INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Projet LANDE

Logiciel : analyse et développement

Rennes

THÈME 2A

Table des matières

1. Composition de l'équipe

Responsable scientifique
Thomas Jensen [CR CNRS]

Assistante de projet
Catherine Godest [TR CNRS]

Personnel Inria
Pascal Fradet [CR]
Florimond Ployette [IR, Atelier]

Personnel Université Rennes 1
Olivier Ridoux [professeur]
Thomas Genet [maître de conférences]
Erwan Jahier [Ater jusqu'en septembre 2001]
Siegfried Rouvrais [Ater jusqu'en septembre 2001]

Personnel Insa
Mireille Ducassé [professeur]

Chercheurs doctorants
Frédéric Besson [allocataire MENRT]
Thomas Colcombet [allocataire ENS, jusqu'en juin 2001]
Marc Éluard [boursier Inria]
Sébastien Ferré [boursier CNRS/RÉGION]
Lakshminarayanan Renganarayanan [boursier Inria, jusqu'en juin 2001]
Yoann Padioleau [allocataire MENRT]
Jean-Philippe Pouzol [boursier Inria]
Valérie Viet Triem Tong [allocataire MENRT]
Thomas de Grenier de Latour [allocataire MENRT, depuis octobre 2001]
Thomas Lefort [boursier Inria, depuis octobre 2001]

Chercheur post-doctorant
François Monin [ingénieur expert]

Collaborateur extérieur
Jacques Noyé [depuis juillet 2001]

2. Présentation et objectifs généraux du projet

2.1. (Sans titre)

Le thème de recherche central du projet Lande est la conception d'outils d'aide au développement et à la validation de logiciels. Notre approche est fondée sur une collection de méthodes formelles permettant de spécifier ou d'extraire une **vue partielle** de l'architecture et du comportement d'un logiciel. Cette approche nous a amenés à étudier deux types de problèmes. D'une part, la spécification d'un logiciel en vues partielles nécessite une vérification de la **cohérence** entre plusieurs vues afin que celles-ci puissent être synthétisées. D'autre part, l'extraction d'une vue demande des techniques d'analyse statique et dynamique précises. Nous insistons sur la nécessité que les réponses apportées à ces problèmes reposent sur des bases formelles (sémantique du langage étudié, définitions de propriétés à vérifier dans des logiques formelles) afin d'obtenir une garantie sur les résultats produits. De plus, il est important que les outils construits soient le plus automatiques possible car les utilisateurs visés ne sont pas nécessairement des experts en méthodes formelles.

Lande est un projet commun avec le CNRS, l'Université de Rennes 1 et l'Insa de Rennes.

2.1.1. Axes de recherche

La **description multi-vues** de l'architecture de gros logiciels a comme objectif de spécifier l'organisation globale de systèmes afin d'améliorer la maîtrise de leur développement (spécification, analyse, programmation, test, maintenance, etc.). Une ambition majeure dans ce domaine est le passage à l'échelle de techniques comme l'analyse, le raffinement ou la vérification de programmes. Nos travaux visent à assurer une forme de cohérence de ces descriptions hétérogènes. Le défi principal est de trouver comment mettre en relation des vues qui mettent en jeu des propriétés de nature très différentes ou qui se situent à des niveaux d'abstraction différents. Une fois les vues mises en relation, il devient possible d'utiliser des techniques standards d'analyse statique ou de vérification afin d'assurer des propriétés de cohérence.

La nouvelle technique de programmation appelée « **programmation par aspects** » consiste à décrire un logiciel comme un ensemble formé d'un composant principal et d'une collection de vues ou d'**aspects** décrivant des tâches comme la gestion mémoire, la synchronisation, les optimisations, etc. Un outil, appelé tisseur, est chargé de produire automatiquement un programme intégrant les différents aspects au composant principal. L'intérêt de cette approche est de localiser (dans les aspects) des choix de mise en oeuvre qui seraient sinon dispersés dans le code source. Après avoir proposé un aspect dédié à la sécurisation de code mobile, nous avons étudié les problèmes d'interactions qui se posent lorsque l'on doit tisser plusieurs aspects. En effet, comme pour les vues, les aspects ne sont pas obligatoirement orthogonaux et des conflits ou ambiguïtés peuvent apparaître lors du tissage. Nous travaillons également sur un langage d'aspect dédié à la composition de composants.

Pour faciliter la navigation et l'organisation de logiciels de taille importante nous cherchons à définir **un cadre logique pour les systèmes d'information** qui décrit uniformément la navigation, l'interrogation et l'analyse des données. Ce cadre est générique par rapport à la logique utilisée pour naviguer et interroger ; en particulier il peut être appliqué à plusieurs types de logiques de programme, comme les types ou des propriétés statiques. Ces travaux se basent sur une extension de la théorie de l'analyse de comcepts.

La validation d'un logiciel utilisent des méthodes d'**analyses et de test de programmes**. Nous nous intéressons à différents aspects de l'**analyse statique** de programmes, aussi bien sur le plan des fondements (spécification d'analyses à partir de règles d'inférence) que des applications (détection des pointeurs pendants pour l'aide à la mise au point de programmes C, analyse de flot de données et de contrôle dans des programmes Java et Java Card, analyse de protocoles cryptographiques) et à la mise en oeuvre d'analyses statiques par des techniques de résolution itérative de systèmes d'équations et de réécriture d'automates d'arbres.

Pour faciliter l'**analyse dynamique** de programmes, nous développons un outil d'analyse de traces d'exécution permettant à l'utilisateur d'exprimer des requêtes dans un langage de programmation logique. Ces requêtes peuvent être traitées à la volée, ce qui permet d'analyser des traces de grande taille. L'outil peut être utilisé pour le débogage de programmes séquentiels et nous étudions maintenant son application au problème de la détection d'intrusion.

En collaboration avec la société AQL nous poursuivons le développement de l'outil Casting dont le noyau utilise une méthode de **génération de suites de tests**. L'outil peut prendre des entrées dans des formats variés et produit des suites de tests selon des stratégies spécifiées par l'utilisateur. Nous adaptons actuellement Casting pour la génération de suites de test à partir de spécifications UML.

La **sécurité logicielle** constitue un domaine d'application privilégié pour le projet. Nous élaborons un cadre pour la définition de propriétés de sécurité et une technique pour leur vérification automatique. Cette technique intègre des techniques d'analyses statiques et de vérification de modèle (« **model checking** »). Ce cadre a été appliqué à la formalisation et la vérification de politiques de sécurité d'applications programmées avec la nouvelle architecutre de sécurité de Java 2 et à la vérification de propriétés de sécurité des cartes à puce multi-applicatives programmées avec le langage Java Card.

3. Fondements scientifiques

3.1. (Sans titre)

Une caractéristique importante des méthodes proposées dans le projet Lande est de reposer sur des bases formelles. S'agissant des langages de programmation, ces bases peuvent être fournies de différentes manières par ce qu'on appelle des **sémantiques**. Ces sémantiques sont ensuite utilisées pour définir des **analyses de programmes** qui permettent d'extraire des informations à partir du code des programmes (analyse statique) ou d'une trace d'exécution (analyse dynamique). Les analyses peuvent avoir différentes applications et celles qui intéressent au premier chef le projet Lande sont l'aide à la mise au point ou **débogage** de programmes et le **test de logiciels**. Ces applications ne concernent pas un langage de programmation spécifique mais la validation des programmes peut être notoirement simplifiée si on peut imposer une discipline de programmation **a priori**. Les langages de haut niveau, en particulier les **langages déclaratifs** peuvent être vus comme un moyen d'introduire une telle discipline.

3.2. Sémantique des langages de programmation

Mots clés : *sémantique, sémantique dénotationnelle, sémantique opérationnelle.*

La sémantique d'un langage de programmation s'attache à donner un sens mathématique aux programmes. Il existe différentes méthodes formelles de définition de sémantique comme les méthodes opérationnelle et dénotationnelle. Une sémantique dénotationnelle attribue un sens aux programmes d'un langage en associant à chaque construction syntaxique du langage une valeur dans un domaine de définition. Une sémantique opérationnelle donne un sens aux programmes en terme d'étapes de calcul (ou réécritures). Quel que soit son mode de définition, une sémantique permet d'ôter toute ambiguïté dans la définition d'un langage de programmation. Elle peut aussi fournir une base pour des techniques de manipulation formelle de programmes : preuves de propriétés de correction, analyse, transformation. C'est dans cette optique que les sémantiques de langages sont utilisées dans le projet Lande.

La sémantique d'un langage de programmation s'attache à donner un sens mathématique aux programmes. Il existe différentes méthodes formelles de définition de sémantique comme les méthodes axiomatique, algébrique, opérationnelle ou dénotationnelle. Nous présentons ici les méthodes dénotationnelle et opérationnelle sur un langage très simple d'expressions arithmétiques :

$$E \ ::= \ N \ \mid \ E_1 \ + \ E_2 \qquad \text{où } N \text{ représente un entier}$$

3.2.1. Sémantiques dénotationnelles

Une sémantique dénotationnelle [Sch86] attribue un sens aux programmes d'un langage à l'aide d'une fonction qui associe à chaque construction syntaxique du langage une valeur dans un domaine de définition. La sémantique d'une expression est construite à partir de celle de ses sous-expressions ; on dit que la sémantique est compositionnelle. La technique de preuve classique quand on travaille avec de telles sémantiques est la récurrence sur la structure (**structural induction**).

En prenant les entiers naturels **Nat** comme domaine sémantique et la fonction **Plus** : **Nat** $\times$ **Nat** $\longrightarrow$ **Nat**, la sémantique dénotationnelle de notre langage se décrit comme suit :

ε	:	Expression $\longrightarrow$**Nat**
$\varepsilon\,[N]$	=	$Val(N)$
$\varepsilon\,[E_1 \ + \ E_2]$	=	**Plus** $(\,\varepsilon\,[E_1], \varepsilon\,[E_2])$

Dans la deuxième ligne de cet exemple, il est important de noter la distinction entre le symbole N, qui dénote un élément de syntaxe du langage, et $Val(N)$ qui représente la valeur correspondant à N dans l'ensemble **Nat**. Sur ce langage élémentaire, la sémantique dénotationnelle apparaît presque comme une paraphrase de la syntaxe. Ce n'est plus le cas pour des langages plus réalistes. Par exemple, la sémantique d'un langage impératif classique encode à l'aide de fonctions un environnement, une mémoire et le flot de contrôle ; la

sémantique d'un programme récursif est la plus petite solution de l'équation qui le définit (**plus petit point fixe**).

3.2.2. Sémantiques opérationnelles

Les sémantiques opérationnelles donnent un sens aux programmes en terme d'étapes de calcul (ou réécritures). Nous présentons ici deux styles de sémantiques opérationnelles : les sémantiques opérationnelles structurelles et les sémantiques naturelles.

Une **sémantique opérationnelle structurelle** (SOS) [NN92] est un système composé d'axiomes et de règles d'inférence qui décrit le comportement du programme en terme d'étapes élémentaires de calcul (on parle de sémantique à petits pas). La technique de preuve classique associée à ce type de sémantique est la récurrence sur le nombre d'étapes de calcul.

La SOS de notre langage se décrit à l'aide d'un axiome et de deux règles d'inférence :

$$N_1 + N_2 \Longrightarrow N \text{ où } N \text{ est la somme de } N_1 \text{ et } N_2$$

$$\frac{E_1 \Longrightarrow E_1'}{E_1 \ + \ E_2 \Longrightarrow E_1' \ + \ E_2} \qquad \frac{E_2 \Longrightarrow E_2'}{N \ + \ E_2 \Longrightarrow N \ + \ E_2'}$$

Une règle d'inférence est constituée d'hypothèses (partie haute) et de conclusions (partie basse). Dans cet exemple, N dénote une expression complètement réduite (c'est à dire un entier) et E_i des expressions quelconques. La seconde règle ne peut donc s'appliquer que si l'expression à gauche du symbole $+$ a déjà été calculée, ce qui impose un ordre d'évaluation des arguments « gauche-droite ».

Une **sémantique naturelle** [Kah87] décrit le comportement du programme par un arbre de dérivation décrivant le calcul de ses composants. Elle ne fait apparaître que les réductions des expressions en leur résultat final (leur forme normale). On parle de sémantique à grands pas et la technique de preuve associée est la récurrence sur les arbres de dérivation.

La sémantique naturelle de notre langage se décrit comme suit.

$$N \Longrightarrow N \qquad \frac{E_1 \Longrightarrow N_1 \quad E_2 \Longrightarrow N_2}{E_1 \ + \ E_2 \Longrightarrow N} \quad \text{où } N \text{ est la somme de } N_1 \text{ et } N_2$$

Contrairement à la SOS précédente, cette sémantique n'impose pas d'ordre d'évaluation particulier entre E_1 et E_2. Les sémantiques naturelles permettent de cumuler certains avantages des SOS et des sémantiques dénotationnelles : comme les premières, elles fournissent des informations sur les étapes de calcul, ce qui facilite la définition d'un certain nombre d'analyses ; comme les secondes, elles déterminent le sens d'une expression en fonction de ceux de ses sous-expressions. Cette forme de compositionnalité facilite les raisonnements sur les programmes.

Quel que soit son mode de définition, une sémantique permet d'ôter toute ambiguïté dans la définition d'un langage de programmation. Elle peut aussi fournir une base pour des techniques de manipulation formelle de programmes : preuves de propriétés de correction, analyse, transformation. C'est dans cette optique que les sémantiques de langages sont utilisées dans le projet Lande.

3.3. Analyse de programmes

Mots clés : *analyse dynamique, analyse statique, sémantique, interprétation abstraite, compilation optimisante.*

Glossaire

Interprétation abstraite L'interprétation abstraite est un cadre permettant de relier différentes interprétations sémantiques d'un programme. Souvent, l'interprétation abstraite sert à montrer la correction d'une analyse, présentée comme une définition de la sémantique d'un langage sur un ensemble de propriétés « abstraites » (par rapport à la sémantique standard du langage).

Itération de points fixes Le résultat d'une analyse est souvent donné comme la solution d'une équation $x = f(x)$ où f est une fonction monotone sur un ordre partiel. Le théorème de Knaster-Tarski indique un algorithme pour trouver un tel point fixe en calculant la limite de la suite itérative $f^n(\bot)$ où $\bot$ désigne l'élément le plus petit dans l'ordre partiel.

L'analyse de programmes désigne l'ensemble des techniques qui permettent de déduire mécaniquement des propriétés des programmes. Ses principaux domaines d'application sont la compilation et l'aide à la mise au point de programmes. Comme exemples d'analyses existantes, nous pouvons citer l'analyse d'alias, le **slicing**, les analyses de dépendances. Une analyse peut être dynamique, elle porte alors sur une trace d'exécution particulière, ou statique, et valable pour toute exécution de programme. Dans les deux cas, sa correction doit être assurée, ce qui signifie que les informations qu'elle procure doivent être cohérentes avec la sémantique du programme analysé.

L'analyse de programmes désigne l'ensemble des techniques qui permettent de déduire mécaniquement des propriétés des programmes. Ses principaux domaines d'application sont la compilation et l'aide à la mise au point de programmes.

