| | Compte-rendu intermédiaire | |
|---|---|---|
| | | |
| | | |

**Projet ANR-08-DEFIS-005-01**

# DECERT

# Déduction certifiée

Programme Défis 2008



## A IDENTIFICATION

| | |
|---|---|
| Acronyme du projet | DECERT |
| Titre du projet | Déduction Certifiée |
| Coordinateur du projet (société/organisme) | Inria – Rennes – Bretagne - Atlantique |
| Date de début du projet<br>Date de fin du projet | 01/01/2009<br>30/09/2012 |
| Site web du projet, le cas échéant | http://decert.gforge.inria.fr/ |

| Rédacteur de ce rapport | |
|---|---|
| Civilité, prénom, nom | Mr Thomas Jensen |
| Téléphone | 02 99 84 74 78 |
| Adresse électronique | Thomas.Jensen@inria.fr |
| Date de rédaction | 2/9/2010 |
| Période faisant l'objet du rapport d'activité | 01/01/2009 – 1/09/2010 |

## B LIVRABLES ET JALONS

| État * | N° | Titre | Nature | Partenaires | Commentaires |
|---|---|---|---|---|---|
| Livré à T0+6 | D0 | DECERT website | Site web | Rennes | |
| Livré à T0+6 | D1 | Report on requirement analysis | Rapport | CEA, Nancy, Orsay, Rennes, Sophia, Systerel | |
| Livré à T0+12 | D2 | Release of Alt-Ergo and haRVey | Logiciel | Nancy, Orsay, Rennes, Sophia | |
| Livré à T0+12 | D3 | Report on new combination methods for arithmetics and non-stably infinite théories | Rapport | Nancy, Orsay | |
| Prévu à T0+24 | D4 | Report on new combination methods for data structure and resource functions | Rapport | Nancy, Orsay | |
| Livré à T0+12 | D5 | Report on strategies for efficient deduction | Rapport | Nancy, Orsay | |
| Prévu à T0+24 | D6 | Report on collaborative décision procédures for arithmetic | Rapport | Nancy, Orsay | |
| Prévu à T0+24 | M1 | New release of Alt-Ergo and haRVey | Jalon | Nancy, Orsay, Rennes, Sophia | |
| Livré à T0+12 | D7 | Preliminary report on a generic proof format for SMT solvers | Rapport | Nancy, Orsay, Rennes, Sophia | |
| Prévu à T0+24 | D8 | Final report on a generic proof format for SMT solvers | Rapport | Nancy, Orsay, Rennes, Sophia | |
| Prévu à T0+24 | D9 | Preliminary report and prototype for proof reconstruction of SMT proof witnesses | Rapport | Nancy, Orsay, Rennes, Sophia | |
| Prévu à T0+36 | D10 | Final report and prototype for proof reconstruction of SMT proof witnesses | Jalon | Nancy, Orsay, Rennes, Sophia | |
| Prévu à T0+24 | D11 | Report on inference of arithmetic invariants using decision procedures | Rapport | Rennes | |
| Prévu à T0+24 | D12 | A PCC protoype for resource usage analysis using linear and non-linear decision procédures | Logiciel | Rennes, Sophia | |
| Prévu à T0+36 | D13 | A PCC prototype for resource usage analysis enhanced with a combination of decision procedures | Logiciel, Jalon | Rennes, Sophia | |
| Prévu à T0+24 | D14 | Preliminary report on integrating SMT proof witnesses into RODIN & Frama-C | Rapport | CEA, Nancy, Orsay, Systerel | |
| Prévu à T0+36 | D15 | Final report on integrating SMT proof witnesses into RODIN & Frama-C | Rapport, Jalon | CEA, Nancy, Orsay, Systerel | |

**Préciser : « Livré le… » ; « Prévu le… » ; « Reprévu le… » ; « Abandonné » ;*

# C RAPPORT D'AVANCEMENT SUR LA PERIODE CONCERNEE

## C.1 DESCRIPTION DES TRAVAUX EFFECTUES

La tâche T1 de recensement des besoins et objectifs du projet a permis de regrouper dans un espace commun les jeux d'essais provenant de tous les partenaires et de constituer ainsi une référence commune pour le projet. Cette tâche a aussi permis de préciser les objectifs qualitatifs du projet en terme d'expressivité, d'efficacité et de témoins de preuve. Systerel a fourni des obligations de preuve issues de B événementiel. Le CEA-LIST a fourni des jeux de tests représentatifs des obligations de preuve issues de la vérification de programmes C par les outils Caveat et Frama-C. Orsay a fourni des obligations de preuve issues de Why et Nancy des buts pour le prouveur SMT veriT. Rennes a fourni des obligations de preuve obtenues à partir de résultats d'analyses statiques. Cela nous a permis de définir une taxonomie des différentes théories et combinaison de théories auxquelles le projet doit s'intéresser.

