

Esquisse et contrôle
Pascale Sénéchaud
LACO Faculté des Sciences
123 Avenue Albert Thomas
87060 Limoges

Introduction

Nous reprenons ici un exemple de contrôle développé par Yves Ledru du L.S.R de Grenoble [Ledru 98]. Cet exemple a déjà fait l'objet d'un nombre d'articles important lors du congrès : "Approches Formelles dans l'Assistance au Développement de Logiciels" qui a eu lieu à Grenoble en janvier 2000 [AFADL'2000]. Ainsi, diverses techniques ont été illustrées sur ce même exemple.

Il ne s'agit pas là d'introduire simplement un autre cadre mais bien d'apporter un nouveau point de vue qui va permettre de modéliser jusqu'au contrôle et cela dans un unique formalisme.

C'est dans le but de modéliser ou au moins de définir proprement la notion de contrôle que cette présentation est faite. C'est aussi en partie pour cela que nous n'avons pas suivi l'organisation du cahier des charges proposée par Y.Ledru [Ledru 98]. Il faut souligner que l'effort de structuration de ce cahier des charges nous a énormément aidé dans le travail présenté ici.

Cette étude utilise des outils dérivés de la théorie des Esquisses dont on trouvera les fondements dans [Ehresmann 66] [Coppey & Lair 84], [Coppey & Lair 88] et les principales notions utilisées ici dans [Duval & Lair 99-1] et [Duval & Lair 00-2].

Nous prenons en compte l'évolution temporelle du système, ainsi notre système est dynamique. Nous structurons notre étude en quatre parties qui sont les suivantes :

- L'espace du système : Il s'agit là de toute la partie statique du système qui, d'un point de vue spécification ne présente aucune difficulté notable. La présentation à l'aide d'esquisses coïncide avec bien d'autres sur cette partie. Elle permet ici de se familiariser avec le formalisme des esquisses.
- L'instant du système : Nous présentons ici la partie instantanée c'est-à-dire que nous fixons le temps et nous décrivons alors le système. Beaucoup de composantes se comportent alors de la même façon aussi nous ne développerons que deux exemples significatifs : un voyant et le journal.
- L'évolution temporelle : Nous montrons ici comment, pour tenir compte de l'évolution temporelle du système tout en restant dans la même famille de structures, il est nécessaire de réfléchir différemment. La présentation faite ici pourrait être complétée : il existe en effet un moyen systématique de décrire l'évolution d'un système donné à partir de l'esquisse déterminée pour la partie instantanée. Cela se fait à l'aide de constructeurs de structures plus complexes dont les esquisses font partie [Duval & Lair 00-3] et [Duval & Lair 99-4].

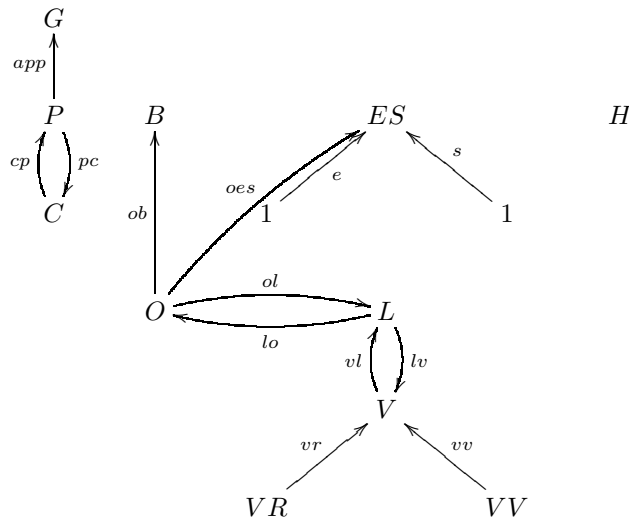
- Le contrôle : Que devient dans ce formalisme la notion essentielle de contrôle ? Nous en donnons ici une définition mathématique qui doit être vue comme un pas de plus dans la modélisation des systèmes contrôlés.