- Les analyses de flots de données qui permettent de détecter notamment les variables inutiles ou les expressions calculées à un point de programme donné.
- Les analyses d'alias qui produisent des informations sur le partage entre variables dans les langages à manipulation explicite de pointeurs.
- Les analyses de nécessité qui identifient les arguments qui sont indispensables à l'évaluation d'une fonction.
- Les analyses de mode qui déterminent le degré d'instanciation des variables dans les prédicats logiques.
- Le filtrage de programmes (**slicing**) qui consiste à identifier les instructions d'un programme nécessaires au calcul de variables données.

On distingue deux classes d'analyses : les analyses dynamiques et les analyses statiques. L'analyse dynamique déduit des propriétés d'un programme à partir d'une trace d'exécution particulière [BGL93]. En revanche, l'analyse statique [NNH99] permet d'établir des propriétés satisfaites par un programme pour toutes ses exécutions. L'information recherchée est en général incalculable ou d'une complexité importante. Une analyse statique ne peut donc calculer qu'une approximation de la solution idéale. En conséquence, les résultats de l'analyse statique sont moins précis mais plus généraux que ceux fournis par une analyse dynamique.

La conception d'une analyse comprend deux phases : la spécification et l'implantation. L'analyse doit être spécifiée d'une manière qui permet de prouver sa correction ; celle-ci garantit la cohérence du résultat de l'analyse par rapport à la sémantique du langage (cf module 3.2). La correction et la précision des analyses ont été étudiées de manière extensive dans le cadre de l'interprétation abstraite [Cou97]. Le résultat de cette première phase de conception d'analyse est souvent un système d'équations récursives dont la solution décrit les propriétés recherchées. On dispose d'algorithmes itératifs pour résoudre ce système d'équations (« itérateurs de points fixes »). On peut également s'appuyer sur des calculs formels sur l'algèbre des propriétés étudiées (calcul symbolique) afin d'améliorer l'efficacité de la résolution.

3.4. Débogage

Mots clés : *environnement de programmation*, *analyse de programme*, *sémantique*.

Glossaire

Erreur Une erreur est une action humaine qui fait qu'un résultat incorrect est produit par un programme. Par exemple, une erreur peut être d'intervertir deux variables A et B.

Faute Une faute est une étape, un processus ou une définition de données erronés dans un programme. Une erreur peut générer une ou plusieurs fautes. Par exemple, une faute induite par l'erreur citée plus haut peut être qu'un test d'arrêt d'une boucle se fait sur A qui n'est pas mise à jour.

Panne Une panne est l'incapacité d'un programme à effectuer ses fonctionnalités requises. Une faute peut générer une ou plusieurs pannes [ANS]. Un exemple de panne résultant de la faute citée plus haut est que le programme ne termine pas.

Le débogage consiste à localiser et corriger les fautes qui sont responsables des pannes logicielles. Le débogage est une activité cognitive complexe qui nécessite, en général, de remonter jusqu'à l'erreur humaine pour comprendre les raisons des fautes qui ont engendré les pannes.

Il existe des outils, communément appelés **débogueurs**, qui aident le programmeur à identifier les comportements non-attendus du programme. Ces outils donnent une image (appelée **trace**) des détails de l'exécution des programmes. On peut identifier trois tâches principales pour la réalisation d'un véritable débogueur. La première tâche consiste à déterminer les informations qui doivent apparaître dans la trace. La deuxième tâche est la mise en oeuvre des traceurs. La troisième tâche consiste à automatiser le filtrage et l'analyse des traces d'exécution afin de donner des informations pertinentes au programmeur qui peut ainsi se concentrer sur le processus cognitif.

Le débogage consiste à localiser et corriger les fautes qui sont responsables des pannes logicielles. Une panne peut être détectée après une exécution, par exemple à la suite de phases de test (cf module 3.5) ou lors d'une phase de vérification formelle. La première situation, la plus fréquente dans la pratique actuelle, correspond à ce qu'on appelle le **débogage dynamique** ; la seconde sera qualifiée de **débogage statique**. Dans les deux cas, l'objectif visé est de faire cesser les pannes identifiées.

Le débogage est une activité cognitive complexe qui nécessite, en général, de remonter jusqu'à l'erreur humaine pour comprendre les raisons des fautes qui ont engendré les pannes. Une panne est un symptôme de faute qui se manifeste en un comportement erroné du programme. Bien souvent le programmeur ne maîtrise pas toutes les facettes du comportement d'un programme. Par exemple, des points de sémantique opérationnelle du langage peuvent lui échapper, le programme peut être trop complexe, ou les librairies utilisées peuvent avoir une documentation obscure. Nous présentons dans un premier temps la problématique du débogage dynamique avant de résumer les particularités introduites par le débogage statique.

Pour ce qui est du débogage dynamique, il existe des outils, communément appelés **débogueurs**, qui aident le programmeur à identifier les comportements du programme qui ne correspondent pas à l'idée qu'il s'en faisait. Ces outils, qui devraient plutôt s'appeler **traceurs**, donnent une image (appelée **trace**) des détails de l'exécution des programmes. Une trace est composée d'**événements** remarquables.

On peut identifier trois tâches principales pour la réalisation d'un véritable débogueur dynamique :

1. La première tâche consiste à déterminer les informations qui doivent apparaître dans la trace. La trace est calquée sur la sémantique opérationnelle du langage sans forcément en donner tous les détails. Elle fournit une abstraction des étapes de calcul dont l'objectif est la compréhension par l'utilisateur du comportement des programmes. Elle dépend donc du langage et du type d'utilisateur potentiel.
2. La deuxième tâche est la mise en oeuvre des traceurs qui nécessite l'insertion d'instructions de trace dans les mécanismes d'exécution des programmes (appelée **instrumentation** dans la suite). Cette instrumentation peut se faire à différents niveaux : dans le code source, dans le compilateur ou dans l'émulateur quand il en existe un. La pratique courante consiste à instrumenter à un niveau bas [Ros96] mais plus l'instrumentation est faite à un niveau haut, plus elle est portable.
3. Quand le programmeur dispose d'un traceur, il lui reste à analyser les traces pour comprendre les comportements des programmes et localiser les fautes. Cependant ces traces donnent souvent trop de détails par rapport à la panne analysée. La troisième tâche consiste à automatiser le filtrage et l'analyse des traces d'exécution afin de donner des informations plus pertinentes au programmeur qui peut ainsi se concentrer sur son processus cognitif.

La dichotomie débogueur statique / débogueur dynamique reflète tout à fait la distinction introduite plus haut (module 3.3) entre analyse statique et analyse dynamique. De fait, un débogueur statique peut être vu comme un analyseur statique dédié à la vérification de certaines classes de propriétés et intégré dans un outil interactif. L'interaction doit permettre à l'utilisateur de vérifier certaines hypothèses sur le comportement du programme et d'identifier d'éventuelles causes de dysfonctionnement sans exécuter le programme. Les trois tâches identifiées plus haut pour le débogage dynamique se retrouvent **mutatis mutandis** dans le contexte

du débogage statique : les traces sont alors des abstractions de la sémantique opérationnelle du langage (cf module 3.2) et le filtrage réalise une approximation permettant de rendre décidable la propriété recherchée.

3.5. Test de logiciels

Mots clés : *critère de test, hypothèse de test, test unitaire, test d'intégration, test fonctionnel, test système, test en boîte noire, test en boîte blanche, test structurel.*

Glossaire

Jeu de test Un jeu de test est un ensemble de données de test.

Critère de test Un critère permet de spécifier formellement un objectif (informel) de test. Un critère de test peut, par exemple, indiquer le parcours de toutes les branches d'un programme, ou l'examen de certains sous-domaines d'une opération.

Validité Un critère de test est dit valide si pour tout programme incorrect, il existe un jeu de test non réussi satisfaisant le critère.

Fiabilité Un critère est dit fiable s'il produit uniquement des jeux de test réussis ou des jeux de test non réussis. Les jeux de test satisfaisant un critère fiable sont donc équivalents du point de vue du test.

Complétude Un critère est dit complet pour un programme s'il produit uniquement des jeux de test qui suffisent à déterminer la correction du programme (pour lequel tout programme passant le jeu de test avec succès est correct) [XMd+94]. Tout critère valide et fiable est complet.

Hypothèse de test La complétude étant hors d'atteinte en général, on peut qualifier un jeu de test par des hypothèses de test qui caractérisent les propriétés qu'un programme doit satisfaire pour que la réussite du test entraîne sa correction.

Le test comporte une grande variété de tâches qui comprend notamment la conception des jeux de test, leur instrumentation, leur exécution, le dépouillement des résultats et la sélection des tests de non-régression (en cas de modification des programmes). La plupart de ces étapes repose sur l'empirisme et l'aide fournie par les outils actuels reste insuffisante. Cependant, certaines de ces tâches peuvent être systématisées et même, dans une certaine mesure, mécanisées. La génération de jeux de test en fait partie et sa systématisation constitue l'objectif majeur des activités du projet Lande sur ce thème. Les principales difficultés à résoudre concernent la formalisation des critères de test et l'analyse des documents d'entrée (spécification ou code source) pour engendrer des données constituant un jeu de test satisfaisant. Le bénéfice d'une telle systématisation est double : d'une part les jeux de test ainsi produits sont de meilleure qualité que ceux que peut inventer un testeur (et justifiés par rapport à un critère précis) ; d'autre part, la possibilité de mécaniser le procédé (au moins partiellement) apporte des gains significatifs en terme de productivité.

On distingue généralement quatre types de tests, chacun étant lié à l'une des phases de conception des logiciels. Les premiers tests soumis au logiciel ont pour cible les composants élémentaires de l'application à tester. Pour cette raison, ils sont appelés **tests unitaires** (on trouve aussi le terme **test de composant**). La seconde phase de test, les **tests d'intégration**, correspond à la phase d'intégration progressive des différents composants élémentaires qui ont déjà passé avec succès l'épreuve des tests unitaires. L'objectif est de mettre en évidence les dysfonctionnements engendrés par leur assemblage. Les **tests fonctionnels** sont ensuite exécutés sur l'application dont tous les composants ont été assemblés et intégrés. Le dernier type de test s'applique à la version complète de l'application déployée dans son environnement d'exécution. Ces tests, que l'on nomme **tests système**, consistent à détecter des fautes ou des comportements incorrects de l'ensemble du système en situation réelle. Les **tests de recette** sont des tests système.

Pour concevoir ces différents types de test, il existe un ensemble de techniques qui se décompose en deux familles [XMd+94]. La première famille réunit les techniques de test dites en **boîte noire** qui reposent sur une spécification (informelle, semi-formelle ou formelle) du programme. Le code du programme est considéré inaccessible et n'est pas utilisé pour sélectionner les données de test. Les tests produits sont dits **fonctionnels**.

La seconde famille est constituée des techniques de test dites en **boîte blanche** qui s'appuient exclusivement sur des analyses du code de l'application [Bei90]. Ces techniques reposent sur l'examen de la structure du programme et le calcul de flots de contrôle ou de données. Les tests produits sont dits **structurels**.

Le test comporte une grande variété de tâches qui comprend notamment la conception des jeux de test, leur instrumentation, leur exécution, le dépouillement des résultats et la sélection des tests de non-régression (en cas de modification des programmes). La plupart de ces étapes repose sur l'empirisme et l'aide fournie par les outils actuels reste insuffisante. Cependant, certaines de ces tâches peuvent être systématisées et même, dans une certaine mesure, mécanisées. La génération de jeux de test en fait partie et sa systématisation constitue l'objectif majeur des activités du projet Lande sur ce thème. Les principales difficultés à résoudre concernent la formalisation des critères de test et l'analyse des documents d'entrée (spécification ou code source) pour engendrer des données constituant un jeu de test satisfaisant. Le bénéfice d'une telle systématisation est double : d'une part les jeux de test ainsi produits sont de meilleure qualité que ceux que peut inventer un testeur (et justifiés par rapport à un critère précis) ; d'autre part, la possibilité de mécaniser le procédé (au moins partiellement) apporte des gains significatifs en terme de productivité.

3.6. Langages déclaratifs

Mots clés : *langage fonctionnel, langage de programmation logique, correction, efficacité, évolutivité, maintenance*.

Les langages de programmation déclaratifs sont fondés sur la déclaration du résultat à atteindre plutôt que du moyen de l'atteindre. Leur mise en oeuvre exige un effort spécifique pour passer automatiquement d'une définition de nature déclarative à une version opérationnelle efficace. En contrepartie, ces langages sont adaptés à l'usage de méthodes formelles (analyse de programmes, vérification). Les langages déclaratifs étudiés dans le projet Lande appartiennent soit à la famille de la programmation fonctionnelle, soit à celle de la programmation logique.

Les langages de programmation forment des familles qui incarnent des disciplines de programmation. La famille des langages de programmation déclaratifs comprend les langages qui sont fondés sur la déclaration du résultat à atteindre plutôt que du moyen de l'atteindre. La discipline mise en oeuvre dans ces langages consiste à s'engager le moins possible dans des détails opérationnels afin de diminuer le fossé entre ce que souhaite le programmeur et ce que le langage de programmation permet d'exprimer.

Le projet Lande s'intéresse à deux espèces de langages de programmation déclaratifs qui sont les langages fonctionnels (Lisp, ML, Haskell, etc.) et les langages logiques (Prolog, λProlog, Mercury, etc.). Une remarque importante à faire à leur sujet est que ces langages utilisent des formalismes qui ont présidé à la formalisation de la notion de calcul : le λ-calcul [Ros84] et le calcul des prédicats. Dans les deux cas, les programmes sont des **formules** mais elles sont interprétées différemment. L'opération essentielle des langages fonctionnels est la **réduction** qui permet de remplacer une formule par une autre formule équivalente, mais plus « simple », jusqu'à obtenir une formule qui n'est plus réductible, et que l'on appelle une **forme normale**. On convient que cette forme normale est le résultat du calcul. L'opération essentielle des langages logiques est la **déduction**. On l'emploie pour construire des preuves, et on convient que le résultat du calcul est extrait de ces preuves. Il s'agit le plus souvent des valeurs données dans les preuves à certaines variables. Pour autant que la correspondance de Curry-Howard s'applique (langages fonctionnels typés), la preuve est l'objet commun à ces deux familles de langages de programmation ; les langages fonctionnels les normalisent, et les langages logiques les construisent.

L'intérêt premier des langages de programmation déclaratifs est qu'ils se prêtent aux manipulations formelles. La raison majeure est l'absence d'**effets de bord** dans ces langages : les entités de base (fonctions ou prédicats) peuvent ainsi être manipulées directement comme des objets mathématiques.

Les enjeux des langages fonctionnels et logiques sont assez similaires. D'une part, il faut réussir à mettre en oeuvre efficacement les calculs décrits dans ces langages. D'autre part, il faut concevoir les outils de programmation qui accompagnent ces langages.

Un autre formalisme déclaratif traité dans le projet Lande est celui des **bases de données déductives**. Il partage les mêmes fondements que la programmation logique mais à des fins différentes. Ici, l'enjeu est la description de grands volumes de données, des lois qui structurent ces données et des requêtes des utilisateurs. La complétude calculatoire n'est plus recherchée. Au contraire, on veut que le problème de répondre à une requête soit décidable.

