Notes de Cours, Diplôme d'Etudes Approfondies d'Informatique, Novembre 1998

Eléments de Programmation par Contraintes

Alain Colmerauer

Table des matières

1 Les bases logiques **7**

2 L'algèbre des arbres **11**
2.1 Qu'est-ce qu'un arbre ? . . . 11
2.2 Arbre rationnel . . . 12
2.3 L'algèbre des arbres . . . 13
2.4 La propriété de solution unique . . . 14
2.5 Forme résolue d'une conjonction à plat . . . 14
2.6 Algorithme de résolution . . . 15

3 Réduction de domaines par calcul de points fixes **17**
3.1 Terminologie . . . 17
3.2 Parties privilégiés . . . 17
3.3 Simplification de contraintes . . . 18

4 Réduction d'intervalles **21**
4.1 Ensembles ordonnées . . . 21
4.2 Intervalles et pavés . . . 21
4.3 Calcul de apx $(\pi_i(r \cap a))$ . . . 22

5 Algorithme de Fourier **25**
5.1 Vecteurs et matrices . . . 25
5.2 Lemme de Farkas . . . 26

Avant propos

Programmer par contraintes consiste à formuler un problème en terme d'inconnues soumis à une contrainte. Voici quatre exemples.

- Trouver les nombre de lapins et de pigeons qui ensemble totalisent 7 têtes et 20 pattes revient à trouver les entiers x et y qui satisfont à la contrainte $[x+y=7] \wedge [4x+2y=20]$. La réponse est $[x=3] \wedge [y=4]$.
- Déterminer la condition pour laquelle l'équation du deuxième degré admet au moins une solution revient à trouver les nombres réels a, b, c qui satisfont à la contrainte $(\exists x)[ax^2+bx+c=0]$. La réponse est $[a\neq 0 \wedge b^2-4ac\geq 0] \vee [a=0 \wedge b\neq 0] \vee [a=0 \wedge c=0]$.
- Trouver dans l'intersection des demi-plans $[y-x\geq 0]$ et $[y+x\leq 4]$ le point (x,y) dont la première coordonnée est maximale revient à trouver le nombre réel x qui satisfait à la contrainte $P(x) \wedge \neg(\exists y)[P(y) \wedge y>x]$, où P est la propriété définie par $P(x) \equiv (\exists y)[y-x\geq 0 \wedge y+x\leq 4]$. La réponse est $x=2$. On remarque ici l'intervention d'une propriété auxiliaire P définie aussi en termes de contraintes.
- Enfin un dernier exemple avec une définition récursive de propriété auxiliaire : On se place dans le domaine des arbres muni de la relation d'égalité et des constructeurs "*cons*", "*nil*", "1", "2" et "3" et l'on cherche à écrire un programme pour concaténer les listes $\mathit{cons}(1, \mathit{cons}(2, \mathit{nil})$ et $\mathrm{cons}(3, \mathrm{nil})$. Ceci revient à déterminer l'arbre z qui satisfait à la contrainte $r(\mathit{cons}(1, \mathit{cons}(2, \mathit{nil})),\ \mathit{cons}(3, \mathit{nil}),\ z)$, où r est la relation ternaire de concaténation définie récursivement par $(x, y, z) \in r \equiv [x = \mathrm{nil} \wedge y = z] \vee (\exists a)(\exists u)(\exists w)[x = \mathit{cons}(a, u) \wedge z = \mathrm{cons}(a, w) \wedge (u, y, w) \in r]$. La réponse est $z = \mathit{cons}(1, \mathit{cons}(2, \mathit{cons}(3, \mathit{nil})))$. On remarque que l'on vient d'écrire un programme Prolog.

Nous nous intéressons d'une part à résoudre des systèmes de contraintes portant sur des inconnues dans différentes structures mathématiques « utiles » et d'autre part à résoudre effectivement des problèmes avec des langages ou des systèmes de programmation par contraintes existants. Plus exactement voici la liste des thèmes abordés :

- Résolution de contraintes dans le domaine des arbres muni d'opérations de construction et de la relation d'égalité.
- Résolution de contraintes linéaires dans le domaine des nombres rationnels. Algorithme de Gauss, algorithme du Simplex.
- Résolution de contraintes non-linéaires dans le domaine des nombres réels.
- Résolution approchées de contraintes variées dans le domaine des réels avec les rationnels vus comme un sous-ensemble des réels, les entiers vus comme un sous-ensemble des rationnels et les booléens vus comme un sous-ensemble des entiers. Algorithmes de réduction, de propagation et de coupures d'intervalles.
- Sémantique des définitions « à la Prolog » de relations auxiliaires.
- Initiation à Prolog IV et à d'autres systèmes de programmation par contraintes.

Chapitre 1

Les bases logiques

Soit **V** un ensemble infini dénombrable dont les éléments sont appelés *variables*, soit **F** un ensemble dont les éléments sont appelés *symboles fonctionnels* et soit **R** un ensemble dont les éléments sont appelés *symboles relationnels*. A chaque élément de **F** et de **R** est attaché un entier n positif ou nul, sa *arité*. On désigne par $\mathbf{F}_n$ l'ensemble des symboles de **F** qui sont d'arité n et par $\mathbf{R}_n$ l'ensemble des symboles de **F** qui sont d'arité n. L'ensemble **L** des *expressions* est l'ensemble $\mathbf{T} \cup \mathbf{P}$ avec **T** et **P** définis comme suit à partir de $\mathbf{V} \cup \mathbf{F}$.

L'ensemble **T** des *termes* est le plus petit ensemble S de suites finies d'élements (juxtaposés) de $\mathbf{V} \cup \mathbf{F}$ qui sont de l'une des deux formes

$v,\ ft_1 \ldots t_n,$

avec v pris dans **V**, avec f pris dans $\mathbf{F}_n$ et avec les t_i pris dans S.

L'ensemble **P** des *formules* est le plus petit ensembles S de suites finies d'éléments de $V \cup F \cup \{=, (,), \mathit{vrai}, \mathit{faux}, \neg, \wedge, \wedge\ \ , \vee, \equiv, \exists, \forall\}$ qui sont de l'une des douze formes

$\mathit{vrai},\ \mathit{faux},\ s{=}t,\ \neg p,\ (p \wedge q),\ (p \wedge\ \ q),\ (p \vee q),\ (p \Rightarrow q)\ (p \equiv q),\ \exists vp,\ \forall vp,$

avec v pris dans **V**, avec s et t pris dans **T** et avec p et q pris dans S. Une occurrence d'une variable v dans une formule p est *liée* si elle se produit à l'intérieur d'une sous-formule de l'une des formes $\exists vp, \exists_0^1 vp, \forall vp$. Elle est est *libre* dans le cas contraire. Une formule *close* ou est une formule sans occurrence libre de variable.

L'ensemble **L** est donc un langage classique du 1$^{\text{er}}$ordre avec égalité. Comme il elle habituel de le faire on introduit la notion d'interprétation pour donner une définition rigoureuse des liens entre la signification d'une expression de **L** et la signification de ses différents composants.

A la façon de Roger Lyndon [1] nous définissons une *interprétation* comme un couple (D, I) formé d'une ensemble non vide D, le domaine de l'interprétation et d'une fonction I d'interprétation. Cette fonction I associe à chaque élément de $\mathbf{V} \cup \mathbf{F} \cup \mathbf{T} \cup \mathcal{P}$ un élément dont la nature est telle que,

si v appartient à **V** alors $I(v)$ appartient à **D**,

si f appartient à $\mathbf{F}_n$ alors $I(f)$ est une application de $\mathbf{D}^n$ dans **D**

si t appartient à **T** alors $I(t)$ appartient à **D**,

si p appartient à $\mathcal{P}$ alors $I(p)$ est la valeur de vérité *true* ou la valeur de vérité *false*

tout en respectant les douze égalités :

