

Équipe CASYS.
Responsable scientifique : Jean-Guillaume Dumas.
Rapport sur la période : du 1 Janvier 2006 au 31 Décembre 2009.

Site internet : <http://ljk.imag.fr/CASYS>

Tutelles : Université Grenoble 1, Université Grenoble 2, Grenoble INP, CNRS, INRIA.

Sommaire

1	Présentation générale	2
2	Composition de l'équipe	3
3	Thèmes de recherche	4
3.1	Calculs algébriques	4
3.1.1	Catégories pour la sémantique des langages de programmation	4
3.1.2	Algèbre linéaire exacte	4
3.1.3	Arithmétique pour la cryptologie et les codes correcteurs	5
3.2	Systèmes dynamiques	6
3.2.1	Équations différentielles	6
3.2.2	Interaction des systèmes dynamiques avec la physique et la biologie, bifurcations	7
3.2.3	Systèmes hybrides, dynamique des réseaux	7
3.2.4	Contrôle et optimisation	9
4	Domaines d'application et impact social, économique ou interdisciplinaire	10
5	Contrats et subventions	11
5.1	Contrats et subventions externes (industriels, européens, nationaux)	11
5.2	Réseaux de recherche (européens, nationaux, régionaux, locaux)	12
5.3	Subventions locales	12
6	Collaborations internationales principales	12
7	Rayonnement	13
7.1	Contributions à la communauté scientifique	13
7.2	Prix et récompenses	14
7.3	Diffusion des connaissances	14
8	Production logicielle	15
9	Activités d'enseignement	16
10	Industrialisation, brevets et transferts de technologie	19
11	Auto-évaluation	19
12	Perspectives de l'équipe de recherche	20
13	Publications (Janvier 2006 à Mai 2009)	21

1 Présentation générale

Projet scientifique et technologique

L'équipe CASYS (Calculs Algébriques et Systèmes Dynamiques) fait partie du Département MAD (Modèles et Algorithmes Déterministes) et regroupe des chercheurs s'intéressant au calcul formel, à l'analyse et au contrôle de systèmes dynamiques classiques ou hybrides (symboliques/exacts/numériques) ainsi qu'à la sémantique de ces calculs.

Nos recherches sont centrées sur les thèmes suivants, liés à plusieurs projets :

- Catégories pour la sémantique des langages de programmation.
- Algèbre linéaire exacte.
- Arithmétique pour la cryptologie et les codes correcteurs.
- Équations différentielles.
- Interaction des systèmes dynamiques avec la physique et la biologie, bifurcations.
- Systèmes hybrides, dynamique des réseaux.
- Optimisation et contrôle.

L'équipe s'articule autour de compétences en mathématiques et en informatique pour développer des algorithmes mêlant des aspects numériques, exacts, formels. Nous développons donc des méthodes hybrides où le continu, numérique, est piloté par des événements discrets, des méthodes exactes pour résoudre des problèmes particulièrement mal conditionnés, ou des problèmes dans des ensembles abstraits où l'approximation n'a aucun sens. Depuis la modélisation, en physique et biologie mais aussi en mathématiques pures, l'idée est de développer des algorithmes efficaces donnant des garanties sur leur exécution et leurs résultats. Il faut ainsi construire les modèles dynamiques adaptés, les simuler et les analyser, donner les outils mathématiques pour le contrôle et la commande optimale. Il faut créer les algorithmes de calcul exact de complexité minimale permettant de résoudre le plus efficacement les problèmes sous-jacents et de prévoir mathématiquement leur comportement. Enfin, il faut optimiser leur design pour leur permettre de concilier efficacité et généricité grâce à une utilisation fine et sophistiquée des langages de programmation et de leur sémantique.

Scientific and Technological Project

The CASYS team (Algebraic Computations and Dynamical Systems) is part of the MAD department and brings together researchers interested in computer algebra, analysis and control of classic or hybrid dynamical systems (symbolic/exact/numeric) as well as in the semantics of these computations.

Our research is centered on the following themes, linked to several projects :

- Categories for the semantics of programming languages.
- Exact linear algebra.
- Arithmetic for cryptology and error-correcting codes.
- Differential equations.
- Dynamical system interaction with physics and biology, bifurcations.
- Hybrid systems, network dynamics.
- Optimization and control.

The team uses competence in mathematics and informatics to develop algorithms associating numerical, exact and algebraic aspects. We thus develop hybrid methods where continuous or numeric behaviors are influenced by discrete events, exact methods for especially badly conditioned problems, or problems in abstract structures where approximation makes no sense. From modelling, in physics and biology but also from questions in pure mathematics, our idea is to develop efficient algorithms giving guarantees on their execution and results. We thus build adapted dynamical models, simulate and analyze them and develop the mathematical tools for their optimal control. In addition, we create the exact algorithms with minimal complexity solving with maximal efficiency the underlying problems, while predicting their behavior. Finally, we optimize their design in order to conciliate efficient and generic programming thanks to a subtle and sophisticated use of the programming languages and their semantics.

2 Composition de l'équipe

<i>Permanents</i>				
Nom	Prénom	Grade	Institution	Date d'arrivée
CHAFFY	Claudine	Maître de conférences	UJF	01/11/1982
COLEMAN	Rodney	Maître de conférences	UJF	01/09/1990
DUMAS	Jean-Guillaume	Maître de conférences	UJF	01/09/2002
DUVAL	Dominique	Professeur	UJF	01/09/2000
FOUSSE	Laurent	Maître de conférences	UJF	01/09/2007
GIRARD	Antoine	Maître de conférences	UJF	01/09/2006
HILDEBRAND	Roland	Chercheur (CR)	CNRS	08/09/2003
JAMES	Guillaume	Professeur	INPG	01/09/2008
JUNG	Françoise	Maître de conférences	UJF	01/10/1989
MAIGNAN	Aude	Maître de conférences	UPMF	01/09/2003
TOURNIER	Evelyne	Professeur	UJF	01/10/1970

<i>Post-doctorant</i>				
Nom	Prénom	Fonction	Institution	Date d'arrivée
MORARESCU	Irinel-Constantin	Post-doctorant	UJF	01/01/2009

<i>Doctorants</i>					
Nom	Prénom	Université	Directeurs	Contrat	1 ^{ère} inscription
BOYER	Brice	UJF	D. Duval, J.-G. Dumas	MESR	2008
FERREIRA	Cynthia	INSA Toulouse	J.-M. Roquejoffre, G. James		2005
LEBELLEGO	Marion	Univ. Paul Sabatier Toulouse	E. Lombardi, G. James		2008

Anciens membres (entre le 1^{er} octobre 2005 et le 30 septembre 2009)

<i>Permanent</i>						
Nom	Prénom	Grade	Institution	Date d'arrivée	Date de départ	Situation actuelle
DELLA DORA	Jean	Professeur	INPG	01/01/1989	31/08/2009	Retraité

<i>Post-doctorant, visiteurs</i>					
Nom	Prénom	Fonction	Date d'arrivée	Date de départ	Institution
EDWARDS	Roderick	Visiteur	22/09/2008	22/11/2008	University of Victoria
PELINOVSKY	Dmitry	Visiteur	20/06/2009	27/06/2009	McMaster University
ZHENG	Gang	Post-doctorant	01/01/2008	31/10/2008	UJF

<i>Doctorants</i>						
Nom	Prénom	1 ^{ère} inscription	Date de départ	Université	Directeurs	Situation actuelle
FARCOT	Étienne	2001	30/12/2005	INPG	J. Della Dora	CR INRIA
KOLB	Sébastien	2002	31/10/2007	INPG	J. Della Dora	CRéA
PERNET	Clément	2003	27/09/2006	UJF	D. Duval, J.-G. Dumas	MCF UJF
RONDEPIERRE	Aude	2002	18/07/2006	INPG	J. Della Dora, J.-G. Dumas	MCF INSA Toulouse

TOURNIER	Laurent	2001	30/12/2005	INPG	J. Della Dora	CR INRA
URBAŃSKA	Anna	2005	08/12/2008	UJF	D. Duval, J.-G. Dumas	Poursuite de la thèse en GB

Évolution de l'équipe :

Après le départ de Michèle Benois en 2005, l'équipe s'est renforcée sur le thème des systèmes hybrides par le recrutement d'Antoine Girard (MCF) en 2006. En 2007, l'UJF a souhaité développer l'aspect cryptologie et a donc procédé au recrutement d'un professeur à l'Institut Fourier et de deux maîtres de conférences, un à Verimag et un au LJK dans l'équipe CASYS, Laurent Fousse. Enfin, Guillaume James de l'INSA Toulouse a été recruté professeur en remplacement de Jean Della Dora, retraité depuis 2008.

3 Thèmes de recherche

Nous identifions deux aspects principaux dans la recherche de l'équipe CASYS : un aspect algorithmique et calcul formel en algèbre linéaire, arithmétique et sémantique pour des structures algébriques ; un aspect modélisation, analyse et commande des systèmes dynamiques, hybrides, différentiels.

3.1 Calculs algébriques

3.1.1 Catégories pour la sémantique des langages de programmation

Participants : D. Duval (PR), J.-G. Dumas (MCF), L. Fousse (MCF).

Enjeux scientifiques et atouts de l'équipe : Nous développons l'utilisation de la théorie des catégories à la sémantique des langages de programmation dans trois directions principales.

Réécriture de graphes. Le principe de l'utilisation de pushouts pour la transformation de graphes est bien connu, mais son adaptation à des situations précises est délicate ; nous étudions les graphes qui modélisent la mémoire (les cellules et les pointeurs).

Structuration de logiciels complexes. Les catégories fournissent une alternative aux logiciels de modélisation diagrammatiques usuels comme UML ; nous utilisons cette approche pour des logiciels complexes en calcul formel.

Sémantique des effets. Les catégories cartésiennes closes fournissent une sémantique catégorique pour les langages fonctionnels ; pour traiter des effets, on doit considérer des monades ou des catégories prémonoidales, nous étudions dans ce cadre le problème fondamental de l'ordre d'évaluation des arguments pour les fonctions multivariées.

Nous collaborons hors LJK sur ces sujets avec R. Echahed (CR CNRS, LIG), F. Prost (MCF, LIG), J.-C. Reynaud (IR CNRS, LSR, puis retraité) et C. Dominguez Perez (Université de la Rioja, Espagne).

Résultats principaux Jan. 2006 – Déc. 2009 :

Réécriture de graphes. Généralisation de l'approche du « double pushout » afin de manipuler des structures de données complexes avec pointeurs. Étude du processus de ramasse-miettes en termes d'adjonction. Mise au point d'une nouvelle méthode utilisant des pushouts hétérogènes afin de « cloner » certaines parties du graphe. Ces 3 résultats ont été présentés et publiés dans 3 congrès internationaux [B56, B55, F129]. Ce thème de recherche est considéré par le LJK comme l'un des faits marquants du laboratoire pour 2007-08.

Structuration de logiciels complexes. Application, entre autres, au logiciel LinBox en C++ pour le calcul linéaire. Ce résultat a été présenté et publié au congrès LMO'06 [B66].

Sémantique des effets. Approche tout à fait nouvelle du problème de la séquentialité de l'évaluation des arguments, avec la notion de catégorie à effets cartésienne. Ce résultat a été présenté au workshop international ACCAT'09 [E97], la procédure pour publication dans la revue JSC est en cours.

Perspectives : Développer les applications de la notion de pushout hétérogène. Publier un article de synthèse sur les logiques diagrammatiques. Appliquer nos techniques à la modélisation par diagrammes dans un cadre orienté objet. Appliquer nos travaux sur la séquentialité à la sémantique des langages impératifs puis orientés objet.

3.1.2 Algèbre linéaire exacte

« Mathematics is the art of reducing any problem to linear algebra » [W Stein, U. of Washington].

Participants : J.-G. Dumas (MCF), L. Fousse (MCF), Clément Pernet (thèse soutenue en 2006, dir. D. Duval et J.-G. Dumas), Anna Urbańska (Doctorante, dir. D. Duval et J.-G. Dumas), Brice Boyer (Doctorant, dir. D. Duval et J.-G. Dumas).

Enjeux scientifiques et atouts de l'équipe : En calcul formel comme en calcul numérique, l'algèbre linéaire est souvent un point majeur pour la résolution efficace des problèmes. Ces quinze dernières années, les progrès non négligeables des machines et considérables de l'algorithmique formelle ont permis au domaine de devenir abordable en pratique.

En effet, en calcul numérique, le modèle algébrique de complexité associé à l'étude de la stabilité et à une utilisation optimale des différentes ressources réelles des machines permet souvent de conclure sur l'efficacité d'une méthode. Différemment, en calcul formel, si la stabilité des algorithmes n'est plus un problème, les coefficients des matrices appartiennent à des domaines a priori moins naturels à manipuler de manière pratique : il s'agit par exemple des entiers, de corps ou de groupes finis, d'anneaux de polynômes, etc.

Résultats principaux Jan. 2006 – Déc. 2009 : Après les percées de la complexité binaire et le développement des logiciels haute-performance comme LinBox, FFLAS-FFPACK et Givaro, ces dernières années, nous avons encore amélioré l'algorithmique de l'algèbre linéaire exacte, à la fois au niveau des ordres de grandeur des complexités théoriques mais aussi au niveau des constantes effectives permettant de fixer LinBox comme la bibliothèque d'algèbre linéaire exacte de référence. Cela inclut notamment :

La démonstration, à partir de la thèse de C. Pernet [D95], **de la réduction du calcul du polynôme caractéristique à la multiplication de matrice** (problème auparavant ouvert dont les derniers développements remontaient aux années 80) et ses applications au calcul sur matrices creuses [B41, A11] ; et l'amélioration d'un ordre de grandeur des précédentes bornes sur la taille des coefficients des polynômes caractéristiques et minimaux entiers [A20].

La réduction d'un tiers de la quantité de mémoire nécessaire à l'algorithme de Strassen-Winograd pour la multiplication rapide de matrices [B40], point de départ de la thèse de B. Boyer.

La proposition d'une arithmétique compressée accélérant les calculs d'algèbre linéaire pour les petits corps finis et l'arithmétique de la division en cryptologie [B46, B47, F131].

La parallélisation efficace des routines de calcul du rang pour réussir à avancer vers la preuve de la conjecture de Vandiver en K-theory [B54].

Le développement d'algorithmes auto-adaptatifs permettant de tirer parti des avantages combinés de plusieurs algorithmes. Grâce à une méthodologie générale [B63], point de départ de la thèse de A. Urbańska, nous avons ainsi réussi à réduire les complexités de nombreux problèmes comme le calcul du déterminant [B68] et la résolution de systèmes parallèle [B67].

Perspectives : A. Urbańska étend dans sa thèse les résultats adaptatifs sur les entiers au cas rationnel et à son application aux problèmes numériques mal conditionnés ; B. Boyer travaille sur le calcul exact des espaces propres et le changement de paradigme de programmation de l'algèbre linéaire qu'implique le passage aux architectures multi-cœurs/GPU ; la résolution du problème ouvert du polynôme caractéristique en boîte noire (problème numéro 9 de E. Kaltofen) permettrait par exemple une résolution effective du problème de l'isomorphisme de graphes pour de nombreuses classes de graphes creux. En particulier, l'extension des méthodes développées dans [B41] nécessite de combiner des résultats fins d'algèbre linéaire sur \mathbb{Z} et de calcul d'index en théorie algorithmique des nombres.

Enfin, les techniques spécifiques à la caractéristique 2 sont absentes de LinBox. Le projet M4RI a donc pour but de pallier ce manque et d'étudier de manière générale les techniques ad hoc pour les petites caractéristiques [H173].

3.1.3 Arithmétique pour la cryptologie et les codes correcteurs

Participants : L. Fousse (MCF), R. Coleman (MCF), J.-G. Dumas (MCF), Brice Boyer (Doctorant, dir. D. Duval et J.-G. Dumas).

Enjeux scientifiques et atouts de l'équipe : Ce thème de recherche s'appuie notamment sur les compétences en algèbre linéaire et en arithmétique présentes dans l'équipe, et est porté par diverses collaborations locales : avec Jean-Louis Roch, Franck Leprevost, Roland Gillard, Yassine Lakhnech puis Philippe Elbaz-Vincent des LIG, Institut Fourier et Verimag, nous avons commencé à collaborer sur plusieurs projets de recherche (voir page 11), en liaison avec les codes correcteurs (Safescale) puis avec la cryptanalyse (PaloAlto). En effet en 2006, l'université Joseph Fourier a recruté trois enseignants chercheurs, Philippe Elbaz-Vincent, professeur à l'institut Fourier, Pascal Lafourcade, maître de conférences à Verimag et L. Fousse, maître de conférences en arithmétique dans l'équipe CASYS du LJK.