3.7. Analyse de concepts

Mots clés : *contexte formel, concept formel, intention/extension, treillis de concepts.*

L'analyse de concepts est une formalisation des notions philosophiques de concept, extension de concept (les individus qui sont sensés appartenir à un concept) et compréhension de concept (les notions communes à tous les individus d'un concept) [GW99].

La formalisation part d'un **contexte formel**, qui est en fait une relation entre individus et descriptions. Les individus sont les objets du discours, par exemple des entrées dans un catalogue, des fonctions d'un programme, ou des points d'une carte. On considérera que les descriptions sont des ensembles d'attributs, par exemple « 330 Mhz et 500 Moctets », même si nous avons montré qu'on peut généraliser les descriptions à une logique arbitraire pour peu que sa relation de déduction forme un treillis [FR00b]. On peut alors trouver les relations suivantes : « fréquence:330 Mhz et capacité:500 Moctets » ou « type: $bignum \longrightarrow int \longrightarrow bignum$ et pré: $Arg_1 = 0 \Longrightarrow Arg_2 \geq 0$ ».

Il est naturel de se demander quels sont les individus qui satisfont telle description, car ils ont tous les attributs de cette description, et quelle est la description commune à un ensemble d'individus, l'intersection des attributs de ces attributs. Cela définit une fonction τ des descriptions vers les ensembles d'individus, et une fonction σ des ensembles d'individus vers les descriptions. Théorème : ces fonctions forment une connexion de Galois :

$$I \leq_i \tau(D) \longleftrightarrow D \leq_d \sigma(I)$$

où $\leq_i$ est l'inclusion ensembliste (des ensembles d'individus) et $\leq_d$ est la relation inverse de l'inclusion ensembliste (des ensembles d'attributs). Dans le cas où les descriptions sont généralisées à une logique arbitraire, $\leq_d$ est la relation de déduction des descriptions.

Les fonctions $\tau\sigma$, sur les ensembles d'individus, et $\sigma\tau$, sur les descriptions, sont donc des opérations de fermeture par rapport à un contexte formel. Cela veut dire qu'un contexte formel détermine des ensembles d'individus et des descriptions qui sont plus canoniques que les autres. Par contre, les autres ensembles d'individus ou descriptions peuvent toujours être canonisés par application de $\tau\sigma$ ou $\sigma\tau$. Noter que des ensembles d'individus différents peuvent avoir la même fermeture (de même pour les descriptions). On dispose donc de plusieurs moyens pour exprimer les mêmes choses.

Un concept formel est une paire (I, D) telle que $D = \sigma(I)$ et $I = \tau(D)$. On appelle I l'**extension** du contexte formel, et D son **intention**[1]. I et D sont donc des fermetures. En fait, on peut désigner un concept formel par n'importe quel ensemble d'individus i ou description d de la façon suivante : $(\tau(d), \sigma\tau(d))$ ou $(\tau\sigma(i), \sigma(i))$. On dit alors que i, ou d, étiquète le concept.

Le théorème fondamental de l'analyse de concepts formels est que l'ensemble des concepts qu'on peut former dans un contexte formel constitue un treillis quand on l'ordonne par inclusion des extensions. Dans un tel treillis, un individu étiquète un concept si et seulement si l'individu est présent dans tous les concepts supérieurs. De même, une description étiquète un concept si elle est satisfaite par tous les concepts inférieurs.

Traditionnellement, l'analyse de concept est mise en oeuvre dans des systèmes d'analyse a posteriori de faits bruts constituant le contexte formel. C'est alors une méthode d'analyse des données, mais nous préférons étudier son emploi dans des systèmes plus dynamiques où elle est considérée comme un modèle d'organisation. Par exemple, munie d'une logique permettant de décrire les différentes vues d'une architecture logicielle, l'analyse de concepts devient un environnement de développement de logiciels qui intègre la

[1] Le vocabulaire de la philosophie utilise le mot **compréhension**. Certains écrivent **intension**.

navigation dans l'architecture. D'où l'idée de la mettre en oeuvre dans un système de fichiers qu'on appellera « système de fichiers logique » [FR00a].

Dans un système de fichiers logique, l'analogue du chemin Unix est la description. Une description désigne un répertoire (virtuel) qui est le concept qu'elle étiquète. On dit qu'un individu appartient à un répertoire si il l'étiquète. Sont considérés comme des sous-répertoires tous les concepts inférieurs au répertoire. On peut ainsi reconstruire interrogation ($ls\ \ d$) et navigation ($cd\ \ d$) dans une perspective unifiée.

4. Domaines d'application

4.1. (Sans titre)

Mots clés : *sécurité, sûreté, confidentialité, intégrité, logiciel critique, carte à puce, commerce électronique, génération de jeux de test, outil de débogage, architecture sécurisée.*

Les deux cibles privilégiées du projet Lande sont :

1. Les applications qui exigent un degré de confiance très important justifiant l'emploi de méthodes formelles. L'accent est mis en particulier sur la sécurité des informations (confidentialité, intégrité).
2. Les logiciels complexes ou qui nécessitent des modifications fréquentes : il s'agit du domaine d'excellence des langages de programmation déclaratifs.

De par sa nature même, le projet Lande est orienté « technologie » plutôt que « domaine d'application ». La plupart des domaines cités ici sont donc des illustrations de travaux passés ou en cours, plutôt que des centres d'intérêt propres du projet. Une exception peut être faite toutefois pour ce qui concerne la sécurité des systèmes d'information (au sens de confidentialité et d'intégrité notamment). Il s'agit d'un domaine d'application où l'exigence de méthodes formelles se fait fortement sentir et qui comporte des implications industrielles majeures, en particulier pour le développement du commerce électronique. Le projet Lande a investi depuis plusieurs années dans ce domaine qui prend une importance croissante dans l'ensemble de ses activités.

De manière générale, on peut identifier deux cibles privilégiées pour les outils formels et les langages de haut niveau qui sont étudiés dans le projet :

- La première concerne les applications complexes ou exigeant un degré de confiance très important justifiant l'emploi de méthodes formelles. Il peut s'agir de logiciels critiques pour la confidentialité ou l'intégrité des informations, la sécurité des personnes. Sur ce thème, nous travaillons (dans le cadre de Dyade et des projets européens « Secsafe » et « Verificard ») à l'analyse et la vérification de transformateurs de bytecodes Java Card, avec comme domaine d'application la sécurité des cartes à puce (cf modules 6.2.3, 7.5,7.6 et 7.7).
  Les descriptions multi-vues ainsi que les langages d'architectures de logiciels constituent une démarche plus récente pour le développement de logiciels complexes. Sur ce thème, nous sommes impliqués dans une action industrielle (l'action CASTOR cf 7.8) qui porte sur la conception d'architectures sécurisées. Elle s'effectue en collaboration avec AQL, EADS Sycomore, TNI et le projet EP-ATR de l'Irisa.
  On peut citer également dans cette catégorie nos travaux sur la génération automatique de jeux de test qui se poursuivent dans le cadre du projet européen « TWO » en collaboration avec l'éditeur d'outils de tests Attol Testware et des industriels utilisateurs comme Siemens et Spacebell (cf module 7.4) et dans le cadre du projet RNTL « Cote » avec Softeam, IMAG, France Télécom R&D et Gemplus (cf module 7.2).

- La seconde cible de nos travaux concerne les logiciels qui nécessitent des modifications fréquentes : on peut citer par exemple les systèmes qui mettent en oeuvre des ensembles de règles (de facturation, de réservation, etc.) devant suivre les évolutions du marché ou de la législation. Il s'agit du domaine d'excellence des langages de programmation déclaratifs. Par exemple, la mise en oeuvre du langage λProlog réalisée dans le projet a notamment été utilisée pour la programmation d'un module de recherche de composants logiciels, pour la reconnaissance de partitions musicales (cf module 5.3).

5. Logiciels

5.1. Générateur de suites de test Casting

Participant : Thomas Jensen.

Nous avons proposé une méthode de génération de suites de test qui forme le noyau de l'outil Casting[2] développé en collaboration avec Lionel Van Aertryck de la société AQL. La méthode est indépendante du format d'entrée, ce qui la rend utilisable aussi bien dans le cas du test structurel que fonctionnel. Les suites de test engendrées dépendent de stratégies spécifiées par l'utilisateur, permettant ainsi d'atteindre la souplesse d'utilisation exigée pour un usage industriel.

Nous avons abordé le problème de la systématisation de la génération de jeux de test en tentant d'abolir la dichotomie « boîte noire/boîte blanche » (cf. module 3.5). Pour ce faire, nous décomposons le processus de production des données de test en trois étapes :

1. L'acquisition des critères de test et la production des hypothèses de test associées, à partir de différents supports d'entrée.
2. La décomposition des opérations en classes d'opérations et la génération d'un graphe d'accessibilité symbolique.
3. La génération des jeux de test par parcours du graphe d'accessibilité en assurant un critère de couverture donné.

Les supports d'entrée peuvent être constitués de spécifications formelles ou informelles, de programmes sources ou de propriétés fournies directement par l'utilisateur. Les opérations peuvent être des machines abstraites dans le cas du langage B, des schémas pour le langage Z, des programmes dans le cas d'un langage de programmation, etc. Dans tous les cas, les critères de test sont implantés par des **stratégies de test** et se traduisent in fine par des **hypothèses d'uniformité et hypothèses de régularité**. Ces hypothèses permettent de préciser le sens (et les limites) des jeux de test qui seront engendrés (cf. module 3.5). D'un point de vue pratique, une stratégie de test correspond à un mode d'extraction de contraintes à partir du texte source. Ces contraintes caractérisent les jeux de données qui devront être engendrés pour chaque opération du système. Le graphe d'accessibilité symbolique indique l'ordre dans lequel les opérations peuvent être appliquées pour satisfaire toutes les contraintes. Dans le cas général en effet on ne peut faire l'hypothèse qu'une opération soit toujours applicable : selon l'état du système, il peut être nécessaire d'effectuer plusieurs opérations intermédiaires avant de pouvoir appliquer une opération donnée. La dernière phase consiste à explorer ce graphe en résolvant les contraintes associées pour générer les données de test effectives.

Ces travaux ont conduit au développement d'un outil d'aide à la génération de jeux de test. La version actuelle de Casting prend en entrée des spécifications dans la notation AMN de la méthode B [Abr96] et fait appel à Ilog Solver[3] pour résoudre les contraintes engendrées.

Le prototype est constitué d'une partie générique qui regroupe tous les traitements internes (élimination des spécifications de cas de test insatisfiables, génération du graphe d'états symboliques, génération des

[2] **Computer Assisted Software Testing**
[3] Ilog Solver est une marque déposée par Ilog.

hypothèses de test et des suites de test, etc.) et une partie liée à la spécification pour laquelle le testeur souhaite engendrer des suites de test (frontal).

Avec ce prototype l'utilisateur a accès à un environnement de génération de suites de test qui lui permet de définir une stratégie de test et de l'appliquer à des spécifications écrites dans un sous-ensemble de B. L'utilisateur dispose de différents moyens de contraindre la recherche de solution (temps alloué au solveur, taux de couverture, etc.) ainsi que la possibilité d'interagir avec le solveur de contraintes de manière à l'orienter directement vers des solutions.

Le développement a été réalisé sous Solaris 2 et il intègre des codes C, C++ (algorithmes de recherche de chemins et de génération de données), λProlog (mise sous forme normale disjonctive) et tcl/tk (interface graphique). L'interface réalisée permet d'assister le testeur dans toutes les phases de la génération des suites de test (choix d'une stratégie, paramétrage et aide à la résolution, visualisation de la couverture obtenue, etc.).

Pour plus de renseignements concernant cet outil et son état d'avancement, on peut se reporter à l'adresse : http://www.irisa.fr/lande/vanaertr/bcasting.html ou contacter Thomas Jensen (jensen@irisa.fr).

5.2. Débogueurs Coca et Morphine

Participant : Mireille Ducassé [correspondant].

Coca [Duc99] est un débogueur automatisé pour C où le mécanisme des points d'arrêt est basé sur des événements relatifs à des constructions du langage. Ces événements ont une sémantique, alors que les lignes du code source utilisées par la plupart des débogueurs n'en ont pas. Morphine [JD99] est un débogueur automatisé pour le langage de programmation en Logique Mercury[SHC96].

Une trace est une séquence d'événements. Elle peut être vue comme une relation d'ordre sur une base de données. Les utilisateurs de nos systèmes peuvent spécifier exactement les événements qu'ils veulent voir en précisant des valeurs pour les attributs des événements. À chaque événement, les variables visibles peuvent être examinées. Le langage d'interrogation de trace est Prolog augmenté de quelques primitives. Le mécanisme d'interrogation de trace cherche dans la trace d'exécution en utilisant à la fois des informations sur le flot de contrôle et sur les données, alors que les débogueurs effectuent habituellement leur recherche de manière exclusive en fonction du contrôle ou en fonction des données. Contrairement aux débogueurs totalement relationnels qui utilisent effectivement une base de données, le mécanisme d'interrogation de trace de Coca et de Morphine repose sur une analyse à la volée : il ne nécessite donc aucun stockage. Coca et Morphine sont donc plus puissants que les débogueurs dont les points d'arrêt sont des lignes du code source et plus efficaces que les débogueurs relationnels.

Un prototype de Coca est opérationnel sous sparc/Solaris2.[5,6]. Il nécessite le compilateur GCC ainsi que le système Prolog Eclipse 4.1. Il intègre des codes C, C++, Prolog et Bison.

Un prototype de Morphine a été développé dans le cadre du projet industriel européen ARGO (**Ruggedized and High performance logic Programming for the Real World**, Industrial RTD Project no 25503, ref. Inria : 1 97 C 843), novembre 1997-juin 1999. Morphine est actuellement maintenu et opérationnel sous sparc/Solaris2.[5,6,7] et i686/Linux2.0, il nécessite le système Eclipse 4.1, ainsi que le compilateur Mercury (versions postérieures au 1999-03-12). Morphine a été déposé à l'agence pour la protection des logiciels sous la référence IDDN.FR.001.090030.00.S.P.2000.000.10600. Il fait partie de la distribution standard de Mercury (http://www.cs.mu.oz.au/research/mercury). Le système Morphine, ainsi que sa documentation, sont également disponibles sur le web http://www-verimag.imag.fr/lande/ jahier/download.html.

Pour plus de renseignements concernant Coca et Morphine, on peut contacter Mireille Ducassé (mailto:ducasse@irisa.fr).

5.3. Compilateur λProlog

Participant : Olivier Ridoux [correspondant].

