Chapitre 1

Algèbres de relations : axiomatisations et algorithmes

Damien Pous

Les relations binaires sont des objets tellement basiques qu'ils sont omniprésents en mathématique et en informatique. Qu'il s'agisse de parler de graphes, de la sémantique de programmes, ou d'un argument de terminaison, des relations sont manipulées à un moment ou à un autre.

Dans ce cours, nous nous intéressons aux relations en elles-mêmes, et nous considérons les points de vue algébrique et algorithmique. Du côté algébrique, il s'agit de comprendre quelles lois régissent le comportement des opérations classiques sur les relations binaires : union, intersection, composition, converse, etc... Du côté algorithmique, il s'agit de trouver des procédures permettant de décider l'égalité ou l'inclusion de relations.

Après avoir défini formellement le calcul des relations, nous nous concentrons sur deux fragments particulièrement importants et bien étudiés dans la littérature : les algèbres de Kleene et les allégories. Enfin, nous montrons comment réunir ces deux fragments, ce qui nous mène à plusieurs questions ouvertes.

1.1 Le calcul des relations

Etant donné un ensemble P, une *relation* sur P est un ensemble de paires d'éléments de P. Par exemple, la relation d'ordre usuelle sur les entiers naturels est une relation. Dans la suite, les relations sont dénotées par les lettres R, S, leur ensemble est noté $\mathcal{P}(P \times P)$, et on écrit $p\,R\,q$ pour $\langle p, q\rangle \in R$.

L'ensemble des relations est naturellement muni d'un ordre partiel, l'inclusion ensembliste, ainsi que de trois opérations binaires : l'union ensembliste, notée $R + S$, l'intersection ensembliste, notée $R \cap S$, et la composition relationnelle :

$$R\cdot S \triangleq \{\langle p, q\rangle \mid \exists r \in P,\ p\,R\,r\ \wedge\ r\,S\,q\} \quad .$$

Il contient également trois relations particulières : la relation vide, notée 0, la relation pleine, notée $\top$, et la relation identité :

$$1 \triangleq \{\langle p, p\rangle \mid p \in P\} \quad .$$

Enfin, on peut considérer trois opérations unaires : le complément ensembliste, noté R^c, la converse et la clôture réflexive transitive :

$$\begin{aligned} &R^\circ \triangleq \{\langle p, q\rangle \mid q\,R\,p\} \quad , \\ &R^\star \triangleq \{\langle p, q\rangle \mid \exists p_0, \dots, p_n,\ p_0 = p\ \wedge\ p_n = q\ \wedge\ \forall i < n,\ p_i\,R\,p_{i+1}\} \quad . \end{aligned}$$

Nous nous limitons à cette liste d'opérations dans ce cours, bien qu'elle soit non exhaustive. Ces opérations permettent souvent d'énoncer des propriétés de manière concise, sans mentionner les points reliés par les relations. Voici quelques exemples :

$1 \subseteq R$	R est réflexive : $\forall p \in P, p\,R\,p$
$R\cdot R \subseteq R$	R est transitive : $\forall pqr,\ p\,R\,r \wedge r\,R\,q \Rightarrow p\,R\,q$
$R\cdot R^\star \cap 1 = 0$	R est acyclique : $\forall p_0 \dots p_n,\ n{>}0,\ (\forall i,\ p_i\,R\,p_{i+1}) \Rightarrow p_0 \neq p_n$
$R^\circ\cdot S \subseteq S\cdot R^\circ$	R et S commutent : $\forall pqr,\ r\,R\,p \wedge r\,S\,q \Rightarrow \exists t,\ q\,R\,t \wedge p\,S\,t$

Exercice 1.1.1. *Donner une expression algébrique pour caractériser la confluence locale d'une relation.*

De plus, ces opérations satisfont un certain nombre de lois. Certaines sont très simples (e.g., la composition est associative, $(R\cdot R')\cdot R'' = R\cdot(R'\cdot R'')$; la relation vide est absorbante pour la composition, $R\cdot 0 = 0 = 0\cdot R$; les clôtures réflexives transitives sont transitives, $R^\star\cdot R^\star \subseteq R^\star$), d'autres sont plus compliquées, voire contre-intuitives.

Exercice 1.1.2. *Parmi les égalités et inclusions suivantes, lesquelles sont universellement vraies ? Dans chaque cas, donner un contre-exemple ou une preuve détaillée.*

$$1 \cap R \subseteq R{\cdot}R \,\cap\, R{\cdot}R{\cdot}R \tag{1.1}$$
$$(R+S)^\star = R^\star{\cdot}(S^\star{\cdot}R)^\star \tag{1.2}$$
$$(R+S)^\star = ((1+R){\cdot}S)^\star \tag{1.3}$$
$$R{\cdot}(S \,\cap\, T) = R{\cdot}S \,\cap\, R{\cdot}T \tag{1.4}$$
$$R{\cdot}S \,\cap\, T \subseteq R{\cdot}(S \,\cap\, R^\circ{\cdot}T) \tag{1.5}$$
$$R{\cdot}S \,\cap\, T \subseteq (R \,\cap\, T{\cdot}S^\circ){\cdot}(S \,\cap\, R^\circ{\cdot}T) \tag{1.6}$$
$$(R \,\cap\, S{\cdot}\top){\cdot}T = R{\cdot}T \,\cap\, S{\cdot}\top \tag{1.7}$$

Se posent alors deux questions :

1. est-il possible d'axiomatiser l'ensemble des lois universellement vraies, c'est à dire donner un petit nombre de lois élémentaires, dont découlent toutes les autres ?
2. est-il possible de décider automatiquement la véracité d'une loi ?

Quand on considère l'ensemble des opérations listées ci-dessus, la réponse est négative dans les deux cas. En effet, Monk a démontré qu'il n'existe pas d'axiomatisation finie [13], et Tarski a démontré l'indécidabilité de la théorie équationnelle correspondante [18, 19]. Dans les deux cas, la clôture réflexive transitive n'est pas nécessaire, mais l'opération de complément joue un rôle crucial. Dans la suite du cours nous nous concentrons donc sur des fragments où cette opération de complément est absente.

Nous mettons maintenant en place des notions et notations nécessaires pour le reste du chapitre.

Soit Σ un ensemble, dont les éléments sont dénotés par les lettres a, b. Les *expressions (relationnelles)* sont définies par la grammaire suivante :

$$e, f, g ::= e + f \mid e \cap f \mid e \cdot f \mid e^\circ \mid e^\star \mid 0 \mid 1 \mid \top \mid a \in \Sigma \ .$$

Etant donnés un ensemble E et une fonction $\sigma : \Sigma \to \mathcal{P}(E \times E)$ associant à toute lettre de Σ une relation sur E, on définit par induction l'extension $\hat\sigma$ de σ aux expressions :

$$\begin{array}{ccc}
\hat\sigma(e+f) \triangleq \hat\sigma(e) + \sigma(f) & \hat\sigma(e^\circ) \triangleq \hat\sigma(e)^\circ & \hat\sigma(1) \triangleq 1 \\
\hat\sigma(e\cap f) \triangleq \hat\sigma(e) \cap \hat\sigma(f) & \hat\sigma(e^\star) \triangleq \hat\sigma(e)^\star & \hat\sigma(\top) \triangleq \top \\
\hat\sigma(e\cdot f) \triangleq \hat\sigma(e) \cdot \sigma(f) & \hat\sigma(0) \triangleq 0 & \hat\sigma(a) \triangleq \sigma(a)
\end{array}$$

Etant données deux expressions e et f, une équation est *valide*, notation $\vDash e = f$, si pour tout ensemble E et pour toute fonction $\sigma : \Sigma \to \mathcal{P}(E \times$

E), on a $\hat{\sigma}(e) = \hat{\sigma}(f)$. Intuitivement, une équation est valide si elle est universellement vraie dans les relations, si elle est vraie quelle que soit la manière d'interpréter ses variables.

