Compte-rendu intermédiaire

Projet ANR-14-CE28-002

SOPRANO

Programme DS0704 201

Ce document est à remplir par le coordinateur en collaboration avec les partenaires du projet. Il doit être transmis par le coordinateur aux échéances prévues dans les actes attributifs :

1. *à l'ANR*
2. *aux pôles de compétitivité ayant accordé leur label au projet.*

L'ensemble des partenaires doit avoir une copie de la version transmise à l'ANR.

Il doit être accompagné d'un résumé public du projet mis à jour, conformément au modèle associé à ce document.

Ce modèle doit être utilisé uniquement pour le(s) compte(s)-rendu(s) intermédiaire(s) défini(s) dans les actes attributifs de financement, hors rapport T0+6 pour lequel il existe un modèle spécifique. Il existe également un modèle spécifique au compte-rendu final.

A Identification

Acronyme du projet	SOPRANO
Titre du projet	Nouveau prouveur automatique pour l'analyse de programmes
Coordinateur du projet (société/organisme)	CEA
Date de début du projet Date de fin du projet	14/01/15 – 14/07/18
Labels et correspondants des pôles de compétitivité (pôle, nom et courriel du corresp.)	Systematic Muriel SHAN SEI FAN <Muriel.SHANSEIFAN@systematic-paris-region.org>
Site web du projet, le cas échéant	soprano-project.fr

Rédacteur de ce rapport	
Civilité, prénom, nom	Mr François Bobot
Téléphone	+33 169089408 / +33 684658592
Courriel	François Bobot <francois.bobot@cea.fr>
Date de rédaction	27/06/2016
Période faisant l'objet du rapport d'activité	Mid-term report (14/07/18)

B Livrables et jalons

Quand le projet en comporte, reproduire ici le tableau des jalons et livrables fourni au début du projet. Mentionner l'ensemble des livrables, y compris les éventuels livrables abandonnés, et ceux non prévus dans la liste initiale.

N°	Intitulé	Nature*	Date de fourniture			Partenaires (souligner le responsable)
			Prévue initialement	Replanifiée	Livrée	
D1.1	Requirement analysis	Rapport	04/15		05/15	Adacore CEA
D6.2	ANR starting report (annulé par ANR)		07/15	Annulé		CEA
D1.2	Set of benchmarks	Données	10/15		04/16	Adacore CEA
D1.3	Benchmark Environment	Logiciel	01/16		04/16	OcamlPro CEA
D2.1	Survey of combination techniques	Rapport	01/16	09/16		UPSud CEA
D3.1	FPA Solver	Rapport	01/16	09/16		UPSud CEA
D4.1	Extension of Alt-Ergo I (FPA)	Logiciel	01/16		05/16	OcamlPro UPSud
D4.2	Preliminary implementation of the SOPRANO solver, roadmap	Logiciel	01/16		04/16	CEA
D6.3	Consortium agreement	CA	01/16	09/16		CEA + tous
D2.2	Combination framework I (first-class domain)	Rapport	07/16	09/16		Inria CEA UPSud

** jalon, rapport, logiciel, prototype, données, …*

C Rapport d'avancement

C.1 Objectifs initiaux du projet

Maximum 10 à 20 lignes.

The initial challenges identified in the proposal were :
- Chal1: identify a sweet spot of theory combination, going beyond Nelson-Oppen and its derivatives, with richer communication between theories and finer cooperation;
- Chal2: design effective and generic learning mechanisms suitable for both SMT-like and CP-like decision procedures, and identify the right compromise between propagation and learning;
- Chal3: address several industry-relevant and hard-to-solve theories, including floating-point arithmetic, nonlinear arithmetic, and bitvectors;

- Chal4: understand how quantifiers can be handled in our synthesis-based cooperation framework.

Since implementing a new solver takes time, the roadmap proposed was to experiment in already existing provers approach for hard-to-solve theories.

C.2 Travaux effectués et résultats atteints sur la période concernée

Maximum 1 page. Travaux et résultats obtenus pendant la période concernée, conformité de l'avancement des travaux avec le plan initialement prévu. Prévision de travaux pour la (les) prochaine(s) période(s).