Le compilateur de λProlog développé à l'Irisa représente un investissement de plusieurs années (à l'origine dans le projet Mali). Son schéma est fondé sur un modèle à continuations [BR93b] et sur la mémoire Mali

[Rid91]. Ce système, appelé Prolog/Mali, implémente le langage λProlog complet, plus des facilités comme l'ordonnancement dynamique des buts (**freeze**), les captures de continuations (d'échec et de succès), et l'appel de procédures C depuis λProlog (et vice-versa). Il constitue un système flexible qui permet la coopération de modules écrits en λProlog et en d'autres langages. Ce trait est couramment employé dans les applications un tant soit peu complexes. Le système comporte aussi un traceur symbolique et un profileur. Ce système a été développé sous Solaris 1 (SunOs 4) puis porté sous Solaris 2 (SunOs 5). Il est disponible sous FTP (ftp://ftp.irisa.fr/local/pm). Les logiciels Mali et Prolog/Mali ont été déposés à l'APP (numéros 87–12–005–01 et 92–27–012–00) et sont munis d'une documentation.

Le compilateur λProlog est employé en enseignement, dans des applications de projets de l'Irisa, et dans d'autres laboratoires plus ou moins distants. Parmi les applications les plus notables, on peut citer : la reconnaissance de partitions d'orchestre (Irisa, projet Imadoc), la coopération entre agents intelligents (SEPT, Caen), la recherche de composants systèmes (Irisa, projet Solidor), la transformation de grammaires attribuées (Irisa, projet Lande) et le compilateur Prolog/Mali, lui-même écrit en Prolog/Mali et en C et C/Motif. Une équipe de l'université d'Édimbourg l'utilise pour le développement d'un démonstrateur automatique pour une logique d'ordre supérieur.

Pour tout renseignement concernant Mali ou Prolog/Mali, le point de contact à l'Irisa est Olivier Ridoux (ridoux@irisa.fr, voir aussi [Rid98][BBR]).

5.4. Solveur de point fixes Reqs

Participants : Thomas Jensen, Florimond Ployette [correspondant].

De nombreux travaux ont été effectués sur les fondements de l'analyse sémantique, la correction et la précision des analyseurs. On peut regretter cependant le peu d'attention accordé jusqu'à présent à la conception d'outils d'analyse génériques. Nous travaillons à la mise au point d'un solveur de point fixe générique qui peut servir de base pour le développement de nouveaux analyseurs. Une analyse produit souvent comme résultat un système d'(in)équations sur un domaine de propriétés dont la solution représente l'information recherchée. La phase de résolution est indépendante du programme analysé ; une méthode de résolution de systèmes d'équations peut donc s'appliquer à des systèmes provenant de différentes analyses. Cette observation suggère la possibilité de réaliser un « moteur d'analyse », c'est-à-dire un outil générique de résolution de systèmes d'(in)équations qui peut servir de base pour implanter des analyseurs. La généricité évoquée ici est relative aux propriétés et aux domaines abstraits considérés. La solution d'un tel système peut être calculée de façon itérative comme le plus petit point fixe d'un opérateur défini par le système d'équations à résoudre.

REQS est un outil de résolution de système d'équations récursives produites dans le cadre d'analyses statiques de programmes. L'objectif de ce travail est de factoriser le travail de résolution de point fixe pour des analyses de programmes impératifs, logiques ou fonctionnels. L'outil propose un ensemble de stratégies permettant d'adapter au mieux la résolution à la nature du système (dense ou non, point fixe local, etc). Pour résoudre un système d'équations sur un domaine donné, l'utilisateur doit, soit fournir une implémentation des opérations utilisées dans les équations, soit utiliser les domaines et opérations prédéfinis dans REQS.

Nous avons réalisé plusieurs expériences avec REQS pour implémenter des analyses provenant de différents types de langage (langages à objets, langage Signal). Dans le domaine de langages à objets, REQS a été utilisé pour implémenter une analyse de classes Java qui tient compte du traitement des exceptions. Cette analyse de classes produit un arbre de flot de contrôle qui sert de base à des analyses plus spécifiques comme la vérification de propriétés de sécurité.

REQS a été est distribué au projet Oasis à l'Unité de Recherche de Sophia Antipolis et il est envisagé une intégration de nos outils d'analyse avec les outils Smartools développés par le projet Oasis.

Pour des renseignements supplémentaires concernant l'outil REQS,x on peut contacter Florimond Ployette (`ployette@irisa.fr`). ou consulter le web (`http://www.irisa.fr/lande/REQS/presentation_reqs.html`).

5.5. Librairie d'automates d'arbres: Timbuk

Participants : Thomas Genet [correspondant], Valérie Viet Triem Tong.

Timbuk [GVTT01] est une librairie de fonctions OCAML destinées à manipuler des automates d'arbres. La classe des automates d'arbres pouvant être décrits est la classe des automates finis ascendants déterministes et non déterministes. Cette librairie fournit les opérations classiques sur les automates d'arbres :

- opérations booléennes : intersection, union, complément
- décision du vide, décision de l'inclusion
- nettoyage, renommage
- déterminisation
- normalisation des transitions
- calcul de l'automate reconnaissant l'ensemble des termes irréductibles pour un système de réécriture linéaire à gauche.

Mais, elle implante également plusieurs opérations plus spécifiques que nous utilisons pour la vérification de protocoles cryptographiques :

- la complétion d'un automate d'arbre par rapport à un système de réécriture donné
- l'approximation de l'ensemble des descendants et de l'ensemble des formes normales d'un automate pour un système de réécriture donné
- le filtrage dans les automates.

Ce logiciel est distribué sous la Gnu Library General Public License et disponible à l'URL suivante :
http://www.irisa.fr/lande/genet/timbuk/

6. Résultats nouveaux

6.1. Méthodes de conception et de structuration de logiciel

Nous décrivons dans cette partie les contributions du projet qui sont de nature linguistique. Dans chaque cas, il s'agit de proposer un formalisme ou un langage spécialisé adapté à un type de problème et conduisant à des traitements automatiques (vérification, analyse, transformation, etc.). Nous abordons successivement nos travaux sur les descriptions multi-vues (module 6.1.1), les agents mobiles (module 6.1.2), la programmation par aspects (module 6.1.3) et un cadre pour la définition de systèmes d'information logiques (module 6.1.4).

6.1.1. Descriptions de systèmes multi-vues

Participants : Pascal Fradet, Thomas Lefort, Lakshminarayanan Renganarayanan.

Mots clés : *description de systèmes*, *vues*, *relations inter-vues*, *cohérence*, *vérification*, *analyse*.

Nous travaillons sur des descriptions composées de multiples points de vue. Le but principal est d'assurer des propriétés de cohérence sur ce style de description hétérogène. Nous avons proposé et implanté un vérificateur d'une classe très riche de propriétés structurelles. L'application de ces travaux est effectuée dans le cadre d'une collaboration industrielle concernant l'aide à la construction de systèmes sécurisés (projet Castor financé par le Celar).

Le développement de systèmes d'information complexes est particulier en ceci qu'il implique :

- des descriptions décomposant le système en sous-parties et le spécifiant à différents niveaux d'abstraction (de l'architecture globale aux composants de base),
- des descriptions de propriétés ou d'aspects très différents (flots de données ou de contrôle, communications, exigences non fonctionnelles),
- la participation de nombreux acteurs spécialisés dans une étape du développement, un sous-système ou un aspect particulier du système (par ex. la sécurité),
- l'utilisation d'outils (analyse de performance, de gestion de configuration) impliquant une description particulière du système.

Clairement, un unique outil, notation ou formalisme ne peut convenir à une telle variété de besoins et de participants. En conséquence, les gros systèmes sont le plus souvent décrits selon différents points de vue. L'idée sous-jacente est de structurer la description d'un système en plusieurs vues reflétant les intérêts et compétences des différents acteurs du développement. L'intérêt des vues est double ; d'une part, chaque vue est décrite dans un formalisme dédié, adapté au domaine concerné, d'autre part, la décomposition d'une description selon des domaines de compétence favorise la séparation des problèmes. Cependant, il est rare que les vues soient totalement indépendantes. Par exemple, une vue répartition des données aura un impact sur une vue tolérance aux fautes. Il est même possible que deux vues répondent à des impératifs conflictuels : par exemple, l'ajout d'un lien de communication améliore la tolérance aux fautes, mais peu s'avérer néfaste pour la sécurité en introduisant un flux d'information illicite. Si ce type d'incohérences persiste, on peut aboutir à des systèmes erronés ou impossible à implémenter. La multiplicité et l'hétérogénéité des descriptions rend nécessaire d'expliciter leurs dépendances et de les exploiter de manière à assurer une forme de cohérence.

Nos travaux précédents considéraient une vue comme spécifiant une famille de systèmes (comme, par exemple, les diagrammes de classe d'UML). La classe des propriétés de cohérence vérifiables automatiquement sur de telles vues est assez restreinte. Nous nous sommes récemment intéressés à la vérification de propriétés de cohérence dans le cas où chaque vue est représentée par un graphe simple. La simplicité du modèle considéré (graphes annotés) a permis d'implanter un vérificateur pour une classe très riche de propriétés structurelles.

Ce travail se concrétise dans le cadre d'une action industrielle conduite en collaboration avec les sociétés AQL, EADS Sycomore et TNI, ainsi que les projets EP-ATR et Lande de l'Irisa. L'objectif de ce projet est de fournir un environnement permettant de décrire l'organisation globale d'un système d'information sous forme de vues et d'étudier ses propriétés de sécurité. Le vérificateur de propriétés a été intégré à l'environnement de modélisation de Castor et à également été adapté à l'analyse de propriétés (synthèse de parades/attaques) sur la vue sécurité [Cas01].

Nous nous intéressons maintenant à la vérification automatique de propriétés de cohérence sémantique (ou de comportement) de descriptions hétérogènes. Le défi principal est de trouver comment mettre en relation des vues qui mettent en jeu des propriétés de nature très différentes ou qui se situent à des niveaux d'abstraction différents.

6.1.2. Agents mobiles pour services distribués

Participants : Pascal Fradet, Siegfried Rouvrais.

Mots clés : *architectures de logiciel*, *interactions*, *agent mobile*, *performance*, *sécurité*, *fiabilité*.

Nous avons étudié l'analyse de propriétés d'interactions exprimées comme des compositions d'agents mobiles, d'invocations distantes (RPC, Remote Procedure Call, et RMI, Remote Method Invocation), ou d'évaluations à distance. Les propriétés analysées sont la performance (en terme de volume de données échangées), la sécurité (confidentialité et intégrité) et la fiabilité des interactions. Nous avons illustré comment ce type d'information permet de guider le concepteur de systèmes distribués dans ses choix d'implantation.

Les agents mobiles ont été récemment proposés comme une nouvelle forme d'interaction des systèmes distribués. Une des raisons qui rendent les agents difficiles à utiliser est que leurs avantages ou inconvénients, comparés aux interactions classiques comme les RPC, portent sur des aspects non fonctionnels (comme les performances). Les propriétés non fonctionnelles sont souvent difficiles à appréhender et choisir la bonne combinaison d'interactions pour implanter un service complexe est une tâche délicate.

Nous avons travaillé à cette question en analysant et en comparant les différents styles d'interaction selon trois types de propriétés : les performances, la sécurité et la fiabilité . Nous avons proposé un cadre linguistique pour spécifier et implanter les services complexes. Les agents mobiles, les invocations distantes, l'évaluation à distance ou toute combinaison de ces protocoles sont représentés comme des expressions fonctionnelles. Ces expressions peuvent alors être analysées et comparées simplement. Pour les performances, nous avons pris comme critère le volume de données échangées sur le réseau. Pour la sécurité, nous nous sommes focalisés sur les propriétés de confidentialité et d'intégrité. Pour la fiabilité, nous avons considéré des mécanismes de tolérance aux fautes connus. Ces analyses permettent de guider le concepteur de systèmes distribués dans

ses choix de protocoles. Ce cadre a été intégré à un environnement de développement basé sur un langage de description d'architectures de logiciels. Il intègre des outils destinés à guider le concepteur de services distribués complexes au regard des propriétés traitées [Rou].

Ce travail est effectué en collaboration avec Valérie Issarny du projet Solidor (UR de Rocquencourt).

6.1.3. Programmation par aspects

Participant : Pascal Fradet.

Mots clés : *interaction entre aspects, analyse et transformation de programme, construction de programme.*

La programmation par aspects propose de décrire un logiciel comme un ensemble formé d'un composant principal et d'une collection d'aspects. Un outil, appelé tisseur, est chargé de produire automatiquement un programme intégrant les différents aspects au composant principal. Nous avons étudié les problèmes posés par le tissage de plusieurs aspects (c'est à dire les interactions entre aspects). Nous étudions également un aspect dédié à la composition de composants. La notion d'« aspect » présente des similarités avec celle de « vue » présentée dans le module 6.1.1. En programmation par aspects, un logiciel est formé d'un composant principal et d'une collection d'aspects décrivant des tâches comme la gestion mémoire, la synchronisation, les optimisations, etc. Un outil, appelé tisseur, est chargé de produire automatiquement un programme intégrant les différents aspects au composant principal. L'intérêt de cette approche est de localiser (dans les aspects) des choix de mise en oeuvre qui seraient sinon dispersés dans le code source.

Comme pour les vues, les aspects ne sont pas obligatoirement orthogonaux. Des interactions (conflits ou ambiguïtés) peuvent apparaître lorsque l'on tisse plusieurs aspects. Ce point est généralement traité de façon manuelle et ad-hoc. Le programmeur doit identifier les interactions et coder la résolution des conflits. Nous avons étudié les interactions possibles selon différents types d'aspects. Le but est double :

- détecter à la compilation les conflits potentiels,
- assister le programmeur dans la résolution des conflits.

L'étude se place dans un cadre formel et générique afin d'explorer ces problèmes d'interactions indépendamment d'un langage de programmation ou d'aspect précis. D'un autre coté, nous avons instancié ces travaux à AspectJ, le langage d'aspect développé par Xerox pour Java [DFS01]. Ce travail est l'objet d'une collaboration avec Mario Südolht et Rémi Douence de l'école de Mines de Nantes.

La recherche en programmation par aspects consiste également à proposer des langages (et tisseurs) dédiés à certaines tâches. Nous avons proposé précédemment une méthode pour imposer des politiques de sécurité par tissage. Nous étudions maintenant un aspect d'assemblage de composants. L'aspect spécifie des ports d'entrées/sorties pour chaque composant ainsi que leurs interconnexions ; le tisseur, lui, se doit de fusionner, selon l'assemblage spécifié, les composants aussi efficacement que possible.

6.1.4. Systèmes d'information logiques

Participants : Sébastien Ferré, Yoann Padioleau, Olivier Ridoux.

Mots clés : *système d'information, analyse de concept, logique.*

Nous étudions la conception de systèmes d'information non-hiérarchiques offrant à la fois des possibilités de navigation et d'interrogation. Nous avons développé pour cela un modèle d'analyse de concepts logiques qui généralise l'analyse de concepts formels de Wille et Ganter [GW99].

Nous étudions l'extension de ce modèle pour la prise en compte de relations entre objets, une métaphore de navigation dans le treillis de concepts logiques, et les algorithmes de consultation, navigation et mise à jour. Sur ce dernier point, l'enjeu principal est de ne jamais construire entièrement le treillis de concepts logiques. La métaphore de navigation envisagée possède les caractéristiques suivantes : une formule désigne un endroit où l'on souhaite lire **ou** écrire, l'interrogation du contenu d'un endroit retourne entre autres la désignation d'endroits proches par des formules (combinant ainsi **interrogation** et **navigation**), et la manipulation des formules se fait aussi bien en prenant en compte leur intention que leur extension. Ce dernier point permet de faire des déductions qui sont correctes dans le contexte courant, mais pas en général.