Résultats principaux Jan. 2006 – Déc. 2009 : Nous avons alors développé nos activités dans le domaine de la cryptologie et des codes correcteurs : Jean-Guillaume Dumas et Laurent Fousse ont démarré une collaboration avec Bruno Salvy du projet INRIA Algorithmes [B47, F131] et Pascal Giorgi du LIRMM sur l'arithmétique à précision fixée ; et L. Fousse entame une collaboration avec Philippe Gaborit et Carlos Aguilar Melchior du laboratoire XLIM sur le retrait privé d'information (Carlos Aguilar Melchior, Laurent Fousse et Philippe Gaborit, Lattice-based Private Searching Scheme with Recursion, en préparation).

Nous avons initié une collaboration avec Vincent Roca du projet INRIA Planète sur de l'algèbre linéaire en caractéristique 2 pour des codes correcteurs LDPC [H173]. Jean-Guillaume Dumas collabore également avec Cécile Canovas du

CEA-LETI-CESTI à Grenoble sur des attaques par perturbations sur RSA [B39]. Enfin, nous sommes partenaires du projet Shiva avec le CEA, plusieurs industriels et plusieurs laboratoires de recherche grenoblois sur de la cryptologie embarquée sur FPGA.

Par ailleurs, nous avons des activités de recherche plus amont et orientées vers la théorie algorithmique des nombres. Jean-Guillaume Dumas a notamment développé un nouvel algorithme probabiliste permettant de calculer des racines primitives pour des tailles de corps finis jusqu'alors inatteignables [A34]. Jean-Guillaume Dumas a également donné la première caractérisation complète des nombres Queneau, et ainsi démontré une conjecture de Joerg Arndt reliant racines primitives et bases normales optimales de type-2 pour $GF(2^n)$ [A10]. Dans ce cadre, Rodney Coleman étudie également la fonction indicatrice d'Euler $\phi(n)$. En particulier, il essaie de caractériser l'image de cette fonction (il s'agit d'un problème théorique ouvert). En préparation : *On the image of Euler's totient function*.

Enfin, la rédaction de supports de cours dans les domaines de la cryptologie, des codes correcteurs et de la compression s'est ensuite concrétisée par la publication d'un ouvrage unifiant les théories sous-jacentes à destination des Masters [C84] ainsi que par plusieurs chapitres d'un ouvrage de référence sur le sujet [C91, C90, C89]. La traduction de cet ouvrage en anglais a été assurée par R. Xu et R. Coleman et la publication est en cours [C83].

Perspectives : Les perspectives de recherche dans ce thème pour l'équipe CASYS s'articulent en plusieurs parties autour du *développement de logiciels pour les codes et la cryptologie adaptés aux nouvelles architectures multi-cœurs*.

Développer les codes spécifiques à l'algèbre linéaire exacte en caractéristique 2 pour les codes correcteurs. Le prototype de bibliothèque d'algèbre linéaire en très petite caractéristique, M4RI [H173], est prometteur dans ce cadre.

Par ailleurs, des expériences de calcul sur processeurs graphiques montrent que de l'algèbre linéaire numérique haute performance est dorénavant possible sur ces multi-cœurs. Un défi technologique, abordé dans la thèse de B. Boyer, est ici de combiner l'approche numérique/exacte de FFLAS [A11] avec la caractéristique 2, les formats spécifiques de matrices pour GPU [B47] et les matrices de codes.

Développer une arithmétique efficace, à précision fixée, spécialisée pour architectures multi-cœurs et cryptologie sur jacobiniennes de courbes. Les dernières générations de calculateurs combinent en effet des processeurs classiques (CPU) multi-cœurs avec des processeurs spécialisés tels que FPGA (Field-programmable gate array) reprogrammables et des GPU (Graphics Processing Unit) afin d'atteindre des performances importantes, et les logiciels actuels d'arithmétiques ne savent pas en tenir compte. D'autre part, les efforts en cryptologie à clef publiques se portent actuellement sur l'utilisation de courbes elliptiques, ou plus généralement de jacobiniennes de courbes, et de couplages.

Plusieurs pistes sont envisagées pour optimiser des bibliothèques spécialisées pour la cryptographie telles que Crypto++, MIRACL ou OpenSSL, actuellement moins efficaces qu'une bibliothèque générique de précision arbitraire comme GMP : modifier les structures de données grâce aux techniques « recursive double size », coupler d'autres arithmétiques plus adaptées comme des bases RNS (*residue number system*) spécialisées, identifier ou construire des représentations et des courbes plus adaptées aux multi-cœurs.

3.2 Systèmes dynamiques

3.2.1 Équations différentielles

Participants : F. Jung (MCF), J. Della Dora (PR), E. Tournier (PR).

Enjeux scientifiques et atouts de l'équipe : Ce thème s'inscrit dans la suite des travaux de l'équipe sur les équations différentielles linéaires (projet européen CATHODE I) et non-linéaires (projet européen CATHODE II). Au cours du quadriennal qui vient de s'écouler, le travail a été recentré sur les équations différentielles linéaires au voisinage des singularités irrégulières, en particulier sur l'étude algorithmique du phénomène de Stokes. Il a abouti à un algorithme de calcul numérique des multiplicateurs de Stokes pour une large classe d'équations différentielles linéaires. Celui-ci est basé sur l'analyse des singularités des transformées de Borel des séries divergentes qui apparaissent dans les solutions. Il s'applique dès que ces séries sont k -sommables, à condition que leur transformées de Borel n'aient que des singularités régulières et ne présentent pas plusieurs singularités alignées sur une même demi-droite issue de l'origine.

Résultats principaux Jan. 2006 – Déc. 2009 : Cette étude a conduit au développement d'un module logiciel, écrit en Maple, qui contient la résolution formelle des équations et la description du phénomène de Stokes et qui permet le calcul numérique et la visualisation graphique d'une solution particulière sur toute la surface de Riemann du logarithme (au voisinage d'une singularité irrégulière).

Perspectives : Ce travail a été effectué en collaboration avec J.-P. Ramis (Toulouse), F. Fauvet et J. Thomann (Strasbourg) [A3, B72, E108, F130]. Il pourra être poursuivi dans différentes directions : en appliquant les programmes développés sur des équations intéressant les physiciens (Prolate wave equations), en élargissant la classe d'équations auxquelles ils s'appliquent, en développant un type de représentation surfacique des solutions, qui nécessite une cartographie du plan complexe rendue plus aisée par la présente description du phénomène de Stokes.

3.2.2 Interaction des systèmes dynamiques avec la physique et la biologie, bifurcations

Participants : G. James (PR), A. Girard (MCF), R. Edwards (PR invité).

Enjeux scientifiques et atouts de l'équipe : Nos travaux concernent des systèmes dynamiques issus de la physique et de la biologie. Ils portent sur la modélisation de systèmes physiques, la simulation des modèles et leur analyse mathématique. Ce dernier point constitue notre activité principale et conduit notamment à l'étude de bifurcations dans des systèmes dynamiques de dimension finie ou infinie. Nous étudions des ondes non linéaires impliquées dans différents processus physiques, comme par exemple les « breathers » (oscillations périodiques en temps et spatialement localisées) qui jouent un rôle important dans la dynamique d'ouverture de l'ADN. Parmi les modèles considérés figurent des réseaux infinis d'oscillateurs, dans lesquels les solutions localisées telles que les breathers [A32] ou les vortex [A1] présentent des caractéristiques nouvelles liées à la discrétisation spatiale des modèles. Une part importante de nos recherches s'effectue en collaboration avec des physiciens et dans le cadre de financements nationaux (*ACI Localisation non linéaire et applications à la physique des molécules biologiques*, 04-07).

Résultats principaux Jan. 2006 – Déc. 2009 : L'étude de systèmes dynamiques sur réseaux s'est beaucoup développée ces vingt dernières années et a apporté des éclairages nouveaux sur différents phénomènes physiques. Un exemple frappant est celui des fluctuations d'ouverture de l'ADN, qui consistent en des vibrations de grande amplitude d'un petit nombre de paires de bases sous l'effet des fluctuations thermiques. Ce phénomène peut être modélisé à l'aide d'une chaîne d'oscillateurs non linéaires correspondant aux différentes paires de bases (modèle de Peyrard et Bishop, 1989). Les non-linéarités et la nature discrète du modèle conduisent à la formation de breathers qualitativement similaires aux oscillations localisées de l'ADN. Bien que fort intéressants, les réseaux non linéaires analysés jusqu'ici négligeaient certains ingrédients importants dans le contexte des biomolécules. Les travaux que nous avons réalisés ont permis de progresser dans différentes directions.

Théorèmes d'existence de breathers et d'orbites périodiques relatives dans des modèles de molécules planaires.

Les théorèmes d'existence de breathers dans des ensembles d'atomes faiblement couplés étaient jusqu'à présent restreints à des réseaux 1D ou bien à des modèles avec des potentiels locaux qui brisent l'invariance euclidienne de ces systèmes. Or ces limitations devaient être levées afin de se rapprocher des expériences réelles dans lesquelles des oscillations localisées sont détectées. Nous avons obtenu une preuve d'existence de breathers pour des systèmes hamiltoniens planaires avec invariance euclidienne [A15]. Ce résultat est valable pour un nombre arbitraire (fini) de particules. Il est basé sur la continuation de breathers par rapport à un paramètre γ mesurant le rapport de masse entre certains groupes d'atomes (l'existence de breathers est démontrée dans la limite d'un grand rapport de masse). Nous avons étendu ces résultats à des orbites périodiques relatives, qui sont périodiques dans un repère en rotation à vitesse constante [A5]. Le système étudié est triatomique avec deux atomes lourds identiques. Nous montrons l'existence de solutions de grande amplitude pour γ grand, étendant ainsi des résultats classiques obtenus au voisinage de configurations d'équilibre.

Amélioration du modèle de Peyrard-Bishop pour l'ADN. Le modèle initialement introduit par Peyrard et Bishop reproduit qualitativement les fluctuations d'ouverture localisées de l'ADN, mais ne donne pas des résultats satisfaisants d'un point de vue quantitatif. En particulier, la durée moyenne d'ouverture des bases excitées est 100 fois trop courte par rapport aux mesures expérimentales et les zones ouvertes sont trop étendues. Nous avons introduit un nouveau modèle pour lequel ces caractéristiques deviennent *quantitativement correctes* [A16, A8]. Ce modèle tient compte du fait que les paires de bases ouvertes fluctuent davantage et leur rotation peut alors gêner leur fermeture, induisant une barrière d'énergie dans leur potentiel d'interaction effectif. Cet effet amène l'existence d'un nouveau type de breathers, qui n'oscillent pas autour de l'état fondamental correspondant à la chaîne fermée mais autour d'un état d'équilibre spatialement localisé. Nous avons démontré l'existence de ces solutions pour un couplage faible entre les bases voisines (James, Levitt et Ferreira, article en préparation). Par ailleurs, nous avons étudié le modèle de Peyrard-Bishop spatialement non homogène (les variations spatiales des paramètres du réseau proviennent de la séquence génétique), et avons fourni une explication géométrique à des bifurcations de breathers induites par des inhomogénéités spatiales [A6].

Perspectives : En bio-mathématiques, nous étudions le couplage entre les vibrations des filaments d'actine et leur nuage ionique (Ferreira, James, Peyrard), et les fluctuations d'ouverture de l'ADN : modélisation du bruit thermique, torsion, hysteresis (Girard, James, Peyrard, Labbé). Par ailleurs nous collaborons avec l'IPG de Strasbourg pour étudier la dynamique de failles sismiques (James, Schmittbuhl, Toussaint, Cochard, Lebellego, Lombardi) : propagation de dislocations, stick-slip. Nous étudions aussi des modèles plus théoriques : chaînes d'oscillateurs avec potentiels quadratiques par morceaux (Edwards et James), justification d'EDP d'enveloppe pour des breathers dans des réseaux 2D (James et MacKay).

3.2.3 Systèmes hybrides, dynamique des réseaux

Participants : A. Girard (MCF), J. Della Dora (PR), R. Edwards (PRI 2008), R. Hildebrand (CR), A. Maignan (MCF), C. Moraescu (Post-doctorant, 2009), G. Zheng (Post-doctorant 2008), A. Rondepierre (thèse soutenue en 2006, dir. J.

Della Dora et J.-G. Dumas).

Enjeux scientifiques et atouts de l'équipe : Un système hybride est un système dynamique résultant de l'interaction entre des processus discrets, décrits par exemple par des automates, et continus, décrits par des équations différentielles. L'étude de ces systèmes complexes est difficile, leur caractère hétérogène rendant inopérantes les méthodes classiques pour l'analyse des systèmes dynamiques continus ou discrets. La recherche sur les systèmes hybrides est par nature pluridisciplinaire et nous entretenons des collaborations fructueuses avec des informaticiens (VERIMAG, Grenoble) et automaticiens (University of Pennsylvania et University of California at Los Angeles, USA). Notre travail dans ce domaine porte sur le développement de méthodes algorithmiques d'analyse et d'abstraction des systèmes hybrides et leur application dans les domaines de l'automatique, du contrôle optimal, de la robotique et des systèmes embarqués. Plus récemment, nous avons considéré un nouveau domaine d'application des systèmes hybrides : l'étude de la dynamique des réseaux, notamment biologiques et sociaux. La qualité de notre travail est reconnue internationalement comme en atteste notre participation aux comités de programme des deux conférences majeures du domaine (Hybrid Systems : Computation and Control, Analysis and Design of Hybrid Systems).

Résultats principaux Jan. 2006 – Déc. 2009 : Nos principales contributions dans ce domaine de recherche sont les suivantes :

Vérification des systèmes hybrides : Il s'agit de vérifier que les trajectoires d'un système hybride satisfont une propriété donnée, pour toutes conditions initiales et perturbations admissibles. Ceci peut se faire par une analyse d'atteignabilité qui consiste à déterminer une approximation de l'enveloppe des trajectoires du système. Pour les systèmes où la dynamique continue est affine par morceaux, nous avons proposé un schéma algorithmique efficace [B74] et pouvant s'adapter à plusieurs types de représentation de l'ensemble atteignable [B49, A7]. Pour les systèmes où la dynamique continue est non-linéaire, une méthode de linéarisation par morceaux, ou hybridisation [A19], permet de se ramener à l'utilisation des techniques citées précédemment. Dans le cadre du projet VAL-AMS, nous avons développé une autre approche qui consiste à simuler un certain nombre de trajectoires du système. Pour chacune de ces trajectoires, on détermine un ensemble de trajectoires voisines qui satisfont également la propriété. L'ensemble des trajectoires du système, ainsi couvert par un nombre fini de tels voisinages, est certifié satisfaire la propriété [B78, B71, B45].

Abstraction des systèmes hybrides : Les techniques d'abstraction ou de réduction de modèles sont des ingrédients indispensables pour l'étude de systèmes hybrides complexes. La problématique centrale de l'abstraction des systèmes hybrides est de pouvoir comparer des modèles de nature différente (continu, discret, hybride). Les relations de simulation sont largement utilisées pour les systèmes discrets, elles décrivent comment une trajectoire du système peut être reproduite par son approximation. Pour les systèmes continus et hybrides, nous avons relaxé cette condition : une relation de simulation approchée décrit comment la trajectoire du système peut être approchée (avec une borne d'erreur garantie) par une trajectoire de son approximation [A24]. Nous avons développé des méthodes de réduction de modèle basées sur cette approche pour des systèmes continus et hybrides [B76, B80, A23, A12]. Les résultats les plus prometteurs, obtenus dans le cadre du projet VAL-AMS, concernent le calcul d'approximations discrètes de systèmes continus ou hybrides avec des applications à des systèmes mécaniques ou des circuits électriques [B59, A17, B51]. Ces techniques d'abstraction peuvent être utilisées pour le contrôle hiérarchique des systèmes hybrides, l'idée est d'effectuer la synthèse du contrôleur pour l'approximation et ensuite d'adapter la loi de commande pour le système initial [A4]. Nous avons utilisé cette approche en robotique pour résoudre des problèmes de planification de trajectoires [A2, B50].

Contrôle optimal de systèmes déterministes : Du point de vue théorique, le contrôle optimal de systèmes dynamiques déterministes se réduit par le principe de maximum de Pontryaguine à un problème d'intégration d'un système hybride Hamiltonien avec des conditions au bord. Nous avons montré un résultat théorique important sur la complexité possible de la solution du système Hamiltonien. Notamment, il a été démontré que pour un certain système linéaire avec coût quadratique, la solution contient un fer à cheval de Smale, et donc du chaos déterministe [B52]. Du point de vue algorithmique, nous avons développé une méthode d'hybridisation pour résoudre des problèmes de contrôle optimal non linéaires par des méthodes de calcul hybride [D96] : après avoir quantifié l'erreur commise entre le domaine contrôlable non linéaire et son approximation hybride, nous proposons une approche constructive pour le calcul du domaine contrôlable, permettant de réduire l'exploration des états discrets de l'automate hybride. Enfin, nous énonçons en particulier un principe du maximum hybride (principe du maximum de Pontryagin et solutions de viscosité des équations d'Hamilton-Jacobi-Bellman) qui nous permet alors de déterminer la structure du contrôle optimal hybride.