De manière similaire, une inéquation est valide, notation $\vDash e \subseteq f$, si l'on a $\hat{\sigma}(e) \subseteq \hat{\sigma}(f)$ pour tout ensemble E et pour toute fonction $\sigma : \Sigma \to \mathcal{P}(E \times E)$. Caractériser les équations valides équivaut à caractériser les inéquations valides, comme le montre l'exercice suivant.

Exercice 1.1.3. *Soit e, f deux expressions. On a clairement $\vDash e = f$ ssi $\vDash e \subseteq f$ et $\vDash f \subseteq e$. Montrer que $\vDash e \subseteq f$ ssi $\vDash e + f = f$ ssi $\vDash e \cap f = e$.*

1.2 Le fragment idéal : les algèbres de Kleene

Dans cette section, nous retirons de la syntaxe les opérations d'intersection et de converse, ainsi que la constante $\top$. Autrement dit, nous nous restreignons aux expressions régulières :

$$e, f, g ::= e + f \mid e \cdot f \mid e^\star \mid 0 \mid 1 \mid a \in \Sigma \ .$$

Nous allons voir qu'avec cette restriction, la validité d'une équation devient un problème décidable, et en fait PSPACE-complet.

1.2.1 Décidabilité

Dénotons par les lettres u, v les mots finis sur l'alphabet Σ, par ϵ le mot vide, et par uv la concaténation de deux mots u et v. Un *langage* est un ensemble de mots (finis). On définit inductivement une fonction $[\cdot]$ associant un langage à toute expression :

$$\begin{aligned}
[e+f] &\triangleq [e] \cup [f] & [0] &\triangleq \emptyset \\
[e \cdot f] &\triangleq \{uv \mid u \in [e], v \in [f]\} & [1] &\triangleq \{\epsilon\} \\
[e^\star] &\triangleq \{u_1 \dots u_n \mid \forall i, u_i \in [e]\} & [a] &\triangleq \{a\}
\end{aligned}$$

La magie de ce fragment du calcul des relations est que l'on a la caractérisation suivante : une équation est valide pour les relations si et seulement si elle correspond à une égalité de langages.

Théorème 1.2.1. *Pour toute paire e, f d'expressions régulières, on a*

$$\vDash e = f \qquad \textit{ssi} \qquad [e] = [f] \ .$$

Nous prouvons ce théorème ci-dessous. Sa principale conséquence, en pratique, est la décidabilité du problème de la validité des équations : $[e]$ et $[f]$ sont des langages réguliers, que l'on peut facilement représenter par des automates finis, puis comparer. On en déduit aussi la complexité précise, puisque l'équivalence de deux expressions régulières est en fait un problème PSPACE-complet [12].

Démonstration. (du théorème 1.2.1)
Montrons tout d'abord l'implication directe. On suppose $\vDash e = f$, il nous suffit donc de trouver une fonction σ de l'alphabet Σ dans un espace de relations $\mathcal{P}(E \times E)$, telle que $\hat{\sigma}(e) = \hat{\sigma}(f)$ implique $[e] = [f]$. Prenons $E = \Sigma^\star$, l'ensemble des mots sur Σ, et définissons σ comme suit :

$$\begin{aligned} \sigma : \Sigma &\to \mathcal{P}(\Sigma^\star \times \Sigma^\star) \\ a &\mapsto \{\langle u, ua\rangle \mid u \in \Sigma^\star\} \end{aligned}$$

On montre alors par que pour toute expression g, on a

$$\hat{\sigma}(g) = \{\langle u, uv\rangle \mid u \in \Sigma^\star, v \in [g]\} \quad ,$$

par induction sur l'expression g :

— $g = g' + g''$: on a

$$\begin{aligned} \hat{\sigma}(g) &= \hat{\sigma}(g') \cup \hat{\sigma}(g'') \\ &= \left\{\langle u, uv\rangle \mid u \in \Sigma^\star, v \in [g']\right\} \cup \left\{\langle u, uv\rangle \mid u \in \Sigma^\star, v \in [g'']\right\} \\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{(par induction)} \\ &= \left\{\langle u, uv\rangle \mid u \in \Sigma^\star, v \in [g'] \cup [g'']\right\} \\ &= \left\{\langle u, uv\rangle \mid u \in \Sigma^\star, v \in [g' + g'']\right\} \end{aligned}$$

— $g = g' \cdot g''$: on a

$$\begin{aligned} \hat{\sigma}(g) &= \hat{\sigma}(g') \cdot \hat{\sigma}(g'') \\ &= \left\{\langle u, uv\rangle \mid u \in \Sigma^\star, v \in [g']\right\} \cdot \left\{\langle u', u'w\rangle \mid u' \in \Sigma^\star, w \in [g'']\right\} \\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{(par induction)} \\ &= \left\{\langle u, uvw\rangle \mid u \in \Sigma^\star, v \in [g'], w \in [g'']\right\} \\ &= \left\{\langle u, uv\rangle \mid u \in \Sigma^\star, v \in [g' \cdot g'']\right\} \end{aligned}$$

— $g = g'^\star$: de manière similaire au point précédent, on a

$$\begin{aligned} \hat{\sigma}(g) &= \hat{\sigma}(g')^\star \\ &= \left\{\langle u, uv\rangle \mid u \in \Sigma^\star, v \in [g']\right\}^\star && \text{(par induction)} \\ &= \left\{\langle u, uv\rangle \mid u \in \Sigma^\star, v \in [g']^\star\right\} \end{aligned}$$

(pour la dernière étape, on démontre d'abord la propriété suivante : $\{\langle u, uv\rangle \mid u \in \Sigma^\star, v \in L\}^k = \left\{\langle u, uv\rangle \mid u \in \Sigma^\star, v \in L^k\right\}$, où $L \subseteq \Sigma^\star$ est un langage arbitraire, par récurrence sur $k \in \mathbb{N}$).

— $g = 0$, $g = 1$, $g = a$: il suffit de dérouler les définitions.

En particulier, on a donc $v \in [g]$ si et seulement si $\langle \epsilon, v\rangle \in \hat{\sigma}(g)$, de telle sorte que $\hat{\sigma}(e) = \hat{\sigma}(f)$ implique $[e] = [f]$.

