Available online at www.sciencedirect.com
SCIENCE DIRECT®

C. R. Acad. Sci. Paris, Ser. I 338 (2004) 433–436

COMPTES RENDUS MATHEMATIQUE

Logique

Une axiomatisation de la substitution

Marcel Crabbé

Université catholique de Louvain, ISP-Centre de Logique, place Mercier, 14, 1348 Louvain-la-Neuve, Belgique

Reçu le 16 janvier 2004 ; accepté le 20 janvier 2004

Présenté par Jean-Yves Girard

Résumé

Nous examinons la notion de substitution de façon abstraite, sans la définir explicitement. Nous épinglons les traits essentiels de la substitution afin de définir un concept de structure substitutive, appelé *logos*. Nous formulons ensuite un théorème de complétude en vue de préciser et de justifier le sentiment que les propriétés de la substitution usuelle peuvent être dérivées uniquement des axiomes de logos. ***Pour citer cet article : M. Crabbé, C. R. Acad. Sci. Paris, Ser. I 338 (2004).***

Abstract

Axiomatisation of substitution. We investigate the notion of substitution in an abstract way, without defining it explicitly. We single out the essential features of the operation of performing a substitution in order to define a concept of substitutive structure, called *logos*. We then prove a completeness theorem making precise and justifying the intuition that formulas true for the usual substitution can be proved from the logos axioms only. ***To cite this article: M. Crabbé, C. R. Acad. Sci. Paris, Ser. I 338 (2004).***

1. Introduction

Confronté au problème de la substitution, on commence généralement par définir celle-ci, plus ou moins péniblement, selon qu'on veut traiter plus ou moins explicitement le problème des variables liées et on démontre ensuite certaines propriétés de cette notion et ce sont ces propriétés et celles-là seulement auxquelles il sera fait référence dans la suite. Il serait donc assez naturel de mettre d'entrée en évidence ces propriétés et de s'en contenter sans se préoccuper de la manière dont elles ont été établies. C'est dans cette optique que nous définissons comme dans [2] une notion de structure substitutive appelée « logos » qui axiomatise la substitution simple. Nous indiquons ensuite comment réduire la substitution simultanée à la simple et nous formulons un théorème de complétude justifiant le sentiment que les axiomes de logos suffisent à établir toutes les propriétés de la substitution. Nous estimons en outre que ces structures méritent d'être étudiées indépendamment de la notion de substitution qui les a motivées.[1]

Adresse e-mail : crabbe@risp.ucl.ac.be (M. Crabbé).

[1] Il est utile de remarquer ici que les recherches inaugurées par l'article [1] ont en commun non seulement de rendre la substitution explicite, mais encore en quelque sorte de la *définir* explicitement dans la mesure où des règles de réduction ont pour effet de la faire rentrer à l'intérieur des termes. Ces recherches ne recoupent donc que très partiellement le propos de cette note, puisque la structure interne des termes d'un logos demeure cachée et, partant, la « définition » de la substitution y est seulement implicite.

1631-073X/$ – see front matter
doi:10.1016/j.crma.2004.01.021

2. Le concept de logos

Un *logos* $\mathcal{L}$ est une structure $\langle \mathsf{Ter}_{\mathcal{L}}, \mathsf{V}_{\mathcal{L}}, \mathsf{vl}_{\mathcal{L}}, \mathsf{sub}_{\mathcal{L}} \rangle$, où $\mathsf{Ter}_{\mathcal{L}}$ est un ensemble, $\mathsf{V}_{\mathcal{L}}$ une partie infinie de $\mathsf{Ter}_{\mathcal{L}}$, $\mathsf{vl}_{\mathcal{L}}$ une application de $\mathsf{Ter}_{\mathcal{L}}$ vers les sous-ensembles finis de $\mathsf{V}_{\mathcal{L}}$ et $\mathsf{sub}_{\mathcal{L}}$ une application de $\mathsf{V}_{\mathcal{L}} \times \mathsf{Ter}_{\mathcal{L}} \times \mathsf{Ter}_{\mathcal{L}}$ vers $\mathsf{Ter}_{\mathcal{L}}$.

