation (6.17), nous prouvons d'abord comme résultat intermédiaire que le plus grand point fixe de f_R (équation 6.9(a)) est égal au plus grand point fixe de la fonction f'_r donnée par

(6.19) $f'_r(X) := s \cap \overline{QL} \cup (P \diamond S_P \cup Q) \diamond X.$

Montrons que la condition sur les domaines est vérifiée, c'est-à-dire que
$(s \cap \overline{QL})L \cap (P \diamond S_P \cup Q)L = \emptyset.$

$$
\begin{array}{ll}
& (s \cap \overline{QL})L \cap (P \diamond S_P \cup Q)L \\
= & \qquad \{ \text{ Théorème 2.21(11,36) et lois booléennes. } \} \\
& sL \cap \overline{QL} \cap (P \diamond S_P)L \\
= & \qquad \{ \ sL \cap (P \diamond S_P)L \subseteq sL \cap (a \cup b)L = \emptyset \text{ (hypothèses 6.3). } \} \\
& \emptyset
\end{array}
$$

(6.20) **Lemme.** *Les plus grands points fixes des fonctions f_R et f'_r (équations 6.9(a) et 6.19) coïncident, c'est-à-dire*

$$\nu_{\sqsubseteq}(f_R) = \nu_{\sqsubseteq}(f'_r).$$

Démonstration. Comme $\nu_{\sqsubseteq}(f_R) = S_R$ (équation 6.11), il suffit de montrer que S_R est le plus grand point fixe de la fonction f'_r. Pour démontrer ce résultat, nous utilisons le théorème de Mills généralisé (4.14). Donc, il suffit de montrer les deux conditions suivantes :

(a) $f'_r(S_R) = S_R$,

(b) $S_R L \subseteq \mathcal{B}(P \diamond S_P \cup Q)$.

Commençons par la condition (a).

$$
\begin{array}{lll}
\text{(a)} & f'_r(S_R) & \\
= & \qquad \{ \text{ Équation 6.19. } \} & \\
& s \cap \overline{QL} \cup (P \diamond S_P \cup Q) \diamond S_R & \\
= & \qquad \{ \ PL \cap QL = \emptyset \text{ (par les hypothèses 6.3) et proposition 3.9(d). } \} & \\
& s \cap \overline{QL} \cup P \diamond S_P \diamond S_R \cup Q \diamond S_R & \\
= & \qquad \{ \text{ Lemme 6.15(a) et } s \subseteq \overline{PL}. \ \} & \\
& s \cap \overline{PL} \cap \overline{QL} \cup P \diamond S_R \cup Q \diamond S_R & \\
= & \qquad \{ \ PL \cap QL = \emptyset, \text{ proposition 3.9(d), loi de De Morgan et } P \cup Q = R. \ \} & \\
& s \cap \overline{RL} \cup R \diamond S_R & \\
= & \qquad \{ \text{ Équations 6.10(a) et 6.11. } \} & \\
& S_R &
\end{array}
$$

(b) $S_R L$

$= \quad$ { Équation 6.10(a). }

$(R^*(s \cap \overline{RL}) \cap \mathcal{A}(R,s) \cap \mathcal{B}(R))L$

$\subseteq \quad$ { Théorème 2.21(36) et loi booléenne. }

$\mathcal{B}(R)$

$\subseteq \quad$ { Lemme 6.14(b). }

$\mathcal{B}(P \triangleleft S_P \cup Q)$

■

Finalement, nous avons les outils nécessaires pour montrer l'équation 6.17.

(6.21) **Lemme.** *Les fonctions f_R et f_r des équations 6.9(a) et 6.18 satisfont*

$$e\nu_{\sqsubseteq}(f_R) = e\nu_{\sqsubseteq}(f_r).$$

Démonstration. Pour démontrer ce théorème, nous utilisons la proposition 2.12(b). Soit $g(X) := (a \cup c \cup d)X$. Montrons d'abord que $g \circ f'_r = f_r$ et $f'_r \circ g = f'_r$.

(a) $(g \circ f'_r)(X)$

$= \quad$ { $g(X) = (a \cup c \cup d)X$ et équation 6.19. }

$(a \cup c \cup d)(s \cap \overline{QL} \cup (P \triangleleft S_P \cup Q) \triangleleft X)$

$= \quad$ { (;) se distribue sur $\cup$. }

$(a \cup c \cup d)(s \cap \overline{QL}) \cup (a \cup c \cup d)(P \triangleleft S_P \cup Q) \triangleleft X$

$= \quad$ { Hypothèses 6.3 ($s \subseteq c \cup d$, $(c \cup d)P = \emptyset$, $aQ = \emptyset$ et $(c \cup d)Q = Q$). }

$s \cap \overline{QL} \cup (aP \triangleleft S_P \cup Q) \triangleleft X$

$= \quad$ { Équation 6.18. }

$f_r(X)$

(b) $(f'_r \circ g)(X)$

$= \quad$ { $g(X) = (a \cup c \cup d)X$. }

$f'_r((a \cup c \cup d)X)$

$= \quad$ { Équation 6.19. }

$s \cap \overline{QL} \cup (P \triangleleft S_P \cup Q) \triangleleft ((a \cup c \cup d)X)$

$= \quad$ { Proposition 3.9(a). }

$s \cap \overline{QL} \cup (P \triangleleft S_P \cup Q) \triangleleft (a \cup c \cup d) \triangleleft X$

$= \quad$ { Proposition 3.9(d) et $\triangleleft$ associative (3.8(i). }

$s \cap \overline{QL} \cup (P \triangleleft S_P \triangleleft (a \cup c \cup d) \cup Q \triangleleft (a \cup c \cup d)) \triangleleft X$

$= \quad$ { Lemme 6.15(b,c). }

$s \cap \overline{QL} \cup (P \triangleleft S_P \cup Q) \triangleleft X$

$$
\begin{array}{ll}
= & \{ \text{ Équation 6.19. } \} \\
f'_r(X) &
\end{array}
$$

Par la proposition 2.12(b) et le résultat (a), nous avons $\nu_{\sqsubseteq}(f_r) = g(\nu_{\sqsubseteq}(f'_r \circ g))$. Par le résultat (b), ceci implique que $\nu_{\sqsubseteq}(f_r) = g(\nu_{\sqsubseteq}(f'_r))$. Par le lemme 6.20, nous déduisons que

(6.22) $\nu_{\sqsubseteq}(f_r) = g(\nu_{\sqsubseteq}(f_R))$.

Cette équation implique le résultat cherché :

$$
\begin{array}{ll}
& e\nu_{\sqsubseteq}(f_R) \\
= & \{ \ e \subseteq a \cup c \cup d \text{ (hypothèses 6.3). } \} \\
& e(a \cup c \cup d)\nu_{\sqsubseteq}(f_R) \\
= & \{ \ g(X) = (a \cup c \cup d)X. \ \} \\
& eg(\nu_{\sqsubseteq}(f_R)) \\
= & \{ \text{ Équation 6.22. } \} \\
& e\nu_{\sqsubseteq}(f_r)
\end{array}
$$

■

Ceci achève la démonstration du théorème 6.5 (voir la discussion qui précède l'équation 6.17). Nous avons prouvé qu'effectivement la relation d'entrée/sortie démoniaque du diagramme $\mathcal{R}$ est égale à la relation d'entrée/sortie du diagramme $\mathcal{R}'$. Le même raisonnement peut être appliqué pour le reste du diagramme $\mathcal{R}$; il suffit d'identifier dans le diagramme $\mathcal{R}'$ un sous-diagramme qui vérifie les hypothèses 6.3 et d'appliquer cette méthode jusqu'à l'obtention des diagrammes élémentaires auxquels nous appliquons les résultats du chapitre 5. Dans la section 6.4, nous allons montrer comment appliquer le théorème 6.5 à certains types de diagrammes.

6.3 Réduction d'une boucle

Notre objectif est de prouver que la relation d'entrée/sortie démoniaque d'un diagramme de boucle (définition 5.8) est égale à la relation d'entrée/sortie démoniaque d'une boucle équivalente que nous allons donner par la suite.

(6.23) **Théorème.** *Soient les diagrammes* $\mathcal{P} = (G \cup P \cup Q, C, e, s)$ *et* $\mathcal{P}' = (GP \cup Q, C, e, s)$ *(comme illustré à la figure 6.4) tels que* G *et* Q *sont déterministes et*

$$G = eGa, \quad P = aPe, \quad Q = eQs, \quad C = \{e, a, s\} \quad \textit{et} \quad GL \cap QL = \emptyset.$$

La relation d'entrée/sortie démoniaque du diagramme $\mathcal{P}$ *est égale à celle du diagramme* $\mathcal{P}'$*, c'est-à-dire*

$$\mathcal{E}(\mathcal{P}) = \mathcal{E}(\mathcal{P}').$$

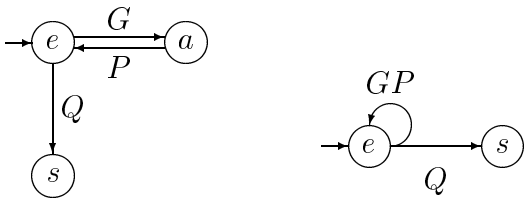


Figure 6.4: Les diagrammes $\mathcal{P}$ et $\mathcal{P}'$

Démonstration. Par le corollaire 6.7, nous avons :

$$\mathcal{E}(\mathcal{P}) = e\nu_{\sqsubseteq}(f),$$

où

$$f(X) := s \cap \overline{GL \cup PL \cup QL} \cup (G \cup P \cup Q) \mathbin{\scriptstyle\square} X.$$

Par le théorème 5.43 (remarquons que $GPL \cap QL = \emptyset$) et l'abréviation 4.7, nous avons

$$\mathcal{E}(\mathcal{P}') = (GP)^*Q \cap (GP)^* \triangleright (GPL \cup QL) \cap \mathcal{B}(GP). \tag{6.24}$$

En appliquant l'équation 5.18, nous allons calculer $\mathcal{E}(\mathcal{P})$ et montrer que cette dernière relation est égale à $\mathcal{E}(\mathcal{P}')$.

Les propriétés $s(G \cup P \cup Q) \subseteq \emptyset$ et $s^\smile = s$ donnent $s(G \cup P \cup Q)L \subseteq \emptyset$; en appliquant la règle de Schröder, nous dérivons aisément $s \subseteq \overline{GL \cup PL \cup QL}$. Donc, l'expression de la fonction f devient :

$$f(X) = s \cup (G \cup P \cup Q) \mathbin{\scriptstyle\square} X.$$

En appliquant le corollaire 6.7 et le théorème 5.43, l'expression de $\mathcal{E}(\mathcal{P})$ est

$$\mathcal{E}(\mathcal{P}) = e(G \cup P \cup Q)^* s \cap e\mathcal{A}(G \cup P \cup Q, s) \cap e\mathcal{B}(G \cup P \cup Q).$$

Simplifions cette expression.

$$\begin{array}{ll} & (G \cup P \cup Q)^* \\ = & \quad \{\ Q(G \cup P) = \emptyset \text{ (car } Q = Qs,\ P = aP,\ G = eG,\ sa = se = \emptyset) \text{ et lemme } \\ & \quad 2.35\text{(e)}.\ \} \\ & (G \cup P)^* Q^* \\ = & \quad \{\ \text{Lemme } 2.35\text{(d)}, \text{ équation } 2.34\text{(b)} \text{ et } Q^2 = \emptyset.\ \} \\ & (G^*P)^* G^* (I \cup Q) \\ = & \quad \{\ \text{Équation } 2.34\text{(b)} \text{ et } G^2 = \emptyset.\ \} \\ & ((I \cup G)P)^* (I \cup G)(I \cup Q) \\ = & \quad \{\ (;) \text{ se distribue sur } \cup,\ GQ = \emptyset.\ \} \\ & (P \cup GP)^* (I \cup G \cup Q) \end{array}$$

$$
\begin{aligned}
&= && \{\ P^2 = \emptyset \text{ et lemme 2.35(e).}\ \}\\
&\quad P^*(GP)^*(I \cup G \cup Q)\\
&= && \{\ \text{Équation 2.34(b) et } P^2 = \emptyset.\ \}\\
&\quad (I \cup P)(GP)^*(I \cup G \cup Q)
\end{aligned}
$$

En utilisant le fait que $G = eGa$, $P = aPe$, $Q = eQs$, la distributivité de (;) sur $\cup$ ainsi que le fait que a, e, s sont des identités partielles deux à deux disjointes, nous déduisons

$$e(G \cup P \cup Q)^* = (GP)^*(e \cup G \cup Q) \tag{6.25}$$

et

$$e(G \cup P \cup Q)^* s = (GP)^* Q. \tag{6.26}$$

Calculons le terme suivant de $\mathcal{E}(\mathcal{P})$, qui est

$$
\begin{aligned}
&\quad e(G \cup P \cup Q)^* \triangleright (sL \cup GL \cup PL \cup QL)\\
&= && \{\ \text{Équation 6.25.}\ \}\\
&\quad (GP)^*(e \cup G \cup Q) \triangleright (sL \cup GL \cup PL \cup QL)\\
&= && \{\ \text{(;) se distribue sur } \cup \text{ et lemme 2.45(g).}\ \}\\
&\quad (GP)^*(e \cup G) \triangleright (sL \cup GL \cup PL \cup QL) \cap (GP)^* Q \triangleright (sL \cup GL \cup PL \cup QL)\\
&= && \{\ \text{Définition 2.44, (;) se distribue sur } \cup,\ Q \triangleright sL = L\ (Q = Qs \text{ et règle de}\\
&&& \quad \text{Schröder}) \text{ et lemme 2.45(n).}\ \}\\
&\quad (GP)^*(e \cup G) \triangleright (sL \cup GL \cup PL \cup QL)\\
&= && \{\ \text{Lemme 2.45(g).}\ \}\\
&\quad (GP)^* e \triangleright (sL \cup GL \cup PL \cup QL) \cap (GP)^* G \triangleright (sL \cup GL \cup PL \cup QL)\\
&= && \{\ \text{Lemme 2.45(i).}\ \}\\
&\quad (GP)^* \triangleright (e \triangleright (sL \cup GL \cup PL \cup QL)) \cap (GP)^* \triangleright (G \triangleright (sL \cup GL \cup PL \cup QL))
\end{aligned}
$$