$$
\begin{array}{lcl}
I(ft_1 \ldots t_n)) & = & I(f)(I(t_1), \ldots, I(t_n)), \\
I(\mathit{vrai}) & = & \mathit{true}, \\
I(\mathit{faux}) & = & \mathit{false}, \\
I(s{=}t) & = & \mathit{true}, \text{ si } I(s) = I(t), \quad \text{et} \quad \mathit{false} \text{ sinon}, \\
I(\neg p) & = & \mathit{true}, \text{ si } I(p) = \mathit{false}, \quad \text{et} \quad \mathit{false} \text{ sinon}, \\
I(p \wedge q) & = & \mathit{true}, \text{ si } I(p) = \mathit{true} \text{ et } I(p) = \mathit{true}, \quad \text{et} \quad \mathit{false} \text{ sinon}, \\
I(p \wedge\ \ q) & = & \mathit{true}, \text{ si } I(p) = \mathit{true} \text{ et } I(p) = \mathit{true}, \quad \text{et} \quad \mathit{false} \text{ sinon}, \\
I(p \vee q) & = & \mathit{true}, \text{ si } I(p) = \mathit{true} \text{ ou } I(p) = \mathit{true}, \quad \text{et} \quad \mathit{false} \text{ sinon}, \\
I(p \Rightarrow q) & = & \mathit{true}, \text{ si } I(p) = \mathit{false} \text{ ou } I(p) = \mathit{true}, \quad \text{et} \quad \mathit{false} \text{ sinon}, \\
I(p \equiv q) & = & \mathit{true}, \text{ si } I(p) = I(q), \quad \text{et} \quad \mathit{false} \text{ sinon}, \\
I((\exists v)p) & = & \mathit{true}, \text{ si il existe } J \in \mathit{proche}(v, I) \text{ avec } J(p) = \mathit{true}, \quad \text{et} \quad \mathit{false} \text{ sinon}, \\
I((\forall v)p) & = & \mathit{true}, \text{ si pour tout } J \in \mathit{proche}(v, I) \text{ on a } J(p) = \mathit{true}, \quad \text{et} \quad \mathit{false} \text{ sinon},
\end{array}
$$

où $proche(v, I)$ est l'ensemble des application J qui diffèrent de I au plus par le fait que $J(v) \neq I(v)$. De ces conditions il s'ensuit bien entendu que la valeur de vérité $I(p)$ d'une formule p ne dépend pas des valeurs $I(v)$ des variables qui n'ont que des occurrences liées dans p.

L'interprétation (D, I) *satisfait* la formule p si $I(p) = true$ et *satisfait* l'ensemble éventuellement vide et éventuellement infini P de formules si elle satisfait chaque élément de P. Si toute interprétation qui satisfait P satisfait p, on dit que la formule p *est vrai dans* P et on écrit $P \models p$.

Une théorie P est un ensemble de formules closes. Une théorie est complète si quel que soit la formule close p on a soit $T \models p$ soit $T \models \neg p$.

Bibliographie

[1] Roger C. Lyndon, Notes on Logic, Van Nostrand Mathematical Studies, 1964.

Chapitre 2

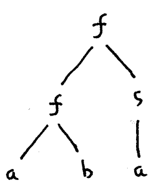
L'algèbre des arbres

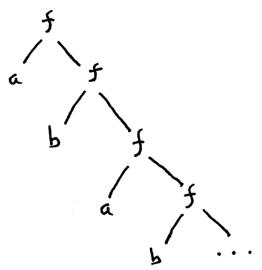
Attention, tout ceci est un brouillon bourré de fautes.

2.1 Qu'est-ce qu'un arbre ?

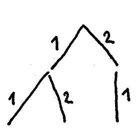
On se donne un ensemble E dont les éléments sont appelés *étiquettes*. A chaque étiquette est associée un entier non négatif n, sa *arité*. On suppose que pour chaque n l'ensemble des étiquettes d'arité n est infini dénombrable.

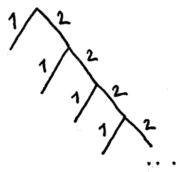
Les arbres qui nous intéressent sont formés de nœuds étiquetés par les éléments de E. Les branches qui partent d'un nœud donné sont ordonnées et leur nombre est égal à l'arité de l'étiquette de ce nœud. Voici deux exemples d'arbres avec $E = \{0, 1, s, f, ...\}$, les étiquettes $0, 1, s, f$ étant respectivement d'arité $0, 0, 1, 2$.





On notera qu'un arbre (que l'on dessine toujours à l'envers) peut comporter des branches infinis mais que l'embranchement de chacun de ses nœuds est toujours fini. Pour aboutir à une définition formelle de nos arbres il faut pouvoir préciser ce qu'est la position d'un nœud. Pour ceci on numérote de 1 à n et de gauche à droite les branches qui connecte un nœud à ses n fils. Sur les deux exemples précédents cela donne :





La position d'un nœud est alors tout simplement la suite d'entiers positifs que l'on rencontre pour aller à ce nœud en partant de la racine de l'arbre. En assimilant un nœud à sa position, un *nœud* x est donc une suite finie $(i_1, \ldots, i_k)$ éventuellemnt vide d'entiers positifs. On note $\mathbf{N}^+$ l'ensemble de toute ces suites finies. A chaque nœud d'un arbre est associé une étiquette. On peut donc représenter les deux arbres précédents par les ensembles d'associations :

$\{\varepsilon \mapsto \mathrm{f},\ (1) \mapsto \mathrm{f},\ (2) \mapsto \mathrm{s},\ (1,1) \mapsto \mathrm{a},\ (1,2) \mapsto \mathrm{b},\ (2,1) \mapsto \mathrm{b}\}$,

$\{\varepsilon \mapsto \mathrm{f},\ (1) \mapsto \mathrm{a},\ (2) \mapsto \mathrm{f},\ (2,1) \mapsto \mathrm{b},\ (2,2) \mapsto \mathrm{f},\ (2,2,1) \mapsto \mathrm{a},\ (2,2,2) \mapsto \mathrm{f},\ (2,2,2,1) \mapsto \mathrm{b}, \ldots\}$, où le signe ε désigne la suite vide.

Définition 2.1.1 Etant donné un ensemble E de symboles avec arités, un *arbre a* étiqueté par E est une application de type $\text{dom}(a) \to E$, où $\text{dom}(a)$ est un sous-ensemble non vide de $(\mathbf{N}_+)^*$, telle que, pour tout $i \in \mathbf{N}_+$ et $x \in \text{dom}(a)$,

1. si $(i)\cdot x \in \text{dom}(a)$ alors $x \in dom(a)$,
2. si l'arité de $a(x)$ est n alors $x\cdot(i) \in \text{dom}(a) \iff i \in 1..n$.

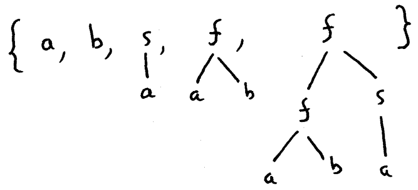
Ici la concaténation de suites d'entiers est noté par un point.

2.2 Arbre rationnel

Dans le dessin d'un arbre figurent d'autres arbres généralement plus petits, ce sont des *sous-arbres.*

Définition 2.2.1 Etant donné un arbre a, le *sous-arbre partant du* nœud x de $\text{dom}(a)$ est l'application $x \cdot y \mapsto a(y)$, avec $x \cdot y \in \text{dom}(a)$.

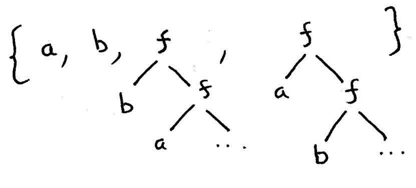
De la définition d'un arbre on conclut immédiatement qu'un sous-arbre est un arbre. Si nous reprenons les deux exemples d'arbres proposés, ceux-ci ont respectivement pour ensembles de sous-arbres :



c'est-à dire

$\{\{\varepsilon \mapsto \text{a}\},$
$\{\varepsilon \mapsto \text{b}\},$
$\{\varepsilon \mapsto \text{s},\ (1) \mapsto \text{b}\},$
$\{\varepsilon \mapsto \text{f},\ (1) \mapsto \text{a},\ (2) \mapsto \text{b}\},$
$\{\varepsilon \mapsto \text{f},\ (1) \mapsto \text{f},\ (2) \mapsto \text{s},\ (1,1) \mapsto \text{a},\ (1,2) \mapsto \text{b},\ (2,1) \mapsto \text{b}\}\}$

et



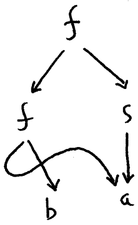
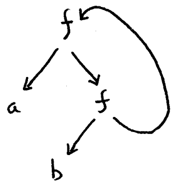
c'est-à-dire

$\{\{\varepsilon \mapsto \text{a}\},$
$\{\varepsilon \mapsto \text{b}\},$
$\{\varepsilon \mapsto \text{f},\ (1) \mapsto \text{a},\ (2) \mapsto \text{f},\ (2,1) \mapsto \text{b},\ (2,2) \mapsto \text{f},\ (2,2,1) \mapsto \text{a}, \ldots\},$
$\{\varepsilon \mapsto \text{f},\ (1) \mapsto \text{b},\ (2) \mapsto \text{f},\ (2,1) \mapsto \text{a},\ (2,2) \mapsto \text{f},\ (2,2,1) \mapsto \text{b}, \ldots\}\}$

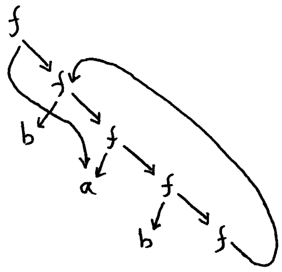
On remarquera que l'arbre infini, c'est-à-dire celui qui a un ensemble infini de nœud, a un ensemble fini de sous-arbres. C'est un arbre « rationnel ».