Dynamiques des réseaux : Dans le cadre du projet CARESSE, nous nous sommes intéressés à la modélisation et à la simulation de systèmes dynamiques composés de plusieurs agents (animaux, individus...) organisés en réseau (biologique, social...). Nous avons proposé un cadre de modélisation, basé sur le formalisme des systèmes hybrides et des grammaires de graphes [F144], où l'évolution de chaque agent est déterminée par l'état de ses voisins et où la topologie du réseau peut être amenée à évoluer (suppression/ajout d'agents ou de liens entre agents). Ce cadre théorique a servi de base au développement du logiciel de modélisation et de simulation DynSys [H171, F128].

Un autre aspect du projet CARESSE porte sur l'analyse de ces systèmes, nous nous sommes en particulier intéressés

au problème d'identification de communautés dans des réseaux soit par des méthodes d'optimisation par relaxation semi-définie [F133], soit en modélisant et en étudiant la dynamique de création de consensus.

Perspectives : Nous souhaitons continuer à développer les axes de recherche actuels. Un nouveau domaine d'application prometteur est celui des systèmes cyber-physiques (systèmes résultant de l'intégration de systèmes informatisés et de processus physiques). Ces systèmes omniprésents dans la technologie moderne (véhicules autonomes, chirurgie robotique...) sont par nature hétérogènes et la théorie des systèmes hybrides offre un cadre rigoureux pour leur étude.

3.2.4 Contrôle et optimisation

Participants : R. Hildebrand (CR), A. Girard (MCF), R. Coleman (MCF).

Enjeux scientifiques et atouts de l'équipe :

Optimisation conique. L'optimisation conique est concernée par le problème de minimisation d'une fonction linéaire sur une section affine d'un cône convexe. Le cas le plus facile à résoudre numériquement et le plus important est celui où le cône concerné est un cône dit autosimilaire. Parmi cette classe de cônes, on trouve l'orthant positif, le cône de Lorentz, et le cône de matrices positive semi-définies, menant respectivement aux programmes linéaires, les programmes coniques quadratiques et les programmes semi-définis. Beaucoup de problèmes, surtout dans le domaine des systèmes dynamiques, ont une description sous forme d'un tel programme conique, ou peuvent être approximés, i.e. relaxés, par un tel programme. Dans le cadre de recherche de l'équipe, on s'intéresse notamment aux applications dans les domaines de l'identification des communautés dans des réseaux, à l'optimisation des expériences pour l'identification des systèmes, et à des questions plus théoriques telles que la représentabilité de problèmes d'optimisation sous forme de programme semi-défini et la qualité de relaxations semi-définies.

Optimisation d'expériences pour l'identification de systèmes. Des systèmes réels tels que colonnes de distillation, bras de robots, cascades de pompes sont souvent trop complexes et/ou incertains pour être modélisés à partir des principes basiques de la physique. Dans ces situations, une approche boîte noire est utilisée pour obtenir un modèle. Notamment, un ensemble paramétrisé de modèles est choisi, et une expérience est réalisée sur le système, consistant en l'application d'un signal d'entrée et la collecte d'un signal de sortie. Les signaux d'entrée et de sortie peuvent être couplés par biais d'un régulateur. Ensuite, le modèle choisi est celui qui prédit le mieux la sortie à partir de l'entrée. La qualité du modèle augmente avec la durée de l'expérience, mais dépend aussi du régulateur ainsi que du spectre du signal d'entrée. Les expériences étant dans la plupart des cas relativement chères, on souhaite optimiser leurs conditions pour obtenir une quantité maximale d'information sur le système en respectant certaines contraintes. Cette tâche est le sujet de l'optimisation des expériences qui nous concerne ici. En général, un problème concret d'optimisation des expériences est considéré comme résolu (ou approximativement résolu) si on réussit à le transformer en un programme semi-défini (ou à obtenir une relaxation semi-définie de celui-ci d'une qualité satisfaisante).

Informatique quantique : séparabilité et intrication. On dit qu'un état d'un système multi-partitionné est *intriqué* s'il existe des corrélations quantiques non-locales entre les différents sous-systèmes. Un état non-intriqué s'appelle *séparable*. L'ensemble des états séparables mixtes est convexe, mais en général difficile à décrire. Les questions d'intrication et de séparabilité jouent un rôle important dans le calcul quantique.

Contrôle optimal de systèmes déterministes. Le contrôle optimal de systèmes dynamiques déterministes est fondé sur le principe de maximum de Pontryaguine, qui réduit le problème à un problème d'intégration d'un système hybride Hamiltonien avec des conditions sur le bord.

Résultats principaux Jan. 2006 – Déc. 2009 : Un résultat majeur était la construction d'une représentation semi-définie pour le cône des applications Lorentz-positives, c'est-à-dire le cône des applications linéaires qui portent un cône de Lorentz dans un autre, préalablement fixé [A28], [F138]. Un autre résultat est la caractérisation de l'ensemble de fonctions $f : [-1, 1] \mapsto [-1, 1]$ tel que $f[X] \succeq 0$ pour toute matrice $X \succeq 0$ à diagonale unitaire et de rang k , où $f[X]$ est la matrice obtenue à partir de X par application de f élément par élément. Ce résultat permet d'améliorer les bornes connues précédemment sur la qualité des relaxations semi-définies de programmes quadratiques binaires. Une publication est en préparation.

Un résultat majeur porte sur l'identification de systèmes linéaires en boucle fermée. Il s'agit d'un algorithme optimisant simultanément le spectre de l'entrée et le régulateur utilisé pendant l'expérience. Il se fonde sur la démonstration de l'exactitude d'une certaine relaxation semi-définie du problème. Auparavant, seule l'optimisation de l'entrée était possible, le régulateur devant être fixé préalablement. Une publication a été soumise et acceptée à la conférence SYSID 09 [B43].

Un résultat majeur porte sur les boules séparables autour de l'état maximalelement mixé pour un système de n q-bits. Auparavant, le rapport entre les meilleures bornes supérieures et inférieures sur le rayon de la boule séparable maximale était divergeant quand le nombre de q-bits tendait vers l'infini. On a réussi à réduire ce rapport à une constante ($\sqrt{34/27} \approx 1,12$) [A26]. Contrairement aux bornes connues précédemment, la nouvelle borne supérieure est constructive, c'est-à-dire qu'elle est obtenue par détermination explicite d'un état quantique mixte de n q-bits situé sur le bord

de l'ensemble des états séparables et proche de l'état maximalement mixé.

Un autre résultat majeur porte sur le calcul de la *concurrence*, une mesure qui quantifie l'intrication des états quantiques mixtes. Un nouveau point de vue sur cette quantité a été développé, en généralisant la concurrence sur le cône des matrices positives (c'est-à-dire, les états mixtes non-normalisés) à des cônes convexes arbitraires. Une formule explicite pour la concurrence a été obtenue sur les cônes de Lorentz. Ceci a permis de calculer la concurrence d'une manière explicite pour les matrices de densité de rang 2 [A25].

Un résultat majeur porte sur la complexité possible de la solution du système Hamiltonien. Notamment, il a été démontré que pour un certain système linéaire avec coût quadratique, la solution contient un fer à cheval de Smale, et donc du chaos déterministe [B52].

Enfin, R. Coleman travaille sur le calcul différentiel dans les espaces normés de dimension infinie, en particulier sur l'optimisation dans de tels espaces. Il a écrit un livre sur ce sujet (Differential Calculus on Normed Vector Spaces). Il s'intéresse surtout au calcul de variations et actuellement prépare un article intitulé « A new look at the brachistochrone problem ».

Perspectives : L'application des relaxations semi-définies pour la recherche de fonctions bisimilaires dans l'analyse des solutions de systèmes dynamiques incertains est envisagée.

Le résultat [B43] étant plutôt d'une nature globale, on souhaite le concrétiser et le raffiner pour certaines situations particulières.

On souhaite étudier si la structure de la solution reste stable sous des perturbations non-linéaires du système d'origine. Si c'est le cas, le chaos déterministe sera présent dans la solution dans le cas générique, à partir d'une certaine dimension du problème.

4 Domaines d'application et impact social, économique ou interdisciplinaire

L'algèbre linéaire exacte haute performance est un outil de base pour de multiples applications, principalement en mathématiques fondamentales, mais également pour tous les problèmes mal conditionnés, là où les méthodes numériques sont instables... L'équipe maintient une base de donnée, faisant dorénavant également partie de l'« UFL Sparse Matrix Collection », de systèmes linéaires creux à coefficients exacts pour la plupart traitables exclusivement grâce à la bibliothèque LinBox :

<http://ljk.imag.fr/membres/Jean-Guillaume.Dumas/simc.html>.

Nos recherches en cryptologie et codes correcteurs s'appliquent directement en sécurité informatique et réseaux, par exemple les attaques par perturbations sur les chiffrements asymétriques permettent de renforcer la sécurité des cartes à puces, des codes LDPC plus efficaces deviendront concurrentiels dans le monde très contraint des communications réseaux.

En collaboration avec Isabelle Joncour, nous développons une adaptation du logiciel DynSys au problème des amas stellaires fermés. Le problème d'un système à N-corps provient de la non-linéarité des équations qui de plus contiennent des singularités lorsque l'approche de deux masses est telle que leur distance approche zéro, ce qui introduit des variations arbitraires de vitesse infiniment grandes. L'idée, ici est, de modéliser la création ou la destruction de binaires (ou plus généralement des n-aires) par des transformations locales de graphes et d'éviter ainsi les problèmes de singularité.

Nous explorons de plus d'autres champs d'applications tels qu'en biologie l'analyse de l'évolution des espèces et la compétition entre espèces. Dans ce cadre d'application, nous utilisons les équations de Lotka-Volterra pour modéliser la dynamique de chaque nœud.

Nos travaux sur les systèmes hybrides ont trouvé des applications en robotique pour des problèmes de planification de trajectoires [A2, B50] par des méthodes de contrôle hiérarchique. Ces méthodes ont aussi été utilisées dans le cadre du projet VAL-AMS pour la conception de circuits électroniques mixtes digitaux/analogiques [B51]. Nos travaux récents sur la dynamique des réseaux doivent nous permettre de mieux comprendre les mécanismes d'émergence de comportements collectifs dans les réseaux sociaux et biologiques.

Nos travaux sur les breathers discrets ont permis de mieux comprendre la formation et les propriétés de ces excitations dans des modèles issus de la physique de la matière condensée, de la biophysique, de l'optique non linéaire. Ces travaux sont reconnus par les physiciens du domaine, comme le montrent nos invitations à des conférences internationales et nos citations dans des revues de physique (par exemple sept travaux cités dans le récent Physics Reports : Flach et Gorbach, *Discrete breathers - advances in theory and applications*, Physics Reports 467, 2008).

Notre travail avec M. Peyrard et S. Cuesta-López (laboratoire de physique, ENS Lyon) a permis d'améliorer grandement un modèle mathématique des fluctuations d'ouverture de l'ADN (Peyrard, Cuesta-López et James, *Nonlinearity* 21, 2008 ; Peyrard, Cuesta-López et James, *J. Biol. Phys.* 35, 2009). Notre modèle est suffisamment fin pour décrire correctement des résultats expérimentaux alors que les précédents modèles s'en écartaient de plusieurs ordres de magnitude. De plus, notre modèle est suffisamment simple pour permettre des simulations numériques des fluctuations d'ouverture (une simulation tout-atome du phénomène est actuellement inenvisageable à cause de la grande variété des échelles de temps mises en jeu). La

compréhension des fluctuations d'ouverture est importante car ce phénomène joue un rôle fondamental dans le fonctionnement de la molécule d'ADN. Nous espérons donc que notre modèle pourra être utilisé pour répondre à des questions profondes concernant le lien entre la dynamique de l'ADN, la séquence génétique et les fonctions de la molécule.

5 Contrats et subventions

5.1 Contrats et subventions externes (industriels, européens, nationaux)

VEDECY 2009-2011, 439 k€. *Verification and design of cyber-physical systems*, ANR, programme ARPEGE, avec Verimag et INRIA Pop-Art.

VAL-AMS 2007-2009, 261 k€. High Confidence Validation of Analog and Mixed Signal Circuits, ANR, programme SETIN. Les partenaires sont VERIMAG (France), LJK (France), INRIA (France). Le coordinateur est Thao Dang (VERIMAG), le responsable scientifique au LJK est Antoine Girard. Le but du projet est de proposer des méthodes de validation des circuits électriques analogiques ou mixtes en développant des techniques d'analyse basées sur la simulation numérique avec des garanties sur la fiabilité des résultats.

<http://www-verimag.imag.fr/~tdang/VAL-AMS>

Localisation non linéaire 2004-2007, 30 k€. ACI NIM (Nouvelles Interfaces des Mathématiques) *Localisation non linéaire et applications à la physique des molécules biologiques*. Coordonnateur : G. James. Partenariat avec le laboratoire de physique de l'ENS Lyon (M. Peyrard), l'Institut Camille Jordan - Univ. Lyon 1 (P. Noble), l'université de Séville (B. Sánchez-Rey, J. Cuevas).

http://www-ljk.imag.fr/membres/Guillaume.James/aci_nim.html

Optimisation of the steelshop floor 2008-2009, 18 k€. Contrat de l'UJF et Floralis avec Dalmine, Spa, Italie, sur l'optimisation du processus de la fabrication de tubes en acier à partir de métaux recyclables. Personnes impliqués côté UJF : Roland Hildebrand (CR) et Anatoli Iouditski (PR, département Statistique).

Shiva 2009-2011, 2200 k€. Projet Ministère de l'industrie : Secured Hardware Immune Versatile Architecture. Ce projet est labellisé Minalogic à Grenoble entre le CEA, plusieurs industriels (CS, Netheos, iWall/Mataru, EasyiiC) et plusieurs laboratoires de recherche grenoblois (LJK, IF, LIG, Verimag). Ce projet devra fournir un module matériel programmable et reconfigurable, avec un haut niveau de sécurité évaluable au sens des critères communs, et s'intégrant sur des plates-formes d'infrastructure réseau à haut débit. Il offrira aux entreprises, aux institutions et aux opérateurs la possibilité de sécuriser leur réseau, par application de leur propre chiffre symétrique, soit choisi ou spécialisé parmi des standards génériques, soit personnalisé.

EAU 2006-2010, 3000 k€. Contrat industriel d'enseignement et recherche avec la société CS (Communications et Systèmes). Formations à la cryptologie et à la sécurité, mise en place d'infrastructures sécurisées.

Safescale 2006-2009, 340 k€. Projet ANR : certification et tolérance aux fautes sur grille de calcul. J.-G. Dumas est responsable du groupe de travail « calcul exact » de ce projet. Ce groupe de travail a deux directions principales : d'une part, la parallélisation du calcul de solutions rationnelles ou entières à précision arbitraire par la parallélisation massive des restes chinois ; et d'autre part, la recherche probabiliste de boîtes de chiffrement à clefs secrètes.

<https://www-lipn.univ-paris13.fr/safescale>

CHPID 2005-2008, 14 k€. Projet Région dans le Cluster ISLE **Calcul Hautes Performances et Informatique Distribuée**. Nous avons coordonné le thème « Nouveaux outils mathématiques pour le calcul scientifique » et en particulier des outils algébriques pour la discrétisation des EDP.

CalCel 2005-2008, 120 k€. Projet Région **Calcul Cellulaire**. Le projet CalCel avait pour but de développer une boîte à outils numérique pour analyser l'évolution d'une colonie d'agents logiciels. Ce projet était commun au laboratoire LJK, au laboratoire ID-IMAG et au laboratoire LIRIS de Lyon. Les responsables étaient Jean Della Dora pour la partie grenobloise et Serge Miguet pour la partie lyonnaise. La première partie du projet a abouti à la création par L. Tournier en 2007 d'*un nouveau modèle hybride pour la biosynthèse des acides aminés essentiels chez la plante Arabidopsis Thaliana*.

<http://ljk.imag.fr/CASYS/CalCel>

LinBox Projet international : algèbre linéaire creuse.

Le projet NSF, NESRC et CNRS LINBOX regroupe 12 chercheurs (USA, France, Canada) sur le développement d'algorithmes efficaces en algèbre linéaire, sur leur traduction en une bibliothèque de programmes et sur l'interfaçage de cette bibliothèque avec les logiciels de calcul scientifique les plus couramment utilisés. J.-G. Dumas a notamment développé le premier prototype de la bibliothèque avec W. Turner (North Carolina) [B66].

<http://linalg.org>

5.2 Réseaux de recherche (européens, nationaux, régionaux, locaux)

IST-2001-35454 ECVision : European Research Network for Cognitive AI-enabled Computer Vision Systems. ECVision était subventionné par l'unité de systèmes cognitifs de l'union européenne. Il a permis d'unifier l'ensemble des 8 projets IST subventionnés du programme V de la communauté européenne.

GDR IM : participation au GDR Informatique Mathématique dans plusieurs groupes de travail (Calcul formel ; Logique, algèbre et calcul ; Codage et cryptographie ; Arithmétique).