Les éléments de $\mathsf{Ter}_{\mathcal{L}}$ sont les *termes* et seront notés $M, N, P, \ldots$; les éléments de $\mathsf{V}_{\mathcal{L}}$ sont les *variables*, notées $x, y, z, \ldots$; $\mathsf{vl}_{\mathcal{L}}(M)$ est l'*ensemble des variables* (libres) de M ; $\mathsf{sub}_{\mathcal{L}}(\langle x, M, N \rangle)$ est le résultat de la *substitution de N à x dans M*. Nous omettons la mention de $\mathcal{L}$ quand ce n'est pas nécessaire et nous adoptons les notations $M[x := N]$ pour $\mathsf{sub}(\langle x, M, N \rangle)$ et $M[x := N][y := P]$ pour $(M[x := N])[y := P]$.
Un logos doit vérifier les axiomes :
1. $\mathsf{vl}(x) = \{x\}$; 2. Si $x \in \mathsf{vl}(M)$, alors $\mathsf{vl}(M[x := N]) = (\mathsf{vl}(M) \setminus \{x\}) \cup \mathsf{vl}(N)$;
3. Si $y \notin \mathsf{vl}(M)$, alors $M[x := y][y := x] = M$;
4. Si $x \neq y$ et $x \notin \mathsf{vl}(P)$, alors $M[x := N][y := P] = M[y := P][x := N[y := P]]$;
5. $x[x := M] = M$; 6. Si $x \notin \mathsf{vl}(M)$, alors $M[x := N] = M$.

3. Exemples

Logos de substitution. L'ensemble des termes d'un langage avec une infinité de variables, muni de la substitution, est évidemment un logos. Plus précisément, soit un ensemble infini de variables et un ensemble de symboles fonctionnels n-aires ϕ^n. Les termes sont définis comme suit : les variables sont des termes ; si $M_1, \ldots, M_n \in \mathsf{Ter}$, alors $\phi^n(M_1, \ldots, M_n) \in \mathsf{Ter}$. $\mathsf{vl}(M)$ et $M[x := N]$ sont définis inductivement de façon à s'interpréter, respectivement, comme l'ensemble des variables de M et le résultat de la substitution de N à x dans M.

Logos des suites finies. Soit un ensemble L qui est la réunion d'un ensemble infini de « variables » et d'un ensemble disjoint de « constantes ». Le logos des suites finies sur L a pour termes l'ensemble des mots sur L et les applications vl et $[x := P]$ sont les prolongements naturels de leurs restrictions à L : $\mathsf{vl}_{\restriction L}(M)$ est $\{M\}$, si M est une variable et $\emptyset$, si c'est une constante ; $\mathsf{sub}_{\restriction L}(x, M, P)$ est P, si M est x et M, sinon.

Termes ensemblistes. Cet exemple généralise celui des logos de substitution en ce qu'il ne suppose plus que les termes sont construits avec des symboles fonctionnels. En plus d'un ensemble infini de variables, du symbole relationnel binaire ε, des parenthèses et des symboles logiques usuels, il y a un abstracteur $\{\,|\quad\}$. Les termes sont définis — simultanément avec les formules — comme suit : les variables sont des termes ; si P et Q sont des termes $P \mathrel{\varepsilon} Q$ est une formule ; si A, B sont des formules et x une variable, alors $\neg A$, $(A \wedge B)$, $(A \vee B)$, $(A \to B)$, $(A \leftrightarrow B)$, $\forall x A$ et $\exists x A$ sont des formules et $\{ x \mid A \}$ est un terme.

Les opérateurs liant les variables sont $\forall$, $\exists$ et $\{\ \mid\ \}$. Si les variables liées sont éliminées par une méthode comme les carrés de Bourbaki, alors $\mathsf{vl}(P)$ et $Q[x := P]$ peuvent être définis de la manière usuelle.

Nous pouvons évidemment restreindre la collection des termes à une sous-collection quelconque fermée par substitution, comme les termes positifs, les termes (faiblement) stratifiés, ...

Ensembles. Soit A un ensemble infini d'« atomes ». Les variables sont les éléments de A et les autres termes sont les ensembles bien fondés héréditairement finis au dessus de A. On obtient un logos si on adopte la définition inductive suivante $\mathsf{vl}(x) = \{x\}$, $x[x := N] = N$, $y[x := N] = y$ (pour $y \neq x$) et, si M n'est pas une variable, $\mathsf{vl}(M) = \bigcup\{ \mathsf{vl}(N) \mid N \in M \}$ et $M[x := N] = \{ P[x := N] \mid P \in M \}$.

Si on généralise cet exemple aux non bien fondés, en utilisant l'axiome d'antifondation *AFA* avec atomes, on obtient une notion de langage avec des termes non bien fondés.

4. La substitution simultanée

La définition suivante montre que la substitution simultanée se réduit à la substitution simple. Soit une suite de variables distinctes $x_1, \dots, x_n$.