Définition 2.2.2 Un arbre *rationnel* est un arbre dont l'ensemble des sous-arbres est fini.

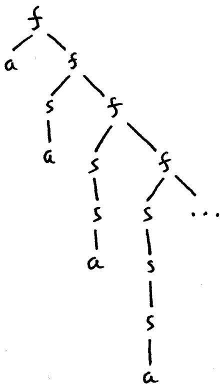
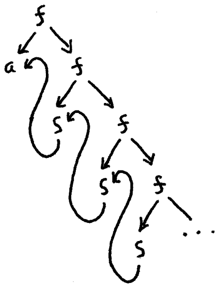
Un arbre rationnel peut toujours être représenté par un diagramme fini : il suffit de fusionner tous les noeuds d'où partent les mêmes sous-arbres. Sur nos deux exemples nous obtenons :

Si on ne fait pas toutes les fusions sur le deuxième arbre on peut aussi obtenir :

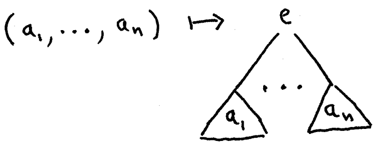


Il faut donc se méfier du fait que le même arbre peut être représenté par différents diagrammes. Enfin il est intéréssant d'exhiber un arbre non rationnel et le diagramme infini que l'on obtient après toutes les fusions possibles de nœuds :

2.3 L'algèbre des arbres

L'opération la plus simple sur les arbres consiste, à partir de n arbres $a_1, ..., a_n$ et d'une étiquette e d'arité n, à construire un nouvel arbre comme suit :



Ceci amène la définition suivante :

Définition 2.3.1 Etant donné l'ensemble A des arbres etiquetés par E, on appelle *constructeur* ou *opération de construction* associée à l'étiquette n-aire e de E, l'application φ_e de A^n dans A, où

$\varphi_e(a_1, \ldots, a_n)$ est l'arbre

$$x \mapsto \begin{cases} e, & \text{si } x = \varepsilon, \\ a_i(y), & \text{si } x \text{ est de la forme } (i)\cdot y \text{ avec } i \in 1..n. \end{cases}$$

avec

$$x \in \{\varepsilon\} \cup \{(i)\cdot y \mid i \in 1..n \text{ et } y \in \mathrm{dom}(a_i)\}.$$

Définition 2.3.2 L'algèbre des arbres construit sur E est le couple $\mathcal{A} = (A, \varphi)$ où A est l'ensemble des arbres étiquetés par E et φ la famille des constructeurs φ_e indicée par E.

On remarque que si φ_e est un constructeur n-aire, l'ensemble des sous-arbres de l'arbre $\varphi_e(a_1, \ldots, a_n)$ s'obtient en prenant l'union des ensembles de sous-arbres des différents a_i et en y ajoutant l'arbre $\varphi(a_1, \ldots, a_n)$, s'il n'y figure pas déjà. De ce fait si les a_i sont rationnels, l'arbre $\varphi(a_1, \ldots, a_n)$ l'est aussi. En désignant par A' l'ensemble des arbres rationnels de A et par φ' la famille φ d'opérations restreintes à A' le couple (A', φ') est donc une sous-algèbre de (A, φ).

2.4 La propriété de solution unique

Parmi les propriétés de l'algèbre des arbres (A, φ) il en est une cachée, difficile à formuler et à démontrer. Nous en aurons besoin par la suite.

Théorème 2.4.1 (Solution unique) Soit $W = \{x_1, \ldots, x_n, u_1, \ldots, u_m\}$ un ensemble d'arbre et, pour chaque $i \in 1..n$, soit $a_i(x_1, \ldots, x_n, u_1, \ldots, u_m)$ un arbre de la forme $\varphi_e(y_1, \ldots, y_p)$ où e est une étiquette d'arité p, dépendant de i, et $\{y_1, \ldots, y_p\}$ un sous-ensemble de W, dépendant de i. On a à la fois

1 $(\forall u_1 \in A) \ldots (\forall u_m \in A)(\exists x_1 \in A) \ldots (\exists x_n \in A)$
$$\begin{pmatrix} & x_1 = a_1(x_1, \ldots, x_n, u_1, \ldots, u_m) \\ & \ldots \\ \wedge & x_n = a_n(x_1, \ldots, x_n, u_1, \ldots, u_m) \end{pmatrix}$$

2 $(\forall u_1 \in A) \ldots (\forall u_m \in A)(\forall x_1 \in A) \ldots (\forall x_n \in A)(\forall y_1 \in A) \ldots (\forall y_n \in A)$
$$\begin{pmatrix} & x_1 = a_1(x_1, \ldots, x_n, u_1, \ldots, u_m) \\ & \ldots \\ \wedge & x_n = a_n(x_1, \ldots, x_n, u_1, \ldots, u_m) \\ \wedge & y_1 = a_1(y_1, \ldots, y_n, u_1, \ldots, u_m) \\ & \ldots \\ \wedge & y_n = a_n(y_1, \ldots, y_n, u_1, \ldots, u_m) \end{pmatrix} \Longrightarrow \begin{pmatrix} & x_1 = y_1 \\ & \ldots \\ \wedge & x_n = y_n \end{pmatrix}$$

2.5 Forme résolue d'une conjonction à plat

Soit V un ensemble de variables soit F un ensemble de symboles d'opérations et soit A l'ensemble des arbres étiquetées par F. Nous travaillerons sur des contraintes de la forme $p_1 \wedge \cdots \wedge p_n$, où les p_i sont de l'une des quatre formes

1 *false*,
4 *true*,
1 $x = y$,
2 $x = fu_1 \ldots u_n$,

où x, y et les u_i sont des éléments de V et f un élément de F d'arité n. De telles contraintes seront dites *conjonctions à plat.*

Définition 2.5.1 Une conjonction à plat est dite *résolue* si elle de la forme *false* ou *true* ou

$$x_1 = t_1 \wedge \cdots \wedge x_n = t_n, \tag{2.1}$$

où les x_i sont des variables distinctes, les t_i des termes, avec la restriction que l'ensemble des équations qui la compose ne contienne pas un sous-ensemble non vide de la forme $\{y_1 = y_2,\ y_2 = y_3,\ \ldots,\ y_{m-1} = y_m\}$, les y_i étant des variables et y_1 et y_m étant la même variable.

Du theorème de solution unique on déduit immédiatement le corollaire suivant

Corollaire 2.5.2 (Du théorème de solution unique) *Soit p une conjonction à plat sous forme résolue distincte de false et soit W l'ensemble des variables qui figurent comme membres gauche de ses équations. Quelle que soit l'application σ de $V-W$ dans A il existe une et une seule application de V dans A qui est solution de p et qui coïncide avec σ sur $V-W$.*

2.6 Algorithme de résolution

L'algorithme qui suit permet de transformer toute conjonction à plat en une contrainte équivalente sous forme résolue. Il consiste à appliquer sur la contrainte initiale et tant que cela est possible les règles de réécriture qui suivent, en considérant que le connecteur $\wedge$ est associatif et commutatif.

Dans ces règles de réécriture on suppose que les variables x de V sont numérotées par des entiers naturels notés $n^{\mathrm{o}}\,(x)$.

$$\begin{array}{lrcl}
1 & \mathit{false} \wedge q & \Longrightarrow & \mathit{false} \\
2 & \mathit{true} \wedge \mathit{true} & \Longrightarrow & \mathit{true} \\
3 & x{=}fu_1..u_m \wedge x{=}gv_1..v_n & \Longrightarrow & \mathit{false} \\
4 & x{=}fu_1..u_n \wedge x{=}fv_1..v_n & \Longrightarrow & x{=}fu_1..u_n \wedge u_1{=}v_1 \wedge .. \wedge u_n{=}v_n \\
5 & y{=}x & \Longrightarrow & x{=}y \\
6 & x{=}x & \Longrightarrow & \mathit{true} \\
7 & x{=}fu_1..u_n \wedge x{=}y & \Longrightarrow & y{=}fu_1..u_n \wedge x{=}y \\
8 & x{=}z \wedge x{=}y & \Longrightarrow & y{=}z \wedge x{=}y
\end{array} \tag{2.2}$$

avec la condition que $n^{\mathrm{o}}\,(x) > n^{\mathrm{o}}\,(y)$.

