Projet Certilab

Spécifications formelles, certification de logiciel

Joëlle Despeyroux

INRIA

8 janvier 1999

PLAN

Composition de l'équipe

Joëlle Despeyroux
(CR INRIA, responsable scientifique)
André Hirschowitz
(professeur UNSA, responsable permanent)
Guillaume Gillard
(doctorant, 1997-2000)
Marino Miculan
(post-doctorant, mai à déc 99)
Nathalie Balax
(assistante de projet)

Thème

Certification de logiciel:

- preuve de propriétés de langages
  Ex: preuve de correction de compilateurs,

- preuve de correction de programmes
  Ex: preuve de correction de protocoles.

Grande demande de chercheurs dans le domaine (Intel, Microsoft, ...).

Domaines d'application:
le nucléaire, l'industrie avionique ou ferroviaire,
le spatial, les télécommunications ou le domaine bancaire.

Projet de recherche:

- transversal,

- essentiellement applicatif.

Preuve de propriétés de langages

(Joëlle, André, Guillaume, Marino)

Acquis

théorique (théories typées, méthodes) et pratique (système et exemples).

Étude d'exemples

(Joëlle, André, Guillaume, Marino)

preuve de conservation des types lors de l'exécution, preuve de correction d'un compilateur.

Imp et Mini-ML, Esterel et Lustre (Dassault), logiques modales, π-calcul et sigma-calcul.

Objectif: langages concurrents et à objets (thèse de Guillaume Gillard).

Programme de recherche

Preuve de propriétés de langages *(suite)*

Méthodes *(Joëlle, André, Guillaume)*

Description des variables (Pb: substitution)

1. indices de de Bruijn,
2. variables définies à α conversion près,
3. variables libres et variables liées,
4. syntaxe abstraite d'ordre supérieur (pb: induction).

Logical Frameworks et systèmes

Théorie des types: Coq, Alf, Twelf, ...
Logique d'ordre sup: HOL, Isabelle, ...
Théorie des ensembles: PVS, ...

Théories typées *(Joëlle)*

collaboration avec F. Pfenning, C. Schürmann (CMU): un système (λ-calcul modal avec case et itération) permettant la récursion sur des termes fonctionnels.

amélioration et extension: thèse de Pierre Leleu.

Preuve de correction de programmes

Étude d'exemples *(Joëlle, André, Marino)*

preuve de correction de:
programmes impératifs,
glaneur de cellule-mémoire (gc),
cache,
protocoles de communication.

Méthodes *(Joëlle, Marino)*

extraction de programme dans Coq,
description formelle du programme dans Unity, TLA, ...,
méthode B,
proof-carrying code,
interprétation abstraite.

Veille technologique *(Joëlle)*

mobilité, réseaux (ambiants de Cardelli).

Domaines d'application

Logiciels sûrs:

1. Conception et prototypage de langages de prog.,
2. Logiciel embarqué (Esterel et Lustre),
3. Aéronautique (interprétation abstraite),
4. Télécommunications (protocoles, sécurité),
5. Programmation du Web (mobilité, réseaux).

Programme de travail sur 3 ans

Objectifs minimaux:

1. bibliothèques de spécifications et de preuves *(Joëlle, André, Guillaume, Marino)*,

2. syntaxe abstraite d'ordre supérieur pour les langages impératifs *(Joëlle, André)*,

3. acquérir une compétence en correction de programmes (priorités: extraction de programme, Unity et le proof-carrying code) *(Joëlle, André, Marino)*.

Logiciels

Développement: aucun envisagé dans l'immédiat.

Contribution au développement de Coq et de CtCoq.

Valorisation industrielle

Contrats industriels actuels:

Dassault-Aerospatiale, Vérilog (Génie 2) - Lustre

Prospective:

CNET	- correction de protocoles
Dyade, action VIP	- théorie des types
Harlequin, Edimbourg	- preuve de gc
Prover, Goteborg	- logiciel sûr
RATP, Digilog	- méthode B
Renault	- code embarqué, Coq

Collaborations scientifiques

Positionnement / projets INRIA

Projet COQ: théorie des types, bibliothèque Coq.