GDR MACS : participation au GDR Modélisation, Analyse et Conduite de Systèmes dynamiques.

GDR MOAD : participation au GDR MODélisation, Asymptotique, Dynamique non linéaire, GDR CNRS 2948.

IFIP WG 1.3 : participation au groupe de travail international « Foundations of System Specification ».

IXXI : membre de l'Institut rhône-alpin des systèmes complexes (IXXI), groupement d'intérêt scientifique créé en 2006 et faisant partie du RNSC (Réseau National des Systèmes Complexes).

5.3 Subventions locales

CARESSE : 2008-2009, 57 k€. Contrôle et Analyse de Réseaux de Systèmes Dynamiques Évolutifs, Pôle MSTIC de l'UJF. Le coordinateur est Antoine Girard. CARESSE porte sur la modélisation, la simulation, l'analyse et le contrôle de réseaux évolutifs de systèmes dynamiques.

<http://ljk.imag.fr/membres/Antoine.Girard/Projects/CARESSE>

PALO-ALTO : 2008-2009, 57 k€. Projet pôle MSTIC de l'UJF : Plate-forme d'Attaques LOGicielles par ALgorithmes et Techniques Optimisés pour architectures Multi-Cœurs Parallèles. Avec Philippe Elbaz-Vincent de l'Institut Fourier, nous portons ce projet centré sur l'arithmétique des entiers à précision fixée, l'arithmétique des jacobiennes de courbes algébriques afin de fournir une plate-forme de cryptographie et de cryptanalyse sur architectures spécifiques comme les GPU et les FPGA.

<http://ljk.imag.fr/membres/Laurent.Fousse/palo-alto>

AHA : 2005-2007, 80 k€. Projet IMAG : Algorithmes Hybrides Adaptatifs. Avec Jean-Louis Roch, nous avons proposé en 2005 un projet IMAG sur le développement d'un cadre générique pour le calcul adaptatif. Il s'agit de construire des algorithmes qui s'adaptent automatiquement au contexte d'exécution (à la fois au niveau des données et au niveau de l'architecture matérielle). Ces travaux sont appliqués au calcul fiable, à l'ordonnancement et affectation par optimisation combinatoire et aux problèmes inverses de vision artificielle (multi-caméras et temps-réel).

<http://aha.gforge.inria.fr>

6 Collaborations internationales principales

University of Pennsylvania Philadelphie, USA. Prof. G.J. Pappas, Dr. A.A. Julius, Dr. G. Fainekos. Nous entretenons une collaboration soutenue avec cette équipe de recherche. Nos travaux communs portent sur la vérification [B71, B78], l'abstraction [A12, A23, A24, B80, B75, B76, B73] et le contrôle hiérarchique [A4, A2, B60, B57, B77] des systèmes hybrides. Antoine Girard a effectué deux séjours d'une semaine dans cette équipe (en mars 2006 et novembre 2008).

University of California at Los Angeles, USA. Prof. P. Tabuada, Dr. G. Pola. Notre collaboration avec cette équipe de recherche est relativement récente. Nos travaux communs portent sur le calcul d'approximations discrètes de systèmes continus ou hybrides [B61, B51].

McMaster University, Canada. Mission d'une semaine de Dmitry Pelinovsky au laboratoire LJK (20-27 Juin 09), financée par l'ambassade de France au Canada, l'IXXI et le projet Val-AMS. Collaboration avec G. James sur la dynamique de réseaux non linéaires.

University of Warwick, Grande-Bretagne. Invitation d'une semaine de G. James à l'université de Warwick, Math. Institute (03-14 Sept. 2007). Collaboration avec Robert MacKay portant sur la justification d'EDP d'enveloppe pour des breathers dans des réseaux 2D d'oscillateurs non linéaires.

University of Victoria, Canada. Mission de deux mois de Roderick Edwards au laboratoire LJK (Octobre-Novembre 08), financée par l'INPG (poste de professeur invité). Collaboration portant sur la dynamique de chaînes d'oscillateurs avec potentiels quadratiques par morceaux.

University of Massachusetts, USA. Collaboration avec Panayotis Kevrekidis sur la dynamique de solitons/vortex dans les équations de Schrödinger non linéaire/Gross-Pitaevskii discrètes [A1, A9].

Universidad de La Rioja, Espagne. Collaboration avec Cesar Dominguez Perez sur la structuration des logiciels complexes.

University of Delaware, USA. Collaboration avec B. David Saunders sur l’algèbre linéaire exacte et la bibliothèque LinBox [B41].

University of Waterloo, Canada. Collaboration avec A. Storjohann, W. Zhou Sur l’algèbre linéaire [B40].

Universidad de Sevilla, Espagne. Collaboration avec B. Sánchez-Rey et J. Cuevas (groupe de physique non linéaire) ayant abouti à des théorèmes d’existence de breathers dans un modèle non linéaire des vibrations des bases de l’ADN [A6].

University of York, Grande-Bretagne, et Università di Camerino, Italie. Collaboration avec S. Severini et S. Manchini sur des aspects quantiques de Laplaciens de graphes [A14].

Université Catholique de Louvain, Belgique. Collaboration avec G. Solari sur l’identification de systèmes ARMAX [A31].

Eidgenössische Technische Hochschule Zürich, Suisse. Collaboration avec P. Koumoutsakos sur l’optimisation de l’écoulement autour d’un cylindre [A18].

7 Rayonnement

7.1 Contributions à la communauté scientifique

Direction d’organisations scientifiques

- *Institut IMAG* : Directeur adjoint, en charge des mathématiques, Jean Della Dora, 2003-2006.
- *Unité de services M²S* : Directeur de l’unité, Jean Della Dora, 2007-2008.
- *Conseil d’administration de l’INPG* : Jean Della Dora, jusqu’en 2008.

Administration de sociétés savantes

- *SIGSAM* : (ACM Special Interest Group on Symbolic and Algebraic Manipulation) advisory board member at large (J.-G. Dumas membre élu pour trois ans, 2007-2010).

Édition

- *Journal of Computation and Mathematics* : Dominique Duval, jusqu’en 2006.
- *Asian Journal of Control* : Antoine Girard, depuis 2008
- *ACM Communications in Computer Algebra* : Jean-Guillaume Dumas, depuis 2006
- *Numerical Algorithms* : Jean Della Dora, depuis 1991.
- *Collection Mathématiques et Applications* : chez Springer, Jean Della Dora.

Organisation de conférences

- *Transgressive Computing 2006* : 24-26 avril 2006, Grenade, Espagne. Organisateur, F. Jung, E. Tournier et J.-G. Dumas.
- *Congrès de la SMAI* : 2007, Antoine Girard.
- *7th Conference on Real Numbers and Computers* : membre du comité d’organisation, juillet 2006 au LORIA, Nancy, L. Fousse.
- *Rencontres du Non Linéaire* : membre du comité scientifique et d’organisation (conférence avec actes ayant lieu tous les ans à l’IHP, sur le thème des phénomènes non linéaires), 2005-2006, G. James.
- *École du Non Linéaire de Peyresq* : membre depuis 2005 du comité scientifique et d’organisation (école annuelle organisée pendant une semaine, en Juin ou Septembre). École interdisciplinaire réunissant physiciens et mathématiciens travaillant dans le domaine du non linéaire, G. James.
- *Lattice dynamical systems* : organisateur du mini-symposium de la conférence Equadiff 2007, 5-11 Août 2007, Vienne et Keynote lecture, G. James.
- *Journée nationale du GDR IM* : co-organisation à Villetaneuse en 2008, D. Duval.
- *Parallel processing for scientific computing 2006* : co-organisation de la session MS1 Adaptive Algorithms for Scientific Computing, 22–24 février 2006, San Francisco, California, J.-G. Dumas.
- *Journées Nationales de Calcul Formel 2010* : 3 – 7 mai 2010, CIRM, Luminy, France. Organisateur, J.-G. Dumas.
- *Journées Nationales de Calcul Formel 2008* : 20 – 24 Octobre 2008, CIRM, Luminy, France. Organisateur, J.-G. Dumas.

Organisation de séminaires

- *Séminaires du LJK-Modèles et Algorithmes Déterministes* : BIPOP-CASYS, répertorié dans l’Agenda des Conférences de Mathématiques de la SMAI et l’IXXI.

Comités de programme

- *Hybrid Systems : Computation and Control* : 2007, 2008 et 2009, Antoine Girard.
- *IEEE International Symposium on Computer Aided Control System Design* : 2008, Antoine Girard.
- *IFAC Conference on Analysis and Design of Hybrid Systems* : 2009, Antoine Girard.
- *IFAC Symposium of System Identification* : 2006 et 2009, Roland Hildebrand.
- *Parallel Symbolic Computations* : 2007, Waterloo, Canada, J.-G. Dumas.
- *International Symposium on Symbolic and Algebraic Computations* : 2006 et 2009, J.-G. Dumas, Gènes, Italie.
- *Transgressive Computing* : 2006, F. Jung, E. Tournier et J.-G. Dumas.

Expertise internationale

- *University of Victoria, USA* : évaluation de dossiers scientifiques, 2008, Jean Della Dora.
- *University of Waterloo, Canada* : évaluation de dossiers scientifiques, 2007, Jean Della Dora.
- *University of London, Canada* : évaluation de dossiers scientifiques, 2007, Jean Della Dora.
- *International Centre for Mathematical Sciences ICMS (Edinburgh)*, évaluation d'une proposition de workshop, 2006, Guillaume James.

7.2 Prix et récompenses

Prix

- *Médaille du LORIA* : pour avoir gagné la compétition de calcul « Many Digits » à Nijmegen avec l'équipe MPFR, 2005, Laurent Fousse.

7.3 Diffusion des connaissances

R. Coleman a écrit un ouvrage sur le calcul différentiel, en cours de révision. J.-G. Dumas a publié un ouvrage de cryptologie, compression et codes correcteurs d'erreurs à destination des Masters [C84] ainsi que plusieurs articles dans la revue *Tangente* [A36, A35] vulgarisant la théorie des codes : cryptologie, hachage La traduction de cet ouvrage en anglais a été assurée par R. Xu et R. Coleman et la publication est en cours [C83]. L. Fousse et J.-G. Dumas préparent actuellement un ouvrage sur les architectures à clefs publiques et la sécurité Web. Enfin, C. Chaffy a écrit de très nombreux photocopiés, plus de 1750 pages, à l'usage des étudiants de L1 :

- *MAT121 : nombres complexes, géométrie euclidienne et introduction à l'algèbre linéaire, analyse approfondie*
 - Les nombres complexes (86 pages)
 - Géométrie analytique dans le plan et dans l'espace. Discussion et résolution de systèmes linéaires (110 pages).
 - Formules de Taylor et développements limités
 - L'essentiel du cours et exemples (64 pages)
 - Le cours est-il compris ? Exercices d'entraînement et tests (112 pages)
 - Équations différentielles linéaires
 - Le cours est-il compris ? Exercices d'entraînement et devoirs (108 pages)
- *MAT112 : algèbre linéaire et géométrie élémentaires*
 - Le calcul algébrique (47 pages)
 - Le langage mathématique (53 pages)
 - Géométrie analytique dans le plan et dans l'espace (45 pages)
 - Discussion et résolution de systèmes linéaires (55 pages)
 - Pour jongler avec les matrices ! (16 pages, en collaboration avec les physiciens)
- *MAT128 : analyse élémentaire*
 - Dérivées et primitives
 - L'essentiel du cours, des exemples et des exercices types (188 pages)
 - Workbook et réponses (71 pages)
 - Équations différentielles linéaires
 - L'essentiel du cours et exemples avec Maple (96 pages)
 - Workbook et réponses (29 pages)
 - Limites et développements limités
 - L'essentiel du cours, des exemples et des exercices types (166 pages)
 - Workbook et réponses (51 pages)
- *MAT129 : algèbre et analyse : pour en savoir plus !*

- Le raisonnement par l'exemple (46 pages)
- Une immersion dans les structures algébriques (20 pages)
- Pour bien débiter en algèbre linéaire ! (146 pages)
- L'algèbre linéaire en pratique (122 pages)
- Les outils de l'analyse réelle (86 pages)
- Les fonctions intégrables-Riemann, intégrales généralisées, séries numériques (48 pages)

8 Production logicielle

CASCADE : Computational Analysis and Simulation using Continuous Approximations for Differential Equations.

<http://www-ljk.imag.fr/CASYS/LOGICIELS/CASCADE>

MATISSE : Metrics for Approximate Transition Systems Simulation and Equivalence.

<http://www-ljk.imag.fr/membres/Antoine.Girard/Software/Matisse>

DynSys : est un logiciel permettant de modéliser et de simuler des réseaux constitués d'agents. Chaque agent et chaque lien du réseau obéissent à un système dynamique qui dépend de son voisinage. Des règles de transformations locales permettent, sous certaines contraintes, d'ajouter ou d'enlever des agents ou des liens du réseau. DynSys est un logiciel développé en C++ et Java. Il possède une interface graphique permettant la visualisation des réseaux successifs.

<http://www-ljk.imag.fr/membres/Stephane.Despreaux/Ingenierie/Dynsys/doc/doc.html>

DESIR : est un module logiciel, écrit en MAPLE permettant d'étudier des équations différentielles linéaires au voisinage de leurs singularités, dans le champ complexe. Il se compose de trois parties : une partie formelle (les algorithmes qui permettent de trouver une base de solutions formelles), une partie numérique et graphique (sommation de séries divergentes et visualisation dans le champ complexe), la description du phénomène de Stokes (rayons de Stokes et approximation numérique des matrices associées). C'est un logiciel libre, à l'état de prototype.

<http://www-ljk.imag.fr/CASYS/LOGICIELS/desir2009.html>

CRQ : *Correctly Rounded Quadrature*. Il s'agit de la bibliothèque de calcul numérique d'intégrales de fonctions réelles avec erreur bornée, en précision arbitraire, développée par Laurent Fousse dans le cadre de sa thèse. Licence GNU LGPL 2.1.

<http://komite.net/laurent/soft/crq/>.

Givaro : La bibliothèque C++ Givaro contient, notamment, de nombreuses variantes d'implémentations des corps finis (corps premiers ou extensions) de taille le mot machine, la reconstruction entière et rationnelle d'entiers modulaires par les restes chinois, une structure de polynômes univariés paramétrée par le domaine des coefficients (donc une structure multivariée récursive), des structures de données vectorielles et matricielles gérées par compteurs de références ... Depuis la version 3.2, Givaro est intégré aux distributions Linux Debian et openBSD et au logiciel SAGE (pour ses corps finis).

<http://ljk.imag.fr/CASYS/LOGICIELS/givaro>

LinBox : est la bibliothèque de référence de l'algèbre linéaire exacte. Elle est notamment intégrée dans le logiciel SAGE et interfacée par Maple.

<http://linalg.org>

FFLAS-FFPACK : est l'équivalent des BLAS et de LAPACK pour les corps finis. Depuis la version 1.3 elle est intégrée à LinBox. Les logiciels Maple et Magma notamment l'utilisent pour leur algèbre linéaire exacte.

<http://ljk.imag.fr/membres/Jean-Guillaume.Dumas/FFLAS>

Simplicial Homology : est un module du logiciel GAP pour les calculs d'homologie de complexes simpliciaux.

<http://www.cis.udel.edu/~dumas/Homology>

Galet : est un générateur automatique d'ordonnancements pour le placement en mémoire d'algorithmes d'algèbre linéaire.

<http://ljk.imag.fr/membres/Jean-Guillaume.Dumas/Galet>

SHOC : est un module hybride symbolique/numérique Maple/C++ pour le contrôle optimal de systèmes dynamiques non-linéaires.

<http://ljk.imag.fr/membres/Jean-Guillaume.Dumas/SHOC>

PaloAlto : est un prototype de bibliothèque d'arithmétique à précision fixée pour la cryptologie.

<http://ljk.imag.fr/membres/Laurent.Fousse/palo-alto>

9 Activités d'enseignement

À l'instar de nos activités de recherche, nos activités d'enseignement sont marquées par une forte intrication de l'informatique et des mathématiques appliquées. En ce sens, CASYS est une équipe particulièrement pluridisciplinaire.

C. Chaffy s'est en particulier fortement investie en première année de Licence à l'UJF : lutter contre la désertification des filières scientifiques à l'Université est vital, mais toutefois peu aisé, face à la concurrence des autres filières.

En particulier, pour être attractif et non rébarbatif, l'enseignement des bases mathématiques indispensables à tout étudiant en sciences ne peut plus être dispensé de la même manière qu'il y a quelques années, c'est-à-dire de façon totalement abstraite. Nous devons tenir compte à la fois du petit nombre d'heures disponibles et du profil de nos étudiants (qui ne sont pas ceux des classes préparatoires aux grandes écoles), leur bagage mathématique étant parfois bien léger. S'agissant d'étudiants frais émoulus du Baccalauréat, leur faire acquérir des méthodes de travail n'est pas non plus chose vaine.