Considérons maintenant l'autre l'implication. Soient un ensemble E et une fonction $\sigma : \Sigma \to \mathcal{P}(E \times E)$; il nous faut montrer que $[e] = [f]$ implique $\hat{\sigma}(e) = \hat{\sigma}(f)$. Cette implication découle immédiatement de la propriété suivante, que l'on démontre par induction sur l'expression g :

$$\hat{\sigma}(g) = \bigcup_{v \in [g]} \hat{\sigma}(v) \ .$$

(Notons l'abus de notation dans le terme de l'union : on applique la fonction $\hat{\sigma}$, qui attend une expression régulière, à v qui est un mot, on utilise donc implicitement l'injection naturelle des mots vers les expressions.)

— $g = g' + g''$: on a

$$\begin{aligned}
\hat{\sigma}(g) &= \hat{\sigma}(g') \cup \hat{\sigma}(g'') \\
&= \bigcup_{v \in [g']} \hat{\sigma}(v) \ \cup \bigcup_{v \in [g'']} \hat{\sigma}(v) && \text{(par induction)} \\
&= \bigcup_{v \in [g'] \cup [g'']} \hat{\sigma}(v) \\
&= \bigcup_{v \in [g' + g'']} \hat{\sigma}(v)
\end{aligned}$$

— $g = g' \cdot g''$: on a

$$\begin{aligned}
\hat{\sigma}(g) &= \hat{\sigma}(g') \cdot \hat{\sigma}(g'') \\
&= \bigcup_{v \in [g']} \hat{\sigma}(v) \cdot \bigcup_{w \in [g'']} \hat{\sigma}(w) && \text{(par induction)} \\
&= \bigcup_{v \in [g'],\ w \in [g'']} \hat{\sigma}(v) \cdot \hat{\sigma}(w) && \text{(distributivité)} \\
&= \bigcup_{v \in [g'],\ w \in [g'']} \hat{\sigma}(v \cdot w) \\
&= \bigcup_{u \in [g' \cdot g'']} \hat{\sigma}(u)
\end{aligned}$$

— $g = g'^\star$: on a

$$\begin{aligned}
\hat\sigma(g) &= \hat\sigma(g')^\star \\
&= \left(\bigcup_{v\in[g']} \hat\sigma(v)\right)^\star && \text{(par induction)} \\
&= \bigcup_{v_1\in[g'],\dots,v_n\in[g']} \hat\sigma(v_1)\cdot\dots\cdot\hat\sigma(v_n) \\
&= \bigcup_{v_1\in[g'],\dots,v_n\in[g']} \hat\sigma(v_1\cdot\dots\cdot v_n) \\
&= \bigcup_{u\in[g']^\star} \hat\sigma(u) \\
&= \bigcup_{u\in[g'^\star]} \hat\sigma(u)
\end{aligned}$$

— $g = 0$, $g = 1$, $g = a$: à nouveau, il suffit de dérouler les définitions.

□

Notons que cette preuve mène à une caractérisation similaire pour les inéquations : pour toutes expressions régulières e et f,

$$\models e \subseteq f \qquad \text{ssi} \qquad [e] \subseteq [f] \ .$$

1.2.2 Axiomatisation

En 1956, Kleene pose déjà la question de l'axiomatisabilité de la théorie précédente [6] : est-il possible de trouver un ensemble fini d'axiomes (d'équations), dont découlent toutes les équations valides entre expressions régulières ?

Dans les années 60, Salomaa donne deux axiomatisations infinies [17], et Redko prouve l'impossibilité d'obtenir une axiomatisation finie [16]. Conway étudie extensivement ce genre de questions dans son monographe sur les algèbres régulières et les automates finis [6], mais ce n'est qu'au début des années 90 que tombent de nouveaux résultats : Krob et Kozen montrent indépendemment que l'on peut axiomatiser la théorie de manière finie, à condition de s'autoriser des axiomes qui ne sont plus de simples équations, mais des implications entre équations (on passe des variétés au quasi-variétés).

La preuve de Krob est longue est difficile [11], mais elle fait complètement le tour de la question : il donne tout d'abord une nouvelle axiomatisation purement équationnelle, infinie mais avec plus de structure

$$\left.\begin{array}{c} e+(f+g)=(e+f)+g \\ e+f=f+e \\ e+0=e \\ e+e=e \end{array}\right\} \text{$\langle +,0\rangle$ est un monoide commutatif idempotent}$$

$$\left.\begin{array}{c} e\cdot(f\cdot g)=(e\cdot f)\cdot g \\ e\cdot 1=e \\ 1\cdot e=e \end{array}\right\} \text{$\langle \cdot,1\rangle$ est un monoide}$$

$$\left.\begin{array}{c} e\cdot(f+g)=e\cdot f+e\cdot g \\ (e+f)\cdot g=e\cdot g+f\cdot g \\ e\cdot 0=0 \\ 0\cdot e=0 \end{array}\right\} \text{distribution entre les deux monoides}$$

$$\left.\begin{array}{c} 1+e\cdot e^\star=e^\star \\ e\cdot f\leq f \quad\Rightarrow\quad e^\star\cdot f\leq f \\ f\cdot e\leq f \quad\Rightarrow\quad f\cdot e^\star\leq f \end{array}\right\} \text{lois sur l'étoile de Kleene}$$

FIGURE *1.1 – Les axiomes des algèbres de Kleene*

que les axiomatisations de Salomaa. Il démontre ensuite que cette infinité d'axiomes peut être prouvée à l'aide de diverses axiomatisations finies, mais faisant intervenir des implications entre équations.

A l'inverse, Kozen va droit au but, en se concentrant sur une axiomatisation particulière (finie et comprenant des implications). Sa preuve n'est pas simple non plus, mais beaucoup plus courte [9, 10].

Théorème 1.2.2 (Kozen'91, Krob'91)**.** *Pour toutes expressions régulières e, f, on a $[e] = [f]$ si et seulement si l'égalité $e = f$ est dérivable à partir des axiomes listés Figure 1.1, où la notation $e \leq f$ est une abréviation pour $e + f = f$.*

Les axiomes sont naturellement agencés en quatre groupes : les trois premiers groupes correspondent au fait que l'on a un semi-anneau non-commutatif et idempotent ; le dernier groupe d'axiomes caractérise l'opération de clôture réflexive transitive, souvent appelée dans ce contexte "étoile de Kleene". Ce dernier groupe n'est pas entièrement symétrique : il manque la loi $1 + e^\star\cdot e = e^\star$, qui est en fait dérivable. Les deux derniers axiomes sont des implications ; intuitivement, ils traduisent le fait que si une expression f est invariante par composition avec une autre expression e, alors elle l'est aussi avec $e^\star$. Ce sont ces implications qui donnent toute sa puissance à cette axiomatisation : elles permettent de raisonner inductivement sur l'étoile de Kleene, de manière algébrique.

On vérifie aisément que chacun de ces axiomes est satisfait dans le modèle des relations binaires mais également lorsque l'on interprète les expressions e, f, g par des langages arbitraires. Ceci donne facilement l'implication retour du théorème 1.2.2 : on ne prouve que des choses vraies à l'aide de ces axiomes.

Toute la difficulté réside dans l'autre direction : la complétude de cet ensemble d'axiomes, le fait que toute équation valide puisse effectivement être déduite de ces axiomes. Nous ne détaillons pas la preuve ici ; une étape clef consiste à démontrer que l'espace des matrices à coefficients dans une algèbre de Kleene est à nouveau une algèbre de Kleene (une algèbre de Kleene étant une structure satisfaisant les axiomes de la figure 1.1).

