Groupe de travail LDP

L'algèbre d'unification

Marc Bagnol

31 juillet 2013

Introduction

L'unification a d'abord été introduite par Herbrand, puis étudiée dans les années 60 par Robinson, comme un élément de sa procédure de déduction automatique. Elle est également au cœur du fonctionnement du langage PROLOG.

On commencera par une introduction aux idées de base de l'unification : termes, substitution, unificateur principal, etc. et on survolera la preuve de l'existence d'unificateurs principaux. Pour plus de détails vous pouvez regarder [5] ou d'autres notes de cours qui trainent sur le web.
La deuxième partie de l'exposé est consacrée aux flux et à l'algèbre d'unification, introduits par J.-Y. Girard pour construire une Géométrie de l'Intéraction finitaire [2].

Références

[1] Jean-Yves GIRARD : Geometry of interaction III : accommodating the additives. *In In : Advances in Linear Logic, LNS 222,CUP, 329–389*, pages 329–389. Cambridge University Press, 1995.

[2] Jean-Yves GIRARD : Geometry of interaction VI : a blueprint for transcendental syntax. preprint.

[3] Gérard HUET : The undecidability of unification in third order logic. 1973.

[4] Gérard HUET : *Résolution d'équations dans les langages d'ordre 1, 2... ω*. Thèse de doctorat, 1976.

[5] Alberto MARTELLI et Ugo MONTANARI : An efficient unification algorithm. *ACM Trans. Program. Lang. Syst.*, 1982.

[6] M. S. PATERSON et M. N. WEGMAN : Linear unification. *In Proceedings of the eighth annual ACM symposium on Theory of computing*, STOC '76. ACM.

---

1 Unification

D'une manière très générale, le problème d'unification consiste à se demander si deux termes donnés peuvent être "rendus égaux" par des substitutions de leurs variables ; ou encore : étant données deux descriptions partielles (les termes avec variables), se demander s'il existe un objet qui satisfait les deux en même temps.

Termes et substitutions

Le cadre est le suivant : on a un ensemble (infini) $\mathcal{V}$ de variables et un ensemble $\mathcal{F}$ de symboles de fonctions d'arités données. On s'intéresse alors aux termes construits sur $\mathcal{V}$ et $\mathcal{F}$.

On va fixer un ensemble de termes une bonne fois pour toutes : on se donne des variables $x, y, z \ldots$, une constante c, deux fonctions unaires f, g et une fonction binaire h. Ce qui donne pour l'ensemble des termes la grammaire :

$$T ::= x, y, z \ldots \mid c \mid f(T) \mid g(T) \mid h(T,T)$$

Une **substitution**, c'est une fonction des variables vers les termes $\theta : \mathcal{V} \to T$ de **domaine** (l'ensemble des variables telles que telle que $\theta(v) \neq v$) fini. On notera $\mathtt{Dom}(\theta)$ le domaine d'une substitution.

On peut écrire une substitution θ de domaine $\{ x_1, \ldots, x_n \}$, telle que $\theta(x_1) = u_1$, $\theta(x_2) = u_2$, ... de la façon suivante :

$$\{ x_1 \mapsto u_1 ; \ldots ; x_n \mapsto u_n \}$$

Les substitutions agissent sur les termes de la manière attendue :

$$t.\{ x_i \mapsto u_i \} := t[u_i/x_i]$$

Exemples :

$h(x,y).\{ x \mapsto c ; z \mapsto f(z) \} = h(c,y)$
$h(f(z),z).\{ x \mapsto c ; z \mapsto f(z) \} = h(ff(z), f(z))$

On peut définir la **composition** de substitutions, de manière à avoir

$$t.(\theta;\theta') = (t.\theta).\theta' \qquad \text{où ";" est la composition séquentielle : } \theta;\theta' = \theta' \circ \theta$$

on écrit $\theta = \{ x_i \mapsto u_i \}$ et $\theta' = \{ y_j \mapsto v_j \}$,

$$\theta;\theta' := \{ x_i \mapsto u_i.\theta' \} \cup \{ y_i \mapsto v_i \mid y_i \notin \mathtt{Dom}(\theta) \}$$

Exemple :

$\theta = \{z \mapsto h(z,x) ; x \mapsto c\}$
$\theta;\theta = \{z \mapsto h(h(z,x),c) ; x \mapsto c\}$
$\theta;\theta;\theta = \{z \mapsto h(h(h(z,x),c),c) ; x \mapsto c\}$

Un peu de vocabulaire :

On appelle un **renommage de variables** une substitution dont l'image est incluse dans $\mathcal{V}$ (elle envoie les variables vers d'autres variables) et bijective. Ce sont les seules substitutions inversibles, au sens de la composition définie plus haut (qui correspond dans ce cas à la composition de fonctions).
On dira que θ et θ' sont égales **à renommage de variables près** s'il existe un renommage de variables α tel que $\theta' = \theta;\alpha$.