$M[x_1 := N_1, \dots, x_n := N_n]$ est *le* terme $M[x_1 := x'_1] \dots [x_n := x'_n][x'_1 := N_1] \dots [x'_n := N_n]$, où les variables $x'_1, \dots, x'_n$ sont distinctes, ne sont pas dans $\mathsf{vl}(M)$ et $x'_j \notin \mathsf{vl}(N_i)$ et $x_j \neq x'_i$, si $1 \leqslant i < j \leqslant n$. Les axiomes de logos permettent de montrer que cette définition est légitime en ce qu'elle est indépendante de la suite $x'_1, \dots, x'_n$ particulière choisie. Ces axiomes suffisent également à établir les propriétés attendues, en particulier les deux suivantes[2] :

$$M[x_1 := x_1, \dots, x_n := x_n] = M, \tag{1}$$

$$M[x_1 := N_1, \dots, x_n := N_n][y := P] = M\big[x_1 := N_1[y := P], \dots, x_n := N_n[y := P]\big], \quad \text{si } y \notin \mathsf{vl}(M) \setminus \{x_1, \dots, x_n\}. \tag{2}$$

5. La complétude

Alors que les quatre derniers axiomes de logos expriment des propriétés fondamentales de la substitution, un énoncé concernant le nombre de termes ou le nombre maximum de variables dans un terme apparaît comme purement contingent. La définition d'équation conditionnelle ci-dessous est destinée à exprimer cette notion de propriété *essentielle* de la substitution par opposition aux propriétés accidentelles.

Le *langage des logos* comprend une infinité dénombrable de variables ainsi que le symbole fonctionnel ternaire Sub, le symbole relationnel binaire $\in_{\mathsf{vl}}$ et les symboles logiques $=, \neg, \wedge, \vee, \rightarrow, \leftrightarrow, \forall$ et $\exists$. Le terme $\mathsf{Sub}(S, T, R)$ est noté $T\ (S := R)$.

Une valuation α des variables du langage par les termes d'un logos $\mathcal{L}$ s'étend par induction aux termes du langage : $\alpha(T\ (S := R))$ est $\alpha(T)[\alpha(S) := \alpha(R)]$, si $\alpha(S)$ est une variable de $\mathcal{L}$ et $\alpha(T)$ sinon. La satisfaction des formules atomiques par α se définit comme suit : $\mathcal{L} \models_\alpha T \in_{\mathsf{vl}} R$ ssi $\alpha(T) \in \mathsf{vl}_{\mathcal{L}}(\alpha(R))$; $\mathcal{L} \models_\alpha T = R$ ssi $\alpha(T) = \alpha(R)$.

Une formule est *valide* dans un logos ssi elle est satisfaite par toute valuation en interprétant les autres connecteurs logiques de la façon standard.

Une *condition* est une formule dans laquelle n'apparaît pas le symbole Sub et où les quantificateurs sont restreints aux formules de la forme $v \in_{\mathsf{vl}} v$. La condition apparemment peu naturelle $v \in_{\mathsf{vl}} v$ exprime en réalité que v est une variable. Une formule comme, par exemple, « w a exactement trois variables distinctes de u et v » s'exprime par une condition. En revanche, on prouve que « $w\ (v := v') = w\ (v := v'')$ », qui n'est pas une condition, ne peut pas non plus s'exprimer comme une condition.

Un *terme simple* est soit une variable, soit un terme de la forme $T\ (v := R)$, où v est une variable et T, R des termes simples.

Une *équation conditionnelle* est une formule de la forme $C \rightarrow T = S$, où C est une condition et T et S des termes simples.

Théorème 5.1. *Une équation conditionnelle est valide dans tout logos ssi elle est valide dans les logos de substitution.*

Démonstration. Une bijection F entre des ensembles finis de termes des logos $\mathcal{S}$ et $\mathcal{L}$ est un *isomorphisme partiel* entre $\mathcal{S}$ et $\mathcal{L}$ ssi

[2] En réalité il suffira pour la suite de supposer que les axiomes de logos justifient la définition de substitution simultanée et entraînent ces deux propriétés — qui s'obtiennent par des raisonnements équationnels. On pourrait donc à la limite s'épargner la peine de les démontrer en les insérant dans la définition même de logos.

– chaque variable d'un terme du domaine de F est dans le domaine de F, et chaque variable d'un terme de l'image de F est dans l'image de F ;
– $M \in \mathsf{vl}_{\mathcal{S}}(N)$ ssi $F(M) \in \mathsf{vl}_{\mathcal{L}}(F(N))$, pour M, N dans le domaine de F.