Exercice 1.2.3. *Démontrer les lois suivantes, en utilisant seulement les axiomes des algèbres de Kleene :*

$$\begin{aligned}
g + e\cdot f \subseteq f &\Rightarrow e^\star\cdot g \subseteq f \\
g + f\cdot e \subseteq f &\Rightarrow g\cdot e^\star \subseteq f \\
1 + e^\star\cdot e &= e^\star \\
e\cdot f \subseteq g\cdot e &\Rightarrow e\cdot f^\star \subseteq g^\star\cdot e \\
e\cdot f = g\cdot e &\Rightarrow e\cdot f^\star = g^\star\cdot e \\
e\cdot(f\cdot e)^\star &= (e\cdot f)^\star\cdot e \\
(e+f)^\star &= e^\star\cdot(f^\star\cdot e)^\star
\end{aligned}$$

1.3 Le fragment bizarre : les allégories

Considérons maintenant un fragment différent, où l'on n'a que la composition, l'intersection, la converse, et les constantes 1 et $\top$. Pour une raison qui deviendra claire à la section 1.4, nous réutilisons les lettres u, v, w pour dénoter les expressions correspondantes, que nous appellerons *termes* :

$$u, v, w ::= u \cdot v \mid u \cap v \mid u^\circ \mid 1 \mid \top \mid a \in \Sigma \ .$$

Modulo la présence de la constante $\top$, ce fragment correspond aux *allégories*, étudiées par Freyd et Scedrov [8] ; il a également été étudié par Andréka et Bredikhin [2]. Nous allons voir que l'on peut décider de la

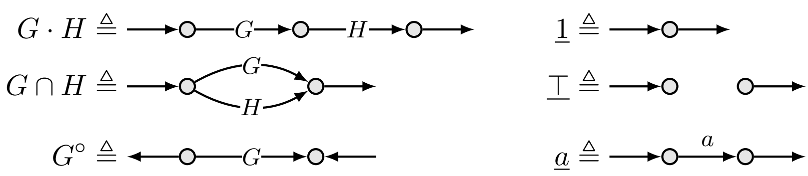


FIGURE 1.2 – *Opérations sur les graphes*

validité des inclusions (et donc des équations) dans ce fragment, mais qu'à nouveau, la théorie correspondante n'est pas finiment axiomatisable de manière purement équationnelle.

1.3.1 Décidabilité

L'idée clef consiste à caractériser les inclusions valides par des homomorphismes de graphes. Plus précisément, de graphes dirigés, aux arêtes étiquetés par Σ, et avec deux sommets distingués.

Définition 1.3.1 (Graphe). *Un* graphe *est un quadruplet $\langle V, E, \iota, o\rangle$, où V est un ensemble de* sommets, *$E \subseteq V \times \Sigma \times V$ est un ensemble d'arêtes étiquetés, et $\iota, o \in V$ sont deux sommets distingués, appelés respectivement* entrée *et* sortie.

On utilise les lettres G, H pour dénoter des graphes, on définit les opérations suivantes :
- $G \cdot H$ est le graphe obtenu en branchant les deux graphes en série, c'est à dire en les mettant bout à bout, en fusionnant la sortie de G avec l'entrée de H ;
- $G \cap H$ est le graphe obtenu en mettant les deux graphes en parallèle, en fusionnant leurs entrées et leurs sorties ;
- G° est le graphe obtenu à partir de G en échangeant entrée et sortie (mais sans inverser les arêtes) ;
- $\underline{1}$ est le graphe sans arête à un sommet $(\langle \{*\}, \emptyset, *, *\rangle)$;
- $\underline{\top}$ est le graphe sans arête à deux sommets, où entrée et sortie sont distinctes $(\langle \{\dagger, \ddagger\}, \emptyset, \dagger, \ddagger\rangle)$;
- pour $a \in \Sigma$, $\underline{a}$ est le graphe à deux sommets et une arête étiquetée par a allant de l'entrée à la sortie $(\langle \{\dagger, \ddagger\}, \{\langle \dagger, a, \ddagger\rangle\}, \dagger, \ddagger\rangle)$.

Ces opérations sont représentées graphiquement sur la figure 1.2 ; l'entrée et la sortie de chaque graphe sont dénotées par deux flèches non étiquetées. Elles permettent naturellement d'associer un graphe $G(u)$ à tout

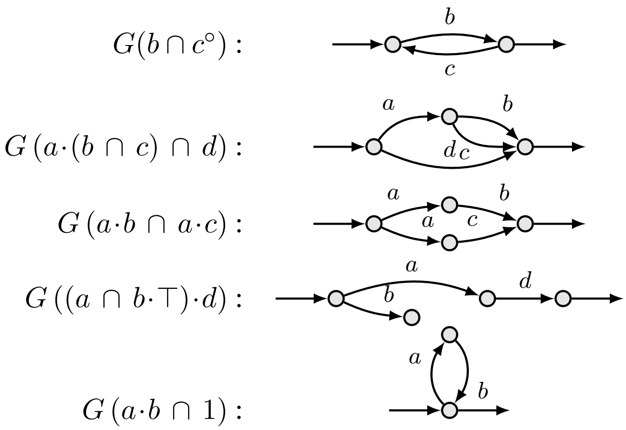


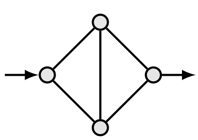
FIGURE 1.3 – *Graphes associés à certains termes.*

terme u, par induction structurelle :

$$
\begin{aligned}
G(u \cdot v) &\triangleq G(u) \cdot G(v) & \qquad G(1) &\triangleq \underline{1} \\
G(u \cap v) &\triangleq G(u) \cap G(v) & G(\top) &\triangleq \underline{\top} \\
G(u^\circ) &\triangleq G(u)^\circ & G(a) &\triangleq \underline{a}
\end{aligned}
$$

Les graphes de quelques termes sont donnés sur la figure 1.3. Ce sont des graphes série-parallèle tant que l'on n'utilise ni la converse ou l'identité, qui introduisent des cycles en présence de l'intersection, ni la constante $\top$, qui peut déconnecter certaines parties des graphes.

Certains graphes ne sont l'image d'aucun terme. Le contre-exemple canonique est le suivant (peu importe l'étiquetage et l'orientation des cinq arêtes, d'où l'omission de ces informations).



(1.8)

On équipe finalement l'ensemble des graphes du préordre suivant :

Définition 1.3.2. *Un* homomorphisme *du graphe G vers le graphe H est une fonction des sommets de G dans ceux de H préservant arêtes étiquetées, entrée, et sortie. On note $H \blacktriangleleft G$ lorsqu'il existe un homomorphisme de G vers H.*

Par exemple, le graphe de $a{\cdot}(b \,\cap\, c) \,\cap\, d$ est plus petit que le graphe de $a{\cdot}b \,\cap\, a{\cdot}c$, grâce à l'homomorphisme représenté sur la figure 1.4 par des flèches en pointillés. Notons que les homomorphismes n'ont besoin

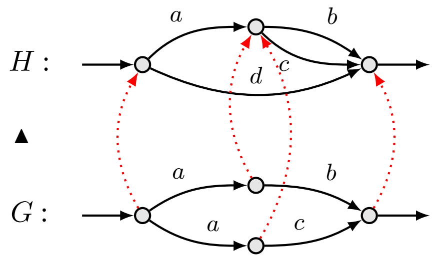


FIGURE 1.4 – *Un homomorphisme de graphe.*

ni d'être injectifs ni d'être surjectifs, de sorte que le préordre n'a aucun lien avec la taille des graphes : un graphe peut parfaitement être plus petit qu'un autre, au sens du préordre, tout en ayant plus de sommets ou d'arêtes (et vice versa).