Théorème 2.6.1 (Terminaison) *On ne peut appliquer qu'un nombre fini de réécritures.*

Preuve. On considère le quadruplet (n_1, n_2, n_3, n_4) où les n_i sont les entiers non négatifs suivants :

n_1 est le nombre d'occurences d'équations de la forme $x{=}fu_1..u_n$,
n_2 est le nombre d'occurences de contraintes atomiques,
n_3 est la somme des $n^{\mathrm{o}}\,(x)$ pour toutes les occurrences de variables x,
n_4 est le nombre d'occurrences d'équations de la forme $x{=}y$, avec $n^{\mathrm{o}}\,(x) < n^{\mathrm{o}}\,(y)$.

Pour chaque règles il existe i tel que $n'_i < n_i$ et $(n'_1, \ldots, n'_{i-1}) = (n_1, \ldots, n_{i-1})$. Ces i valent 1 ou 2 pour la règle 1, valent 2 pour la règle 2, valent 1 pour les règles 3,4, valent 4 pour la règle 5 et valent 3 pour les règles 6,7,8. Les entiers n_1, n_2, n_3, n_4 étant astreints à être non négatifs, on en conclut que l'on ne pourra indéfiniment appliquer des règles.

Chapitre 3

Réduction de domaines par calcul de points fixes

3.1 Terminologie

Si E est un ensemble quelconque et G un sous ensemble de l'ensemble $\mathcal{P}(E)$ on introduit les notations suivantes

$\cap G = \{x \in E \,|\, \text{pour tout } a \in G, \text{ on a } x \in a\}$,

$\cup G = \{x \in E \,|\, \text{il existe } a \in G, \text{ avec } x \in a\}$

Lorsque G est non vide la valeur de $\cap G$ ne dépend pas de E mais uniquement de G et on l'appelle la partie commune des éléments de G ou l'intersection des éléments de G. La valeur de $\cup G$ ne dépend jamais de E et on l'appelle l'union des éléments de G.

Si r est un sous-ensemble de E^n et i un entier strictement positif i, la i^e*projection* de r est le sous-ensemble éventuellement vide de E :

$\pi_i(r) = \{e \in E \,|\, \text{il existe un élément de } r \text{ de la forme } (d_1, \ldots, d_n) \text{ avec } n \geq i \text{ et } e = d_i\}$.

3.2 Parties privilégiés

On se donne un ensemble $\mathbf{D}$ et un sous-ensemble non vide $\mathbf{I}$ de l'ensemble $\mathcal{P}(\mathbf{D})$ des parties de $\mathbf{D}$. Les éléments de $\mathbf{I}$ sont dits parties *privilégiés* de $\mathbf{D}$. On fait l'hypothèse suivante sur l'ensemble $\mathbf{I}$:

Hypothèse 3.2.1 *L'ensemble* $\mathbf{I}$ *a trois propriétés :*

1. $\mathbf{D} \in \mathbf{I}$,
2. *quel que soient* $a \in \mathbf{I}$ *et* $b \in \mathbf{I}$, *on a* $a \cap b \in \mathbf{I}$,
3. *toute suite strictement décroissante d'éléments de* $\mathbf{I}$ *est finie, et ceci en prenant comme relation d'ordre l'inclusion.*

Propriété 3.2.2 *Si* G *est un sous-ensemble non vide de* $\mathbf{I}$ *(fini ou infini) alors la partie commune* $\cap G$ *des éléments de* G *appartient à* $\mathbf{I}$.

PREUVE Considérons des suites d'éléments de $\mathbf{I}$ de la forme $a_1, \ldots, a_n$ tels que $a_1 \in G$ et tels que, pour chaque i entre 1 et $n-1$ il existe $b \in G$ avec $a_{i+1} = a_i \cap b$ et $a_{i+1} \neq a_i$. D'après la deuxième hypothèse sur $\mathbf{I}$, les a_i appartiennent tous à $\mathbf{I}$ et par construction les a_{i+1} sont strictement inclus dans les a_i. D'après la troisième hypothèse sur $\mathbf{I}$ on peut donc construire une telle suite $a_1, \ldots, a_n$ qui ne peut être prolongée. Du fait que $a_n \in \mathbf{I}$, pour montrer que $\cap G \in \mathbf{I}$ il suffit de montrer que $a_n = \cap G$. Du fait que $a_n \in G$ on a aussi $\cap G \subseteq a_n$. Il ne reste qu'à montrer que $a_n \subseteq \cap G$.

Si ce n'était pas le cas il existerait $b \in G$ tels que $a_n \not\subseteq b$ et en posant $a_{n+1} = a_n \cap b$ la suite $a_1, \ldots, a_n, a_{n+1}$ prolongerait la suite $a_1, \ldots, a_n$ supposée non prolongeable. Ceci termine la preuve.

Propriété 3.2.3 *Pour tout sous-ensemble* x *de* $\mathbf{D}$, *le plus petit (au sens de l'inclusion) élément de* $\mathbf{I}$ *qui contient* x *existe toujours. On le note* $apx(x)$.

Preuve Soit x un sous-ensemble de $\mathbf{D}$. Du fait que $\mathbf{D} \in \mathbf{I}$ l'ensemble $G = \{y \in \mathbf{I} \,|\, x \subseteq y\}$ n'est pas vide. D'après la propriété 3.2.2, on a alors $\cap G \in \mathbf{I}$. De la façon dont G est défini on a $\cap G \in G$ et aussi $\cap G \subseteq y$ pour tout $y \in G$. Il s'ensuit que $\cap G$ est le plus petit élément de $\mathbf{I}$ qui contient x. La partie privilégiée $\mathrm{apx}\,(x)$ existe donc. Ceci termine la preuve.

Désignons par $\mathbf{I}^{(n)}$ l'ensemble des sous-ensembles de $\mathbf{D}^n$ qui sont de la forme $a_1 \times \cdots \times a_n$ avec chaque a_i appartenant à $\mathbf{I}$. Si on remplace $\mathbf{D}$ par $\mathbf{D}^n$, l'ensemble $\mathbf{I}^{(n)}$ vérifient les trois hypothèses faites sur $\mathbf{I}$. De ce fait la propriété 3.2.3 portant sur le couple $(\mathbf{D}, \mathbf{I})$ se transpose au couple $(\mathbf{D}^n, \mathbf{I}^{(n)})$:

Propriété 3.2.4 *Pour tout sous-ensemble r de $\mathbf{D}^n$, le plus petit (au sens de l'inclusion) élément de $\mathbf{I}^{(n)}$ qui contient r existe toujours. On le note $apx\,(r)$.*

Terminons cette partie en remarquent que si r et s sont des sous-ensemble de $\mathbf{D}^n$ on a les quatre propriétés :

(1)	$r \subseteq \mathrm{apx}\,(r)$,	(contraction),
(2)	$\mathrm{apx}\,(\mathrm{apx}\,(r)) = \mathrm{apx}\,(r)$,	(idempotence),
(3)	si $r \subseteq r$ alors $\mathrm{apx}\,(r) \subseteq \mathrm{apx}\,(s)$,	(croissance),
(4)	$\mathrm{apx}\,(r) = \mathrm{apx}\,(\pi_1(r)) \times \cdots \times \mathrm{apx}\,(\pi_n(r))$.	

3.3 Simplification de contraintes

Soit R un ensemble de relation r dans $\mathbf{D}$ de diverses arités. Chaque relation r d'arité n est un sous-ensemble de $\mathbf{D}^n$. Soient k variables $x_1, \ldots, x_k$ pour représenter des éléments de $\mathbf{D}$ On considère des contraintes de la forme

$$x_1 \in a_1 \wedge \cdots \wedge x_k \in a_k \wedge p_1 \wedge \ldots \wedge p_l, \tag{3.1}$$

où les a_i sont des éléments de $\mathbf{I}$ et où chaque p_i est une contrainte de la forme

$$(y_1, \ldots, y_n) \in r,$$

les y_i étant des variables distinctes prises parmi les x_i et r étant un élément de R d'arité n.