1 L'espace du système

Le système est composé d'un ensemble de bâtiments, d'un ensemble de personnes réparties en différents groupes et d'une horloge. Chaque bâtiment est équipé de portes qui ne peuvent servir qu'en entrée ou en sortie et d'un système de contrôle et de gestion des entrées-sorties (voyants, lecteurs de cartes...). La finalité du système est d'enregistrer les accès de manière à pouvoir les contrôler.

Chaque sommet dans l'esquisse que l'on va décrire aura une interprétation dans la catégorie des ensembles et chaque flèche sera interprétée comme une application entre ensembles.

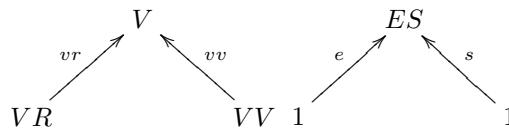
La construction de l'esquisse S_e donnée à l'issue de cette première partie se fait en deux temps : on construit d'abord une esquisse S_0 correspondant à la partie "matériel" du système puis on enrichit S_0 pour obtenir S_e qui tiendra compte du fait que l'on cherche à enregistrer les accès. Soit l'esquisse S_0 suivante :



avec les cônes projectifs distingués :

1

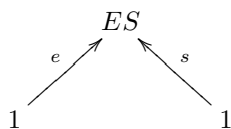
de base vide, et les cônes inductifs distingués :



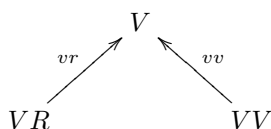
Le sommet P est interprété comme l'ensemble des personnes ayant accès aux bâtiments, le sommet G

comme l'ensemble des groupes, le sommet H comme celui des valeurs d'une horloge, le sommet B comme celui des bâtiments, le sommet O comme celui des portes et le sommet ES comme un ensemble à deux éléments permettant de préciser si une porte donnée est une entrée ou une sortie du bâtiment considéré.

Pour que le sommet ES soit effectivement interprété comme un ensemble à deux éléments on distingue dans l'esquisse S_0 le cône inductif de sommet ES et de base $(1, 1)$ suivant :



Les sommets L, C, V sont interprétés respectivement comme l'ensemble des lecteurs de cartes, l'ensemble des cartes et l'ensemble des voyants. Ce dernier étant exclusivement constitué des voyants verts et des voyants rouges, l'esquisse S_0 contient le cône inductif distingué suivant :



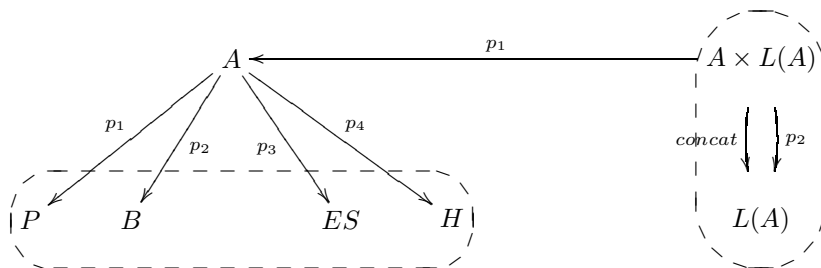
Dans cette esquisse le fait qu'une personne n'appartienne qu'à un seul groupe se traduit par la présence d'une flèche app de domaine P et de codomaine G . L'interprétation de app par n'importe quel modèle dans la catégorie des ensembles fournit une application de l'ensemble des personnes vers l'ensemble des groupes : ainsi à chaque personne est bien associée un et un seul groupe.

Les flèches de cette esquisse correspondent à certains faits décrits dans le cahier des charges d'Y.Ledru :

- la flèche ob représente l'appartenance d'une porte à un bâtiment (et non plusieurs),
- la flèche oes représente le fait qu'une porte est une sortie ou une entrée (et non des deux),
- les flèches lo et ol représentent l'association bijective entre les ouvertures et les lecteurs de cartes que l'on précise par les équations : $lo \circ ol \sim Id$ et $ol \circ lo \sim Id$,
- les flèches lv et vl représentent l'association bijective entre les voyants et les lecteurs de cartes que l'on précise par les équations : $lv \circ vl \sim Id$ et $vl \circ lv \sim Id$,
- les flèches cp et pc représentent l'association bijective entre les personnes et les cartes que l'on précise par les équations : $cp \circ pc \sim Id$ et $pc \circ cp \sim Id$.