Le miracle dans le fragment considéré ici est que l'on a la caractérisation suivante : une inclusion est valide pour les relations si et seulement si elle correspond à un homomorphisme de graphe :

Théorème 1.3.3 ([2, Théorème 1], [8, page 208])**.** *Pour toute paire u, v de termes, on a*

$$\vDash u \subseteq v \qquad \textit{ssi} \qquad G(u) \blacktriangleleft G(v) \ .$$

Les graphes de termes étant finis, on peut chercher un homomorphisme entre deux tels graphes de manière exhaustive, d'où la décidabilité du problème.

Exercice 1.3.4. *Prouver les lois* (1.1), (1.5), (1.6), *et* (1.7) *de l'exercice 1.1.2, en utilisant le théorème 1.3.3.*

On a besoin d'un lemme pour prouver le théorème.

Lemme 1.3.5. *Soit u un terme et $G(u) = \langle V, E, \iota, o\rangle$ son graphe. Soit S un ensemble et $\sigma : \Sigma \to \mathcal{P}(S \times S)$ une fonction d'interprétation. Pour tous éléments $i, j \in S$, on a $\langle i, j\rangle \in \hat{\sigma}(u)$ ssi il existe une fonction $\phi : V \to S$ telle que :*

$$\begin{cases} \phi(\iota) = i \,, \\ \phi(o) = j \,, \ \textit{et} \\ \langle p, a, q\rangle \in E \ \Rightarrow \ \langle \phi(p), \phi(q)\rangle \in \sigma(a) \ . \end{cases}$$

Démonstration. On procède par induction sur u :

— $u = v \cdot w$: notons $G(v) = \langle V_v, E_v, \iota_v, o_v \rangle$ et $G(w) = \langle V_w, E_w, \iota_w, o_w \rangle$. On a $\langle i,j \rangle \in \hat{\sigma}(u) = \hat{\sigma}(v) \cdot \hat{\sigma}(w)$ ssi il existe $k \in S$ tel que $\langle i,k \rangle \in \hat{\sigma}(v)$ et $\langle k,j \rangle \in \hat{\sigma}(w)$. Par induction, cette dernière propriété est équivalente à l'existence de deux fonctions $\phi_u : V_u \to S$ et $\phi_v : V_v \to S$ telles que $\phi_u(\iota_u) = i$, $\phi_u(o_u) = k$, $\langle p,a,q \rangle \in E_u$ implique $\langle \phi_u(p), \phi_u(q) \rangle \in \sigma(a)$, $\phi_v(\iota_v) = k$, $\phi_v(o_v) = j$, et $\langle p,a,q \rangle \in E_v$ implique $\langle \phi_v(p), \phi_v(q) \rangle \in \sigma(a)$. En recollant ces deux fonctions, on montre aisément l'équivalence avec l'existence d'une unique fonction depuis le graphe $G(u) = G(v) \cdot G(w)$ satisfaisant les propriétés de l'énoncé.

— $u = v \cap w$: avec les notations du point précédent, on a $\langle i,j \rangle \in \hat{\sigma}(u) = \hat{\sigma}(v) \cap \hat{\sigma}(w)$ ssi $\langle i,j \rangle \in \hat{\sigma}(v)$ et $\langle i,j \rangle \in \hat{\sigma}(w)$. Par induction, cette conjonction est équivalente à l'existence de deux fonctions $\phi_u : V_u \to S$ et $\phi_v : V_v \to S$ telles que $\phi_x(\iota_x) = i$, $\phi_x(o_x) = j$, et $\langle p,a,q \rangle \in E_x$ implique $\langle \phi_x(p), \phi_x(q) \rangle \in \sigma(a)$, pour $x \in \{u,v\}$. Comme précédemment, on montre aisément l'équivalence avec l'existence d'une unique fonction depuis le graphe $G(u) = G(v) \cap G(w)$, satisfaisant les propriétés de l'énoncé.

— $u = 1$: par définition, on a $\langle i,j \rangle \in \hat{\sigma}(u) = 1$ ssi $i = j$, et l'existence d'une fonction ϕ satisfaisant les propriétés de l'énoncé pour le graphe $\underline{1}$ est également équivalente à $i = j$.

— $u = \top$: par définition, $\langle i,j \rangle \in \hat{\sigma}(u) = \top$ est toujours vrai ; et l'existence d'une fonction ϕ satisfaisant les propriétés de l'énoncé pour le graphe $\underline{\top}$ est toujours garantie.

— $u = a$: $\hat{\sigma}(u) = \sigma(a)$ l'existence d'une fonction ϕ satisfaisant les propriétés de l'énoncé pour le graphe $\underline{a}$ équivaut à l'appartenance du couple $\langle i,j \rangle$ à $\sigma(a)$. □

Démonstration. (du théorème 1.3.3)
Notons $G(u) = \langle V, E, \iota, o \rangle$ et $G(v) = \langle V', E', \iota', o' \rangle$.

Commençons par l'implication de droite à gauche : supposons $G(u) \blacktriangleleft G(v)$, c'est à dire l'existence d'un homomorphisme γ de $G(v)$ dans $G(u)$, et montrons $\vDash u \subseteq v$. Soit S un ensemble et $\sigma : \Sigma \to \mathcal{P}(S \times S)$ une fonction d'interprétation ; pour tout $\langle i,j \rangle \in \hat{\sigma}(u)$ (†), montrons que $\langle i,j \rangle \in \hat{\sigma}(v)$ (‡). Soit $\phi : V \to S$ la fonction donnée par le lemme 1.3.5 à partir de l'hypothèse (†) ; par le même lemme, il suffit pour prouver (‡) de trouver une fonction $\psi : V' \to S$ satisfaisant $\psi(\iota') = i$, $\psi(o') = j$, et $\langle p', a, q' \rangle \in E'$ implique $\langle \psi(p'), \psi(q') \rangle \in \sigma(a)$. La fonction composée $\phi \circ \gamma$ convient.