On dit qu'une substitution $\theta = \{x_i \mapsto u_i\}$ est **idempotente** si $\theta;\theta = \theta$. Cette propriété est évidemment équivalente au fait qu'aucun des x_i n'apparaît dans aucun des u_j. Toute substitution est égale à une substitution idempotente à renommage des variables près.

On dit qu'une substitution θ' est une **instance** de θ s'il existe σ telle que $\theta' = \theta;\sigma$.
On peut montrer que si θ_1 et θ_2 sont des instances l'une de l'autre, alors elles sont égales à renommage de variable près.

Problèmes d'unification

On dit que deux termes t, u sont **unifiables** s'il existe une substitution θ telle que

$$t.\theta = u.\theta$$

Dans ce cas on écrit $t \sim u$ et on dit que θ est un **unificateur** de t et u.

De plus, on dira qu'un unificateur θ de t et u est **principal** si tout autre unificateur de t et u est une instance de θ. Ainsi, les unificateurs principaux de deux termes (s'il en existe) sont égaux à renommage de variable près.

On étend ces notions de la manière évidente aux ensembles d'équations d'unification $\{u_i \sim^? v_i\}$.

Exemples :

$f(x) \sim f(c)$ *avec* $\theta = \{x \mapsto c\}$

$g(f(x)) \not\sim f(f(x))$

$h(x, v) \sim h(u, y)$ *avec* $\theta = \{x \mapsto u\,;\ y \mapsto v\}$

$x \not\sim f(x)$

$f(x) \sim f(g(y))$ *avec*
$\theta = \{x \mapsto g(g(c)); y \mapsto g(c)\}$ *(non principal)*
ou $\theta = \{x \mapsto g(z)\,;\ y \mapsto z\}$ *(principal)*

Il se trouve (on survolera la preuve dans la prochaine section) que si deux termes sont unifiables, alors ils ont un unificateur principal.

Théorème 1.1 : MGU [1]

> Si un ensemble fini d'équations d'unification E admet un unificateur, alors il admet un unificateur principal.

La preuve est effective, basée sur un algorithme qui trouve un unificateur principal. il s'agit donc d'un problème décidable. Plus précisément

Théorème 1.2 : Linéarité [6]

> Il existe un algorithme fonctionnant en temps linéaire qui détermine si un ensemble d'équations d'unification a une solution, et fournit un unificateur principal dans ce cas.

Remarque. *On est ici dans le cas simple "unification du premier ordre (les variables sont d'arité zéro), sans congruence". Si on autorise des variables pour les symboles de fonctions, le problème devient indécidable (en fait semi-décidable [3, 4]).*

Preuve du théorème 1.1

On donne les grandes étapes de la preuve donnée dans [5] et son découpage en lemmes, sans entrer dans trop de détails.

La première étape est de définir deux opérations qu'on peut appliquer à un ensemble d'équations $E = \{u_i \sim^? v_i\}$:

- **réduction de variable :** si $x \sim^? t$ (où x est une variable) appartient à E, on le réduit en E' qui est E dans lequel on a appliqué la substitution $\{x \mapsto t\}$ à tous les termes de toutes les autres équations et où on a conservé $x \sim^? t$.
- **réduction de fonction :** si $p(\vec{u_i}) \sim^? p(\vec{v_i})$ (où p est un symbole de fonction) appartient à E, on le réduit en E' en remplaçant l'équation par $u_i \sim^? v_i$ pour tout i.

1. Pour *Most General Unifier*.

On dit que deux systèmes E et E' sont **equivalents** s'ils ont le même ensemble de solutions.

Les deux opérations, réduction de variable et réduction de fonction, ne modifient pas (sous certaines conditions) les solutions du système.

Lemme 1.3 :

> Si $x \sim^? t$ appartient à E alors
> - soit la variable x apparaît dans t (et $t \neq x$), dans ce cas E n'a pas de solution ;
> - soit le système E' obtenu par réduction de variable est équivalent à E.

Lemme 1.4 :

> Si $p(\vec{u_i}) \sim^? q(\vec{v_i})$ (où p et q sont des symboles de fonctions) appartient à E alors
> - soit $p \neq q$, dans ce cas E n'a pas de solution ;
> - soit le système E' obtenu par réduction de fonction est équivalent à E.

L'idée de l'algorithme est de progressivement transformer l'ensemble d'équations en un ensemble d'équation d'une forme particulière dont la solution est évidente :

On appelle système en **forme résolue** un système de la forme $E = \{x_i \sim^? t_i\}$ où
- les x_i sont des variables ;
- les variables x_i sont deux à deux distinctes ;
- chaque variable x_i n'apparaît dans aucun t_j.

