HAL
open science

# Action Miró/Mirho

Luigi Liquori, Dominique Colnet, Joelle Despeyroux

## To cite this version:

Luigi Liquori, Dominique Colnet, Joelle Despeyroux. Action Miró/Mirho. 2001. hal-01151339

**HAL Id: hal-01151339**

**https://inria.hal.science/hal-01151339v1**

Submitted on 13 May 2015

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

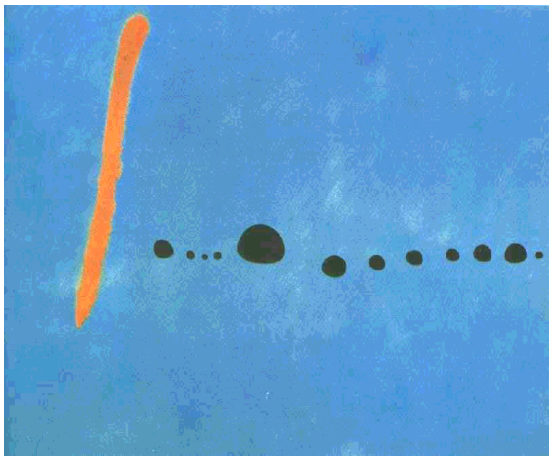
# *Action Miró*

*Systèmes à Objets, Types et Prototypes :*

*Sémantique et Validation*

*INRIA Lorraine et INRIA Sophia Antipolis*

THÈME 2A



Version 1.3, Juillet 2002

# Table des matières

**1 Composition de l'équipe** **3**

**2 Présentation et objectifs généraux** **3**
2.1 Pourquoi Miró . . . 3
2.2 Objectifs généraux de Miró . . . 3
2.3 Guide de lecture . . . 4

**3 Contexte (ou Fondements scientifiques)** **4**
3.1 Introduction . . . 4
3.2 Les langages, calculs et systèmes à objets . . . 5
3.2.1 Le langage Eiffel et le compilateur SmallEiffel . . . 5
3.2.2 Le principe d'analyse globale et spécialisation des méthodes vivantes . . . 5
3.2.3 Implantation de la liaison dynamique par sélection dichotomique . . . 8
3.2.4 Les calculs à prototypes et leurs systèmes de types . . . 8
3.2.5 Fonctions *vs.* objets : un conflit sans cause . . . 9
3.3 La construction de logiciel certifié . . . 10
3.3.1 Formalisation des objets à travers la réécriture d'ordre supérieur . . . 10
3.3.2 La théorie de types . . . 11
3.3.3 Le logiciel certifié . . . 12
3.3.4 Les assistants à la preuve . . . 13
3.3.5 Méthodes de spécification dans les assistants à la preuve . . . 14

**4 Acquis des membres de l'action** **15**
4.1 Certification de logiciel et théories typées . . . 15
4.2 Techniques de compilation efficace . . . 17
4.3 Qualité et optimisation du code dans les programmes Java . . . 17
4.4 Lambda-calcul, calculs à objets et types . . . 18

**5 Programme de recherche** **18**
5.1 Introduction . . . 18
5.2 FunTalk et SmallTalk2K . . . 18
5.2.1 Les caractéristiques du langage FunTalk/SmallTalk2K . . . 19
5.2.2 Phase formelle de conception de FunTalk/SmallTalk2K . . . 20
5.2.3 Phase de conception et d'implantation . . . 21
5.3 Eiffel et SmallEiffel . . . 21
5.3.1 Match-O, un dialecte d'Eiffel probablement sûr . . . 21
5.3.2 Amélioration de l'analyse globale . . . 23
5.3.3 Couplage avec des techniques d'analyse dynamique . . . 23
5.3.4 Généralisation à des systèmes non figés . . . 24
5.3.5 L'évolution du langage Eiffel . . . 24
5.4 Réécriture, types et preuves . . . 25
5.4.1 Le Rho-calcul typé . . . 25
5.4.2 Les systèmes de types purs avec motifs . . . 25

5.4.3 Les théories typées et les calculs formels . . . . . 26
5.4.4 Les preuves formelles . . . . . 27
5.5 Le système d'exploitation Isaac . . . . . 27
5.5.1 Le système d'exploitation Isaac . . . . . 28
5.5.2 Le langage Lisaac . . . . . 28
5.6 Récapitulatif et programme de travail . . . . . 29

**6 Domaines d'applications 30**
6.1 Introduction . . . . . 30
6.2 Électronique embarquée . . . . . 31
6.2.1 PDA et PDA-OS . . . . . 31
6.2.2 Systèmes d'exploitation . . . . . 31
6.3 Télécommunications . . . . . 32

**7 Positionnement pas rapport aux autres projets 33**
7.1 Miró et l'INRIA . . . . . 33
7.2 Miró et l'INRIA-Lorraine . . . . . 33
7.3 Miró et l'INRIA-Sophia . . . . . 34
7.4 Miró et l'INRIA\{Lorraine, Sophia} . . . . . 35
7.5 Miró et les autres groupes en France . . . . . 36
7.6 Miró et l'Europe . . . . . 37
7.7 Miró et les États-Unis et le Canada . . . . . 37

**8 Logiciels 38**
8.1 SmallEiffel : The GNU Eiffel Compiler . . . . . 38
8.2 FunTalk / SmallTalk2K . . . . . 39
8.3 Isaac / Lisaac . . . . . 39

**9 Actions régionales, nationales et internationales 40**
9.1 Équipes associées à l'étranger 2001-2002 . . . . . 40
9.2 Projets européens . . . . . 40
9.3 Action QSL (CPER) . . . . . 40
9.4 Groupes de recherches (GDR) . . . . . 41
9.5 Accueils de chercheurs . . . . . 41

**10 Diffusion de résultats 41**
10.1 Miró en "Tour de France" . . . . . 41
10.2 Enseignement . . . . . 41
10.3 Thèses et stages . . . . . 42
10.4 Administration de la recherche . . . . . 42

**11 Bibliographie 43**

*Miró est un projet commun à l'INRIA Lorraine & Sophia Antipolis et à l'Université Nancy 2.*

# 1 Composition de l'équipe

**Responsable scientifique**
Luigi Liquori [CR INRIA Lorraine]
**Responsables permanents**
Dominique Colnet [Professeur, Université Nancy 2]
Joëlle Despeyroux [CR INRIA Sophia Antipolis]
**Personnel Inria**
Olivier Zendra [CR INRIA Lorraine]
**Ingénieurs experts**
Philippe Ribet [Ingénieur expert INRIA, 6/2001-6/2003]
Jérôme Boutet [Ingénieur associé INRIA, 7/2002-7/2003]
**Chercheurs doctorants**
Alberto Ciaffaglione [Co-tutelle INPL-Univ. Udine, 3/2001-10/2002]
Benoît Sonntag [Doctorant INRIA, 10/2002]
**Collaborateurs extérieurs**
André Hirschowitz [Professeur, Université de Nice-Sophia]
Furio Honsell [*Ad Honorem*, Président des Universités de Udine, Italie]
**Assistantes de projet**
Nathalie Bellesso [INRIA Sophia Antipolis, à temps partiel]
Laurence Benini ou Sophie Drouot [INRIA Lorraine, à temps partiel]

# 2 Présentation et objectifs généraux

## 2.1 Pourquoi Miró

Johachim Miró [227] est, à notre humble avis, un grand peintre *à objets* ; en fait, ses tableaux de la période 1940-1960 sont basés sur l'utilisation de nombreux objets géométriques : points, points colorés, carrés, cercles, fenêtres, lignes, courbes, etc. Tous ces éléments sont très chers aux amateurs de la programmation par objets. On peut même aller jusqu'à imaginer que ce peintre, qui s'est installé en France à Montmartre au début des années 50, a certainement inspiré les concepteurs de Simula, de SmallTalk, et la communauté d'informaticiens qui ont étudié les aspects théoriques du paradigme à objets.

## 2.2 Objectifs généraux de Miró

Les langages à objets ont acquis une importance prépondérante dans les applications informatiques à grande échelle. Cette utilisation a rendu nécessaire l'étude formelle de ces langages pour à la fois mieux en cerner les caractéristiques fondamentales et aussi pour pouvoir définir de nouveaux langages à objets et concurrents, capables de combiner une plus grande expressivité avec une sécurité et efficacité d'utilisation.

L'action explore la possibilité de "concilier" la programmation à objets et la programmation fonctionnelle, tout en gardant l'esprit de l'une et l'élégance mathématique de l'autre, et s'intéresse à la certification des outils développés autour de ces langages (interprètes, compilateurs, ...), avec comme assistant à la preuve privilégié le système Coq.

En complément de ces axes de recherche principaux, nous étudions des théories typées, dans la recherche de nouveaux systèmes améliorant l'activité de la preuve formelle, et dans la compilation efficace des langages de programmation à objets.

Notre programme de recherche se focalise essentiellement sur les axes suivants :

1. l'étude, la définition et l'implantation certifiée d'un langage de programmation à classes (et de son compilateur) , appelé *SmallTalk2K*, et d'un langage à prototypes (*c.à.d.* à objets purs), appelé *FunTalk* (et d'un interprète et d'un compilateur), langage intermédiaire du compilateur de SmallTalk2K ;
2. l'étude de l'efficacité et de la sûreté des langages à objets et notamment d'*Eiffel* (et ses évolutions) et de son compilateur *SmallEiffel* ;
3. l'étude de systèmes de types pour les langages à objets et pour les assistants de preuves ; la réécriture et les calculs formels ($\lambda, \varsigma, \rho, \pi, \ldots$) comme base des langages de programmation à objets, fonctionnels et concurrents ;
4. l'étude du système d'exploitation *Isaac* et de son langage propriétaire à prototypes *Lisaac*.

### 2.3 Guide de lecture

La structure du document est la suivante : la section 3 présente les fondements scientifiques, la section 4 les acquis de l'action. La section 5 présente le programme de recherche détaillé. La section 6 passe en revue les différents domaines d'application. La section 7 place Miró dans le contexte national, international et de l'INRIA en particulier. La section 8 présente les logiciels développés ou en cours de développement. La section 9 présente les actions régionales, nationales et internationales. La section 10 présente la diffusion des résultats au sein de la communauté scientifique. La lecture du présent document ne nécessite aucun pré-requis.

**N.B.** Suite à l'expertise de J. Despeyroux en tant que relectrice de l'action Miró, l'action Certilab de l'INRIA Sophia Antipolis a fusionné avec Miró le 14 janvier 2002. Miró est donc devenu une action bi-localisée entre Nancy et Sophia Antipolis.

## 3 Contexte (ou Fondements scientifiques)

### 3.1 Introduction

Cette section présente les fondements scientifiques de Miró, le langage à objets Eiffel et son compilateur GNU SmallEiffel, les calculs à objets purs, dits *à prototypes*, les systèmes d'exploitations (à objets), les calculs de réécriture, et notamment le Rho-calcul, l'interaction entre les langages à objets et les langages fonctionnels, la théorie des types, les preuves formelles, ainsi que les assistants à la preuve.

## 3.2 Les langages, calculs et systèmes à objets

### 3.2.1 Le langage Eiffel et le compilateur SmallEiffel

Eiffel concrétise une certaine idée du développement de logiciels, qui repose sur le fait qu'il peut être effectué comme un ouvrage d'ingénieur, ayant pour but d'atteindre un certain niveau de qualité logicielle, au terme d'un processus rigoureux de production et d'enrichissement de composants réutilisables, scientifiquement spécifiés, paramétrables, et communiquant sur la base de contrats clairement définis et organisés selon des classifications multi-critères systématiques.

Si la notion de classe en programmation à objets trouve sa raison d'être dans une implantation des types de données abstraits, il ne suffit pas qu'une classe soit connue au travers des seules opérations qui lui sont applicables, mais aussi au travers les propriétés formelles de ces opérations. En Eiffel, le rôle des *assertions* est multiple : elles aident à produire du code correct et robuste, favorisent une documentation de haut niveau, fournissent un support de mise au point et servent de base au traitement des exceptions. L'action Miró focalise sa recherche sur Eiffel, dans le cadre du développement du compilateur *SmallEiffel*.

### 3.2.2 Le principe d'analyse globale et spécialisation des méthodes vivantes

**Analyse globale.** Le fait de considérer le programme dans son ensemble (*whole system analysis*) par opposition à la compilation séparée.

Afin de *spécialiser* l'ensemble du programme, *c.à.d.* générer du code adapté autant que possible au contexte spécifique au programme compilé [102], l'équipe Miró s'intéresse souvent (dans le cadre du compilateur SmallEiffel) à une *approche globale* au système. Dans ce cas on peux s'appuyer sur des algorithmes d'analyse globale, de prédiction de type et d'expansion en ligne (*inlining*) puissants [106, 160, 36, 57, 80].

L'*analyse globale* consiste à rassembler des informations sur l'ensemble du système compilé. Ceci va à l'encontre des pratiques actuellement les plus courantes pour la compilation des langages à objets, qui reposent sur la compilation séparée de fichiers sources indépendants, dont le principal inconvénient est qu'elle rend l'optimisation globale plus difficile. En effet, la compilation séparée est souvent considérée comme la seule technique permettant des (re)compilations rapides, grâce à son incrémentalité intrinsèque. Elle est de plus bien adaptée à l'utilisation de bibliothèques logicielles du marché fournies sans leur code source et intégrées lors de l'édition de liens. En revanche, son principal inconvénient est qu'elle ne permet d'optimiser que *localement*, à l'échelle du fichier source compilé. Elle ne permet ainsi pas de prendre en compte dans l'optimisation les fichiers et bibliothèques déjà compilés. L'analyse globale se focalise sur l'optimisation du système dans son ensemble. Elle a pour but de permettre au compilateur de préciser le *contexte* dans lequel chaque élément du code source (expression, instruction, variable, méthode, etc.) va être compilé. Ceci permet de passer de la génération d'un code le plus général possible à la production de code plus spécialisé, et donc potentiellement plus efficace. Afin d'avoir une analyse globale aussi rapide que possible, il est important de ne pas compiler tout le code source accessible (y compris dans les bibliothèques) sans discrimination, mais seulement le code indispensable au système, *c.à.d.* le code *vivant* de ce système.

En Eiffel, le point de départ d'un programme, appelé la *racine* de l'application, est spécifié par une paire composée d'une classe initiale et de l'une de ses procédures de création. La première étape du processus d'analyse statique globale calcule quelles parties du code source Eiffel sont *vivantes* (accessibles depuis la racine) ou *mortes* (inaccessibles). Ceci peux s'effectuer pour (comme *e.g.* en SmallEiffel) de façon totalement statique, *c.à.d.* sans analyse de flot. Le résultat de ce premier calcul est donc indépendant de l'ordre des instructions dans le programme.

Le processus de calcul du code vivant ainsi que de l'ensemble des types vivants est à la fois récursif et itératif. La récursivité est utilisée pour suivre le graphe d'appel de l'application. Le processus est répété itérativement en partant des méthodes vivantes de chaque type vivant jusqu'à être capable d'effectuer une itération complète sans ajouter ni nouveau type vivant ni nouvelle méthode vivante.

Par exemple en SmallEiffel, l'algorithme actuel de calcul du code vivant, même s'il donne des résultats plus qu'acceptables, n'est pas parfait. Par exemple, pour un appel `foo.bar`, lorsque le type statique `foo` de `foo` ne fait pas partie des types vivants, on ne devrait pas considérer la définition de `bar` dans ce type comme vivante car, dans certains cas, ce code peut amener l'algorithme à considérer à tort qu'un autre type est vivant. Cette constatation fait apparaître un besoin criant de pouvoir *garantir* que le calcul du code vivant est correct (et décidable avec une complexité acceptable). Une veine de recherche importante dans ce domaine est de formaliser le processus de calcul du code vivant dans le but de converger vers un implantation approchant plus précisément la partie réellement vivante de l'application.

La *spécialisation automatique du code* en fonction du type du receveur est un point essentiel dans la stratégie de compilation de SmallEiffel [109]. Cette spécialisation consiste en quelque sorte à essayer de dérouler avant l'exécution le mécanisme de liaison dynamique, ce qui peut être considéré comme une forme d'évaluation partielle.

La figure 1 montre comment la méthode `display`, définie dans la classe FRUIT, héritée dans les classes PEACH et APPLE, est automatiquement spécialisée lors de la traduction en code C. En effet, comme le prédicat `stone_fruit` prend la valeur vrai, dans la classe PEACH et la valeur faux dans la classe APPLE, l'expression conditionnelle est toujours vraie dans la classe PEACH et toujours fausse dans la classe APPLE. Ainsi, il ne subsiste aucune trace de l'expression conditionnelle au niveau du code généré. En outre, dans le véritable code généré par SmallEiffel, l'argument `Current` (`self` de SmallTalk ou `this` de Java) des fonctions `PEACHdisplay` et `APPLEdisplay`, destiné à référencer le receveur, est supprimé car non utilisé dans le code spécialisé.

Ainsi, toutes les méthodes vivantes d'un type vivant sont également spécialisées. En raison de la duplication-spécialisation du code dans tous les types vivants, la pseudo variable `Current` a toujours un seul et unique type dynamique, le type vivant dans lequel cette méthode est spécialisée. Tous les appels concernant `Current` sont donc des appels directs ne nécessitant *jamais* de code de liaison dynamique. Le receveur étant en général l'objet le plus utilisé dans une méthode, cette optimisation concerne une très grande partie des envois de messages. Pour cette raison, les scores d'inférence de type atteignent des niveaux très élevés ($\sim 90\%$).

Contrairement à ce que l'on pourrait craindre, cette technique de duplication-spécialisation des méthodes n'entraîne pas d'augmentation importante de la taille des exécutables. En fait, les exécutables produits par SmallEiffel sont souvent plus petits que ceux produits par les compilateurs du commerce, voire plus petits que les exécutables obtenus à partir de classes

```
deferred class FRUIT                                  1
feature
  stone_fruit : BOOLEAN is deferred end;
  display is
    do
      if stone_fruit then
        io.put_string("It is a stone fruit.%N");
      else
        io.put_string("It may be an apple.%N");
      end;
    end;
end
```

```
class PEACH                                           2
inherit FRUIT;
feature
  stone_fruit : BOOLEAN is true;
end
```

```
class APPLE                                           3
inherit FRUIT;
feature
  stone_fruit : BOOLEAN is false;
end
```

```
PEACHdisplay(PEACH* Current) {                        4
  printf("It is a stone fruit.\n"); }
```

```
APPLEdisplay(APPLE* Current) {                        5
  printf("It may be an apple.\n"); }
```

FIG. 1 – Spécialisation du code généré pour la méthode `display` définie dans la classe FRUIT. Les cadres **1**, **2** et **3** correspondent respectivement au source Eiffel des classes FRUIT, PEACH et APPLE. Les cadres **4** et **5** montrent le code C généré pour les classes PEACH et APPLE.

C++ (cf. par exemple [106]). Ceci est dû en partie au fait que la spécialisation des méthodes tend à élaguer du code, comme dans l'exemple de la figure 1.

De plus, l'implantation de la liaison dynamique à l'aide de code de sélection dichotomique (*Binary Tree Dispatch*) permet le remplacement direct (*inlining*) de nombreuses méthodes. En particulier, toutes les fonctions d'écriture et de lecture d'attributs ne sont jamais ni appelées, ni même définies [160].

La technique de duplication-spécialisation est particulièrement bien adaptée à un contexte d'analyse globale où l'on ne considère que le code vivant. En particulier, le fait de travailler sur un système fermé permet de spécialiser le code de toutes les *classes feuilles*, les classes sans sous-classes dans le système fermé. Plus généralement, on appelle un *type feuille* un type vivant sans sous-type vivant dans le système fermé. Du point de vue spécialisation de code, le fait que le type d'une expression soit un type feuille n'est pas sans importance : comme dans le cas de `Current`, un envoi de message appliqué sur une expression dont le type est un type feuille correspond à un appel direct, sans liaison dynamique. La seule différence entre `Current` et une expression de type feuille consiste à envisager également le cas où l'expression ne référence aucun objet lors de l'exécution (`Void`).

```
if ( typeId < 3 )
   then
      if ( typeId < 2 ) then specialized code for type #1
                        else specialized code for type #2
      endif
   else
      if ( typeId < 4 ) then specialized code for type #3
                        else specialized code for type #4
      endif
endif
```

FIG. 2 – Le code généré pour implanter la liaison dynamique avec sélection dichotomique.

### 3.2.3 Implantation de la liaison dynamique par sélection dichotomique

La connaissance de l'ensemble des types vivants offre d'importantes possibilités d'optimisations du code généré. Une des plus remarquables optimisations réalisée dans le cadre du compilateur SmallEiffel a consisté à implanter la liaison dynamique en générant du code de sélection dichotomique. Tous les types vivants étant connus, on associe statiquement à chacun de ces types un identifiant entier qui sert d'indicateur à l'exécution. La détermination du type dynamique de l'objet receveur est réalisée par du code de sélection dichotomique comme présenté à la figure 2.

Le principal avantage de cette technique est d'éviter l'utilisation de tableaux de pointeurs de fonctions, *Virtual Function Tables* (VFT), comme en C++ par exemple. En outre, il est souvent possible de remplacer un appel de fonction par le code qui lui correspond (*inlining*) au cœur même du code de sélection dichotomique (voir [160]).

### 3.2.4 Les calculs à prototypes et leurs systèmes de types

Parmi les langages à objets, les langages à prototypes [20] (ou langages à délégation) constituent un axe de recherche important de l'action Miró ; en particulier, on s'intéresse souvent aux aspects théoriques de ces langages, notamment aux *calculs à objets*, calculs où la création des nouveaux objets est déléguée aux objets eux-mêmes (calculs à délégation ou *delegation-based*). Ces calculs sont très importants pour fournir des sémantiques opérationnelles, dénotationnelles, et des systèmes de types sophistiqués pour les langages à objets.