The work of the consortium focused first on **floating-point numbers** because **Adacore provided very neat examples** of problems found in programs that were not currently solved by SMT solvers used by Adacore. We tried the CP (Constraint Programming) library Colibri (CEA) and the tool for automatic proof generation of arithmetic properties Gappa (INRIA) on these examples. We found that not only the simplest ones (proved using domain propagation) were proved but also more difficult ones that need more symbolic reasoning. By giving manually specific hints to Gappa, **nearly all the examples are proved**. The automation has been achieved through experimentation in the Colibri library and discussion about interesting mathematical properties of floating-point operators. At the end the Colibri library is able to prove the correction of vector normalization functions which use a floating-point square root and division. During this time, techniques similar to the one used in Gappa have been implemented in the Alt-Ergo prover.

The solver **Alt-Ergo gained the ability to handle floating points** using inspiration from the Gappa solver. The floating points are modeled with reals but with a built-in notion of over-approximation of its floating-point interval, and built-in computation of the rounding of constants. The reasoning is done, like in Gappa and Colibri, by propagation; however contrary to them instead of being hard coded they are **expressed in the Alt-Ergo high-level input language** as lemmas with semantic triggers. Semantic triggers are a new extension of usual triggers used by SMT solvers.

In parallel since January 2016, handling of **bitvector** has been tackled in the **SOPRANO-solver and in Colibri**. The main advantage of the Colibri implementation compared to previous SMT techniques is the **communication between the bit-vector constraints and the integer constraints**.

Since the Colibri library seems so efficient, we wanted to compare it with other solvers. It has been turned into a standalone prover which accepts the **SMTLIB2 language with the support for the integer, the real, the floating-point and the bit-vector theories**. Results were very promising compared to Z3 and the toolchain from Ada to Colibri is going to be finalized soon.

All projects for building provers have some kind of benchmarking tools but different from each other. In SOPRANO, the goal has been to **release this benchmarking tool**, called **OCI**, and to make it as versatile as possible. Its main selling point is the possibility to **compile, run and compare any git versions** and to **manage dependencies** of the tools (for example to check that a new version of the compiler doesn't cause major regressions). At the end its versatility allows to use it for the continuous integration of the Frama-C platform (ANR CAT, ANR U3CAT) and all

its plugins. There are discussion about using it for testing the proof assistant Coq and all its contributions.

Some members of the project are chairing the CP Meets Verification 2016 Workshop which aims at fostering lively discussions and debates about the use of CP tools for program verification and the relation between CP and SMT (Sat Modulo Theory) solvers.

So all the planned technical milestones have been reached, and others not planned such as Colibri usable freely by academics as a standalone prover. However reports are slightly of schedule and the new techniques developed have not yet been published. From the identified challenges the Chal3 is well underway. Solutions for the challenges Chal1 and Chal2 are currently tried and tested in the SOPRANO solver.

C.3 Difficultés rencontrées et solutions

Maximum 10 à 20 lignes. Difficultés éventuelles rencontrées et solutions de remplacement envisagées ex : impasse technique, abandon d'un prestataire, maîtrise des délais, maîtrise des budgets. Faut-il revoir le contenu du projet ? Faut-il revoir le calendrier du projet ?

The consortium agreement is behind schedule. The final version has been sent to all partners for signature and most of them signed it.

C.4 Faits et résultats marquants

En quelques lignes pour chaque fait ou résultat marquant. Cet élément pourrait donner lieu à communication, après accord du coordinateur du projet.

- OCI: released and available on GitHub
- Colibri standalone prover with SMTLIB input language ready to participate in SMT-COMP
- Colibri combine floating points, bitvectors, bounded signed and unsigned integers
- Alt-Ergo with floating points handling and generic semantic triggers framework

C.5 Travaux spécifiques aux entreprises (le cas échéant)

Entreprise AdaCore

Entreprise	AdaCore
Rédacteur (nom + adresse mél)	Claire Dross dross@adacore.com

During the project, existing tools, Colibri and Alt-Ergo, have been improved to better handle verification conditions coming from the verification of SPARK programs. These improvements include in particular the support of floating-point arithmetic inside Alt-Ergo. This implementation will be beneficial to our users, since floating-point arithmetic is one of the most important limitations of the GNATprove tool. Development has already been done in the tool to take advantage of specific support for floating-point arithmetic in SMT solvers but this has not been integrated yet because of the lack of efficient implementations in the solvers we use (Z3, CVC4, and Alt-Ergo).