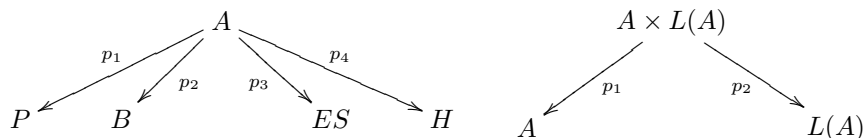
Enrichissons maintenant S_0 pour obtenir S_e :

L'idée de contrôle et de la gestion du système est d'avoir à sa disposition un enregistrement des accès. L'esquisse S_e est alors la suivante :



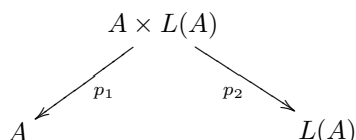
L'esquisse S_0 n'est pas toute représentée sur le graphe précédent : Seules apparaissent les parties ayant une utilité pour comprendre l'enrichissement fait ici. Ceci explique la présence des pointillés sur le graphe de S_e . Ce procédé sera réutilisé par la suite.

Les sommets rajoutés à l'esquisse S_0 sont les sommets A , $L(A)$ et $A \times L(A)$. Les cônes projectifs distingués de S_e sont ceux de S_0 et :



Si M est un modèle de l'esquisse S_e , c'est-à-dire un foncteur de S_e dans la catégorie des ensembles, le sommet A sera interprété comme l'ensemble $M(A)$ de tous les quadruplets d'éléments des ensembles $M(P)$, $M(B)$, $M(ES)$, $M(H)$.

En ce qui concerne $L(A)$, l'idée est de faire en sorte que si M est un modèle comme ci-dessus, $M(L(A))$ corresponde aux listes d'éléments de $M(A)$. Nous ne nous étendrons pas ici sur la manière d'obtenir cette propriété pour $L(A)$. En fait $L(A)$ n'est pas un simple sommet mais correspond au sommet "principal" d'une esquisse décrivant les listes d'éléments de $M(A)$ ce que l'on note dans l'esquisse S_e , par des pointillés. Nous ne verrons ici sur les listes que ce dont nous avons besoin à savoir le cône projectif distingué suivant :



et la flèche *concat* de domaine $A \times L(A)$ et de codomaine $L(A)$ permettant d'ajouter un élément à une liste.

Le sommet $L(A)$ est interprété comme un ensemble dont on peut voir les éléments comme les valeurs possibles d'un journal qui serait la liste des événements qui se sont produits. Bien évidemment, seules nous intéressent les valeurs correspondant aux événements qui se sont réalisés.

Tant que l'on décrit la partie statique, on reste au niveau d'une esquisse. Mais, même si l'on parle d'esquisse par la suite, il serait plus juste de travailler dans le type d'une esquisse [Duval & Reynaud 94-1], [Duval & Reynaud 94-2]. En effet nous allons utiliser des flèches qui ne sont pas dans l'esquisse à proprement parler mais qui existent forcément dans son type.

2 L'instant du système

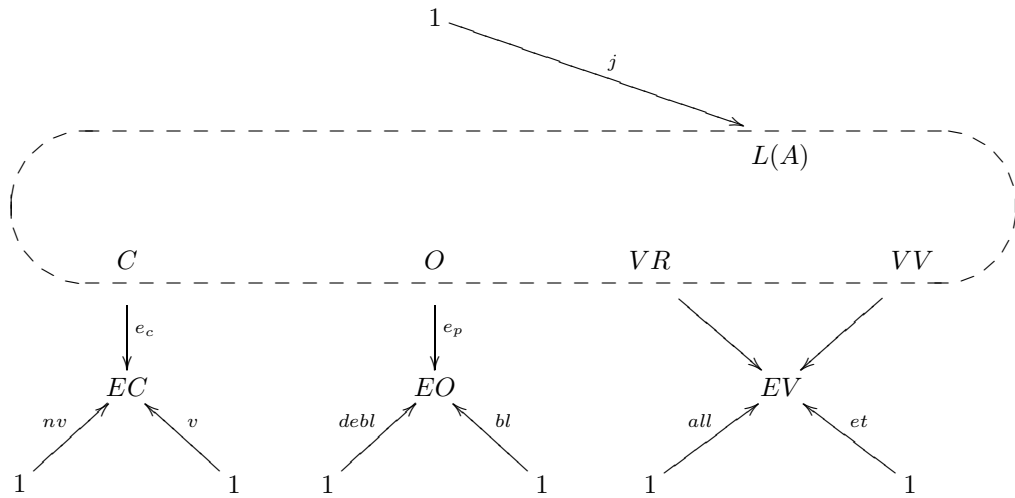
Nous décrivons ici la partie instantanée du système. Pour ce faire nous enrichissons l'esquisse S_e en une esquisse S_i . Nous voulons tenir compte des faits suivants :