Le *Lambda Calcul des Objets (LCO)* défini par Fisher, Honsell et Mitchell [65] à l'université de Stanford, et le *Calcul à Objets (OC)* défini par Abadi et Cardelli [1] au Centre de Recherche Digital de Palo Alto en sont les principaux représentants. En particulier, les aspects de typage et d'implantation des dits calculs ont été développés dans [143, 144, 129, 120, 90, 141, 183, 87, 139, 43, 47].

Dans les calculs à objets purs, les objets sont définis directement à partir d'autres objets, en utilisant ces derniers comme prototypes. Les seules opérations sur les objets sont l'extension d'un objet avec une variable ou une méthode (*object extension*), et la surcharge d'une variable ou d'une méthode (*object overriding*). L'objet modifié hérite de toutes les propriétés

du prototype. Plusieurs modèles fonctionnels et impératifs avec différents systèmes de typage ont été présentés dans les dernières années [148, 38, 82, 81, 83, 84, 37, 1, 151, 71, 28, 65, 122, 89, 213, 153, 88, 93, 154, 123, 124, 125].

Les calculs LCO et OC conduisent à divers systèmes de types qui empêchent statiquement l'erreur `message-not-found` à l'exécution, qui apparaît quand un objet reçoit un message qui n'est pas présent dans son interface. Les systèmes de types pour LCO et OC sont très puissants : en particulier ils permettent la *mytype method specialization*, *c.à.d.* la possibilité de spécialiser les types des méthodes héritées (une telle possibilité est déjà offerte par le langage Eiffel, avec le type `like Current`, qui malheureusement a un système de types qui ne prévient pas statiquement l'erreur `message-not-found`). Avec le calcul à prototypes on peut modéliser des langages comme Self [158], Obliq [51], Kevo [192], Emerald [73], Cecil [171], et Omega [42].

Les langages à prototypes (et ses calculs sous-jacents) peuvent aussi être utilisés en tant que "langages cibles" pour implanter et étudier des propriétés formelles des langages à classes, puisque les classes peuvent être vues comme des objets capables de recevoir le message `new` de création d'un objet.

### 3.2.5 Fonctions *vs.* objets : un conflit sans cause

**Mots clés** : Self, O-Haskell, Claire, ML2000, Moby, Obliq, OCaml, Eiffel.

**Glossaire :**

**Self.** Langage à objets où tout est objet (pas de classe, rien que des objets) [158].

**O-Haskell.** Version à objets de Haskell [211, 32], qui est un langage fonctionnel pur, *c.à.d.* sans la possibilité d'avoir accès à la représentation interne des structures en mémoire (pas d'effet de bord).

**Claire.** Langage fonctionnel, logique et à objets développé chez Bouygues Telecom par Y. Caseau et F. Laburthe [101].

**ML2000.** Nouvelle définition du langage ML. Il contient en *built-in* la notion d'objets et de *type objet* [220].

**Moby.** Langage de programmation à prototypes en cours de développement chez AT & T [206, 123, 125].

**Obliq.** Langage de programmation à prototype développé chez Digital/Compaq. Ce langage est conçu pour la mobilité du code [51].

**OCaml.** Langage fonctionnel et à objets développé dans le projet INRIA Cristal [218].

**Eiffel.** Langage à base de classes statiquement typé intégrant depuis peu certains paradigmes habituellement réservés aux langages purement fonctionnels (fermeture et évaluation partielle).

Les langages à objets sont quasi universellement considérés comme intrinsèquement impératifs : en fait ils ont une notion d'état, *c.à.d.* de variables propres à chaque instance d'objet. Néanmoins :

- une grande partie de la littérature scientifique sur la théorie des langages à objets a été développée au travers de petits langages à objets fonctionnels purs (voir par exemple, à ce sujet, le papier sur *Featherweight Java* de A. Igarashi, B. Pierce et P. Wadler [134]) ;

– des concepts comme l'héritage, la liaison dynamique, l'envoi de message, la surcharge de méthodes et l'extension dynamique des objets ne sont pas du tout en contradiction avec le paradigme fonctionnel lui même.

L'un des objectifs de Miró consiste à explorer la possibilité de "concilier" le monde objet et le monde fonctionnel, tout en gardant l'esprit de l'un et l'élégance mathématique de l'autre.

## 3.3 La construction de logiciel certifié

Une partie de nos recherches concerne la certification de logiciel. Nous nous intéressons notamment à la spécification des langages de programmation et aux preuves de propriétés de langages (dont deux exemples typiques sont la preuve de conservation des types d'un langage lors de son exécution, et la preuve de correction d'un compilateur). Nous travaillons dans ce domaine à différents niveaux (théorie et pratique) et en suivant différentes approches.

### 3.3.1 Formalisation des objets à travers la réécriture d'ordre supérieur

**Mots clés** : Lambda-calcul, Rho-calcul, sémantique, théorie de types.

**Glossaire :**

**Rho-calcul.** Calcul de réécriture d'ordre supérieur [26, 103, 104].

Le Rho-calcul peut être utilisé pour formaliser et intégrer le paradigme à objets et la réécriture. Le Rho-calcul intègre les propriétés complémentaires de la réécriture du premier ordre et du Lambda-calcul ainsi que des caractéristiques permettant d'exprimer le non-déterminisme. Ce calcul est suffisamment puissant pour décrire non seulement la réécriture avec des règles conditionnelles mais aussi leur contrôle. Ainsi, le Rho-calcul permet la description des langages basés sur la réécriture. La syntaxe du Rho-calcul est très simple :

$$\begin{array}{rcll} t & ::= & a \mid X \mid t \to t \mid t \bullet t \mid & \text{termes simples} \\ & & null \mid t, t & \text{séquences} \end{array}$$

où $a$ dénote une constante, $X$ dénote une variable, $t \to t$ une fonction, $t \bullet t$ une application, $null$ dénote une séquence vide, et $t, t$ une séquence. Dans le Rho-calcul, l'application est une opération décrite au même niveau du calcul que l'abstraction, *c.à.d.* les règles de réécriture. On obtient ainsi un calcul similaire au Lambda-calcul avec motifs de S. P. Jones [22] où l'abstraction est faite non seulement par rapport à une variable mais en considérant aussi le contexte de la variable.

Le Rho-calcul peut être employé pour donner une sémantique à l'application des règles du langage Elan [91], un environnement de programmation et de prototypage reposant sur la logique de réécriture associée à la notion de stratégie. Le Rho-calcul est également un excellent candidat pour étudier l'expression du paradigme à objets dans un calcul de réécriture ; en fait, l'interprétation dénotationnelle de l'appel d'une méthode $m$ sur un objet $obj$ dans la programmation à objet (Kamin [138]) peut être simplement représentée en Rho-calcul en terme de filtrage et application. La figure 3 présente, par exemple, le codage en Rho-calcul d'un simple objet $Point$ et d'une simple classe $PointClass$ [1] (on présente soit un codage fonctionnel, soit un codage impératif, grâce au $\rho$-term $kill_m$, qui sélectionne une méthode dans l'objet et l'élimine).

$$
\begin{array}{rcl}
Point & \triangleq & val \to S \to v(1\ 1), \\
 & & get \to S \to S.val, \\
 & & set \to S \to v(X\ Y) \to (S.val := S' \to v(X\ Y)) \\
PClass & \triangleq & new \to S \to (val \to S' \to (S.preval)\bullet S', \\
 & & \qquad get \to S' \to (S.preget)\bullet S', \\
 & & \qquad set \to S' \to (S.preset)\bullet S'), \\
 & & preval \to S \to S' \to v(1\ 1), \\
 & & preget \to S \to S' \to S'.val, \\
 & & preset \to S \to S' \to v(X\ Y) \to (S'.val := S'' \to v(X\ Y)) \\
 & \text{où} & \\
obj.m & \triangleq & obj\bullet m\bullet obj \quad \text{Kamin } \textit{self-application} \\
(a.m := b) & \triangleq & (m \to b, a) \ \textit{update} \text{ fonctionnel} \\
(a.m := b) & \triangleq & (m \to b, kill_m\bullet a) \ \textit{update} \text{ impératif grâce à } kill_m \\
kill_m & \triangleq & (X, m \to Z, Y) \to X, Y \\
 & \text{et} & \\
PClass.new & \mapsto\!\!\!\!\to & Point
\end{array}
$$

FIG. 3 – Codage d'un objet *Point* et d'une classe *PointClass* en Rho-calcul [1].

### 3.3.2 La théorie de types

**Mots clés** : Théories typées, Calcul des Constructions (co-)Inductives.

**Glossaire :**

**Calcul des Constructions (CC).** Système de types dépendants, polymorphes et d'ordre supérieur pour le $\lambda$-calcul, introduit par T. Coquand et G. Huet [58]. Ce système, étendu avec les types (co-)inductifs (ICC) [35], constitue le noyau du système Coq.

Les théories typées, grâce à l'isomorphisme de Curry-Howard, [68] fournissent une base théorique aux assistants à la preuve. Suivant cet isomorphisme, une propriété à démontrer est spécifiée par un type et une démonstration de cette propriété devient un $\lambda$-terme (*c.à.d.* un programme fonctionnel) ayant ce type. On voit que la puissance d'expression de la théorie choisie a une grande influence sur le niveau d'abstraction avec lequel l'utilisateur pourra exprimer la propriété à prouver, comme sur la facilité (ou la difficulté !) qu'il aura à faire sa preuve. Ces dernières années ont vu différentes tentatives pour enrichir les théories typées connues, par l'ajout de modules, de sous-typage, de types inductifs, de types quotients et même de types objets. L'un des axes de recherche courants est la recherche de nouvelles théories typées permettant la récursion sur des termes de type fonctionnel.

### 3.3.3 Le logiciel certifié

**Mots clés** : Preuves formelles, logiciel certifié.

> *Les logiciels sont de plus en plus complexes. Hier encore, un logiciel représentait quelques milliers de lignes de code, tandis qu'aujourd'hui de façon courante ces produits en nécessitent plusieurs millions, ce qui entraîne une quantité plus importante d'erreurs de programmation. Une étude menée par le National Institute of Standards and Technology évalue à 60 milliards de dollars par an le coût des bogues informatiques, dont 22 milliards de dollars pourraient être évités si l'industrie informatique améliorait ses équipements de test des logiciels. Dans ce secteur qui emploie 700 000 ingénieurs et dont le chiffre d'affaires atteint 180 milliards de dollars, les développeurs consacrent environ 80% de leurs dépenses à identifier et à corriger des erreurs de programmation, mais cela ne suffit pas à empêcher la multiplication des bogues [226].*

Dans le domaine du logiciel certifié, on distingue en général la validation d'outils généraux pour les langages de programmation (tels que des interpréteurs, ou des compilateurs) de la validation des programmes eux-mêmes.

Dans le premier cas, on parle de *preuve de propriétés de langages*. Deux exemples typiques de ce domaine sont la preuve de conservation de types d'un langage lors de son exécution, et la preuve de correction d'un compilateur. La première propriété assure une certaine cohérence entre le système de vérification de type et les règles d'évaluation d'un langage. Ce type de preuve, essentiel pour les concepteurs du langage, donne par ailleurs au programmeur une certaine confiance dans les outils qu'il utilise.

La *preuve de correction de programmes* consiste généralement à prouver certaines propriétés d'un programme, par exemple la validité d'un invariant. Cependant, dans le cas idéal où l'on peut extraire un programme à partir de sa spécification, la preuve de correction de programmes devient *programmation certifiée*. À l'intersection des deux domaines, on trouve la certification d'un interpréteur, ou d'un compilateur.

Plus généralement, les compétences sur les preuves formelles intéressent potentiellement l'ensemble des domaines industriels où la présence d'erreurs même minimes dans les programmes peut avoir des conséquences graves : danger pour la vie humaine comme dans l'énergie nucléaire ou les transports (avions, automobiles), la chirurgie assistée par ordinateur, ou simplement coût prohibitif comme dans le commerce électronique et les réseaux de télécommunication, l'aérospatial, les *SoC, i.e. Systems on Chips*, les cartes à puces ou bien dans les domaines où les enjeux financiers sont importants comme le domaine bancaire. Tous ces domaines ont besoin de *logiciels certifiés*.

De nombreuses équipes de recherche mettent au point des techniques qui permettent de développer des logiciels validés vis-à-vis de spécifications, ce qui permettrait "théoriquement" de réduire le risque d'erreur à zéro (en "pratique" des erreurs peuvent également se glisser dans les spécifications). Ces techniques sont plus ou moins coûteuses et plus ou moins générales. Avec le logiciel Coq, fondé sur une théorie typée du Calcul des Constructions (co-)Inductives, on se trouve à un bout du spectre : on peut aborder des problèmes variés et complexes mais

avec un coût de développement plus important que d'habitude[1]. Il est donc intéressant de diminuer ce coût, d'une part par la recherche de théories typées et de méthodes de formalisation permettant des spécifications et des preuves plus concises, d'autre part par le développement de bibliothèques d'exemples.

### 3.3.4 Les assistants à la preuve

**Mots clés** : Coq, PCoq, PVS, Isabelle, HOL, Twelf.

**Glossaire :**

**Coq.** Assistant à la preuve fondé sur le Calcul des Constructions (co-)Inductives [178].

**PCoq.** Interfaces graphiques pour Coq permettant le *proof by pointing c.à.d.* utiliser la structure des formules logiques pour aider l'utilisateur à effectuer les étapes du raisonnement en les désignant à la souris [167, 182].

**PVS.** Assistant à la preuve disposant de stratégies de développement de preuve automatiques pour le model-checking [191].

**Isabelle.** Assistant de preuves fondé sur la logique d'ordre supérieur [72, 21] permettant des preuves plus courtes que le système Coq grâce à la réécriture et à l'unification d'ordre supérieur. Puisque la meta-logique d'Isabelle est nettement moins expressive que celle de Coq, les preuves Coq les plus abstraites ne peuvent pas s'exprimer dans Isabelle.

**HOL.** Assistant de preuves fondé aussi sur la logique d'ordre supérieur [188].

**Twelf.** Assistant de preuves qui utilise la syntaxe abstraite d'ordre supérieur et le principe d'induction [193].

Les assistants à la preuve sont très utilisés ces dernières années pour essayer de démontrer des propriétés très difficiles comme, par exemple, la normalisation forte d'un calcul ou la conservation de types pour un langage de programmation. Depuis peu, on s'intéresse aussi à la production de *logiciels sûrs*. Dans ce domaine, les systèmes basés sur une théorie typée vérifiant l'isomorphisme de Curry-Howard sont non seulement *a priori* les plus fiables (puisque leurs fondements sont connus), mais aussi les plus puissants, en terme d'expressivité. Dans le cas où l'on peut extraire un programme à partir de sa spécification, la preuve de correction de programme devient *programmation certifiée*. La spécification d'un langage de programmation se prête bien à être formalisée à l'aide de propriétés mathématiques directement transposables dans les démonstrateurs de théorèmes. La preuve de correction d'un compilateur (qui est lui-même un logiciel) représente un exemple typique de l'utilité des démonstrateurs de théorèmes.

Parmi les assistants à la preuve, l'un des plus prometteurs semble être le système Coq : avec son système de types basé sur les types (co-)inductifs, il permet la spécification des langages (exprimés à l'aide des grammaires inductives) et de leurs systèmes de types. Avec Coq, ont été développées récemment beaucoup de bibliothèques : la preuve des propriétés des programmes impératifs, la modélisation de la *scope extrusion* dans le $\pi$-calcul, ainsi que la normalisation forte d'une restriction de Coq lui-même (voir le papier "*Coq in Coq*" de B. Barras [166], une sorte de mini-bootstrap du système lui même), etc.

Le système PCoq, interface homme machine dédiée au système Coq, développée dans le projet Lemme permet le *proof by pointing*, *c.à.d.* que l'environment utilise la structure des

[1] Les techniques de *Model Checking* sont à l'autre bout du spectre.

formules logiques pour aider systématiquement l'utilisateur à effectuer les étapes de base du raisonnement en les désignant à la souris. Une autre interface pour Coq est proofGeneral [195] développée au LFCS d'Edinburgh.

Pour résumer, notre intérêt sera focalisé :

- sur les aspects théoriques, voire fondateurs, de ces outils [103, 104, 76, 114, 113, 75] ;
- sur les aspects d'utilisation de ces outils, car l'un des objectifs principaux de Miró est la construction d'un interprète et d'un compilateur sûr et certifié, pour un langage à objets.

### 3.3.5 Méthodes de spécification dans les assistants à la preuve

Aussi surprenant que cela puisse paraître, il n'y a toujours pas de consensus sur le choix de la représentation des variables dans un langage fonctionnel. On dispose à l'heure actuelle de plusieurs familles de méthodes pour décrire les variables et leur manipulation, *c.à.d.* essentiellement la substitution, à $\alpha$-conversion près (un terme est défini modulo le renommage de ses variables). L'action Miró expérimente toutes ces méthodes sur différents langages dans le système Coq.

La technique la plus connue est celle des indices de N. de Bruijn. Les variables sont implémentées par des entiers, représentant leur profondeur dans le terme, le nombre de liaisons entre leur occurrence et la racine du terme. Par exemple, les termes $\lambda x.x$ et $\lambda x.\lambda y.x$ seront respectivement représentés par les termes $(lam\ 0)$ et $(lam\ (lam\ 1))$. Les termes sont bien définis à $\alpha$-conversion près, mais ces termes étant eux-mêmes déjà illisibles, les spécifications le sont naturellement aussi, d'autant plus qu'un tel terme doit être complètement ré-écrit lorsqu'il est plongé dans un autre terme (les entiers doivent tous être décalés) ! Ce problème rend les preuves arbitrairement compliquées. Dans la plupart des cas, les trois quarts du développement concernent la manipulation des indices de N. de Bruijn, et non la sémantique elle-même.

La preuve de la propriété de conservation de types (simples) pour un $\pi$-calcul polyadique semble déjà déraisonnable, sinon impossible, dans cette approche. Cette technique, encore très utilisée, paraît donc hautement inadaptée à la formalisation des langages de programmation. Cependant, il existe un cas où l'utilisation des indices de N. de Bruijn est tout à fait indiquée : le cas du *bootstrap* d'un langage implémenté en utilisant ces indices. C'est le cas de la formalisation de "*Coq in Coq*", réalisée par B. Barras.

G. Gillard a exploré une technique due à A. Gordon [131]. Cette méthode, implémentée dans le système HOL, consiste à spécifier les termes à $\alpha$-conversion près, sur une syntaxe utilisant des indices de N. de Bruijn (qui disparaissent dans la syntaxe finale). La méthode semble permettre des spécifications relativement proches de ce que l'on écrit sur le papier, une fois prouvé un ensemble de lemmes sur les spécifications contenant des indices de N. de Bruijn.

J. McKinna et R. Pollack [147, 159] utilisent pour spécifier des règles de typage une technique de premier ordre intéressante qui distingue les variables libres (formalisées par des *paramètres*) des variables liées (formalisées par des *variables*). Les descriptions sémantiques renomment judicieusement les variables d'un terme en paramètres avant tout traitement des sous-termes, pour effectuer la substitution inverse à la fin du traitement, évitant ainsi le problème de "capture de variable". Leur approche nous semble être aujourd'hui l'une des meilleures.

Ainsi, il ne peut pas y avoir de phénomène de capture de variable lors d'une substitution (l'introduction d'une variable déjà liée dans un terme nécessite normalement son *renommage*

préalable pour éviter toute capture de variable libre). J. McKinna et R. Pollack ont ainsi formalisé "*Lego in Lego*" [187, 33] (Lego et Coq sont des systèmes très voisins).

Enfin, il existe une méthode qui permet d'utiliser directement les fonctions du système choisi (Coq par exemple) pour formaliser les notions de variables liées et de substitution du langage à décrire. On appelle ce type de description une spécification d'ordre supérieur. L'idée de base de la méthode est de représenter les variables du langage spécifié (le langage dit "objet") par les variables du langage utilisé pour spécifier (le langage dit "méta"). Ainsi, un constructeur d'un langage $L$ sera défini par des déclarations du type : $lam : (L \Rightarrow L) \Rightarrow L$. Le fils d'un nœud $lam$ est ici une fonction (méta). Cette technique permet souvent les descriptions et les preuves les plus concises et les plus élégantes.

Cette technique permet également de formaliser les *side conditions* (variables libres dans une hypothèse) et les changements de contexte (déchargement d'une hypothèse en déduction naturelle) dans les règles d'inférence. Elle fournit souvent la description la plus concise et la plus élégante d'un langage. De plus, par voie de conséquence, les preuves sont aussi grandement facilitées. Dans cette approche, on économise même la preuve du lemme de substitution, cœur techniquement difficile, commun à toutes les preuves de propriétés d'un langage fonctionnel. L'utilisateur peut se concentrer sur les difficultés de son langage, sans devoir ré-implémenter les fonctions que le système a déjà implémentées pour lui.

Le problème est que les schémas de récurrence et les principes d'induction usuels ne s'appliquent pas aux termes définis en suivant cette approche. La solution à long terme passe par la conception d'une nouvelle théorie typée. La solution à court terme consiste à inventer de nouvelles méthodes de description des langages dans les systèmes existants. J. Despeyroux a proposé différentes solutions, en suivant ces deux voies (voir section 4).