Or une approche de type « calcul formel », qui s'appuie sur des processus constructifs et du calcul, en utilisant beaucoup d'images, se révèle en fait assez efficace pour la compréhension de bien des notions nouvelles : les étudiants ne « décrochent » pas car ils se rendent compte qu'avec un minimum de travail (c'est bien là le problème de la majorité d'entre eux !), ils obtiennent des résultats. Cela les encourage ensuite à persévérer plutôt que de baisser les bras : la confiance est la clé du succès ! De plus, la règle très avantageuse instaurée entre le contrôle continu et l'examen terminal vise aussi à réduire le taux d'abandon en cours d'année.

Ce type d'enseignement demande un renouvellement constant ; beaucoup d'interactions avec les étudiants permettent de l'améliorer d'année en année et même si, sur le papier, le contenu semble le même, la manière de le « vendre » évolue avec chaque promotion.

S'agissant par exemple d'Unités d'Enseignement qui concernent 300 à 450 étudiants, une organisation sans faille est nécessaire à leur bonne marche (coordination de l'équipe enseignante). La compléter par des devoirs à la maison réguliers et surtout des photocopiés permet d'une part, de cadrer l'enseignement et d'autre part de rassurer les étudiants ... de même que les enseignants vacataires qui assurent une grande part des travaux dirigés en L1.

L'objectif est une formation d'excellence en L1 à l'UJF, contribuant ainsi à sa notoriété, formation qui ne laisse personne de côté : les étudiants qui se réorienteront en cours de route tout comme ceux qui sont faibles mais peuvent progresser, ceux qui sont moyens et doivent devenir bons si l'on s'occupe d'eux, enfin ceux qui sont bons mais peuvent devenir encore meilleurs s'ils sont stimulés.

Outre les enseignements de mathématiques et d'informatique de premier cycle, et nos enseignements de master 2, nous sommes par ailleurs très impliqués dans les enseignements intermédiaires très spécifiques de type « Math-Info » (calcul scientifique, algorithmique, cryptologie) enrichis par les thèmes de recherche de l'équipe qui est composée de membres de culture et de formation à la fois mathématique et informatique.

La liste des enseignements des membres de l'équipe est fournie par la suite, et nous pouvons remarquer notre implication dans les enseignements d'informatique de base : algorithmique et structures de données (E. Tournier L3 MI), programmation (J.-G. Dumas, M1 MAI), bases de données (D. Duval), introduction à la logique (L. Fousse).

Nous avons également largement contribué au développement d'enseignements spécifiques. Ces enseignements se font au niveau Master et sont très liés aux activités de recherche de l'équipe, comme par exemple dans les domaines de la réécriture et de la sémantique des langages de programmation. Par ailleurs, ces dernières années, les compétences en calcul formel, en algorithmique, en théorie des nombres ont permis à plusieurs membres de l'équipe (D. Duval, J.-G. Dumas, F. Jung, R. Coleman) de se former à l'enseignement de la cryptologie, de la compression de données et de la correction d'erreur. La rédaction de supports de cours dans ces domaines s'est ensuite concrétisée par la publication d'un ouvrage à destination des Master, ainsi que par plusieurs chapitres d'un ouvrage de référence sur le sujet. L'équipe a été impliquée dans la construction de la majorité des enseignements de ce domaine à Grenoble (d'abord à l'Ensimag et à l'école INP Telecom puis à Polytech en RICM, en Master Informatique, en Master de Mathématiques Pures, en Master de Mathématiques Appliquées et Industrielles, dans MOSIG, et dans le Master Professionnel Sécurité, cryptologie et codage de l'information que nous avons contribué à monter avec le LIG et l'IF, dès 2001 et dans lequel L. Fousse et J.-G. Dumas interviennent largement, J.-G. Dumas est notamment membre du jury de ce M2). Ensuite, avec Jean-Louis Roch, nous avons été amenés, à travers un contrat de formation avec la société C-S, à développer une filière internationale en Master 1 et 2 de Cryptologie et Sécurité à Grenoble. Cette formation a jeté les bases du Master 1 MOSIG (Master of Science in Informatics at Grenoble) et le Master 2 Cryptologie et Sécurité est devenu, par internationalisation des enseignements, le programme spécialisé SCIS (Security and Cryptology of Informatic Systems) du MOSIG. En 2006, l'université Joseph Fourier a souhaité renforcer sa compétence dans le domaine en recrutant trois enseignants chercheurs, Philippe Elbaz-Vincent, professeur à l'institut Fourier, Pascal Lafourcade, maître de conférences à Verimag et Laurent Fousse, maître de conférences en arithmétique dans l'équipe. Nous avons également fait évoluer les enseignements de L3 (MetI, RICM) vers des aspects plus algébriques et informatiques à destination des étudiants amenés à suivre les formations de type « Math-Info » de Master (CSCI mais aussi CAO, GVR, RO, ...).

Dans ce cadre, la place de l'équipe (deux professeurs et un maître de conférences de vingt-septième section, un volume d'environ 4,5 postes dans ces thèmes pour l'ensemble de l'équipe) dans l'enseignement d'informatique au sein du LJK est primordiale.

Responsabilités de filières

- *Jean Della Dora* : Directeur adjoint de l'ENSIMAG, jusqu'en septembre 2006.
- *Françoise Jung* : Directrice de l'IUP MAI (2005-2007), puis responsable de la L3 MetI à l'UJF.
- *Jean-Guillaume Dumas* : responsable du Master 1 MAI (Mathématiques Appliquées et Industrielles) à l'UJF depuis 2006.
- *Evelyne Tournier* : responsable formation continue et formation en alternance et en apprentissage de l'UFR IMAG.
- *Evelyne Tournier* : responsable validation d'acquis d'expérience de l'UFR IMAG.
- *Claudine Chaffy* : architecture des Unités d'Enseignement de mathématiques en L1 au DLST pour 2006-2010 (avec un an d'avance sur le quadriennal) ; mise au point de leurs programmes et de leurs modalités d'évaluation en concertation avec les enseignants de L'IMAG, de l'Institut Fourier et les collègues de physique ; création et gestion des UEs MAT128 et MAT129.

Principaux enseignements (septembre 2005 à juin 2009)

Enseignant	Cours	Niveau	Université	Heures	Années
C. Chaffy	Apprentissage du raisonnement et analyse élémentaire	L1	UJF	82	2005-2006
C. Chaffy	Nombres complexes, géométrie et introduction à l'algèbre linéaire, analyse approfondie (18 groupes)	L1	UJF	110	2005-2006
C. Chaffy	Algèbre linéaire et géométrie élémentaires	L1	UJF	154	2006-2009
C. Chaffy	Analyse élémentaire (13, 11, 10 groupes)	L1	UJF	218	2006-2009
C. Chaffy	Algèbre et analyse : pour en savoir plus !	L1	UJF	249	2006-2009
C. Chaffy	Soutien au S2 dans les deux UEs ci-dessus (PRL)	L1	UJF	15	2006-2009
R. Coleman	EDP	M1	UJF	103	2005-2007
R. Coleman	Arithmétique, polynômes, séries	L2	UJF	188	2005-2009
R. Coleman	Arithmétique, structures algébriques, polynômes	L2	UJF	163	2007-2009
R. Coleman	Calcul matriciel, intégrales multiples	L2	UJF	36	2005-2006
R. Coleman	Algèbre, analyse	L1	UJF	208	2005-2009
J. Della Dora	Méthodes numériques	Ensimag 1	Ensimag		2005-2009
J. Della Dora	Systèmes dynamiques	Ensimag 2	Ensimag		2005-2009
J. Della Dora	Maths For Fun	Ensimag 3 et M2RMA	UJF/Ensimag	30	2007-2009
J. Della Dora	Programmation numérique	Ensimag 1	Ensimag		2005-2009
J.-G. Dumas	Cryptologie	M1 Info., M1 Maths, M1 MAI, Ensimag, MOSIG	UJF/Ensimag	300	2005-2009
J.-G. Dumas	Calcul exact	M2R MA	UJF	50	2005-2009
J.-G. Dumas	Public Key Infrastructures	M2P CSCI	UJF	200	2005-2009
J.-G. Dumas	C++, Programmation efficace	M1 MAI	UJF	120	2005-2008
J.-G. Dumas	Compression de données	M1 Info.	UJF	80	2005-2007
J.-G. Dumas	Maths For Fun	Ensimag 3 et M2RMA	UJF/Ensimag	15	2007-2009
D. Duval	Catégories et Applications à l'Informatique	M2R SL	UJF	36	2006-2007

D. Duval	Maths For Fun	Ensimag 3 et M2RMA	UJF/Ensimag	15	2007-2009
D. Duval	Spécification en Calcul Formel	M2R MA	UJF	72	2005-2009
D. Duval	Bases de données	M2P CCI et RICM 2	UJF	64	2005-2009
D. Duval	Traitement Algébrique de l'Information	Ensimag 2	Ensimag	45	2005-2007
D. Duval	Programmation par contrat	M1 MAI	UJF	150	2005-2009
D. Duval	Outils Formels, cryptographie	RICM 2	Polytech	45	2005-2009
D. Duval	Maths Discrètes	RICM 1	Polytech	130	2005-2009
D. Duval	« Ouverture » : Codage	L3	UJF	22	2006-2007
D. Duval	Stages/projets	RICM 2, 3, M2P CCI	UJF/Polytech		2005-2009
L. Fousse	Cryptology	L2, M1, MOSIG	Nancy 1, UJF, Ensimag	137	2005-2009
L. Fousse	Algo. & Maths discrètes	L1, L3	Nancy 1, UJF	132	2005-2009
L. Fousse	Algèbre & Géométrie élémentaires	L1	UJF	108	2007-2009
L. Fousse	Logique	L1	UJF	16	2008-2009
L. Fousse	Maths For Fun	Ensimag 3 et M2RMA	UJF/Ensimag	15	2007-2009
G. James	Méthodes numériques	L3	Ensimag	100	2008-2009
G. James	EDP et différences finies	M1	Ensimag	50	2008-2009
G. James	Systèmes dynamiques, bifurcations et applications	M2RMA	UJF	14	2008-2009
G. James	Systèmes dynamiques	M1	Ensimag	19	2008-2009
G. James	L2, formation continue, INSA Toulouse			600	2005-2008
F. Jung	Mathématiques pour la CAO	L3 MAI-IUP	UJF	108	2005-2007
F. Jung	Analyse approfondie	L3 MAI-IUP	UJF	72	2005-2009
F. Jung	Algèbre et arithmétique effectives	L3 MetI	UJF	162	2006-2009
F. Jung	Optimisation continue	L3 MetI	UJF	54	2006-2009
F. Jung	Découverte des mathématiques appliquées	L1	UJF	126	2005-2008
F. Jung	Algèbre et arithmétique	L2	UJF	40	2008-2009
F. Jung	Responsabilité des stages	L3 MetI et M1 MAI	UJF	160	2005-2009
F. Jung	Discrete Math. and Algebra	M1 CSCI	UJF-INPG	120	2006-2009
F. Jung	Maths For Fun	Ensimag 3 et M2RMA	UJF/Ensimag	15	2007-2009
A. Girard	Systèmes dynamiques hybrides	M2R	UJF	52.5	2007-2009
A. Girard	Systèmes dynamiques	M1	Ensimag	131	2005-2009
A. Girard	Encadrement projet étudiant	M1	UJF/Ensimag	49	2005-2009
A. Girard	Outils mathématiques pour les signaux et les systèmes	L2	UJF	72	2007-2009
A. Girard	Algèbre et Analyse	L1	UJF	217	2006-2009
A. Girard	Découverte des mathématiques appliquées	L1	UJF	24	2008-2009
R. Hildebrand	Optimisation	Master MA2	Ensimag	9	2006-2007
R. Hildebrand	Optimisation convexe	Magistère	Ensimag / UJF	18	2007-2008
A. Maignan	Algèbre linéaire	2ème année	IUT-UPMF	244	2005-2009
A. Maignan	Graphes	2ème année	IUT-UPMF	21	2005-2006
A. Maignan	Arithmétique et logique	1ère année	IUT-UPMF	310	2005-2009
A. Maignan	Analyse	1ère année	IUT-UPMF	114	2005-2009
A. Maignan	Suivi de stages	1ère et 2ème année	IUT-UPMF	75	2006-2007
E. Tournier	Algorithmique et Programmation	L3 MI	UJF	252	2005-2009
E. Tournier	Graphes	L3 MI	UJF	228	2005-2009
E. Tournier	Calcul Formel	M1 MAI	UJF	80	2005-2009
E. Tournier	Projet	Miage	UJF	50	2007-2009

E. Tournier	Projet tutoré	L3 Pro Webdev	UJF	64	2005-2009
E. Tournier	Stages	L3 MI, L3 Pro	UJF	18	2005-2009
E. Tournier	FC, apprentissage	UFR IMAG	UJF	100	2005-2009
E. Tournier	VAE	UFR IMAG	UJF	40	

10 Industrialisation, brevets et transferts de technologie

Les contrats EAU, SHIVA et « Optimisation of the steelshop floor » décrits section 5, sont des contrats industriels comprenant des transferts technologiques.

11 Auto-évaluation

Émanant des différentes compétences de ses membres, l'ossature de l'équipe CASYS se forme autour de l'algèbre, de l'algorithmique et des systèmes dynamiques.

Notre activité scientifique s'est traduite par un nombre important de publications dans des revues et conférences internationales de rang A, et par la production de logiciels largement diffusés et en pointe dans leurs domaines.

Le large spectre de résultats obtenus et notre production logicielle importante reposent sur des interactions sous-jacentes entre nos différentes spécialités : l'algèbre linéaire exacte et formelle, par exemple, est une brique de base essentielle et spécifique de l'équipe et est utilisée pour caractériser des formes normales de systèmes dynamiques ou hybrides, pour la cryptanalyse du code RSA ou des problèmes de logarithme discret ; le calcul des séries solutions d'équations différentielles ou de la discrétisation hybride est formel ; les systèmes biologiques sont le siège de nombreux phénomènes non linéaires (comme les fluctuations d'ouverture de l'ADN), dont l'étude requiert des outils performants issus de la théorie des systèmes dynamiques ; l'étude de la sémantique des langages de programmation formalise les interactions objets mathématiques/objets informatiques et permet souvent de concilier l'efficacité de nos bibliothèques hautes performances avec une généricité importante. À terme, cela facilite également l'intégration de nos bibliothèques dans des logiciels de plus haut niveau comme Maple, SAGE.

Nos recherches s'appuient sur des collaborations multiples à la fois grenobloises, nationales ou internationales. Celles-ci s'effectuent dans le cadre de projets financés industriels ou académiques, et ont des applications dans des thèmes émergents comme la bio-mathématique, les réseaux sociaux ou encore la sécurité sur GPU, . . .

Plus précisément les résultats marquants de l'équipe, détaillés en section 3 s'articulent autour de deux aspects principaux, un aspect algorithmique et calcul formel en algèbre linéaire, arithmétique et sémantique pour des structures algébriques et un aspect modélisation, analyse et commande des systèmes dynamiques, hybrides, différentiels :

Nous avons développé l'utilisation de la théorie des catégories à la sémantique des langages de programmation dans trois directions principales : **Réécriture de graphes**, généralisation de l'approche du « double pushout » afin de manipuler des structures de données complexes avec pointeurs et étude du processus de ramasse-miettes en termes d'adjonction [B56, B55, F129] ; **Structuration de logiciels complexes**, application, entre autres, au logiciel LinBox en C++ pour le calcul linéaire [B66] ; **Sémantique des effets**, approche tout à fait nouvelle du problème de la séquentialité de l'évaluation des arguments, avec la notion de catégorie à effets cartésienne [E97].

Nous avons continué nos travaux en algèbre linéaire exacte, notamment par **La démonstration de la réduction du calcul du polynôme caractéristique à la multiplication de matrice** [D95, B41, A11] et l'amélioration des bornes sur la taille des coefficients des polynômes caractéristiques et minimaux entiers [A20] ; **La réduction d'un tiers** de la quantité de mémoire nécessaire à l'algorithme de Strassen-Winograd pour la multiplication rapide de matrices [B40] ; **La proposition d'une arithmétique compressée** accélérant les calculs d'algèbre linéaire pour les petits corps finis et l'arithmétique de la division en cryptologie [B46, B47, F131] ; **La parallélisation efficace** des routines de calcul du rang pour réussir à avancer vers la preuve de la conjecture de Vandiver en K-theory [B54] ; **Le développement d'algorithmes auto-adaptatifs** permettant de tirer parti des avantages combinés de plusieurs algorithmes [B63, B68, B67].