In the same way, since Colibri now supports SMTLIB2 syntax, work has started to try and integrate it as a backend of the GNATprove tool. From the experiments done on small examples during the project, we hope for interesting results from this integration, especially regarding conversions between floating-point numbers, bitvectors and mathematical integers.

Entreprise OCamlPro

Entreprise	OCamlPro
Rédacteur (nom + adresse mél)	Mohamed Iguernlala <iguer.pro@gmail.com>

Concernant Alt-Ergo, un premier prototype d'intégration d'un raisonnement flottant dans le solver a été développé. Cette première tentative, bien que prometteuse sur le papier, a été très difficile à faire évoluer. En effet, elle s'attaquait à la fois à l'intégration du raisonnement flottant dans Alt-Ergo et à l'efficacité maximale d'une telle intégration. Un second prototype, beaucoup plus modulaire et facile à étendre, apportant des modifications minimales et maîtrisées à Alt-Ergo, est en cours de développement. Les premiers résultats obtenus sont plutôt encourageants. Ce travail est effectué en étroite collaboration avec nos partenaires au Laboratoire de Recherche en Informatique.

Le second axe exploré coté Alt-Ergo est la génération de contre-exemples pour les formules qui ne sont pas prouvés valides. Le prototype implémentant cette extension est à un stade très avancé et est déjà fonctionnelle. Il reste néanmoins quelques questions d'ingénierie et d'autres d'ordre théorique à aborder avant d'envisager une intégration dans la version principale d'Alt-Ergo.

Le LRI et OCamlPro ont également collaboré avec l'ONERA pour explorer l'intégration d'optimisation semi-définie positive dans Alt-Ergo afin de traiter une certaine classe de problèmes d'arithmétique non-linéaire. Les expérimentations sur une suite de tests issue du domaine de l'avionique montrent que l'approche est intéressante et permet de résoudre des problèmes qu'aucun autre solveur SMT de l'état de l'art n'arrive à prouver.

C.6 Réunions du consortium (projets collaboratifs)

Date	Lieu	Partenaires présents	Thème de la réunion
14/01/2015	CEA	All	Kick-off
05/06/2015	CEA	All	Floating points
08/06/2015	CEA	All	Non-linear arithmetic
07/10/2015	UPSUD	CEA, UPSUD	Floating points in Alt-Ergo
08/01/2016	CEA	All	OCI; Improvements on floating points
01/07/2016	Adacore	All	Floating points; Bitvectors; Models; SOPRANO prover

C.7 Commentaires libres

Commentaires du coordinateur

Commentaire général à l'appréciation du coordinateur, sur l'état d'avancement du projet, les interactions entre les différents partenaires…

…

Commentaires des autres partenaires

Éventuellement, commentaires libres des autres partenaires

…

Question(s) posée(s) à l'ANR

Éventuellement, question(s) posée(s) à l'ANR…

…

D VALORISATION ET IMPACT DU PROJET DEPUIS LE DÉBUT

Cette partie rassemble des éléments cumulés depuis le début du projet qui seront suivis tout au long de son avancée, et repris dans son bilan final.

D.1 PUBLICATIONS ET COMMUNICATIONS

Citer les publications résultant du projet en utilisant les normes habituelles du domaine. Si la publication est accessible en ligne, préciser l'adresse. L'ANR encourage, dans le respect des droits des co-auteurs et des éditeurs, à publier les articles résultant des projets qu'elle finance dans l'archive ouverte pluridisciplinaire HAL :
***Attention** : éviter une inflation artificielle des publications, mentionner uniquement celles qui résultent directement du projet (postérieures à son démarrage, et qui citent le soutien de l'ANR et la référence du projet).*

Liste des publications multipartenaires (résultant d'un travail mené en commun)		
International	**Revues à comité de lecture**	1. 2.
	Ouvrages ou chapitres d'ouvrage	1. 2.
	Communications (conférence)	1. 2.
	Technical Reports or Publications in Progress	1. Sylvain Conchon, Evelyne Contejean, Mohamed Iguernlala: Reconstructing Shostak for Parametric Theories 2. Pierre Roux, Sylvain Conchon, Mohamed Iguernlala: Solving Non-Linear Arithmetic: a Numerical Alternative
France	**Revues à comité de lecture**	1. 2.
	Ouvrages ou chapitres d'ouvrage	1. 2.
	Communications (conférence)	1. 2.
Actions de diffusion	**Articles de vulgarisation**	1. 2.
	Conférences de vulgarisation	1. 2.
	Autres	1. 2.