Par le théorème 2.27(j) (car e est déterministe) et les propriétés $es = \emptyset$, $eG = G$, $eP = \emptyset$, $eQ = Q$, $Gs = \emptyset$, $G^2 = \emptyset$ et $GQ = \emptyset$, nous déduisons

$$e \triangleright (sL \cup GL \cup PL \cup QL) = \overline{eL} \cup GL \cup QL$$

et

$$G \triangleright (sL \cup GL \cup PL \cup QL) = \overline{GL} \cup GPL.$$

Donc,

$$
\begin{aligned}
&\quad (GP)^* \triangleright (e \triangleright (sL \cup GL \cup PL \cup QL)) \cap (GP)^* \triangleright (G \triangleright (sL \cup GL \cup PL \cup QL))\\
&= && \{\ \text{Expressions précédentes.}\ \}\\
&\quad (GP)^* \triangleright (\overline{eL} \cup GL \cup QL) \cap (GP)^* \triangleright (\overline{GL} \cup GPL)\\
&= && \{\ \text{Lemme 2.45(e).}\ \}\\
&\quad (GP)^* \triangleright ((\overline{eL} \cup GL \cup QL) \cap (\overline{GL} \cup GPL))\\
&= && \{\ \text{Lois booléennes, } \overline{eL} \subseteq \overline{GL} \text{ et } QL \subseteq \overline{GL} \text{ (car } GL \cap QL = \emptyset).\ \}\\
&\quad (GP)^* \triangleright (\overline{eL} \cup GPL \cup QL)
\end{aligned}
$$

Par conséquent,

$$
\begin{aligned}
& e\mathcal{A}(G \cup P \cup Q, s) \\
= & \qquad \{ \text{ Abréviation 4.7. } \} \\
& e((G \cup P \cup Q)^* \triangleright (sL \cup GL \cup PL \cup QL)) \\
= & \qquad \{ \text{ Résultats précédents. } \} \\
& e((GP)^* \triangleright (\overline{eL} \cup GPL \cup QL)) \\
= & \qquad \{ \text{ Théorème 2.27(j). } \} \\
& e((GP)^* \triangleright (e \triangleright (GPL \cup QL))) \\
= & \qquad \{ \text{ Lemme 2.45(i) et } e(GP)^*e = e(GP)^* \text{ (équation 2.34, (;) se distribue sur } \cup \text{ et } Pe = P). \} \\
& e((GP)^* \triangleright (GPL \cup QL))
\end{aligned}
$$

$$e\mathcal{A}(G \cup P \cup Q, s) = e((GP)^* \triangleright (GPL \cup QL)). \tag{6.27}$$

Avant de calculer $e\mathcal{B}(G \cup P \cup Q)$, calculons d'abord $\mathcal{B}(G \cup P \cup Q)$.

$$
\begin{aligned}
& \mathcal{B}(G \cup P \cup Q) \\
= & \qquad \{ \text{ Lemme 2.59. } \} \\
& (Q^*(G \cup P))^* \triangleright \mathcal{B}(Q) \cap \mathcal{B}(Q^*(G \cup P)) \\
= & \qquad \{ \mathcal{B}(Q) = L \text{ (car } Q^2 = \emptyset \text{ et proposition 2.54(b)), } R \triangleright L = L \text{ et équation 2.33(b). } \} \\
& \mathcal{B}((I \cup Q)(G \cup P)) \\
= & \qquad \{ \text{ (;) se distribue sur } \cup \text{ et } Q(G \cup P) = \emptyset. \} \\
& \mathcal{B}(G \cup P) \\
= & \qquad \{ \text{ Lemme 2.59. } \} \\
& (G^*P)^* \triangleright \mathcal{B}(G) \cap \mathcal{B}(G^*P) \\
= & \qquad \{ \mathcal{B}(G) = L \text{ (car } G^2 = \emptyset \text{ et proposition 2.54(b)), } R \triangleright L = L, \text{ équation 2.33(b) et (;) se distribue sur } \cup. \} \\
& \mathcal{B}(P \cup GP) \\
= & \qquad \{ \text{ Lemme 2.59. } \} \\
& ((GP)^*P)^* \triangleright \mathcal{B}(GP) \cap \mathcal{B}((GP)^*P) \\
= & \qquad \{ \text{ Équation 2.31. } \} \\
& ((I \cup (GP)^*GP)P)^* \triangleright \mathcal{B}(GP) \cap \mathcal{B}((I \cup (GP)^*GP)P) \\
= & \qquad \{ \text{ (;) se distribue sur } \cup, P^2 = \emptyset \text{ et } \mathcal{B}(P) = L \text{ (car } P^2 = \emptyset \text{ et proposition 2.54(b)). } \} \\
& P^* \triangleright \mathcal{B}(GP)
\end{aligned}
$$

Ceci implique que

$$e\mathcal{B}(G \cup P \cup Q) = \mathcal{B}(GP) \cap eL, \tag{6.28}$$

puisque

$$
\begin{array}{ll}
& e\mathcal{B}(G \cup P \cup Q) \\
= & \qquad \{ \text{ Expression précédente. } \} \\
& e(P^* \triangleright \mathcal{B}(GP)) \\
= & \qquad \{ \text{ Définition 2.44 et théorème 2.27(f). } \} \\
& eP^* \triangleright \mathcal{B}(GP) \cap eL \\
= & \qquad \{ \text{ Équation 2.33(b) et } eP = \emptyset. \} \\
& e \triangleright \mathcal{B}(GP) \cap eL \\
= & \qquad \{ \text{ Théorèmes 2.27(f) et 2.29(f). } \} \\
& \mathcal{B}(GP) \cap eL
\end{array}
$$

En faisant l'intersection des trois termes 6.26, 6.27 et 6.28 et en utilisant l'expression de $\mathcal{E}(\mathcal{P})$ (équation 5.18), nous obtenons :

$$\mathcal{E}(\mathcal{P}) = (GP)^*Q \cap e((GP)^* \triangleright (GPL \cup QL)) \cap \mathcal{B}(GP) \cap eL. \tag{6.29}$$

Montrons que

$$\mathcal{E}(\mathcal{P}) = \mathcal{E}(\mathcal{P}'),$$

où $\mathcal{E}(\mathcal{P}')$ est donnée dans l'équation 6.24.

$$
\begin{array}{ll}
& \mathcal{E}(\mathcal{P}) \\
= & \qquad \{ \text{ Équation 6.29. } \} \\
& (GP)^*Q \cap e((GP)^* \triangleright (GPL \cup QL)) \cap \mathcal{B}(GP) \cap eL \\
= & \qquad \{ \text{ Théorème 2.29(f). } \} \\
& e(GP)^*Q \cap (GP)^* \triangleright (GPL \cup QL) \cap \mathcal{B}(GP) \\
= & \qquad \{ \text{ Équation 6.26. } \} \\
& (GP)^*Q \cap (GP)^* \triangleright (GPL \cup QL) \cap \mathcal{B}(GP) \\
= & \qquad \{ \text{ De léquation 6.24, nous tirons } e(GP)^*Q = (GP)^*Q. \} \\
& \mathcal{E}(\mathcal{P}')
\end{array}
$$

■

6.4 Application

Dans cette section nous allons montrer comment appliquer le théorème 6.5 afin de calculer la relation d'entrée/sortie de certains diagrammes composés.

Ces résultats vont nous servir dans le prochain chapitre où nous aurons à calculer la relation d'entrée/sortie des diagrammes composés correspondant aux instructions du langage des commandes gardées.

6.4.1 Séquence

Soient les diagrammes $\mathcal{P}$, $\mathcal{P}_1$ et $\mathcal{P}_2$ tels que

$$\begin{aligned}\mathcal{P} &= (P_1 \cup P_2, C, e_1, s_2),\\ \mathcal{P}_1 &= (P_1, C_1, e_1, s_1),\\ \mathcal{P}_2 &= (P_2, C_2, s_1, s_2)\end{aligned}$$

où

$$C = C_1 \cup C_2, \quad (\bigcup C_1) \cap (\bigcup C_2) = s_1 \quad \text{et} \quad s_1 \subseteq \overline{P_1 L}.$$

Supposons que les diagrammes $\mathcal{P}_1$ et $\mathcal{P}_2$ ne sont pas atomiques. Notre but est de calculer la relation d'entrée/sortie $\mathcal{E}(\mathcal{P})$ du diagramme $\mathcal{P}$ en appliquant le théorème 6.5 et les résultats du chapitre 5. Pour celà, nous allons réduire P_1 et P_2 de manière à obtenir un diagramme de séquence (5.4). Considérons les substitutions suivantes où les variables à gauche sont celles du théorème 6.5 :

(6.30) **Substitutions.**

$$\begin{aligned} a &:= e_1, & P &:= P_1,\\ b &:= (\bigcup C_1) \cap \overline{e_1 \cup s_1}, & Q &:= P_2,\\ c &:= s_1, & e &:= e_1,\\ d &:= (\bigcup C_2) \cap \overline{s_1}, & s &:= s_2. \end{aligned}$$

La relation $(\bigcup C_1) \cap \overline{e_1 \cup s_1}$ représente les points de contrôle du diagramme $\mathcal{P}_1$ qui sont différents des points d'entrée et de sortie (c'est-à-dire les points internes). En utilisant $cP = \emptyset$ ainsi que les propriétés vérifiés par a, b, nous obtenons $(a \cup b)P(a \cup b \cup c) = (\bigcup C_1)P(\bigcup C_1) = P$. Il n'est pas difficile de vérifier que les hypothèses 6.3 sont satisfaites. Par le théorème 6.5, nous avons alors

(6.31) $\mathcal{E}(\mathcal{P}) = \mathcal{E}(\mathcal{E}(\mathcal{P}_1) \cup P_2, C', e, s),$

où $C' = C_2 \cup \{e_1\}$.

Par hypothèse, $\mathcal{P}_2 = (P_2, C_2, s_1, s_2)$ est un diagramme ; nous pouvons procéder de la même façon et appliquer une autre fois le théorème 6.5 au nouveau diagramme $(\mathcal{E}(\mathcal{P}_1) \cup P_2, C, e, s)$ pour obtenir

$$\mathcal{E}(\mathcal{P}) = \mathcal{E}(\mathcal{P}'),$$

où

$$\mathcal{P}' = (\mathcal{E}(\mathcal{P}_1) \cup \mathcal{E}(\mathcal{P}_2), C'', e_1, s_2),$$

où $C'' = \{e_1, s_1, s_2\}$.

Par définition de $\mathcal{E}$, $\mathcal{P}_1$ et $\mathcal{P}_2$, nous avons $\mathcal{E}(\mathcal{P}_1) = e_1\mathcal{E}(\mathcal{P}_1)s_1$ et $\mathcal{E}(\mathcal{P}_2) = s_1\mathcal{E}(\mathcal{P}_2)s_2$. Donc, $\mathcal{P}'$ est un diagramme de séquence (définition 5.4). En appliquant l'équation 5.33, nous obtenons :

(6.32) $\mathcal{E}(\mathcal{P}) = \mathcal{E}(\mathcal{P}_1) \diamond \mathcal{E}(\mathcal{P}_2).$

6.4.2 Choix

Considérons les diagrammes

$$\mathcal{P} = (P, C, e, s)$$
$$\mathcal{P}_1 = (P_1, C_1, e_1, s),$$
$$\mathcal{P}_2 = (P_2, C_2, e_2, s),$$

où

$$C = C_1 \cup C_2 \cup \{e\}, \quad P = G_1 \cup P_1 \cup G_2 \cup P_2, \quad G_1 = eG_1e_1, \quad G_2 = eG_2e_2$$
$$(\bigcup C_1) \cap (\bigcup C_2) = s, \quad s_1 \subseteq \overline{P_1 L}, \quad s_2 \subseteq \overline{P_2 L}.$$

Notre but est de réduire P_1 et P_2 pour obtenir un diagramme de choix (définition 5.6). Suivons la même méthode que pour la séquence.

(6.33) **Substitutions.**

$$a := e_1, \qquad P := P_1,$$
$$b := (\bigcup C_1) \cap \overline{e_1 \cup s}, \qquad Q := G_1 \cup G_2 \cup P_2,$$
$$c := s, \qquad e := e,$$
$$d := (\bigcup C_2 \cup e) \cap \overline{s} \qquad s := s.$$

En considérant ces notations et les propriétés vérifiées par les gardes G_1 et G_2 ainsi que les diagrammes $\mathcal{P}_1$ et $\mathcal{P}_2$, il est facile de voir que les hypothèses 6.3 sont satisfaites. Donc, le théorème 6.5 est applicable et nous avons

$$\mathcal{E}(\mathcal{P}) = \mathcal{E}(\mathcal{P}')$$

où

$$\mathcal{P}' = (\mathcal{E}(\mathcal{P}_1) \cup P_2 \cup G_1 \cup G_2, C', e, s)$$

et $C' = C_2 \cup \{e, e_1\}$.