Définition 3.3.1 *L'ensemble des* règles de réductions *associée à l'ensemble R de relation sur $\mathbf{D}$ est l'ensemble des règles de réécritures de la forme*

$$\begin{pmatrix} & (y_1, \ldots, y_n) \in r \\ \wedge & y_1 \in b_1 \\ & \cdots \\ \wedge & y_n \in b_n \end{pmatrix} \Longrightarrow \begin{pmatrix} & (y_1, \ldots, y_n) \in r \\ \wedge & y_1 \in b'_1 \\ & \cdots \\ \wedge & y_n \in b'_n \end{pmatrix} \tag{3.2}$$

où r est un élément quelconque de R d'arité n, où les b_i et les b'_i sont des éléments de $\mathbf{I}$ tels qu'à la fois

$$b_1 \times \cdots \times b_n \supsetneq b'_1 \times \cdots \times b'_n \quad \textit{et} \quad r \cap (b_1 \times \cdots \times b_n) \;=\; r \cap (b'_1 \times \cdots \times b'_n).$$

Propriété 3.3.2 *Si r et b sont des sous-ensemble de $\mathbf{D}^n$ et si $b \in \mathbf{I}^{(n)}$ alors, pour l'inclusion, les plus petit éléments des ensembles*

$$\{b' \in \mathbf{I}^{(n)} \,|\, (r \cap b) = (r \cap b')\},$$
$$\{b' \in \mathbf{I}^{(n)} \,|\, (r \cap b) \subseteq b'\}$$

existent et sont égaux.

Preuve Soient les ensembles

$$G = \{b' \in \mathbf{I}^{(n)} \,|\, (r \cap b) = (r \cap b')\},$$
$$H = \{b' \in \mathbf{I}^{(n)} \,|\, (r \cap b) \subseteq b'\}.$$

D'après la propriété 3.2.4, H admet un plus petit élément noté $\mathrm{apx}\,(r \cap b)$. Il reste à montrer que cet élément est le plus petit élément de l'ensemble G.

Montrons que $\mathrm{apx}\,(r \cap b) \in G$. Du fait que $r \cap b \subseteq \mathrm{apx}\,(r \cap b)$ on a $r \cap b \subseteq r \cap \mathrm{apx}\,(r \cap b)$. Du fait que $r \cap b \subseteq b$ on a $\mathrm{apx}\,(r \cap b) \subseteq b$ et donc $r \cap \mathrm{apx}\,(r \cap b) \subseteq r \cap b$. Donc $r \cap b = r \cap \mathrm{apx}\,(r \cap b)$.

Montrons que si $b' \in G$ alors $\mathrm{apx}\,(r \cap b) \subseteq b'$. On a toujours $r \cap b' \subseteq b'$ et donc $\mathrm{apx}\,(r \cap b') \subseteq b'$. Donc, si $b' \in H$ alors $r \cap b = r \cap b'$ et donc $\mathrm{apx}\,(r \cap b) = \mathrm{apx}\,(r \cap b') \subseteq b'$. Ceci termine la preuve.

Soient p et q des contraintes de la forme (3.1). On écrit $p \xrightarrow{R} q$ pour signifier que dans l'ensemble de règles de réécriture associé à R, il existe une règle de la forme $p' \Longrightarrow q'$ telle que, en tenant compte de ce que le connecteur $\wedge$ est associatif et commutatif, la contrainte q s'obtient en remplaçant dans p une occurrence de la formule p' par la formule q'.

On remarque tout de suite que si $p \xrightarrow{R} q$ alors les contraintes p et q de la forme (3.1) sont équivalentes.

Propriété 3.3.3 *Soit $q_1, q_2, \ldots$ une suite non prolongable de contraintes q_i de la forme (3.1) tel que $q_i \xrightarrow{R} q_{i+1}$ pour tout i tel que q_i et q_{i+1} existent. On a les deux deux points :*

1. *la suite $q_1, q_2, \ldots$ est toujours finie,*
2. *le dernier élément de la suite $q_1, q_2, \ldots$ ne dépend que du choix du premier.*

PREUVE Montrons la propriété 1 du théorème. Supposons que cette propriété ne soit pas vraie. D'après la forme des règles de réécriture, le passage de q_i à q_{i+1} se fait en en remplaçant au moins une des k contraintes de la forme $y_j \in a_j$ par une contrainte de la forme $y_j \in a'_j$ avec a'_i strictement inclus dans a_i. Ce nombre k étant constant, si la suite $q_1, q_2, \ldots$ est infinie, il existe un indice j pour lequel l'ensemble a_j de la contrainte $y_j \in a_j$ figurant dans q_1 est diminué une infinité de fois. Il existe donc une suite strictement décroissante d'éléments de $\mathbf{I}$ ce qui contredit la première hypothèse faite sur $\mathbf{I}$.

Montrons la propriété 2 du théorème dans le cas particulier où les q_i sont de la forme

$$x_1 \in a_1 \wedge \cdots \wedge x_k \in a_k \wedge (x_1, \ldots, x_k) \in r_1 \wedge \cdots \wedge (x_1, \ldots, x_k) \in r_l. \tag{3.3}$$

Soit $q_1, \ldots, q_m$ une suite non prolongeable de telles contraintes avec $q_i \xrightarrow{R} q_{i+1}$, pour chaque i entre 1 et $m-1$. Il faut montrer que q_n ne dépend que de q_1. En désignant par $bloc(q_i)$ l'ensemble $a_1 \times \cdots \times a_n$ associé à la contrainte q_i, il suffira de montrer que $bloc(q_m)$ ne dépend que de q_1. Pour ceci nous allons montrer que $bloc(q_m)$ est égal au plus grand (pour l'inclusion) élément de l'ensemble

$$G = \{a \in \mathbf{I}^{(n)} \mid a \subseteq bloc(q_1) \text{ et } a = \operatorname{apx}(r_i \cap a) \text{ pour chaque } i \text{ entre 1 et } l\}.$$

Montrons que $bloc(q_m) \in G$. La suite $q_1, \ldots, q_n$ n'étant pas prolongeable, aucune règle de réécriture ne peut s'appliquer sur q_n et donc il n'existe aucun $j \in 1..l$ et aucun élément $b' \in \mathbf{I}^{(k)}$ tel qu'à la fois $bloc(q_n)) \supsetneq b'$ et $r_j \cap bloc(q_i) = r_j \cap b'$. D'après la propriété 3.3.2 il s'ensuit que $bloc(q_m) = \operatorname{apx}(r_j \cap bloc(q_m))$ pour tout $j \in 1..l$ et donc que $bloc(q_m) \in G$.
Montrons que si $a \in G$ alors $a \subseteq bloc(q_m)$. Pour ceci nous supposerons que $a \in G$ et nous montrerons par récurrence sur i que si $a \subseteq bloc(q_i)$, pour tout i entre 1 et m. On a $a \subseteq bloc(q_1)$, car tous les éléments de G sont inclus dans $bloc(q_1)$. Supposons que $a \subseteq bloc(q_i)$ et montrons que $a \subseteq bloc(q_{i+1})$. Du fait que $q_i \xrightarrow{R} q_{i+1}$, il existe un indice j tel que $bloc(q_i)) \supsetneq bloc(q_{i+1})$ et $r_j \cap bloc(q_i) = r_j \cap bloc(q_{i+1})$. De la propriété 3.3.2 on déduit que

$$\operatorname{apx}(r_j \cap bloc(q_i)) \subseteq bloc(q_{i+1}).$$

De $a \subseteq bloc(q_i)$ on déduit $(r_j \cap a) \subseteq (r_j \cap bloc(q_i))$ et donc, du fait que apx est croissant, $\operatorname{apx}(r_j \cap a) \subseteq \operatorname{apx}(r_j \cap bloc(q_i))$, et donc, d'après l'inclusion précédente, $a \subseteq bloc(q_{i+1})$.

Montrons la propriété 2 du théorème dans le cas général. A chaque contrainte de la forme

$$(y_1, \ldots, y_m) \in r, \tag{3.4}$$

où les y_i sont des variables distinctes prises parmis les x_i et où r est une relation d'arité n prise dans R, associons la contrainte

$$(x_1, \ldots, x_k) \in r', \tag{3.5}$$

où r' est le sous-ensemble de $\mathbf{D}^k$ défini par

$$(a_1, \ldots, a_k) \in r' \iff \left(\begin{array}{l} \text{il existe } (b_1, \ldots, b_m) \in \mathbf{D}^k \text{ tel que,} \\ \text{pour chaque } i \text{ entre 1 et } k \text{ et } j \text{ entre 1 et } n, \\ a_i = b_j \text{ si les variable } x_i \text{ et } y_j \text{ sont identiques.} \end{array} \right)$$

Soit R' l'ensemble des relations r' ainsi définies. A chaque suite $q_1, \ldots, q_n$ de contraintes telles que $q_i \xrightarrow{R} q_{i+1}$, pour chaque i entre 1 et $n-1$, associons la suite $q'_1, \ldots, q'_n$ obtenue en remplaçant dans chaque q_i chaque contrainte de la forme (3.4) par la contrainte correspondante (3.5). Par construction on alors $q'_i \xrightarrow{R'} q'_{i+1}$, pour chaque i entre 1 et $n-1$. Du fait que nous avons montré que q'_n ne dépend que du choix de q'_1, il s'ensuit que q_n ne dépend que du choix de q_1. Ceci termine la preuve.