Nous avons observé que les calculs qui permettent la navigation dans un système d'information logique peuvent être généralisés pour permettre l'expression d'opérations de fouille de donnée comme l'extraction de règles d'association [FR00b]. L'expérience avec un prototype a montré que la logique utilisée pour les descriptions devait pouvoir exprimer une modalité « All I Know » [Lev90]. En effet, l'utilisateur s'attend à déduire que X n'est pas l'auteur d'un article si X ne figure pas dans la liste des auteurs, mais la logique classique ne le permet pas. Il faut inclure une sorte d'hypothèse du monde clos qui laisse la logique monotone pour rester compatible avec le formalisme de l'analyse de concepts. Nous avons défini et mis en oeuvre une telle logique [Fer01]. Elle est maintenant un composant standard de notre prototype. D'une façon plus générale, on voit que le concepteur d'un système d'information logique doit définir la logique de description des individus. Afin de soulager sa tâche, nous avons étudié le moyen de définir une logique par le moyen de composants élémentaires que nous avons appelé **foncteurs logiques** [FR01]. Nous avons défini et mis en oeuvre plusieurs foncteurs qui vont de la logique propositionnelle à la déduction sur les intervalles en passant par un foncteur « All I know ». Nous avons déterminé des critères de compatibilité (des types) qui spécifient quels sont les agencements de foncteurs qui forment des systèmes logiques corrects.

Comme exemple de mise en oeuvre, nous avons réalisé un système de fichiers (sous Linux) qui offre les fonctions de l'analyse de concepts formels sous l'interface standard d'un système de fichiers virtuel. Dans cette réalisation, seul le système de fichiers est spécifique, et les couches supérieures comme le **shell** restent inchangées. Nous recherchons maintenant comment mettre en oeuvre un système de fichiers basé sur l'analyse de concepts logiques de façon la plus générique possible. Nous avons aussi développé un autre prototype qui met en oeuvre toute la généralité des systèmes d'information logique, mais simule un système de fichiers en mémoire. Notre objectif est de réconcilier les deux types de prototype à moyen terme.

6.1.5. Transformations certifiées de programmes Java Card

Participants : Thomas Genet, Thomas Jensen, François Monin.

Mots clés : *transformation*, *optimisation*, *code intermédiaire*, *carte à puce*, *Java Card*, *preuve formelle*.

Nous avons conçu et breveté une méthode qui permet de prouver la correction des transformations effectuées sur le code intermédiaire Java Card pour permettre son installation sur une carte à puce. Cette preuve a été vérifiée avec l'assistant de preuve Coq. La formalisation de ces transformations forme la base de travaux qui visent à construire un transformateur Java Card certifié en Coq. Notre effort de formalisation des différents aspects de Java et de sa mise en oeuvre a entre autres porté sur la vérification d'optimisations pour Java Card. La définition du langage Java Card comprend un langage intermédiaire (le « Java Card byte code ») et un format (le format CAP pour « Converted APplet format ») utilisé pour stocker des applications sur une carte. Le format Cap joue un rôle semblable à celui du format des fichiers de classes (« class files ») de Java mais regroupe le code des classes de tout un package de Java contrairement aux fichiers de classes de Java (qui ne représentent qu'une seule classe par fichier). Ceci permet de remplacer des références symboliques entre classes à travers le « constant pool » par des adresses de mémoire, ce qui est plus rapide et permet de supprimer des entrées dans le « constant pool ». Une autre optimisation, nécessaire puisqu'il n'y a pas de chaînes de caractères en Java Card, s'appelle la « tokenization »: elle consiste à remplacer les noms de méthodes, champs, **etc.** par un numéro (un « token »). Ceci permet entre autres d'utiliser le nom (c'est-à-dire le « token ») pour indexer une table de méthodes au lieu d'effectuer une recherche à travers le « constant pool » et la hiérarchie de classes pour implémenter l'appel de méthodes virtuelles.

Pour prouver la correction de ces optimisations, nous avons développé un cadre qui permet de décrire la sémantique des deux formats [DJ]. La différence entre les deux formats est encapsulée dans des fonctions auxiliaires, ce qui permet d'utiliser le même système d'inférence pour spécifier les deux sémantiques. En utilisant la notion de relation logique, il a été possible de définir une relation liant une entité dans un format à l'entité lui correspondant dans l'autre format. La tâche restant à accomplir pour établir l'équivalence consiste alors à montrer que lesdites fonctions auxiliaires respectent ces relations ce qui représente une simplification majeure de la preuve. Cette technique a permis d'effectuer la preuve de correction avec l'assistance de l'outil Coq.

Dans le cadre du projet européen « Verificard » nous nous appuyons sur cette formalisation pour concevoir des transformations du byte code Java Card. L'objectif est de fournir des transformations certifiées, développées à l'aide d'un assistant de preuve. Dans un premier temps, nous nous sommes focalisés sur la « tokenisation » d'une hiérarchie de classes Java Card simplifiées. Ensuite nous allons étendre cette transformation à une représentation de classes Java Card plus proche du format réel ainsi qu'à la mise en composants de « class files » Java Card.

6.2. Validation de logiciel

Nous présentons d'abord des résultats fondamentaux sur l'analyse de flot de contrôle de programmes fonctionnels et à objets (module 6.2.1) avant de détailler un certain nombre de recherches portant sur des analyses particulières : la vérification de politiques de sécurité (module 6.2.3) et la preuve de protocoles cryptographiques à l'aide de l'interprétation abstraite (module 6.2.2). Nous décrivons ensuite nos travaux sur le débogage dynamique (module 6.2.5), la sémantique et la génération de traces (module 6.2.6) et leur application au problème de la détection d'intrusion.

6.2.1. Fondements de l'analyse de flot de contrôle

Participants : Frédéric Besson, Thomas Jensen.

Mots clés : *analyse de flot de contrôle, types non-standard, interprétation abstraite, programmation fonctionnelle et à objets.*

L'analyse de flot de contrôle est fondamentale pour la vérification de programmes fonctionnels et à objets dont le flot de contrôle ne se déduit pas par une analyse syntaxique du programme. Nos travaux ont porté sur la classification de différentes analyses de programmes à objets par la technique de l'interprétation abstraite et sur l'analyse de flot de contrôle de langages fonctionnels par l'inférence de types d'intersection de rang 2.

L'analyse de flot de contrôle est fondamentale pour la vérification de programmes fonctionnels et à objets dont le flot de contrôle ne se déduit pas avec une analyse syntaxique du programme. Pour les programmes à objets avec méthodes virtuelles, une analyse de flot de contrôle doit déterminer une sur-approximation de l'ensemble de méthodes qui peuvent effectivement être appelées par l'invocation d'une méthode virtuelle. À partir de cette information, l'analyse produit un graphe de flot de contrôle qui à chaque appel de méthode indique où dans le programme l'exécution va se poursuivre. Ces graphes servent ensuite pour rendre d'autres analyses plus précises ou pour vérifier des propriétés comme les propriétés de sécurité (voir 6.2.3).

Une partie de nos travaux a été consacrée à une comparaison de la précision de différentes analyses de flot de contrôle pour les programmes à objets. Une telle comparaison est rendue difficile du fait que les analyses existantes sont exprimées avec des formalismes différentes et pour différents langages à objets. Nous avons utilisé la théorie de l'interprétation abstraite pour construire un cadre sémantique qui permet de comparer la précision des analyses et nous avons appliqué ce cadre à des analyses existantes comme la « rapid type analysis » et l'analyse « 0-CFA » [JS01].

D'autres travaux ont poursuivi nos études de la spécification d'analyses par des systèmes de types « non-standard ». Avec A. Banerjee de Kansas State University nous avons conçu un algorithme pour l'analyse de flot de contrôle d'un langage fonctionnel d'ordre supérieur [BJ]. L'algorithme est fondé sur un système de types d'intersection de rang 2, modifiés pour pouvoir modéliser le flot de fonctions d'un programme. La restriction du rang de types d'intersection est connu pour rendre l'inférence de types d'intersection standards décidable. Dans notre cas, cette restriction permet de réduire l'inférence de ces types à un problème de résolution de contraintes « de premier ordre », ce qui reduit la complexité de l'algorithme.

Nous poursuivons actuellement le travail autour de l'analyse de flot de contrôle pour les langages à objet comme Java et Java Card. Ce travail concerne à la fois la conception de nouvelles analyses adaptées à traiter des fragments de programmes et la mise en oeuvre d'analyses existantes pour fournir des graphes de flot de contrôle pour les vérifications de propriétés de sécurité (voir 6.2.3 et 6.2.4).

6.2.2. Preuve et interprétation abstraite pour la vérification de protocoles cryptographiques

Participants : Valérie Viet Triem Tong, Thomas Genet.

Mots clés : *preuve assistée, interprétation abstraite, vérification, protocoles cryptographiques*.

Nous nous intéressons à l'utilisation des interprétations abstraites pour la simplification de certaines preuves réalisées à l'aide de démonstrateurs ou d'assistants de preuve. En simplifiant ces preuves, nous souhaitons améliorer l'automatisation de ces outils et ainsi faciliter leur utilisation pour la vérification de systèmes ou de logiciels ayant un niveau de complexité intermédiaire. Parmi les cibles privilégiées de ce type de vérification on trouve les protocoles cryptographiques, dont les propriétés essentielles peuvent être partiellement vérifiées par interprétation abstraite, mais dont la vérification complète nécessite des mécanismes de preuves plus puissants comme, par exemple, l'induction.

La vérification des protocoles cryptographiques nécessite des techniques d'analyse particulièrement fines et sophistiquées. En effet, à cause des enjeux notamment dans le secteur bancaire, la sécurité de ces protocoles doit être garantie contre tout type d'attaque et ceci dans un contexte d'utilisation très général : pas de limites sur le nombre de sessions ou sur le nombre d'acteurs exécutant le protocole en même temps. Actuellement, la principale technique de vérification des protocoles cryptographiques – le model-checking – permet de découvrir certaines attaques, mais ne permet pas de garantir un protocole contre leur existence.

En utilisant des techniques de réécriture et d'automates d'arbres, nous avons proposé une méthode de vérification de protocoles cryptographique [GK00] utilisant une forme d'interprétation abstraite et un mécanisme de déduction simple sur des contraintes ensemblistes. À partir d'une description d'un protocole sous la forme d'un système de réécriture et d'un ensemble de requêtes possibles décrit par un automate d'arbre, nous calculons automatiquement une sur-approximation du comportement du protocole sur les requêtes possibles. Cette approximation est obtenue sous la forme d'un automate d'arbre reconnaissant un sur-ensemble des messages pouvant être échangés entre un nombre quelconque d'acteurs, pendant un nombre quelconque de sessions. À partir de ce sur-ensemble, pour montrer que le protocole a les propriétés souhaitées, il est suffisant de montrer que l'intersection entre l'ensemble approximation et un ensemble contenant tous les cas d'erreurs est vide. Ce travail a été réalisé en collaboration avec Francis Klay de France Telecom R&D.

Actuellement, nous affinons cette technique d'un point de vue théorique comme d'un point de vue pratique. Du point de vue théorique, tout d'abord, la modélisation du protocole, des acteurs, des intrus et de leur environnement a été revue. Nous avons clarifié la notion d'agent exécutant le protocole en remarquant que, selon les contextes, les notions recouvertes par ce terme sont très différentes. Pour un administrateur système, par exemple, un agent coïncide avec un login (c-à-d un identifiant). Pour un utilisateur de protocole de commerce électronique, les trois agents seront : la banque, le commerçant, l'acheteur (c-à-d un rôle). Pour le législateur, l'agent est l'auteur d'une transaction ou d'un message (c-à-d une personne physique). Enfin, en vérification, les agents sont séparés en deux catégories : honnêtes ou malhonnêtes (c-à-d une moralité). À partir de ce constat nous construisons 4 ensembles : l'ensemble des identifiants (qui peuvent etre des login, des numéros de clients, des adresses IP), l'ensemble des rôles (banque, acheteur, serveur de clés ...), l'ensemble {**honnête, malhonnête** } définissant la moralité et enfin l'ensemble (éventuellement infini) des personnes physiques et nous choisissons d'appeler "acteur" une relation sur les ensembles **Rôle**, **Personne**, **Moralité** et **Identifiant**. Ceci permet de relier, par exemple, une personne physique a plusieurs identifiants et, réciproquement, un identifiant à toutes les personnes physiques susceptibles de l'utiliser. Ceci permet également de faire apparaître qu'un identifiant partagé peut être utilisé par des acteurs honnêtes ou non ou encore, qu'un même rôle peut être joué par plusieurs personnes physiques différentes, etc.

D'un point de vue plus pratique, une nouvelle implantation des algorithmes de vérification, a été développée. Cette implantation, nommée Timbuk (voir section 5.5) permet de définir un système de réécriture, des automates d'arbres, des règles d'approximation statiques ou dynamiques et de calculer une sur-approximation de l'ensemble des termes accessibles. Cette nouvelle implantation a d'ores et déjà permis de revérifier plus simplement et plus rapidement des protocoles cryptographiques que nous avions déjà vérifiés [GK00]. Elle est maintenant en cours d'expérimentation sur la nouvelle modélisation des protocoles cryptographiques. Timbuk est également utilisé par Frédéric Oehl et David Sinclair de l'université de Dublin pour la vérification de protocoles cryptographiques dans une approche combinant à la fois un assistant de preuve (Isabelle/HOL) et des approximations (réalisées avec Timbuk) [OS01].

À terme, ceci doit permettre de vérifier des propriétés plus fines sur des protocoles cryptographiques plus complexes comme le protocole SET de VISA et MASTERCARD.

En dehors du cas particulier de la vérification des protocoles cryptographiques, l'intérêt d'un système comme Timbuk est de prouver facilement des propriétés sur des systèmes de réécriture non terminants qui sont généralement en dehors du spectre des outils classiques de démonstration pour lesquels la terminaison est indispensable [GVTT01].

6.2.3. Analyse de propriétés de sécurité

Participants : Frédéric Besson, Marc Eluard, Thomas Jensen, Thomas de Grenier de Latour.

Mots clés : *téléchargement, sécurité, chargement dynamique, Java*.

Nous avons proposé un cadre de définition de politiques de sécurité reposant sur une logique temporelle linéaire à deux niveaux. Nous avons montré que ce modèle est suffisamment expressif pour décrire une variété de politiques de sécurité communes et nous avons proposé une méthode de « model checking » automatique pour la vérification de propriétés de cette logique. Ensuite nous avons montré comment la politique de sécurité du dernier environnement de développement de Java (JDK 1.2) peut s'exprimer dans notre logique. La sécurité d'un système informatique dépend en général d'un ensemble de contrôles de nature très variée (vérification formelle, analyse statique, analyse dynamique, gestionnaire de sécurité, protocole d'authentification, contrôles d'accès, etc.). Une difficulté majeure dans ce domaine est de pouvoir déterminer la politique globale de sécurité qui est assurée par cette association de contrôles spécifiques. L'évolution récente vers des langages de programmation qui offrent des fonctions de sécurité propres (comme Java ou Telescript) permet d'espérer des progrès en matière de vérification formelle de politiques de sécurité. Beaucoup reste cependant à accomplir comme le montrent les discussions récurrentes sur la sécurité des différentes versions d'environnements de Java. Dans ce contexte, on peut décomposer le problème en trois tâches complémentaires :

- La définition formelle de la sémantique du langage de programmation $\mathcal{L}$ (avec ses fonctions de sécurité).
- La spécification formelle de la politique de sécurité $\mathcal{P}$ qui doit être assurée.
- La vérification que la politique $\mathcal{P}$ est effectivement assurée par un système donné (décrit dans le langage $\mathcal{L}$).