Par hypothèse, $\mathcal{P}_2 = (P_2, C_2, e_2, s)$ est un diagramme ; nous pouvons appliquer une autre fois le théorème 6.5 au diagramme $\mathcal{P}'$ pour obtenir le diagramme

$$(\mathcal{E}(\mathcal{P}_1) \cup \mathcal{E}(\mathcal{P}_2) \cup G_1 \cup G_2, \{e, e_1, e_2, s\}, e, s).$$

Par définition de $\mathcal{E}$, les diagrammes $\mathcal{P}_1$ et $\mathcal{P}_2$ vérifient $\mathcal{E}(\mathcal{P}_1) = e_1\mathcal{E}(\mathcal{P}_1)s$ et $\mathcal{E}(\mathcal{P}_2) = e_2\mathcal{E}(\mathcal{P}_2)s$. Par conséquent, $(\mathcal{E}(\mathcal{P}_1) \cup \mathcal{E}(\mathcal{P}_2) \cup G_1 \cup G_2, \{e, e_1, e_2, s\}, e, s)$ est un diagramme de choix (définition 5.6). Par application de l'équation 5.31, nous déduisons que :

(6.34) $\mathcal{E}(\mathcal{P}) = G_1 \triangleleft \mathcal{E}(\mathcal{P}_1) \cap G_2 \triangleright \mathcal{E}(\mathcal{P}_2)L \cup G_2 \triangleleft \mathcal{E}(\mathcal{P}_2) \cap G_1 \triangleright \mathcal{E}(\mathcal{P}_1)L.$

Si les gardes G_1 et G_2 sont des identités partielles, nous appliquons la proposition 5.32(d) et l'équation précédente devient

(6.35) $\mathcal{E}(\mathcal{P}) = G_2^{\sim} \triangleleft G_1 \triangleleft \mathcal{E}(\mathcal{P}_1) \sqcap G_1^{\sim} \triangleleft G_2 \triangleleft \mathcal{E}(\mathcal{P}_2) \sqcap G_1 \triangleleft G_2 \triangleleft (\mathcal{E}(\mathcal{P}_1) \sqcup \mathcal{E}(\mathcal{P}_2)).$

6.4.3 Boucle

Finalement, nous considérons les diagrammes

$$\mathcal{W} = (W, C, s_1, s),$$
$$\mathcal{P} = (P, C_1, e_1, s_1),$$

où

$$W = G \cup P \cup Q, \qquad G = s_1 G e_1, \quad Q = s_1 Q s, \quad GL \cap QL = \emptyset,$$
$$s_1 \subseteq \overline{PL}, \quad C = C_1 \cup \{s\} \qquad .$$

Supposons de plus que les relations G et Q sont déterministes.

Notre but est de réduire les diagrammes $\mathcal{W}$ et $\mathcal{P}$ pour obtenir un diagramme de boucle. Afin d'appliquer le théorème 6.5, définissons les substitutions appropriées.

(6.36) **Substitutions.**

$$a := e_1, \qquad P := P,$$
$$b := (\bigcup C_1) \cap \overline{e_1 \cup s_1}, \qquad Q := G \cup Q,$$
$$c := s_1, \qquad e := s_1,$$
$$d := s \qquad s := s.$$

En considérant ces notations ainsi que les propriétés vérifiées par P et les gardes G et Q, il n'est pas difficile de prouver que les hypothèses 6.3 sont satisfaites. Par conséquent, en appliquant le théorème 6.5, nous obtenons :

$$\mathcal{P}' = (G \cup \mathcal{E}(\mathcal{P}) \cup Q, \{e, e_1, s\}, e, s).$$

Par définition de $\mathcal{E}$, $\mathcal{P}$ et des gardes G et Q, nous avons

$$G = eGe_1, \quad \mathcal{E}(\mathcal{P}) = e_1 \mathcal{E}(\mathcal{P}) e, \quad Q = eQs, \quad \text{et} \quad GL \cap QL = \emptyset.$$

Par application du théorème 6.23, nous déduisons que

$$\mathcal{E}(\mathcal{P}') = \mathcal{E}(\mathcal{P}''),$$

où

$$\mathcal{P}'' = (G\mathcal{E}(\mathcal{P}) \cup Q, \{e, e_1, s\}, e, s).$$

Par définition de $\mathcal{E}$, G et $\mathcal{P}$, nous avons $G\mathcal{E}(\mathcal{P}) = eG\mathcal{E}(\mathcal{P})e$ et $Q = eQs$. Ceci implique que le diagramme $\mathcal{P}''$ est un diagramme de boucle (définition 5.8). Par application de l'équation 5.39, nous avons :

(6.37) $\mathcal{E}(\mathcal{P}'') = (G\mathcal{E}(\mathcal{P}))^* Q \cap \mathcal{A}(G\mathcal{E}(\mathcal{P}), Q) \cap \mathcal{B}(G\mathcal{E}(\mathcal{P}))$.

Finalement, nous concluons que

$$\mathcal{E}(\mathcal{W}) = \mathcal{E}(\mathcal{P}'').$$

6.5 Conclusion

Dans ce chapitre nous avons montré comment calculer la relation d'entrée/sortie démoniaque des diagrammes composés. Notre résultat principal est le théorème 6.5, dans lequel nous montrons que la relation d'entrée/sortie d'un diagramme composé est égale à celle d'un diagramme où chaque sous-diagramme est remplacé par sa relation d'entrée/sortie, jusqu'à l'obtention des diagrammes élémentaires auxquels nous appliquons les résultats du chapitre 5. Pour prouver ce théorème, nous avons présenté plusieurs résultats intermédiaires, quelques-uns ayant été démontrés par l'intermédiaire du théorème de Mills généralisé 4.14. Nous avons donné un résultat utile (théorème 6.23) sur la réduction d'une boucle : la relation d'entrée/sortie d'un diagramme de boucle avec trois branches est égale à la relation d'entrée/sortie du diagramme avec un arc (boucle) et une branche (voir la figure 6.4). Dans la section 6.4, nous avons appliqué le théorème (6.5) à des diagrammes composés correspondant aux instructions du langage des commandes gardées dont les étapes (à part les gardes) ne sont pas nécessairement atomiques. Les résultats de cette dernière section vont nous être utiles pour montrer que la sémantique dénotationnelle démoniaque d'un programme est égale à sa sémantique opérationnelle démoniaque, que nous allons définir dans le prochain chapitre. Dans les chapitres 5 et 6, nous avons donc montré comment associer à un diagramme sa relation d'entrée/sortie démoniaque ; nous avons traité la flèche qui concerne la fonction $\mathcal{E}$ dans le diagramme de la figure 1.1.

Chapitre 7

Sémantique opérationnelle

Dans les chapitres 5 et 6, nous avons défini la notion de diagramme et celle de relation d'entrée/sortie démoniaque d'un diagramme. En partant de ces notions, nous allons définir la sémantique opérationnelle démoniaque des programmes séquentiels non déterministes. Les programmes et le langage sont les mêmes que ceux utilisés pour définir la sémantique dénotationnelle démoniaque (section 3.2), c'est-à-dire que nous considérons des programmes impératifs et le langage des commandes gardées de Dijkstra [30], qui permet l'expression du non-déterminisme.

L'autre objectif de ce chapitre est de montrer que la sémantique opérationnelle démoniaque d'un programme séquentiel non déterministe est égale à sa sémantique dénotationnelle démoniaque.

Dans la section suivante, nous présentons des résultats préliminaires utiles pour ce chapitre.

7.1 Résultats préliminaires

Notons que le lemme suivant aurait pu être présenté dans le chapitre 2. Étant donné qu'il ne sert que dans ce chapitre, nous avons préféré le mettre ici.

(7.1) **Lemme.** *Soient les relations P, Q, R, S et (π_1, π_2) un produit.*

(a) $[P,Q] \triangleright \pi_1 R \breve{\pi_1} = [P \triangleright R, L] \cup [L, \overline{QL}]$,

(b) $[P,Q] \triangleright \pi_2 R \breve{\pi_2} = [L, Q \triangleright R] \cup [\overline{PL}, L]$,

(c) $[P,Q] \triangleright [R,S] = [P \triangleright R, Q \triangleright S] \cup [\overline{PL}, L] \cup [L, \overline{QL}]$,

(d) $[P,Q] \square [R,S] = [P \square R, Q \square S]$

Démonstration.

(a)
$$
\begin{aligned}
& [P,Q] \triangleright \pi_1 R \pi_1^{\smile} \\
= & \quad \{ \text{ Définitions 2.36, 2.44 et théorème 2.27(g). } \} \\
& [P,Q]\pi_1 \triangleright R\pi_1^{\smile} \\
= & \quad \{ \text{ Lemme 2.40(e). } \} \\
& (\pi_1 P \cap \pi_2 QL) \triangleright R\pi_1^{\smile} \\
= & \quad \{ \text{ Lemme 2.45(j). } \} \\
& \pi_1 P \triangleright R\pi_1^{\smile} \cup \overline{\pi_2 QL} \\
= & \quad \{ \text{ Définition 2.36 et théorème 2.27(g). } \} \\
& \pi_1 P \triangleright R\pi_1^{\smile} \cup \pi_2 \overline{QL} \\
= & \quad \{ \text{ Définition 2.44, théorème 2.27(g, i), } \pi_i L = L\pi_i^{\smile} = L, \text{ où } i = 1,2, \\
& \quad \text{définition 2.36 et lois booléennes. } \} \\
& \pi_1(P \triangleright R)\pi_1^{\smile} \cap \pi_2 L\pi_2^{\smile} \cup \pi_1 L\pi_1^{\smile} \cap \pi_2 \overline{QL}\pi_2^{\smile} \\
= & \quad \{ \text{ Définition 2.38. } \} \\
& [P \triangleright R, L] \cup [L, \overline{QL}]
\end{aligned}
$$

(b) Se démontre d'une manière similaire.

(c)
$$
\begin{aligned}
& [P,Q] \triangleright [R,S] \\
= & \quad \{ \text{ Définition 2.38 et lemme 2.45(e). } \} \\
& [P,Q] \triangleright \pi_1 R\pi_1^{\smile} \cap [P,Q] \triangleright \pi_2 S\pi_2^{\smile} \\
= & \quad \{ \text{ Lemme 7.1(a,b). } \} \\
& ([P \triangleright R, L] \cup [L, \overline{QL}]) \cap ([L, Q \triangleright S] \cup [\overline{PL}, L]) \\
= & \quad \{ \text{ Lemme 2.40(a) et lois booléennes. } \} \\
& [P \triangleright R, Q \triangleright S] \cup [P \triangleright R \cap \overline{PL}, L] \cup [L, \overline{QL} \cap Q \triangleright S] \cup [\overline{PL}, \overline{QL}] \\
= & \quad \{ \overline{PL} \subseteq P \triangleright R, \text{ de même } \overline{QL} \subseteq Q \triangleright S. \} \\
& [P \triangleright R, Q \triangleright S] \cup [\overline{PL}, L] \cup [L, \overline{QL}] \cup [\overline{PL}, \overline{QL}] \\
= & \quad \{ \text{ Lemme 2.40(c), } \overline{PL} \subseteq L \text{ et } \overline{QL} \subseteq L. \} \\
& [P \triangleright R, Q \triangleright S] \cup [\overline{PL}, L] \cup [L, \overline{QL}]
\end{aligned}
$$

(d)
$$
\begin{aligned}
& [P,Q] \triangleleft [R,S] \\
= & \quad \{ \text{ Définition 3.7. } \} \\
& [P,Q][R,S] \cap [P,Q] \triangleright [R,S]L \\
= & \quad \{ \text{ Lemme 2.40(d,j). } \} \\
& [PR, QS] \cap [P,Q] \triangleright [RL, SL] \\
= & \quad \{ \text{ Lemme 7.1(c). } \} \\
& [PR, QS] \cap ([P \triangleright RL, Q \triangleright SL] \cup [\overline{PL}, L] \cup [L, \overline{QL}]) \\
= & \quad \{ \text{ Lemme 2.40(a) et } PR \subseteq PL,\ QS \subseteq QL \text{ et lois booléennes. } \}
\end{aligned}
$$

$$
\begin{aligned}
& [PR \cap P \triangleright RL, QS \cap Q \triangleright SL] \\
= & \qquad \{ \text{ Définition 3.7. } \} \\
& [P \,\square\, R, Q \,\square\, S].
\end{aligned}
$$

■

(7.2) **Lemme.** *Soient $\mathcal{P} = (P, C, e, s)$ un diagramme et σ une relation telle que $\sigma\sigma^{\smile} = I$ et $\sigma^{\smile}\sigma \subseteq I$.*

(a) $\mathcal{P}_\sigma := (\sigma^{\smile}P\sigma, \sigma^{\smile}C\sigma, \sigma^{\smile}e\sigma, \sigma^{\smile}s\sigma)$, où $\sigma^{\smile}C\sigma := \{\sigma^{\smile}c\sigma : c \in C\}$, est un diagramme.

(b) $\mathcal{E}(\mathcal{P}_\sigma) = \sigma^{\smile}\mathcal{E}(\mathcal{P})\sigma$.

Démonstration.

(a) Montrons que $\mathcal{P}_\sigma$ est un diagramme (définition 5.1) ; il nous faut donc montrer que les éléments de $\sigma^{\smile}C\sigma$ sont des identités partielles deux à deux disjointes, $\sigma^{\smile}e\sigma$ et $\sigma^{\smile}s\sigma \in \sigma^{\smile}C\sigma$ (ce qui est vrai car e et s sont des éléments de C) et finalement que

$$(\bigcup \sigma^{\smile}C\sigma)\sigma^{\smile}P\sigma(\bigcup \sigma^{\smile}C\sigma) = \sigma^{\smile}P\sigma.$$

- Soit $c \in C$. Par hypothèse, $c \subseteq I$ et $\sigma^{\smile}\sigma \subseteq I$, par conséquent $\sigma^{\smile}c\sigma \subseteq I$.
- Soient c_1 et c_2, deux éléments de l'ensemble C tels que $c_1 \neq c_2$. On trouve que $\sigma^{\smile}c_1\sigma\sigma^{\smile}c_2\sigma = \emptyset$ car $\sigma\sigma^{\smile} = I$ et $c_1c_2 = \emptyset$ (c_1 et c_2 sont disjoints par définition de C).
- Comme (;) se distribue sur $\cup$ à droite et à gauche, nous déduisons que

  $$\bigcup(\sigma^{\smile}C\sigma) = \sigma^{\smile}(\bigcup C)\sigma.$$

  Par conséquent,

  $$(\bigcup \sigma^{\smile}C\sigma)\sigma^{\smile}P\sigma(\cup\sigma^{\smile}C\sigma) = \sigma^{\smile}(\bigcup C)\sigma\sigma^{\smile}P\sigma\sigma^{\smile}(\cup C)\sigma.$$

  Étant donné que $\sigma\sigma^{\smile} = I$ et $(\bigcup C)P(\bigcup C) = P$, nous concluons que

  $$(\bigcup \sigma^{\smile}C\sigma)\sigma^{\smile}P\sigma(\bigcup \sigma^{\smile}C\sigma) = \sigma^{\smile}P\sigma.$$

Ainsi, nous avons prouvé que $\mathcal{P}_\sigma$ est un diagramme.