Pour conclure sur ces différentes méthodes de description des liaisons dans les langages de programmation, la méthode due à J. McKinna et R. Pollack nous semble aujourd'hui la meilleure pour décrire un langage fonctionnel en l'absence d'un système permettant l'utilisation conjointe de la syntaxe abstraite d'ordre supérieur et de l'induction. La technique de spécification d'ordre supérieur est la plus abstraite, la plus élégante ; c'est celle que nous préférerons toujours chaque fois que ce sera possible. Cette technique ne nous semble pas encore avoir fait ses preuves pour les langages impératifs, bien qu'il existe plusieurs expériences dans ces langages. Cependant la recherche est encore active sur ce sujet, que nous avons inclus dans nos objectifs de recherche. Ceci dit, cette méthode ne sera vraiment fiable que lorsque l'on disposera d'un système de type dans lequel les principes de récursion et d'induction sur des termes de type fonctionnel (termes usuels dans les spécifications à l'ordre supérieur) pourront être formalisés (et prouvés corrects). Enfin, A. Pitts [66] a introduit récemment une méthode du premier ordre, consistant à formaliser les variables à $\alpha$-conversion près, qui semble intéressante, et que nous devrons tester.

# 4 Acquis des membres de l'action

## 4.1 Certification de logiciel et théories typées

Le domaine de recherche de J. Despeyroux concerne la certification de logiciel. J. Despeyroux s'est intéressé notamment à la spécification des langages de programmation et aux

preuves de propriétés de langages (dont deux exemples typiques sont la preuve de conservation de types d'un langage lors de son exécution, et la preuve de correction d'un compilateur). Elle travaille dans ce domaine à différents niveaux (théorie et pratique) et en suivant différentes approches. Après une thèse (1982) dans le domaine des types abstraits algébriques, J. Despeyroux a participé, entre 1983 et 1987, à l'élaboration de la Sémantique Naturelle (issue de la la Sémantique Opérationnelle Structurelle de G. Plotkin) en étudiant les preuves de traduction dans cette approche [118]. À cette époque, elle faisait des preuves "sur papier". De 1988 à 1991, elle a développé son propre système d'assistant à la preuve (nommé Théo). Depuis, elle préfère utiliser des systèmes d'assistant à la preuve développés par d'autres.

En 1992, J. Despeyroux a découvert le grand intérêt des spécifications dites "d'ordre supérieur", qui utilisent une méthode proposée par, notamment, G. Plotkin et F. Pfenning. Aussi surprenant que cela puisse paraître, il n'y a toujours pas de consensus sur le choix de la représentation des variables dans un langage fonctionnel. Les spécifications utilisant les indices de N. de Bruijn (technique la plus connue) sont souvent illisibles et les preuves selon cette approche arbitrairement compliquées. À l'opposé, les méthodes dites "d'ordre supérieur" consistent à utiliser directement les fonctions du système choisi (le Calcul des Constructions et le système Coq par exemple) pour formaliser les notions de variables liées et de substitution du langage à décrire.

Cette approche à l'ordre supérieur permet des spécifications et des preuves concises, claires et élégantes (dans lesquelles les termes dépendants de variables sont représentés comme des fonctions de ces variables). Malheureusement, les principes d'induction et de récursion connus à l'époque ne s'appliquaient pas aux structures (termes de type fonctionnel) utilisées dans cette approche. Pour attaquer ce problème, ouvert depuis 1986 et réputé difficile, J. Despeyroux a travaillé dans deux directions complémentaires.

D'une part, en collaboration avec A. Hirschowitz [114] puis avec A. Felty (U. Ottawa) [113] J. Despeyroux a proposé deux nouvelles méthodes de spécification d'ordre supérieur, permettant d'utiliser l'induction classique proposée, par exemple, dans le système Coq. L'idée maîtresse de ces méthodes, qui a été reprise dans la définition de nouvelles théories typées, est de considérer un terme ouvert, dépendant d'une liste de variables, comme une fonction de cette liste de variables. Les termes "valides" sont définis par un prédicat. Dans la première méthode (la plus intéressante), les sémantiques sont données sur les termes valides, qui sont des termes fonctionnels.

D'autre part, dans un premier pas vers la définition d'un système de type qui incorpore la méthodologie du système LF (*Logical Framework* développé à Edimbourg) dans des systèmes comme Coq et en collaboration avec F. Pfenning (CMU) et C. Schürmann (Yale) [117, 75] puis avec un doctorant, P. Leleu [60, 115, 61], J. Despeyroux a proposé récemment plusieurs systèmes permettant la récursion sur des termes de type fonctionnel. Ces systèmes sont des $\lambda$-calculs modaux étendus avec des opérateurs de raisonnement par cas et d'itération préservant l'adéquation des représentations fonctionnelles (*i.e.* représentations utilisant la syntaxe abstraite d'ordre supérieur).

Ces systèmes ont toutes les propriétés souhaitées : préservation du typage par la réduction, confluence, normalisation forte de la réduction et extension conservative par rapport au $\lambda$-calcul simplement typé. L'un de ces systèmes a été étendu aux types dépendants, sans l'élimination forte [116].

J. Despeyroux a réalisé l'étude de nombreux exemples sur de petits langages impératifs (Imp de Winskel) [176] ou applicatifs classiques (Mini-ML) [118, 105, 114] sur papier en 1986, en machine depuis, principalement dans le système Coq. Ces exemples sont repris dans des notes de cours rédigées pour le DEA MDFI de Marseille [176]. Depuis 1997, elle participe à la formalisation de différents calculs concurrents ou/et à objets, en suivant différentes approches (d'ordre supérieur ou non). Ces études ont été, et sont réalisées dans le cadre de stages d'été et d'une thèse de doctorat (Guillaume Gillard). J. Despeyroux a proposé récemment une spécification originale du $\pi$-calcul [119].

## 4.2 Techniques de compilation efficace

Le compilateur SmallEiffel [18, 106, 79] [160, 107], démarré en 1994 par D. Colnet, a donné lieu en 1995 à la première diffusion dans le domaine public d'un prototype de compilateur Eiffel gratuit. Depuis 1995, ce compilateur est utilisé par les étudiants de la licence d'informatique de l'U.H.P. Nancy 1 ainsi que par les élèves de l'ESIAL. Depuis sa création, SmallEiffel en est à sa $26^{ème}$ version et ne cesse de s'améliorer et de se diffuser au plan international.

La distribution actuelle de SmallEiffel comporte : un traducteur Eiffel vers ANSI-C, un traducteur Eiffel vers la machine virtuelle Java (*JVM bytecode*), un indenteur de programme, un extracteur d'interfaces paramétrable (HTML, TEX, etc.), une bibliothèque de base richement garnie ainsi qu'un bon nombre d'outils supplémentaires comme par exemple un dé-compilateur de *bytecode* Java.

Grâce à la technique originale d'inférence de types développée, plus de 80% des appels des méthodes sont couramment liés statiquement (la vitesse d'un exécutable Eiffel est comparable à celle d'un programme écrit en C++ ou en C).

De par sa qualité reconnue au plan international, SmallEiffel a été promu logiciel GNU par R. Stallman, auteur d' `Emacs` et `gcc`, président fondateur de la FSF (*Free Software Foundation*), qui nous a fait l'honneur de venir nous rencontrer au LORIA afin de concrétiser le label GNU. Ainsi, depuis janvier 1998, SmallEiffel est officiellement *SmallEiffel, The GNU Eiffel Compiler*.

Le résultat principal des recherches effectuées dans le cadre de la thèse de doctorat d'O. Zendra [36] a été le développement et la diffusion du compilateur SmallEiffel. Intégrant les techniques d'optimisation développées dans la thèse d'O. Zendra, SmallEiffel produit un code d'excellente qualité, dont les performances sont en général supérieures (voire très supérieures) à celles des autres compilateurs Eiffel disponibles dans le commerce.

## 4.3 Qualité et optimisation du code dans les programmes Java

Récemment, O. Zendra a mené des recherches consistant à étudier les interactions entre logiciels et matériel afin d'optimiser au mieux des programmes écrits dans des langages à objets. Ces recherches se focalisent plus particulièrement sur l'optimisation des programmes Java et les interactions entre JVM et processeur [228, 163]. Le langage Java s'impose depuis plusieurs années avec une très grande rapidité, dans toutes les couches de l'industrie. Il rencontre cependant certains problèmes, notamment de lenteur. Cette voie de recherche a pour but d'étudier et d'améliorer les optimisations de code effectuées par les compilateurs, afin de permettre aux développeurs informatiques de produire des programmes (traitements de texte,

tableurs, navigateurs Internet, outils multimédia, contrôleurs embarqués, etc.) plus rapides, moins gourmands en mémoire et plus sûrs.

### 4.4 Lambda-calcul, calculs à objets et types

Les compétences de L. Liquori qui pourront être utiles à l'action Miró sont une (petite) connaissance du lambda-calcul, ses systèmes de types (dépendants, polymorphe et d'ordre supérieur) et ses logiques sous-jacentes via l'hysomorphisme de Curry-Howard, les calculs à objets purs (à la LCO, OC) et leurs systèmes de types, les systèmes de réécriture et en particulier le Rho-calcul ainsi que quelques connaissances dans le domaine des télécommunications grâce à son expérience chez Telecom Italia Labs (97-98) et a ses cours à l'École des Mines de Nancy (99-02).

## 5 Programme de recherche

### 5.1 Introduction

Notre programme de recherche se focalise essentiellement sur les axes suivants :

1. l'étude, la définition et l'implantation certifiée d'un langage de programmation à classes (et de son compilateur) , appelé *SmallTalk2K*, et d'un langage à prototypes (*c.à.d.* à objets purs), appelé *FunTalk* (et d'un interprète et d'un compilateur), langage intermédiaire du compilateur de SmallTalk2K ;
2. l'étude de l'efficacité et de la sûreté des langages à objets et notamment d'*Eiffel* (et ses évolutions) et de son compilateur *SmallEiffel* ;
3. l'étude de systèmes de types pour les langages à objets et pour les assistants de preuves ; la réécriture et les calculs formels ($\lambda, \varsigma, \rho, \pi, \ldots$) comme base des langages de programmation à objets, fonctionnels et concurrents ;
4. l'étude du système d'exploitation *Isaac* et de son langage propriétaire à prototypes *Lisaac*.

### 5.2 FunTalk et SmallTalk2K

**Mots clés** : SmallTalk, FunTalk, Eiffel, Self, LCO, OC.

**Participants** : Alberto Ciaffaglione, Joëlle Despeyroux, Luigi Liquori, Olivier Zendra.

Nous avons pour objectif de définir un nouveau langage à objets inspiré à la fois du langage Eiffel pour ce qui concerne les aspects génie logiciel, et des langages à prototypes pour ce qui concerne les aspects formels. En outre, les aspects dynamiques du langage SmallTalk nous semblent appropriés pour augmenter l'expressivité du langage.

Il est bien connu que le langage SmallTalk a été le premier espace de travail ou *système* complètement orienté vers les objets. SmallTalk était plus qu'un langage puisqu'il avait déjà un environnement composé d'un *Browser de classes* (pour "naviguer" dans les bibliothèques), un *Workspace* (pour tester les applications), et un *Debugger*, eux-mêmes écrits en SmallTalk !

Beaucoup de concepts de SmallTalk ont été repris dans d'autres langages comme Java, C++ et Eiffel, par exemple. Malheureusement et heureusement, cela dépend du point de vue suivant lequel on se place, le langage SmallTalk est un langage interprété, donc lent, mais aussi très expressif, car il n'est pas typé. Il est largement utilisé dans les projets où la vitesse d'exécution n'est pas cruciale comme, par exemple, dans le prototypage d'applications.

Depuis plus d'une dizaine d'années, plusieurs équipes ont essayé de trouver un système de typage sûr pour SmallTalk sans trop restreindre l'expressivité du langage. Dans la théorie de types, on connaît très bien les équations :

- langages typés : pas expressifs mais sûrs ;
- langages non typés : très expressifs mais pas sûrs.

### 5.2.1 Les caractéristiques du langage FunTalk/SmallTalk2K

L'absence de typage statique confère une très grande expressivité au langage SmallTalk : il permet la création dynamique de classes et la définition réflexive du système. On souhaite conserver une grande partie de l'expressivité de SmallTalk dans le langage SmallTalk2K. Bien sûr, le système de types que nous allons définir a pour objectif de rejeter statiquement certains *mauvais* programmes (voir *e.g.* celui de la figure 4, écrit en Eiffel). Notre objectif consiste à conserver les acquis des langages Eiffel et SmallTalk avec un système de typage sûr.

Puisque le système de types sera fortement inspiré du travail de recherche sur les langages à prototypes, on pourra par exemple ajouter la modification dynamique des instances comme dans les langages à délégations (comme par exemple le langage Beta [15] qui est une sorte de langage hybride à classes et à objets). Cette possibilité permettra, par exemple, d'écrire en SmallTalk2K l'affectation suivante (on utilise une syntaxe à la Java et on suppose l'existence d'une simple classe `POINT`) :

```
point = new POINT(2,4);
point.set(int dx,int dy) = {new body pour set};
point.set(3,5);
```

Cela correspond à changer dynamiquement le comportement d'une seule instance de la classe `POINT` qui, après l'affectation de `set`, aura un comportement pour la méthode `set` *différent* de toutes les autres instances de `POINT`. Une telle caractéristique est déjà présente dans des langages à prototypes comme Self par exemple, et a été récemment explorée dans le cadre du langage Java [112].

Nos objectifs ici sont de concevoir la sémantique et un compilateur d'un langage *intermédiaire* à prototypes, fortement typé, appelé FunTalk. La définition de SmallTalk2K pourra être exprimée à travers ce langage. Un programme écrit en SmallTalk2K pourrait être pré-compilé vers un programme en FunTalk équivalent en utilisant, par exemple, les transformations en *continuation passing style (CPS)* [190, 224] ou une capture "brutale" de la pile.

Le langage SmallTalk2K pouvant être vu comme une couche à classes au dessus du langage bas niveau à prototypes FunTalk, nous envisageons la possibilité de rendre disponible dans SmallTalk2K quelques primitives propres au langage FunTalk (par exemple la modification ou l'extension dynamique des méthodes dans un objet, *c.à.d.* dans une instance de classe). La sémantique statique et dynamique de FunTalk pourra être inspirée des calculs à prototypes

OC et LCO en version impérative. Dans ce cas, l'efficacité d'exécution du code compilé n'est pas un problème, mais la définition sémantique du langage devient beaucoup plus compliquée. On formalisera la mémoire avec des techniques standard.

### 5.2.2 Phase formelle de conception de FunTalk/SmallTalk2K

La phase formelle de la construction d'un langage (avec son interprète et compilateur) sûr et certifié est un objectif très ambitieux.

On prévoit les étapes suivantes :

- étude des langages OCaml, Haskell, Obliq, Self, Beta, Kevo, Emerald, Cecil, Moby, ainsi que des calculs $O_1, O_2, O_3$ basées sur OC [1], et LCO [65] (à la base de Moby) ;
- description d'une syntaxe, d'une sémantique opérationnelle (*small-step*) et d'une sémantique naturelle (*big step*) avec stratégie d'évaluation pour le langage FunTalk ;
- description d'un système de types pour FunTalk inspiré des systèmes de types pour les calculs LCO et OC. Ce système devra prévoir la *mytype method specialisation*, *c.à.d.* le `like Current` d'Eiffel, une solide notion de *subtyping* et/ou *matching* [96, 9, 84] et la possibilité de typer statiquement les méthodes binaires ;
- démonstration du théorème de préservation des types (*subject reduction*) et de complétude (*type soundness*), *c.à.d.* respecter le slogan de Milner *"well-typed programs cannot go wrong"*, pour FunTalk ; l'expérience acquise avec le Lambda-calcul, le Rho-calcul, les calculs LCO et OC et leurs systèmes de types sera très utile dans cette phase ;
- description d'une syntaxe pour le langage SmallTalk2K et sa traduction en langage intermédiaire FunTalk. Deux techniques de compilations seront considérées (en particulier pour la gestion des exceptions) : intuitivement, la première favorise l'élégance et la seconde les performances du code compilé :
  - les transformations en *continuation passing style* (ou à la *stackless closure-passing style*) à la SMLNJ [224, 6] ;
  - la capture "brutale" du point d'exécution, *c.à.d.* une sorte d'*execution stack capture* à la OCaml, Bigloo ;
- description d'un interprète pour FunTalk ou d'une phase de compilation de FunTalk ; deux choix sont à présent possibles, notamment une traduction vers JVM bytecode de Sun ou vers la nouvelle plate-forme .NET de Microsoft. Le premier choix permettra de factoriser la recherche des dernières années en France (à l'INRIA en particulier) et à l'étranger autour de la validation de la JVM et du langage Java (entre autres [225, 150]).

Pendant le développement théorique du langage FunTalk, on étudiera la possibilité de formaliser et de prouver les théorèmes fondamentaux, *e.g.* conservation des types et complétude, avec l'assistant de preuves Coq. La vérification ainsi qu'une possible extraction de programmes à partir de preuves en Coq devrait nous aider à la production d'un premier interprète / compilateur pour FunTalk certifié. L'extraction de programmes en Coq est sans doute un sujet de recherche très intriguant qui nous intéresse beaucoup ; une particulière attention sera dévouée au choix d'une méthode de codage (premier ordre ou ordre supérieur) qui permettra au moins la certification du logiciel visé (interprète ou compilateur).

### 5.2.3 Phase de conception et d'implantation

Nous prévoyons les étapes suivantes pour la construction des interprètes, compilateurs et environnements pour SmallTalk2K et FunTalk :

- construction (non certifiée) d'un premier interprète pour FunTalk `ft` ;
- ajout d'un module de type checking à l'interprète (non certifié) de FunTalk ;
- certification (validation) de l'interprète et du module de contrôle de types en Coq (*type soundness*) ;
- étude d'extraction via Coq de l'interprète typé pour FunTalk `coqft` ;
- étude de possibilité d'utilisation de FunTalk comme un langage de script, dans le style de Ruby [223], Python [222], ... ;
- construction (non certifiée) d'un compilateur FunTalk vers JVM de Sun ou .NET de Microsoft `ft2jvm`, `ft2net` ;
- étude d'extraction via Coq du compilateur pour FunTalk `coqft2jvm`, `coqft2net` ;
- auto-compilation (*i.e. bootstrapping*) du compilateur pour FunTalk. À partir d'un compilateur pour FunTalk (écrit dans un langage quelconque ou extrait par un assistant de preuve type Coq, pas forcément le plus efficace mais, on l'espère, certifié "sûr" [168, 132]) on construira un compilateur optimisée pour FunTalk ;
- construction d'un premier compilateur (non certifié) du langage SmallTalk2K en FunTalk `st2ft` ;
- étude d'extraction via Coq du compilateur `coqst2ft` ;
- construction de l'environnement (*c.à.d.* quelques bibliothèques pour SmallTalk2K en SmallTalk2K ou en FunTalk (en quasi totale similitude avec SmallTalk) ;
- évaluation du langage et de son environnement sur des programmes non triviaux.

## 5.3 Eiffel et SmallEiffel

**Mots clés** : Eiffel, typage sûr, covariance, liaison dynamique, analyse globale, prédiction de type, auto-compilation.

**Participants** : Dominique Colnet, Luigi Liquori, Philippe Ribet, Olivier Zendra.

**Glossaire :**

**Typage sûr.** Dans ce contexte, le fait que les indications de types écrites dans le programme soient respectées lors de l'exécution.

**Auto-compilation.** Compilation du compilateur en utilisant le texte source du compilateur lui-même (*bootstrap*).

### 5.3.1 Match-O, un dialecte d'Eiffel probablement sûr

Malheureusement, Eiffel qui est le langage qui se rapproche le plus de SmallTalk du point de vue de son expressivité, possède un système de types qui n'est pas sûr, *c.à.d.* qu'un programme bien typé selon les règles d'Eiffel peut se révéler incorrect à l'exécution (pendant l'exécution il soulèvera un exception concernant une erreur de type). Dans un langage à objets, une telle erreur se produit lors de l'exécution quand un objet reçoit un message qui n'est pas présent dans son interface.

Si l'on fait abstraction du *principe de cohérence globale* de B. Meyer [19], qui n'est implanté dans aucun compilateur Eiffel, on peut dire que le langage Eiffel n'est pas un langage avec un système de types sûr. Considérons par exemple le programme Eiffel de la figure 4. Dans cet exemple on définit deux classes `POINT` et `PIXEL` qui possèdent une méthode `is_equal` spécialisée dans `PIXEL`. La classe `MAIN` crée deux instances de `POINT` et une de `PIXEL`. L'affectation `p :=r` est acceptée par le compilateur puisque `r` qui est de type `PIXEL` peut être aussi considérée comme une expression de type `POINT`. Malheureusement, l'appel `p.is_equal(q)` produit une erreur lors de l'exécution car c'est la version spécialisée de `is_equal`, définie dans `PIXEL`, que l'on exécute (liaison dynamique oblige). En effet, cette redéfinition suppose que l'argument `q` possède la méthode `status`. Comme le type dynamique de `q` est `POINT`, l'invocation de `status` avec une instance de `POINT` provoque une erreur. Le même problème, induit en fait par la redéfinition covariante de `is_equal`, se produit également à l'issue d'un passage d'argument (fonction `breakit`) (voir aussi le papier "*On Binary Methods*" [44]).

```
class POINT inherit ANY redefine is_equal end;
creation set
feature
   x: REAL; y: REAL;
   set(a: real, b: real) is
      do
         x:= a; y:= b;
      end;
   is_equal(other: like Current): BOOLEAN is
      do
         Result := (x = other.x) and (y = other.y);
      end
end

class PIXEL inherit POINT redefine is_equal end;
creation set
feature
   status: BOOLEAN;
   set_status(s: BOOLEAN) is
      do
         status := s;
      end;
   is_equal(other: like Current): BOOLEAN is
      do
         Result := (x = other.x) and (y = other.y)
                   and (status = other.status);
      end;
end
```

```
class MAIN creation main
feature
   p: POINT; q: POINT; r: PIXEL;
   main is
      do
         !!p.set(1,1); -- New POINT in variable p
         !!q.set(2,2); -- New POINT in variable q
         !!r.set(3,3); -- New PIXEL in variable r
         p:= r; -- Accepted because of subtyping.
         if p.is_equal(q)   -- CRASH! (1)
         then ... else ... end;
         breakit(r,q) -- Accepted because of subtyping.
      end;
   breakit(p1, p2: POINT) is
      do
         if p1.is_equal(p2) -- CRASH! (2)
         then ... else ... end;
      end;
end
```

FIG. 4 – Un programme Eiffel qui laisse apparaître un problème de type lors de l'exécution.