Nous avons étudié ces trois aspects en fournissant un cadre général de spécification de politiques de sécurité et en décrivant son instanciation au langage Java et à son environnement de développement JDK 1.2 [JLT99],[Jen99].

Notre cadre de définition de politiques de sécurité repose sur un modèle abstrait de programmes comportant des opérations génériques de contrôle de sécurité. Leur sémantique opérationnelle est définie comme un système de transitions sur des états constitués de piles de contrôle. Les politiques de sécurité sont exprimées dans une logique temporelle linéaire à deux niveaux (les objets étant définis par des suites de piles). Nous avons montré que ce formalisme est suffisamment expressif pour décrire une variété de politiques de sécurité communes (séparation des devoirs ou « segregation of duty », protection de ressources, bac à sable) avec une attention particulière à la politique de sécurité du dernier environnement de développement de Java (JDK 1.2) et des propriétés de sécurité d'applications pour les cartes à puce multi-applicatives programmées en Java Card.

Dans une communication précédente, nous avons proposé une méthode automatique (et complète) de vérification de propriétés pour cette logique [JLT99]. Cette méthode de vérification était soumise à certaines restrictions (concernant notamment la récursivité mutuelle). Ces restrictions ont pu être levées grâce à une nouvelle technique de « model checking » basée sur une représentation de formules temporelles par des automates finis [BJMT01]. Nous étudions maintenant comment modulariser cette méthode de vérification afin de mieux analyser des applications utilisant le chargement dynamique de classes en Java.

6.2.4. Analyse de sécurité d'applettes Java Card

Participants : Marc Eluard, Thomas Jensen.

Mots clés : *cartes à puce multi-applicatives, Java Card, pare feu, sémantique opérationnelle, résolution de contraintes.*.

Le langage Java Card définit un modèle de sécurité différent du modèle de Java. Par défaut, les applettes installées sur une carte Java Card sont séparées par un pare-feu et ne peuvent communiquer entre elles. La communication entre applettes se fait par la création et les échanges des objets partagés. Nous nous sommes attaqués au problème de vérifier que les accès aux données rendus possibles par des objets partagés ne divulguent pas des informations confidentielles. Pour ce faire, il a d'abord été nécessaire de donner une déscription formelle (en terme d'une sémantique opérationnelle) du pare feu Java Card [lJD01][SJl01]. Pour calculer une approximation sûre des accès effectués pendant l'exécution, nous nous appuyons sur des analyses statiques de flot de données et de contrôle. Nous avons conçu une analyse de flot de contrôle pour Java Card qui prend en compte les actions du pare feu sur les interactions entre applettes pour modéliser finement les comportements possibles d'une applette Java Card. Cette analyse nous a amené à modifier l'algorithme itératif de résolution de systèmes de contraintes pour qu'il génère le système à resoudre de façon paresseuse en fonction des resultats obtenus par les itérations précedentes [Élu01]. Ces travaux se poursuivent dans le projet européen IST SECSAFE (cf module 7.6).

6.2.5. Analyse de trace automatisée

Participants : Mireille Ducassé, Erwan Jahier.

Mots clés : *débogage, analyse dynamique, traceur abstrait, Prolog, Mercury, langage C.*

Nous avons développé des outils qui analysent les traces d'exécution de programmes générées par un traceur bas niveau. Les programmeurs peuvent spécifier de manière précise ce qu'ils veulent observer du comportement du programme à l'aide de requêtes exprimées en Prolog. À partir du langage de requêtes, nous avons bâti des analyses qui fournissent des vues abstraites des exécutions selon certains critères. Il a également été possible de mettre en oeuvre à faible coût des traceurs abstraits pour des langages de haut niveau. Les techniques de base exploitent une trace dont le seul pré-requis est d'être séquentielle. Nous avons montré cette généralité en appliquant ces principes aux langages Prolog, Mercury et C.

Nous avons développé des outils (cf. module 5.2) qui analysent les traces d'exécution de programmes générées par un traceur bas niveau (cf. module 3.4). Le programmeur peut poser des questions sur les exécutions à l'aide de Prolog et de quelques primitives dans une forme concise en s'appuyant sur la logique et les mécanismes de recherche du langage. Les programmeurs peuvent donc, à l'aide de requêtes de haut niveau, spécifier de manière précise ce qu'ils veulent observer du comportement du programme.

Le prototype initial, Opium [Duc99], était essentiellement dédié au débogage. Nous avons montré avec Morphine comment il est possible d'utiliser un traceur doté d'un module d'analyse de traces pour faire davantage que du débogage. Par exemple, nous pouvons calculer un taux de couverture de jeu de test afin d'en évaluer la qualité. Des « moniteurs » qui surveillent le comportement des programmes peuvent également être facilement mis en oeuvre. Ainsi, au lieu de fabriquer des instrumentations **ad hoc** comme c'est le cas actuellement pour de tels outils, on peut utiliser un environnement uniforme, ce qui permet une synergie entre les outils. De plus, les instrumentations **ad hoc** nécessitent de bien connaître le système à instrumenter, que l'instrumentation se fasse au niveau bas ou par transformation de source à source. Même si elle n'est pas techniquement très difficile, cette tâche demande un effort de programmation non négligeable. Dans notre cas, l'instrumentation étant générique, elle est faite une fois pour toutes et les analyses spécifiques peuvent être relativement simples [JD02].

À partir du langage de requêtes, nous avons également bâti des analyses qui fournissent des vues abstraites graphiques d'exécutions Mercury (par exemple, arbres de preuves, graphes de flot de contrôle). Grâce à la flexibilité de nos mécanismes, chacune de ces vues ne nécessite que quelques lignes de Mercury. Les temps d'exécution sont acceptables [DJ01].

Nous avons un projet RNTL en cours sur l'analyse de trace d'exécutions de programmes sous contraintes (cf. module 7.1). Dans ce cadre, nous collaborons avec l'INRIA Rocquencourt sur la conception d'un modèle de trace et la méthodologie de conception de traceurs [LDDJ01]. À cette occasion, M. Ducassé co-encadre avec P. Deransart la thèse de Ludovic Langevine.

6.2.6. *Sémantique des traces*

Participants : Mireille Ducassé, Erwan Jahier, Olivier Ridoux.

Mots clés : *débogage, traceur, modèle de traces, sémantique, continuation, Prolog.*

Nous proposons une architecture formelle pour spécifier, prototyper et valider des modèles de traces d'exécutions Prolog. Cette architecture est basée sur une sémantique opérationnelle par continuations. Les spécifications formelles peuvent être exécutées par une transcription directe en λProlog. Cela permet d'expérimenter différents modèles de traces et de les valider.

Le modèle de base pour tracer des exécutions Prolog est le modèle de Byrd [Byr80]. De nombreux systèmes l'utilisent, mais avec différentes interprétations ce qui fait qu'ils génèrent des traces différentes. Ces divergences ne sont certainement pas toutes intentionnelles, certaines étant dues au fait que la spécification originale est informelle.

Pour remédier à ce problème, nous proposons une architecture formelle permettant de spécifier, de prototyper et de valider des modèles de traces d'exécutions de Prolog. Cette architecture est basée sur une sémantique opérationnelle par continuation. Nous donnons une spécification formelle du modèle de traces de Byrd et nous montrons comment cette spécification peut être étendue pour spécifier des modèles de traces plus riches. Nous montrons également comment ces spécifications peuvent être exécutées par une transcription directe en λProlog ; nous obtenons ainsi un méta-interprète Prolog qui calcule des traces d'exécutions. Ce méta-interprète peut être utilisé pour expérimenter différents modèles de traces et pour les valider [JDR01].

6.2.7. *Détection d'intrusions*

Participants : Mireille Ducassé, Jean-Philippe Pouzol.

Mots clés : *sécurité, analyse d'audit, intrusion, attaque.*

Dans la continuité des travaux sur l'analyse de traces, Lande démarre une activité autour de l'analyse d'audits dans le cadre de la détection d'intrusions. La détection d'intrusions est une analyse de l'activité d'un système visant à rapporter à l'officier de sécurité toute utilisation suspecte. Nous concevons un langage de haut niveau de spécification de signatures d'attaques.

Dans la continuité des travaux sur l'analyse de traces, Lande démarre une activité autour de l'analyse d'audits dans le cadre de la détection d'intrusions.

Une stratégie classique pour sécuriser un système informatique consiste à construire un bouclier protecteur autour de lui. Les utilisateurs désirant accéder aux données ou ressources du système doivent franchir des barrières de sécurité que constituent, par exemple, des mécanismes d'identification ou de cryptographie. Toutefois, le développement des systèmes ouverts, ainsi que la prolifération de machines hétérogènes connectées à des réseaux, rendent complexe et peu praticable la mise en oeuvre de mécanismes de sécurité totalement fiables.

Une défense possible face aux utilisations abusives d'un système est la **détection d'intrusions**. La détection d'intrusions est une analyse de l'activité du système visant à rapporter à l'officier de sécurité toute utilisation suspecte. Afin de procéder à cette analyse il convient d'effectuer un audit, dit de sécurité, qui alimentera le processus d'analyse. Cet audit fournit une séquence d'événements qui s'apparente à une trace d'exécution de programme.

Nous concevons un langage de haut niveau de spécification de signatures d'attaques. Les signatures d'attaques sont les manifestations des attaques dans les systèmes attaqués. Dans les systèmes existants, les signatures d'attaques sont très proches des algorithmes de détection. De ce fait, elles contiennent trop de détails de bas niveau. Des approches récentes ont proposé des langages déclaratifs de spécification de signatures qui élèvent le niveau d'abstraction. Cependant, ces langages n'ont pas toujours de support opérationnel.

Nous montrons comment transformer des signatures déclaratives en signatures opérationnelles. Un langage de spécification de signatures, appelé **Sutekh**, est proposé. Un algorithme qui produit automatiquement des règles de détection pour des systèmes existants est défini [PD01].

Ces travaux se situent dans le contexte du projet RNTL Dico (cf module 7.3).

7. Contrats industriels

7.1. Projet RNTL OADYMPPAC

Participants : Mireille Ducassé, Erwan Jahier.

Mots clés : *environnement de programmation, programmation logique avec contraintes, débogage, visualisation.*

Le projet OADYMPPAC a démarré officiellement le 15 novembre 2000, pour 3 ans. Un des objectifs du projet est de mettre en forme et d'expérimenter des techniques de trace génériques pour des programmes logiques avec contraintes. Cela facilitera la définition d'outils d'observation et de mise au point. Un autre aspect est d'étudier l'apport, à la conception de tels outils, des progrès réalisés en matière de visualisation d'information sur de grands ensembles de données. Cela permettra, en parallèle, la définition et l'expérimentation de nouveaux outils de mise au point. Il y a deux champs d'application : d'une part, la programmation avec contraintes et, en particulier, une meilleure compréhension du comportement des solveurs ; d'autre part le développement de techniques génériques de visualisation d'information adaptées à l'analyse visuelle des traces produites par les phénomènes dynamiques.

Domaine de recherche assez récent, la visualisation interactive d'information a pour objectif d'aider la compréhension de données ou de processus abstraits au moyen de la production de représentations visuelles interactives de ces données. La visualisation d'information se présente comme un sous-domaine des sciences cognitives appliquées, dont le but est d'amplifier les mécanismes de cognition en tirant profit au mieux des particularités connues de notre système perceptif.

Le projet travaille, actuellement, sur les formats de traces communs aux divers outils (cf module 6.2.5). Un modèle de trace [LDDJ01] ainsi que des formats d'échange concrets (HTML) ont été spécifiés. Des analyses de traces ainsi que des outils de visualisation sont en cours de conception. Le projet maintient une page d'information http://contraintes.inria.fr/OADymPPaC/.

Cette action bénéficie d'un soutien du ministère de la recherche, sous la forme d'un contrat RNTL. Les partenaires industriels du consortium sont Ilog et Cosytec. Nos partenaires universitaires sont l'INRIA Rocquencourt, l'université d'Orléans et l'école des Mines de Nantes.

7.2. Projet RNTL « Cote » : Test de composants

Participant : Thomas Jensen.

Mots clés : *Test, UML.*

Le projet Lande en collaboration avec Lionel van Aertryck de la société AQL participe avec les projets Triskell et Vertecs de l'Irisa au projet « Cote » qui a comme autres partenaires Softeam, IMAG, France Télécom R&D et Gemplus. Le projet est de nature « pré-compétitif » et a comme objectif de fournir des méthodes, techniques et outils pour tester et vérifier les composants logiciels. Le projet vise à réunir et étendre des techniques de test appliquées sur des modèles, afin de les transposer à l'approche de conception de logiciels par composants. Le cadre choisi est celui du langage UML qui fournit un langage suffisamment riche pour décrire à la fois l'architecture des composants et les cas de test. La participation de projet Lande concerne particulièrement la génération de cas de test à partir d'une stratégie de test choisie (voir aussi la description de l'outil Casting 5.1).

7.3. Projet RNTL Dico

Participants : Mireille Ducassé, Jean-Philippe Pouzol.

Mots clés : *Détection d'intrusions coopérative*.

Les techniques de détection d'intrusions, bien que prometteuses, sont encore imparfaites. Elles génèrent en effet des alertes de granularité trop fine, provoquent beaucoup de faux positifs (alerte générée alors qu'il n'y a pas d'attaque) et de faux négatifs (pas d'alerte générée alors qu'il y a une attaque). Tout cela complique l'analyse et le diagnostic final d'un administrateur de sécurité, en le submergeant d'alertes parmi lesquelles il est difficile, voire impossible, d'extraire les plus pertinentes.

Il est donc nécessaire de proposer de nouvelles approches pour améliorer le taux d'attaques détectées, la qualité du diagnostic ainsi que les performances des outils de détection d'intrusions. L'objectif du projet est double. Il s'agit de proposer de nouvelles techniques pour, d'une part, détecter des malveillances et, d'autre part, réduire le nombre et améliorer la qualité des alertes générées par corrélation.

Dans ce cadre, Lande participera plus particulièrement à la définition d'un langage de description de haut niveau de scénarios, permettant la description des attaques (cf module 6.2.7). En collaboration avec l'équipe Armor, Lande se propose de développer une sonde de détection d'intrusions qui utilisera les résultats précédents. Le projet RNTL mettra en commun toutes les sondes implantées par les partenaires. Il développera des bases de données de corrélation et un environnement d'expérimentation pour la Détection d'intrusions coopérative.