(b) Posons

$$f(X) := \sigma^{\smile}s\sigma \cap \overline{\sigma^{\smile}PL} \cup (\sigma^{\smile}P\sigma) \,\square\, X, \quad g(X) := s \cap \overline{PL} \cup P \,\square\, X. \tag{7.3}$$

En utilisant le corollaire 6.7, nous avons

$$\mathcal{E}(\mathcal{P}_\sigma) = \sigma^{\smile}e\sigma\nu_{\sqsubseteq}(f), \tag{7.4}$$

et

$$\mathcal{E}(\mathcal{P}) = e\nu_{\sqsubseteq}(g). \tag{7.5}$$

En utilisant les équations 7.4 et 7.5, l'équation 7.2(b) qu'il faut démontrer, devient

$$\sigma^{\smile} e\sigma\nu_{\sqsubseteq}(f) = \sigma^{\smile} e\nu_{\sqsubseteq}(g)\sigma. \tag{7.6}$$

Tout d'abord montrons que

$$\nu_{\sqsubseteq}(f) = \sigma^{\smile}\nu_{\sqsubseteq}(g)\sigma. \tag{7.7}$$

Pour prouver cette équation, nous appliquons la proposition 2.12(d). Soit la fonction h définie par

$$h(X) := \sigma^{\smile} X\sigma. \tag{7.8}$$

Vérifions premièrement que $f \circ h = h \circ g$.

$$\begin{aligned}
& f(h(X)) \\
= & \quad \{ \text{ Équations 7.3 et 7.8. } \} \\
& \sigma^{\smile} s\sigma \cap \overline{\sigma^{\smile} PL} \cup (\sigma^{\smile} P\sigma) \triangleleft (\sigma^{\smile} X\sigma) \\
= & \quad \{ \text{ Théorème 2.27(g,j) } (\sigma \text{ application et } \sigma^{\smile} \text{ déterministe}) \text{ et définition} \\
& \quad 3.7\ (\triangleleft). \} \\
& \sigma^{\smile} s\sigma \cap (\sigma^{\smile}\overline{PL} \cup \overline{\sigma^{\smile} L}) \cup \sigma^{\smile} P\sigma\sigma^{\smile} X\sigma \cap (\sigma^{\smile} P) \triangleright (\sigma\sigma^{\smile} X\sigma L) \\
= & \quad \{ \text{ Loi booléenne, } \sigma^{\smile} s\sigma \subseteq \sigma^{\smile} L, \ , \ \sigma\sigma^{\smile} = I, \text{ définition 3.7 } (\triangleleft) \text{ et propo-} \\
& \quad \text{sition 3.9(a,c). } \} \\
& \sigma^{\smile} s\sigma \cap \sigma^{\smile}\overline{PL} \cup (\sigma^{\smile} \triangleleft P) \triangleleft (X \triangleleft \sigma) \\
= & \quad \{ \text{ Théorème 3.8(i) et proposition 3.9(a,c). } \} \\
& \sigma^{\smile} s\sigma \cap \sigma^{\smile}\overline{PL} \cup \sigma^{\smile}(P \triangleleft X)\sigma \\
= & \quad \{ \text{ Théorème 2.27(a), théorème 2.21(36) et } (;) \text{ se distribue sur } \cup. \} \\
& \sigma^{\smile}(s \cap \overline{PL} \cup P \triangleleft X)\sigma \\
= & \quad \{ \text{ Équations 7.3 et 7.8. } \} \\
& h(g(X))
\end{aligned}$$

Par la proposition 2.12(d), nous déduisons que $\nu_{\sqsubseteq}(f) = h(\nu_{\sqsubseteq}(g))$. En remplaçant h par son expression (voir 7.8), nous obtenons l'équation 7.7.

En composant chaque membre de l'équation 7.7 par la relation $\sigma^{\smile} e\sigma$ et en utilisant le fait que $\sigma\sigma^{\smile} = I$, nous obtenons l'équation 7.6.

Ainsi nous avons prouvé que la relation d'entrée/sortie du diagramme $\mathcal{P}_\sigma$ est égale à $\sigma^{\smile}\mathcal{E}(\mathcal{P})\sigma$. ∎

7.2 Sémantique opérationnelle démoniaque

Dans ce qui suit, nous définissons la sémantique opérationnelle démoniaque d'un programme.

Soit une algèbre de relations $\mathrm{Rel}(\mathbf{N}\times S)$ (voir 2.19(b)), où $\mathbf{N}$ est l'ensemble des entiers naturels. Les entiers représentent les sommets du graphe représentant le programme p et S est l'ensemble des états de ce programme.

Tout d'abord introduisons quelques fonctions utiles pour définir la sémantique opérationnelle.

(a) Les projections $\pi_1 : \mathbf{N} \times S \to \mathbf{N}$ et $\pi_2 : \mathbf{N} \times S \to S$. La paire (π_1, π_2) forme un produit direct. Tout au long de ce chapitre, les produits cartésiens considérés (définition 2.38) sont relatifs à (π_1, π_2).

(b) La fonction $\mathcal{Q}$, qui va de l'ensemble des programmes vers l'ensemble des diagrammes associe donc à chaque programme p le diagramme $\mathcal{Q}[\![p]\!] = (P, C, e, s)$ où P est un élément de l'algèbre $\mathrm{Rel}(\mathbf{N} \times S)$. Pour un exemple voir 5.2.

(c) La fonction $\mathcal{F}$: $\mathrm{Rel}(\mathbf{N} \times S) \to \mathrm{Rel}(S)$ associe à chaque relation X la relation $\mathcal{F}(X) = \pi_2^{\smile} X \pi_2$. La fonction $\mathcal{F}$ associe à chaque relation sur $\mathbf{N} \times S$ sa projection sur S. Posons

$$\mathcal{O} := \mathcal{F} \circ \mathcal{E} \circ \mathcal{Q}. \tag{7.9}$$

La sémantique opérationnelle démoniaque d'un programme p est donnée par la relation $\mathcal{O}[\![p]\!] = \mathcal{F}(\mathcal{E}(\mathcal{Q}[\![p]\!]))$.

Par conséquent, $\mathcal{O}$ est une fonction de l'ensemble des programmes vers l'algèbre de relations $\mathrm{Rel}(S)$.

Notons que la présence de l'opération $*$ dans l'expression $\mathcal{E}(\mathcal{Q}[\![p]\!]) = eP^*(s \cap \overline{PL}) \cap eP^*\triangleright(PL \cup sL) \cap e\mathcal{B}(P)$ permet de décrire comment les données initiales sont transformées pendant l'exécution du diagramme $\mathcal{Q}[\![p]\!]$. La projection de la relation $\mathcal{E}(\mathcal{Q}[\![p]\!])$ règle un problème de type: la sémantique d'un programme p est donnée par une relation sur l'ensemble des états S, tandis que la relation d'entrée/sortie du diagramme $\mathcal{Q}[\![p]\!]$ est une relation sur l'ensemble $\mathbf{N} \times S$; la fonction $\mathcal{F}$ permet d'éliminer la composante des points de contrôle $\mathbf{N}$.

7.3 Comparaison des sémantiques

Notre objectif dans cette section est de comparer les sémantiques opérationnelle et dénotationnelle. Plus exactement, nous allons montrer leur égalité, ce qui revient à prouver que tout programme p vérifie

$$\mathcal{D}[\![p]\!] = \mathcal{O}[\![p]\!]. \tag{7.10}$$

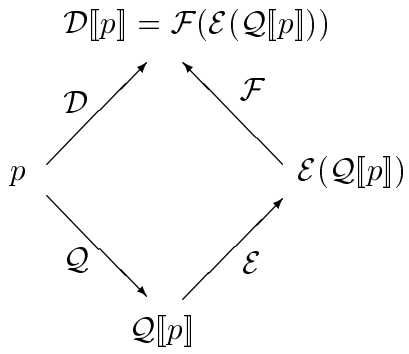


Figure 7.1: $\mathcal{O}[\![p]\!] := \mathcal{F}(\mathcal{E}(\mathcal{Q}[\![p]\!])) = \mathcal{D}[\![p]\!]$

Ceci est équivalent à montrer que le diagramme (dans le sens conventionnel du terme) de la figure 7.1 commute.

Autrement dit, nous devons montrer qu'à chaque programme p est associé un diagramme $\mathcal{Q}[\![p]\!]$ et que la projection par la fonction $\mathcal{F}$ de la relation d'entrée/sortie $\mathcal{E}(\mathcal{Q}[\![p]\!])$ du diagramme $\mathcal{Q}[\![p]\!]$ est égale à la sémantique dénotationnelle démoniaque $\mathcal{D}[\![p]\!]$ du programme p.

(7.11) **Remarque.** Comme nous considérons l'algèbre de relations $\mathrm{Rel}(\mathbf{N} \times S)$ (voir 2.19(b)), où $\mathbf{N}$ est l'ensemble des entiers naturels et S est l'ensemble des états du programme, P est une relation sur $\mathbf{N} \times S$ et les éléments de l'ensemble C sont de la forme $[xx^{\smile}, I]$ où x est une relation sur $\mathbf{N}$ qui représente un point de contrôle du programme p (voir exemple 5.2). Par exemple, la relation

$$0 := \{(0, n) \mid n \in \mathbf{N}\}$$

est la relation qui repésente le point de contrôle 0 du programme. Cette relation est un point (voir définition 2.23(h)).

Il convient de noter qu'en utilisant la définition 2.23(h), la remarque 2.24 et le lemme 2.40(j), il n'est pas difficile de prouver que les éléments de C sont des identités partielles deux à deux disjointes. La relation $[xy^{\smile}, Q]$ sur $\mathbf{N} \times S$ nous indique qu'il y a une transition du point de contrôle x au point de contrôle y et que le changement d'état qui accompagne le passage de x à y est décrit par la relation Q. Les relations e et s sont données par $[xx^{\smile}, I]$ et $[yy^{\smile}, I]$ où x et y sont respectivement le point de contrôle initial et le point de contrôle final (ou terminal) du programme p. ∎

Soient x et y des points sur $\mathbf{N}$, tels que $e = [xx^{\smile}, I]$ et $s = [yy^{\smile}, I]$. Montrons que l'équation

(7.12) $\mathcal{E}(\mathcal{Q}[\![p]\!]) = [xy^{\smile}, \mathcal{D}[\![p]\!]]$

implique l'équation 7.10.

$$
\begin{aligned}
& \mathcal{O}[\![p]\!] \\
= & \qquad \{ \text{ Définition 7.9. } \} \\
& \mathcal{F}(\mathcal{E}(\mathcal{Q}[\![p]\!])) \\
= & \qquad \{ \text{ Définition de } \mathcal{F} \text{ et équation 7.12. } \} \\
& \pi_2^{\smile}[xy^{\smile}, \mathcal{D}[\![p]\!]]\pi_2 \\
= & \qquad \{ \text{ Lemme 2.40(h) et } xy^{\smile} \neq \emptyset \text{ (règle de Tarski). } \} \\
& \mathcal{D}[\![p]\!]
\end{aligned}
$$

Par conséquent, au lieu de prouver l'équation 7.10, il suffit de prouver que l'équation 7.12 est vérifiée par tout programme p (c'est-à-dire qu'il existe des points x, y tels que l'égalité est vérifiée). Étant donné que les affectations sont des programmes atomiques et que les constructeurs de séquence, de choix gardé et de boucle permettent de construire les programmes complexes, nous allons définir l'affectation pour qu'elle vérifie l'équation 7.12. Ensuite, nous définissons la fonction $\mathcal{Q}[\![p]\!]$ inductivement de manière appropriée et nous montrons que si p est obtenu par application des constructeurs à des programmes qui satisfont l'équation 7.12, alors p satisfait l'équation 7.12.

7.3.1 Affectation

Considérons l'affectation donnée dans la section 3.2,

$$x_i := f(x),$$

où $0 \leq i \leq n$, $x = (x_0, \ldots, x_n)$. Il est facile de voir que le diagramme associé à l'affectation est atomique. Les entiers 0 et 1 dénotent les sommets du graphe et $\mathcal{D}[\![x_i := f(x)]\!]$ (voir l'équation 3.13) est la relation qui accompagne le changement de 0 à 1. En utilisant la définition du produit direct (voir 2.36) nous avons

$$\mathcal{E}(\mathcal{Q}[\![x_i := f(x)]\!]) = [01^{\smile}, \mathcal{D}[\![x_i := f(x)]\!]], \tag{7.13}$$

où 0 et 1 sont respectivement le point de contrôle initial et le point de contrôle final de l'affectation en question.

Avant de traiter les autres cas, nous décrivons la méthode que nous allons suivre pour montrer que les autres constructeurs vérifient l'hypothèse d'induction 7.12. En premier lieu, en utilisant la notion de somme directe, nous combinons les diagrammes associés aux programmes donnés par hypothèse. Ensuite, nous montrons que le quadruplet obtenu est effectivement un diagramme. La troisième étape consiste à calculer la relation d'entrée/sortie du nouveau diagramme. Finalement, nous supposons que l'hypothèse d'induction 7.12 est vérifiée par les diagrammes donnés par hypothèse et nous vérifions que le nouveau diagramme satisfait aussi l'équation 7.12.