Dans [108], D. Colnet et L. Liquori ont défini un dialecte d'Eiffel, appelé *Match-O* en raison de l'ajout d'un nouveau type appelé "type `match`". Match-O n'a pas encore une sémantique formelle, mais son nouveau système de types, inspiré des travaux de K. Bruce *et al.* [94, 170, 169, 44, 198, 46, 96] *rejette* le programme (erroné) de la figure 4 lors de la compilation. Ainsi, dans Match-O, on remplace systématiquement le type `like Current` par le type `match Current`. Intuitivement, le type `match Current`, permet d'exprimer le fait qu'une entité est exactement du même type que le receveur au regard du principe de liaison dynamique. Cette nouvelle notation de type, que nous proposons d'ajouter dans Eiffel, permet à la fois de mieux

décrire le type des entités manipulées mais aussi d'obtenir des programmes plus sûrs. Une étude complète de l'intégration du type `match` par rapport à la définition de classes génériques est en cours. Nous avons écrit un compilateur qui implante ce dialecte, accessible à `http://www.loria.fr/~colnet/Match-O/macho.tgz`. Une version journal est également en cours de rédaction avec O. Zendra en parallèle au perfectionnement de la maquette.

L'expérience du dialecte Match-O s'est révélée très positive, car une partie du code de la maquette (notamment relative à la comparaison des objets) a déjà été incluse dans la nouvelle distribution de SmallEiffel.

Comme tous les langages de taille réelle, le langage Eiffel est en cours d'évolution : en particulier, la communauté qui développe Eiffel (autour de B. Meyer) s'intéresse à établir une passerelle vers le monde .NET de Microsoft ; Eiffel# [217] est un dialecte de Eiffel qui "compile" de manière naturelle vers la plate-forme .NET ; le système de types d'Eiffel# bloque la covariance (en similitude avec Match-O) et l'héritage multiple.

### 5.3.2 Amélioration de l'analyse globale

Bien qu'il donne actuellement d'excellents résultats, l'algorithme d'analyse globale et de prédiction de type peut encore être amélioré. Des informations supplémentaires peuvent être rassemblées en augmentant la précision de l'analyse statique. Une voie qui se présente naturellement à l'esprit consiste à prendre en compte le flot d'exécution, de façon à quasiment éliminer les parties du code qui sont considérées vivantes par notre algorithme actuel alors qu'il s'agit en fait de code mort. Ceci permettrait également d'affiner encore la précision de la prédiction de type, d'où une amélioration potentielle des performances de la liaison dynamique. Cependant, il est important d'évaluer le coût à la compilation d'une telle analyse *flow sensitive*, qui pourrait s'avérer incompatible avec la compilation rapide requise pour des environnements de développement incrémental. Il est également possible d'augmenter encore la spécialisation du code généré en l'adaptant non seulement au type du receveur, mais aussi aux types dynamiques des paramètres des méthodes. C'est ce que fait l'algorithme du produit cartésien (*Cartesian Product Algorithm*) [85] proposé par O. Agesen. Ceci impose cependant la génération de très nombreuses versions d'une même méthode, qui devraient être plus efficaces car plus spécifiques, mais qui risquent de provoquer un accroissement important de la taille du code généré et du temps de compilation. Il semble donc intéressant d'étudier plus en détail les différents degrés de spécialisation possibles et l'adéquation des compromis qu'ils représentent.

### 5.3.3 Couplage avec des techniques d'analyse dynamique

Les travaux sur SmallEiffel se sont pour l'instant focalisés sur les bénéfices de l'analyse et l'optimisation statiques, faites lors de la compilation. Un domaine de recherche connexe et très actif existe, qui porte sur les techniques d'analyse et d'optimisations dynamiques, *c.à.d.* effectuées pendant l'exécution du programme compilé. Il nous semblerait judicieux d'aborder aussi ce domaine très actuel, qui génère une littérature importante. Nous souhaitons étudier ces techniques dynamiques et leurs apports au processus de compilation, notamment au niveau du couplage possible entre l'analyse globale statique et l'analyse dynamique. Nous pensons en effet qu'il est possible de bénéficier de synergies importantes entre ces deux mondes et que les

informations statistiques, de profils, rassemblées au cours de l'analyse dynamique devraient permettre d'améliorer encore les performances des programmes compilés à l'aide de notre système actuel. Ces techniques dynamiques appliquées à la liaison dynamique (basées généralement sur divers types de caches à l'exécution), par opposition aux techniques statiques (basées sur des informations et structures définies à la compilation) comme celles sur lesquelles nous avons travaillé jusqu'à présent, nous apparaissent comme particulièrement intéressantes. Elles présentent à notre avis un fort potentiel, notamment en complément de techniques statiquement calculées. Comme nous l'avons déjà souligné, la liaison dynamique et son implantation optimale sont en effet pour nous des clés importantes vers des programmes à objets performants.

### 5.3.4 Généralisation à des systèmes non figés

Pour l'instant, nos travaux ont porté sur des systèmes complets et figés, sans chargement ni création dynamique de classe. Dans l'optique de rendre les techniques que nous avons étudiées encore plus largement utilisables, il nous semble souhaitable d'étendre leurs capacités aux cas de systèmes incomplets. Des extensions relativement simples sont possibles pour utiliser ces techniques dans de tels contextes, comme la compilation séparée d'applications ou de bibliothèques, mais elles semblent de nature à dégrader fortement les performances du code compilé dans ces conditions. Il nous paraît donc indispensable d'étudier des solutions permettant d'éviter cette dégradation. Ceci pourrait impliquer de fortes modifications des algorithmes actuellement utilisés dans le compilateur SmallEiffel. Dans le même ordre d'idée, nous souhaitons vivement étendre nos recherches de façon à y inclure la compilation de langages plus dynamiques, tout particulièrement Java ou même Self. Ce type de langages offre des possibilités différentes de celles des langages de classes plus classiques, statiques, mais impose des contraintes plus importantes au compilateur. Ceci devrait nous amener très rapidement à nous intéresser à la compilation dynamique (en ligne) proprement dite, qui, elle, permet de s'adapter à un environnement et un source changeants.

### 5.3.5 L'évolution du langage Eiffel

La définition du langage Eiffel est encore en cours d'évolution. L'action Miró s'intéresse à cette évolution aussi bien au niveau des décisions de modification qu'au niveau de l'implantabilité de ces choix. La nouvelle définition prévoit l'ajout d'un nouveau type de base, type *Tuples*, qui donne la possibilité de manipuler des N-uplets typés de valeurs. Avec le type *Tuples*, il sera possible de typer plus strictement les fonctions ayant plusieurs résultats ainsi que les fonctions à nombre variable d'arguments. La méthode d'analyse globale devrait permettre de spécialiser chaque sorte de *Tuples* vivant. Dans la nouvelle définition d'Eiffel, un *agent* est, en quelque sorte, comparable à une fermeture, *closure*, d'un langage fonctionnel. L'objectif de cet ajout consiste essentiellement à pouvoir augmenter l'expressivité dans les assertions. Les agents permettent également une certaine forme d'évaluation partielle, comme dans les langages fonctionnels. De nouvelles possibilités d'introspection sont également en projet. Ces dernières n'étant que consultatives (*e.g.* la réflexivité, *i.e.* combien de méthodes dans une classe, type des arguments d'une méthode, etc.), cela ne devrait pas remettre en cause l'hypothèse du système fermé qui est un point clef dans la stratégie de compilation de SmallEiffel.

## 5.4 Réécriture, types et preuves

**Participants :** Gilles Barthe [Projet Lemme], Horatiu Cirstea [Projet Prothéo], Jöelle Despeyroux, Claude Kirchner [Projet Prothéo], Luigi Liquori.

### 5.4.1 Le Rho-calcul typé

En 2001-2002, la collaboration avec des éléments du projet Prothéo est devenue plus étroite. Nous avons publié deux articles à des conférences internationales ; dans [103], nous avons montré comment le Rho-calcul peut être utilisé en tant que *lingua franca* pour capturer différents paradigmes de programmation, comme, par exemple, la programmation à objets. En particulier, nous avons présenté un codage du LCO [65] et du OC [1] en Rho-calcul. La possibilité de codifier d'une façon naturelle le comportement de `self` (`this` de Java) dans le Rho-calcul permet une représentation des objets comme de simples ensembles, et des méthodes comme de simples règles de réécriture. Dans un certain sens, tous les formalismes et techniques propres aux calculs à prototypes, type LCO et AC, peuvent être reproduits dans le Rho-calcul.

En outre, dans [104], nous avons proposé le Rho-calcul dans un cadre de typage à la Church, en présentant huit systèmes de types placés dans un cube à la Barendregt (voir figure 5). Le plus puissant de ces systèmes s'inspire essentiellement de l'*Extended Calculus of Constructions* de Z. Luo (ECC) [145].

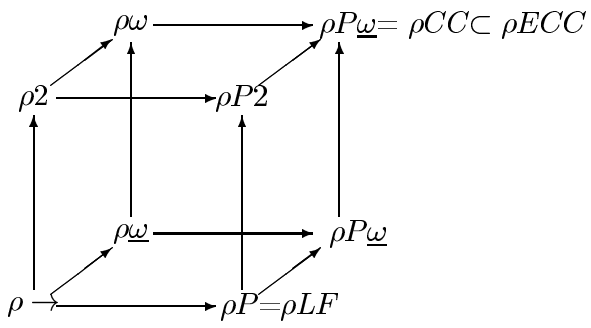



FIG. 5 – Le Rho-cube.

On pense que l'étude du Rho-calcul (typé ou non) est fondamentale et prometteuse pour explorer différentes sémantiques des langages à objets, et étendre le Calcul de Constructions (et peut-être aussi Coq) avec une solide notion de réécriture (voir aussi [40]). Les recherches les plus fondamentales dans Miró seront menées dans ce sens.

### 5.4.2 Les systèmes de types purs avec motifs

En 2002, la collaboration avec G. Barthe du projet Lemme s'est intensifiée. Nous avons soumis un article à une conférence internationale [196] et nous sommes en train de rédiger une version longue pour un journal ; dans notre travail nous définissons une extension des *Pure Type Systems,* **PTS** [41] avec pattern matching (*Pure Patterns Type Systems,* $\mathbf{P^2TS}$). Cette

extension est fortement inspirée du papier *Lambda Calculus with Patterns* de V. van Oostrom [194]. Avec J. Despeyroux on s'intéresse également à l'intégration dans les $\mathbf{P}^2\mathbf{T}\,\mathbf{S}$ d'algorithmes (décidables) d'unification d'ordre supérieur (*e.g.* à la D. Miller [149]).

La syntaxe des $\mathbf{P}^2\mathbf{T}\,\mathbf{S}$ est très simple :

$$\begin{array}{lcll} \Gamma & ::= & \emptyset \mid \Gamma, a{:}t \mid \Gamma, X{:}t & \text{contextes} \\ t & ::= & a \mid X \mid \lambda t{:}\Gamma.t \mid \Pi t{:}\Gamma.t \mid t\,t \mid [t \ll_\Gamma t].t \mid t,t & \text{termes} \end{array}$$

où $\Gamma$ dénote un contexte, $a$ dénote une constante, $X$ dénote une variable, $\lambda t{:}\Gamma.t$ une fonction avec motifs, $\Pi t{:}\Gamma.t$ un type produit avec motifs, $t\,t$ une application, $[t_1 \ll_\Gamma t_3].t_2$ une *delayed matching abstraction* où $[t_1 \ll_\Gamma t_3]$ représente une équation de filtrage pas encore résolue, et $t,t$ une séquence. Les règles d'évaluation ont la forme suivante :

$$\begin{array}{llcl} (\rho) & (\lambda t_1{:}\Gamma.t_2)t_3 & \rightarrow & [t_1 \ll_\Gamma t_3].t_2 \\ (\sigma) & [t_1 \ll_\Gamma t_3].t_2 & \rightarrow & \sigma_{(t_1 \ll_\Gamma t_3)}(t_2) \\ (\delta) & (t_1,t_2)\,t_3 & \rightarrow & t_1\,t_3, t_1\,t_3 \end{array}$$

où $\sigma_{(t_1 \ll_\Gamma t_3)}$ est la solution d'une équation de filtrage. En complète similitude avec le $\lambda$-cube de Barendregt, on peut envisager (cela est actuellement en cours d'étude) un "cube" des systèmes de types avec motifs à la Barendregt (montré en figure 6), qui pourrait être à la base d'un futur noyau d'un assistant à la preuve dans l'esprit du système Coq.

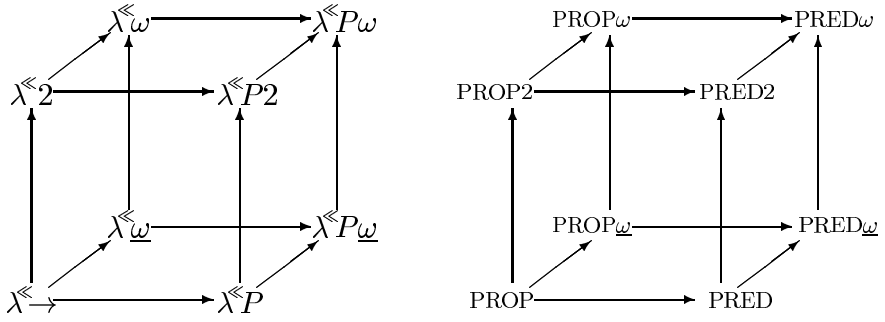



FIG. 6 – Le $\mathbf{P}^2\mathbf{T}\,\mathbf{S}$-cube et le LOGIC-cube

### 5.4.3 Les théories typées et les calculs formels

**Participants** : Alberto Ciaffaglione [Projet Prothéo], Joëlle Despeyroux, Luigi Liquori.

Nous avons mentionné précédemment (section 4) le travail pionnier réalisé par J. Despeyroux, en collaboration avec F. Pfenning, C. Schürmann et P. Leleu, dans la recherche de nouvelles théories typées permettant la récursion sur des termes de type fonctionnel.

L'extension de ces systèmes aux produits dépendants, dans toute sa généralité, apparaît difficile. F. Pfenning et C. Schürmann ont préféré, comme D. Miller, introduire un système

à deux niveaux : un niveau pour les expressions, et un niveau pour la récursion. C'est une approche raisonnable. Ceci dit, le but à long terme reste la définition d'un système intégrant la récursion et les types inductifs aux expressions et prédicats, au même niveau, comme dans le Calcul des Constructions Inductives [35].

Comme d'autres projets de l'INRIA (*e.g.* Mimosa, Moscova, ...), l'action Miró s'intéresse aux calculs (et à ses systèmes de types) qui modélisent la mobilité, le réseau et ses problèmes de sécurité. Récemment, dans la littérature scientifique, on a assisté à la naissance d'une *plethora* de calculs comme, par exemple, les Ambients de Cardelli et Gordon [48, 100], le Join-calcul de Fournet, Gonthier, Lévy, Maranget et Rémy [126], le Blue-calcul de Boudol [92], le Spi-calcul de Abadi et Gordon [146], et le Pi-calcul de Milner [70]. En outre, des travaux récents ont montré comment le paradigme à objets et ses concepts de base peuvent facilement s'intégrer dans ces nouveaux calculs.

L. Liquori avait proposé une extension du Blue Calcul [92] : le *Deep Blue Calcul* [210]. Le Deep Blue Calcul est un descendant direct du Blue Calcul. Ce calcul pourrait être vu comme une extension du Blue Calcul et du calcul des objets de Abadi et Cardelli. La recherche visait à chercher des transformations en CPS qui traduisaient le Deep Blue Calcul dans le Blue Calcul. L'idée était de démontrer que le Blue Calcul pouvait être vu comme un langage cible pour le Deep Blue et celui-ci pouvait être considéré comme point de départ pour la définition de langages à objets concurrents d'ordre supérieur.

On cherchera à être "à la page" par rapport à ces sujets de recherche et à ce que, éventuellement, les concepts de mobilité, réseaux et sécurité puissent s'intégrer d'une façon naturelle dans les calculs et/ou langages auxquels on s'intéresse.

### 5.4.4 Les preuves formelles

Nous nous intéresserons ici principalement à la certification des outils développés dans l'action autour des langages et calculs à objets. Cependant, partant du principe qu'un projet de recherche a pour vocation d'appréhender une problématique dans son ensemble, plutôt que dans des cas trop particuliers, nous nous attacherons à étudier les moyens d'améliorer le confort, et en fait la faisabilité, des preuves formelles en général. Pour ce faire, nous poursuivrons les recherches entreprises par J. Despeyroux, A. Hirschowitz, P. Leleu et G. Gillard : étude de petits exemples de formalisation de langages (principalement les langages et calculs concurrents et à objets), développement de méthodes de formalisation de ces langages, et étude de nouvelles théories typées améliorant l'activité de preuve (voir sections 3.3.2, 5.4.3).

Les preuves demandées sont encore très peu automatisées. L'action Miró veut investir dans ce domaine de recherche stratégique. Les éléments logiciels présents dans les appareils modernes ont une importance cruciale pour le bon fonctionnement de ces appareils. Dans de nombreux cas, il n'est plus possible de recourir uniquement à des campagnes de tests pour assurer leur correction et des techniques de programmation certifiée doivent être développées et mises à la portée des ingénieurs.

## 5.5 Le système d'exploitation Isaac

**Participants** : Dominique Colnet, Cyril Proch, Benoît Sonntag, Olivier Zendra.

### 5.5.1 Le système d'exploitation Isaac

L'évolution des technologies et du matériel nous amène à revoir la conception du noyau des systèmes d'exploitation actuels. Nous pensons que l'introduction de concepts objets de haut niveau au cœur même des systèmes d'exploitation simplifie et optimise l'utilisation des divers composants physiques d'un ordinateur. Ce type de démarche apporte un réel progrès aussi bien dans l'adaptation dynamique du système, que dans la simplification et le pouvoir expressif du code. Isaac est avant tout un nouveau système d'exploitation objet. Il allie modularité, flexibilité, adaptabilité, évolutivité et rapidité. D'un genre nouveau, il ne possède aucun noyau, ni micro noyau et fonctionne directement sur l'architecture de la machine. Aucune machine virtuelle n'est nécessaire et aucune autre entité que l'objet n'est présent. Actuellement, les objets qui constituent Isaac tirent pleinement partie de sa flexibilité pour modéliser de manière élégante et répondre aux attentes d'un système traditionnel du noyau jusqu'à l'interface utilisateur. La plus grande particularité d'Isaac est de garder suffisamment de sémantique dans le binaire pour que les objets conservent toutes leurs expressivités objets durant l'exécution. Le système est capable d'avoir une vision suffisamment fine des objets pour les manipuler, les inter-connecter, les cloner, ou changer les liens de multi-héritages durant l'exécution même.

Isaac [155] est constitué de son propre modèle objet à base de prototypes, le langage Lisaac qui a permis de le réaliser ressemble conceptuellement à Self avec des atouts directement liés à la conception de système portable et proche de la machine. Son compilateur produit du code binaire efficace grâce à des optimisations de haut niveau : produit cartésien, prédiction de type, suppression de la liaison dynamique, suppression de la récursivité, spécialisation du code, ... Par son modèle simple et homogène, nous sommes en droit de penser qu'il devient possible de construire et de faire évoluer les applications par simple ajout d'objet ou par mutation des prototypes existants via le clonage et l'héritage dynamique.

Son spectre d'application est varié : sa forte modularité et sa légèreté (moins d'un mega indispensable) lui permettent de s'adapter naturellement à des architectures exotiques comme les assistants personnels (palm) ou l'informatique embarquée. En effet, il devient facile d'assembler son système d'exploitation à la carte pour répondre au mieux à des contraintes industrielles et matérielles.

Sans une baisse des performances, Isaac possède des mécanismes très particuliers de protection directement gérés par le matériel qui permet de garantir une sécurité inviolable sur les objets essentiels du système. Sa forte modularité provenant des concepts objets lui permet d'aguerrir une certaine stabilité naturelle : un objet endommagé n'affecte pas (ou peu) l'intégrité du système.

### 5.5.2 Le langage Lisaac

Le langage à prototypes *Lisaac*, proche de Self, apporte un modèle uniforme pour la réalisation de nos concepts. Il se démarque par sa capacité à communiquer entres objets déjà compilés connus ou partiellement connus. Il possède les qualités de flexibilité de Self avec des outils directement liés à la mise en place de systèmes d'exploitation ou plus généralement à la programmation de bas niveau avec un langage de haut niveau. Nous avons développé un compilateur pour un langage spécialisé à base de prototypes, nommé Lisaac, qui nous sert à implanter notre système d'exploitation Isaac. Le compilateur Lisaac utilise des méthodes de

compilation avancées comme l'analyse de flot pour développer l'algorithme du produit cartésien (CPA) de prédiction de type. Les premiers résultats sont encourageants et ont donné lieu à une première publication internationale présentant notre langage [156]. Le stage de DEA de C. Proch [212] a considérablement fait évoluer la syntaxe du langage ainsi que la compréhension de la sémantique du langage lui même. Les nouvelles possibilités qu'offre ce langage au niveau de la programmation de bas niveau permettent également d'uniformiser le modèle de notre système Isaac.