Dans le cadre des tâches T2 et T3, nous avons travaillé à étendre les méthodes de combinaison de procédures de décision et à améliorer leur efficacité. La méthode de combinaison introduite par Nelson et Oppen (1980) impose deux limitations: les théories doivent être formées sur des signatures disjointes et doivent satisfaire l'hypothèse dite de stable infinité. Les résultats que nous avons obtenus permettent de repousser ces deux limitations.

- Nous avons développé un nouveau cadre de combinaison pour des mélanges de théories non-disjointes qui modélisent des structures de données partageant certains fragments de l'arithmétique. Le résultat est obtenu en montrant que les théories considérées satisfont les hypothèses de la méthode de combinaison non-disjointe introduite par Ghilardi en 2004 puis raffinée en 2007 grâce à de nouvelles hypothèses de terminaison. Notre méthode repose sur la capacité à calculer et à échanger les conséquences logiques sur la signature partagée. Nous avons développé un calcul de superposition complet adapté au fragment de l'arithmétique considéré. Nous avons effectué plusieurs études de cas concernant le partage d'une arithmétique de comptage [TACAS09,FROCOS09-NiRiRu] (avec une opération d'incrémentation) et de la théories des groupes abéliens [CADE09-NiRiRu].

- Nous avons développé un nouveau cadre plus large de combinaison applicable à des théories disjointes qui ne sont pas nécessairement stablement infinies [FROCOS09-Fo]. Cette méthode s'appuie sur le calcul du spectre d'une formule (l'ensemble des cardinalités des modèles). Nous avons montré que le calcul de ce spectre est possible pour des fragments classiques de la logique du premier ordre tels que: la classe de Bernays-Schönfinkel-Ramsey, la classe de Löwenheim avec égalité, le fragment à deux variables, les fragments gardés.

- Nous avons amélioré la procédure de décision pour l'arithmétique du démonstrateur Alt-Ergo suivant plusieurs directions : 1) intégration d'un module d'arithmétique d'intervalles pour les entiers, coopérant avec le module déjà présent de Fourier-Motzkin sur les rationnels 2) intégration d'un traitement prédéfini pour les symboles Associatifs/Commutatifs 3) traitement partiel de l'arithmétique non-linéaire par la coopération des extensions 1. et 2. sur la multiplication entière 4) analyse par cas sur les entiers. Ces améliorations ont permis de décharger des obligations de preuves (identifiées lors de la tâche T1) jusqu'à présent hors de portée des prouveurs SMT de l'état de l'art.

- Pour l'arithmétique linéaire, nous avons aussi montré comment générer des témoins de preuve (cf tâche 4) en corrigeant les erreurs d'arrondi dues aux calculs flottants des outils de programmation linéaire [SMT2010-Be].

Pour la tâche T4, nous définissons un format de preuve générique pour les prouveurs SMT. Ce format a l'ambition de devenir un standard pour interfacer un SMT solveur avec des outils qui requièrent une preuve de non-satisfiabilité. Ces outils sont les assistants de preuve comme Coq ou Isabelle/HOL mais aussi les outils de vérification comme Frama-C et Rodin.
Le format de preuve est extensible et paramétré par des règles de déduction propres à chaque prouveur SMT. Un pas de preuve atomique est une règle de déduction qui produit une nouvelle clause conséquence logique de clauses données en argument. Le format de preuve structure la composition de ces pas de preuve atomiques. Il propose notamment des mécanismes pour (1) nommer des termes et (2) effectuer des preuves modulaires et imbriquées. Le premier point est

fondamental pour obtenir des preuves petites et le second point est compatible avec la structure modulaire des prouveurs SMT. Le format de preuve assure par construction la correction des preuves. Plus précisément, si toutes les règles de déduction sont correctes et que la preuve permet de déduire la clause vide (c-à-d faux) alors le problème est bien non-satisfiable.

Nous avons commencé l'étude de la compression des preuves, en s'intéressant d'abord aux preuves propositionnelles. Une méthode de compression générale, s'appuyant sur la représentation des preuves sous forme d'hypergraphes et sur la réécriture de graphe est en cours d'élaboration. Une version préliminaire de ce travail a été présentée au Workshop SMT [SMT10-FoMeWo].