Liste des publications monopartenaires (impliquant un seul partenaire)		
International	**Revues à comité de lecture**	1. 2.
	Ouvrages ou chapitres d'ouvrage	1. 2.

	Communications (conférence)	1. Quentin Plazar: Adding Symbolic Reasoning to FD with Arrays for Attacking SMTlib Formulae, Workshop SweConsNet 2016 2. Quentin Plazar: Symbolic Reasoning for Constraint Solvers with Arrays, doctoral program CP 2016 3. Zakaria Chihani: Tight coupling between bit-vector and integer domains can surpass bit-blasting SMT solvers, Workshop CP meets Verif. 2016
	Technical Reports or Publications in Progress	1. Zakaria Chihani: Efficient tight coupling between bit-vector and integer domains
France	**Revues à comité de lecture**	1. 2.
	Ouvrages ou chapitres d'ouvrage	1. 2.
	Communications (conférence)	1. François Bobot: OCI - For All Your Continuous Integration and Benchmarking Needs, Ocaml User in PariS 16/02/16 2.
Actions de diffusion	**Articles de vulgarisation**	1. 2.
	Conférences de vulgarisation	1. 2.
	Autres	1.

D.2 Autres éléments de valorisation

Les éléments de valorisation sont les retombées autres que les publications. On détaillera notamment :

- *brevets nationaux et internationaux, licences, et autres éléments de propriété intellectuelle consécutifs au projet.*
- *logiciels et tout autre prototype*
- *actions de normalisation*
- *lancement de produit ou service, nouveau projet, contrat,…*
- *le développement d'un nouveau partenariat,*
- *la création d'une plate-forme à la disposition d'une communauté*
- *création d'entreprise, essaimage, levées de fonds*
- *autres (ouverture internationale,..).*

Ce tableau détaille les brevets nationaux et internationaux, licences, et autres éléments de valorisation consécutifs au projet, du savoir-faire, des retombées diverses en précisant les partenariats éventuels. Voir en particulier celles annoncées dans l'annexe technique.

Liste des éléments. Préciser les titres, années et commentaires	
Brevets internationaux obtenus	1. 2.
Brevet internationaux en cours d'obtention	1. 2.
Brevets nationaux obtenus	1. 2.
Brevet nationaux en cours d'obtention	1. 2.
Licences d'exploitation (obtention / cession)	1. 2.
Créations d'entreprises ou essaimage	1. 2.
Prototype/Logiciels	1. Plateform of continuous integration and benchmarking: OCI (OCaml, LGPL) 2. Colibri (Prolog, Freeware pour académique) 3. Alt-Ergo with floating points support (OCaml, Cecill-C) 4. Alt-Ergo with Semidefinite programming (OCaml) 5. ocplib-simplex: a library for simplex solver (OCaml, LGPL) 6. SOPRANO provers currently called Popop (OCaml, LGPL)
Nouveaux projets collaboratifs	1. 2.
Colloques scientifiques	1. Arnaud Gotlieb, Sébastien Bardin: Program Chairs of CP 2016

	2. Sébastien Bardin, Bobot François: Program Chairs CP Meets Verification 2016 3. Sylvain Conchon : Program Chair of ICFEM 2015 4. Sylvain Conchon : invited talk at UITP 2016
Autres (préciser)	1. Sylvain Conchon : co-organiser of the SMT competition 2016

D.3 Pôles de compétitivité (projet labellisés)

Pour les projets labellisés par un ou plusieurs pôles de compétitivité,

Collaboration du projet avec le(s) pôle(s) ayant labellisé

Quelles collaborations y a-t-il eu entre votre projet et le(s) pôle(s) de compétitivité l'ayant labellisé ?