Un système en forme résolue $E = \{x_i \sim^? t_i\}$ a pour unificateur évident $\theta = \{x_i \mapsto t_i\}$, de plus

Lemme 1.5 :

> La substitution $\theta = \{x_i \mapsto t_i\}$ est un unificateur *principal* pour le système $E = \{x_i \sim^? t_i\}$.

On définit donc l'algorithme suivant :

```
Tant qu'une des réductions est possible: choisir une équation de E,
Si elle est de la forme x ~? x: la supprimer
Si elle est de la forme t ~? x (où t n'est pas une variable):
 la remplacer par x ~? t
Si elle est de la forme x ~? t et x apparaît ailleurs dans E:
   Si x apparaît dans t: ECHEC
   Sinon appliquer la réduction de variable
Si elle est de la forme p(u_i) ~? q(v_i):
   Si p ≠ q: ECHEC
   Sinon appliquer la réduction de fonction
```

Il est clair que si l'algorithme termine sur un échec, par les lemmes 1.3 et 1.4, E n'a pas de solution. S'il termine car aucune transformation ne s'applique, le système est en forme résolue et équivalent (encore par les lemmes 1.3 et 1.4) au système de départ, on a donc un unificateur principal par le lemme 1.5.

Reste donc à prouver que

Lemme 1.6 :

> L'algorithme décrit ci-dessus termine quels que soient les choix effectués à chaque itération.

Ce qu'on fait par exemple en associant un poids à tout système d'équations puis en montrant que les opérations font toutes décroitre strictement ce poids.

2 Algèbre d'unification

Les flux

Étant donné un ensemble de termes T, on définit l'ensemble $\mathscr{F}(T)$ des **flux** de T comme l'ensemble des expressions de la forme

$$u \leftarrow v \quad \text{où } u \text{ et } v \text{ ont exactement les mêmes ensembles de variables}$$

qu'on considèrera à renommage des variables près. Par exemple $f(x) \leftarrow g(x) = f(y) \leftarrow g(y) = \dots$ et $h(x,y) \leftarrow h(y,x) = h(y,x) \leftarrow h(x,y) = \dots$ [2] sont des flux.

La condition sur les variables permet de définir une action sur les termes clos avec de bonnes propriétés (voir plus bas).

On peut munir les flux d'une composition partielle.
Une intuition utile pour comprendre la façon dont elle est définie est d'y penser comme des *filtrages* (ou `match ... with ...`) à la ML (CAML, HASKELL, etc.) la composition de deux flux correspond exactement à la composition de filtrages.

Soient donc deux flux $l_1 = u \leftarrow v$ et $l_2 = t \leftarrow w$. On suppose avoir choisi deux représentants de leurs classes d'équivalence dont les ensembles de variables sont *disjoints*.

Leur **composition** (ou **produit**) $l_1 l_2$ est définie si $v \sim t$ (avec un unificateur principal θ) et vaut dans ce cas

$$u.\theta \leftarrow w.\theta$$

Exemples :

$$\big(g(x) \leftarrow f f(x)\big)\,\big(f(y) \leftarrow f g(y)\big) = g f(z) \leftarrow f g(z)$$
$$\big(g(x) \leftarrow h(f g(x), g(c))\big)\,\big(h(f(y), y) \leftarrow f f(y)\big) = g(c) \leftarrow f f g(c)$$

Le fait que la classe d'équivalence du résultat ne dépende pas des représentants choisis ni de l'unificateur principal choisi vient en particulier du fait que deux unificateurs principaux sont égaux à renommage de variable près.

Cette composition est associative, au sens où $l_1(l_2 l_3)$ est défini si et seulement si $(l_1 l_2) l_3$ est défini et ces deux flux sont égaux dans ce cas. C'est une conséquence de l'existence d'unificateurs principaux pour les ensembles d'équations.

Elle admet un élément neutre, $1 := x \leftarrow x$. Si l'on ajoute un flux $\perp$ pour donner un résultat en cas d'échec de l'unification, l'ensemble des flux devient un monoïde.

De plus, on définit un adjoint (par analogie avec l'adjoint en algèbre linéaire), $(u \leftarrow v)^\dagger := v \leftarrow u$.
Cette opération est involutive et compatible avec le produit $(l_1 l_2)^\dagger = l_2^\dagger l_1^\dagger$. On peut alors voir que $\mathscr{F}(T) \cup \{\perp\}$ est un *monoïde inversif*.