Montrons maintenant l'implication directe. On suppose $\vDash u \subseteq v$, et il nous faut trouver un homomorphisme de $G(v)$ dans $G(u)$. Soit σ la fonc-

$$\left.\begin{aligned} e\cap(f\cap g)&=(e\cap f)\cap g\\ e\cap f&=f\cap e\\ e\cap\top&=e\\ e\cap e&=e\end{aligned}\right\}\ \begin{array}{l}\langle\cap,\top\rangle\text{ est un monoide}\\ \text{commutatif idempotent}\end{array}$$

$$\left.\begin{aligned} e\cdot(f\cdot g)&=(e\cdot f)\cdot g\\ e\cdot 1&=e\\ 1\cdot e&=e\end{aligned}\right\}\ \langle\cdot,1\rangle\text{ est un monoide}$$

$$\left.\begin{aligned} e\cdot(f\cap g)&\subseteq e\cdot f\\ (f\cap g)\cdot e&\subseteq f\cdot e\end{aligned}\right\}\ \text{monotonie du produit}$$

$$\left.\begin{aligned} e^{\circ\circ}&=e\\ (e\cap f)^\circ&\subseteq e^\circ\\ (e\cdot f)^\circ&\subseteq f^\circ\cdot e^\circ\end{aligned}\right\}\ \begin{array}{l}\text{la converse est une involution}\\ \text{monotone renversant le produit}\end{array}$$

$$e{\cdot}f\ \cap\ g\subseteq(e\ \cap\ g{\cdot}f^\circ)\cdot f\quad\}\ \text{loi de modularité}$$

FIGURE 1.5 – *Les axiomes des allégories*

tion d'interprétation suivante :

$$\begin{aligned}\sigma:\Sigma&\to\mathcal{P}(V\times V)\\ a&\mapsto\{\langle p,q\rangle\mid\langle p,a,q\rangle\in E\}\end{aligned}$$

Par le lemme 1.3.5, en utilisant la fonction identité, on a $\langle\iota,o\rangle\in\hat{\sigma}(u)$. Par hypothèse, on en déduit $\langle\iota,o\rangle\in\hat{\sigma}(v)$, d'où en utilisant à nouveau le lemme 1.3.5, l'existence d'une fonction $\phi:V'\to V$ satisfaisant certaines propriétés. Ces propriétés expriment précisément le fait que ϕ est un homomorphisme de $G(v)$ dans $G(u)$. $\square$

1.3.2 Axiomatisation

Freyd et Scedrov définissent les *allégories* [8] comme étant les structures satisfaisant les axiomes de la figure 1.5 [1]. Notons tout d'abord que le produit ne distribue pas sur les intersections : il est monotone en ses

1. A quelques détails près, notamment le fait qu'ils ne considèrent pas la constante $\top$, et qu'ils travaillent dans un cadre catégorique où les différentes opérations sont typées.

deux arguments, ce qui implique les inclusions suivantes mais pas leurs contreparties :

$$e \cdot (f \cap g) \subseteq e{\cdot}f \ \cap \ e{\cdot}g$$
$$(f \cap g) \cdot e \subseteq f{\cdot}e \ \cap \ g{\cdot}e$$

On peut aussi déduire des axiomes que la converse renverse le produit, distribue sur les intersections, et préserve les constantes 1 et $\top$:

$$(e \cap f)^\circ = e^\circ \cap f^\circ \qquad\qquad \top^\circ = \top$$
$$(e \cdot f)^\circ = f^\circ \cdot e^\circ \qquad\qquad 1^\circ = 1$$

Le dernier axiome est moins naturel. Il est appelé *loi de modularité*, il est équivalent en présence des autres axiomes à son symétrique :

$$e{\cdot}f \ \cap \ g \subseteq e \cdot (f \ \cap \ e^\circ{\cdot}g)$$

Il a pour conséquence l'inclusion suivante, connue sous le nom de *loi de Dedekind* :

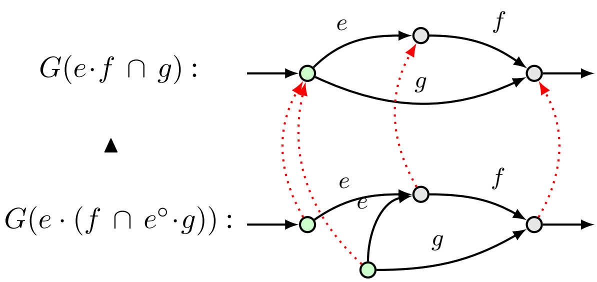
$$e{\cdot}f \ \cap \ g \subseteq (e \ \cap \ g{\cdot}f^\circ) \cdot (f \ \cap \ e^\circ{\cdot}g)$$

Exercice 1.3.6. *Prouver les huit lois précédentes à partir des axiomes de la figure 1.5.*

Malheureusement, cette axiomatisation finie et purement équationnelle n'est pas complète pour le calcul des relations : certaines équations valides ne sont pas des conséquences des axiomes. Freyd et Scedrov ont en fait démontré qu'il n'existe pas d'axiomatisation purement équationnelle finie. Sans aller jusqu'à le prouver, nous donnons ici quelques intuitions sur ce résultat. Vérifions tout d'abord que l'axiomatisation est correcte :

Exercice 1.3.7. *Prouver que chacun des axiomes est valide, en utilisant le théorème 1.3.3 : dessiner chacun des graphes et expliciter les homomorphismes correspondant à chaque inclusion.*

On constate en faisant l'exercice ci-dessus que le seul homomorphisme non injectif est celui correspondant à la loi de modularité, et que cet homomorphisme égalise exactement deux sommets :



On a en fait le résultat suivant :

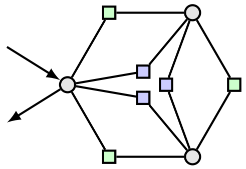
Proposition 1.3.8. *Soient u et v deux termes. S'il existe un homomorphisme de $G(v)$ vers $G(u)$ égalisant au plus deux sommets, alors l'inclusion $u \subseteq v$ est prouvable à partir des axiomes des allégories.*

Démonstration. Exercice laissé au lecteur par Freyd et Scedrov [8]. □

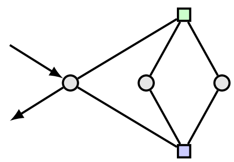
La réciproque n'est bien sûr pas vraie : de nombreuses inclusions dérivables à partir des axiomes correspondent à des homomorphismes arbitraires (par exemple, la loi de Dedekind, où deux paires de sommets sont égalisées, ou l'inclusion (1.1) de l'exercice 1.1.2, où les cinq sommets du membre droit sont égalisés).

Considérons maintenant un homomorphisme arbitraire depuis le graphe d'un terme v vers celui d'un terme u. Cet homomorphisme peut être décomposé de plusieurs manières en une séquence d'homomorphismes égalisant au plus deux sommets chacun. On pourrait donc croire qu'il suffit d'utiliser la proposition 1.3.8 pour obtenir une suite d'inclusions dérivables, menant à une preuve de $u \subseteq v$ à partir des axiomes des allégories.

Le problème est que les graphes intermédiaires apparaissant à travers cette séquence d'homomorphismes ne sont pas toujours des graphes issus de termes (cf. le graphe (1.8)). Voici un contre-exemple ; à nouveau nous n'étiquetons pas les arêtes et nous ne donnons pas leur orientation : ces informations importent peu. Considérons le graphe suivant :



Ce graphe correspond à un terme de la forme $1 \cap \Pi_{i=1,2,3}(a_i{\cdot}b_i \cap c_i{\cdot}d_i)$. Si l'on égalise les trois sommets carrés du centre, ainsi que les trois sommets carrés de l'extérieur, on obtient le graphe suivant :



Ce graphe est associé à un terme, de la forme $1 \cap i{\cdot}(e{\cdot}f \cap g{\cdot}h){\cdot}j$, de telle sorte que l'homomorphisme implicitement considéré correspond bien à une inclusion valide entre deux termes.