Pour la tâche T5, nous travaillons à plusieurs approches pour intégrer prouver SMT et assistants de preuve (en particulier Coq).

- Nous avons terminé l'implémentation dans Coq d'une tactique réflexive pour la logique du premier ordre avec théories prédéfinies. Cette tactique est basée d'une part, pour la partie théorie, sur l'algorithme de combinaison de procédures de décision CC(X) et d'autre part, pour la partie purement propositionnelle, sur un solveur SAT à la DPLL qui manipule des formules CNF à l'aide d'une technique d'évaluation paresseuse [JFLA,FroCos09-LeCo].

- Nous avons terminé la partie SAT de l'intégration des SMT dans Coq [ITP2010b]. Nous sommes maintenant capables de remonter et de vérifier efficacement les traces de résolutions fournies par les SAT solveurs dans Coq. Nous avons récemment entamé l'intégration de la partie «théorie» des SMT. Dans un premier temps, nous nous sommes concentrés sur la combinaison «arithmétique linéaire» et «égalité» pour les formules universellement quantifiées. Une évaluation a montré que pour l'arithmétique linéaire, les procédures automatiques existantes dans Coq sont suffisantes pour traiter les problèmes habituellement rencontrés par les SMT. Pour l'égalité, nous avons commencé à développer un vérificateur de traces pour l'algorithme de clôture par congruence («congruence closure»).

Pour la tâche 6, nous développons un prototype d'infrastructure *proof-carrying code* (PCC) pour inférer et valider automatiquement des invariants numériques de programmes. Un point crucial de notre approche est que la *Trusted Computing Base* de l'infrastructure est programmée et prouvée correcte en Coq. Ainsi, quand l'infrastructure certifie qu'un programme possède la propriété d'être exempt de comportements indéfinis (par exemple divisions par zéro, ou accès hors des bornes de tableaux) nous construisons automatiquement un théorème Coq qui établit cette propriété. Dans ce cadre, nous étudions plusieurs approches qui font varier différentes dimensions telles que l'effort de preuve, le temps de vérification et la taille du certificat.
Pour le langage While, nous avons un interprète abstraite certifié en Coq qui est générique par rapport au domaine abstrait [ITP2010a]. Cet interprète ne requiert pas de certificat et a été instancié à des domaines numériques non-relationnels tels que signes, congruence ou intervalles.
Pour le byte-code Java, nous validons des invariants numériques linéaires calculés par des domaines relationnels tels que octogones et polyèdres [TGC2010]. Dans ce cas, nous utilisons une approche à base de certification de résultat qui requiert donc des certificats mais limite l'effort de preuve et accélère la vérification. De manière plus prospective, nous développons une théorie pour calculer et valider des invariants polynomiaux calculés par des bases de Gröbner.

Le but de la tâche 7 est l'intégration des procédures dans les outils Rodin et Frama-C.
Pour la plateforme Rodin, un premier prototype de traduction du langage mathématique Rodin vers le formalisme SMT a été développé pour l'arithmétique linéaire et la théorie des ensembles du premier ordre. Ce prototype a permis de réaliser un début d'intégration de quatre solveurs dans la plate-forme Rodin qui donne des résultats très encourageants. Ce travail est réalisé en étroite collaboration entre Systerel et Nancy.
Le CEA LIST a évalué le prouveur alt-ergo et cette évaluation se poursuit sur les nouvelles versions d'alt-ergo et les obligations de preuves générées par de nouveaux greffons de Frama-C. L'intégration de VeriT parmi les prouveurs supportés par la plate-forme Why est en cours. La remontée des résultats des prouveurs (trace de preuve ou contre-exemple) par Frama-C/Why vers le programme initial s'inscrit dans un cadre plus large de gestion globale d'une activité de vérification. À terme, il s'agira d'utiliser les informations des prouveurs pour affiner les relations de dépendances entre les propriétés exprimées sur le source. Les composants de base de cette fonctionnalité sont implantés.

## C.2 RESULTATS MARQUANTS (SI APPLICABLE)

Certification efficace des traces de résolution fournies par les SAT solveurs dans l'assistant de preuve Coq [ITP2010b].

Un prototype PCC pour du byte code Java, certifié en Coq, efficace et précis pour prouver de manière sûre l'absence d'accès hors des bornes des tableaux [TGC2010].