En 2001, nous avons spécifié un nouveau format d'exécutable pour Isaac, lui permettant une meilleure flexibilité et une meilleure évolutivité. Ce format permettra aussi dans un futur proche l'intégration des produits GNU de manière transparente pour le système. Il est en cours d'implantation. Le gestionnaire du système de fichier d'Isaac a fait l'objet d'une réformalisation complète permettant une modularité et une bonne abstraction de la notion de fichier sous forme d'objet. L'interface utilisateur d'Isaac a également nécessité l'étude d'une forte abstraction des besoins en terme d'ergonomie. Notre modèle d'interface peut ainsi se décliner très simplement vers une représentation concrète diverse et appropriée à l'utilisateur. Sa représentation peut être graphique, vocale ou autre. Elle passe d'une représentation à une autre par simple modification d'héritage dynamique de l'interface abstraite.

Enfin, une formalisation du langage Lisaac est en cours d'étude. Nous pensons que ce langage pourrait être formalisé avec une sémantique opérationnelle relativement simple car le langage a une taille raisonnable (une vingtaine de constructeurs). En conclusion :

- Isaac est un système d'exploitation entièrement conçu avec des objets ;
- Lisaac est un langage simple de programmation à prototype dans la veine de Self, avec lequel le système Isaac est décrit.

Nous estimons que le langage Lisaac est, peut-être, une forme sophistiquée et pas encore formalisée d'un langage à la Self avec un contrôle statique des types ; cette possibilité est actuellement étudiée dans l'action Miró ; Lisaac pourrait être compilé vers le langage intermédiaire FunTalk ; dans le cas affirmatif, on pourrait envisager un système d'exploitation complètement à objets — et à notre connaissance le premier, basé sur Isaac, et, potentiellement, certifié sûr.

## 5.6 Récapitulatif et programme de travail

Compte tenu des effectifs actuels de l'action, bien conscients de nos limites, nous envisageons le programme de recherche suivant :

- **à court terme, *c.à.d.* sur environ 2 ans :**
  - description complète de la syntaxe, de la sémantique statique et dynamique du langage FunTalk ; démonstration de propriétés fondamentales sémantiques sur papier et début de leur formalisation dans un assistant de preuve ;
  - construction d'un compilateur et peut-être d'une machine virtuelle jouet pour FunTalk (en utilisant *e.g.* SmallEiffel ou Self) ; syntaxe du langage SmallTalk2K ;
  - étude, à travers l'analyse globale à la base du compilateur SmallEiffel, de la possibilité de résoudre le problème de sécurité du langage Eiffel sans modifier la définition du langage (en utilisant l'expérience sur les `match-type` en Match-O) ;
  - étude et implantation d'une bibliothèque d'interfaçage homme-machine pour Eiffel, en utilisant le langage Eiffel lui-même et la programmation par contrat et les agents ;

  - méta théorie du $\rho$-cube et des $\mathbf{P^2T\,S}$ et étude des différentes méthodes de formalisation et de preuves des langages et calculs à objets : choix d'une méthode ;
  - maturation du langage à prototypes Lisaac ; étude de la portabilité du système d'exploitation Lisaac sur d'autres processeurs ; portage des produits GNU sur l'OS Isaac ;
  - étude des optimisations du langage Java, notamment en utilisant les techniques développées pour SmallEiffel et de l'impact des architectures matérielles sur les performances des programmes à objets ;
- **à moyen terme, soit environ 4 ans :**
  - réalisation du compilateur et de la machine virtuelle pour FunTalk certifié (et peut-être extrait automatiquement) ; bootstrap d'un compilateur optimisé FunTalk écrit en FunTalk et début de sa certification semi-automatique ; validation de FunTalk avec exemples non triviaux ; certification partielle du compilateur optimisé et/ou de la machine virtuelle FunTalk ;
  - étude d'une logique possible pour le $\rho$-cube (peut-on envisager un isomorphisme à la Curry-Howard ?) et des $\mathbf{P^2T\,S}$ (peuvent-ils être à la base d'un futur noyau d'un assistant à la preuve dans l'esprit du système Coq ?) ;
  - continuation de l'étude de nouvelles théories typées facilitant la description des liaisons (*i.e. binders*) dans les langages de programmation ;
  - continuation de l'étude de différentes méthodes de formalisation et de preuve des langages et calculs concurrents et à objets ;
  - maturation du système Isaac avec en particulier la diffusion du système Isaac et de ses outils de compilation ;
  - étude de l'impact de l'utilisation de l'héritage dynamique pour l'implantation des systèmes d'exploitation.
  - modélisation et prédiction de l'impact des architectures matérielles sur l'exécution des programmes à objets ;
- **à long terme, soit plus de 4 ans :**
  - continuation de l'étude de nouvelles théories typées, comme par exemple celles présentées en [104, 61] ;
  - certification complète du compilateur optimisé et/ou de la machine virtuelle FunTalk ; *plug-in* des transformations CPS dans ce compilateur, afin de le transformer en un compilateur SmallTalk2K !
  - design et développement d'un premier environment complet (compilateur et/ou machine virtuelle et espace de travail, comme browser, workspace, debugger) pour SmallTalk2K en SmallTalk2K ou en FunTalk.

# 6 Domaines d'applications

## 6.1 Introduction

**Mots clés** : PDA, PDA-OS, téléphones mobiles, Mobile-OS, programmation sûre, logiciel certifié, code mobile, internet, télécommunications.

Les domaines concernés sont : les ordinateurs de poche et leurs systèmes d'exploitation, les

téléphones mobiles, les télécommunications, les systèmes d'exploitation en général, la génération de code pour les micro-contrôleurs synthétisables, l'électronique embarquée, les *SoC, i.e. Systems on Chips*), ou bien dans des domaines où les enjeux financiers sont importants (comme l'aérospatial, les télécommunications ou le domaine bancaire) et comme dit précédemment, tous les domaines touchant aux logiciels critiques.

## 6.2 Électronique embarquée

### 6.2.1 PDA et PDA-OS

**Participants** : Jérôme Boutet, Dominique Colnet, Benoît Sonntag.

L'évolution des technologies et du matériel permet aujourd'hui d'intégrer des outils informatiques performants dans des appareils divers et de petites tailles. Nous nous intéressons particulièrement à l'expansion massive des agendas électroniques.

Actuellement nous observons un phénomène de diversité comparable à celui du début des ordinateurs personnels. Cette diversité se situe à tous les niveaux de cette nouvelle informatique. Nous constatons une variété au niveau des processeurs, des systèmes d'exploitation et de l'interface utilisateur qui reflètent les différentes possibilités du matériel : commande par clavier, écran tactile ou reconnaissance vocale.

Dans ce domaine, deux grandes tendances se dégagent aujourd'hui : les applications écrites en langage C pour les performances, ou dans un langage interprété pour la portabilité. La puissance qu'offrent les *palms* est certes impressionnante, mais reste un sujet de préoccupation pour le développeur. Il nous paraît donc indispensable de lier performance du code compilé spécifique à un processeur avec portabilité et standardisation de l'interface de programmation. La sûreté de ce genre d'application paraît être une priorité.

Nous n'avons pas encore de solution et de direction très claire dans cette type d'applications, mais nous pensons que le langage Eiffel et, peut être, le langage FunTalk ainsi que le système Isaac pourront nous être utiles sur ce type de plate-formes.

### 6.2.2 Systèmes d'exploitation

**Mots clés** : Isaac, Self, prototype, Architecture à *Blackboards*.

**Participants** : Dominique Colnet, Benoît Sonntag.

**Glossaire :**
**Isaac.** Système d'exploitation entièrement à objets dynamiques et prototypes [156, 157].
**Lisaac.** Langage à prototypes, conçu pour l'implantation de l'OS à objets Isaac.

Dans l'action Miró, nous explorons la possibilité d'intégration de concepts objets au cœur même des systèmes d'exploitation. Cette branche de recherche fait l'objet de la thèse de B. Sonntag. L'évolution des technologies et du matériel nous amène à revoir la conception du noyau des systèmes d'exploitation actuels. Nous pensons que l'introduction de concepts objets au cœur même des systèmes d'exploitation simplifierait et optimiserait l'utilisation des divers composants physiques d'un ordinateur. De manière générale, notre démarche consiste à repenser la définition d'un noyau système en intégrant des concepts objets, voire multi-agents.

Nous sommes aujourd'hui en mesure d'affirmer que ce type de démarche apporte un réel progrès aussi bien dans l'adaptation dynamique du système que dans la simplification et le pouvoir expressif du code. De plus, notre approche a des répercussions notoires pour l'utilisateur de ce type de système. L'ultime attente réside en sa capacité de s'adapter, et de s'auto-gérer pour concevoir automatiquement des liens entres les objets (liens de clientèle, mais aussi d'héritage), qui permettront de construire une application dynamiquement selon les actions et les types de données traitées par l'utilisateur à un instant donné.

Pour mener à bien nos objectifs, sans délaisser les performances globales du système, nous avons commencé par étudier les architectures de processeurs (notamment Intel x86). Cette étude avait deux objectifs : permettre une portabilité rapide du système et une utilisation approfondie des capacités du processeur pour la mise en place des mécanismes objets. Parmi les différents concepts des langages à objets existants, nous avons choisi de privilégier les prototypes, et de construire un langage à prototypes, Lisaac, permettant l'élaboration du système.

Parallèlement à ce développement, B. Sonntag a conçu et réalisé avec ce langage un système d'exploitation expérimental appelé *Isaac*, *entièrement objet* et accédant directement le matériel sans aucune autre couche intermédiaire. Ainsi, il n'utilise le BIOS d'un PC qu'au moment du boot. Isaac possède aussi une interface graphique de haut niveau et pourra supporter l'ensemble des produits GNU via une simple compilation. Il est suffisamment avancé et compact pour servir de base à l'incorporation rapide de nouveau concepts et à l'étude de nombreux problèmes liés à l'interaction entre les objets et les systèmes d'exploitation. De plus, les premières réalisations menées par B. Sonntag semblent montrer qu'un tel système d'exploitation est extrêmement compact et se prête particulièrement bien aux systèmes embarqués.

Enfin, une formalisation du langage propriétaire à la base du système Isaac est en cours d'étude. Nous pensons que ce langage pourrait être formalisé avec une sémantique opérationnelle relativement simple car le langage a une taille raisonnable (une vingtaine de constructeurs).

## 6.3 Télécommunications

**Participants** : Claudio Casetti [Polytechnique de Turin], Luigi Liquori.

Parmi les problématiques plus intéressantes dans le cadre des applications écrites dans un langage à prototypes, on rappelle la problématique du "logiciel reconfigurable" (ou de l'*hot swapping*), *c.à.d.* la possibilité d'une application de se réconfigurer à *run-time*, par exemple, à travers la modification du corps d'une méthode suite au soulèvement d'une exception. *"... Ce problème est particulièrement important dans le cadre des applications de télécommunications, en particulier les centrales téléphoniques qui ne peuvent pas se permettre de* rebooter *à chaque mise à jour du logiciel"* [207].

En outre, nous pensons que la communauté des télécommunications est prête à introduire les méthodes formelles dans le cycle de développement des logiciels. Comme exemple, nous citons (en anglais) une contribution de C. Casetti et L. Liquori à une expression d'intérêt (EoI) envoyée à la Communauté Européenne pour la formation d'un réseau d'excellence (NoE) nommé *Design and dimensioning of the 3rd Generation Internet* (appel à proposition prévu

fin 2002).

*Proposed contribution to the NoE By L. Liquori (INRIA) and C. Casetti (Politecnico di Torino)*

> "It is well known that models/standard/protocols in telecommunications are written using not sophisticated type systems or languages, such as *e.g.* ASN.1 or GDMO : as a simple example, the semantics between Managers and Agents is defined in terms of Managed Objects, specified according to the GDMO standard language; for each management domain, the proper information model is defined : information between Manager and Agent, exchanged in the form of operations, is given in *plain english*; this "way of life" is error-prone and leads to many and dangereous errors that usually can be discovered by the engineers whose task is to *implement* protocols/behaviours/objects into suitables software objects or Object Oriented Simulation Environment. In the best of scenarios, ambiguities and criticism will come out in this simulation stage.
>
> We think that the community of researchers involved in developing standards, protocols and applications for telecommunication is now mature to use formal methods (based on logics, mathematics, lambda calculi, type systems, rewriting, statics analysis, ...) and proof assistants (such as Coq, Isabelle, PVS, B, ...) to design / check / validate / certify / develops protocols / advanced-services / applications / emulators in the 3rd generation internet. The major cost in the design phase (it is well understood that a fairly concrete mathematical model costs more in terms of human resources than a UML chart or an ITU reccommendation) will benefit from a major "solidity" of the specification of protocols and related software; in case of some proof assistant the proved specifications can be turned directly into executable code (C in case of a B-development, OCaml in case of Coq-development).
>
> We are of course far from a "democratization" of such proof assistants (which can actually be used only by experts) but their recent use in the setting of formal certification of critical applications such as smartcard, embedded software, compilers, protocols for cryptography, Java language ... shows that in the near future their use will be as widespread as the use of C++ libraries or design patterns or object orientation.
>
> Our (modest) contribution to the NoE will be to foster the idea that 3rd Generation Internet should put special emphasis on formal methods and formal certification, by showing their application to the development of advanced protocols in the TCP/IP stack"

# 7 Positionnement pas rapport aux autres projets

## 7.1 Miró et l'INRIA

L'INRIA est un environnement de recherche très riche ; nous pensons profiter de cet environnement afin que, par exemple, les "produits" FunTalk/SmallTalk2K, SmallEiffel et Isaac soient étiquetés comme des véritables produits *"made in INRIA"*. On considère Miró comme une "action ouverte", où différentes composantes de l'INRIA pourraient apporter leur contribution afin d'améliorer et d'enrichir le projet lui-même.

## 7.2 Miró et l'INRIA-Lorraine

Parmi les *contributions possibles* au sein du LORIA, sans que cette liste soit exhaustive, nous souhaitons les collaborations suivantes :

- **Prothéo.** L'action Miró collabore depuis sa naissance avec les chercheurs du projet Prothéo. Les travaux réalisés sont essentiellement autour du Rho-calcul [103, 104]. On pourrait également envisager l'utilisation du langage Elan et du Rho-calcul pour une partie de la *validation* de la sémantique opérationnelle de FunTalk / SmallTalk2K (problèmes de confluence, de stratégie et de typage) ;
- **Orpailleur.** Les systèmes à base de connaissances pour raisonner et résoudre des problèmes dans des domaines de la feuille des donnés sont à la base de cet action ; ce problèmes pourraient être modélisés avec des langages à objets basés sur les prototypes. Nous espérons que cette action nous fournira des études de cas ;
- **Calligramme.** La connaissance de ce projet des problématiques de typage en général et des continuations peut être utile dans la construction et la conception du système de types de SmallTalk2K. En outre, l'expérience de P. de Groote en $\lambda$-calcul ainsi qu'en problèmes d'unification d'ordre supérieur pourrait nous être utile dans le cadre de future extensions des $\mathbf{P^2TS}$ ;

En outre, on pourrait avoir d'éventuelles interactions avec **Cassis** (sur la construction des outils de *model checking*), **Model** (la méthode B d'Abrial [2] nous intéresse pour l'extraction de code exécutable à partir de machines abstraites), **Types** (étude des systèmes de types dans le cadre de certaines logiques *resources conscious*, *e.g.* BI [135]).

## 7.3 Miró et l'INRIA-Sophia

À l'INRIA-Sophia, nous souhaitons plus particulièrement les collaborations avec les projets suivants :

- **Lemme.** Le projet Lemme s'intéresse aux preuves formelles en Coq et focalise sa recherche sur la formalisation de théories mathématiques et d'algorithmes, avec comme application industrielle principale, aujourd'hui, les algorithmes de cryptographie, d'arithmétique des ordinateurs et de géométrie.
  Y. Bertot est (aussi) intéressé par la preuve des compilateurs certifiés pour des langages impératifs [168] ; cette publication représente, à notre connaissance, un excellent exemple d'extraction (semi)automatique d'un compilateur pour un langage impératif à travers un assistant à la preuve ! On aimerait bien pouvoir profiter de cette expérience dans le cadre de FunTalk/SmallTalk2K.
  G. Barthe s'intéresse à la formalisation de Java et JavaCard et aux preuves de sécurité dans ces langages et est aussi très compétent dans le domaine de la théorie des types. G. Barthe a rendu visite à Miró@Nancy en octobre 2001 pour présenter ses travaux sur la certification de JavaCard ainsi qu'en juillet 2002 pour étudier le cadre de Pure Pattern Type Systems [196].
- **Mimosa.** Le projet Mimosa s'intéresse à la mobilité. Les membres du projet sont des spécialistes, entre autres, du $\lambda$-calcul, du $\pi$-calcul, et de leurs diverses extensions (notamment avec des objets). Plus récemment, le projet s'est intéressé aux problèmes de sécurité dans les processus mobiles.
  Le projet travaille en relation avec le projet Moscova et a aussi des échanges avec le projet Cristal de l'INRIA Rocquencourt. Les projets Mimosa et Moscova abordent la recherche de ces langages par le côté concurrent (et fonctionnel), le projet Cristal par le

côté fonctionnel (et objets), et nous, à plus long terme, par le côté objet (et fonctionnel). En outre, on espère pouvoir profiter des compétences de M. Serrano, auteur du compilateur Bigloo [216], un des compilateurs Scheme les plus performants sur le marché (bootstrappé, compile2c, compile2jvm, threads, ...).

- **Oasis.** Le projet Oasis développe un système appelé SmartTools [221] qui pourrait nous intéresser. SmartTools est un générateur interactif et générique d'environments de spécification des sémantiques des langages de programmation. SmartTools est l'évolution du système Centaur [179] ; il est basé sur la technologie Java et XML. Ce logiciel permet de générer automatiquement des environnements de développement pour n'importe quel langage, à partir de spécifications déclaratives. À partir des spécifications formelles d'un langage, SmartTools génère automatiquement un ensemble d'outils de développement qui vont permettre de développer très rapidement un environnement interactif de programmation, dédié à ce langage. Nous pensons que cette approche scientifique pourrait être adaptée pour la définition de notre langage FunTalk/SmallTalk2K et nous souhaitons établir un échange de compétence dans ce domaine et savoir s'il y a une possibilité d'utilisation de SmartTools dans le cadre de FunTalk/SmallTalk2K.

  Enfin, récemment nous avons eu d'enrichissantes discussions avec B. Serpette sur la certification d'interprètes et de compilateurs de mini-langages à objets (*e.g.* FunTalk en Coq) et sur le choix des plates-formes pour le code compilé (JVM, .NET). L'action Miró compte intensifier cet échange de compétences à la rentrée 2002.

En outre, on pourrait avoir d'éventuelles interactions avec les projets **Tick** (étude et implémentation des systèmes réactifs synchrones), et **Planète** (sur les protocoles et les applications pour l'Internet).

## 7.4 Miró et l'INRIA\{Lorraine, Sophia}

D'autres projets (à l'INRIA et dans d'autres établissements en France) corrélés à notre travail de recherche intéressent potentiellement le projet Miró :

- **Cristal.** Ce projet est sans doute la référence dans la compilation des langages fonctionnels et à objets, ainsi que des problèmes de sûreté de typage pour calculs à prototypes ; le projet Cristal est engagé dans le développement du langage OCaml et est (a été) particulièrement actif dans la définition de ML2000 (encore vivant ?) ;
- **Logical.** Ce projet est sans doute la référence dans le domaine de la théorie des types et des assistants à la preuve. Au niveau théorique, le projet a introduit le Calcul des Constructions (co-)Inductives, dont les dernières évolutions incluent l'extraction (de programmes à partir de preuves) et les modules. Le projet s'intéresse aussi à la logique et à la réécriture. Dans le même temps, le projet développe un système d'assistance à la preuve, qui est certainement le plus sophistiqué à l'heure actuelle, en partie grâce au grand pouvoir d'expression du Calcul des Constructions (co-)Inductives, sa base théorique. On pense que la partie plus théorique du projet Miró est très corrélée avec ce projet, notamment sur la possibilité d'ajouter la réécriture dans Coq [104, 25, 196] ;
- **Lande.** Ce projet est aussi intéressant pour la conception de méthodes et d'outils d'aide au développement et à la validation de logiciels ; en particulier les travaux sur l'analyse statique de T. Jensen et D. Le Métayer (Trusted Logic) et T. Thorn [136] peuvent, dans

une certaine mesure, inspirer une réflexion similaire dans le compilateur SmallEiffel ; le groupe de O. Ridoux est à l'avant-garde dans la compilation de langages logiques à travers les continuations [34], des outils formels que nous souhaitons utiliser dans SmallTalk2K/FunTalk ; enfin le projet Lande est très actif dans la spécification de la plate-forme *JavaCard* [225].

En outre, on pourrait avoir d'éventuelles interactions avec :

- les actions/projets issus de **Solidor** (maintenant action **Aces** et projet **Arles**), autour de l'électronique embarquée ;
- l'action **Klee** autour de P. Cointe, en ce qui concerne les langages à prototypes et la programmation par aspect [219] ;
- le projet **Espresso** autour de J.P. Talpin, autour des environnements de spécification de programmes réactifs synchrones ;
- le projet **Triskell**, autour de la construction fiable et efficace d'applications par assemblage de composants logiciels ;
- le projet **Sardes** autour des architectures de systèmes réflexifs pour les environnements distribués ;
- l'action **Compsys** autour du prototypage rapide d'applications sur FPGA.