Le prochain cas que nous traitons est celui de la séquence.

7.3.2 Séquence

Soient p_1, p_2 deux programmes et $\mathcal{Q}[\![p_1]\!] = (P_1, C_1, e_1, s_1)$, $\mathcal{Q}[\![p_2]\!] = (P_2, C_2, e_2, s_2)$ les diagrammes associés respectivement à ces programmes. Les relations d'entrée e_1 et e_2 et

les relations de sortie s_1 et s_2 des diagrammes $\mathcal{Q}[\![p_1]\!]$ et $\mathcal{Q}[\![p_2]\!]$ sont respectivement (voir remarque 7.11) :

$$(7.14)\quad e_1 = [x_1 x_1^{\smile}, I],\quad s_1 = [y_1 y_1^{\smile}, I],\quad e_2 = [x_2 x_2^{\smile}, I],\quad s_2 = [y_2 y_2^{\smile}, I],$$

où x_1, y_1, x_2 et y_2 sont des points sur $\mathbf{N}$ représentant respectivement les points de contrôle initiaux et finaux des programmes p_1 et p_2.

Notre but ici est de coller en séquence les diagrammes $\mathcal{Q}[\![p_1]\!]$ et $\mathcal{Q}[\![p_2]\!]$ de manière que le point de sortie du programme p_1 coïncide avec le point d'entrée du programme p_2 (voir le graphe 5.5). Cela se fait en renommant les points de contrôle des deux diagrammes de manière à ce qu'ils soient distincts, sauf que le point de sortie de p_1 est renommé de la même manière que le point d'entrée de p_2. Le renommage se fait au moyen des injections σ_1 et σ_2. L'idée de base est simple, même si les détails techniques sont un peu lourds.

Les relations σ_1 et σ_2 vérifient les conditions suivantes :

$$(7.15)\quad \sigma_1\sigma_1^{\smile} = I,\qquad \sigma_2\sigma_2^{\smile} = I,\qquad \sigma_1\sigma_2^{\smile} = y_1 x_2^{\smile},\qquad \sigma_1^{\smile}\sigma_1 \subseteq I,\qquad \sigma_2^{\smile}\sigma_2 \subseteq I,$$

ce qui signifie que les relations σ_1 et σ_2 sont des injections totales qui peuvent être considérées comme des fonctions de renommage. Par exemple, le point de contrôle x_1 du programme p_1 est renommé en $\sigma_1^{\smile} x_1$. La condition $\sigma_1\sigma_2^{\smile} = y_1 x_2^{\smile}$ signifie que le point de contrôle y_1 (point de contrôle final du programme p_1) coïncide (est connecté) avec le point de contrôle x_2 (point de contrôle initial du programme p_2).

Les éléments de C_1 et C_2 vérifient la propriété suivante :

$$(7.16)\quad c_1[\sigma_1\sigma_2^{\smile}, I] = \emptyset,\ \text{où } c_1 \in C_1 \text{ et } c_1 \neq s_1.$$

Par la remarque 7.11, il existe un point x tel que $c_1 = [x x^{\smile}, I]$ et $x \neq y_1$ (car $c_1 \neq s_1$), d'où

$$\begin{array}{ll} & c_1[\sigma_1\sigma_2^{\smile}, I] \\ = & \qquad \{\ c_1 = [x x^{\smile}, I] \text{ et } \sigma_1\sigma_2^{\smile} = y_1 x_2^{\smile} \text{ (équation 7.15).}\ \} \\ & [x x^{\smile}, I][y_1 x_2^{\smile}, I] \\ = & \qquad \{\ \text{Lemme 2.40(j).}\ \} \\ & [x x^{\smile} y_1 x_2^{\smile}, I] \\ = & \qquad \{\ \text{Remarque 2.24 } (x \neq y_1).\ \} \\ & \emptyset \end{array}$$

D'une façon analogue nous avons

$$(7.17)\quad [\sigma_1\sigma_2^{\smile}, I]c_2 = \emptyset,\ \text{où } c_2 \in C_2 \text{ et } c_2 \neq e_2.$$

Soit le programme $p := p_1; p_2$ qui est la séquence des programmes p_1 et p_2. Dans ce qui suit, en utilisant les relations σ_1 et σ_2 ainsi que les diagrammes associés aux programmes p_1 et p_2, nous allons définir un quadruplet $\mathcal{Q}[\![p]\!]$ et montrer par la suite que ce dernier est effectivement un diagramme.

Posons $\mathcal{Q}[\![p]\!] := (P, C, e, s)$, où

(7.18) $P := [\sigma_1^\smile, I]P_1[\sigma_1, I] \cup [\sigma_2^\smile, I]P_2[\sigma_2, I],$
$C := \{[\sigma_i^\smile, I]c[\sigma_i, I] \mid c \in C_i,\ i = 1, 2, \},$
$e := [\sigma_1^\smile, I]e_1[\sigma_1, I],$
$s := [\sigma_2^\smile, I]s_2[\sigma_2, I].$

(7.19) **Remarque.** Si σ est une application injective, en appliquant le lemme 2.40(j), $\sigma^\smile\sigma \subseteq I$ et $\sigma\sigma^\smile = I$, il est facile de voir que la relation $[\sigma, I]$ est aussi une application injective. Comme (σ_1, σ_2) sont des applications injectives (7.15), $[\sigma_1, I]$ et $[\sigma_2, I]$ le sont aussi. ∎

Par la remarque 7.19 et le lemme 7.2, les quadruplets

- $\mathcal{Q}_1[\![p_1]\!] := ([\sigma_1^\smile, I]P_1[\sigma_1, I], [\sigma_1^\smile, I]C_1[\sigma_1, I], [\sigma_1^\smile, I]e_1[\sigma_1, I], [\sigma_1^\smile, I]s_1[\sigma_1, I]),$
- $\mathcal{Q}_2[\![p_2]\!] := ([\sigma_2^\smile, I]P_2[\sigma_2, I], [\sigma_2^\smile, I]C_2[\sigma_2, I], [\sigma_2^\smile, I]e_2[\sigma_2, I], [\sigma_2^\smile, I]s_1[\sigma_2, I])$

sont des diagrammes.

Avant de prouver que $\mathcal{Q}[\![p]\!]$ est effectivement un diagramme, nous montrons d'abord que la relation de sortie du diagramme $\mathcal{Q}_1[\![p_1]\!]$ est égale à la relation d'entrée du diagramme $\mathcal{Q}_2[\![p_2]\!]$, c'est-à-dire

(7.20) $[\sigma_1^\smile, I]s_1[\sigma_1, I] = [\sigma_2^\smile, I]e_2[\sigma_2, I].$

En remplaçant s_1 et e_2 dans l'équation 7.20 par leurs valeurs (7.14) et en appliquant le lemme 2.40(j), nous obtenons

(7.21) $[\sigma_1^\smile y_1 y_1^\smile \sigma_1, I] = [\sigma_2^\smile x_2 x_2^\smile \sigma_2, I].$

Il est facile de voir que l'équation 7.21 découle de

(7.22) $\sigma_1^\smile y_1 = \sigma_2^\smile x_2.$

En effet,

$$\begin{array}{ll} & \sigma_1\sigma_2^\smile = y_1 x_2^\smile \\ \Rightarrow & \sigma_1^\smile\sigma_1\sigma_2^\smile x_2 = \sigma_1^\smile y_1 x_2^\smile x_2 \\ \Rightarrow & \qquad \{ \text{ Remarque 2.24 } (x_2^\smile x_2 = L) \text{ et } \sigma_1^\smile\sigma_1 = I. \ \} \\ & \sigma_1^\smile y_1 \subseteq \sigma_2^\smile x_2 \end{array}$$

De la même manière, nous montrons que $\sigma_2^\smile x_2 \subseteq \sigma_1^\smile y_1$. D'où le résultat.

Nous sommes maintenant en mesure de prouver que $\mathcal{Q}[\![p]\!] = (P, C, e, s)$ (7.18) est effectivement un diagramme (définition 5.1). Autrement dit, nous devons vérifier que chaque élément de C est une identité partielle, que les éléments (différents) de C sont deux à deux disjoints, que $e, s \in C$ et finalement que $(\bigcup C)P(\bigcup C) = P$.

- Par la remarque 7.19 et le fait que les éléments de C_1 et C_2 sont des identités partielles, nous déduisons que les éléments de C (7.18) le sont aussi.

- Prenons arbitrairement deux identités partielles différentes c et c' appartenant à l'ensemble C. En considérant la structure de l'ensemble C (7.18), trois cas sont possibles :

  - $c = [\sigma_1^\smile, I]c_1[\sigma_1, I]$ et $c' = [\sigma_1^\smile, I]c_1'[\sigma_1, I]$, où c_1, $c_1' \in C_1$. Par la remarque 7.19 et le lemme 7.2, nous déduisons que $cc' = \emptyset$.
  - $c = [\sigma_2^\smile, I]c_2[\sigma_2, I]$ et $c' = [\sigma_2^\smile, I]c_2'[\sigma_2, I]$, où c_2, $c_2' \in C_2$. Ce cas se traite de la manière que le cas précédent.
  - $c = [\sigma_1^\smile, I]c_1[\sigma_1, I]$ avec $c_1 \in C_1$ et $c' = [\sigma_2^\smile, I]c_2[\sigma_2, I]$ avec $c_2 \in C_2$ (ou le cas symétrique). Si $c_1 = s_1$ et $c_2 = e_2$, nous avons $c = c'$. Puisque $c \neq c'$, par hypothèse, nous devons avoir $c_1 \neq s_1$ ou $c_2 \neq e_2$. D'où

    $$\begin{array}{ll} & cc' \\ = & \quad \{ \text{ Expressions de } c \text{ et } c'. \} \\ & ([\sigma_1^\smile, I]c_1[\sigma_1, I])([\sigma_2^\smile, I]c_2[\sigma_2, I]) \\ = & \quad \{ \text{ Lemme 2.40(j). } \} \\ & [\sigma_1^\smile, I]c_1[\sigma_1\sigma_2^\smile, I]c_2[\sigma_2, I] \\ = & \quad \{ \text{ Équation 7.16 si } c_1 \neq s_1 \text{ et par 7.17 si } c_2 \neq e_2. \} \\ & \emptyset \end{array}$$

    Nous concluons que les éléments de C sont deux à deux disjoints.

- Il est facile de voir que les relations $[\sigma_1^\smile, I]e_1[\sigma_1, I]$ et $[\sigma_2^\smile, I]s_2[\sigma_2, I]$ sont des éléments de l'ensemble C (équation 7.18). Ceci découle de $e_1 \in C_1$ et $s_2 \in C_2$.

- Finalement, montrons que $(\bigcup C)P(\bigcup C) = P$. Puisque $(\bigcup C) \subseteq I$, il suffit de montrer que $P \subseteq (\bigcup C)P(\bigcup C)$. Comme (;) se distribue sur $\cup$, nous avons

  $$\bigcup C = [\sigma_1^\smile, I](\bigcup C_1)[\sigma_1, I] \cup [\sigma_2^\smile, I](\bigcup C_2)[\sigma_2, I].$$

  Calculons d'abord $(\bigcup C)P$.

  $$\begin{array}{ll} & (\bigcup C)P \\ = & \quad \{ \text{ Équation 7.18. } \} \\ & ([\sigma_1^\smile, I](\bigcup C_1)[\sigma_1, I] \cup [\sigma_2^\smile, I](\bigcup C_2)[\sigma_2, I])([\sigma_1^\smile, I]P_1[\sigma_1, I] \cup [\sigma_2^\smile, I]P_2[\sigma_2, I]) \\ = & \quad \{ \text{ (;) se distribue sur } \cup, \text{ lemme 2.40(j) et équation 7.15. } \} \\ & [\sigma_1^\smile, I](\bigcup C_1)P_1[\sigma_1, I] \cup [\sigma_1^\smile, I](\bigcup C_1)[\sigma_1\sigma_2^\smile, I]P_2[\sigma_2, I] \\ & \cup [\sigma_2^\smile, I](\bigcup C_2)[\sigma_2\sigma_1^\smile, I]P_1[\sigma_1, I] \cup [\sigma_2^\smile, I](\bigcup C_2)P_2[\sigma_2, I] \\ = & \quad \{ \text{ Équations 7.16 et 7.17. } \} \\ & [\sigma_1^\smile, I](\bigcup C_1)P_1[\sigma_1, I] \cup [\sigma_1^\smile, I]s_1[\sigma_1\sigma_2^\smile, I]P_2[\sigma_2, I] \\ & \cup [\sigma_2^\smile, I]e_2[\sigma_2\sigma_1^\smile, I]P_1[\sigma_1, I] \cup [\sigma_2^\smile, I](\bigcup C_2)P_2[\sigma_2, I]. \end{array}$$

En procédant d'une façon similaire et en considérant le fait que $(\bigcup C_1)P_1(\bigcup C_1) = P_1$ et $(\bigcup C_2)P_2(\bigcup C_2) = P_2$ et que $P = [\sigma_1^\smile, I]P_1[\sigma_1, I] \cup [\sigma_2^\smile, I]P_2[\sigma_2, I]$, il est facile de déduire que $P = (\bigcup C)P(\bigcup C)$.

Ainsi, nous avons montré que $\mathcal{Q}[\![p]\!] = (P, C, e, s)$ est effectivement un diagramme.

Nous allons calculer la relation d'entrée/sortie du diagramme $\mathcal{Q}[\![p]\!]$ et prouver ensuite que l'hypothèse d'induction 7.12 est vérifiée par le programme $p = p_1; p_2$.