Chapitre 4

Réduction d'intervalles

4.1 Ensembles ordonnées

Tout d'abords quelques mots sur les ensembles ordonnés. Un *ensemble ordonné* est un couple $(\mathbf{D}, \preceq)$ où $\mathbf{D}$ est un ensemble quelconque et $\preceq$ une *relation d'ordre* dans cet ensemble, c'est-à-dire un sous-ensemble de $\mathbf{D} \times \mathbf{D}$ tel que, en écrivant $e \preceq d$ au lieu de $(e, d) \in \preceq$, pour tous les éléments e, d, f de $\mathbf{D}$, on ait les trois propriétés bien connues,
(1) $e \preceq e$, (réfléxivité),
(2) $e \preceq d$ et $d \preceq e$ entraîne $e = d$, (antisymétrie),
(3) $e \preceq d$ et $d \preceq f$ entraîne $x \preceq z$, (transitivité).
La relation d'ordre $\preceq$ est dite *totale* si, pour tous les éléments e, d de $\mathbf{D}$, elle satisfait à la condition supplémentaire,
(4) $e \preceq d$ ou $d \preceq e$.
Elle est dite *partielle* dans le cas contraire.

Soit a un sous-ensemble de $\mathbf{D}$. Un élément e de a est dit *plus petit élément* de a si $e \preceq d$ pour tout élément d de a. Un tel élément, s'il existe, est unique et on le note $\mathit{min}\, a$. Il existe toujours si a est fini et si la relation d'ordre $\preceq$ est totale. Un élément e de a qui est telle que $d \preceq e$ entraîne $d = e$, pour tout élément d de a, est dit *élément minimal* de a. Si l'ensemble a est fini alors pour chacun de ses éléments d il existe un élément minimal de e tel que $e \preceq d$. Un élément e de a qui est tel que $d \preceq e$, pour tout élément d de a, est dit *majorant* de a dans $\mathbf{D}$. En particulier si a est vide, tous les éléments de $\mathbf{D}$ sont des majorants de a. Si l'ensemble des majorants de a dans $\mathbf{D}$ admet un plus petit élément alors cet élément est dit *borne supérieure* de a dans $\mathbf{D}$. On le note $\mathit{sup}\, a$.

On définit de la même façon les notions de *plus grand élément* de a, noté $\mathit{max}\, a$, *d'élément maximal* de a, de *minorant* de a dans $\mathbf{D}$ et de *borne inférieure* de a dans $\mathbf{D}$, notée $\mathit{sup}\, a$, en interchangeant dans tout ce que nous venons d'écrire les mots « petit » et « grand » et les expressions $e \preceq d$ et $d \preceq e$.

On remarque que, si a admet un plus petit élément, cet élément est sa borne inférieure dans n'importe lequel de ses sur-ensembles et de même, s'il admet un plus grand élément, cet élément est sa borne supérieure dans n'importe lequel de ses sur-ensembles.

Comme exemples d'ensemble ordonnées citons $(\mathcal{P}(E), \subseteq)$, $(\mathbf{R}, \leq)$, $(\mathbf{Q}, \leq)$, $(\mathbf{Z}, \leq)$, $(\mathbf{Z}, \leq)$, où $\mathcal{P}(E)$ est l'ensemble des parties d'un ensemble donné E et $\subseteq$ la relation d'ordre partielle d'inclusion, où $\mathbf{R}$ est l'ensemble des nombres réels, $\mathbf{Q}$ l'ensemble des nombres rationels, $\mathbf{Z}$ l'ensemble des entiers relatifs, $\mathbf{N}$ l'ensemble des entiers naturels et où à chaque fois $\preceq$ est l'ordre total naturel dans l'ensemble considéré.

4.2 Intervalles et pavés

D'une façon générale, si $(\mathbf{D}, \preceq)$ est un ensemble ordonné, formé d'un ensemble $\mathbf{D}$ d'au moins deux éléments et d'une relation d'ordre total $\preceq$ sur $\mathbf{D}$, nous appelons *intervalle de* $(\mathbf{D}, \preceq)$ tout sous-ensemble éventuellement vide de $\mathbf{D}$, qui est de la forme

$$\{d \in \mathbf{D} \,|\, e \preceq d \text{ et } d \preceq e'\},$$

où e et e' sont des éléments quelconques de $\mathbf{D}$. Nous le notons $[e, e']$. Le fait que nous n'imposions pas $e \preceq e'$ et que l'ensemble $\mathbf{D}$ ait plus d'un élément assure que l'ensemble vide fait partie des intervalles. Dans le cas particulier où l'ensemble ordonné est l'ensemble $(\mathbf{N}, \leq)$ des entiers naturels, nous écrivons $e..e'$ au lieu de $[e, e']$.

Un *pavé de dimension* n, ou n*-pavé*, sur $(\mathbf{D}, \preceq)$ est un sous-ensemble de $\mathbf{D}^n$ de la forme $a_1 \times \cdots \times a_n$, avec $n \geq 1$, où chaque a_i est un intervalle de $(\mathbf{D}, \preceq)$. Du fait que les a_i peuvent être vides, l'ensemble vide $\emptyset$ est un pavé de dimension n pour tout n. Lorsque a n'est pas vide, les a_i tels que $a = a_1 \times \cdots \times a_n$ sont uniques et on a $(a_1, \ldots, a_n) = (\pi_1(a), \ldots, \pi_n(a))$.

Soit a un sous-ensemble de $\mathbf{D}$. Nous désignons par $\mathit{min}\,(a)$ et $\mathit{max}\,(a)$, lorsqu'ils existent, le plus petit élément et le plus grand élément de a dans $(\mathbf{D}, \preceq)$. Nous gardons les notations classiques $\min a$ et $\max a$ pour l'ensemble ordonné particulier $(\mathbf{N}, \leq)$. Nous désignons par $\mathrm{apx}\,(a)$ le plus petit intervalle de $(\mathbf{D}, \preceq)$ qui contient a, s'il existe. La notion de plus petit est prise au sens de l'inclusion. Bien entendu si $\mathit{min}\,(a)$ et $\mathit{max}\,(a)$ existent, $\mathrm{apx}\,(a)$ existe et est égal à $[\mathit{min}\,(a), \mathit{max}\,(a)]$. Nous généralisons la notation $apx(a)$ comme suit :

Définition 4.2.1 Si r un sous-ensemble de $\mathbf{D}^n$, nous désignons par $\mathrm{apx}\,(r)$ le plus petit n-pavé sur $(\mathbf{D}, \preceq)$ qui contient r, s'il existe. La notion de plus petit est prise au sens de l'inclusion.

On montre que :

Propriété 4.2.2 Si r est un sous-ensemble de $\mathbf{D}^n$ alors, soit les ensembles $\mathrm{apx}\,(\pi_1(r)) \times \cdots \times \mathrm{apx}\,(\pi_n(r))$ et $\mathrm{apx}\,(r)$ n'existent pas, soit ils existent et sont égaux.

4.3 Calcul de apx $(\pi_i(r \cap a))$

Donnons nous une bonne fois pour toutes un ensemble totalement ordonné $(\mathbf{D}, \preceq)$ ayant un plus petit élément $\mathit{min}\,(\mathbf{D})$ et un plus grand éléments $\mathit{max}\,(\mathbf{D})$. Les éléments $\underline{\emptyset}$ et $\overline{\emptyset}$ existent donc et sont respectivement égaux à $\mathit{max}\,(\mathbf{D})$ et $\mathit{min}\,(\mathbf{D})$. De ce fait si a est un intervalle, même vide, de $(\mathbf{D}, \preceq)$, les éléments $\underline{a}$ et $\overline{a}$ existent et on a toujours $a = [\underline{a}, \overline{a}]$.

Soit a un sous-ensemble de $\mathbf{D}$. Une application f de a dans $\mathbf{D}$ est *croissante* si pour tout e et d pris dans a on a $e \preceq d$ entraine $f(e) \preceq f(d)$, *décroissante* si pour tout e et d pris dans $\mathbf{D}$ on a $e \preceq d$ entraine $f(d) \preceq f(e)$ et *monotone* si elle est croissante ou décroissante.