Enfin, le récent recrutement INRIA de D. Miller et de C. Palamidessi à l'UR Futurs sera observé avec attention par notre action.

## 7.5 Miró et les autres groupes en France

- **Plume, LIP, ENS-Lyon.** L. Liquori collabore depuis 1998 avec P. Lescanne ; nous travaillons en particulier sur la définition d'un cadre général pour la fondation des sémantiques à réécriture de langages basés à objets. Nous avons particulièrement étudié les problèmes liés à l'extension d'un calcul fonctionnel (sans mutation) à une version impérative (avec mutation). Ce cadre permet une classification très naturelle de nombreux calculs basés sur les objets en fonction des principales techniques d'implémentation de l'héritage qu'ils mettent en œuvre (la *délégation* et l'*embedding*), et en fonction de leur stratégie. Une première étude a abouti à la définition de $\mathrm{Obj}^a$ qui est un cadre pour des calculs à objets prenant en compte à la fois les langages à objets mutables, les langages à objets non mutables, ainsi que les langages à délégation et les langages à embedding [139]. Ce cadre a été formalisé dans un article en cours de soumission qui en présente la problématique sous-jacente [120].
- **ENS Ulm.** L. Liquori collabore depuis 1996 avec G. Castagna [141] sur les aspects les plus théoriques des calcul à objets. On pense profiter des récentes compétences de G. Castagna dans la recherche des calculs à objets pour la mobilité.
- **FOC, Paris VI & CNAM.** Récemment, L. Liquori a commencé une collaboration avec le groupe FOC (T. Hardin, V. Donzeau-Gouge, C. Dubois *et al.*). Le groupe s'occupe de la conception d'un "dialecte" d'OCaml, et de son compilateur qui prend en compte les aspects "preuves" dans le cadre de la construction des algorithmes certifiés en Coq. Une première journée de travail a déjà été organisée au CNAM le 18/6/02.
- **PPS, Paris Jussieu VII.** Parmi les "possibles" collaborations avec les chercheurs de cette équipe, nous citons C. Berline, R. Di Cosmo, P.L. Curien, Y.L. Krivine, et P-A.

Melliés, sur les aspects typage, preuves et calculs.
- **Démons, Paris Sud XI.** Parmi les "possibles" collaborations avec les chercheurs de cette équipe, nous citons C. Paulin-Mohring, J-C. Filliâtre, J-P. Jouannaud, D. Kesner, surtout sur Coq, certification de logiciel, et extraction de programmes à partir de preuves.

## 7.6 Miró et l'Europe

- **Le projet IST Types.** L. Liquori et J. Despeyroux travaillent en collaboration avec les membres du projet européen TYPES depuis l'origine (1984). Le projet Types a, en particulier, été le lieu de nombreux et fructueux échanges d'idées entre J. Despeyroux et, notamment, G. Plotkin à Edinbourgh et M. Hofmann maintenant à Munich, sur les principes de récursion et d'induction pour les objets de type fonctionnel.
- **SLP, DIMI, Univ. Udine, Italie.** L. Liquori collabore activement avec le groupe *Semantics and Logics of Programs* de Udine, de F. Honsell, P. Di Gianantonio, M. Miculan *et al.* avec des échanges d'étudiants en DEA, co-tutelles, proposition d'équipes associées, et articles [129, 200].
- **SLC, Dip. Informatica, Univ. Turin, Italie.** L. Liquori a toujours maintenu des relations étroites avec le groupe *Semantics and Logics of Computation* de Turin de M. Dezani-Ciancaglini, S. Ronchi della Rocca, V. Bono, et M. Coppo *et al.* pendant et après sa thèse de Ph.D.
- **Dip. Telematica, Polytechnique Turin, Italie.** Depuis 99, L. Liquori a entamé une collaboration fructueuse avec C. Casetti dans le cadre d'une recherche orientée télécommunications. Nous espérons profiter de nos compétences complémentaires dans le cadre du montage d'un projet IST européen (*6th IST Framework Programme*).
- **ETH. Zurich.** D. Colnet collabore depuis toujours avec le concepteur du langage Eiffel, B. Meyer. Récemment, il lui a rendu visite à ETH dans le cadre de la normalisation ECMA du langage lui-même.

## 7.7 Miró et les États-Unis et le Canada

- **CMU, DCS-Yale.** La collaboration de J. Despeyroux avec F. Pfenning (CMU) et C. Schurmann (CMU puis DCC, Yale) sur la récursion pour les objets de type fonctionnel, mentionnée plus haut (section 4) a été très fructueuse et a fait l'objet de plusieurs articles. Nous espérons avoir d'autres occasions de collaborer ensemble sur ce sujet qui nous tient à cœur.
- **Site, Ottawa.** J. Despeyroux a fait la connaissance d'A. Felty à l'INRIA en 1989. Ils ont eu depuis de nombreux échanges sur un domaine de recherche commun : la formalisation des langages de programmation à l'ordre supérieur. Cette longue collaboration informelle s'est concrétisée en particulier par la publication d'un travail en commun (section 4), par une visite de 2 mois 1/2 de J. Despeyroux aux Bell-Labs (lorsque A. Felty y était) et par une relation bilatérale en 2000-2002. Une visite de J. Despeyroux à l'université d'Ottawa est prévue à l'automne 2002.
- **McGill, Montréal.** Dans le cadre de son post-doctorat au sein de l'*Adaptive Computation Laboratory* (ACL) de McGill University à Montréal, O. Zendra a mené des recherches

consistant à étudier les interactions entre logiciels et matériel, afin d'optimiser au mieux des programmes écrits dans des langages à objets [163]. Des échanges scientifiques enrichissants avaient déjà pu avoir lieu à diverses reprises avec des membres de l'ACL (notamment le Prof. K. Driesen) et des membres du Compilers and Concurrency Laboratory, anciennement ACAPS (Prof. L. Hendren) de McGill University. Ces échanges, bien que de qualité, avaient été généralement limités pour des raisons de contraintes temporelles, à des conférences et visites, et à des courriers électroniques. Ils avaient cependant fait apparaître très clairement la communauté de nos centres d'intérêts (compilation, optimisation, liaison dynamique) et la complémentarité de nos compétences et approches, les chercheurs de l'ACL de McGill se concentrant plus particulièrement sur le bas ou très bas niveau (architecture matérielle) alors que nous nous focalisons sur un niveau plus haut, lié à la sémantique des programmes.

– **WPI, Worcester.** L. Liquori collabore depuis 1999 avec D. Dougherty sur la définition d'un cadre général pour la fondation des sémantiques à réécriture de langages basés sur les objets. Nous avons particulièrement étudié les problèmes liés à l'extension d'un calcul fonctionnel (sans mutation) à une version impérative (avec mutation) [120].

En outre, nous souhaiterions faire un appel à des groupes qui, dans une certaine mesure, nous ont influencés et qui travaillent dans des domaines directement corrélés à nos recherches ; sans que cette liste soit exhaustive, nous rappelons les groupes TACOMA@Tromsø-Cornell, Church@Boston, {Flint,Haskell}@Yale, {TILT,TAL}@Cornell, SIP@Princeton, C- -@Harward, OSUIF@Ucsb, SUIF@Stanford, CYCLONE@Att, PCC@Berkeley, FOX@Cmu, Express@GeorgiaTech, {SML/NJ,Moby}@Bell, Self@Sun, MSR@{Redmond,Cambridge}, ....

# 8 Logiciels

## 8.1 SmallEiffel : The GNU Eiffel Compiler

**Participants** : Dominique Colnet, Olivier Zendra, Philippe Ribet.

Les buts éminemment pratiques de nos travaux sur SmallEiffel nous ont dès le début amenés à nous poser la question de la validation expérimentale de nos idées. Il nous est fort naturellement apparu qu'une des meilleures façons de le faire consistait à les implanter dans un compilateur créé *ex nihilo*, dont les deux objectifs principaux étaient qu'il soit capable de compiler vite, tout en générant du code efficace. Afin de mettre nos travaux à disposition du plus grand nombre, nous avons choisi de diffuser SmallEiffel comme logiciel libre (`http://SmallEiffel.loria.fr`).

SmallEiffel nous a ainsi servi d'outil expérimental dans lequel nous avons pu implanter nos idées et valider nos hypothèses, ainsi que de vecteur de diffusion auprès de la communauté scientifique et du public. Mais il a aussi constitué un sujet d'observation, un banc d'essai significatif, extrêmement intéressant et plein d'enseignements, facilitant ainsi l'émergence de nouvelles idées. En effet, rappelons que SmallEiffel est complètement auto-compilé (*bootstrapped*) en Eiffel et représente dans sa version `-0.74` environ 110 000 lignes d'Eiffel pour environ 300 classes vivantes, ce à quoi il convient d'ajouter l'ensemble de la série de programmes utilisés pour valider le compilateur, soit environ 2500 classes représentant 250 000 lignes d'Eiffel.

Intégrant les techniques d'optimisation développées dans la thèse d'O. Zendra, SmallEiffel produit un code d'excellente qualité, dont les performances sont en général supérieures (voire très supérieures) à celles des autres compilateurs Eiffel disponibles dans le commerce. Il se compare également très favorablement aux compilateurs C++.

La très bonne qualité du code généré par SmallEiffel permet l'obtention d'exécutables de très petite taille, grâce notamment à la *compilation sur nécessité* et la *spécialisation des primitives*. De même, cette spécialisation est indéniablement à l'origine de la rapidité des exécutables produits. SmallEiffel étant écrit en Eiffel, ses exécutables bénéficient eux aussi des optimisations appliquées aux programmes compilés. Ses propres performances, en terme de mémoire et surtout de temps de compilation sont elles aussi excellentes, comparées aux autres compilateurs Eiffel ou à des compilateurs C++.

Ces qualités montrent donc l'efficacité des techniques sur lesquelles nous avons focalisé notre travail. Elles montrent également que les objectifs initiaux (processus de compilation plus efficace, code généré plus efficace, portabilité) ont été atteints de façon fort satisfaisante.

**Opérations développement du logiciel (ODL).** Dans le cadre du développement du logiciel SmallEiffel, l'action a obtenu pour l'année 2001 un financement de l'INRIA de 15K€ et un ingénieur expert pour 12 mois. Ce contrat a été reconduit en 2002. Le but principal de P. Ribet est l'étude et l'implantation d'une bibliothèque d'interfaçage homme-machine pour Eiffel, en utilisant le langage Eiffel lui même et la programmation par contrat.

## 8.2 FunTalk / SmallTalk2K

**Participants** : Alberto Ciaffaglione, Luigi Liquori, Jöelle Despeyroux, Olivier Zendra.

Nous avons commencé la définition du langage SmallTalk2k/FunTalk. Pour développer notre objectif, nous avons proposé 2 sujets de DEA. En 2001, les étudiants V. Croizier et S. Salvati ont conçu la syntaxe, la sémantique opérationnelle et le système de types du langage FunTalk. Un simple interprète non typé (réalisé en Eiffel) pour FunTalk a déjà été implanté. Le système de types sera prochainement intégré dans l'interprète [204, 215]. De plus, A. Ciaffaglione un élève en thèse en cotutelle INPL-Université de Udine, sous la direction de C. Kirchner (co-encadré par L. Liquori) et F. Honsell a commencé la formalisation d'un sous-ensemble de FunTalk, essentiellement **imp**$\varsigma$ de Abadi et Cardelli, en Coq : on a formalisé la sémantique opérationnelle et un système de type du premier ordre. Une page web FunTalk/SmallTalk sera bientôt disponible à l'addresse `http://www.loria.fr/~lliquori/FunTalk`.

**Le contrat plan état-région (CPER).** La Région Lorraine a financé en 2001 et 2002, avec 30K€ le programme *SmallTalk2K : Construction d'un Compilateur et d'un Environnement "Sûr" pour un Langage à Objet* [201].

## 8.3 Isaac / Lisaac

**Participants** : Jérôme Boutet, Dominique Colnet, Benoît Sonntag.

Le *challenge* actuel du système Isaac est celui d'établir une passerelle fiable entre les outils

présents sous UNIX et le système lui même. En effet, pour que notre système d'exploitation ne reste pas un système "jouet" et expérimental, il est indispensable d'établir des passerelles et de l'ouvrir par compatibilité avec d'autres systèmes déjà présents. Une première documentation du système Isaac se trouve sur la page web `http://www.loria.fr/~bsonntag`. En 2002 nous avons proposé un sujet de DEA : l'étudiant C. Proch [212] a sensiblement amélioré la syntaxe et la sémantique opérationnelle de Lisaac. Un interprète avec debogueur a été implanté.

**Portage de Isaac sur PDA.** La commission nationale INRIA des postes d'accueil d'ingénieur associé 2002, a décidé de retenir notre proposition du portage du système d'exploitation Isaac sur une architecture différente de la gamme des processeurs Intel (architecture x86). En particulier on focalisera notre intérêt sur les architectures utilisées dans les assistants personnels (PDAs). J. Boutet travaillera, à partir de septembre 2002, sur le portage de la `GlibC` sur Isaac (pour augmenter rapidement et avec un effort limité le nombre d'applications disponibles sur Isaac), et sur le portage d'Isaac lui même sur les architectures StrongARM, Motorola MC68K et DragonBall.

# 9 Actions régionales, nationales et internationales

## 9.1 Équipes associées à l'étranger 2001-2002

Dans le cadre des relations internationales de l'INRIA, l'action Miró a répondu à l'appel à propositions pour la constitution d'équipes associées à l'étranger. Nous avons décidé de nous associer avec l'équipe *Semantics of Logic and Programming (SLP)* de l'Université d'Udine, équipe dirigée par le prof. F. Honsell (`http://www.dimi.uniud.it/SLP/gruppo.html`). Le titre de la proposition est *Formal semantics and certified tools for the language FunTalk* [208]. Cette proposition n'a pas été acceptée mais nous comptons la retravailler et la re-soumettre en automne 2002.

## 9.2 Projets européens

- J. Despeyroux et L. Liquori participent au working group européen IST TYPES.
- J. Despeyroux et L. Liquori participent au projet IST *Appsem II : Applied Semantics.*
- L. Liquori et C. Casetti du Polytechnique de Turin ont participé à l'expression d'intérêt (EoI) de la Communauté Européenne pour la formation d'un réseau d'excellence (NoE) nommé *"Design and dimensioning of the 3rd Generation Internet"* (appel à proposition prévu fin 2002).

## 9.3 Action QSL (CPER)

L'action Miró participe activement au CPER (Contrat Plan État Région) sous forme de rapporteur de propositions d'actions, participation à la conception de la plate-forme logicielle, organisation de journées séminaires, et diffusion auprès des industriels d'Alsace et Lorraine.

### 9.4 Groupes de recherches (GDR)

L. Liquori participe aux GDRs *Mélanges de systèmes algébriques et de systèmes logiques* et *Objets et Composants Logiciels : spécification, vérification, sémantique.* D. Colnet et O. Zendra participent au GDR *Objets et Composants Logiciels : implémentation de langages à objets.*

### 9.5 Accueils de chercheurs

L´action Miró a accueilli en 2001-2002 les chercheurs suivants :

- avril 2001 (30 jours) : Richard Walker, Australian National University (ANU), de Canberra, Australie, pour effectuer un travail conjoint sur SmallEiffel,
- septembre 2001 (3 jours) : Gilles Barthe, projet INRIA Lemme (*Reasoning about Javacard*),
- novembre 2001 (5 jours) : Dan Dougherty, WPI (*Normal forms and reduction for theories of binary relations*),
- décembre 2001 (4 jours) : Claudio Casetti, École Polytechnique de Turin (*Enhancing the TCP Protocol* et *Advanced TCP/IP*),
- décembre 2001 (3 jours) : Rossano Gaeta, Università di Torino (*ATM : theory and applications*),
- mars 2002 : (2 jours) : Yves Bertot, projet INRIA Lemme (*Certification d'un compilateur pour un langage impératif*),
- mars 2002 : (1 jour) : Pierre Cointe et Mario Südholt, action INRIA Klee, Nantes (*AOP : Aspect Oriented Programming*),
- juillet 2002 : (3 jours) Gilles Barthe, projet INRIA Lemme (*Pure Pattern Type Systems*).

## 10 Diffusion de résultats

### 10.1 Miró en "Tour de France"

L. Liquori a commencé un petit "tour de France" de projets de recherches, notamment à l'INRIA. Nous envisageons la visite de quelques projets INRIA corrélés à notre travail de recherche pour présenter, discuter et réviser le projet Miró à l'aide de séminaires informels, notre but étant de profiter au maximum des compétences de l'INRIA pour mieux adapter notre programme de recherche et/ou trouver des collaborations. Voici pour mémoire la liste des rencontres et présentations effectuées (et prévues) à ce jour :

```
- mars 2001 : INRIA Rocquencourt (Cristal & Logical & Moscova),
- juin 2001 : INRIA Sophia (Certilab & Lemme & Mimosa),
- juillet 2001 : École des Mines de Nantes (Klee, de P. Cointe),
- octobre 2001 : ENS Lyon (Plume, de P. Lescanne).
- septembre-octobre 2002 : visite aux rapporteurs (si possible)
```

### 10.2 Enseignement

- D. Colnet a été de 1999 à 2001 en délégation à l'INRIA. Néanmoins, il a animé à l'ESIAL (U.H.P. - Nancy 1) le cours *Programmation à objets*, où il utilise avec succès depuis 1994

le langage Eiffel et son compilateur SmallEiffel.
- J. Despeyroux a été responsable du module *Mécanisation des preuves* au DEA MDFI de Marseille de 1995 à 2002. Elle est également intervenue dans le module de tronc commun *Méthodes formelles et fiabilité du logiciel*, créé sur son initiative au DEA d'informatique de Nice, en 2000.
- L. Liquori a été responsable de 1999 à 2002 à l'École des Mines de Nancy du cours de $2^{ème}$ année *Fondements de l'algorithmique et de la programmation* et du cours du $3^{ème}$ année *Réseaux et Télécommunications* ; par ailleurs, depuis 2000 il participe au module de DEA IAEM Nancy ayant pour titre : *Sémantique des langages de programmation.*
- O. Zendra a participé, durant son post-doctorat, à l'enseignement des modules *CS308-764.2001 : Run-time Support for Object-Oriented Programming Languages* et *CS 505 - High Performance Computer Architecture* à la School of Computer Science de McGill University, Canada. Il y a également collaboré à l'encadrement de M. Holly, étudiant en *Master of Computer Science* travaillant sur les systèmes adaptatifs et l'évaluation des prédicteurs de branchements dans les micro-architectures.

## 10.3 Thèses et stages

Thèses et DEAs dans l'action (2001-2002) :
- A. Ciaffaglione, (doctorant INPL en cotutelle France-Italie) ; *Towards Certified Software for (manipulating) Reals and Objects* : le sujet de thèse porte, en outre, sur le développement et la formalisation en Coq d'un nouveau langage à objets, FunTalk, et de son compilateur (encadrants : L. Liquori 25% et C. Kirchner 25%) ;
- B. Sonntag, doctorant CCH-INRIA, 2001-2002 : *Intégration de concepts objets au cœur même des systèmes d'exploitation* (encadrant : D. Colnet) ;
- Cyril Proch, DEA, 2002 : *Lisaac : implantation et définition d'un langage à base de prototypes* (encadrants : D. Colnet 50% et O. Zendra 50%) ;
- V. Croizier, DEA, 2001 : *FunTalk : Sémantique et Validation* (encadrants : D. Colnet 50% et L. Liquori 50%) ;
- S. Salvati, DEA, 2001 : *FunTalk : Sémantique et Démonstration* (encadrants : D. Colnet 20% et L. Liquori 80%).

## 10.4 Administration de la recherche

- D. Colnet est membre du Département de Formation Doctorale (DFD) de Nancy et membre de la commission de spécialistes $27^{ème}$ section de l'U.H.P. Nancy 1 depuis 1997. Il est membre actif du groupe ECMA (`http://www.ecma.ch`) de normalisation du langage Eiffel (TC39-TG4). Il a participé aux comités de programmes de TOOLS Europe (1999 et 2000) et TOOLS USA (2002). Il est membre de la commission nationale de l'INRIA pour l'attribution des ODL (Opérations de Développement Logiciel) depuis 2000.
- J. Despeyroux a participé aux comités de programmes des *Workshop on Logical Frameworks and Meta languages*, affilié à PLI-99, puis à LICS-00 (*chairman*).
- J. Despeyroux a organisé les 2 éditions (1999 et 2002) de l'école d'été internationale *Theory and Practice of Formal Proofs*, organisée sous l'égide du WG européen ESPRIT

*Types*, à Giens, du 30 août au 10 septembre 99, et du 2 au 13 septembre 2002 (`http://www-sop.inria.fr/certilab/types-sum-school02/`).