Action sur les termes clos

On note $\mathtt{cl}(T)$ l'ensemble des termes clos (sans variables) de T. $\mathscr{F}(T)$ agit sur $\mathtt{cl}(T)$ de la façon suivante :

$$(u \leftarrow v).t := \begin{cases} \text{si } v \sim t \text{ avec unificateur principal } \theta : u.\theta \\ \text{indéfini sinon} \end{cases}$$

Le résultat est bien un terme clos car les variables de u sont contenues dans les variables de v (en fait elles sont même identiques) et toutes instancées en des termes clos.

2. $\cdots \neq h(x,y) \leftarrow h(x,y)$

Inversement, comme les variables de v sont contenues dans les variables de u, l'action est injective sur les termes pour lesquels elle est définie. Les flux agissent donc comme des bijections partielles de l'ensemble des termes.

On voit bien ici l'intérêt d'avoir posé la contrainte sur les variables des flux : on a ainsi une action (partielle) bien définie sur les termes clos, et cette action est injective. À tout flux $u \leftarrow v$, on peut donc associer une bijection partielle $[u \leftarrow v]$ sur les termes clos, des instances de v vers les instances de u.

De plus on a bien une "action partielle" (ce n'est pas une notion très standard) au sens où $1.t = t$ et $(l_1 l_2).t = l_1.(l_2.t)$ pour tout t.

Algèbre engendrée

On s'intéresse à l'algèbre engendrée par les flux, que l'on peut définir de différentes manières. La plus simple (mais peut-être pas le plus générale) consiste à poser l'espace de Hilbert $\mathbb{H} := l_2(\mathtt{cl}(T))$, l'espace des fonctions de carré sommable sur $\mathtt{cl}(T)$.
Le fait que $\mathscr{F}(T)$ agisse partiellement sur $\mathtt{cl}(T)$ permet de définir pour chaque flux l un opérateur $\langle l \rangle$ défini sur la base des δ_t (les fonctions caractéristiques des singletons $\{t\}$) de $\mathbb{H}$ par :

$$\langle l \rangle(\delta_t) := \begin{cases} \delta_{l.t} & \text{si } l.t \text{ est défini} \\ 0 & \text{sinon} \end{cases}$$

Comme de plus l'action est une injection partielle, les $\langle l \rangle$ sont en fait des isométries partielles de $\mathbb{H}$.

On définit la sous algèbre de $B(\mathbb{H})$ engendrée par les $\langle l \rangle$: **l'algèbre d'unification** qu'on notera $\mathscr{A}(T)$.

On a par ailleurs $\langle l^\dagger \rangle = \langle l \rangle^\dagger$, $\mathscr{A}(T) = \big(\mathscr{A}(T)\big)^\dagger$ est donc une $*$-algèbre.

Remarque. *On peut montrer facilement que l'algèbre de Von Neumann engendrée par $\mathscr{A}(T)$ est $B(\mathbb{H})$.*

Deux isométries de $\mathscr{A}(T)$

On pose $P := \langle f(x) \leftarrow x \rangle$ et $Q := \langle g(x) \leftarrow x \rangle$. P et Q sont des isométries de $\mathbb{H}$ vers deux sous espaces orthogonaux : l'espace engendré par les termes qui commencent par f et celui engendré par les termes qui commencent par g.

On peut alors poser l'isomorphisme (au sens *isomorphism into*, car non surjectif) d' $*$-algèbres

$$\phi : \begin{array}{ccc} \mathscr{A}(T) \oplus \mathscr{A}(T) & \longrightarrow & \mathscr{A}(T) \\ x \oplus y & \mapsto & PxP^\dagger + QyQ^\dagger \end{array}$$

Exemple : $\phi\big(\langle u \leftarrow v \rangle \oplus \langle t \leftarrow w \rangle\big) = \langle f(u) \leftarrow f(v) \rangle + \langle g(t) \leftarrow g(w) \rangle$

ϕ est en particulier une isométrie ($||\phi(h)|| = ||h||$ pour tout h).

De plus, on peut définir un **produit tensoriel interne**, qu'on notera $\overline{\otimes}$ (ou simplement $\otimes$ s'il n'y a pas de risque de confusion avec le produit tensoriel habituel) de la façon suivante

$$(u \leftarrow v) \overline{\otimes} (t \leftarrow w) := h(u,t) \leftarrow h(v,w)$$

qu'on étend ensuite à tout $\mathscr{A}(T)$ par bilinéarité.

Ce produit tensoriel *interne* permet de même de définir un isomorphisme (*into*), donc isométrique, de $\mathscr{A}(T) \otimes \mathscr{A}(T)$ dans $\mathscr{A}(T)$.

Ces deux propriétés sont essentielles pour la construction d'une Géométrie de l'Interaction [1] dans $\mathscr{A}(T)$.