Un voyant donné, peut être éteint ou allumé, une porte peut être bloquée ou débloquée, une carte peut être valide ou non valide.

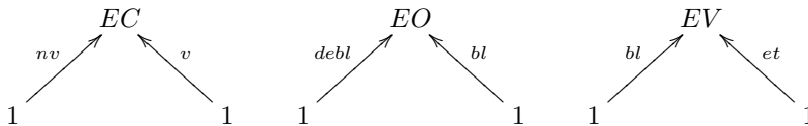
Certains sommets (seuls représentés ici) de l'esquisse S_e (ceux correspondants aux voyants, aux portes et aux cartes) vont alors être mis en relation, via des flèches supplémentaires dans l'esquisse S_i , à de nouveaux sommets ($E0, EV, EC$) représentant les "états" possibles décrits ci-dessus.

Par ailleurs la valeur du journal dont on parle à la fin du paragraphe précédent a une réalité instantanément d'où la présence de la flèche j dans l'esquisse S_i (nous y reviendrons plus tard). L'esquisse S_i

est décrite de la façon suivante :



avec les nouveaux cônes inductifs suivants :



l'interprétation des sommets EC , EO et EV étant respectivement $\{Valide, Nonvalide\}, \{Bloquee, Debloquee\}, \{Allume, Eteint\}$.

On peut déjà traduire certains faits du cahier des charges de Y. Ledru [Ledru 98].

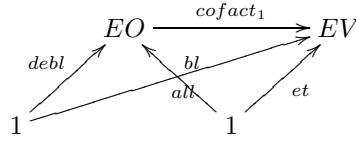
Par exemple : “Un voyant vert indique l'état bloqué ou débloqué de la porte” peut aussi se traduire par : “Si la porte est bloquée alors son voyant vert est éteint sinon il est allumé”.

Cette dernière phrase contient un “si”... “alors”... “sinon” qui se traduit par un terme dans le type de S_i , et montre la puissance des esquisses à cônes inductifs distingués [Duval & Reynaud 94-1], [Duval & Reynaud 94-2] :

On considère une porte P , qui correspond dans l'esquisse S_i à une flèche p de domaine 1 et de codomaine O car au niveau des modèles ensemblistes prendre une application d'un ensemble à un élément vers un ensemble X c'est exactement prendre un élément de X .

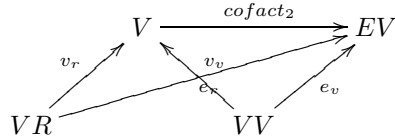
L'état de cette porte se lit par $e_p \circ p$, flèche de 1 dans EO . Pour dire “si la porte considérée est bloquée alors le voyant correspondant est éteint, sinon il est allumé”, on considère l'unique flèche $cofact_1$ de domaine EO et de codomaine EV telle que :

$cofact_1 \circ bl \sim et$ et $cofact_1 \circ debl \sim all$. On est assuré de l'existence et de l'unicité de $cofact_1$ par le fait que EO est le sommet d'un cône inductif distingué de base $(1, 1)$ et donc que pour tout autre cône de sommet X et de même base il existe une unique flèche qui fait commuter le diagramme suivant (ici $X = EV$):



En considérant la composée $cofact_1 \circ ep \circ p$ on a une flèche de 1 vers EV . Cette flèche correspond à l'état d'un voyant. Il suffit maintenant de dire qu'il s'agit de l'état du voyant vert associé à la porte choisie ; il faut donc récupérer la flèche représentant le voyant associé à P qui n'est autre que $lv \circ ol \circ p$ de 1 vers V . Si le voyant correspondant à cette dernière flèche est vert alors son état doit correspondre à $cofact_1 \circ ep \circ p$, ce qui fait appel à la structure inductive distinguée du cône de sommet V de base (VR, VV) .