Cette action a obtenu le label RNTL au printemps 2001. Son financement est en cours de négociation avec le ministère de la recherche. Nos partenaires industriels sont NetSecure Software et France Telecom R&D. Nos partenaires universitaires sont l'école normale supérieure de Cachan (laboratoire LSV) et la FERIA de Toulouse avec ses composants ONERA et IRIT. Dans le cadre de ces coopérations, Mireille Ducassé co-encadre avec Hervé Debar et Ludovic Mé la thèse CIFFRE de Benjamin Morin, qui se déroule chez France Telecom R&D.

7.4. Action Two

Participants : Thomas Jensen, Olivier Ridoux, Lionel Van Aertryck.

Mots clés : *test en boîte noire, test en boîte blanche, test structurel, objectif de test, contrainte, jeu de test, suite de test.*

Nous avons proposé une méthode de génération de suites de test qui forme le noyau de l'outil Casting développé en collaboration avec la société AQL. La première version du prototype prend en entrée des spécifications B. Nous travaillons maintenant, en collaboration avec différents partenaires universitaires et industriels, à l'exploitation de ces techniques pour la génération de jeux de test structurels (pour C, C++ et UML).

Nos travaux sur la génération automatique de jeux de test ont été initiés dans le cadre d'une collaboration avec la société rennaise AQL à travers une bourse Cifre puis le stage de post-doc industriel de Lionel Van Aertryck. Ils ont conduit à la réalisation du prototype Casting, un outil qui permet de générer des jeux de test à partir de spécifications B. Cette génération peut être automatique ou interactive en fonction des besoins de l'utilisateur. Le prototype en question est maintenant robuste et il en a été fait plusieurs démonstrations, notamment lors de la conférence B.

Ces travaux sur la génération automatique de jeux de test ont pris une nouvelle dimension dans le cadre de deux collaborations industrielles : le projet européen Two (**Test and Warning Office**, Industrial RTD Project no 25503, ref. Inria : 1 98 C 344) et l'action effectuée dans le cadre du projet RNTL « Cote ».

Le projet Two a commencé en octobre 1998 et s'est terminé en 2001. Il a impliqué le centre de recherche du CEA, le Politecnico di Milano (Italie), les sociétés Elsag Bailey (Italie), Siemens (Allemagne), Spacebel Informatique (Belgique) et l'éditeur d'outils de tests Attol Testware (France) qui pilote le projet.

L'objectif du projet Two a été de concevoir un outil de génération de jeux de test structurels pour C et C++. Cet outil se décompose en trois phases principales : l'analyse des codes sources, la génération de contraintes correspondant à un objectif de test donné et la résolution de ces contraintes pour engendrer les jeux de test effectifs. Notre intervention se situe essentiellement dans la troisième phase. L'outil mis au point dans le

cadre du projet Two sera intégré à l'environnement de test actuellement commercialisé par Attol Testware : il facilitera la tâche du testeur tout en permettant les mesures de taux de couverture offertes par l'outil Attol Coverage. Les services ajoutés qui ont été fournis par le projet Two correspondent à une demande forte de la part des utilisateurs actuels de l'environnement d'Attol Testware.

7.5. Action Java-Sécurité

Participants : Marc Eluard, Thomas Jensen.

Mots clés : *téléchargement, vérification, analyse, sécurité, sûreté, chargement dynamique, visibilité, typage, Java.*

Dans le cadre de l'action VIP du GIE Dyade, nous avons proposé une formalisation de la sémantique de certains aspects du langage Java et Java Card. Nous nous sommes focalisés en ce qui concerne Java sur les règles de visibilité (des classes et de leurs membres) et leur évolution lors du chargement dynamique de classes et en ce qui concerne Java Card sur le pare-feu et les objets partageables qui servent à sécuriser la communication entre applettes installées sur une carte à puce multi-applicative.

Nous participons à l'action VIP du GIE Bull-Inria Dyade. Le thème de cette collaboration est la formalisation de certains aspects de la sémantique de Java et la preuve de propriétés de sécurité de programmes (cf. module 6.2.3). L'étude des problèmes de sécurité (au sens de confidentialité et d'intégrité notamment) dans le contexte du langage Java représente un défi de première importance pour plusieurs raisons :

- La sûreté (au sens du typage) et la sécurité sont présentées comme des arguments pour la promotion d'un langage qui a vocation à être utilisé dans des contextes mettant en jeu des coopérations entre des codes issus de sites différents.
- Le langage inclut des caractéristiques complexes (comme le chargement dynamique ou des règles de visibilité inhabituelles) qui justifient le besoin de définition formelle. Une telle définition permettrait de clarifier certains aspects du langage et servirait de base à un raisonnement rigoureux sur des propriétés cruciales comme la sûreté du typage ou la garantie de politiques de sécurité.
- Le développement de Java Card, la version de Java dédiée aux cartes à puce, augmente encore l'importance des défis cités plus haut et permet de les aborder dans un cadre restreint, permettant l'application de techniques (analyse, preuve) plus sophistiquées.

Nous nous sommes attaqués à cette formalisation en nous focalisant sur les règles de visibilité (des classes et de leurs membres) et leur évolution lors du chargement dynamique de classes. Il s'agit en effet de caractéristiques particulières de Java qui ont un impact direct sur la sécurité et dont les définitions informelles ne sont pas exemptes d'ambiguïtés ou d'insuffisances. Cette formalisation en terme de systèmes d'inférence nous a permis de décrire de manière rigoureuse l'origine d'une erreur de sécurité qui avait été découverte empiriquement par des chercheurs d'ATT.

Nous avons ensuite étudié comment décrire formellement le pare-feu de Java Card. La spécification du langage Java Card comprend la description d'un pare-feu entre les applettes installées sur une carte. Ce pare-feu garantit par défaut une séparation totale entre différentes applettes mais il peut être contourné en s'appuyant sur la notion d'**objets partagées** qui permettent d'échanger des objets entre applettes. Afin d'analyser les conséquences en matière de sécurité d'un partage des objets il est nécessaire de mettre la description informelle de la spécification Java Card sous une forme qui permet d'effectuer des vérifications formelles. Nous avons décrit une sémantique opérationnelle du pare-feu Java Card et nous étudions actuellement comment extraire de cette sémantique des analyses statiques permettant de construire des modèles abstraits afin d'y appliquer nos techniques (décrites en module 6.2.3 de vérification de propriétés de sécurité.

7.6. Action Secsafe

Participants : Thomas Jensen, Marc Éluard, Frédéric Besson, Florimond Ployette, Thomas de Grenier de Latour.

Mots clés : *Sécurité, analyse statique, cartes à puce, code mobile, Java, Java Card.*.

Le projet européen Secsafe porte sur la sécurité de logiciels et l'analyse statique avec une focalisation sur les langage Java et Java Card. Deux domaines d'application sont visés : le code mobile et les cartes à puce. Le projet a deux partenaires académiques (Imperial College de l'Université de Londres et l'Université technique du Danemark) et la PME Trusted Logic, spécialisée en sécurité et cartes à puce.

Le projet européen Secsafe qui a commencé en 2000 porte sur la sécurité de logiciels et l'analyse statique avec une focalisation sur les langage Java et Java Card. Le choix de Java comme langage à étudier permet d'appliquer nos analyses à deux domaines différents : le code mobile et les cartes à puce. Les analyses sont fondées sur nos travaux de formalisation de Java et Java Card (voir modules 6.2.3 et 7.5). Le projet a deux partenaires académiques (Imperial College de l'Université de Londres et l'Université technique du Danemark) et la PME Trusted Logic, spécialisée en sécurité et cartes à puce.

7.7. Action Verificard

Participants : Thomas Jensen, Thomas Genet, François Monin.

Mots clés : *cartes à puce, Java Card, transformation et compilation de programmes, assistants de preuves.*

Le projet Verificard (IST R&D 2000-26328) est un projet entre l'université de Nijmegen, l'université technique de Munich, l'université de Hagen, Swedish Institute of Computer Science, Schlumberger CP8, Gemplus et l'Inria. Le projet a comme objectif de fournir des méthodes de validation et de vérification d'une plate-forme et d'applications Java Card. Pour ce faire, on propose d'intégrer des techniques de vérification de modèles dans des assistants de preuves comme Coq, PVS ou HOL. Comme la sécurité d'une application est conditionnée par le bon fonctionnement de la plate-forme d'exécution, une partie du projet concerne le développement d'outils certifié pour la manipulation de programmes Java Card. Notre participation porte sur la construction d'un transformateur certifié pour le byte code Java Card (voir 6.1.5).

7.8. Action Castor

Participants : Pascal Fradet, Thomas Lefort, Lakshminarayanan Renganarayanan.

Mots clés : *architectures de logiciel, vues, cohérence, sécurité, analyse, vérification.*

L'objectif du projet Castor est de fournir un environnement permettant de décrire l'architecture d'un système d'informations et d'étudier ses propriétés de sécurité. L'analyse d'une telle architecture doit permettre de modéliser ou synthétiser des scénarios d'attaques, de détecter des failles de sécurité et de guider dans la mise en oeuvre de parades. Le projet Castor, financé par le Celar, regroupe les sociétés Sycomore EADS, AQL et TNI et les projets EP-ATR et Lande de l'Irisa. Son objectif est de fournir un environnement permettant de décrire l'organisation globale d'un système d'informations sous forme de vues et d'étudier ses propriétés de sécurité. Nous nous sommes concentré sur les problèmes de cohérence liés aux descriptions multi-vues et à l'analyse de sécurité (voir section 6.1.1). Un prototype de vérification et d'analyse a été intégré à l'environnement de modélisation Castor.

8. Actions régionales, nationales et internationales

8.1. Actions nationales

Le projet Lande participe à l'action ASP « Unification des méthodes de test ». Les autres partenaires sont le LAMI (Evry), le LRI (Orsay) et le LSR-Imag (Grenoble).

Le projet Lande participe à l'Action de Recherche Coopérative S-Java qui associe les projets Oasis, Coq et Lande et une équipe de l'ENS à trois partenaires industriels : France Telecom R&D, Gemplus et Trusted Logic. L'objectif de l'action est de concevoir des méthodes de conception et d'analyse de programmes Java certifiés.

Le projet Lande participe à l'action SmartTool dans le cadre du GIE Bull-Inria Dyade sur le développement d'un environnement de programmation. Les autres partenaires sont les projets Oasis, Coq et l'action Vasy ainsi que Bull et Microsoft.

8.2. Réseaux et groupes de travail internationaux

Mireille Ducassé est membre de l'ACM (Association for Computing Machinery). Mireille Ducassé, Erwan Jahier et Olivier Ridoux sont membres de l'ALP (Association for Logic Programming).

8.3. Relations bilatérales internationales

Thomas Jensen est, avec S. Peyton Jones de Microsoft Research, chercheur consultant sur le projet australien « Constraint-based program analysis » conduit par les universités de Monash et de Melbourne.

9. Diffusion des résultats

9.1. Animation de la communauté scientifique

Mireille Ducassé édite un numéro spécial du « Journal of Automated Software Engineering » sur le débogage automatisé [Duc02]. Elle a été membre des comités de programme de LOPSTR 2001 (LOgic-based Program Synthesis and TRansformation), et de WLPE'01 (International Workshop on Logic Programming Environments). Elle est membre du bureau de l'Association Française de Programmation en Logique et avec Contraintes. Elle est membre élu du conseil scientifique de l'Insa de Rennes depuis septembre 1994, présidente de la commission de spécialistes 27e section de l'INSA de Rennes et membre des commissions de spécialistes 27e section des universités de Rennes 1 et de la Réunion. Elle est rapporteur pour l'HDR de Frédéric Mesnard (La Réunion) et membre du jury de thèse de François Pennaneac'h (direction Jean-Marc Jézéquel).

Olivier Ridoux a fait partie du comité de programme de FLOPS2001. Il a été rapporteur pour les HDR de Jean-Paul Bodeveix (Toulouse) et Frédéric Mesnard (La Réunion), et membre des jurys des thèses d'Irène Grosclaude (direction Marie-Odile Cordier) et Marc Éluard (direction Thomas Jensen). Il a organisé les « journées pédagogiques de l'Ifsic » sur le thème de « analyse de données et entrepôts de données ».

Thomas Jensen a présidé le comité de programmes de la conférence e-Smart 2001 sur la programmation et la sécurité de cartes à puce [AJ01]. Il a fait partie des comités de programme de European Symposium on Programming (ESOP'2002) et du Workshop on Model Checking and Abstract interpretation. Par ailleurs, il a été examinateur sur la thèse d'Eva Rose (Université de Paris 7). À partir de 2001, il est responsable scientifique de l'école « Jeunes Chercheurs » en Programmation organisée sous l'égide du GDR ALP.

9.2. Enseignement universitaire

Pascal Fradet et Thomas Jensen assurent un module de DEA de l'IFSIC, Université de Rennes 1, sur la sémantique et l'analyse de programmes.

Pascal Fradet donne un mini-cours sur la sécurité des logiciels en 5ème année INSA et intervient dans un cours d'initiation à la programmation en DEUG.

Thomas Jensen et Mireille Ducassé ont donné chacun un cours d'une journée respectivement sur l'analyse statique et la méthode formelle B à l'école « Jeunes Chercheurs » en Programmation à Cargèse.

Olivier Ridoux est le responsable de la maîtrise d'informatique de l'université de Rennes 1. Il enseigne la programmation et le génie logiciel en DEUG, et les systèmes d'exploitation et la compilation en maîtrise d'informatique. Il co-encadre à l'Université de Bretagne Sud un doctorat sur « une approche logique pour la compréhension des énoncés oraux » [VAR01].

Mireille Ducassé est responsable de l'option industrielle de la dernière année de la formation d'ingénieur en informatique de l'INSA de Rennes. Elle enseigne la compilation et la méthode formelle « B » au niveau bac+4, ainsi que la qualité du logiciel au niveau bac+5. Elle encadre un projet annuel de 8 étudiants, niveau bac+4, qui travaillent sur le logiciel Coca (cf module 5.2). Un rapport technique avec une étude de cas pédagogique pour « B » a été publié [DR01].

Thomas Genet enseigne la programmation fonctionnelle en DEUG, la méthode formelle « B » en maîtrise d'informatique. Il assure également un module de DEA sur les méthodes déductives pour la vérification (en collaboration avec Vlad Rusu du projet VERTECS).

Le projet a encadré les étudiants de DEA suivants : Thomas de Grenier de Latour (*vérification de sécurité modulaire*), Ludovic Langevine (*Trace de programmes logiques avec contraintes*), Thomas Lefort (*OCL et résolution de contraintes*).

Par ailleurs, le projet a reçu Emmanuel Hainry de l'ENS Lyon en juin-juillet 2001 pour un stage de première année de magistère portant sur l'analyse de programmes Java Card. Il a également re cu, deux semaines, Gyongyi Szilagyi chercheuse à l'académie des sciences hongroise, sur l'analyse de programmes logiques avec contraintes dans le cadre du projet RNTL OADYMPPAC (cf module 7.1).

9.3. Participation à des colloques, séminaires, invitations

Mireille Ducassé a été invitée à présenter ses travaux sur le débogage automatisé au centre de recherche de la NASA à AMES, Californie.