Nous avons appliqué nos recherches en calcul formel à la cryptologie aux codes correcteurs et à l'algorithmique de la théorie des nombres par des **attaques par perturbations sur l'exponentiation et RSA** [B39] ; le développement de l'**algèbre linéaire en caractéristique 2** pour des codes correcteurs LDPC [H173] ; un nouvel algorithme probabiliste permettant de **calculer des racines primitives** pour des tailles jusqu'alors inatteignables [A34] et la démonstration d'une conjecture de Joerg Arndt reliant racines primitives et bases normales optimales de type-2 pour $GF(2^n)$ [A10] ; la publication d'un **ouvrage unifiant les théories sous-jacentes à destination des Masters** [C84] et plusieurs chapitres d'un ouvrage de référence sur le sujet [C91, C90, C89, C83].

Nous avons poursuivi nos travaux sur les séries solutions d'équations différentielles par **la description du phénomène de Stokes (calcul des matrices) au voisinage d'une singularité irrégulière, permettant le suivi d'une solution particulière sur toute la surface de Riemann du logarithme** [H172].

Nous avons développé des interactions des systèmes dynamiques avec la physique et la biologie par des **Théorèmes d'existence de breathers et d'orbites périodiques relatives dans des modèles de molécules planaires** pour des systèmes hamiltoniens planaires avec invariance euclidienne [A15] ou encore des orbites périodiques relatives [A5]; et l'**Amélioration du modèle de Peyrard-Bishop pour l'ADN**, par un nouveau modèle pour lequel les fluctuations d'ouverture localisées de l'ADN deviennent *quantitativement correctes* [A16, A8] et avons fourni une explication géométrique à des bifurcations de breathers induites par des inhomogénéités spatiales [A6].

Nous avons continué l'étude des systèmes hybrides avec leur **Vérification** : schéma algorithmique efficace [B74], représentation de l'ensemble atteignable [B49, A7], linéarisation par morceaux, ou hybridisation [A19], garantie d'atteignabilité [B78, B71, B45]; **Abstraction** : une relation de simulation approchée décrit comment la trajectoire du système peut être approchée par une trajectoire de son approximation [A24], les modèles de systèmes continus et hybrides sont réduits [B76, B80, A23, A12], des approximations discrètes de systèmes continus ou hybrides sont obtenus avec des applications à des systèmes mécaniques ou des circuits électriques [B59, A17, B51], les systèmes sont contrôlés hiérarchiquement [A4] et cette approche est utilisée en robotique pour résoudre des problèmes de planification de trajectoires [A2, B50]; **Contrôle optimal de systèmes déterministes** : nous avons montré un résultat théorique important sur la complexité possible de la solution du système Hamiltonien [B52], nous avons développé une méthode d'hybridisation pour résoudre des problèmes de contrôle optimal non linéaires par des méthodes de calcul hybride [D96]; **Dynamiques des réseaux** : modélisation et à la simulation de systèmes dynamiques composés de plusieurs agents organisés en réseau [F144, H171, F128] et identification de communautés dans des réseaux [F133].

Enfin nous avons continué le développement des approches pour l'optimisation avec **la construction d'une représentation semi-définie pour le cône des applications Lorentz-positives** [A28, F138]; **l'identification de systèmes linéaires en boucle fermée** en démontrant l'exactitude d'une certaine relaxation semi-définie du problème [B43]; **la détermination explicite d'un état quantique mixte de n q-bits** permet la réduction à une constante des bornes supérieures et inférieures sur le rayon des boules séparables autour de l'état maximale mixte pour un système de n q-bits [A26]; **le calcul explicite de la concurrence**, une mesure qui quantifie l'intrication des états quantiques mixtes pour les matrices de densité de rang 2 [A25].

12 Perspectives de l'équipe de recherche

L'équipe CASYS est fondée sur un socle Mathématique-Informatique centré autour des thématiques suivantes : systèmes dynamiques classiques et hybrides, analyse non linéaire, contrôle, optimisation, modélisation, interaction avec la physique et la biologie, calcul formel haute performance, algèbre linéaire, cryptologie, arithmétique, sémantique des langages de programmation, logique diagrammatique.

L'équipe s'investit de manière intensive dans ces différentes directions de recherche. Les perspectives pour le prochain quadriennal sont nombreuses. Nous allons étendre l'étude des systèmes hybrides par exemple pour traiter les systèmes dynamiques multi-affines et polynomiaux, les systèmes hybrides où la dynamique discrète est donnée par l'exécution d'un logiciel de commande ou encore pour concevoir des contrôleurs embarqués hybrides. Nous allons également développer les interfaces avec la physique par exemple sur la dynamique non-linéaire de l'ADN et l'étude des failles sismiques. Par ailleurs nous continuons le programme de catégorisation des langages de programmation vers la définition de sémantiques décorées adaptées tout d'abord aux langages impératifs, puis aux langages orientés objet. Enfin nous continuerons les progrès en arithmétique et algèbre linéaire et les appliquerons par exemple au retrait privé d'information, aux codes correcteurs LDPC ou aux attaques sur chiffrements embarqués. Ces derniers développements pourront s'effectuer dans le cadre d'une nouvelle fédération de recherche (FED) regroupant les équipes impliquées aux LJK, LIG, Vérimag, Institut Fourier.

Ces perspectives sont ou seront l'objet de demandes de financements locaux ou nationaux :

- Dépôt de projet PEPS au CNRS : Dynamique d'ouverture de l'ADN, modélisation, analyse, simulation (programme PEPS physique théorique et interfaces), puis dépôt de projet BQR INP prévu en 2010. Thème : dynamique non linéaire de l'ADN, modélisation des fluctuations d'ouverture. Projet en collaboration avec Michel Peyrard (lab. de physique ENS Lyon) et S. Labbé.
- Dépôt de projet ANR prévu fin 2009, en partenariat avec J. Schmittbuhl, R. Toussaint (IPG de Strasbourg) et E. Lombardi (Institut de Math de Toulouse). Thèmes : dynamique non linéaire des failles sismiques, friction dans des interfaces liquides-solides, hydrofractures.
- Dépôt de projet ANR prévu en 2010 sur la cryptanalyse et/ou l'arithmétique pour la cryptologie, avec P. Giorgi (Montpellier), G. Villard (Lyon), B. Allombert (Bordeaux) ...

En outre, plusieurs projets sont en cours de montage :

- Formalisation de la collaboration avec BIPOP sur l'étude numérique de systèmes dynamiques non réguliers intervenant dans la dynamique des failles sismiques.
- Formalisation de la collaboration avec Limoges : retrait privé d'information.
- Formalisation de la collaboration avec Planete : algèbre linéaire exacte pour les codes correcteurs LDPC.

- Formalisation de la collaboration avec le CEA : attaques par perturbation sur chiffrements algébriques.
- Formalisation de la collaboration avec Lyon et Chambéry sur les catégories et l'informatique.

Evelyne Tournier et Rodney Coleman sont amenés à prendre leur retraite durant le quadriennal 2010-2013. Les perspectives de recherche décrites en section 3 concernent pour partie l'interaction informatique-mathématiques, le calcul formel et la cryptologie, les systèmes complexes, les phénomènes non linéaires et l'interaction des mathématiques avec la biologie et la physique, qui sont au centre des objectifs de l'équipe. Pour mener ses travaux, l'équipe aura donc un besoin essentiel des supports de postes qui seront libérés lors de ces départs à la retraite (poste de PR 27 avec un profil interaction informatique-mathématiques, et poste de MCF ou PR 26).

13 Publications (Janvier 2006 à Mai 2009)

International and national peer-reviewed journals [ACL]

2009 : [A8, A6, A4, A3, A2, A7, A5, A1]

2008 : [A17, A11, A9, A15, A13, A16, A12, A18, A14, A10]

2007 : [A29, A28, A30, A25, A27, A23, A26, A22, A31, A24, A20, A32, A21, A19]

2006 : [A38, A33, A37, A36, A35, A34]

International and national peer-reviewed conference proceedings [ACT]

2009 : [B43, B42, B44, B41, B40, B39]

2008 : [B45, B53, B50, B48, B46, B52, B47, B51, B49]

2007 : [B61, B60, B55, B54, B58, B56, B59, B57]

2006 : [B77, B81, B62, B71, B67, B80, B75, B76, B73, B79, B72, B68, B64, B63, B78, B74, B66, B70, B65, B69]

Invited conferences, seminars and tutorials [INV]

2009 : [E98, E100, E99, E97, E101]

2008 : [E104, E102, E106]

2007 : [E117, E114]

2006 : [E125, E119, E122, E124, E123]

Short communications [COM] and posters [AFF] in conferences and workshops

2009 : []

2008 : [E108, E107, E105, E103]

2007 : [E115, E111, E110, E116, E109, E112, E113]

2006 : [E118, E121, E120]

Scientific books and book chapters [OS]

2009 : [C83, C82]

2008 : [C87, C88]

2007 : [C84]

2006 : [C92, C91, C90, C89]

Book or proceedings editing [DO]

2009 : []

2008 : []

2007 : []

2006 : [C85, C86]

Doctoral dissertations and habilitation theses [TH]

2009 : []
2008 : []
2007 : [D93]
2006 : [D94, D95, D96]

Softwares

2009 : [H172, H171, H170]
2008 : [H173]
2007 : []
2006 : [H174]

Techreports

2009 : [F128, F127, F126, F129, F130]
2008 : [F132, F131, F133]
2007 : [F136, F134, F139, F140, F135, F138, F137]
2006 : [F143, F141, F144, F142]

Seminars

2009 : [G149, G146, G147, G145, G148]
2008 : [G150, G153, G152, G151]
2007 : [G156, G157, G159, G154, G155, G158]
2006 : [G169, G163, G168, G165, G166, G167, G162, G161, G164, G160]

	2006	2007	2008	2009	Total
ACL – International and national peer-reviewed journals	6	14	10	8	38
ACT – International and national peer-reviewed conference proceedings	20	8	9	6	43
INV – Invited conferences	5	2	3	5	15
COM / AFF – Short communications and posters in conferences and workshops	3	7	4	0	14
OS – Scientific books and book chapters	4	1	2	2	9
DO – Book or proceedings editing	2	0	0	0	2
TH – Doctoral dissertations and habilitation theses	3	1	0	0	4
AP – Other publications	15	13	8	13	49
Total	58	46	36	34	174

ACL – International and national peer-reviewed journals

- [A1] Jesús Cuevas, Guillaume James, Panayotis Kevrekidis et Kody Law. Vortex solutions of the discrete Gross-Pitaevskii equation starting from the anti-continuum limit. *Physica D*, pages 1–10, 2009. to appear.
- [A2] Georgios E. Fainekos, Antoine Girard, Hadas Kress-Gazit et George J. Pappas. Temporal logic motion planning for dynamic robots. *Automatica*, 45(2) :343–352, février 2009.
- [A3] Frédéric Fauvet, Françoise Richard-Jung et Jean Thomann. Automatic computation of Stokes matrices. *Numer. Algorithms*, 50(2) :179–213, février 2009.
- [A4] Antoine Girard et George J. Pappas. Hierarchical control system design using approximate simulation. *Automatica*, 45(2) :566–571, février 2009.
- [A5] Guillaume James, Pascal Noble et Yannick Sire. Continuation of relative periodic orbits in a class of triatomic Hamiltonian systems. *Ann. Inst. Henri Poincaré-Anal. non linéaire*, pages 1–28, 2009. to appear.
- [A6] Guillaume James, Bernardo Sánchez-Rey et Jesús Cuevas. Breathers in inhomogeneous lattices : an analysis via center manifold reduction. *Rev. Math. Phys.*, 21(1) :1–59, février 2009.
- [A7] Colas Le Guernic et Antoine Girard. Reachability analysis of linear systems using support functions. *Nonl. Anal. Hybrid Syst.*, 2009. to appear.
- [A8] Michel Peyrard, Santiago Cuesta-López et Guillaume James. Nonlinear analysis of the dynamics of DNA breathing. *J. Biol. Phys.*, 35(1) :73–89, février 2009.
- [A9] Jesús Cuevas, Guillaume James, Panayotis Kevrekidis, Boris Malomed et Bernardo Sánchez-Rey. Approximation of solitons in the discrete NLS equation. *J. Nonlinear Math. Phys.*, 15(supplement 3) :124–136, octobre 2008. Special Issue : Nonlinear Evolution Equations and Dynamical Systems 2007.
- [A10] Jean-Guillaume Dumas. Caractérisation des Quenines et leur représentation spirale. *Math. Hum. Sci.*, 184(2008(4)) :9–23, 2008.
- [A11] Jean-Guillaume Dumas, Pascal Giorgi et Clément Pernet. Dense linear algebra over finite fields : the FFLAS and FFPACK packages. *ACM Trans. Math. Softw.*, 35(3) :1–35, octobre 2008.
- [A12] Antoine Girard, Agung A. Julius et George J. Pappas. Approximate simulation relations for hybrid systems. *Discret. Event Dyn. Syst.-Theory Appl.*, 18(2) :163–179, juin 2008.
- [A13] Roland Hildebrand. Semidefinite descriptions of low-dimensional separable matrix cones. *Linear Alg. Appl.*, 429(4) :901–932, août 2008.
- [A14] Roland Hildebrand, Stefano Mancini et Simone Severini. Combinatorial Laplacians and positivity under partial transpose. *Math. Struct. Comput. Sci.*, 18(1) :205–219, février 2008.
- [A15] Guillaume James et Pascal Noble. Weak coupling limit and localized oscillations in Euclidean invariant Hamiltonian systems. *J. Nonlinear Sci.*, 18(4) :433–461, août 2008.
- [A16] Michel Peyrard, Santiago Cuesta-López et Guillaume James. Modelling DNA at the mesoscale : a challenge for nonlinear science ? *Nonlinearity*, 21(6) :91–100, juin 2008.
- [A17] Giordano Pola, Antoine Girard et Paulo Tabuada. Approximately bisimilar symbolic models for nonlinear control systems. *Automatica*, 44(10) :2508–2516, octobre 2008.
- [A18] Philippe Poncet, Roland Hildebrand, Georges-Henri Cottet et Petros Koumoutsakos. Spatially distributed control for optimal drag reduction of the flow past a circular cylinder. *J. Fluid Mech.*, 599 :111–120, mars 2008.
- [A19] Eugene Asarin, Thao Dang et Antoine Girard. Hybridization methods for the analysis of non-linear systems. *Acta Inform.*, 43(7) :451–476, janvier 2007. Special issue on Hybrid Systems.
- [A20] Jean-Guillaume Dumas. Bounds on the coefficients of the characteristic and minimal polynomials. *J. Ineq. Pure Appl. Math.*, 8(2) :1–15, avril 2007.
- [A21] Laurent Fousse. Multiple-precision correctly rounded Newton-Cotes quadrature. *Rairo-Inform. Théor. Appl.*, 41(2) :103–121, janvier 2007. Special issue : Real Numbers.
- [A22] Laurent Fousse, Guillaume Hanrot, Vincent Lefèvre, Patrick Pélissier et Paul Zimmermann. MPFR : A multiple-precision binary floating-point library with correct rounding. *ACM Trans. Math. Softw.*, 33(2) :1–15, juin 2007.
- [A23] Antoine Girard et George J. Pappas. Approximate bisimulation relations for constrained linear systems. *Automatica*, 43(8) :1307–1317, août 2007.

- [A24] Antoine Girard et George J. Pappas. Approximation metrics for discrete and continuous systems. *IEEE Trans. Autom. Control*, 52(5) :782–798, mai 2007.
- [A25] Roland Hildebrand. Concurrence revisited. *J. Math. Phys.*, 48 :1–23, octobre 2007.
- [A26] Roland Hildebrand. Entangled states close to the maximally mixed state. *Phys. Rev. A*, 75(6) :1–10, juin 2007.
- [A27] Roland Hildebrand. Exactness of sums of squares relaxations involving 3x3 matrices and Lorentz cones. *Linear Alg. Appl.*, 426(3) :815–840, octobre 2007.
- [A28] Roland Hildebrand. An LMI description for the cone of Lorentz-positive maps. *Linear Multilinear Algebra*, 55(6) :551–573, novembre 2007.
- [A29] Roland Hildebrand. Positive maps of second-order cones. *Linear Multilinear Algebra*, 55(6) :575–597, novembre 2007.
- [A30] Roland Hildebrand. Positive partial transpose from spectra. *Phys. Rev. A*, 76(5) :1–5, novembre 2007.
- [A31] Roland Hildebrand et Gabriel Solari. Identification for control : optimal input intended to identify a minimum variance controller. *Automatica*, 43(5) :758–767, mai 2007.
- [A32] Guillaume James et Michael Kastner. Bifurcations of discrete breathers in a diatomic Fermi-Pasta-Ulam chain. *Non-linearity*, 20(3) :631–657, mars 2007.
- [A33] Xavier Bombois, Gérard Scorletti, Michel Gevers, Paul Van Den Hof et Roland Hildebrand. Least costly identification experiment for control. *Automatica*, 42(10) :1651–1662, octobre 2006.
- [A34] Jacques Dubrois et Jean-Guillaume Dumas. Efficient polynomial time algorithms computing industrial-strength primitive roots. *Inf. Process. Lett.*, 97(2) :41–45, janvier 2006.
- [A35] Jean-Guillaume Dumas et Jean-Louis Roch. Signature électronique et hachage. *Tangente*, 26, juin 2006. Hors série : Cryptographie et codes secrets.
- [A36] Jean-Guillaume Dumas et Denis Trystram. Les anniversaires des briseurs de code. *Tangente*, 26, juin 2006. Hors série : Cryptographie et codes secrets.
- [A37] Antoine Girard. Towards a multiresolution approach to linear control. *IEEE Trans. Autom. Control*, 51(8) :1261–1270, août 2006.
- [A38] Roland Hildebrand. On the approximation of convex functions with cumulant generating functions. *C. R. Math.*, 343(8) :545–550, octobre 2006.