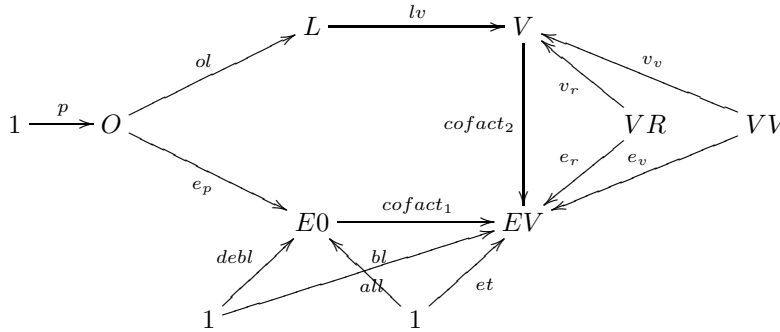
Autrement dit, il faut considérer l'unique flèche $cofact_2$ de domaine V et de codomaine EV telle que $cofact_2 \circ v_r \sim e_r$ et $cofact_2 \circ v_v \sim e_v$; on impose alors que le diagramme suivant commute :



Finalement dire la phrase "Si la porte est bloquée alors son voyant vert est éteint sinon il est allumé" se traduit dans l'esquisse S_i (ou plutôt dans son type) par l'équation :

$$cofact_1 \circ e_p \circ p \sim cofact_2 \circ lv \circ ol \circ p$$

avec dans S_i :



On écrit plutôt l'équation

$$cofact_1 \circ e_p \sim cofact_2 \circ lv \circ ol$$

car la flèche p y est superflue, ce qui correspond au fait que la propriété à décrire est vraie pour toutes les portes. Toutes les contraintes du cahier des charges concernant les états des composantes du système, sans modification d'états se traduisent avec des équations écrites à l'aide de termes de l'esquisse S_i . L'exemple ci-dessus est parmi les plus compliqués.

En dehors des "états" des composantes matérielles du système, la valeur du journal est également instantanée. La question que l'on peut se poser ici est : que nous permet de faire l'esquisse S_i , ou son type, au niveau du journal ?

On aurait ainsi fabriqué une flèche de 1 vers 1 qui ne serait pas l'identité.

Il faut donc passer à un niveau d'abstraction plus grand dès que l'on veut parler de la modification "d'états" ou de valeurs. Plus précisément, lorsque l'on cherche à prendre en compte un changement sur une valeur sans avoir une loi globale de changement qui porte sur l'ensemble des valeurs possibles. Dans le cas du journal, la modification de la valeur courante du journal ne s'écrit pas comme une flèche de $L(A)$ dans lui-même.

3 L'évolution temporelle

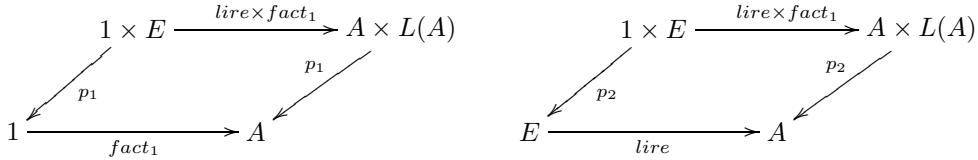
On va construire une esquisse dans laquelle nous allons pouvoir écrire les modifications temporelles du système. Nous la noterons S_t . Pour simplifier nous noterons de manière systématique le sommet du cône projectif distingué de base (X, Y) , $X \times Y$.