Yoann Padioleau et Olivier Ridoux ont présenté leurs travaux sur l'expressions des contraintes en formules de Harrop (voir RA2000) au LIFO (Laboratoire d'Informatique Fondamentale d'Orléans). Noter aussi la publication par le Journal of Functional and Logic Programming d'un article sur l'analyse statique typée (voir aussi RA2000 [RB01]).

Thomas Jensen a donné des conférences invitées sur l'analyse statique pour la sécurité logicielle au Dagstuhl workshop « Security through Verification and Analysis » et à la conférence « Mathematical Foundations of Programming Semantics (MFPS 17) ».

10. Bibliographie

Bibliographie de référence

[BBR] C. BELLEANNÉE, P. BRISSET, O. RIDOUX. *A pragmatic reconstruction of λProlog.* in « Journal of Logic Programming, 41(1), 1999. », note : Version française dans TSI 14(9):1131–1164:1995.

[BL93] J.-P. BANÂTRE, D. LE MÉTAYER. *Programming by multiset transformation.* in « Communications of the ACM », numéro 1, volume 36, 1993, pages 98-111.

[DF98] R. DOUENCE, P. FRADET. *A systematic study of functional language implementations.* in « ACM Transactions on Programming Languages and Systems », numéro 2, volume 20, 1998, pages 344–387.

[DN94] M. DUCASSÉ, J. NOYÉ. *Logic programming environments: dynamic program analysis and debugging.* in « Elsevier Journal of Logic Programming », volume 19/20, mai/juillet, 1994, pages 351-384, http://www.irisa.fr/EXTERNE/bibli/pi/pi910.html

[Duc99] M. DUCASSÉ. *Opium: An extendable trace analyser for Prolog.* in « Elsevier Journal of Logic programming », volume 39, 1999, pages 177-223, note : Special issue on Synthesis, Transformation and Analysis of Logic Programs, A. Bossi and Y. Deville (eds).

[FR00] S. FERRÉ, O. RIDOUX. *A File System Based on Concept Analysis.* éditeurs Y. SAGIV., in « DOOD2000, 1st Int. Conf. Computational Logic, LNAI 1861 », 2000.

[Fra00] P. FRADET. *Approches langages pour la conception et la mise en oeuvre de programmes.* document d'habilitation à diriger des recherches, Université de Rennes 1, novembre, 2000.

[GK00] T. GENET, F. KLAY. *Rewriting for Cryptographic Protocol Verification.* in « Proceedings 17th International Conference on Automated Deduction », série Lecture Notes in Artificial Intelligence, volume 1831, Springer-Verlag, 2000, ftp://ftp.irisa.fr/local/lande/tg-fk-cade00.ps.gz

[Jen97] T. JENSEN. *Disjunctive Program Analysis for Algebraic Data Types.* in « ACM Transactions on Programming Languages and Systems », numéro 5, volume 19, 1997, pages 752–804.

[Jen99] T. JENSEN. *Analyse statiques de programmes : fondements et applications.* document d'habilitation à diriger des recherches, Université de Rennes 1, décembre, 1999.

[JLT99] T. JENSEN, D. LE MÉTAYER, T. THORN. *Verification of control flow based security properties.* in « Proc. of the 20th IEEE Symp. on Security and Privacy », New York: IEEE Computer Society, pages 89–103, mai, 1999.

[Rid98] O. RIDOUX. *λProlog de A à Z, ... ou presque.* document d'habilitation à diriger des recherches, Université de Rennes 1, avril, 1998.

Livres et monographies

[AJ00] éditeurs I. ATTALI, T. JENSEN., *Proceedings of the International Workshop on Java Card (Java Card 2000).* address Cannes, France, éditeurs I. ATTALI, T. JENSEN., Inria, septembre, 2000.

[AJ01] éditeurs I. ATTALI, T. JENSEN., *Smart Card Programming and Security (e-Smart 2001).* éditeurs I. ATTALI, T. JENSEN., Springer LNCS vol. 2140, septembre, 2001.

[Duc02] éditeurs M. DUCASSÉ., *Journal of Automated Software Engineering 9(1), special issue on automated debugging.* éditeurs M. DUCASSÉ., Kluwer, janvier 2002.

Thèses et habilitations à diriger des recherche

[Élu01] M. ÉLUARD. *Analyse de sécurité pour la certification d'applications Java Card.* thèse de doctorat, Université de Rennes 1, décembre, 2001, note : N. d'ordre : 2614.

Articles et chapitres de livre

[BFMre] J.-P. BANÂTRE, P. FRADET, D. L. MÉTAYER. *Gamma and the chemical reaction model: fifteen years after.* in « Multiset Processing (C.S. Calude, Gh. Paun, G. Rozenberg, A. Salomaa, eds.) », Springer-Verlag, (à paraître).

[BJ] A. BANERJEE, T. JENSEN. *Control-flow analysis with rank-2 intersection types.* in « Mathematical Structures in Computer Science », note : à paraître.

[BJMT01] F. BESSON, T. JENSEN, D. L. MÉTAYER, T. THORN. *Model ckecking security prperties of control flow graphs.* in « Journal of Computer Security », volume 9, 2001, pages 217–250.

[DJ] E. DENNEY, T. JENSEN. *Correctness of Java Card method lookup via logical relations.* in « Theoretical Computer Science », note : à paraître.

[DJ01] M. DUCASSÉ, E. JAHIER. *Efficient Automated Trace Analysis: Examples with Morphine.* in « Electronic Notes in Theoretical Computer Science », numéro 2, volume 55, 2001, note : K. Havelund and G. Rosu (Eds), proceedings of the first Workshop on Runtime Verification.

[JD02] E. JAHIER, M. DUCASSÉ. *Generic Program Monitoring by Trace Analysis.* in « Theory and Practice of Logic Programming », 2002, http://www.inria.fr/rrrt/rr-4323.html note : Version préliminaire en Rapport de Recherche INRIA RR-4323, Novembre 2001.

[RB01] O. RIDOUX, P. BOIZUMAULT. *Typed Static Analysis: Application to the Groundness Analysis of Typed Prolog.* in « Journal of Functional and Logic Programming », numéro 4, volume 2001, July, 2001.

Communications à des congrès, colloques, etc.

[Fer01] S. FERRÉ. *Complete and Incomplete Knowledge in Logical Information Systems.* éditeurs S. BENFERHAT, P. BESNARD., in « European Conference on Symbolic and Quantitative Approaches to Reasoning with Uncertainty, LNAI 2143 », 2001.

[FR00b] S. FERRÉ, O. RIDOUX. *A logical Generalization of Formal Concept Analysis.* éditeurs B. GANTER, G. MINEAU., in « 8th Int. Conf. Conceptual Structures, LNAI 1867 », 2000.

[FR01] S. FERRÉ, O. RIDOUX. *The Principles of a Toolbox for the Implementation of Customized Logics.* éditeurs A. PETTOROSSI., in « Int. Conf. Logic for Program Synthesis and Transformation », 2001.

[GVTT01] T. GENET, V. VIET TRIEM TONG. *Reachability Analysis of Term Rewriting Systems with Timbuk.* in « Proceedings of the 8th International Conference on Logic for Programming, Artificial Intelligence and Reasoning », série Lecture Notes in Artificial Intelligence, volume 2250, Springer-Verlag, pages 691–702, 2001.

[JDR01] E. JAHIER, M. DUCASSÉ, O. RIDOUX. *Specifying Prolog Trace Models with a Continuation Semantics.* éditeurs K.-K. LAU., in « Logic Based Program Synthesis and Transformation », Springer-Verlag, Lecture Notes in Computer Science 2042, 2001.

[JS01] T. JENSEN, F. SPOTO. *Class analysis of object-oriented programs through abstract interpretation.* éditeurs F. HONSELL, M. MICULAN., in « Proc. of Foundations of Software Science and Computation Structures (FoSSaCS'01) », Springer LNCS vol .2030, pages 261–275, 2001.

[LDDJ01] L. LANGEVINE, P. DERANSART, M. DUCASSÉ, E. JAHIER. *Prototyping **clp(fd)** tracers: a trace model and an experimental validation environment.* éditeurs T. KUSALIK., in « Proceedings of the 11th Workshop on Logic Programming Environments », Computer Research Repository, CS.PL/0111043, 2001.

[lJD01] M. ÉLUARD, T. JENSEN, E. DENNEY. *An Operational Semantics of the Java Card Firewall.* éditeurs I.

ATTALI, T. JENSEN., in « Smart Card Programming and Security (e-Smart 2001 », volume Springer LNCS vol. 2140, septembre, 2001.

[PD01] J.-P. POUZOL, M. DUCASSÉ. *From Declarative Signatures to Misuse IDS.* éditeurs W. LEE, L. MÉ, A. WESPI., in « Recent Advances in Intrusion Detection, Proceedings of the 4th International Symposium », Springer-Verlag, Lecture Notes in Computer Science 2212, pages 1-21, 2001.

[SJl01] I. SIVERONI, T. JENSEN, M. ÉLUARD. *A Formal Specification of the Java Card Applet Firewall.* éditeurs H. R. NIELSON., in « Nordic Workshop on Secure IT-Systems », novembre, 2001.

[VAR01] J. VILLANEAU, J.-Y. ANTOINE, O. RIDOUX. *Combining Syntax and Pragmatic Knowledge for the Understanding of Spontaneous Spoken Sentences.* éditeurs P. DEGROOTE, G. MORILL, C. RETORÉ., in « 4th Int. Conf. Logical Aspects of Computational Linguistics », 2001.

Rapports de recherche et publications internes

[DFS01] R. DOUENCE, P. FRADET, M. SÜDHOLT. *A study of aspect interactions.* rapport de recherche, 2001.

[DR01] M. DUCASSÉ, L. ROZÉ. *Revisiting the « Traffic lights » B case study.* Publication Interne, numéro 1424, institution IRISA, November, 2001, http://www.irisa.fr/bibli/publi/pi/2001/1424/1424.html

[Rou] S. ROUVRAIS. *Construction de services distribués: une approche à base d'agents mobiles.* Publication interne, numéro 1421, institution IRISA, novembre, http://www.inria.fr/rrrt/rr-4315.html

Divers

[Cas01] *Castor : Dossier de définition & dossier de justification (Tome 2).* Rapport d'études, AQL, Irisa, Sycomore, TNI, juin, 2001.

Bibliographie générale

[Abr96] R. ABRIAL. *The B-Book: Assigning programs to meanings.* Cambridge University Press, 1996.

[ANS] *ANSI/IEEE Standard 729-1983.* note : Glossary of Software Engineering Terminology.

[BBR] C. BELLEANNÉE, P. BRISSET, O. RIDOUX. *A pragmatic reconstruction of λProlog.* in « Journal of Logic Programming, 41(1), 1999. », note : Version française dans TSI 14(9):1131–1164:1995.

[Bei90] B. BEIZER. *Software testing techniques.* volume 2nd ed., International Thomson Computer Press, 1990.

[BGL93] B. BRUEGGE, T. GOTTSCHALK, B. LUO. *A framework for dynamic program analyzers.* in « Proc. of the OOPSLA'93 Conference », pages 65-82, 1993.

[BR93b] P. BRISSET, O. RIDOUX. *Continuations in λProlog.* éditeurs D. WARREN., in « 10th Int. Conf. Logic Programming », MIT Press, pages 27–43, 1993.

[Byr80] L. BYRD. *Understanding the Control Flow of Prolog Programs.* éditeurs S.-A. TÄRNLUND., in « Logic Programming Workshop », address Debrecen, Hungary, 1980.

[Cou97] P. COUSOT. *Abstract Interpretation Based Static Analysis Parameterized by Semantics.* éditeurs P. VAN HENTENRYCK., in « Proc. of 4th Static Analysis Symposium », Springer Verlag, LNCS vol. 1302, pages 388–394, 1997.

[Duc99] M. DUCASSÉ. *Coca: An automated Debugger for C.* in « Proceedings of the 21st International Conference on Software Engineering », ACM Press, pages 504-513, mai, 1999, http://www.inria.fr/rrrt/rr-3489.html note : (également RR-3489 INRIA).

[FR00a] S. FERRÉ, O. RIDOUX. *A File System Based on Concept Analysis.* éditeurs Y. SAGIV., in « DOOD2000, 1st Int. Conf. Computational Logic, LNAI 1861 », 2000.

[FR00b] S. FERRÉ, O. RIDOUX. *A logical Generalization of Formal Concept Analysis.* éditeurs B. GANTER, G. MINEAU., in « 8th Int. Conf. Conceptual Structures, LNAI 1867 », 2000.

[GW99] B. GANTER, R. WILLE. *Formal Concept Analysis: Mathematical Foundations.* Springer, 1999.

[JD99] E. JAHIER, M. DUCASSÉ. *An automated debugger for Mercury - Morphine 0.1 User and reference manuals.* mai, 1999, note : RT-231 INRIA (également PI-1234 IRISA).

[Kah87] G. KAHN. *Natural semantics.* in « Proceedings of STACS'87 », série LNCS 247, Springer Verlag, pages 22-39, 1987.

[Lev90] H. J. LEVESQUE. *All I Know: A Study in Autoepistemic Logic.* in « Artificial Intelligence », numéro 3, volume 42, 1990, pages 263–309.

[NN92] H. R. NIELSON, F. NIELSON. *Semantics with applications.* John Wiley & Sons, INC., 1992.

[NNH99] F. NIELSON, H. NIELSON, C. HANKIN. *Principles of Program Analysis.* Springer, 1999.

[OS01] F. OEHL, D. SINCLAIR. *Combining two approaches for the formal verification of cryptographic protocols.* in « Proceedings of ICLP Workshop on Specification, Analysis and Validation for Emerging technologies in computational logic », 2001.

[Rid91] O. RIDOUX. *MALIv06: Tutorial and Reference Manual.* Publication Interne, numéro 611, institution Irisa, 1991, note : ftp://ftp.irisa.fr/local/lande/or-tr-irisa611-91.ps.Z.

[Rid98] O. RIDOUX. *λProlog de A à Z, ... ou presque.* document d'habilitation à diriger des recherches, Université de Rennes 1, avril, 1998.

[Ros84] J. ROSSER. *Highlights of the History of the Lambda-Calculus.* in « Annals of the History of Computing », numéro 4, volume 6, 1984.

[Ros96] J. ROSENBERG. *How debuggers work.* série Wiley Computer Publishing, John Wiley & Sons, INC., 1996, note : ISBN 0-471-14966-7.

[Sch86] D. SCHMIDT. *Denotational Semantics.* Allyn & Bacon, 1986.

[SHC96] Z. SOMOGYI, F. HENDERSON, T. CONWAY. *The execution algorithm of Mercury, an efficient purely declarative logic programming language.* in « Journal of logic Programming », volume 29, October-December, 1996, pages 17-64, http://www.cs.mu.oz.au/research/mercury/information/papers.html

[XMd+94] S. XANTAKIS, M. MAURICE, A. DE AMESCUA, O. HOURI, L. GRIFFET. *Test et contrôle des logiciels. Méthodes techniques et outils.* EC2, 1994.