- J. Despeyroux a été membre de la Commission de Spécialistes à l'Université de Nice Sophia Antipolis (UNSA) de mars 1998 à septembre 2001, et membre de la Commission d'Évaluation de l'INRIA de janvier 1999 à août 2002.
- J. Despeyroux a été, avec R. Harper (CMU), éditeur invité de l'édition spéciale du *Journal of Functional Programming*, sur les *Logical Frameworks and Meta Languages*, prévue pour l'été 2002.
- L. Liquori est responsable des relations de l'École des Mines de Nancy avec les universités italiennes. En 2001, 2 élèves en DEA d'informatique sont arrivés à Nancy ainsi que 7 élèves à l'École des Mines. En 2002 on prévoit 8 élèves à l'École des Mines.
- L. Liquori a participé au jury de thèse de l'UHP-Nancy 1 de H. Dubois et à la commission de spécialistes pour le concours de MdC à l´École des Mines de Nancy 2001 et d'ATER à Nancy. Il est membre du comité de programme de LMO-03.
- O. Zendra est membre du jury du concours international annuel *Eiffel Struggle* organisé par le consortium NICE, en coopération avec l'Eiffel Forum, l'Eiffel Liberty Journal (ELJ) et les principales sociétés fournissant des outils Eiffel.
- D. Colnet et O. Zendra sont membres actifs du Nonprofit International Consortium for Eiffel (NICE), et participent à la définition des standards pour le langage Eiffel.

**N.B.** Les publications de l'action Miró sont labelisées avec un ✓.

# 11 Bibliographie

## Livres et monographies

[1] M. Abadi, L. Cardelli, *A Theory of Objects*, Springer Verlag, 1996.

[2] J. R. Abrial, *The B-Book : Assigning Programs to Meanings*, Cambridge University Press, 1996.

[3] A. Aho, R. Sethi, J. Ullman, *Compilateurs. Principes, techniques et outils*, InterEditions, Paris, 1989.

[4] A. V. Aho, R. Sethi, J. D. Ullman, *Principles Of Compiler Design*, Addison-Wesley, 1990.

[5] A. V. Aho, J. D. Ullman, *Principles of Compiler Design*, Addison-Wesley, Reading, Massachusetts, 1977.

[6] A. Appel, *Modern Compiler Implementation in Java*, Cambridge University Press, 1998.

[7] H. P. Barendregt, *The Lambda Calculus : Its Syntax and Semantics*, édition revised, *Studies in Logic and the Foundations of Mathematics*, *103*, North-Holland, Amsterdam, 1984.

[8] J. Bennett, *Introduction to Compiling Techniques. A first course using ANSI C, lex and yacc.*, McGraw-Hill, London, 1996.

[9] K. Bruce, *Foundations of Object-Oriented Languages : Types and Semantics*, The MIT Press, 2002, `http://www.cs.williams.edu/~kim/FOOLbook.html`.

[10] G. Castagna, *Object-Oriented Programming : A Unified Foundation*, *Progress in Theoretical Computer Science*, Birkäuser, Boston, 1996.

[11] P. Cunin, M. Griffiths, J. Voiron, *Comprendre la Compilation*, Springer-Verlag, Berlin, 1980.

[12] A. Goldberg, D. Robson, *Smalltalk-80 : the Language and its Implementation*, Addison-Wesley, 1983.

[13] D. Gries, *Compiler Construction for Digital Computer*, J. Wiley ans Sons, New York, 1971.

[14] J.-M. Jézéquel, M. Train, C. Mingins, *Design Patterns and Contracts*, Addison-Wesley, 1999.

[15] O. Madsen, K. Moller-Pedersen, B. Nygaard, *Object-Oriented Programming in the Beta Programming Language*, Addison-Wesley, 1993.

[16] ✓ G. Masini, A. Napoli, D. Colnet, D. Léonard, K. Tombre, *Les langages à objets*, InterEditions, Paris, 1989.

[17] ✓ G. Masini, A. Napoli, D. Colnet, D. Léonard, K. Tombre, *Linguaggi per la programmazione a oggetti*, Gruppo Editoriale Jackson, Milano, 1991.

[18] ✓ G. Masini, A. Napoli, D. Colnet, D. Léonard, K. Tombre, *Object-Oriented Languages*, Academic Press, Lyon, 1991.

[19] B. Meyer, *Eiffel, The Language*, Prentice Hall, 1994.

[20] J. Noble, A. Taivalsaari, I. Moore (éditeurs), *Prototype-Based Object-Oriented Programming : Concepts, Languages, and Applications*, Springer Verlag, 1999.

[21] L. C. Paulson, *Isabelle : A Generic Theorem Prover*, Springer-Verlag LNCS 828, 1994.

[22] S. Peyton-Jones, *The implementation of functional programming languages*, Prentice Hall, Inc., 1987.

[23] J.-P. Tremblay, P. G. Sorenson, *The Theory and Practice of Compiler Writing*, McGraw-Hill, London, 1985.

[24] R. Wilhelm, D. Maurer, *Les compilateurs théorie.construction.génération.*, Masson, Paris, 1994.

## Thèses et habilitations à diriger des recherches

[25] F. Blanqui, *Type Theory and Rewriting*, thèse de doctorat, University Paris-Sud, 2001.

[26] H. Cirstea, *Calcul de Réécriture : Fondements et Applications*, Thèse de Doctorat, Université Henri Poincaré - Nancy I, 2000.

[27] ✓ D. Colnet, *Compilation, langages à objets et programmation par contrats. Expérience acquise dans le cadre du projet "SmallEiffel The GNU Eiffel Compiler"*, Thèse d'habilitation à diriger des recherches, Université Henri Poincaré – Nancy 1, 2000.

[28] K. Fisher, *Type System for Object-Oriented Programming Languages*, thèse de doctorat, University of Stanford, 1996, `ftp ://theory.stanford.edu/pub/kfisher/thesis.ps.gz`.

[29] ✓ G. Gillard, *Formalisation des langages concurrents et à objets modulo l'alpha-conversion*, Ph.d. thesis, Nice University, 2001.

[30] ✓ P. Leleu, *Syntaxe abstraite d'ordre supérieur et récursion dans les théories typées*, Ph.d. thesis, École Nationale des Ponts et Chaussées (ENPC), 1998.

[31] ✓ L. Liquori, *Type Assigment Systems for Lambda Calculi and for the Lambda Calculus of Objects*, Thèse de Doctorat, Université de Turin, 1996.

[32] J. Nordlander, *Reactive Objects and Functional Programming*, thèse de doctorat, Dept. of Computing Science, Chalmers University of Technology, Göteborg, Sweden, 1999.

[33] R. Pollack, *The Theory of LEGO : A Proof Checker for the Extended Calculus of Constructions*, thèse de doctorat, University of Edinburgh, 1994.

[34] O. Ridoux, *λ-Prolog de A à Z, ... ou presque*, Habilitation à diriger le recherches, Université de Rennes 1, 1998.

[35] B. Werner, *Une Théorie des Constructions Inductives*, Thèse de Doctorat, Université Paris 7, 1994.

[36] ✓ O. Zendra, *Traduction et optimisation dans les langages à objets*, Thèse de Doctorat, Université Henri Poincaré – Nancy 1, 2000.

## Articles et chapitres de livre

[37] M. Abadi, L. Cardelli, « A Theory of Primitive Objects : Untyped and First Order Systems », *Information and Computation 125*, 2, 1996, p. 78–102.

[38] M. Abadi, « Baby Modula–3 and a Theory of Objects », *Journal of Functional Programming 4*, 2, 1994, p. 249–283.

[39] A. V. Aho, S. C. Johnson, « LR Parsing (YACC - Yet Another Compiler Compiler) », *ACM Computing Surveys*, 1974.

[40] F. Barbanera, M. Fernandez, H. Geuvers, « Modularity of Strong Normalization in the algebraic-λ-cube », *Journal of Functional Programming 7*, 6, 1997, p. 613–660.

[41] H. Barendregt, « Lambda Calculi with Types », *in : Handbook of Logic in Computer Science*, S. Abramsky, D. Gabbai, et T. Maibaum (éditeurs), *II*, Oxford University Press, 1992, p. 118–310.

[42] G. Blashek, « Type-safe OOP with prototypes : the concepts of Omega », *Structured Programming 12*, 12, 1991, p. 1–9.

[43] ✓ V. Bono, M. Bugliesi, M. Dezani-Ciancaglini, L. Liquori, « Subtyping for Extensible, Incomplete Objects », *Fundamenta Informaticae 38*, 4, 1999, p. 325–364.

[44] K. Bruce, L. Cardelli, G. Castagna, T. H. O. Group, G. Leavens, B. Pierce, « On Binary Methods », *Theory and Practice of Object Systems 1*, 3, 1996.

[45] K. Bruce, G. Longo, « A Modest Model of Records, Inheritance and Bounded Quantification », *Information and Computation 87*, 1/2, 1990, p. 196–240.

[46] K. Bruce, « A Paradigmatic Object–Oriented Programming Language : Design, Static Typing and Semantics », *Journal of Functional Programming 4*, 2, 1994, p. 127–206.

[47] ✓ M. Bugliesi, G. Delzanno, L. Liquori, M. Martelli, « Object Calculi in Linear Logic », *Journal of Logic and Computation 10*, 1, 2000, p. 75–104.

[48] L. Cardelli, A. D. Gordon, « Mobile Ambients », *Theoretical Computer Science 240*, 1, 2000.

[49] L. Cardelli, J. Mitchell, « Operations on Records », *Mathematical Structures in Computer Sciences 1*, 1, 1991, p. 3–48.

[50] L. Cardelli, P. Wegner, « On Understanding Types, Data Abstraction and Polymorphism », *Computing Surveys 17*, 4, 1985, p. 471–522.

[51] L. Cardelli, « Obliq : A Language with Distributed Scope », *Computing Systems 8*, 1, 1995, p. 27–59.

[52] G. Castagna, G. Ghelli, G. Longo, « A Calculus for Overloaded Functions with Subtyping », *Information and Computation 117*, 1, 1995, p. 115–135.

[53] G. Castagna, « Covariance and Contravariance : Conflict Without a Cause », *TOPLAS 17*, 3, 1995, p. 431–447.

[54] A. Church, « A Formulation of the Simple Theory of Types », *Journal of Symbolic Logic 5*, 1941, p. 56–68.

[55] ✓ D. Colnet, P. Coucaud, O. Zendra, « Eiffel : la puissance de la recherche au service de vos programmes », *Programmez ! 2*, 1998, p. 82–83.

[56] ✓ D. Colnet, G. Masini, A. Napoli, K. Tombre, D. Léonard, « La montée des langages à Objets », *Le Monde Informatique 376*, 1989, p. 22–24.

[57] ✓ D. Colnet, O. Zendra, « Global System Analysis at Work », *Journal of Object-Oriented Programming 14*, 1, 2001, p. 10–13.

[58] T. Coquand, G. Huet, « The Calculus of Constructions », *Information and Computation 76*, 2/3, 1988, p. 95–120.

[59] N. G. de Bruijn, « Lambda Calculus Notation with Nameless Dummies, A Tool for Automatic Formula Manipulation, With Application to the Church-Rosser Theorem », *Indag. Math. 34*, 5, 1972.

[60] ✓ J. Despeyroux, P. Leleu, « Metatheoretic Results for a Modal lambda-Calculus », *Journal of Functional and Logic Programming 2000*, 1, 2000.

[61] ✓ J. Despeyroux, P. Leleu, « Recursion over Objects of Functional Type », *Mathematical Structures in Computer Sciences 11*, 4, 2001.

[62] ✓ J. Despeyroux, « Theo : an interactive proof development system », *The Scandinavian Journal on Computer Science and Numerical Analysis (BIT), édition spéciale sur "Programming Logic" 32*, 1992, p. 15–29.

[63] M. Felleisen, D. P. Friedman, « A Syntactic Theory of Sequential State », *Theoretical Computer Science 69*, 1989, p. 243–287.

[64] M. Felleisen, R. Hieb, « The revised report on the syntactic theories of sequential control and state », *Theoretical Computer Science 102*, 1992.

[65] K. Fisher, F. Honsell, J. C. Mitchell, « A Lambda Calculus of Objects and Method Specialization », *Nordic Journal of Computing 1*, 1, 1994, p. 3–37.

[66] M. J. Gabbay, A. M. Pitts, « A New Approach to Abstract Syntax with Variable Binding », *Formal Aspects of Computing ?*, 2001, p. ?–?, Special issue in honour of Rod Burstall. To appear.

[67] R. Harper, F. Honsell, G. D. Plotkin, « A Framework for Defining Logics », *Journal of ACM 40*, 1, 1994, p. 143–184.

[68] W. A. Howard, « The Formulae-as-Types Notion of Construction », *in : To H.B. Curry : Essays on Combinatory Logic, Lambda Calculus and Formalism*, J. P. Seldin et J. R. Hyndley (éditeurs), Academic Press, 1980, p. 479–490.

[69] D. Miller, G. Nadathur, F. Pfenning, A. Shedrov, « Uniform Proofs as a Foundation for Logic Programming », *Annals of Pure and Applier Logics 51*, 1991, p. 125–157.

[70] R. Milner, J. Parrow, D. Walker, « A Calculus of Mobile Processes I and II », *Information and Computation 100*, 1, 1992, p. 1–77.

[71] J. Palsberg, T. Jim, « Type Inference for Simple Object Types is NP-Complete », *Nordic Journal of Computing 4*, 3, 1997, p. 259–286.

[72] L. C. Paulson, « Isabelle : The next 700 theorem provers », *in : Logic and Computer Science*, P. Odifreddi (éditeur), Academic Press, 1990, p. 361–386.

[73] K. R. Rajendra, E. Tempero, H. M. Levy, A. P. Black, N. C. Hutchinson, E. Jul, « Emerald : a general-purpose programming language », *Software Practice and Experience 21*, 1, 1991, p. 91–118.

[74] J. C. Reynolds, « Types, Abstractions, and Parametric Polymorphism », *Information Processing*, 1983, p. 513–523.

[75] ✓ C. Schürmann, J. Despeyroux, F.Pfenning, « Primitive Recursion for Higher-Order Abstract Syntax », *Theoretical Computer Science 266*, 1-2, 2001, p. 1–57.

[76] ✓ S. van Bakel, L. Liquori, S. Ronchi della Rocca, P. Urzyczyn, « Comparing Cubes of Typed and Type Assignment System », *Annals of Pure and Applier Logics 86*, 3, 1997, p. 267–303.

[77] A. K. Wright, M. Felleisen, « A Syntactic Approach to Type Soundness », *Information and Computation 115*, 1, 1994.

[78] ✓ O. Zendra, D. Colnet, P. Coucaud, « SmallEiffel : l'Eiffel à Très Grande Vitesse », *Programmez ! 3*, 1998, p. 64–67.

[79] ✓ O. Zendra, D. Colnet, P. Coucaud, « With SmallEiffel, The GNU Eiffel Compiler, Eiffel joins the Free Software community. », *GNU Bulletin 25*, 1998.

[80] ✓ O. Zendra, D. Colnet, « Coping with aliasing in the GNU Eiffel Compiler implementation », *Software - Practice and Experience 31*, 6, 2001, p. 601–613.

## Communications à des congrès, colloques, etc.

[81] M. Abadi, L. Cardelli, « A Theory of Primitive Objects : second-order systems », *in : Proc. of ESOP*, *LNCS*, Springer Verlag, 1994.

[82] M. Abadi, L. Cardelli, « A Theory of Primitive Objects : untyped and first order systems », *in : Proc. of TACS*, *LNCS*, *789*, Springer Verlag, p. 296–320, 1994.

[83] M. Abadi, L. Cardelli, « An Imperative Object Calculus », *in : Proc. of TAPSOFT/FASE*, *LNCS*, Springer Verlag, p. 471–485, 1995. Also in *Theory and Practice of Object Systems* 1(3) :151-166, 1995.

[84] M. Abadi, L. Cardelli, « On Subtyping and Matching », *in : Proc. of ECOOP*, *LNCS*, *952*, Springer Verlag, p. 145–167, 1995.

[85] O. Agesen, « The Cartesian Product Algorithm : Simple and Precise Type Inference Of Parametric Polymorphism », *in : Proc. of ECOOP*, *LNCS*, *952*, Springer-Verlag, p. 2–26, 1995.

[86] ✓ V. Bono, M. Bugliesi, M. Dezani-Ciancaglini, L. Liquori, « Subtyping Constraint for Incomplete Objects », *in : Proc. of TAPSOFT/CAAP*, *LNCS*, *1214*, Springer Verlag, p. 465–477, 1997.

[87] ✓ V. Bono, M. Bugliesi, L. Liquori, « A Lambda Calculus of Incomplete Objects », *in : Proc. of MFCS*, *LNCS*, *1113*, Springer Verlag, p. 218–229, 1996.

[88] V. Bono, M. Bugliesi, « Matching Constraints for the Lambda Calculus of Objects », *in : Proc. of TLCA*, *LNCS*, *1210*, Springer Verlag, p. 46–62, 1997.

[89] V. Bono, K. Fisher, « An Imperative, First-Order Calculus with Object Extension », *in : Proc. of ECOOP*, *LNCS*, 1445, Springer Verlag, p. 462–497, 1998.

[90] ✓ V. Bono, L. Liquori, « A Subtyping for the Fisher-Honsell-Mitchell Lambda Calculus of Objects », *in : Proc. of CSL*, *LNCS*, *933*, Springer Verlag, p. 16–30, 1995.

[91] P. Borovanský, C. Kirchner, H. Kirchner, P.-E. Moreau, C. Ringeissen, « An Overview of ELAN », *in : Proc. of WRLA*, *15*, Electronic Notes in Theoretical Computer Science, 1998.

[92] G. Boudol, « The $\pi$-Calculus in Direct Style », *in : Proc. of POPL*, The ACM Press, p. 228–241, 1997.

[93] K. Bruce, L. Cardelli, C. B. Pierce, « Comparing Object Encoding », *in : Proc. of TACS*, *LNCS*, *1281*, Springer Verlag, p. 415–438, 1997.

[94] K. Bruce, A. Shuett, R. van Gent, « PolyTOIL : a Type-Safe Polymorphic Object Oriented Language », *in : Proc. of ECOOP*, *LNCS*, *952*, Springer Verlag, p. 27–51, 1995.

[95] K. Bruce, « Safe Type Checking in a Statically-typed Object-oriented Programming Language », *in : Proc of POPL*, p. 285–298, 1993. Extended version in *Journal of Functional Programming.*

[96] K. Bruce, « Subtyping is not a Good Match for Object-oriented Programming Languages », *in : Proc. of ECOOP*, *LNCS*, *1241*, Springer Verlag, 1997.

[97] ✓ M. Bugliesi, G. Delzanno, L. Liquori, M. Martelli, « A Linear Logic Calculus of Objects », *in : Proc. of JICSLP*, T. M. Press (éditeur), p. 67–81, 1996.

[98] ✓ G. Canals, D. Colnet, S. Cruz-Lara, J. C. Derniame, « GEPI : un Générateur d'Environnements de Programmation Intégrés », *in : Le genie logiciel et ses applications*, p. 406–421, Toulouse, 1988.

[99] P. Canning, W. Cook, W. Hill, W. Olthoff, « F-Bounded Polymorphism for Object-Oriented Programming », *in : Proc. of ICFP*, The ACM Press, p. 273–280, 1989.

[100] L. Cardelli, G. Ghelli, A. D. Gordon, « Mobility Types for Mobile Ambients », *in : Proc. of ICALP*, *LNCS*, 1644, Springer Verlag, p. 230–239, 1999.

[101] Y. Caseau, F. Laburthe, « CLAIRE : Combining Objects and Rules for Problem Solving », *in : Proc. of ICLP*, T. M. Press (éditeur), p. 245–259, 1999.

[102] C. Chambers, D. Ungar, « Customization : Optimizing Compiler Technology for Self, a Dinamically-typed Object-Oriented Programming Language », *in : Proc. of PLDI*, p. 146–160, 1989.

[103] ✓ H. Cirstea, C. Kirchner, L. Liquori, « Matching Power », *in : Proc. of RTA*, *LNCS*, *2030*, Springer Verlag, p. 168–183, 2001.

[104] ✓ H. Cirstea, C. Kirchner, L. Liquori, « The Rho Cube », *in : Proc. of ESOP/FOSSACS*, *LNCS*, *2051*, Springer Verlag, p. 77–92, 2001.

[105] ✓ D. Clement, J. Despeyroux, T. Despeyroux, G. Kahn, « A Simple Applicative Language : Mini-ML », *in : Proc. of LFP*, ACM Press, 1986.

[106] ✓ S. Collin, D. Colnet, O. Zendra, « Type Inference for Late Binding. The SmallEiffel Compiler. », *in : Proc. of JMLC*, *LNCS*, *1204*, Springer Verlag, p. 67–81, 1997.

[107] ✓ D. Colnet, P. Coucaud, O. Zendra, « Compiler Support to Customize the Mark and Sweep Algorithm », *in : Proc. of ISMM*, p. 154–165, 1998.

[108] ✓ D. Colnet, L. Liquori, « Match-O, a Statically Safe (?) Dialect of Eiffel », *in : Proc. of TOOLS*, IEEE Computer Society, p. 190–201, 2000.

[109] ✓ D. Colnet, O. Zendra, « Optimizations of Eiffel programs : SmallEiffel, The GNU Eiffel Compiler », *in : Proc. of TOOLS*, IEEE Computer Society, p. 341–350, 1999.

[110] W. Cook, W. Hill, P. Canning, « Inheritance is not Subtyping », *in : Proc. of POPL*, The ACM Press, p. 125–135, 1990.

[111] W. R. Cook, « A Proposal to Make Eiffel Type Safe », *in : Proc. of ECOOP*, Cambridge University Press, p. 57–70, 1989.

[112] F. DAMIANI, S. DROSSOPOULOU, M. DEZANI-CIANCAGLINI, P. GIANNINI, « Fickle : Dynamic Object Reclassification », *in : Proc. of ECOOP*, *LNCS*, Springer Verlag, 2001.

[113] ✓ J. DESPEYROUX, A. FELTY, A. HIRSCHOWITZ, « Higher-order Abstract Syntax in Coq », *in : Proc. of TLCA*, *902*, Springer Verlag, p. 124–138, 1995.