ACT – International and national peer-reviewed conference proceedings

- [B39] Alexandre Berzati, Cécile Canovas, Jean-Guillaume Dumas et Louis Goubin. Fault attacks on RSA public keys : Left-to-right implementations are also vulnerable. Dans Marc Fischlin, éditeur, *RSA Conference 2009, Cryptographers' Track, April, 2009*, volume 5473 of *Lecture Notes in Computer Science*, pages 414–428, San Francisco, Etats-Unis, 2009. Springer.
- [B40] Brice Boyer, Jean-Guillaume Dumas, Clément Pernet et Wei Zhou. Memory efficient scheduling of Strassen-Winograd's matrix multiplication algorithm. Dans *International Symposium on Symbolic and Algebraic Computation 2009, ISSAC'09, July, 2009*, Séoul, Corée du Sud, 2009. to appear.
- [B41] Jean-Guillaume Dumas, Clément Pernet et B. David Saunders. On finding multiplicities of characteristic polynomial factors of black-box matrices. Dans *International Symposium on Symbolic and Algebraic Computation 2009, ISSAC'09, July, 2009*, Séoul, Corée du Sud, 2009. to appear.
- [B42] Dominique Duval, Rachid Echahed et Frédéric Prost. A heterogeneous pushout approach to term-graph transformation. Dans *20th International Conference on Rewriting Techniques and Applications, RTA 2009, June, 2009*, volume 5595 of *Lecture Notes in Computer Science*, pages 194–208, Brasília, Brésil, juin 2009. Springer.
- [B43] Roland Hildebrand et Gabriel Solari. Closed-loop optimal input design : The partial correlation approach. Dans *15th IFAC Symposium of System Identification, July, 2009*, France, juillet 2009.
- [B44] Colas Le Guernic et Antoine Girard. Reachability analysis of hybrid systems using support functions. Dans *Computer Aided Verification, June, 2009*, Lecture Notes in Computer Science, Grenoble, France, 2009. Springer.
- [B45] Gang Zheng et Antoine Girard. Bounded and unbounded safety verification using bisimulation metrics. Dans *12th International Conference on Hybrid Systems : Computation and Control, HSCC 2009, April, 2009*, Lecture Notes in Computer Science, San Francisco, Etats-Unis, 2009.

- [B46] Jean-Guillaume Dumas. Q-adic transform revisited. Dans J. Rafael Sendra et Laureano González Vega, éditeurs, *International Symposium on Symbolic and Algebraic Computation, ISSAC 2008, July, 2008*, pages 63–69, Hagenberg, Autriche, juillet 2008. ACM.
- [B47] Jean-Guillaume Dumas, Laurent Fousse et Bruno Salvy. Compressed modular matrix multiplication. Dans *Milestones in Computer Algebra, MICA'2008, May, 2008*, pages 133–140, Tobago, Trinidad et Tobago, mai 2008.
- [B48] Antoine Girard et Colas Le Guernic. Efficient reachability analysis for linear systems using support functions. Dans *17th IFAC World Congress, July, 2008*, Seoul, Corée du Sud, juillet 2008. IFAC.
- [B49] Antoine Girard et Colas Le Guernic. Zonotope/hyperplane intersection for hybrid systems reachability analysis. Dans Magnus Egerstedt et Bud Mishra, éditeurs, *Hybrid Systems : Computation and Control, April, 2008*, volume 4981 of *Lecture Notes in Computer Science*, pages 215–228, Saint Louis, MO, Etats-Unis, avril 2008. Springer.
- [B50] Antoine Girard et Samuel Martin. Motion planning for nonlinear systems using hybridizations and robust controllers on simplices. Dans *47th IEEE Conference on Decision and Control, December, 2008*, Cancun, Mexique, décembre 2008. IEEE.
- [B51] Antoine Girard, Giordano Pola et Paulo Tabuada. Approximately bisimilar symbolic models for incrementally stable switched systems. Dans Magnus Egerstedt et Bud Mishra, éditeurs, *11th International Workshop on Hybrid Systems : Computation and Control, HSCC 2008, April, 2008*, volume 4981 of *Lecture Notes in Computer Science*, pages 201–214, Saint Louis, MO, Etats-Unis, avril 2008. Springer.
- [B52] Roland Hildebrand. A control problem with a Smale's Horseshoe in the solution. Dans *International Conference "Differential Equations and Topology" Dedicated to the Centennial Anniversary of Lev Semenovich Pontryagin, June, 2008*, pages 253–254, Moscou, Russie, juin 2008.
- [B53] Roland Hildebrand. Optimal inputs for FIR system identification. Dans *47th IEEE Conference on Decision and Control, CDC 2008, December, 2008*, pages 5525–5530, Cancun, Mexique, décembre 2008. IEEE.
- [B54] Jean-Guillaume Dumas, Philippe Elbaz-Vincent, Pascal Giorgi et Anna Urbańska. Parallel computation of the rank of large sparse matrices from algebraic K-theory. Dans Stephen M. Watt, éditeur, *Parallel Symbolic Computation'07, PASCO 2007, July, 2007*, pages 43–52, Ontario, Canada, France, juillet 2007. Waterloo Univeristy.
- [B55] Dominique Duval, Rachid Echahed et Frédéric Prost. Adjunction for garbage collection with application to graph rewriting. Dans Franz Baader, éditeur, *Term Rewriting and Applications, proceedings of the 18th International Conference on Rewriting Techniques and Applications, RTA 2007, June, 2007*, volume 4533 of *Lecture Notes in Computer Science*, pages 122–136, Paris, France, août 2007. Springer.
- [B56] Dominique Duval, Rachid Echahed et Frédéric Prost. Modeling pointer redirection as cyclic term-graph rewriting. Dans *Third International Workshop on Term Graph Rewriting, TERMGRAPH'06, April, 2006*, volume 176 of *Electronic Notes in Computer Science*, pages 65–84, Vienne, Autriche, mai 2007. Elsevier.
- [B57] Georgios E. Fainekos, Antoine Girard et George J. Pappas. Hierarchical synthesis of hybrid controllers from temporal logic specifications. Dans Alberto Bemporad, Antonio Bicchi et Giorgio Buttazzo, éditeurs, *Hybrid Systems : Computation and Control, HSCC 2007, April, 2007*, volume 4416 of *Lecture Notes in Computer Science*, pages 203–216, Pise, Italie, avril 2007. Springer.
- [B58] Laurent Fousse. Accurate multiple-precision Gauss-Legendre quadrature. Dans *IEEE Symposium on Computer Arithmetic, ARITH18, June, 2007*, pages 150–160, Montpellier, France, juin 2007. IEEE.
- [B59] Antoine Girard. Approximately bisimilar finite abstractions of stable linear systems. Dans Alberto Bemporad, Antonio Bicchi et Giorgio Buttazzo, éditeurs, *Hybrid Systems : Computation and Control, April, 2007*, volume 4416 of *Lecture Notes in Computer Science*, pages 231–244, Pise, Italie, avril 2007. Springer.
- [B60] Antoine Girard et George J. Pappas. Approximate hierarchies of linear control systems. Dans *46th IEEE Conference on Decision and Control, December, 2007*, pages 3727–3732, New Orleans, LA, Etats-Unis, décembre 2007. IEEE, IEEE.
- [B61] Giordano Pola, Antoine Girard et Paulo Tabuada. Symbolic models for nonlinear control systems using approximate bisimulation. Dans *46th IEEE Conference on Decision and Control, December, 2007*, pages 4656–4661, New Orleans, LA, Etats-Unis, décembre 2007. IEEE, IEEE.
- [B62] Eugene Asarin, Thao Dang, Goran Frehse, Antoine Girard, Colas Le Guernic et Oded Maler. Recent progress in continuous and hybrid reachability analysis. Dans *International Symposium on Computer-Aided Control System Design, CACSD 2006, October, 2006*, pages 1582–1587, Munich, Allemagne, octobre 2006. IEEE.
- [B63] Van-Dat Cung, Vincent Danjean, Jean-Guillaume Dumas, Thierry Gautier, Guillaume Huard, Bruno Raffin, Christophe Rapine, Jean-Louis Roch et Denis Trystram. Adaptive and hybrid algorithms : classification and illustration

- on triangular system solving. Dans Jean-Guillaume Dumas, éditeur, *Transgressive Computing, April, 2006*, pages 131–148, Grenade, Espagne, avril 2006.
- [B64] Jean Della Dora, Aude Maignan et Laurent Tournier. Dynamic systems : an algorithmic point of view. Dans Jean-Guillaume Dumas, éditeur, *Transgressive Computing 2006, April, 2006*, pages 3–14, Grenade, Espagne, avril 2006. invited conference.
- [B65] César Domínguez, Dominique Duval, Laureano Lambán et Julio Rubio García. Towards diagrammatic specifications of symbolic computations systems. Dans Thierry Coquand, Henri Lombardi et Marie-Françoise Roy, éditeurs, *Mathematics, Algorithms, Proofs, January, 2005*, numéro 05021 dans Dagstuhl Seminar Proceedings, pages 1–23, Dagstuhl, Allemagne, janvier 2006. Internationales Begegnungs- und Forschungszentrum für Informatik (IBFI).
- [B66] Jean-Guillaume Dumas et Dominique Duval. Vers une modélisation diagrammatique de la bibliothèque C++ d’algèbre linéaire LinBox. Dans Roger Rousseau, Christelle Urtado et Sylvain Vauttier, éditeurs, *Langages et Modèles à Objets, LMO’06, March, 2006*, pages 117–132, Nîmes, France, mars 2006. Hermès.
- [B67] Jean-Guillaume Dumas, Clément Pernet et Jean-Louis Roch. Adaptive and hybrid algorithms. Dans Wolfram Decker, Mike Dewar, Etich Kaltofen et Stephen Watt, éditeurs, *Challenges in Symbolic Computation Software, July, 2006*, numéro 06271 dans Dagstuhl Seminar Proceedings, Dagstuhl, Allemagne, juillet 2006.
- [B68] Jean-Guillaume Dumas et Anna Urbańska. An introspective algorithm for the integer determinant. Dans Jean-Guillaume Dumas, éditeur, *Transgressive Computing, April, 2006*, pages 185–202, Grenade, Espagne, avril 2006.
- [B69] Dominique Duval et Jean-Claude Reynaud. About raising and handling exceptions. Dans *18th International Workshop on Algebraic Development Techniques, WADT’06, June, 2006*, La Roche en Ardenne, Belgique, 2006.
- [B70] Dominique Duval et Jean-Claude Reynaud. Dynamic logic and exceptions : an introduction. Dans Thierry Coquand, Henri Lombardi et Marie-Françoise Roy, éditeurs, *Mathematics, Algorithms, Proofs, January, 2005*, numéro 05021 dans Dagstuhl Seminar Proceedings, pages 1–13, Dagstuhl, Allemagne, janvier 2006. Internationales Begegnungs- und Forschungszentrum fuer Informatik (IBFI).
- [B71] Georgios E. Fainekos, Antoine Girard et George J. Pappas. Temporal logic verification using simulation. Dans Eugene Asarin et Patricia Bouyer, éditeurs, *Formal Modelling and Analysis of Timed Systems, FORMATS 2006, September, 2006*, volume 4202 of *Lecture Notes in Computer Science*, pages 171–186, Paris, France, septembre 2006. Springer.
- [B72] Frédéric Fauvet, Françoise Richard-Jung et Jean Thomann. Algorithms for the splitting of formal series ; applications to alien differential calculus. Dans Jean-Guillaume Dumas, éditeur, *Transgressive Computing 2006, April, 2006*, pages 231–246, Grenade, Espagne, avril 2006.
- [B73] Antoine Girard, Agung A. Julius et George J. Pappas. Approximate simulation relations for hybrid systems. Dans Christos Cassandras, Alessandro Giua, Carla Seatzu et Janan Zaytoon, éditeurs, *Analysis and Design of Hybrid Systems, ADHS’06, June, 2006*, IFAC Proceedings, pages 106–111, Alghero, Italie, juin 2006. IFAC, Elsevier.
- [B74] Antoine Girard, Colas Le Guernic et Oded Maler. Efficient computation of reachable sets of linear time-invariant systems with inputs. Dans Joao P. Hespanha et Ashish Tiwari, éditeurs, *Hybrid Systems : Computation and Control, HSCC 2006, March, 2006*, volume 3927 of *Lecture Notes in Computer Science*, pages 257–271, Santa Barbara, Etats-Unis, mars 2006. Springer.
- [B75] Antoine Girard et George J. Pappas. Approximate bisimulations for constrained linear systems. Dans *Conference on Decision and Control and European Control Conference, December, 2005*, pages 4700–4705, Seville, Espagne, juin 2006. IEEE, IEEE.
- [B76] Antoine Girard et George J. Pappas. Approximate bisimulations for nonlinear dynamical systems. Dans *Conference on Decision and Control and European Control Conference, December, 2005*, pages 684–689, Seville, Espagne, juin 2006. IEEE, IEEE.
- [B77] Antoine Girard et George J. Pappas. Hierarchical control using approximate simulation relations. Dans *45th IEEE Conference on Decision and Control, December, 2006*, pages 264–269, San Diego, Etats-Unis, décembre 2006. IEEE, IEEE.
- [B78] Antoine Girard et George J. Pappas. Verification using simulation. Dans Joao P. Hespanha et Ashish Tiwari, éditeurs, *Hybrid Systems : Computation and Control, HSCC 2006, March, 2006*, volume 3927 of *Lecture Notes in Computer Science*, pages 272–286, Santa Barbara, Etats-Unis, mars 2006. Springer.
- [B79] Roland Hildebrand. Self-similar trajectories in multi-input systems. Dans Jean-Guillaume Dumas, éditeur, *Transgressive Computing 2006, April, 2006*, pages 287–302, Grenade, Espagne, avril 2006.
- [B80] Agung A. Julius, Antoine Girard et George J. Pappas. Approximate bisimulation for a class of stochastic hybrid systems. Dans *American Control Conference, June, 2006*, pages 4724–4729, Portland, Etats-Unis, juin 2006. IEEE.

- [B81] Truong Nghiem, George J. Pappas, Antoine Girard et Rajeev Alur. Time-triggered implementations of dynamic controllers. Dans Sang Lyul Min et Wang Yi, éditeurs, *Conference on Embedded Software, EMSOFT'06, October, 2006*, pages 2–11, Seoul, Corée du Sud, octobre 2006. ACM and IEEE.

OS – Scientific books and book chapters, DO – Book or proceedings editing

— OS – Scientific books —

- [C82] Rodney Coleman. *Differential calculus on normed vector spaces*. Springer, 2009. En cours de révision.
- [C83] Jean-Guillaume Dumas, Jean-Louis Roch, Éric Tannier, Sébastien Varrette, Romain Xu et Rodney Coleman. *Foundations of Coding : Compression, Encryption, Error-Correction*. Dunod, 2009. to appear. 374 pages.
- [C84] Jean-Guillaume Dumas, Jean-Louis Roch, Éric Tannier et Sébastien Varrette. *Théorie des codes : Compression, Cryptage, Correction*. Sciences Sup. Dunod, janvier 2007. . 352 pages.
- [C85] Jean-Guillaume Dumas, éditeur. *Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computations*. ISSAC. ACM press, juillet 2006. ISBN 1-59593-276-3. 361 pages.
- [C86] Jean-Guillaume Dumas, éditeur. *Proceedings of Transgressive Computing 2006*. U. J. Fourier, Grenoble, France, avril 2006. . 448 pages.