Pour pouvoir mettre à jour les valeurs du journal, on utilise un processus dû à C.Lair et D.Duval [Duval & Lair 00-3], [Duval & Lair 99-4]. Pour la compréhension de l'exemple nous resterons au niveau des esquisses, sachant qu'en fait à partir de S_i et d'une autre esquisse on pourrait construire de manière automatique l'esquisse S_t , dont l'entière connaissance est souvent superflue. Ici, d'ailleurs nous ne regarderons dans l'esquisse S_t que l'évolution du journal.

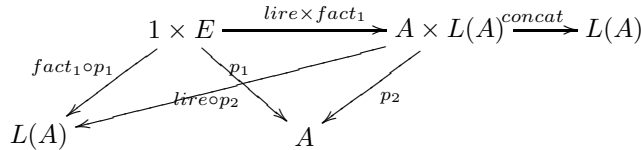
La manipulation du journal passe, jusqu'à présent par la connaissance de sa valeur. En fait que fait-on de cette valeur ? On veut essentiellement pouvoir la lire et la modifier.

Pour construire l'esquisse S_t on procède par enrichissement de S_i en supprimant la flèche j , qui ne sert plus. On introduit une nouvelle sorte E qui nous permettra un accès indirect sur le journal via une nouvelle flèche *lire* de domaine E et de codomaine $L(A)$. L'interprétation de E dans un modèle de S_t est alors l'ensemble des journaux possibles. Que devient alors la mise à jour du journal ?

On a toujours la flèche $fact_1$ de domaine 1 et de codomaine A qui correspond à l'événement à rajouter au journal. La nouvelle valeur du journal s'écrit : $concat \circ (lire \times fact_1)$ où l'on note $lire \times fact_1$ l'unique flèche de domaine $1 \times E$ et de codomaine $A \times L(A)$ telle que les diagrammes :

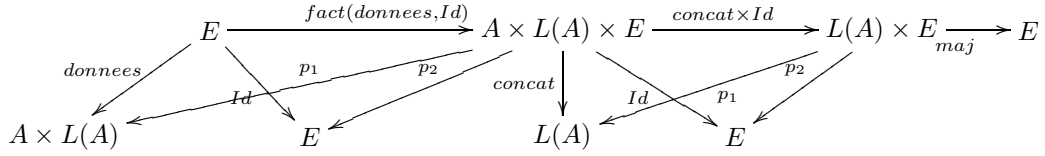


commutent. La situation peut se résumer par :



Le sommet $1 \times E$ correspond au sommet du cône projectif distingué de base $(1, E)$. Comme le sommet 1 correspond aux ensembles à un élément, il est suffisamment clair que le sommet E et $1 \times E$ auront des interprétations isomorphes : nous dirons donc que nous avons construit comme nouvelle valeur du journal une flèche de E vers $L(A)$, que nous notons $concat \circ donnees$. La flèche $lire \times fact_1$ correspond en effet aux données nécessaires à la construction de la nouvelle valeur du journal et la flèche $concat$ au traitement de ces données. Reste à faire la mise à jour. Nous introduisons pour cela une flèche notée maj de domaine $L(A) \times E$ et de codomaine E , permettant la mise à jour de E .

Finalement pour écrire la mise à jour du journal on a localement dans S_t :



où $fact(donnees, Id)$ est l'unique flèche de E dans $A \times L(A) \times E$ telles que $p_1 \circ fact(donnees, Id) \sim donnees$ et $p_2 \circ fact(donnees, Id) \sim Id$ et où $concat \times Id$ est celle telle que $p_1 \circ concat \times Id \sim concat$ et $p_2 \circ concat \times Id \sim Id$.

Avec l'équation : $lire \sim lire \circ maj \circ (concat \times Id) \circ fact(donnees, Id)$, en supposant que le journal est vide au départ.

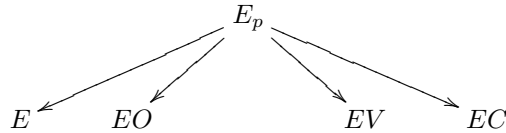
On pourra remarquer que la flèche maj comporte E dans son domaine, ce qui oblige à rajouter E en domaine et en codomaine du traitement, même si celui-ci n'apporte pas de modification sur E .