Soit maintenant un sous-ensemble r de $\mathbf{D}^n$, une application f de r dans $\mathbf{D}$ et un élément i de $1..n$. L'application f est *monotone dans sa composante* i si, quels que soient le n-uplet $(e_1, \ldots, e_n)$ de r, l'application $d \mapsto f(e_1, \ldots, e_{i-1}, d, e_{i+1}, \ldots, e_n)$ de $\pi_i(r)$ dans $\mathbf{D}$ est monotone.

Propriété 4.3.1 (Valeure extrêmes) *Soit* $a = a_1 \times \cdots \times a_n$ *un* n*-pavé non vide de* $(\mathbf{D}, \preceq)$ *et soit* f *une application de* a *dans* $\mathbf{D}$ *qui est monotone dans toutes ses composantes. Les éléments* $\mathit{min}\,(\{f(d) \mid d \in a\})$ *et* $\mathit{max}\,(\{f(d) \mid d \in a\})$ *existent et sont respectivement égaux à*

$$\mathit{min}\,(\{f(d) \mid d \in \{\mathit{min}\,(a_1), \mathit{max}\,(a_1)\} \times \cdots \times \{\mathit{min}\,(a_n), \mathit{max}\,(a_n)\}\}),$$
$$\mathit{max}\,(\{f(d) \mid d \in \{\mathit{min}\,(a_1), \mathit{max}\,(a_1)\} \times \cdots \times \{\mathit{min}\,(a_n), \mathit{max}\,(a_n)\}\})$$

Preuve A faire comme exercice. Ceci termine la preuve.

Définition 4.3.2 Si r est un sous-ensemble de $\mathbf{D}^n$ et i un élément de $1..n$, on introduit, si elles existent, les applications de $\mathbf{D}^n$ dans $\mathcal{P}(\mathbf{D})$:

$$r_{(i)} : (e_1, \ldots, e_{i-1}, e_{i+1}, \ldots, e_n) \mapsto \underline{\{d \in \mathbf{D} \mid (e_1, \ldots, e_{i-1}, d, e_{i+1}, \ldots, e_n) \in r\}},$$
$$r^{(i)} : (e_1, \ldots, e_{i-1}, e_{i+1}, \ldots, e_n) \mapsto \overline{\{d \in \mathbf{D} \mid (e_1, \ldots, e_{i-1}, d, e_{i+1}, \ldots, e_n) \in r\}}.$$

Propriété 4.3.3 *Soient n un entier positif, i un élément de $1..n$ et r un sous-ensemble de $\mathbf{D}^n$ tel que :*
(1) l'ensemble $apx(r)$ existe,
(2) pour tout n-pavé a, l'ensemble $\pi_i(r \cap a)$ est un intervalle,
(3) les applications $d \mapsto r_{(i)}(d)$ et $d \mapsto r^{(i)}(d)$ de $apx(r)$ dans $\mathbf{D}$, qui existent alors, sont monotones dans toutes leurs composantes.
Alors, pour tout n-pavé a, l'ensemble $apx(\pi_i(r \cap a))$ existe et est égal à

$$b_i \cap [\underline{\{r_{(i)}(d) \mid d \in s\}},\ \overline{\{r^{(i)}(d) \mid d \in s\}}\,]$$

avec

$$\begin{array}{ll} b_j = \pi_j(a \cap apx(r)), & \text{pour tout } j \in 1..n, \\ c_j = b_j \cap \{\underline{b_j}, \overline{b_j}\}, & \text{pour tout } j \in (1..n) - \{i\}, \\ s = c_1 \times \cdots \times c_{i-1} \times c_{i+1} \times \cdots \times c_n. & \end{array}$$

Preuve Posons $b' = b_1 \times \cdots \times b_{i-1} \times \mathbf{D} \times b_{i+1} \times \cdots \times b_n$ et $b'' = b_1 \times \cdots \times b_{i-1} \times b_{i+1} \times \cdots \times b_n$. On a la suite d'égalités :

$$\begin{array}{l} \mathrm{apx}\,(\pi_i(r \cap a)) = \\ \pi_i(r \cap a) = \\ \pi_i(r \cap a \cap \mathrm{apx}\,(r)) = \\ \pi_i(r \cap b_1 \times \cdots \times b_n) = \\ b_i \cap \pi_i(r \cap b') = \\ b_i \cap [\underline{\pi_i(r \cap b')},\ \overline{\pi_i(r \cap b')}] = \\ b_i \cap [\underline{\{r_{(i)}(d) \mid d \in b''\}},\ \overline{\{r^{(i)}(d) \mid d \in b''\}}] = \\ b_i \cap [\underline{\{r_{(i)}(d) \mid d \in s\}},\ \overline{\{r^{(i)}(d) \mid d \in s\}}] \end{array}$$

Pour montrer la dernière égalité on considère deux cas. Si $s = \emptyset$ alors au moins un b_j avec $j \neq i$ est vide et donc $b'' = \emptyset$. Les deux membres de l'égalité sont alors égaux à $b_i \cap [\underline{\emptyset}, \overline{\emptyset}]$, c'est-à-dire $b_i \cap [max\,(\mathbf{D}), min\,(\mathbf{D})]$, c'est-à-dire $\emptyset$. Si $s \neq \emptyset$ alors s est fini et le dernier membre de l'égalité s'écrit

$$b_i \cap [min\,(\{r_{(i)}(d) \mid d \in s\}),\ max\,(\{r^{(i)}(d) \mid d \in s\})].$$

Du fait qu'aucun b_j avec $j \neq i$ n'est vide, chaque c_j avec $j \neq i$ est égal à $\{min\,(b_j), max\,(b_j)\}$. D'après la propriété 4.3.1, le dernier membre de l'égalité est alors égal à

$$b_i \cap [min\,(\{r_{(i)}(d) \mid d \in b''\}),\ max\,(\{r^{(i)}(d) \mid d \in b''\})]$$

et donc égal au premier membre de la dernière égalité. Ceci termine la preuve.

Exemple 4.3.4 (*plus*) Soit $(\hat{\mathbf{R}}, \leq)$ l'ensemble totalement ordonné obtenu en posant $\hat{\mathbf{R}} = \mathbf{R} \cup \{-\infty, +\infty\}$ et en prolongeant la relation d'ordre $\leq$ de façon à ce que $-\infty$ et $+\infty$ soient le plus petite élément et le plus grand élément de $\hat{\mathbf{R}}$. Soit la relation ternaire

$$plus = \{(x, y, z) \in \mathbf{R}^3 \mid z = x + y\}.$$

L'ensemble $\mathrm{apx}\,(plus)$ est égal à $[-\infty, +\infty]^3$ et existe donc. Pour tout 3-pavé a sur $(\hat{\mathbf{R}}, \leq)$ et tout $i \in 1..3$, l'ensemble $\pi_i(plus \cap a)$ est bien un intervalle. Mais l'application $d \mapsto plus_{(3)}(d)$ n'est pas monotone dans toutes ses composantes car

$$(plus_{(3)}(\infty, 0),\ plus_{(3)}(0, 0),\ plus_{(3)}(1, 0)) \ = \ (+\infty, 0, 1).$$

On ne peut donc pas utiliser la proprités 4.3.3 pour calculer $\mathrm{apx}\,(plus \cap a)$.

