

Prix de thèse SPECIF 2000

Lauréat et Accessits

Lauréat: Bruno Lévy

- Titre de la thèse: Topologie Algorithmique: Combinatoire et Plongement
- Laboratoire : LORIA (Laboratoire Lorrain de Recherche en Informatique et ses Applications)
Inria Lorraine - Projet ISA - Gocad,
- Directeur de thèse: Jean-Laurent Mallet

Résumé de la thèse

Dans le domaine de la modélisation 3D, l'objectif est de définir des moyens de représenter une réalité physique par des objets informatiques. Afin de permettre des simulations de phénomènes physiques, le modèle informatique doit représenter non seulement la forme des objets concernés, mais aussi des propriétés physiques attachées à ces objets.

La modélisation 3D s'appuie sur deux principales familles de méthodes. L'une de ces familles de méthodes, appelée souvent "courbes et surfaces", se fonde sur une représentation des objets à modéliser par des fonctions (le plus souvent polynomiales). L'autre famille de représentations consiste à discrétiser les objets en cellules (sommet, segments, polygones, polyèdres . . .). Nous étudions ici les problèmes liés à ce dernier type de représentation discrète des objets, ainsi que ses relations avec les "courbes et surfaces". En utilisant le formalisme offert par la Topologie, une branche moderne des mathématiques, nous allons étudier les problèmes suivants:

- Définir des structures de données efficaces pour représenter la décomposition des objets en éléments discrets.
- Générer et éditer interactivement des objets, de manière à respecter des données ainsi que des contraintes globales concernant la forme des objets.
- Construire une paramétrisation sous contraintes d'une surface triangulée, afin de pouvoir facilement lui associer des valeurs.

Le premier point sera traité en utilisant certains résultats de topologie combinatoire, et les deux derniers seront étudiés en termes d'homéomorphisme et de transformation continue.

Nous présenterons également plusieurs applications de ces méthodes, permettant de résoudre des problèmes de modélisation en géologie numérique. Par exemple, nous montrerons comment modéliser de manière précise les variations de porosité de la roche à l'intérieur d'un réservoir naturel. Des applications possibles de nos méthodes à l'image de synthèse et au placage de textures seront également évoquées.

Accessits: Albert Cohen et Phong Q. Nguyen

(par ordre alphabétique)

Albert Cohen

- Titre de la thèse: Analyse et transformation de programmes : du modèle polyédrique aux langages formels
- Laboratoire : Laboratoire PRiSM, Université de Versailles Saint-Quentin-en-Yvelines
- Directeurs de thèse: Paul Feautrier et Jean-François Collard

Résumé de la thèse

Les microprocesseurs et les architectures parallèles d'aujourd'hui lancent de nouveaux défis aux techniques de compilation. En présence de parallélisme, les optimisations deviennent trop spécifiques et complexes pour être laissées au soin du programmeur. Les techniques de parallélisation automatique dépassent le cadre traditionnel des applications numériques et abordent de nouveaux modèles de programmes, tels que les nids de boucles non affines, les appels récursifs et les structures de données dynamiques. Des analyses précises sont au cœur de la détection du parallélisme, elles rassemblent des informations à la compilation sur les propriétés des programmes à l'exécution. Ces informations valident des transformations utiles pour l'extraction du parallélisme et la génération d'un code optimisé.

Cette thèse aborde principalement des analyses et des transformations avec une vision par instances, c'est-à-dire considérant les propriétés individuelles de chaque instance d'une instruction à l'exécution. Une nouvelle formalisation à l'aide de langages formels nous permet tout d'abord d'étudier une analyse de dépendances et de définitions visibles par instances pour programmes récursifs. L'application de cette analyse à l'expansion et la parallélisation de programmes récursifs dévoile des résultats encourageants. Les nids de boucles quelconques font l'objet de la deuxième partie de ce travail. Une nouvelle étude des techniques de parallélisation fondées sur l'expansion nous permet de proposer des solutions à des problèmes d'optimisation cruciaux.

Les contributions se répartissent en quatre catégories fortement interdépendantes. Les trois premières concernent la parallélisation automatique

et la quatrième catégorie présente des résultats sur les transductions rationnelles et algébriques.

Structures de contrôle et de données : au delà du modèle polyédrique

Dans le chapitre 2, nous définissons un modèle de programmes et des abstractions mathématiques pour les instances d'instructions et les éléments de structures de données. Ce cadre général permet de présenter nos techniques dans un cadre formel, en particulier dans le cas des structures récursives.

De nouvelles analyses de dépendances et de définitions visibles sont proposées dans le chapitre 4. Elles utilisent un formalisme de la théorie des langages formels, plus précisément des transductions rationnelles et algébriques. Une nouvelle définition des variables d'induction adaptée aux programmes récursifs permet de décrire l'effet de chaque instance à l'aide d'une transduction. Une comparaison avec d'autres analyses est effectuée.

En revanche, lorsque nous avons conçu des algorithmes pour les nids de boucles sur tableaux — un cas particulier de notre modèle — nous sommes restés fidèles aux vecteurs d'itération et nous avons profité de la quantité d'algorithmes permettant la manipulation de relations affines dans l'arithmétique de Presburger.