— OS – Book chapters, DO – Book or proceedings editing —

- [C87] Thao Dang, Goran Frehse, Antoine Girard et Colas Le Guernic. Outils pour l'analyse des modèles hybrides. Dans Olivier H. Roux et Claude Jard, éditeurs, *Approches formelles des systèmes embarqués communicants*, Traité IC2, chapter 8. Hermes, octobre 2008.
- [C88] Guillaume James et Yannick Sire. Center manifold theory in the context of infinite one-dimensional lattices. Dans Giovanni Gallavotti, éditeur, *The Fermi-Pasta-Ulam Problem. A Status Report*, volume 728 of *Lecture Notes in Physics*, chapter 6, pages 207–238. Springer, janvier 2008.
- [C89] Pascal Bouvry, Jean-Guillaume Dumas, Roland Gillard, Jean-Louis Roch et Sébastien Varrette. Cryptographie à clef secrète. Dans Touradj Ebrahimi, Franck Leprévost et Bertrand Warusfel, éditeurs, *Enjeux de la sécurité multimédia*, Traité IC2 : Information - Commande - Communication, pages 121–198. Hermès, février 2006.
- [C90] Jean-Guillaume Dumas, Franck Leprévost, Jean-Louis Roch, Valentin Savin et Sébastien Varrette. Cryptographie à clef publique. Dans Touradj Ebrahimi, Franck Leprévost et Bertrand Warusfel, éditeurs, *Enjeux de la sécurité multimédia*, Traité IC2 : Information - Commande - Communication, pages 199–280. Hermès, février 2006.
- [C91] Jean-Guillaume Dumas, Franck Leprévost, Jean-Louis Roch et Sébastien Varrette. Architectures PKI. Dans Touradj Ebrahimi, Franck Leprévost et Bertrand Warusfel, éditeurs, *Enjeux de la sécurité multimédia*, volume 2 of *Traité IC2 : Information - Commande - Communication*, pages 187–210. Hermès, février 2006.
- [C92] Michel Gevers, Xavier Bombois, Gérard Scorletti, Paul Van Den Hof et Roland Hildebrand. Experiment design for robust control : Why do more work than is needed ? Dans Bruce A. Francis, Malcolm C. Smith et Jan C. Willems, éditeurs, *Control of Uncertain Systems : Modelling, Approximation, and Design. A Workshop on the Occasion of Keith Glover's 60th Birthday*, volume 329 of *Lecture Notes in Control and Information Sciences*, pages 139–162. Springer, mars 2006.

TH – Doctoral dissertations and habilitation theses

- [D93] Sébastien Kolb. *Théorie des bifurcations appliquée à l'analyse de la dynamique du vol des hélicoptères*. PhD thesis, Institut National Polytechnique de Grenoble, juin 2007.
- [D94] Laurent Fousse. *Intégration numérique avec erreur bornée en précision arbitraire*. PhD thesis, Université Nancy 1, décembre 2006.
- [D95] Clément Pernet. *Algèbre linéaire exacte efficace : le calcul du polynôme caractéristique*. PhD thesis, Université Joseph Fourier, septembre 2006.
- [D96] Aude Rondepierre. *Algorithmes hybrides pour le contrôle optimal des systèmes non linéaires*. PhD thesis, Institut National Polytechnique de Grenoble, juillet 2006.

INV – Invited conferences, COM / AFF – Short communications and posters in conferences and workshops

- [E97] Jean-Guillaume Dumas, Dominique Duval et Jean-Claude Reynaud. Sequential products for effects. Dans *Applied and Computational Category Theory*, York, Royaume-Uni. invited conference, mars 2009.
- [E98] Antoine Girard. Symbolic models of control systems. Dans *Heterogeneity in control systems*, Nancy, France. invited conference, mai 2009.
- [E99] Antoine Girard. Vérification des systèmes hybrides. Dans *École des Journées Doctoriales du GDR MACS*, Angers, France. invited conference, mars 2009.
- [E100] Guillaume James. Dynamique non linéaire de l'ADN et formation de breathers. Dans *GDR MOAD*, Grenoble, France. invited conference, mars 2009.
- [E101] Guillaume James. Time-periodic oscillations in weakly inhomogeneous nonlinear lattices. Dans *Coherence and persistence in nonlinear waves, CPNLW09*, Université de Nice, France. invited conference, janvier 2009.
- [E102] Jean-Guillaume Dumas. Arithmétique compressée pour des petits corps finis. Dans *Rencontres Arithmétique de l'Informatique Mathématique*, Lille, France. invited conference, juin 2008.
- [E103] Jean-Guillaume Dumas. Compromis temps/mémoire en algèbre linéaire dense sur des corps finis. Dans *GDR Informatique Mathématique*, Paris, France. janvier 2008.
- [E104] Jean-Guillaume Dumas. Simultaneous modular reduction and Kronecker substitution for small finite fields. Dans *Sage Days 10*, LORIA Nancy, France. invited conference, octobre 2008.
- [E105] Dominique Duval, Rachid Echahed et Frédéric Prost. A double-pushout approach for modeling pointer redirection. Dans *IFIP WG1.3 meeting*, Sierra Nevada, Espagne. janvier 2008.
- [E106] Antoine Girard. Modèles symboliques de systèmes dynamiques pour la conception de systèmes embarqués sûrs. Dans *Colloque en hommage à Louis Bolliet : l'Informatique à Venir*, Grenoble, France. invited conference, mai 2008.
- [E107] Antoine Girard. Systèmes à commutation, stabilité, représentation symbolique et commande. Dans *GT Systèmes dynamiques hybrides du GDR MACS*, France. janvier 2008.
- [E108] Françoise Richard-Jung. Automatic computation of Stokes matrices and application to the graphical representation of solutions of linear ODE. Dans *Algorithmes formels et numériques pour les équations différentielles et aux différences*, Limoges, France. mars 2008.
- [E109] Jean-Guillaume Dumas. Outils pour un intergiciel générique en calcul formel. Dans *Journées Nationales de Calcul Formel*, CIRM, Luminy, France. février 2007.
- [E110] Dominique Duval, Jean-Guillaume Dumas et Jean-Claude Reynaud. Sequential products in effect categories. Dans *Journées ARROWS*, Nancy, France. juin 2007.
- [E111] Laurent Fousse. Calcul rapide de coefficients pour l'intégration numérique. Dans *Journées 2007 de l'ANR GECKO*, Sophia Antipolis, France. novembre 2007.
- [E112] Laurent Fousse. CRQ : une bibliothèque pour l'intégration numérique certifiée en précision arbitraire. Dans *Journées Nationales de Calcul Formel, JCNF 2007*, CIRM, Luminy, France. janvier 2007.
- [E113] Laurent Fousse. Implémentation efficace d'ECM. Dans *Rencontres Arithmétiques de l'Informatique Mathématique (GDR IM)*, Montpellier, France. janvier 2007.
- [E114] Antoine Girard. Méthodes algorithmiques pour l'analyse des systèmes hybrides. Dans *Journées Nationales du GDR MACS*, Reims, France. invited conference, juillet 2007.
- [E115] Antoine Girard. VAL-AMS : High confidence validation of analog and mixed signal circuits. Dans *Grand Colloque STIC*, France. novembre 2007.
- [E116] Roland Hildebrand. Semidefinite description of separable cones involving the Lorentz cone. Dans *Convex optimization and applications in control theory, probability and statistics*, Luminy, Marseille, France. avril 2007.
- [E117] Guillaume James. Bifurcations of discrete breathers in inhomogeneous lattices. Dans *Hamiltonian lattice dynamical systems*, Leiden, Pays-Bas. invited conference, octobre 2007.
- [E118] Jean-Guillaume Dumas. Adaptive triangular system solving. Dans *Challenges in Symbolic Computation Software*, Dagstuhl Seminar 06271, Allemagne. juillet 2006.
- [E119] Jean-Guillaume Dumas. Exact linear algebra software. Dans *International Congress on Mathematical Software, ICMS'2006*, Castro Urdiales, Espagne. invited conference, septembre 2006.

- [E120] Laurent Fousse. The elliptic curve factorization method. Dans *TYPES Workshop on Numbers and Proofs*, Orsay, France. juin 2006.
- [E121] Laurent Fousse. Quelques algorithmes pour l'intégration numérique en précision arbitraire. Dans *Journées Nationales d'Arithmétique des Ordinateurs*, ENS Lyon, France. juin 2006.
- [E122] Antoine Girard. Approximation metrics for discrete and continuous systems. Dans *Workshop Topics in Computation and Control*, Santa Barbara, Etats-Unis. invited conference, mars 2006.
- [E123] Antoine Girard. Relations de simulation approchées pour la vérification des systèmes dynamiques continus et hybrides. Dans *Groupe de travail "Systèmes Dynamiques Hybrides"*, Paris, France. invited conference, février 2006.
- [E124] Antoine Girard. Zonotope techniques for reachability analysis. Dans *Workshop Topics in Computation and Control*, Santa Barbara, Etats-Unis. invited conference, mars 2006.
- [E125] Guillaume James. Travelling breathers in nonlinear oscillator chains. Dans *Nonlinear dynamics of acoustic modes in finite lattices : localization, equipartition, transport*, Dresde, Allemagne. invited conference, décembre 2006.

Techreports

- [F126] Stéphane Despréaux et Aude Maignan. Dynamical systems based on dynamic graphs. Rapport de recherche, LJK, France, mai 2009. submitted.
- [F127] Stéphane Despréaux et Aude Maignan. A program for dynamical systems based on dynamic graphs : Dynsys. Rapport de recherche, LJK, France, mai 2009. submitted.
- [F128] Stéphane Despréaux et Aude Maignan. A short tutorial for Dynsys : A program for dynamical systems based on dynamic graphs. Rapport technique, LJK, France, mai 2009.
- [F129] Jean-Guillaume Dumas, Dominique Duval et Jean-Claude Reynaud. Cartesian effect categories are Freyd-categories. Rapport de recherche hal-00369328, HAL, mars 2009.
- [F130] Françoise Richard-Jung. Graphical representation of solutions of linear ODEs, using Stokes matrices. Rapport technique, LJK, France, 2009. soumis à Numer. Alg.
- [F131] Jean-Guillaume Dumas, Laurent Fousse et Bruno Salvy. Simultaneous modular reduction and Kronecker substitution for small finite fields. Rapport de recherche hal-00315772, HAL, août 2008.
- [F132] Dominique Duval, Rachid Echahed et Frédéric Prost. A cloning pushout approach to term-graph transformation. Rapport de recherche hal-00340202, HAL, novembre 2008.
- [F133] Roland Hildebrand. Identification of community structure in networks with convex optimization. Rapport de recherche 0806.1896, arXiv, France, juin 2008. submitted.
- [F134] Jean-Guillaume Dumas, Dominique Duval et Jean-Claude Reynaud. Sequential products in effect categories. Rapport de recherche hal-00161303, HAL, juillet 2007.
- [F135] Jean-Guillaume Dumas, Philippe Elbaz-Vincent, Pascal Giorgi et Anna Urbańska. Parallel computation of the rank of large sparse matrices from algebraic K-theory. Rapport de recherche hal-00142141, HAL, avril 2007.
- [F136] Dominique Duval. Diagrammatic inference. Rapport de recherche hal-00177075, HAL, octobre 2007.
- [F137] Roland Hildebrand. Entangled states close to the maximally mixed state. Rapport de recherche quant-ph/0702040, arXiv, février 2007.
- [F138] Roland Hildebrand. An LMI description for the cone of Lorentz-positive maps II. Rapport de recherche 2007/08/1747, Optimization Online, mars 2007. submitted.
- [F139] Truong Nghiem, George J. Pappas, Rajeev Alur et Antoine Girard. Time-triggered implementations of dynamic controllers. Rapport de recherche, LJK, juin 2007. submitted.
- [F140] Anna Urbańska. Towards an exact adaptive algorithm for the determinant of a rational matrix. Rapport de recherche hal-00150872, HAL, mai 2007.
- [F141] Roland Hildebrand. Concurrence of Lorentz-positive maps. Rapport de recherche quant-ph/0612064, arXiv, décembre 2006.
- [F142] Roland Hildebrand. Separable balls around the maximally mixed state for a 3-qubit system. Rapport de recherche quant-ph/0601201, arXiv, janvier 2006.
- [F143] Roland Hildebrand, Stefano Mancini et Simone Severini. Combinatorial Laplacians and positivity under partial transpose. Rapport de recherche cs.CC/0607036, arXiv, décembre 2006. Soumis à Mathematical Structures in Computer Science.
- [F144] Aude Maignan. Modélisation des systèmes dynamiques évolutifs. Rapport technique, LJK, France, septembre 2006.

Seminars

- [G145] Laurent Fousse. Filtrés à mot-clés secret et réseaux euclidiens, mars 2009, Séminaire du département MAD, LJK. Talk given at Grenoble, France.
- [G146] Laurent Fousse. Filtrés à mot-clés secrets et réseaux euclidiens, mai 2009, XLIM. Talk given at Limoges, France.
- [G147] Laurent Fousse. Filtrés à mot-clés secrets et réseaux euclidiens, mars 2009, Séminaire de cryptologie, codage et infrastructures sécurisées. Talk given at Grenoble, France.
- [G148] Laurent Fousse. Filtrés à mot-clés secrets et réseaux euclidiens, mars 2009, Séminaire de Cryptologie GREYC. Talk given at Caen, France.
- [G149] Antoine Girard. Symbolic models for control systems, juin 2009, IRCCyN. Talk given at Nantes, France.
- [G150] Jean-Guillaume Dumas. Attaques laser sur RSA embarqué, décembre 2008, MAD circus. Talk given at Grenoble, France.
- [G151] Jean-Guillaume Dumas. Comment casser RSA et le logarithme discret ?, janvier 2008, Séminaire Modèles et Algorithmes Déterministes. Talk given at Grenoble, France.
- [G152] Dominique Duval, Jean-Claude Reynaud, Christian Lair et Jean-Guillaume Dumas. Logiques diagrammatiques et effets de bord, juin 2008, Groupe de travail Sémantique et Réalisabilité, équipe PPS. Talk given at Paris, France.
- [G153] Laurent Fousse. Réduction modulaire simultanée et substitution de Kronecker pour les petits corps finis, septembre 2008, Séminaire Arénaire. Talk given at ENS Lyon, France.
- [G154] Jean-Guillaume Dumas. Algèbre linéaire exacte, mars 2007. Talk given at Orsay, France.
- [G155] Dominique Duval. Sémantiques pour un langage impératif, février 2007, Colloquium du LACO. Talk given at Limoges, France.
- [G156] Laurent Fousse. CRQ : une bibliothèque pour l'intégration numérique certifiée en précision arbitraire, juin 2007, Séminaire BIPOP-CASYS. Talk given at Grenoble, France.
- [G157] Antoine Girard. Hierarchical abstractions of dynamical systems using approximate simulation and bisimulation relations, mai 2007, Department of Electrical Engineering Seminar. Talk given at University of L'Aquila, Italie.
- [G158] Guillaume James. Bifurcations of discrete breathers in inhomogeneous lattices. Dans *Advanced study group : Localizing energy through nonlinearity, discreteness and disorder*, Dresde, Allemagne. invited conference, août 2007.
- [G159] Aude Maignan. Modélisation des systèmes dynamiques évolutifs, mars 2007, Séminaire BIPOP-CASYS. Talk given at Grenoble, France.
- [G160] Jean-Guillaume Dumas. Algèbre linéaire exacte, janvier 2006, Université Paris 11. Talk given at Orsay, France.
- [G161] Jean-Guillaume Dumas. Racines primitives industrielles, février 2006, Séminaire de cryptologie. Talk given at Institut Fourier, Grenoble, France.
- [G162] Jean-Guillaume Dumas. Résolution exacte de problèmes mal conditionnés, mars 2006, Institut Camille Jordan. Talk given at Lyon, France.
- [G163] Laurent Fousse. Intégration numérique avec erreur bornée en précision arbitraire, décembre 2006, Séminaire de l'équipe Algorithms. Talk given at INRIA Rocquencourt, France.
- [G164] Laurent Fousse. Intégration numérique multi-précision de Gauss-Legendre avec erreur bornée, janvier 2006, Séminaire de l'équipe DALI. Talk given at Perpignan, France.
- [G165] Antoine Girard. Méthodes algorithmiques pour l'analyse des systèmes hybrides, avril 2006, Verimag. Talk given at Grenoble, France.
- [G166] Antoine Girard. Méthodes algorithmiques pour l'analyse des systèmes hybrides, avril 2006, INRIA. Talk given at Grenoble, France.
- [G167] Antoine Girard. Méthodes algorithmiques pour l'analyse des systèmes hybrides, avril 2006, Laboratoire Jean Kuntzmann. Talk given at Grenoble, France.
- [G168] Antoine Girard. Modélisation hiérarchique des systèmes dynamiques, novembre 2006, Laboratoire Jean Kuntzmann. Talk given at Grenoble, France.
- [G169] Guillaume James. Bifurcations of discrete breathers in nonlinear lattices, décembre 2006, Imperial College, dynamics seminar. Talk given at Londres, Royaume-Uni invited conference.

Softwares

- [H170] Brice Boyer et Jean-Guillaume Dumas. Galet : Matrix multiplication schedule generator. Software LJK, janvier 2009.
- [H171] Stéphane Després et Aude Maignan. Dynsys. Software LJK, mai 2009.
- [H172] Françoise Richard-Jung. DESIR (new version, including automatic computation of Stokes matrices). Software LJK, mai 2009.
- [H173] Jean-Guillaume Dumas et Clément Pernet. Exact linear system resolution. Software LJK, novembre 2008.
- [H174] Laurent Fousse. CRQ : Correctly rounded quadrature library. Software INRIA, octobre 2006.