Par va-et-vient, on a $\mathcal{S} \models_\alpha C$ ssi $\mathcal{L} \models_\beta C$, pour toute condition C et isomorphisme partiel F tel que $\beta(v) = F(\alpha(v))$ — pour les v libres dans C — et dont le domaine inclut les images par α des variables libres de C.

Soit X un ensemble fini de termes d'un logos $\mathcal{L}$ incluant toutes leurs variables. À chaque terme M de X qui n'est pas une variable, on associe injectivement un symbole fonctionnel ϕ_M d'un logos de substitution $\mathcal{S}$ dont l'arité est le nombre de variables de M et on définit une bijection $\nu_{\ldots}$ entre les variables de X et un ensemble fini de variables de $\mathcal{S}$. Fixons un ordre strict $\prec$ sur les variables dans l'image de ν. Alors, la surjection F sur X définie par

$$F(\nu_x) = x\ ; \qquad F\big(\phi_M(\nu_{x_1}, \ldots, \nu_{x_n})\big) = M,$$

avec $\nu_{x_1} \prec \cdots \prec \nu_{x_n}$ et $\mathsf{vl}_{\mathcal{L}}(M) = \{x_1, \ldots, x_n\}$, est un isomorphisme partiel entre $\mathcal{S}$ et $\mathcal{L}$.

Comme les termes d'un logos de substitution ont une construction unique à partir des variables et des symboles fonctionnels, on peut — grâce à la propriété (1) — prolonger F en une fonction $\widehat{F}$ définie inductivement pour tous les termes de $\mathcal{S}$ contenant les ϕ_M et les variables dans l'image de ν :

$$\widehat{F}\big(\phi_M(M_1, \ldots, M_n)\big) = M\big[x_1 := \widehat{F}(M_1), \ldots, x_n := \widehat{F}(M_n)\big],$$

où $F(\phi_M(\nu_{x_1}, \ldots, \nu_{x_n})) = M$. En utilisant les axiomes 5 et 6 ainsi que la propriété (2), on montre par induction sur les termes de $\mathcal{S}$ que $\widehat{F}(M[\nu_y := N]) = \widehat{F}(M)[y := \widehat{F}(N)]$.

Supposons maintenant que l'équation conditionnelle $C \to U = V$ est valide dans $\mathcal{S}$ et soit β une valuation dans un logos $\mathcal{L}$ qui rend C vrai. Donnons-nous, comme ci-dessus, un isomorphisme partiel F entre un logos de substitution $\mathcal{S}$ et $\mathcal{L}$, dont l'image inclut l'image de β. Soit encore une valuation α dans $\mathcal{S}$ telle que $F(\alpha(v)) = \beta(v)$, pour les variables libres v de $C \to U = V$. On a vu que C est vrai dans $\mathcal{S}$ pour la valuation α. Par conséquent $\alpha(U) = \alpha(V)$. Il reste donc à vérifier que $\beta(U) = \beta(V)$. Pour cela nous montrons par induction que $\widehat{F}(\alpha(T)) = \beta(T)$, pour tout terme simple « engendré » par les variables libres de $C \to E$. En effet, dans le cas non trivial où $\alpha(v)$ est une variable de $\mathcal{S}$, nous obtenons :

$$\widehat{F}\big(\alpha(T(v := S))\big) = \widehat{F}\big(\alpha(T)\big[\alpha(v) := \alpha(S)\big]\big) = \widehat{F}\big(\alpha(T)\big[\nu_{\beta(v)} := \alpha(S)\big]\big) = \beta(T)\big[\beta(v) := \beta(S)\big]. \qquad \square$$

En adoptant la notation sans parenthèses, dite « polonaise », pour identifier un terme d'un logos de substitution à une suite finie de symboles fonctionnels et de variables, on obtient le

Corollaire 5.2. *Soit L^* le logos des suites finies sur un ensemble L incluant un ensemble infini de constantes. Une équation conditionnelle est valide dans L^* ssi elle valide dans tout logos.*

Remarquons que ce dernier résultat serait faux si L ne comportait que des variables. En effet en ce cas la « commutativité » v *est la seule variable de* u *et de* $u' \to u(v := u') = u'(v := u)$ serait valide dans L^*, mais non dans les logos de substitution.

Le théorème de complétude a pour conséquence pratique que si les termes d'un système formel forment un logos, on peut les traiter du point de vue de la substitution sans se préoccuper de leur structure interne ou tout simplement comme des termes de la logique du premier ordre.

Références

[1] M. Abadi, L. Cardelli, P.-L. Curien, J.-J. Lévy, Explicit substitutions, J. Funct. Programming 1 (1991) 375–416.
[2] M. Crabbé, Prelogic of logoi, Studia Logica 35 (1976) 219–226.