[114] ✓ J. DESPEYROUX, A. HIRSCHOWITZ, « Higher-Order Syntax and Induction in Coq », *in : In Proc. of LPAR*, *LNCS*, *822*, Springer Verlag, p. 159–173, 1994.

[115] ✓ J. DESPEYROUX, P. LELEU, « A Modal $\lambda$-calcul with iteration and case constructs », *in : Proc. of TYPES*, *LNCS*, Springer Verlag, 1998.

[116] ✓ J. DESPEYROUX, P. LELEU, « Primitive recursion for higher-order abstract syntax with dependant types », *in : Proc. of IMLA*, 1999. FLoC satellite workshop.

[117] ✓ J. DESPEYROUX, F. PFENNING, C. SCHÜRMANN, « Primitive Recursion for Higher-Order Abstract Syntax », *in : Proc. of TLCA*, *LNCS*, 1210, Springer Verlag, p. 147–163, 1997.

[118] ✓ J. DESPEYROUX, « Proof of translation in Natural Semantics », *in : Proc. of LICS*, IEEE Computer Society, 1986.

[119] ✓ J. DESPEYROUX, « A Higher-order specification of the pi-calculus », *in : Proc. of the IFIP-TCS*, 2000.

[120] ✓ D. DOUGHERTY, F. LANG, P. LESCANNE, L. LIQUORI, K. ROSE, « A Generic Object-calculus based on Addressed Term Rewriting Systems », *in : Proc. of Westapp*, Logic Group Preprint series No 210. Utrecht University, the Netherlands, p. 6–25, 2001.

[121] K. FISHER, J. C. MICHELL, « Notes on Typed Object-Oriented Programming », *in : Proc. of TACS*, *LNCS*, *789*, Springer Verlag, p. 844–885, 1994.

[122] K. FISHER, J. C. MITCHELL, « A Delegation-based Object Calculus with Subtyping », *in : Proc. of FCT*, *LNCS*, *965*, Springer Verlag, p. 42–61, 1995.

[123] K. FISHER, J. H. REPPY, « The Design of a Class Mechanism for Moby », *in : Proc. of PLDI*, *SIGPLAN Notices*, *34*, The ACM Press, p. 37–49, 1999.

[124] K. FISHER, J. H. REPPY, « A Calculus for Compiling and Linking Classes », *in : Proc. of ESOP*, *LNCS*, *1782*, Springer Verlag, p. 153–149, 2000.

[125] K. FISHER, J. H. REPPY, « Extending Moby with Inheritance-Based Subtyping », *in : Proc. of ECOOP*, *LNCS*, *1850*, Springer Verlag, p. 83–107, 2000.

[126] C. FOURNET, G. GONTHIER, J.-J. LÉVY, L. MARANGET, D. RÉMY, « A Calculus of Mobile Agents », *in : Proc. of CONCUR*, *LNCS*, *1119*, Springer Verlag, p. 406–421, 1996.

[127] A. GAWECKI, F. MATTHES, « Integrating Subtyping, Matching, and Type Quantification : a Practical Perspective », *in : Proc. of ECOOP*, *LNCS*, *1098*, Springer Verlag, p. 26–47, 1996.

[128] H. GEUVERS, B. WERNER, « On the Church-Rosser Property for Expressive Type Systems and its Consequences for their Metatheoretic Study », *in : Proc. of LICS*, p. 320–329, 1994.

[129] ✓ P. D. GIANANTONIO, F. HONSELL, L. LIQUORI, « A Lambda Calculus of Objects with Self-inflicted Extension », *in : Proc. of OOPSLA*, The ACM Press, p. 166–178, 1998.

[130] ✓ G. GILLARD, « A formalization of a concurrent object calculus up to alpha-conversion », *in : Proc. of CADE*, *LNCS*, Springer Verlag, 2000.

[131] A. D. GORDON, « A Mechanisation of Name-Carrying Syntax up to Alpha-Conversion », *in : Proc. of HUG*, *LNCS*, *780*, Springer-Verlag, 1994.

[132] J. HANNAN, F. PFENNING, « Compiler Verification in LF », *in : Proc. of LICS*, p. 407–418, 1992.

[133] M. HOFMANN, « Semantical analysis of higher-order abstract syntax », *in : Proc. of LICS*, IEEE Computer Society, 1999.

[134] A. IGARASHI, B. PIERCE, P. WADLER, « Featherweight Java : A minimal core calculus for Java and GJ », *in : Proc. of OOPSLA*, The ACM Press, p. 132–146, 1999.

[135] S. S. ISHTIAQ, P. W. O'HEARN, « BI as an Assertion Language for Mutable Data Structures », *in : Proc. of POPL*, The ACM Press, p. 14–26, 2001.

[136] T. JENSEN, D. L. MÉTAYER, T. THORN, « Verification of control flow based security properties », *in : Proc. of ISSP*, IEEE Computer Society, p. 89–103, 1999.

[137] ✓ J. K. LIMAM, P. VERNEL, D. COLNET, « Design of a customizable processor IP », *in : International Workshop on IP Based Synthesis and System Design*, p. 181–185, Grenoble, 1999. LORIA 99-R-380.

[138] S. N. KAMIN, « Inheritance in Smalltalk-80 : A Denotational Definition », *in : Proc. of POPL*, T. A. Press (éditeur), p. 80–87, 1988.

[139] ✓ F. LANG, P. LESCANNE, L. LIQUORI, « A Framework for Defining Object-Calculi (Extended Abstract) », *in : Proc. of FM*, *LNCS*, *1709*, Springer Verlag, p. 963–982, 1999.

[140] D. LEIVANT, « Polymorphic Type Inference », *in : Proc. of POPL*, The ACM Press, p. 88–98, 1983.

[141] ✓ L. LIQUORI, G. CASTAGNA, « A Typed Lambda Calculus of Objects », *in : Proc. of Asian*, *LNCS*, *1179*, Springer Verlag, p. 129–141, 1996.

[142] ✓ L. LIQUORI, M. SAPINO, « Dealing with Explicit Exceptions », *in : Proc. of GULP-PRODE, Joint Conference on Declarative Programming*, p. 296–308, 1994.

[143] ✓ L. LIQUORI, « An Extended Theory of Primitive Objects : First Order System », *in : Proc. of ECOOP*, *LNCS*, *1241*, Springer Verlag, p. 146–169, 1997.

[144] ✓ L. LIQUORI, « On Object Extension », *in : Proc. of ECOOP*, *LNCS*, *1445*, Springer Verlag, p. 498–552, 1998.

[145] Z. LUO, « ECC : An Extended Calculus of Constructions », *in : Proc. of LICS*, IEEE Computer Society, p. 385–395, 1990.

[146] A. D. G. M. ABADI, « A Calculus for Cryptographic Protocols : The Spi Calculus », *in : Proc. of ACM Conference on Computer and Communications Security*, The ACM Press, p. 36–47, 1997.

[147] J. MCKINNA, R. POLLACK, « Pure Type Systems Formalized », *in : In Proc. of TLCA*, *LNCS*, *664*, Springer Verlag, p. 289–305, 93.

[148] J. C. MICHELL, « Toward a Typed Foundation for Method Specialization and Inheritance », *in : Proc. of POPL*, The ACM Press, p. 109–124, 1990.

[149] D. MILLER, « A Logic Programming Language with Lambda-Abstraction, Function Variables, and Simple Unification », *in : Proc. of ELP*, *LNCS*, *475*, Springer Verlag, p. 253–281, 1991.

[150] T. NIPKOW, D. VON OHEIMB, « Java Light is Type-Safe – Definitely », *in : Proc. of POPL*, The ACM Press, p. 161–170, 1998.

[151] J. PALSBERG, « Efficient Inference of Object Types », *in : Proc. of LICS*, p. 186–195, 1993.

[152] R. POLLACK, « Closure Under Alpha-Conversion », *in : Proc. Types*, *LNCS*, *806*, Springer Verlag, p. 313–332, 1994.

[153] D. RÉMY, « From Classes to Objects via Subtyping », *in : Proc. of ESOP*, *LNCS*, *1381*, Springer Verlag, p. 200–220, 1998.

[154] J. RIECKE, C. STONE, « Privacy via Subsumption », *in : Electronic proc. of FOOL-98*, 1998. Also in *Theory and Practice of Object Systems*.

[155] ✓ B. SONNTAG, D. COLNET, O. ZENDRA, « Dynamic inheritance : a powerful mechanism for operating system design », *in : In Workshop ECOOP-OOOSWS*, 2002.

[156] ✓ B. SONNTAG, D. COLNET, « Lisaac : the power of simplicity at work for operating system », *in : Proc. of TOOLS*, The ACS Press, 2002. To appear.

[157] ✓ B. SONNTAG, « Utilisation de la segmentation mémoire du processeur à partir d'un langage de haut niveau », *in : Proc. of Conférence Française sur les Systèmes d'Exploitation, CFSE*, p. 107–116, 2001.

[158] D. UNGAR, R. B. SMITH, « Self : The power of simplicity », *in : Proc. of OOPSLA*, The ACM Press, p. 227–241, 1987.

[159] L. VAN BENTHEM JUTTING, J. MCKINNA, R. POLLACK, « Checking Algorithms for Pure Type Systems », *in : Proc. of Types, LNCS, 806*, Springer Verlag, p. 19–61, 1994.

[160] ✓ O. ZENDRA, D. COLNET, S. COLLIN, « Efficient Dynamic Dispatch without Virtual Function Tables. The SmallEiffel Compiler. », *in : Proc. of OOPSLA, 32(10)*, The ACM Press, p. 125–141, 1997.

[161] ✓ O. ZENDRA, D. COLNET, « Adding external iterators to an existing Eiffel class library », *in : Proc. of TOOLS*, IEEE Computer Society, p. 188–199, 1999.

[162] ✓ O. ZENDRA, D. COLNET, « Vers un usage plus sûr de l'aliasing avec Eiffel », *in : Proc. of LMO*, Hermes, p. 183–194, 2000.

[163] ✓ O. ZENDRA, K. DRIESEN, « Stress-testing Control Structures for Dynamic Dispatch in Java », *in : Proc. of JVM*, USENIX, 2002.

## Rapports de recherche et publications internes

[164] ✓ D. BACCHIEGA, D. GOTTA, L. LIQUORI, M. PORTA, R. ROSSI, « MOMIX-emSDH2. Simulatore di Agent di Element Manager SDH2.0. Versione 2.2.3. Manuale Utente e Guida di Riferimento », *Rapport Technique n°DTR 97.0413*, CSELT, Centro Studi e Laboratori Telecomunicazioni, Telecom Italia Centre de Recherche, 1997.

[165] ✓ D. BACCHIEGA, D. GOTTA, L. LIQUORI, M. PORTA, M. R. VOTTA, « Ipotesi evolutive del Sistema MOMIX per la Specifica e Qualificazione di Sistemi TMN », *Rapport Technique n°DTR 98.0089*, CSELT, Centro Studi e Laboratori Telecomunicazioni, Telecom Italia Centre de Recherche, 1998.

[166] B. BARRAS, « Coq in Coq », *Rapport Technique n°3026*, INRIA, Roquencour, 1996.

[167] Y. BERTOT, L. THÉRY, « The CtCoq System : Desing and Architecture », *rapport technique n°3540*, INRIA, 1998.

[168] Y. BERTOT, « A certified compiler for an imperative language », *rapport technique n°RR-3488*, INRIA, 1998.

[169] K. BRUCE, « Increasing Java's expressiveness with `ThisType` and Match-bounded Polymorphism », *rapport de recherche*, Williams College, 1997.

[170] K. BRUCE, « Typing in Object-Orinted Language : Achieving Expressiveness and Safety », *rapport de recherche*, Williams College, 1997.

[171] G. CHAMBERS, « The Cecil language specifications and rationale », *rapport de recherche n°93-03-05*, University of Washington, Dept. of Computer Science and Engineering, 1993.

[172] ✓ D. Colnet, G. Masini, A. Napoli, Y. Noiret, K. Tombre, « Les Langages Orientés Objets », *Rapport CRIN n°86-R-077*, Centre de Recherche en Informatique de Nancy, 1986.

[173] ✓ D. Colnet, E. Stapf, O. Zendra, « NICE ELKS 2000 proposal », *rapport de recherche*, LORIA - UMR 7503, 1999, loria 99-R-359.

[174] ✓ D. Colnet, O. Zendra, P. Coucaud, « Using Type Inference to Customize the Garbage Collector in an Object-Oriented Language. The SmallEiffel Compiler. », *rapport de recherche*, LORIA - UMR 7503, 1998.

[175] ✓ D. Colnet, « De CEYX », *Rapport CRIN n°86-E-035*, Centre de Recherche en Informatique de Nancy, 1986.

[176] ✓ J. Despeyroux, « Sémantique Naturelle : Spécifications et Preuves », *rapport de recherche n°RR-3359*, INRIA, 1998.

[177] ✓ J. Despeyroux, « Rapport d'activité Action Certilab », *rapport de recherche*, INRIA Sophia-Antipolis, 2001.

[178] G. Huet, G. Kahn, C. Paulin-Mohring, « The Coq Proof Assistant - A tutorial, Version 6.1 », *rapport technique n°204*, INRIA, 1997, Version révisée distribuée avec Coq. `http://coq.inria.fr/`.

[179] I. Jacobs, L.Rideau, « A Centaur tutorial », *rapport technique n°140*, INRIA, 1992, INRIA Sophia-Antipolis. `http://www-sop.inria.fr/croap/centaur/centaur.html`.

[180] G. Kahn, « Natural Semantics », *rapport de recherche n°601*, Institut National de Recherche en Informatique et en Automatique, Sophia Antipolis, France, 1987.

[181] ✓ F. Lang, P. Lescanne, L. Liquori, « A Framework for Defining Object-Calculi », *rapport de recherche n°RR1998-51*, Laboratoire de l'informatique du parallèlisme, ENS de Lyon, France, 1998, Available online at `ftp://ftp.ens-lyon.fr/pub/LIP/Rapports/RR/RR1998/RR1998-51.ps.Z`.

[182] P. Lequang, Y. Bertot, L. Rideau, L. Pottier, « The Pcoq System », *rapport technique*, INRIA, 1999, Sophia-Antipolis. `http://www-sop.inria.fr/lemme/pcoq/`.

[183] ✓ L. Liquori, « An Extended Theory of Primitive Objects », *rapport de recherche n°CS-23-96*, Computer Science Department, University of Turin, Italy, 1996.

[184] ✓ L. Liquori, « On Object Extension », *rapport de recherche*, Department of Mathematic and Computer Science, University of Udine, Italy, 1997.

[185] ✓ L. Liquori, « Bounded Polymorphism for Extensible Objects », *rapport de recherche n°RR 1999-16*, École Normale Supérieure de Lyon, France, 1999.

[186] ✓ L. Liquori, « Rapport d'activité Action Miró », *rapport de recherche*, INRIA Lorraine & Sophia-Antipolis, 2001.

[187] Z. Luo, R. Pollack, « The LEGO Proof Development System : A User's Manual », *rapport de recherche n°ECS-LFCS-92-211*, University of Edinburgh, 1992.

[188] U. of Cambridge Computer Laboratory, *The HOL System*, 1993.

[189] G. Plotkin, « A Structural Approach to Operational Semantics », *rapport de recherche n°DAIMI FN-19*, Computer Science Department, Aarhus University, Denmark, 1981.

[190] J. Reppy, « Local CPS conversion in a direct style compiler », *rapport technique*, Bell Labs, Lucent Technologies, 2000.

[191] N. Shankar, S. Owre, J. M. Rushby, *PVS Tutorial*, Computer Science Laboratory, SRI International, Menlo Park, CA, 1993.

[192] A. TAIVALSAARY, « Kevo, a prototype-based object-oriented language based on concatenation and module operations », *rapport de recherche n°LACIR 92-02*, University of Victoria, 1983.

[193] THE TWELF TEAM, « The Twelf Proof Assistant », *rapport de recherche*.

[194] V. VAN OOSTROM, « Lambda Calculus with Patterns », *Technical Report n°IR-228*, Faculteit der Wiskunde en Informatica, Vrije Universiteit Amsterdam, 1990.

## Divers

[195] D. ASPINALL, « Proof General Home Page », `www.dcs.ed.ac.uk/`, 2002.

[196] ✓ G. BARTHE, H. CIRSTEA, C. KIRCHNER, L. LIQUORI, « Pure Pattern Type Systems », `www.loria.fr/~lliquori/PPTS.ps.gz`, 2002.

[197] V. BONO, M. BUGLIESI, « Matching and Subtyping for the Lambda Calculus of Objects », Technical Report, 1997.

[198] J. BURSTEIN, *`Rupiah` : an Extension to Java Supporting Match-bounded Parametric Polymorphism, `ThisType`, and Exact Typing*, Bachelor thesis, Williams College, 1998.

[199] L. CARDELLI, « Personal @-communication », 1996.

[200] ✓ A. CIAFFAGLIONE, P. D. GIANANTONIO, F. HONSELL, L. LIQUORI, « Foundations for Dynamic Objet Reclassifications », manuscript, extended and revised version of [129].

[201] ✓ D. COLNET, L. LIQUORI, « SmallTalk-2K : Construction d'un Compilateur et d'un Environnement "Sûr" pour un Langage à Objet », 2000, Demande de Subvention à la Région Lorraine pour l'an 2001-2002. Soutien aux jeunes équipes de recherche et aux projets émergents.

[202] ✓ D. COLNET, « *Prototypage, programmation objet : application à l'édition structurelle* », Thèse de l'Université de Nancy I, 1989.

[203] ✓ V. CROIZIER, S. SALVATI, *Desing and Implementation of FunTalk*, Dea en informatique, LORIA, Nancy, 2001.

[204] ✓ V. CROIZIER, « FunTalk : Formalisations et Validation », 2001, Stage de DEA.

[205] T. DESPEYROUX, A. HIRSCHOWITZ, « A categorical approach to Higher-Order Abstract Syntax », forthcoming paper, 1994.

[206] K. FISHER, D. GROSSMANN, D. MACQUEEN, R. PUCELLA, J. REPPY, J. RIECKE, S. WEIRICH, « The Moby Programming Language », 2000, `http://www.cs.bell-labs.com/who/jhr/moby/index.html`.

[207] X. LEROY, « About Miró », @discussion.

[208] ✓ L. LIQUORI, M. MICULAN, « Formal semantics and certified compilers for the language FunTalk », 2001, Proposition pour équipe associés, `http://www.loria.fr/~lliquori/PAPERS/miro-slp.ps.gz`.

[209] ✓ L. LIQUORI, *Semantica e Pragmatica di un Linguaggio Funzionale con le Continuazioni Esplicite*, Laurea in science dell'informazione, Université de Udine, Italie, 1990.

[210] ✓ L. LIQUORI, « The Deep Blue Calculus », Manuscript, `http://www.loria.fr/~lliquori/PAPERS/deep-blue.ps.gz`, 1998.

[211] J. PETERSON, K. HAMMOND, L. AUGUSTSSON, B. BOUTEL, W. BURTON, J. FASEL, A. GORDON, J. HUGHES, P. HUDAK, T. JOHNSSON, M. JONES, E. MEIJER, S. PEYTON-JONES, A. REID, P. WADLER, « Haskell 1.4 : A Non-strict, Purely Functional Language », 1997, `http://www.haskell.org/onlinereport/`.

[212] ✓ C. Proch, « Lisaac : implantation et définition d'un langage à base de prototypes », 2002, Stage de DEA.

[213] D. Rémy, « Refined Subtyping and Row Variables for Record Types », Draft, 1995.

[214] D. Rémy, « From Classes to Objects via Subtyping », Draft, INRIA, 1997.

[215] ✓ S. Salvati, « FunTalk : Formalisations et Démonstrations », 2001, Stage de DEA.

[216] M. Serrano, « The Bigloo Compiler », 2002, http://www-sop.inria.fr/mimosa/fp/Bigloo.

[217] R. Simon, R. Stapf, B. Meyer, « Full Eiffel on .NET », 2002, http://www.inf.ethz.ch/personal/meyer/publications/msdn/eiffel-net/.

[218] The Cristal INRIA Project, « The Objective Caml », 2000, http://pauillac.inria.fr/ocaml/.

[219] The MIT ETR Editors, « Emerging Technologies That Will Change the World », MIT Enterprise Technology Review, Jan/Feb 2001, http://www.technologyreview.com/articles/tr10_toc0101.asp.

[220] The ML2000 Working Group, « Principles and a Preliminary Design for ML2000 », 1999.

[221] The Oasis INRIA project, « Action SmartTools : Outils interactifs génériques », 2000, http://www-sop.inria.fr/oasis/SmartTools/.

[222] The Python Organization, « The Python Language », 2002, http://www.python.org.

[223] The Ruby Organization, « The Ruby Language », 2002, http://www.ruby.org.

[224] The SMLNJ Team, « The Standard ML of New Yersey », 2002, http://cm.bell-labs.com/cm/cs/what/smlnj/index.html/.

[225] The Verificard Team, « The Verificard IST Project », 2002, http://www.verificard.com/.

[226] Web site de l'ambassade de France au États-Unis, « Catching bugs would save big bucks », juillet 2002, http://www.info-france-usa.org/fr.

[227] Web site Fundació Joan Miró, 2002, http://http://www.bcn.fjmiro.es/.

[228] ✓ O. Zendra, K. Driesen, F. Qian, L. Hendren, « Evaluation of the runtime performance of control flow structures for dynamic dispatch in Java », Poster and extended abstract. OOPSLA Conference Companion, The ACM Press, 2001.