Donc le diagramme $\mathcal{Q}[\![p]\!]$ est construit à partir de deux diagrammes $\mathcal{Q}_1[\![p_1]\!]$ et $\mathcal{Q}_2[\![p_2]\!]$ tels que la relation de sortie du premier coïncide avec la relation d'entrée du deuxième (par 7.20). Le diagramme $\mathcal{Q}[\![p]\!]$ vérifie donc les hypothèses du diagramme 6.4.1. Par conséquent l'équation 6.32 est applicable au diagramme $\mathcal{Q}[\![p]\!]$ et nous avons

$$\mathcal{E}(\mathcal{Q}[\![p]\!]) = (\mathcal{E}(\mathcal{Q}_1[\![p_1]\!]) \circ \mathcal{E}(\mathcal{Q}_2[\![p_2]\!]).$$

Par la remarque 7.19 et le lemme 7.2(b), ceci est équivalent à

$$\mathcal{E}(\mathcal{Q}[\![p]\!]) = ([\sigma_1^\smile, I]\mathcal{E}(\mathcal{Q}[\![p_1]\!])[\sigma_1, I]) \circ ([\sigma_2^\smile, I]\mathcal{E}(\mathcal{Q}[\![p_2]\!])[\sigma_2, I]). \tag{7.23}$$

Or, par l'application de l'hypothèse d'induction 7.12, nous avons

$$\mathcal{E}(\mathcal{Q}[\![p_1]\!]) = [x_1 y_1^\smile, \mathcal{D}[\![p_1]\!]]. \tag{7.24}$$

D'une manière analogue nous avons

$$\mathcal{E}(\mathcal{Q}[\![p_2]\!]) = [x_2 y_2^\smile, \mathcal{D}[\![p_2]\!]]. \tag{7.25}$$

Nous avons maintenant tous les outils nécessaires pour montrer que l'hypothèse d'induction 7.12 est satisfaite par le programme $p = p_1; p_2$, c'est-à-dire

$$\mathcal{E}(\mathcal{Q}[\![p_1; p_2]\!]) = [\sigma_1^\smile x_1 y_2^\smile \sigma_2, \mathcal{D}[\![p_1; p_2]\!]]. \tag{7.26}$$

Il n'est pas difficile de montrer que $\sigma_1^\smile x_1$ et $\sigma_2^\smile y_2$ sont des points sur $\mathbf{N}$, vérifiant $e = [\sigma_1^\smile x_1 x_1^\smile \sigma_1, I]$ et $s = [\sigma_2^\smile y_2 y_2^\smile \sigma_2, I]$ (ceci se déduit de 7.14, 7.15 et 2.40(j)).

Démonstration.

$$\begin{aligned}
& \mathcal{E}(\mathcal{Q}[\![p_1; p_2]\!]) \\
= & \quad \{ \text{ Équation 7.23. } \} \\
& ([\sigma_1^\smile, I]\mathcal{E}(\mathcal{Q}[\![p_1]\!])[\sigma_1, I]) \circ ([\sigma_2^\smile, I]\mathcal{E}(\mathcal{Q}[\![p_2]\!])[\sigma_2, I]) \\
= & \quad \{ \text{ Équations 7.24 et 7.25. } \} \\
& ([\sigma_1^\smile, I][x_1 y_1^\smile, \mathcal{D}[\![p_1]\!]][\sigma_1, I]) \circ ([\sigma_2^\smile, I][x_2 y_2^\smile, \mathcal{D}[\![p_2]\!]][\sigma_2, I]) \\
= & \quad \{ \text{ Lemme 2.40(j). } \} \\
& ([\sigma_1^\smile x_1 y_1^\smile \sigma_1, \mathcal{D}[\![p_1]\!]]) \circ ([\sigma_2^\smile x_2 y_2^\smile \sigma_2, \mathcal{D}[\![p_2]\!]]) \\
= & \quad \{ \text{ Lemme 7.1(d). } \} \\
& [(\sigma_1^\smile x_1 y_1^\smile \sigma_1) \circ (\sigma_2^\smile x_2 y_2^\smile \sigma_2), \mathcal{D}[\![p_1]\!] \circ \mathcal{D}[\![p_2]\!]]
\end{aligned}$$

$=$ { Proposition 3.9(a) ($\sigma_1^{\smile} x_1 y_1^{\smile} \sigma_1$ déterministe par 2.23(h) et σ_1 déterministe). }
$[\sigma_1^{\smile} x_1 y_1^{\smile} \sigma_1 \sigma_2^{\smile} x_2 y_2^{\smile} \sigma_2, \mathcal{D}[\![p_1]\!] \triangleright \mathcal{D}[\![p_2]\!]]$
$=$ { Équation 7.15 ($\sigma_1 \sigma_2^{\smile} = y_1 x_2^{\smile}$), définition 2.23(h) et règle de Tarski (définition 2.18(e)). }
$[\sigma_1^{\smile} x_1 y_2^{\smile} \sigma_2, \mathcal{D}[\![p_1]\!] \triangleright \mathcal{D}[\![p_2]\!]]$
$=$ { Équation 3.14. }
$[\sigma_1^{\smile} x_1 y_2^{\smile} \sigma_2, \mathcal{D}[\![p_1; p_2]\!]]$

Ainsi nous avons prouvé que l'hypothèse d'induction 7.12 est effectivement vérifiée pour la séquence.

7.3.3 Choix gardé

Soient p_1 et p_2 deux programmes, g_1 et g_2 deux gardes. Notre but est de vérifier si le programme **if** $g_1 \to p_1 [\!] \; g_2 \to p_2$ **fi** (voir le diagramme 5.6) satisfait l'équation 7.12. Le traitement du choix gardé ressemble en partie à celui de la séquence et en partie à celui de la boucle, qui est présenté ci-dessous. Par conséquent, nous donnons directement le résultat.

L'équation 3.15 implique que

$$\mathcal{E}(\mathcal{Q}[\![\textbf{ if } g_1 \to p_1 [\!] \; g_2 \to p_2 \textbf{ fi}]\!]) = [x y^{\smile}, \mathcal{D}[\![\textbf{ if } g_1 \to p_1 [\!] \; g_2 \to p_2 \textbf{ fi }]\!]], \tag{7.27}$$

où x et y sont respectivement le point de contrôle initial et le point de contrôle final du programme **if** $g_1 \to p_1 [\!] \; g_2 \to p_2$ **fi** .

Nous déduisons que l'hypothèse d'induction 7.12 est vérifiée pour le choix gardé.

7.3.4 Boucle

Finalement, nous traitons le cas de la boucle.

Soit p un programme et $\mathcal{Q}[\![p]\!] = (P, C_1, e_1, s_1)$ le diagramme associé au programme p où $e_1 := [x_1 x_1^{\smile}, I]$ et $s := [y_1 y_1^{\smile}, I]$. Soit le programme $w :=$ **do** $g \to p$ **od** (voir 5.8 pour la définition du diagramme associé).

Nous cherchons à prouver que l'hypothèse d'induction 7.12 est vérifiée par le programme w. Commençons par construire le diagramme $\mathcal{Q}[\![w]\!] = (W, C, s_1, s)$. Il suffit d'ajouter un seul point de contrôle. Posons $s := [y y^{\smile}, I]$, où y est tel que $s(\bigcup C_1) = \emptyset$. Autrement dit, y est un point sur les naturels qui n'est pas déjà utilisé comme point de contrôle dans $\mathcal{Q}[\![p]\!]$. Prenons

- $C := C_1 \cup \{s\}$,
- $W := [y_1 x_1^{\smile}, \mathcal{G}(g)] \cup P \cup [y_1 y^{\smile}, \mathcal{G}(g)^{\sim}]$.

Montrons que $\mathcal{Q}[\![w]\!]$ est un diagramme (définition 5.1). Il suffit de montrer que $W \subseteq (\bigcup C) W (\bigcup C)$, les autres propriétés étant faciles à vérifier. En tenant compte des remarques 7.11 et 2.24, du lemme 2.40(j), du fait que $[x_1^{\smile} x_1, I]$ et $[y_1^{\smile} y_1, I]$ sont des éléments

de C_1 (rappelons que les éléments de C_1 sont deux à deux disjoints) et que $s = [yy^\smile, I]$ et vérifie $s(\bigcup C_1) = \emptyset$, il n'est pas difficile de montrer que les propriétés suivantes sont satisfaites :

$$(7.28)\quad \begin{array}{ll} (\bigcup C_1)[y_1x_1^\smile, \mathcal{G}(g)] = [y_1x_1^\smile, \mathcal{G}(g)], & s[y_1x_1^\smile, \mathcal{G}(g)] = \emptyset, \\ (\bigcup C_1)[y_1y^\smile, \mathcal{G}(g)^\sim] = [y_1y^\smile, \mathcal{G}(g)^\sim], & s[y_1y^\smile, \mathcal{G}(g)^\sim] = \emptyset. \end{array}$$

Par conséquent,

$$\begin{array}{ll} & (\bigcup C)W \\ = & \qquad \{ \text{ Expressions de } C \text{ et } W. \ \} \\ & (\bigcup C_1 \cup s)([y_1x_1^\smile, \mathcal{G}(g)] \cup P \cup [y_1y^\smile, \mathcal{G}(g)^\sim]) \\ = & \qquad \{ \ (;) \text{ se distribue sur } \cup \text{ et équation 7.28. } \} \\ & [y_1x_1^\smile, \mathcal{G}(g)] \cup (\bigcup C_1)P \cup sP \cup [y_1y^\smile, \mathcal{G}(g)^\sim]) \\ = & \qquad \{ \ sP = s(\bigcup C_1)P(\bigcup C_1) = \emptyset \text{ (car par hypothèse } s(\bigcup C_1) = \emptyset). \ \} \\ & [y_1x_1^\smile, \mathcal{G}(g)] \cup (\bigcup C_1)P \cup [y_1y^\smile, \mathcal{G}(g)^\sim] \end{array}$$

En procédant d'une façon analogue et en utilisant les propriétés suivantes, sinilaires aux propriétés 7.28,

- $[y_1x_1^\smile, \mathcal{G}(g)](\bigcup C_1) = [y_1x_1^\smile, \mathcal{G}(g)]$,
- $[y_1x_1^\smile, \mathcal{G}(g)]s = \emptyset$,
- $[y_1y^\smile, \mathcal{G}(g)^\sim](\bigcup C_1) = \emptyset$,
- $[y_1y^\smile, \mathcal{G}(g)^\sim]s = [y_1y^\smile, \mathcal{G}(g)^\sim]$,

nous obtenons : $W \subseteq (\bigcup C)W(\bigcup C)$. Donc, $\mathcal{Q}[\![p]\!]$ est effectivement un diagramme. Dans ce qui suit, nous allons calculer sa relation d'entrée/sortie.

Remarquons qu'en posant

$$(7.29)\quad G := [y_1x_1^\smile, \mathcal{G}(g)], \quad P := P, \quad Q := [y_1y^\smile, \mathcal{G}(g)^\sim],$$

nous obtenons le diagramme $\mathcal{W}$ de la sous-section 6.4.3. Donc, l'équation 6.37 est applicable au diagramme $\mathcal{Q}[\![w]\!]$ et nous avons

$$(7.30)\quad \mathcal{E}(\mathcal{Q}[\![w]\!]) = (G\mathcal{E}(\mathcal{Q}[\![p]\!]))^*Q \cap \mathcal{A}(G\mathcal{E}(\mathcal{Q}[\![p]\!]), Q) \cap \mathcal{B}(G\mathcal{E}(\mathcal{Q}[\![p]\!])).$$

Remarquons $QL \cap G\mathcal{E}(\mathcal{Q}[\![p]\!]L = \emptyset$. Par le théorème 5.43 nous avons

$$(7.31)\quad \mathcal{E}(\mathcal{Q}[\![w]\!]) = \bigsqcup\{X \mid X = Q \cup G\mathcal{E}(\mathcal{Q}[\![p]\!]) \triangleleft X\}.$$

En appliquant l'hypothèse d'induction 7.12 au diagramme $\mathcal{Q}[\![p]\!]$, nous obtenons

$$(7.32)\quad \mathcal{E}(\mathcal{Q}[\![p]\!]) = [x_1y_1^\smile, \mathcal{D}[\![p]\!] \triangleleft X].$$

En appliquant les équations 7.32, 7.29, la remarque 2.24 et le lemme 2.40(j), l'équation 7.31 devient

(7.33) $\mathcal{E}(\mathcal{Q}[\![w]\!]) = \bigsqcup\{X \mid X = [y_1 y^{\smile}, \mathcal{G}(g)^{\sim}] \cup [y_1 y_1^{\smile}, \mathcal{G}(g)\mathcal{D}[\![p]\!]] \triangleleft X\}$.

Afin d'alléger les notations et gagner sur la clarté des preuves, nous adoptons les abréviations suivantes :

(7.34) **Abréviation.**

$$A := y_1 y_1^{\smile}, \qquad B := y_1 y^{\smile},$$
$$f(X) := [B, \mathcal{G}(g)^{\sim}] \cup [A, \mathcal{G}(g)\mathcal{D}[\![p]\!]] \triangleleft X, \qquad g(X) := \mathcal{G}(g)^{\sim} \cup \mathcal{G}(g)\mathcal{D}[\![p]\!] \triangleleft X.$$

■

En utilisant l'équation 2.11(b), l'abréviation 7.34 et l'équation 7.33, montrons que

(7.35) $\nu(f) = [B, \nu(g)]$.

En appliquant la définition 2.23(h), il est facile de voir que les relations A et B vérifient les propriétés suivantes :

(7.36) $AB = B, \quad AL = BL, \quad A \subseteq I$.

Avant de montrer l'équation 7.35, donnons le lemme suivant.

(7.37) **Lemme.** *Soient A, B les relations données dans l'abréviation 7.34, et P et Q des relations quelconques.*

(a) $[A, P]^*[B, Q] = [B, P^*Q]$,

(b) $\mathcal{A}([A, P], [B, Q]) = [BL, \mathcal{A}(P, Q)]$.