## C.3 REUNIONS DU CONSORTIUM (SI APPLICABLE)

| Date | Lieu | Partenaires présents | Thème de la réunion |
|---|---|---|---|
| 26-27/01/2009 | Rennes | Tous | Réunion de lancement |
| 23-24/06/2009 | Paris | Tous | Procédures de décision arithmétique & Réunion plénière |
| 25-26/11/2009 | Paris | Tous | Format de preuve & Réunion plénière |
| 28-29/06/2010 | Sophia | Tous | Format de preuve & Réunion plénière |
| 01-03/03/2010 | Nancy | Rennes,Nancy | Procédures de décision arithmétique |
| 14/07/2010 | Edimbourg, GB | Nancy, Rennes, Sophia | Formats de preuve |

## C.4 COMMENTAIRES LIBRES

### *Commentaire du coordinateur*

Le projet DECERT avance de façon satisfaisante tant au niveau scientifique qu'au niveau collaboratif, avec des collaborations entre sites et des réunions plénières riches en interaction. Un objectif de coordination sera de transformer ces collaborations en des publications communes. Un autre objectif sera de s'assurer que le budget (personnels et fonctionnement) sera utilisé avant la fin du projet.

### *Commentaire des autres partenaires*

### *Question(s) posée(s) à l'ANR*

# D IMPACT DU PROJET DEPUIS LE DEBUT.

## D.1 INDICATEURS D'IMPACT

### *Nombre de publications et de communications (à détailler en D.2)*

| | | Publications multipartenaires | Publications monopartenaires |
|---|---|---|---|
| **International** | **Revues à comité de lecture** | | |
| | **Ouvrages ou chapitres d'ouvrage** | | |
| | **Communications (conférence)** | | 13 |
| **France** | **Revues à comité de lecture** | | |
| | **Ouvrages ou chapitres d'ouvrage** | | |
| | **Communications (conférence)** | | 1 |
| **Actions de diffusion** | **Articles vulgarisation** | | |
| | **Conférences vulgarisation** | | |
| | **Autres** | | |

### *Autres valorisations scientifiques (à détailler en D.3)*

| | Nombre, années et commentaires (valorisations avérées ou probables) |
|---|---|
| **Brevets internationaux obtenus** | |
| **Brevet internationaux en cours d'obtention** | |
| **Brevets nationaux obtenus** | |
| **Brevet nationaux en cours d'obtention** | |
| **Licences d'exploitation (obtention / cession)** | |
| **Créations d'entreprises ou essaimage** | |
| **Nouveaux projets collaboratifs** | |
| **Colloques scientifiques** | |
| **Autres (préciser)** | Dépôt APP du logiciel Alt-Ergo v0.9<br>Distribution du solveur SMT veriT sous licence BSD |

## D.2 LISTE DES PUBLICATIONS ET COMMUNICATIONS

**Conférences internationales**


[TGC2010] Frédéric Besson, Thomas Jensen, David Pichardie and Tiphaine Turpin. Certified Result Checking for Polyhedral Analysis of Bytecode Programs. Trustworthy Global Computing 2010. LNCS, Springer, 2010.

[ITP2010a] David Pichardie and David Cachera. A certified denotational abstract interpreter. In *Proc. of International Conference on Interactive Theorem Proving (ITP'10)*, LNCS 6172, Springer, 2010.

[SMT2010-Be] Frédéric Besson : On using an inexact floating-point LP solver for deciding linear arithmetic in an SMT solver. Workshop SMT 2010.

[TACAS09] Enrica Nicolini, Christophe Ringeissen, Michaël Rusinowitch: Satisfiability Procedures for Combination of Theories Sharing Integer Offsets. TACAS 2009, LNCS 5505, 428-442, Springer

[FROCOS09-NiRiRu] Enrica Nicolini, Christophe Ringeissen, Michaël Rusinowitch: Data Structures with Arithmetic Constraints: A Non-disjoint Combination. FroCos 2009, LNCS 5749, pp 319-334. Springer.

[ITP2010b] Michaël Armand, Benjamin Grégoire, Arnaud Spiwack and Laurent Théry Extending Coq with Imperative Features and its Application to SAT Verification, In *Proc. of International Conference on Interactive Theorem Proving (ITP'10)*, LNCS 6172, Springer, 2010.

[FROCOS09-Fo] Pascal Fontaine: Combinations of Theories for Decidable Fragments of First-Order Logic. FroCos 2009, LNCS 5749, 263-278. Springer.