Pour l'état des voyants, comme pour celui des portes et des cartes, on aurait pu choisir de mettre dans S_t des flèches de changements d'états sur les sommets EV, EO, EC pour passer d'un état à l'autre.

4 Le contrôle

Le contrôle doit permettre la détection et la prévention des tentatives de fraudes. Typiquement on aimerait pouvoir écrire : "Si l'état de la carte lue est non-valide alors bloquer la porte", ou encore "si une personne est autorisée à entrer, vérifier dans le journal qu'elle est bien hors du bâtiment, si oui débloquer la porte, mettre à jour le journal, les voyants...".

Le contrôle est en fait une composée de flèches dans le type de l'esquisse S_t , mais elle engendre des modifications d'états des composantes aussi nous introduisons le sommet E_p dans S_t , et le cône projectif distingué suivant :



Ainsi E_p correspond à l'état global du système et nous définissons le contrôle comme un ensemble fini de flèches de domaine E_p et de codomaine E_p . Il semble alors que décrire les actions du contrôleur soit simplement de composer des flèches de domaine E_p et de codomaine E_p ce qui appartient au domaine de la syntaxe.

Conclusion

L'utilisation de la théorie des esquisses pour traiter l'exemple de contrôle d'accès permet une structuration du système mettant en évidence l'aspect dynamique de tels exemples. L'aspect nouveau est sans doute le fait que tout le système peut se décrire à l'intérieur d'une même structure sur laquelle nous avons des propriétés universelles depuis la partie statique jusqu'au contrôle. L'intérêt de cette présentation réside également en le fait qu'il n'est pas forcément nécessaire de construire tout S_t .

Je tiens à remercier D.Duval pour m'avoir suggéré cette étude et pour les relectures attentives de ce travail.

References

- [AFADL'2000] *Approches Formelles dans l'Assistance au Développements de Logiciels* Actes des Journées du 26 au 28 janvier 2000, LSR-IMAG, Grenoble 2000
- [Coppey & Lair 84] L. Coppey, C. Lair. *Leçons de théorie des esquisses (I)*. Diagrammes 12, Paris, 1984.
- [Coppey & Lair 88] L. Coppey, C. Lair. *Leçons de théorie des esquisses (II)*. Diagrammes 19, Paris, 1988.
- [Duval & Lair 99-1] D. Duval, C. Lair. *Skeches and specifications : Reference Manuel. First part : Compositive graphs* Rapport de recherche du LACO, 1999.
<http://www.unilim.fr/laco/rapports>
- [Duval & Lair 00-2] D. Duval, C. Lair. *Skeches and specifications : Reference Manuel. Second part : Projective sketches* Rapport de recherche du LACO, 2000.
<http://www.unilim.fr/laco/rapports>
- [Duval & Lair 00-3] D. Duval, C. Lair. *Skeches and specifications : User's guide. First part : Specifications by mosaics* Rapport de recherche du LACO, 2000.
<http://www.unilim.fr/laco/rapports>
- [Duval & Lair 99-4] D. Duval, C. Lair. *Skeches and specifications : User's Guide. Second part : Specifications in Kit form* Rapport de recherche du LACO, 1999.
<http://www.unilim.fr/laco/rapports>
- [Duval & Reynaud 94-1] D. Duval, J.-C. Reynaud. *Sketches and Computation - I basic definition and static evaluation* Mathematical Structures for Computer Science, vol 4 pp 185-238, 1994
- [Duval & Reynaud 94-2] D. Duval, J.-C. Reynaud. *Sketches and Computation- II dynamic evaluation and applications* Mathematical Structures for Computer Science, vol 4 pp 239-271, 1994
- [Ehresmann 66] C.Ehresmann. *Introduction to the theory of structured categories* Technical Report 10, University of Kansas at Lawrence, 1966
- [Ledru 98] Y. Ledru, G. Padiou, J. Jaray. *Présentation d'un banc d'essai pour l'évaluation des méthodes formelles basé sur l'étude de cas du contrôle d'accès* 1998
http://www.lsr.images//Les.Personnes/Yves.Ledru/Controle_acces