Démonstration.

(a)
$$\begin{aligned}
& [A, P]^*[B, Q] \\
= & \quad \{ \text{ Équation 2.33(b). } \} \\
& (I \cup [A, P]^+)[B, Q] \\
= & \quad \{ (;) \text{ se distribue sur } \cup \text{ et lemme 2.40(k), } A^+ = A \text{ (équation 7.36 et théorème 2.29(b)). } \} \\
& [B, Q] \cup [A, P^+][B, Q] \\
= & \quad \{ \text{ Lemme 2.40(j). } \} \\
& [B, Q] \cup [AB, P^+Q] \\
= & \quad \{ \text{ Équation 7.36, lemme 2.40(c), } (;) \text{ se distribue sur } \cup \text{ et équation 2.33(b). } \} \\
& [B, P^*Q]
\end{aligned}$$

(b) $\mathcal{A}([A,P],[B,Q])$

$=$ { Abréviation 4.7. }

$[A,P]^* \triangleright ([A,P]L \cup [B,Q]L)$

$=$ { Équation 2.33(b), $I = [I,I]$, équation 7.36, lemme 2.40(c,d). }

$([I,I] \cup [A,P]^+) \triangleright [BL, PL \cup QL]$

$=$ { Lemme 2.40(k), équation 2.33(b) et équation 7.36. }

$[I,P^*] \triangleright [BL, PL \cup QL]$

$=$ { Lemme 7.1(c). }

$[I \triangleright BL, P^* \triangleright (PL \cup QL)] \cup [\overline{IL}, L] \cup [L, \overline{P^*L}])$

$=$ { Loi booléenne, $I \triangleright BL = BL$, $IL = L$, $P^*L = L$, définition 2.36 et abréviation 4.7. }

$[BL, \mathcal{A}(P,Q)]$

■

Maintenant, montrons l'équation 7.35.

$\nu(f)$

$=$ { Théorème 5.43 }

$[A, \mathcal{G}(g)\mathcal{D}[\![p]\!]]^*[B, \mathcal{G}(g)^\sim] \cap \mathcal{A}([A, \mathcal{G}(g)\mathcal{D}[\![p]\!]], [B, \mathcal{G}(g)^\sim]) \cap \mathcal{B}([A, \mathcal{G}(g)\mathcal{D}[\![p]\!]])$

$=$ { Lemme 7.37(a,b). }

$[B, (\mathcal{G}(g)\mathcal{D}[\![p]\!])^*\mathcal{G}(g)^\sim] \cap [BL, \mathcal{A}(\mathcal{G}(g)\mathcal{D}[\![p]\!], \mathcal{G}(g)^\sim)] \cap \mathcal{B}([A, \mathcal{G}(g)\mathcal{D}[\![p]\!]])$

$=$ { Lemme 2.40(a) et lemme 2.55(d). }

$[B, (\mathcal{G}(g)\mathcal{D}[\![p]\!])^*\mathcal{G}(g)^\sim \cap \mathcal{A}(\mathcal{G}(g)\mathcal{D}[\![p]\!], \mathcal{G}(g)^\sim)] \cap ([\mathcal{B}(A), L] \cup [L, \mathcal{B}(\mathcal{G}(g)\mathcal{D}[\![p]\!])]$

$=$ { Proposition 2.54(c) (A déterministe, $A \subseteq I$, $\mathcal{B}(A) = \overline{AL} = \overline{BL}$ par 7.36) et lemme 2.40(a). }

$[B, (\mathcal{G}(g)\mathcal{D}[\![p]\!])^*\mathcal{G}(g)^\sim \cap \mathcal{A}(\mathcal{G}(g)\mathcal{D}[\![p]\!], \mathcal{G}(g)^\sim) \cap \mathcal{B}(\mathcal{G}(g)\mathcal{D}[\![p]\!])]$

$=$ { Théorème 5.43, loi booléenne et abréviation 7.34. }

$[B, \nu(g)]$

■

En remplaçant f, B et g par leurs valeurs (abréviation 7.34) dans l'équation 7.35, nous trouvons l'équation suivante :

$$\mathcal{E}(\mathcal{Q}[\![w]\!]) = [y_1 y^\smile, \bigsqcup\{X \mid X = \mathcal{G}(g)^\sim \cup \mathcal{G}(g)\mathcal{D}[\![p]\!] \triangleright X\}]. \tag{7.38}$$

En appliquant l'équation 3.19, l'équation précédente devient

$$\mathcal{E}(\mathcal{Q}[\![w]\!]) = [y_1 y^\smile, \mathcal{D}[\![w]\!]]. \tag{7.39}$$

Ainsi nous avons prouvé que l'hypothèse d'induction 7.12 est vérifiée par le programme $w := \mathbf{do}\ g \to p\ \mathbf{od}$. ∎

Donc, en procédant par induction, nous avons prouvé que l'hypothèse d'induction 7.12 est vérifiée par la séquence (7.26), par le choix gardé (7.27) et finalement par la boucle (7.38). Comme nous considérons des programmes impératifs dont les constructeurs sont la séquence, le choix gardé et la boucle, alors nous pouvons affirmer que tout programme p vérifie $\mathcal{O}[\![p]\!] = \mathcal{D}[\![p]\!]$, c'est-à-dire que la sémantique opérationnelle démoniaque d'un programme non déterministe p est égale à la sémantique dénotationnelle de ce programme.

7.4 Conclusion

Dans ce chapitre nous avons défini la notion de sémantique opérationnelle démoniaque d'un programme non déterministe p. Cette sémantique a été donnée à partir de la notion de diagramme et de relation d'entrée/sortie de diagramme. En procédant par induction sur les constructeurs, nous avons montré que la sémantique opérationnelle démoniaque d'un programme est égale à sa sémantique dénotationnelle démoniaque. Comme résultat intermédiaire, nous avons aussi montré comment combiner des diagrammes en séquence et en boucle pour obtenir un nouveau diagramme. Finalement, nous avons montré l'égalité entre la sémantique opérationnelle et la sémantique dénotationnelle. Ceci implique que la figure 7.1 commute.

Chapitre 8

Conclusion générale

Dans cette thèse, nous avons présenté une sémantique opérationnelle du langage des commandes gardées de Dijkstra. Pour ce faire, nous avons associé à chaque programme un diagramme relationnel. Un diagramme relationnel est essentiellement une représentation, dans le formalisme de l'algèbre des relations, d'un système de transitions dont les arcs sont étiquetés par des relations. Nous avons ensuite défini la notion de relation d'entrée/sortie démoniaque d'un diagramme. Cette démarche nous a permis d'associer à chaque programme (non déterministe) une relation d'entrée/sortie correspondant à sa pire exécution. Nous avons montré que la relation ainsi obtenue est aussi celle qui est assignée par une sémantique dénotationnelle définie dans des travaux antérieurs [1, 27]. En d'autres termes, nous avons montré l'équivalence de notre sémantique opérationnelle avec une sémantique dénotationnelle relationnelle déjà connue. L'intérêt de cette démonstration réside dans le fait que les définitions dénotationnelles classiques requièrent une bonne dose d'intuition pour être formulées et comprises, alors que l'association d'un diagramme à un programme est tout à fait naturelle.

Comme résultat intermédiaire, nous avons démontré une règle de vérification de boucles, qui est une généralisation à un contexte non déterministe d'un théorème de Mills connu sous le nom de *règle de vérification de boucle de Mills*, énoncé initialement pour les programmes déterministes. Ce théorème permet de s'assurer qu'une relation donnée est effectivement la sémantique d'une boucle donnée.

L'opérateur d'implication relative $\triangleright$ nous a donné la possibilité de simplifier nos preuves et de les améliorer en réduisant l'usage de l'opérateur de complémentation. Pour éviter l'utilisation exagérée de ce dernier, Backhouse *et al.* recommandent l'usage des résidus. L'implication relative et l'opération de résiduation à gauche sont très semblables ; en effet, $Q \triangleright R = Q^{\smile} \backslash R$. Pour notre application, l'emploi de l'implication relative plutôt que du résidu a permis de diminuer le nombre d'inverses ($^{\smile}$).

La notion de point fixe a été très utilisée dans nos preuves. Entre autres à cause de $\mathcal{B}(R)$ (partie initiale de R), qui est le plus petit point fixe de $f(X) := R \triangleright X$. Ceci nous a obligé à développer certains résultats intéressants sur les points fixes des fonctions monotones par rapport à « $\subseteq$ » ou « $\sqsubseteq$ » (2.55, 2.57, 2.59 et 5.43).

La règle de vérification de boucles non déterministes est très utile pour la dérivation et la vérification des boucles. Pour la vérification, si nous avons une condition de boucle et un corps de boucle, ce théorème nous aide à vérifier si une relation quelconque W est

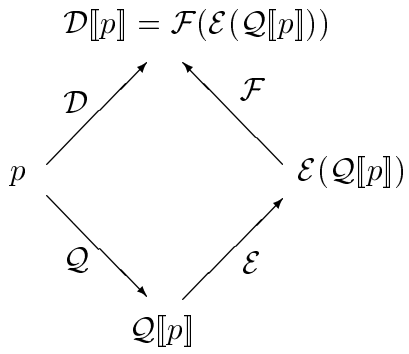


Figure 8.1: $\mathcal{O}[\![p]\!] := \mathcal{F}(\mathcal{E}(\mathcal{Q}[\![p]\!])) = \mathcal{D}[\![p]\!]$

effectivement la sémantique de la boucle en question. Pour le contexte de dérivation de boucle, le théorème est plus utile dans l'autre direction : si nous avons une spécification (relation) W d'une boucle, nous pouvons trouver intuitivement les abstractions g et B de la condition de boucle et du corps de boucle, respectivement, et utiliser ce théorème pour vérifier que ce choix de g et B est correct. Finalement, ce théorème nous a permis de montrer que le plus grand point fixe des fonctions de la forme $f(X) := Q \cup P \,\square\, X$, où $PL \cap QL = \emptyset$, est égal à $P^*Q \cap \mathcal{A}(P,Q) \cap \mathcal{B}(P)$ (théorème 5.43). Dans cette thèse, ce théorème a été utilisé à plusieurs reprises.

Notre approche opérationnelle consiste à associer un diagramme relationnel $\mathcal{Q}[\![p]\!]$ à un programme p et à calculer la relation d'entrée/sortie $\mathcal{E}(\mathcal{Q}[\![p]\!])$ du diagramme $\mathcal{Q}[\![p]\!]$. Cette relation $\mathcal{E}(\mathcal{Q}[\![p]\!])$ est définie sur le produit cartésien de l'ensemble des points de contrôle et de l'ensemble des états. Afin d'éliminer les points de contrôle, nous appliquons la fonction $\mathcal{F}$ à la relation $\mathcal{E}(\mathcal{Q}[\![p]\!])$. Finalement, nous obtenons $\mathcal{O}[\![p]\!] := \mathcal{F}(\mathcal{E}(\mathcal{Q}[\![p]\!]))$, qui est égale à $\mathcal{D}[\![p]\!]$, la sémantique dénotationnelle démoniaque du programme p. Autrement dit, nous avons montré que le diagramme 8.1 (au sens conventionnel du terme) commute.

8.1 Liens avec d'autres travaux

D'autres approches ont été utilisées pour définir la sémantique démoniaque. Le formalisme qui est le plus utilisé dans ce domaine est celui des transformateurs de prédicats [6, 7, 31, 70, 83]. D'autres travaux ont été menés avec l'approche relationnelle [33, 44, 45] où, pour traiter les boucles infinies, ces auteurs ajoutent à l'espace un état $\perp$ pour dénoter la non-terminaison. Berghammer [14], Maddux [57] et Parnas [71] traitent la non-terminaison en représentant le programme par une paire (relation, ensemble), où la relation décrit un comportement entrée/sortie du programme et l'ensemble décrit le domaine de terminaison garantie. Les approches précédentes ont un certain avantage, car les opérations entre les relations ou entre les paires (relation, ensemble) sont des opérations totales. Cependant certaines relations ou paires (relation, ensemble) sont des spécifications non implantables [44].

8.2 Perspectives de recherche

Nous avons l'intention d'utiliser le concept de diagramme relationnel pour la description du parallélisme. C'est une démarche naturelle, étant donné que les systèmes de transitions (fort apparentés à nos diagrammes) sont déjà utilisés à cette fin. Ceci nous permettra peut-être de dériver des règles de raffinement de spécifications en programmes parallèles.

Nous examinerons aussi les applications pratiques, en particulier celle de la vérification de programmes de plus grande taille au moyen de la règle de vérification de boucles non déterministes.

Bibliographie

[1] A. Alikacem, S. Ben Mohamed Sghaier, J. Desharnais, M. El Ouali et F. Tchier. From demonic semantics to loop construction : A relation algebraic approach. *3e Conf. Maghrébine en Génie Logiciel et Intelligence Artificielle*, pages 239–248, Rabat, Maroc, avril 1994.

[2] C. Arts. Galois connections presented calculationally. Rapport de recherche, Department of Mathematics and Computer Science, Eindhoven University of Technology, Pays-Bas, 1992.

[3] R. J. R. Back. *On the correctness of refinement in program development.* 1978. Department of Computer Science, University of Helsinki. Thèse de Doctorat.

[4] R. J. R. Back. Correctness preserving program refinement : Proof theory and application. *Mathematical Center Tracts*, 131:417–433, 1980.

[5] R. J. R. Back. Proving total correctness of nondeterministic programs in infinity logic. *Acta Inf.*, 15(3):233–249, 1981.

[6] R. J. R. Back. A continuous semantics for unbounded nondeterminism. *Theoretical Comput. Sci.*, 23:187–210, 1983.

[7] R. J. R. Back. Combining angels, demons and miracles in program specifications. *Theoretical Comput. Sci.*, 100:365–383, 1992.