Cet homomorphisme égalise d'un coup deux groupes de trois sommets. Cherchons maintenant à le décomposer en une séquence de quatre homomorphismes égalisant chacun exactement deux sommets. Le premier homomorphisme doit égaliser deux sommets bleus ou deux sommets verts, et quelque soit le cas, on obtient un graphe qui n'est le graphe d'aucun terme.

En formalisant plus précisément cette idée, on obtient une inclusion valide qui n'est pas prouvable à partir des axiomes, d'où l'incomplétude de l'axiomatisation. On peut même généraliser un peu le contre-exemple, et montrer que toute axiomatisation complète doit contenir des axiomes correspondant à des homomorphismes égalisant un nombre arbitraire de sommets, d'où l'impossibilité d'avoir une axiomatisation finie [8, page 210].

1.4 Mettre tout ensemble

Revenons au problème initial, celui du calcul des relations sans complément. Nous avons vu que deux fragments étaient décidables : le fragment correspondant aux expressions régulières $(+, \cdot, \cdot^\star, 0, 1)$, et celui correspondant aux allégories $(\cap, \cdot, \cdot^\circ, \top, 1)$. Que se passe-t-il lorsque l'on prend toutes les opérations ?

Notons tout d'abord que la fonction $[\cdot]$ associant un langage (régulier) à toute expression régulière peut naturellement être étendue aux opérations des allégories :

$$\begin{aligned} [e \cap f] &\triangleq [e] \cap [f] \\ [e^\circ] &\triangleq \{a_n \dots a_1 \mid a_1 \dots a_n \in [e]\} \\ [\top] &\triangleq \Sigma^\star \end{aligned}$$

Cependant, la caractérisation obtenue au théorème 1.2.1 ne fonctionne plus avec ces opérations. En effet, on a par exemple

$$\begin{aligned} [a \cap b] = \{a\} \cap \{b\} = \emptyset = [0] &\text{ mais } \not\models a \cap b = 0 \\ [a^\circ] = \{a\} = [a] &\text{ mais } \not\models a^\circ = a \\ [a] = \{a\} \not\subseteq \{aaa\} = [a \cdot a^\circ \cdot a] &\text{ mais } \models a \subseteq a \cdot a^\circ \cdot a \\ [\top \cdot a \cdot \top \cdot b \cdot \top] \neq [\top \cdot b \cdot \top \cdot a \cdot \top] &\text{ mais } \models \top \cdot a \cdot \top \cdot b \cdot \top = \top \cdot b \cdot \top \cdot a \cdot \top \end{aligned}$$

Pour obtenir une caractérisation, il faut en fait remplacer les mots (les éléments $\Sigma^\star$) par des graphes, et donc considérer des langages de graphes.

Définition 1.4.1. *Le* langage de graphes *d'une expression e, noté $\mathcal{G}(e)$, est défini comme suit, par induction sur e :*

$$\begin{aligned}
\mathcal{G}(e+f) &\triangleq \mathcal{G}(e) \cup \mathcal{G}(f) & \mathcal{G}(0) &\triangleq \emptyset \\
\mathcal{G}(e \cap f) &\triangleq \{G \cap H \mid G \in \mathcal{G}(e)\,,\ H \in \mathcal{G}(f)\} & \mathcal{G}(\top) &\triangleq \{\underline{\top}\} \\
\mathcal{G}(e \cdot f) &\triangleq \{G \cdot H \mid G \in \mathcal{G}(e)\,,\ H \in \mathcal{G}(f)\} & \mathcal{G}(1) &\triangleq \{\underline{1}\} \\
\mathcal{G}(e^\star) &\triangleq \{G_1 \cdot \dots \cdot G_n \mid n \in \mathbb{N},\ \forall i \leq n, , G_i \in \mathcal{G}(e)\} & \mathcal{G}(a) &\triangleq \{\underline{a}\} \\
\mathcal{G}(e^\circ) &\triangleq \{G^\circ \mid G \in \mathcal{G}(e)\}
\end{aligned}$$

Cette définition généralise la notion usuelle de langage : lorsque l'expression considérée ne contient ni intersection, ni converse, ni la constante $\top$, alors les graphes associés sont isomorphes aux mots : ce sont de simple fils étiquetés par un certain nombre de lettres de Σ.

Pour généraliser aussi le cas des allégories, il faut faire intervenir les homomorphismes de graphes. Etant donné un ensemble L de graphes, on note ${}^{◀}L$ sa *clôture par le bas* vis à vis du préordre (◀) :

$$^{◀}L \triangleq \{G \mid \exists H, G ◀ H,\ H \in L\} \quad .$$

On obtient enfin la caractérisation suivante :

Théorème 1.4.2. *Pour toute paire e, f d'expressions, on a*

$$\models e \subseteq f \qquad \textit{ssi} \qquad \mathcal{G}(e) \subseteq {}^{◀}\mathcal{G}(f) \quad .$$

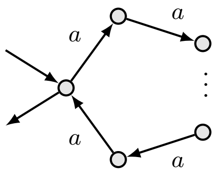
Démonstration. Similaire à la preuve du théorème 1.2.1, en exploitant le théorème 1.3.3 (cf. [5, théorème 6], l'ajout de la constante $\top$ ne pose pas de difficulté). □

Cette caractérisation généralise bien les théorèmes 1.2.1 et 1.3.3. Si e et f sont des expressions régulières, alors tous les graphes de $\mathcal{G}(e)$ et $\mathcal{G}(f)$ sont des fils, et le seul homomorphisme possible entre deux tels graphes est l'identité, d'où $\mathcal{G}(e) \subseteq {}^{◀}\mathcal{G}(f)$ ssi $\mathcal{G}(e) \subseteq \mathcal{G}(f)$. Si e et f sont maintenant de simples termes u et v, alors $\mathcal{G}(e) = \{G(u)\}$ et $\mathcal{G}(f) = \{G(v)\}$, de telle sorte que $\mathcal{G}(e) \subseteq {}^{◀}\mathcal{G}(f)$ équivaut à $G(u) ◀ G(v)$.

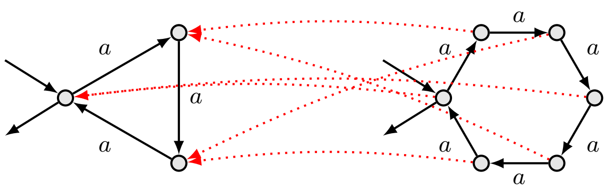
Notons aussi que pour tous langages de graphes L, K, on a $L \subseteq {}^{◀}K$ ssi ${}^{◀}L \subseteq {}^{◀}K$. Les équations valides sont donc naturellement caractérisées comme suit :

$$\models e = f \qquad \text{ssi} \qquad {}^{◀}\mathcal{G}(e) = {}^{◀}\mathcal{G}(f) \quad .$$

Pour illustrer ce théorème, considérons les expressions $e \triangleq a^+ \cap 1$ et $f \triangleq (a{\cdot}a)^+ \cap 1$, où g^+ est une abréviation pour $g{\cdot}g^\star$. L'ensemble de graphes $\mathcal{G}(e)$ est l'ensemble des cycles non triviaux étiquetés par des a :