[CADE09-NiRiRu] Enrica Nicolini, Christophe Ringeissen, Michaël Rusinowitch: Combinable Extensions of Abelian Groups. CADE 2009, LNCS 5663, pp 51-66. Springer.

[CADE09] Thomas Bouton, Diego Caminha B. de Oliveira, David Déharbe, Pascal Fontaine: veriT: An Open, Trustable and Efficient SMT-Solver. CADE 2009, LNCS 5663, pp 151-156. Springer.

[SMT10-FoMeWo] Pascal Fontaine, Stephan Merz, Bruno Woltzenlogel Paleo: Exploring and Exploiting Algebraic and Graphical Properties of Resolution. Worskshop SMT 2010.

[PAAR10] Thomas Bouton, Diego Caminha B. de Oliveira, David Déharbe, Pascal Fontaine: GridTPT: a distributed platform for Theorem Prover Testing. Workshop on Practical Aspects of Automated Reasoning, 2010.

[FroCos09-LeCo] Stéphane Lescuyer et Sylvain Conchon. Improving Coq Propositional Reasoning Using Lazy CNF Conversion. FroCos'09, LNCS 5749, Springer 2009.

[ABZ] David Déharbe. Automatic Verification for a Class of Proof Obligation with SMT-Solvers, ABZ 2010, LNCS 5977 Springer.

**Conférences nationales**

[JFLA] Stéphane Lescuyer. Conteneurs de première classe en Coq. JFLA 2010, La Ciotat, France, 2010.

## D.3 LISTE DES ELEMENTS DE VALORISATION

Le solveur SMT veriT est distribué sous licence BSD. Il a été présenté à CADE [CADE09] et a participé aux compétitions 2009 et 2010. Il a obtenu la seconde place dans plusieurs catégories en 2010.

GridTPT, la plateforme de test de régression et d'évaluation de veriT est distribuée sous licence BSD. Elle a fait l'objet d'une présentation au Workshop PAAR de FLoC 2010 [PAAR10].

Nous avons réalisé le dépôt APP du logiciel Alt-Ergo v0.9
Nous avons participé au groupe de travail international sur le format de trace SMT

Le prototype d'intégration de solveurs SMT dans la plate-forme Rodin sera librement disponible sur le site SourceForge de la plate-forme Rodin d'ici la fin 2010

## D.4 PERSONNELS RECRUTES EN CDD (HORS STAGIAIRES)

| **Identification** | | | | **Avant le recrutement sur le projet** | | | **Recrutement sur le projet** | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Nom et prénom | Sexe H/F | Adresse email (1) | Date des dernières nouvelles | Dernier diplôme obtenu au moment du recrutement | Lieu d'études (France, UE, hors UE) | Expérience prof. antérieure (ans) | Partenaire ayant embauché la personne | Poste dans le projet (2) | Date de recrutement | Durée missions (mois) (3) |
| Li Pey-Yu | F | pei-yu.li@irisa.fr | 30/06/2010 | License | France | | Rennes | Vacataire | 01/02/2010 | 5 |
| Arthur Milchior | H | Arthur.milchior@ens.fr | 20/11/2009 | Deug | France | | Orsay | Vacataire | 15/06/2009 | 3 |
| Michael Armand | H | Michael.Armand@sophia.inria.fr | Contrat en cours | Master2 | France | | Sophia | Doctorant | 01/10/2009 | 36 |
| Thomas Bouton | H | thomas.bouton@gmail.com | 31/08/2010 | Ingénieur | France | | Nancy | Ingénieur | 1/09/2009 | 12 |

## D.5 ÉTAT FINANCIER

| Nom du partenaire | Crédits consommés (en %) | Commentaire éventuel |
|---|---|---|
| Rennes | 14.25% | Post-doc encore à recruter |
| Orsay | 16.47% | Post-doc encore à recruter |
| Systerel | 24.4% | Charge plus importante sur les deux dernières années |
| Sophia | 23.78% | DÉCERT AYANT COMMENCÉ EN JANVIER, NOUS N'AVONS PU RECRUTER NOTRE THÉSARD (MICHAËL ARMAND) QU'AU 1/10/2009, il y donc un décalage de 10 mois pour les dépenses relatives à cette thèse. La demande de prolongation de l'ANR pour couvrir ce décalage a déjà été acceptée. |
| CEA | 54% | |
| Nancy | 82 % | |

# E ANNEXES EVENTUELLES