[8] R. C. Backhouse, M. Bijsterveld, R. van Geldrop et J. van der Woude. Category theory as coherently constructive lattice theory. Rapport de recherche, Department of Mathematics and Computer Science, Eindhoven University of Technology, Pays-Bas, 1995.

http:/www.win.tue.nl:82/win/cs/wp/papers/abstract/html.

[9] R. C. Backhouse et H. Doornbos. Mathematical induction made calculational. Computing science note 94/16, Department of Mathematics and Computer Science, Eindhoven University of Technology, Pays-Bas, 1994.

http:/www.win.tue.nl:82/win/cs/wp/papers/abstract/html.

[10] R. C. Backhouse, P. Hoogendijk, E. Voermans et J. van der Woude. A relational theory of datatypes. Rapport de recherche, Department of Mathematics and Computer Science, Eindhoven University of Technology, Pays-Bas, 1992.

http:/www.win.tue.nl:82/win/cs/wp/papers/abstract/html.

[11] R. C. Backhouse et J. van der Woude. Demonic operators and monotype factors. *Mathematical Structures in Comput. Sci.*, 3(4):417–433, décembre 1993. Aussi : Computing Science Note 92/11, Department of Mathematics and Computer Science, Eindhoven University of Technology, Pays-Bas, 1992.

[12] R. Berghammer. Relational specification of data types and programs. Rapport technique 9109, Fakultät für Informatik, Universität der Bundeswehr München, Allemagne, septembre 1991.

[13] R. Berghammer et G. Schmidt. Relational specifications. *Algebraic Logic*, de Banach Center Publications, volume 28, pages 167–190. Éditeur C. Rauszer. Académie polonaise des Sciences, 1993.

[14] R. Berghammer et H. Zierer. Relational algebraic semantics of deterministic and nondeterministic programs. *Theoretical Comput. Sci.*, 43:123–147, 1986.

[15] C. Bohm. On a family of Turing machines and the related programming languages. *ICC Bull.*, 3:187–194, 1964.

[16] N. Boudriga, F. Elloumi et A. Mili. On the lattice of specifications : Applications to a specification methodology. *Formal Aspects of Computing*, 4:544–571, 1992.

[17] M. Bréal. *Semantics : Studies in the science of meaning.* Henry Holt and Company, 1900.

[18] M. Broy. A theory for nondeterminism, parallelism, communications and concurrency. *Theoretical Comput. Sci.*, 46:1–61, 1986.

[19] L. H. Chin et A. Tarski. Distributive and modular laws in the arithmetic of relation algebras. *University of California Publications*, 1:341–384, 1951.

[20] B. A. Davey et H. A. Priestley. *Introduction to Lattices and Order.* Cambridge Mathematical Textbooks. Cambridge University Press, Cambridge, 1990.

[21] J. W. de Bakker. A calculus for recursive program schemes. *Automata, Languages and Programming*, pages 167–196. M. Nivat. North Holland, 1972.

[22] J. W. de Bakker. Semantics and termination of nondeterministic recursive programs. *Automata, Languages and Programming*, 1976.

[23] J. W. de Bakker. *Mathematical theory of program correctness.* Prentice-Hall, 1980.

[24] J. Desharnais. *Abstract relational semantics.* School of Computer Science, Univ. McGill, Montréal, 1989. Thèse de Doctorat.

[25] J. Desharnais, S. Baltagi et B. Chaib-draa. Simple weak sufficient conditions for sharpness. Rapport de recherche DIUL-RR-9405, Département d'Informatique, Université Laval, Québec, Canada, novembre 1994.

[26] J. Desharnais, N. Belkhiter, S. Ben Mohamed Sghaier, F. Tchier, A. Jaoua, A. Mili et N. Zaguia. Embedding a demonic semilattice in a relation algebra. *Theoretical Comput. Sci.*, 149:333–360, 1995.

[27] J. Desharnais, A. Mili et T. T. Nguyen. Refinement and demonic semantics. Dans *Relational methods in computer science*. Chris Brink et Gunther Schmidt, en coopération avec Rudolf Albrecht. Springer-Verlag, 1997.

[28] J. Desharnais et F. Tchier. Demonic relational semantics of sequential programs. Rapport de recherche DIUL-RR-9406, Département d'Informatique, Université Laval, Québec, Canada, décembre 1995.

[29] E. W. Dijkstra. Guarded commands, nondeterminacy and formal derivation of programs. *Commun. ACM*, 18 : (8), 453–457, 1975.

[30] E. W. Dijkstra. *A discipline of programming*. Prentice-Hall, 1976.

[31] E. W. Dijkstra. *Predicate calculus and program semantics*. Springer-Verlag, 1990.

[32] E. W. Dijkstra et W. Feijen. *Predicate calculus and program semantics*. Addison-Wesley, 1988.

[33] R. M. Dijkstra. Relational calculus and relational program semantics. Department of Computing Science, University of Groningen, 1994.

[34] W. H. Feijen. A bagatelle (for files). University of Texas at Austin, 1988.

[35] R. W. Floyd. Assigning meanings to programs. *Proceedings AMS Symposium in Applied Mathematics*, volume 19, pages 19–31, 1967.

[36] M. Frappier. *A Relational Basis for Program Construction by Parts*. Department of Computer Science, University of Ottawa, 1995. Thèse de Doctorat.

[37] P. Gardiner et C. Morgan. Data refinement of predicate transformers. *Theoretical Comput. Sci.*, 87:143–162, 1991.

[38] R. D. Gumb. *Programming logics : an introduction to verification and semantics*. John Wiley and Sons, 1989.

[39] C. A. Gunter. *Semantics of programming languages*. MIT Press, Cambridge, Massachusetts, London, England, 1992.

[40] E. Hehner. Predicative programming, Parts I and II. *Commun. ACM*, 27:134–151, février 1984.

[41] M. Hennessy. *The semantics of programming languges, an elementary introduction using structural operational semantics*. John Wiley and Sons, 1990.

[42] W. H. Hesselink. An algebraic calculus of commands. Rapport de recherche CS 8808, Department of Mathematics and computer Science, University of Groningen, 1988.

[43] C. A. R. Hoare. An axiomatic basis for computer programming. *Commun. ACM*, 12:576–580,583, 1969.

[44] C. A. R. Hoare et J. He. The weakest prespecification. *Fundam. Inform.*, IX, partie I:51–84, partie II : 217–252, 1986.

[45] C. A. R. Hoare et J. He. The weakest prespecification. *Inf. Process. Lett.*, 24:127–132, 1987.

[46] Y. I. Ianov. On the equivalence and transformation of program schemes. *Dokl. Akad. Nauk*, 113:39–42, 1957.

[47] D. Jacobs et D. Gries. General correctness ; a unification of partial and total correctness. *Acta Inf.*, 22:67–83, 1985.

[48] B. Jönsson. Boolean algebras with operators, part II. *American Journal of Mathematics*, 74:127–162, 1952.

[49] B. Jönsson. Varieties of relation algebras. *Algebra Universalis*, 15:273–298, 1982.

[50] B. Jönsson. The theory of binary relations. *Algebraic Logic, Colloq. Math. Soc.*, pages 245–292, Amsterdam, 1991.

[51] B. Jönsson et A. Tarski. Representation problems for relation algebra. *Bulletin of the American Mathematical Society*, 80, 1948.

[52] B. Knaster. Un théorème sur les fonctions d'ensemble. *Annales de la Société Polonaise de Mathématiques*, 6:133–134, 1928.

[53] R. C. Linger, H. Mills et B. Witt. *Structured programming : theory and practice.* Addison-Wesley, 1979.

[54] C. Livercy. *Théorie des programmes.* Dunod, Paris, 1978.

[55] R. D. Maddux. Introductory course on relations algebras, finite-dimensional cylindric algebras, and their interconnections. *Colloq. Math. Soc.*, volume 54, pages 361–392, Amsterdam, 1991.

[56] R. D. Maddux. The origin of relation algebras in the developement and axiomatization of the calculus of relations. *Studia Logica*, 50:421–455, 1991.

[57] R. D. Maddux. The working relational model for predicate transformer semantics. *Theoretical Comput. Sci.*, 1995.

[58] Z. Manna. *Mathematical theory of computation.* McGraw-Hill, New York, 1974.

[59] J. McCarthy. A basis for a mathematical theory of computation. *Computer Programming and Formal Systems*, P. Braffort et D. Hirschherg, éditeurs, North–Holland, Amesterdam, pages 33–69, 1963.

[60] B. Meyer. *Introduction à la théorie des langages de programmation.* Inter-Éditions, 1992.

[61] A. Mili. A relational approach to the design of deterministic programs. *Acta Inf.*, pages 315–328, 1983.

[62] A. Mili, J. Desharnais et F. Mili. Relational heuristics for the design of deterministic programs. *Acta Inf.*, 24(3):239–276, 1987.

[63] H. D. Mills. The new math of computer programming. *Commun. ACM*, 18(1):43–48, janvier 1975.

[64] H. D. Mills, V. R. Basili, J. D. Gannon et R. G. Hamlet. *Principles of computer programming. A mathematical approach.* Allyn and Bacon, Inc., 1987.

[65] R. Milne et C. Strachey. *A theory of programming language semantics.* Chapman and Hall Ltd.,Londres, 1976.

[66] C. Morgan et K. Robinson. Specification statements and refinement. *IBM J. Res. Dev. 31*, volume 5. Springer-Verlag, 1987. Réimprimé dans : C. Morgan et T. Vickers (éditeurs), *On the refinement calculus*, 23–46, 1994.

[67] C. C. Morgan. The specification statement. *ACM Trans. Programming Languges and Systems*, 10(3):403–419, 1988.

[68] J. M. Morris. A theoretical basis for stepwise refinement and the programming calculus. *Theoretical Comput. Sci.*, 9:287–306, 1987.

[69] T. T. Nguyen. A relational model of demonic nondeterministic programs. *Int. J. Foundations Comput. Sci.*, 2(2):101–131, 1991.

[70] T. T. Nguyen. The connection between predicate logic and demonic relation calculus. Dagstuhl Seminar Report 80-17.01-21.01.94 (9403). Dans Relational Methods in Computer Science, 1994.

[71] D. L. Parnas. A generalized control structure and its formal definition. *Commun. ACM*, 26(8):437–453, 1983.

[72] G. Plotkin. Structural operational semantics. *Lecture Notes, DAIMI FN, Aarhus University*, 19, 1981.

[73] M. Rabin et D. Scott. Finite automata and their decision problems. *IBM Journal of Research*, 3(2):115–125, 1959.

[74] J. Riguet. Programmation et théorie des catégories. *Proc. ICC. Symp. Symbolic Languages in Data Processing, Gordon and Breach, New York*, pages 83–98, New York, avril 1962.

[75] W. P. D. Roever. *Recursive program schemes : semantics and proof theory.* Math. Centrum Tracts, Amsterdam, 1974.

[76] D. A. Schmidt. *Denotational Semantics–A methodology for language development.* Allyn and Bacon, Boston (Mass.), 1986.

[77] G. Schmidt et T. Ströhlein. *Relationen und Graphen.* Springer-Verlag, Berlin, 1989.

[78] G. Schmidt et T. Ströhlein. *Relations and graphs.* EATCS Monographs in Computer Science. Springer-Verlag, Berlin, 1993.

[79] G. Schmidt et T. Ströhlein. Relations algebras : Concept of points and representability. *Disc. Math.*, 54:83–92, 1985.

[80] D. Scott. Outline of a mathematical theory of computation. *Proceedings of the fourth Annual Princeton Conference on Information Science and Systems*, pages 169–176, 1970.

[81] D. S. Scott. Lattice theory, data types and semantics. *New York University Symp. on Formal Semantics*, pages 64–106. Prentice-Hall, 1971. Éditeur, Randall Rustin.

[82] D. S. Scott et C. Strachey. Toward a mathematical semantics for computer languages. *Proceedings of Symp. on Computers and Automata*, pages 19–46, 1971. Éditeur, J. Fox.

[83] E. Sekerinski. A calculus for predicative programming. *Second International Conference on the Mathematics of Program Construction*, volume 669 of *Lecture Notes in Comput. Sci.* Springer-Verlag, 1993. Éditeurs, R. S. Bird et C. C. Morgan et J. C. P. Woodcock.

[84] H. Sondergaard et P. Sestoft. Non-determinism in functional languages. *The Computer Journal*, 35:514–522, 1992.

[85] C. Strachey. Towards a formal semantics. *Formal Language Description Languages for Computer Programming*, pages 198–220. North-Holland Publishing Co., Amsterdam, 1966.

[86] C. Strachey. The varieties of programming languages. *Technical Monographs PRG-10, Programming Research Group*, 1973. Éditeur, University Oxford.

[87] A. Tarski. On the calculus of relations. *J. Symb. Log.*, 6(3):73–89, 1941.

[88] A. Tarski. A lattice-theoretical fixpoint theorem and its applications. *Pacific Journal of Mathematics*, 5:285–309, 1955.

[89] F. Tchier et J. Desharnais. A generalisation of a theorem of Mills. *Proceedings of the Tenth International Symposium on Computer and Information Sciences, ISCISX*, pages 27–34, Turquie, novembre 1995.

[90] F. Tchier et J. Desharnais. La sémantique démoniaque par des graphes de contrôles relationnels. *4e Conf. Maghrébine en Génie Logiciel et Intelligence Artificielle*, pages 17–28, Algérie, avril 1996.

[91] F. Tchier, R. Khédri et J. Desharnais. Une sémantique relationnelle démoniaque. volume 209, Montréal, Canada, mai 1994. *Résumé, 62e congrès de l'ACFAS.*

[92] R. D. Tennent. The denotational semantics of programming languages. *Commun. ACM*, pages 437–453, 1976.

[93] R. D. Tennent. *Principles of programming languages.* Prentice-Hall International, 1981.

Index