Expansion de la mémoire : résoudre de nouveaux problèmes

L'application de l'expansion de la mémoire à la parallélisation est une technique ancienne, mais les analyses de définitions visibles par instances se sont récemment étendues aux programmes avec des expressions conditionnelles, avec des références complexes aux structures de données — par exemple des index de tableaux non affines — ou avec des appels récursifs, et cela pose de nouvelles questions. La première est de garantir que les accès en lecture dans le programme expansé réfèrent la bonne cellule mémoire ; la deuxième question réside dans l'adéquation des techniques d'expansion avec les nouveaux modèles de programmes.

Les deux questions sont traitées dans les sections 5.1 à 5.4 pour les nids de boucles (sans restrictions) sur tableaux. Nous présentons notamment une nouvelle technique pour réduire le surcoût de l'expansion à l'exécution, et nous étendons aux nids de boucles sans restrictions une méthode de réduction de l'occupation en mémoire. La combinaison des deux est étudiée et nous proposons des algorithmes pour optimiser la restauration du flot des données à l'exécution. Quelques résultats expérimentaux sont présentés pour une architecture à mémoire partagée.

L'expansion de la mémoire pour programmes récursifs est un domaine de recherche totalement nouveau, et nous avons découvert que l'abstraction mathématique pour les définitions visibles — les transductions — peut engendrer des surcoûts importants. Nous avons néanmoins développé des algorithmes qui expansent des programmes récursifs particuliers avec un faible surcoût à l'exécution.

Parallélisme : extension des techniques classiques

Notre analyse de dépendance a été mise à profit pour paralléliser des programmes récursifs. Celle-ci démontre de nouvelles applications pratiques des transductions. Notre premier algorithme ressemble aux méthodes classiques, mais il profite de l'information plus précise recueillie par l'analyse et on obtient en général de meilleurs résultats. Un autre algorithme permet la parallélisation par instances de programmes récursifs : cette nouvelle technique est rendue possible par l'utilisation de transductions. Quelques résultats expérimentaux sont décrits, en combinant expansion et parallélisation sur un programme récursif bien connu.

Théorie des langages formels : quelques contributions et des applications

Les derniers résultats de ce travail n'appartiennent pas au domaine de la compilation. Ils se trouvent principalement dans le chapitre 3. Nous définissons une sous-classe des transductions rationnelles qui admet une structure d'algèbre booléenne et de nombreuses autres propriétés intéressantes. Nous montrons que cette classe n'est pas décidable parmi les transductions rationnelles, mais des techniques d'approximation conservatrices permettent de bénéficier de ces propriétés dans la classe des transductions rationnelles tout entière. Nous présentons enfin quelques nouveaux résultats sur la composition de transductions rationnelles sur des monoïdes non libres, avant d'étudier l'approximation de transductions algébriques.

Phong Q. Nguyen

- Titre de la thèse: La géométrie des nombres en cryptologie
- Laboratoire : Laboratoire d'informatique de l'École normale supérieure (Paris)
- Directeur de thèse: Jacques Stern

Résumé de la thèse

La cryptographie a pour but principal de garantir la confidentialité et l'authenticité des communications, au moyen de protocoles de chiffrement et d'authentification. Son importance s'est considérablement accrue avec le développement des réseaux informatiques et du commerce électronique. Malheureusement, aucun des systèmes cryptographiques d'intérêt pratique connus aujourd'hui ne dispose d'une preuve absolue de sécurité. Dans le meilleur des cas, on sait parfois qu'un système est sûr si un certain problème calculatoire est difficile, mais bien souvent, on en est réduit à étudier toutes les attaques possibles, faute de pouvoir identifier précisément le problème sous-jacent. L'étude des attaques des procédés cryptographiques est l'objet de la cryptanalyse.

Cette thèse porte sur de nouvelles applications de la géométrie des nombres en cryptanalyse. La géométrie des nombres est une branche de la théorie des nombres fondée il y a un siècle par Hermann Minkowski comme un pont

entre la géométrie, l'approximation diophantienne et l'étude des formes quadratiques. Ses développements algorithmiques, notamment l'algorithme de Lenstra-Lenstra-Lovász, ont eu des applications spectaculaires en cryptanalyse. Depuis peu, la géométrie des nombres intervient également en cryptographie : les problèmes algorithmiques de la géométrie des nombres sont à la base de nouveaux systèmes cryptographiques, suite à de récentes découvertes de Miklós Ajtai en théorie de la complexité.

Nous présentons de nouvelles techniques issues de la géométrie des nombres, en particulier la notion de réseau orthogonal, qui permettent d'attaquer avec succès divers systèmes de chiffrement et de signature proposés ces dernières années. Cette thèse se décompose en trois parties, chacune comprenant deux cryptanalyses. La première partie s'intéresse à des systèmes de chiffrement s'appuyant sur la difficulté de problèmes dits de sacs à dos : les cryptosystèmes de Qu-Vanstone (Certicom) et d'Itoh-Okamoto-Mambo (JAIST). La seconde partie s'intéresse à des systèmes de chiffrement à base de problèmes algorithmiques de la géométrie des nombres : les cryptosystèmes d'Ajtai-Dwork (IBM), et de Goldreich-Goldwasser-Halevi (MIT). La troisième et dernière partie est consacrée à des protocoles de signatures électroniques accélérées : les schémas de Béguin-Quisquater (UCL) et de Boyko-Peinado-Venkatesan (Microsoft et MIT).