…

Activités financées par le complément de pôle (laboratoires publics uniquement)

Détailler les activités réalisées par les laboratoires publics avec le complément de financement accordé au titre de la labellisation. Préciser notamment les partenaires impliqués et la collaboration menée avec le ou les pôles.

Montant du complément accordé par l'ANR (pour chaque labo public)	- Partenaire XXX : xxx € - Partenaire YYY : yyy €

Type d'action menée	Détails (exemples non limitatifs)	Dépenses complément de pôle*
Actions contribuant à la réflexion stratégique et à la programmation scientifique du pôle	Ex : Participation aux journées thématiques organisées par le pôle	Xxx : xxy € Yyy : yyy €
Actions de communication scientifique et publique bénéficiant à la notoriété du pôle	Ex : colloque de projets	Xxx : xxy € Yyy : yyy €
Développement de la recherche partenariale (recherche de partenaires, frais de gestion du partenariat, ingénierie de projets,…)	Ex : accord de consortium, frais de formation à la propriété intellectuelle, à la gestion de projets, dépenses relatives au montage du projet	Xxx : xxy € Yyy : yyy €
Valorisation de la recherche et transfert vers le monde industriel	Ex : étude de brevetabilité	Xxx : xxy € Yyy : yyy €

* Estimation des dépenses imputées sur le complément de financement accordé au titre de la labellisation par un pôle de compétitivité, partenaires publics seulement.

D.4 Personnels recrutés en CDD (hors stagiaires)

Ce tableau dresse le bilan du projet en termes de recrutement de personnels non permanents sur CDD ou assimilé. Renseigner une ligne par personne embauchée sur le projet quand l'embauche a été financée partiellement ou en totalité par l'aide de l'ANR et quand la contribution au projet a été d'une durée au moins égale à 3 mois, tous contrats confondus, l'aide de l'ANR pouvant ne représenter qu'une partie de la rémunération de la personne sur la durée de sa participation au projet.
Les stagiaires bénéficiant d'une convention de stage avec un établissement d'enseignement ne doivent pas être mentionnés.

Des données complémentaires sur le devenir professionnel des personnes concernées seront demandées à la fin du projet. Elles pourront faire l'objet d'un suivi jusqu'à 5 ans après la fin du projet.

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)

Quentin PLAZAR	H		Toujours en poste	Diplôme d'ingénieur (Supélec)	France	0	Inria	Doctorant	01/10/2015	36
Kailiang Ji	H		Toujours en poste	PhD	France	0	UPSUD	Post-Doc	01/11/2015	12

Aide pour le remplissage

(1) Adresse email : indiquer une adresse email la plus pérenne possible
(2) Poste dans le projet : post-doc, doctorant, ingénieur ou niveau ingénieur, technicien, vacataire, autre (préciser)
(3) Durée missions : indiquer en mois la durée totale des missions (y compris celles non financées par l'ANR) effectuées ou prévues sur le projet

Les informations personnelles recueillies feront l'objet d'un traitement de données informatisées pour les seuls besoins de l'étude anonymisée sur le devenir professionnel des personnes recrutées sur les projets ANR. Elles ne feront l'objet d'aucune cession et seront conservées par l'ANR pendant une durée maximale de 5 ans après la fin du projet concerné. Conformément à la loi n° 78-17 du 6 janvier 1978 modifiée, relative à l'Informatique, aux Fichiers et aux Libertés, les personnes concernées disposent d'un droit d'accès, de rectification et de suppression des données personnelles les concernant. Les personnes concernées seront informées directement de ce droit lorsque leurs coordonnées sont renseignées. Elles peuvent exercer ce droit en s'adressant l'ANR (http://www.agence-nationale-recherche.fr/Contact).

D.5 État financier

Donner un état indicatif de la consommation des crédits par les partenaires. Indiquer la conformité par rapport aux prévisions et expliquer les écarts significatifs éventuels.

Nom du partenaire	Crédits consommés (en %)	Commentaire éventuel
Inria	25	The thesis started late but will finish on time
AdaCore	40	
OcamlPro	40	
UPSUD	27	
CEA	45	

E Annexes éventuelles