Actema : une interface graphique et gestuelle pour preuves formelles (démonstration)

Pablo Donato, Pierre-Yves Strub, Benjamin Werner

Actema : une interface graphique et gestuelle pour preuves formelles

Pablo Donato, Pierre-Yves Strub, and Benjamin Werner

LIX, École Polytechnique, France

Introduction

Le principe des systèmes de preuves interactifs est que l'utilisateur construit incrémentalement une preuve par une boucle d'interaction. On progresse à travers une séquence d'états, chacun correspondant à une preuve incomplète. Chacun de ces états est lui même composé d'un ensemble fini de *buts* ; la preuve est achevée lorsque cet ensemble de buts est vide.

Du point de vue de l'utilisateur, un but apparaît comme un séquent, tel que défini par Gentzen. C'est-à-dire, en logique intuitioniste :

— Une proposition A qu'il s'agit de prouver et qu'on peut appeler la *conclusion* du but ;
— un ensemble de propositions Γ décrivant les *hypothèses*.

L'utilisateur effectue des actions sur un but à la fois. Ces actions transforment le but, ou plus exactement remplacent le but par un ensemble de buts.

Dans le paradigme dominant, ces commandes sont textuelles. Depuis Robin Milner et LCFF [2], elles sont appelées des *tactiques*.

Le prototype que nous présentons propose de remplacer ces commandes textuelles par des actions effectuées sur une interface graphique. En ce sens, c'est une continuation du travail effectué sur le *Proof-by-Pointing* (PbP) initié dans les années 1990 par Gilles Kahn, Yves Bertot, Laurent Théry et leur équipe [1]. Dans les deux cas l'utilisateur effectue des actions sur les éléments *(items)* du but, à savoir sa conclusion et ses hypothèses. Une nouveauté de notre travail est que nous ne nous restreignons pas à des *click* sur des sous-expressions des éléments, mais autorisons d'autres actions, comme le glissé-déposé *(drag-and-drop)* d'un élément sur un autre. Ceci enrichit le langage des actions de manière, nous l'espérons, intuitive. Précisons qu'il ne s'agit pas de remplacer mais de compléter les actions PbP. Il s'agit donc d'aller vers un paradigme plus général de construction de preuves par actions.

Nous avons implémenté un petit prototype pour démontrer et expérimenter cette approche.

Disposition

Les caractéristiques que nous proposons devraient pouvoir être déclinées pour de nombreux formalismes logiques ; le prototype actuel implémente la logique du premier ordre intuitioniste avec support pour l'égalité.

Un avantage du paradigme des preuves-par-actions est qu'il permet une présentation très dépouillée de l'état de preuve ; un but apparaît comme un ensemble d'éléments dont la nature est définie par leur couleurs respectives :

— Un *élément rouge* qui porte la proposition devant être prouvée, c'est-à-dire la *conclusion*,
— des *éléments bleus*, qui sont les *hypothèses* locales.

Chaque but apparaît sur un onglet. Dans ces onglets, les éléments apparaissent donc comme des rectangles bleus ou rouges, munis chacun de la proposition de l'élément. Par défaut, la conclusion rouge est sur la droite et les hypothèses bleues sur la gauche ; voir la figure 1 pour un état possible.

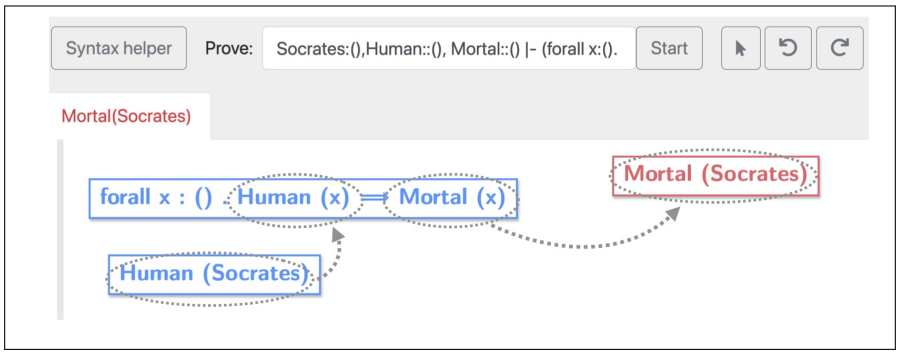

FIGURE 1 – Une capture partielle d'écran montrant le prototype. La conclusion est en rouge à droite, les deux hypothèses en bleu sur la gauche. Les flèches en pointillé ont été rajoutées pour indiquer deux actions de glisser-déposer possibles.

Les éléments sont ce sur quoi l'utilisateur peut agir : soit en cliquant sur l'un d'entre eux, soit en les déplaçant.

L'intuition sous-jacente au glisser-déposer est, nous l'espérons, relativement simple. Elle est basée sur la distinction entre éléments rouges et bleus, et souligne un point simple mais fondamental : même si la conclusion et les hypothèses sont exprimées dans le même langage logique, elles jouent des rôles distincts dans la preuve. Il y a même un symétrie à l'œuvre :

— la conclusion rouge A *attend* une justification de la validité de A ;
— en revanche, une hypothèse bleue B *fournit* une justification de la validité de B dans l'état courant.

Ceci se matérialise par l'instance la plus simple d'action drag-and-drop. Etant donné un but dont la conclusion est une proposition A, si ce but comporte également une hypothèse A, on peut déposer l'un de ces deux éléments sur l'autre, ce qui résout ce but. D'un point de vue logique, il s'agit là d'une utilisation de la règle axiome.

Une grande partie du travail consiste à généraliser cette idée à des situations plus complexes, tout en gardant un comportement intuitif. Sur le plan théorique, cela correspond à généraliser la règle axiome, et est très lié à l'approche d'inférence profonde. Comprendre ceci a permis de mieux définir le comportement du glisser-déposer. Remarquez que souvent, ces actions ne vont pas résoudre le but, mais transformer la conclusion courante. D'autres actions vont combiner deux hypothèses pour en faire apparaître une nouvelle. Dans le cas de la figure 1, il y a deux actions possibles :

— On peut déposer l'hypothèse du haut sur la conclusion, ce qui va transformer en Human(Socrates) (qui peut ensuite être prouvé en utilisant la seconde hypothèse).
— On peut déposer une des deux hypothèses sur l'autre, ce qui va engendrer une nouvelle hypothèse Mortal(Socrates).

Références

[1] Yves Bertot, Gilles Kahn, and Laurent Théry. Proof by pointing. In Masami Hagiya and John C. Mitchell, editors, *Theoretical Aspects of Computer Software*, volume 789, pages 141–160. Springer Berlin Heidelberg, 1994. Series Title : Lecture Notes in Computer Science.

[2] Robin Milner. The use of machines to assist in rigorous proof. *Philosophical Transactions of the Royal Society of London. Series A, Mathematical and Physical Sciences*, 312(1522) :411–422, 1984.