Exemple 4.3.5 (*plusbis*) Plaçons nous toujours dans $(\hat{\mathbf{R}}, \leq)$ et posons $I = \{-\infty, +\infty\}$. La relation précédente se prolonge naturellement en la relation

$$\begin{array}{rcl} plusbis & = & plus \,\cup \\ & & \{(x, y, z) \in I^3 \mid x = z \text{ ou } y = z\} \cup \\ & & \{(x, y, z) \in \mathbf{R} \times I \times I \mid y = z\} \cup \\ & & \{(x, y, z) \in I \times \mathbf{R} \times I \mid x = z\} \cup \\ & & \{(x, y, z) \in I \times I \times \mathbf{R} \mid x \neq y\} \end{array}$$

qui satisfait à toutes les conditions requises pour calculer apx $(plusbis \cap a)$ en se servant de la propriété 4.3.3. En convenant que $-(-\infty) = +\infty$ et $-(+\infty) = -\infty$ on a

$$plusbis_{(1)}(x, y) = \begin{cases} y - x, & \text{si } (x, y) \in \mathbf{R} \times \mathbf{R}, \\ -x, & \text{si } (x, y) \in I \times \mathbf{R}, \\ y, & \text{si } (x, y) \in \mathbf{R} \times I, \\ min\,\{-x, y\}, & \text{si } (x, y) \in I \times I, \end{cases}$$

$$plusbis^{(1)}(x, y) = \begin{cases} y - x, & \text{si } (x, y) \in \mathbf{R} \times \mathbf{R}, \\ -x, & \text{si } (x, y) \in I \times \mathbf{R}, \\ y, & \text{si } (x, y) \in \mathbf{R} \times I, \\ max\,\{-x, y\}, & \text{si } (x, y) \in I \times I, \end{cases}$$

$$plusbis_{(2)}(x, y) = plusbis_{(1)}(x, y),$$

$$plusbis^{(2)}(x, y) = plusbis^{(1)}(x, y),$$

$$plusbis_{(3)}(x, y) = \begin{cases} x + y, & \text{si } (x, y) \in \mathbf{R} \times \mathbf{R}, \\ x, & \text{si } (x, y) \in I \times \mathbf{R}, \\ y, & \text{si } (x, y) \in \mathbf{R} \times I, \\ min\,\{x, y\}, & \text{si } (x, y) \in I \times I, \end{cases}$$

$$plusbis^{(3)}(x, y) = \begin{cases} x + y, & \text{si } (x, y) \in \mathbf{R} \times \mathbf{R}, \\ x, & \text{si } (x, y) \in I \times \mathbf{R}, \\ y, & \text{si } (x, y) \in \mathbf{R} \times I, \\ max\,\{x, y\}, & \text{si } (x, y) \in I \times I. \end{cases}$$

On trouve donc

$$\text{apx}\,(\pi_1(plusbis \cap a_1 \times a_2 \times a_3 = a_1 \cap [plusbis_{(1)}(\overline{a_2}, \underline{a_3}),\ plusbis^{(1)}(\underline{a_2}, \overline{a_3})],$$

$$\text{apx}\,(\pi_2(plusbis \cap a_1 \times a_2 \times a_3 = a_2 \cap [plusbis_{(1)}(\overline{a_1}, \underline{a_3}),\ plusbis^{(1)}(\underline{a_1}, \overline{a_3}]),$$

$$\text{apx}\,(\pi_3(plusbis \cap a_1 \times a_2 \times a_3 = a_3 \cap [plusbis_{(3)}(\underline{a_1}, \underline{a_2}),\ plusbis^{(3)}(\overline{a_1}, \overline{a_2})],$$

Chapitre 5

Algorithme de Fourier

Soit P_n une formule de la forme

$P_n : [a_{11}x_1+\ldots+a_{1n}x_n+b_1 \geq 0 \wedge \cdots \wedge a_{mn}x_1+\ldots+a_{mn}x_n+b_n \geq 0]$

On veut déterminer si la propriété $(\exists x_1)\cdots(\exists x_n)P_n$ est où n'est pas vraie.

Algorithme En partant de P_n construire la suite de propositions $P_n, P_{n-1}, \ldots, P_0$ où chaque P_{j-1} est calculé comme suit à partir de P_j : Réordonner les inéquations de P_j et multipler en les coefficients par des réels positifs de façon à obtenir une formule équivalente de la forme

$$\begin{array}{l} \bigwedge_{i=1}^{p} [c_{i1}x_1+\cdots+c_{ij-1}x_{j-1}+0x_j+c_{i0} \geq 0] \\ \qquad\qquad\qquad \wedge \\ \bigwedge_{i=1}^{q} [d_{i1}x_1+\cdots+d_{ij-1}x_{j-1}-x_j+d_{i0} \geq 0] \\ \qquad\qquad\qquad \wedge \\ \bigwedge_{i=1}^{r} [e_{i1}x_1+\cdots+e_{ij-1}x_{j-1}+x_j+e_{i0} \geq 0]. \end{array}$$

Prendre pour P_{i-1} la formule

$$\begin{array}{l} \bigwedge_{i=1}^{p} [c_{i1}x_1 + \cdots + c_{ij-1}x_{j-1} + c_{i0} \geq 0] \\ \qquad\qquad\qquad\qquad\qquad \wedge \\ \bigwedge_{i=1}^{q} \bigwedge_{k=1}^{r} [(d_{i1}+e_{k1})x_1+\cdots+(d_{ij-1}+e_{kj-1})x_{j-1}+(d_{i0}+e_{i0}) \geq 0]. \end{array}$$

Thèorème La propriété $(\exists x_1)\cdots(\exists x_n)P_n$ est vraie si et seulement si P_0 ne contient aucune inéquation de la forme $k \geq 0$, où k est un réel strictement négatif.

Démonstration Les propriété $(\exists x_j)P_j$ et P_{j-1} sont constamment équivalentes car elles sont toutes les deux équivalentes à la propriéte

$$\begin{array}{l} \bigwedge_{i=1}^{p} [c_{i1}x_1 + \cdots + c_{ij-1}x_{j-1} + c_0 \geq 0] \\ \qquad\qquad\qquad\qquad\qquad \wedge \\ \max(\{-\infty\} \cup \{d_{i1}x_1+\cdots+d_{ij-1}x_{j-1}+d_{i0} \,|\, i \in \{1,\ldots,q\}\}) \geq \\ \min(\{+\infty\} \cup \{e_{i1}x_1+\cdots+e_{ij-1}x_{j-1}+e_{i0} \,|\, i \in \{1,\ldots,r\}\}). \end{array}$$

La propriété $(\exists x_1)\cdots(\exists x_n)P_n$ est donc équivalente à la propriété P_0 qui par constructions est de la forme $\bigwedge_i [k_i \geq 0]$. Elle est donc vraie si et seulement si aucun des k_i n'est strictement positif.

5.1 Vecteurs et matrices

Un vecteur x de dimension n est une application $i \mapsto x_i$ avec $i \in \{1,\ldots,n\}$ et $x_i \in \mathbf{R}$; on le note $(x_1,\ldots,x_n)$. Une matrice A de dimension $m \times n$ est une application $(i,j) \mapsto a_{ij}$ avec $i \in \{1,\ldots,m\}$, $j \in \{1,\ldots,n\}$ et $a_{ij} \in \mathbf{R}$; on la note

$$\begin{bmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \ldots & a_{mn} \end{bmatrix}.$$

Si x et y sont des vecteurs de dimension n et m on note Ax et yA les vecteurs $i \mapsto \sum_{j=1}^{n} a_{ij}x_j$ et $j \mapsto \sum_{i=1}^{m} a_{ij}y_i$ de dimensions n et m. Si x et y sont des vecteurs de même dimension n on note xy le réel $\sum_{i=1}^{n} x_i x_j$ et si ρ désigne l'une des relations $<, \leq, >, \geq$ on écrit $x\rho y$ pour $x_1\rho y_1 \wedge \cdots \wedge x_n \rho y_n$. Enfin lorsqu'il n'y a pas de risque de confusion on utilise 0 pour désigner un vecteur de la forme $(0, \ldots, 0)$.

5.2 Lemme de Farkas

Théorème $(\exists x \in \mathbf{R}^n)[Ax+b \geq 0] \equiv \neg(\exists y \in \mathbf{R}^m)[y \geq 0 \wedge yA = 0 \wedge yb < 0]$

Démonstration Soient G et D les membres gauche et droit de l'équivalence.

Montrons que $G \Rightarrow D$. Supposons G et $\neg D$ et montrons qu'on arrive à une contradiction. Il existe donc x et y tels que $Ax+b \geq 0$, $y \geq 0$, $yA=0$ et $yb<0$. On a donc $y(Ax+b) \geq 0$, c'est-à-dire $yAx+yb \geq 0$, et donc $yb \geq 0$ ce qui contredit $yb<0$.

Montrons que $\neg G \Rightarrow \neg D$. Supposons que $\neg G$. En explicitant les notations matricielles cela revient à supposer que $(\exists x_1) \cdots (\exists x_n) P_n$, où P_n est la propriété introduite pour décrire l'algorithme de Fourier. Cet algorithme permet alors de calculer une inéquation de la forme $k \geq 0$, où k est un réel strictement négatif obtenu par une combinaison linéaire des membres gauches des inéquations

$$a_{i1}x_1 + \ldots + a_{in}x_n + b_i \geq 0$$

avec des coefficients non négatifs y_i. Il s'ensuit qu'il existe $k \in \mathbf{R}$ et $y \in \mathbf{R}^n$ tel que $y \geq 0$, $yA = 0$ et $yb = k$ ce qui n'est rien d'autre que la propriété $\neg D$.