Projet CRISTAL: preuves de correction d'OCaml, typage des langages parallèles et à objets.

Action LEMME: programmes certifiés, exs CtCoq.

Projet MEIJE: π-calcul en Coq, Esterel certifié, model-checking et preuves intéractives?

Action OASIS: applications Java

Collaborations scientifiques *(suite)*

Collaborations nationales

(ENS Lyon - correction pour un gc)

CERMICS - Réné Lalement, π-calcul en Coq

CNAM - V. Donzeau-Gouge, Mini-ML

Projets COQ, CROAP, MEIJE et PROTHEO - appel à idées CNRS/DRET/MENESR:
maîtrise des systèmes complexes réactifs et sûrs

Projets CRISTAL, CROAP et COQ - Action de Recherche Concertée:
preuves de propriétés d'OCaml

Collaborations scientifiques *(suite)*

Collaborations européennes

Projets Esprit BRA "Logical Frameworks" (89-91), "Types pour les preuves et les programmmes" (92-95). Depuis 96: *Working Group* "Types".
15 sites en Europe.

Chalmers, Suède	- Thierry Coquand, théorie des types
(Helsinski, Finlande	- Jan von Plato, protocoles)
Münich, Allemagne	- Tobias Nipkow, Java en Isabelle
Cambridge, GB	- (Larry Paulson, protocoles)
	- Gabbay et Pitts, description des variables
Durham, GB	- Robert Pollack, description des variables
Edimbourg, GB	- Rod Burstall, Healfdene Goguen, gc
	- Goguen, Compagnoni, théorie des types
	- M. Hofmann, induction & ordre sup.
	- G. Plotkin , ind. & ordre sup.
Londres, GB	- Ishtiaq et D. Pym, théorie des types
Udine, Italie	- Furio Honsell, exs en LF, π en Coq
(Utrecht, Pays-Bas	- Marc Bezem, protocoles)

Collaborations scientifiques *(suite)*

Collaborations internationales

CMU	- Frank Pfenning, induction & ordre sup.
Penn	- Dale Miller, ind. & ordre sup.
Bell Labs	- Amy Felty (D. McQueen), preuves
Cornell	- (R. Constable), preuves

Diffusion des résultats

Animation de la communauté scientifique

Joëlle: Commission de Spécialistes à Nice
Joëlle: resp. scientifique de l'école d'été Types'99
André: en géométrie algébrique:
- coord. de 1 réseau HCM et 3 euroconfs HCM (93-97),
- a initialisé 3 séries d'euroconfs (Europroj, Gael, Gaf),
- directeur du GDR GAC.

Enseignement

Joëlle: Dea MDFI de Marseille (coord. locale, module)
Joëlle: Dea d'info. de Nice (module proposé)
André: prof. à Nice, en Maths - géométrie algébrique

Thèses

Pierre Leleu (95-98), (99-) DDE de Rouen
Guillaume Gillard, 3ième année

Stages de DEA

Joëlle: Paris 7, CERMICS, X, ENS (1 ou 2 / an)
4 stages proposés pour 99

Diffusion des résultats *(suite)*

Colloques et séminaires

Types, LICS, TLCA, CONCUR et CADE.
Joëlle: 1 conférence invitée en 99
André: 3 conférences invitées en 98

Journaux

JAR	Automated Reasoning
JFP	Functional Programming
JIC	Information and Computation
JLC	Logic and Computation
JSC	Symbolic Computation
TCS	Theoretical Computer Science
JFLP	Functional and Logic Programming
...	

Soumissions en cours: TCS et JFLP.
Draft: JFP.

Conclusion

Thème de recherche cohérent

axe stratégique de l'INRIA - logiciel sûr

justifiant la création d'un projet

bien implanté dans l'INRIA, niv. national et international

besoin d'un apport en capital humain