De son côté, $\mathcal{G}(f)$ est l'ensemble des cycles non-triviaux et de longueur paire. On a donc immédiatement $\mathcal{G}(f) \subseteq \mathcal{G}(e) \subseteq {}^{\blacktriangleleft}\mathcal{G}(e)$, d'où $\vDash f \subseteq e$. L'autre inclusion est aussi valide : à tout cycle de $\mathcal{G}(e)$, possiblement impair, on peut associer le cycle de longueur double, dans $\mathcal{G}(f)$; on a alors bien un homomorphisme du cycle double dans le cycle simple :



Exercice 1.4.3. *Prouver de la même manière les inclusions et l'égalité suivantes :*

$$(a \cap b{\cdot}b)^\star \subseteq a^\star \cap b^\star$$
$$((a \cap b){\cdot}(1 \cap b){\cdot}(a \cap b))^\star \subseteq (a \cap b{\cdot}b)^\star$$
$$(a \cap b{\cdot}\top)^\star{\cdot}(1 \cap b{\cdot}\top) = (1 \cap \top{\cdot}b^\circ){\cdot}(a \cap \top{\cdot}b^\circ)^\star$$

Avec Paul Brunet [5], nous avons proposé un modèle d'automates permettant de reconnaître les langages de graphes associés aux expressions du calcul des relations. Ce modèle d'automates s'inspire grandement des réseaux de Petri [15, 14], qui permettent d'explorer des structures plus complexes que les mots usuels. A chaque expression e on peut ainsi associer un *automate de Petri* dont le langage est précisément ${}^{\blacktriangleleft}\mathcal{G}(e)$. Grâce au théorème 1.4.2, le problème de la validité des équations et des inclusions dans le calcul des relations sans complément se ramène donc à problème de comparaison d'automates.

Nous n'avons pour l'instant résolu ce dernier problème que pour un fragment du calcul : il nous faut interdire l'opération de converse et la constante 1, et remplacer la clôture réflexive-transitive $\cdot^\star$ par la clôture transitive $\cdot^+$ (car la clôture réflexive fait implicitement apparaître l'identité : on a $1 = 0^\star$) [2]. Sous cette restriction, les graphes considérés sont toujours acycliques, ce qui rend les automates plus simples à comparer. Le problème de la comparaison des automates est alors EXPSPACE-complet. La théorie équationelle correspondante a récemment été étudiée par Andréka, Mikulás, et Németi [1].

Notons que c'est l'opération d'intersection qui pose les principales difficultés : sans l'intersection ni la constante $\top$, on obtient les *algèbres de Kleene avec converse*, dont Bernátsky, Bloom, Ésik et Stefanescu ont montré la décidabilité [3] ainsi l'axiomatisabilité relativement aux algèbres de Kleene : les trois axiomes suivants suffisent dès lors qu'ils sont adjoints à n'importe quelle axiomatisation complète des algèbres de Kleene (i.e., les axiomes de la figure 1.1) [7].

$$\begin{array}{lll} (e \cdot f)^\circ = f^\circ \cdot e^\circ & \qquad e^{\circ\star} = e^{\star\circ} & \qquad e \subseteq e \cdot e^\circ \cdot e \\ (e + f)^\circ = e^\circ + e^\circ & \qquad e^{\circ\circ} = e & \end{array}$$

1.5 Questions ouvertes

Nous concluons ce chapitre par trois questions qui restent ouvertes à ce jour.

La première est celle de la décidabilité du calcul des relations sans complément en entier : sans intersection ni constante $\top$, le problème est PSPACE-complet [4] ; sans converse ni identité, il est EXPSPACE-facile [5] (nous avons démontré l'EXPSPACE-complétude de la question d'automates à laquelle on peut ramener le problème, mais notre réduction ne nous permet pas d'obtenir l'EXPSPACE-difficulté de ce problème).

La deuxième question concerne les allégories : existe-t-il une axiomatisation finie et complète pour les allégories, quitte à utiliser des implications comme axiomes, comme pour les algèbres de Kleene ?

Enfin, est-il possible d'axiomatiser le calcul des relations sans complément ? Par exemple, les axiomes des algèbres de Kleene suffisent-ils lorsqu'on leur adjoint une axiomatisation complète des allégories ? Qu'en est-il sur le fragment sans converse ni identité étudié par Andréka Mikulás et Németi [1] ?

Remerciements Je tiens à remercier Paul Brunet, avec qui nous avons obtenu l'ensemble des nouveaux résultats présentés dans ce cours.

2. Nous ne considérons pas la constante $\top$ dans l'article suscité, mais elle ne pose pas de difficulté dans ce cadre.

Bibliographie

[1] H. Andréka, S. Mikulás, and I. Németi. The equational theory of Kleene lattices. *Theoretical Computer Science*, 412(52) :7099–7108, 2011.

[2] H. Andréka and D. Bredikhin. The equational theory of union-free algebras of relations. *Algebra Universalis*, 33(4) :516–532, 1995.

[3] S. L. Bloom, Z. Ésik, and G. Stefanescu. Notes on equational theories of relations. *Algebra Universalis*, 33(1) :98–126, 1995.

[4] P. Brunet and D. Pous. Kleene algebra with converse. In *Proc. RAMiCS*, volume 8428 of *Lecture Notes in Computer Science*, pages 101–118. Springer Verlag, 2014.

[5] P. Brunet and D. Pous. Petri automata for kleene allegories. In *Proc. LICS*, pages 68–79. ACM, 2015.

[6] J. H. Conway. *Regular algebra and finite machines*. Chapman and Hall, 1971.

[7] Z. Ésik and L. Bernátsky. Equational properties of Kleene algebras of relations with conversion. *Theoretical Computer Science*, 137(2) :237–251, 1995.

[8] P. Freyd and A. Scedrov. *Categories, Allegories*. North Holland, 1990.

[9] D. Kozen. A completeness theorem for Kleene Algebras and the algebra of regular events. In *Proc. LICS*, pages 214–225. IEEE Computer Society, 1991.

[10] D. Kozen. A completeness theorem for Kleene algebras and the algebra of regular events. *Information and Computation*, 110(2) :366–390, 1994.

[11] D. Krob. Complete systems of B-rational identities. *Theoretical Computer Science*, 89(2) :207–343, 1991.

[12] A. Meyer and L. J. Stockmeyer. Word problems requiring exponential time. In *Proc. STOC*, pages 1–9. ACM, 1973.

[13] D. Monk. On representable relation algebras. *Michigan Math. J.*, 11(3) :207–210, 09 1964.

[14] T. Murata. Petri nets: Properties, analysis and applications. *Proc. of the IEEE*, 77(4) :541–580, Apr 1989.

[15] C. A. Petri. Fundamentals of a theory of asynchronous information flow. In *IFIP Congress*, pages 386–390, 1962.

[16] V. Redko. On defining relations for the algebra of regular events. *Ukr. Mat. Z.*, 16 :120–, 1964.

[17] A. Salomaa. Two complete axiom systems for the algebra of regular events. *Journal of the ACM*, 13(1) :158–169, 1966.

[18] A. Tarski. On the calculus of relations. *J. Symbolic logic*, 6 :73–89, 1941.

[19] A. Tarski and S. Givant. *A Formalization of Set Theory without Variables*, volume 41 of *Colloquium Publications*. American Mathematical Society, Providence, Rhode Island, 1987.