

# Les laboratoires de la



**FSMP**  
Fondation Sciences  
Mathématiques de Paris



**Institut de Recherche en Informatique  
Fondamentale**  
UMR 8243  
Université Paris Diderot

## Direction et administration

Directeur : Pierre Fraigniaud

Directeur adjoint : Thomas Ehrhard

Responsables administratives : Odile Ainardi, Noelle Delgado, Nadia Ibellatti

Tél. : +33(0)1 57 27 92 56/74 - Fax : +33(0)1 57 27 94 09/92 97

Université Paris Diderot, Case 7014, Bâtiment Sophie Germain, 75205 Paris Cedex 13

Web : <https://www.irif.univ-paris-diderot.fr/>

## Effectifs et équipes

L'IRIF compte actuellement une centaine de membres permanents, se répartissant en environ 55 enseignants-chercheurs, 30 chercheurs CNRS, 8 chercheurs INRIA et 6 personnels administratifs ou techniques. L'effectif total de l'IRIF, incluant doctorants, postdoctorants, et visiteurs de longue durée s'élève à près de 170 personnes. 6 thèmes de recherche :

**Algorithmes et complexité** - Responsable : Frédéric Magniez

**Algorithmique distribuée et graphes** - Responsable : Nicolas Schabanel

**Automates et applications** - Responsable : Olivier Serre

**Combinatoire** - Responsable : Sylvie Corteel

**Modélisation et vérification** - Responsable : Ahmed Bouajjani

**Preuves, programmes et systèmes** - Responsable : Yves Guiraud

## Thèmes de recherche

### Algorithmes et complexité

La théorie des algorithmes efficaces est le socle commun des axes de recherche que l'équipe étudie, à la fois en calcul classique et quantique.

Dans le domaine du calcul classique, l'équipe étudie la complexité de problèmes variés dans plusieurs modèles de calcul, en élaborant des algorithmes efficaces et en prouvant des bornes inférieures. L'équipe étudie plus particulièrement les domaines des algorithmes d'approximation, du property testing, des streaming algorithms, des online algorithms, de la théorie algorithmique des jeux, de la complexité de communication, et de la théorie de la cryptographie. Bon nombre des problématiques dans ces domaines requièrent, ou bénéficient, d'approches probabilistes.

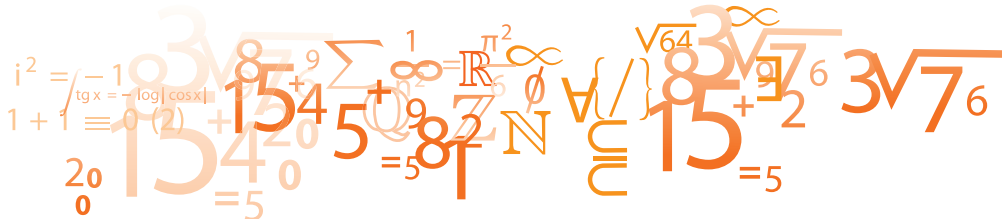
En calcul quantique l'équipe étudie le potentiel des algorithmes quantiques, cherche à mieux cerner l'apport de l'information quantique pour le calcul, la cryptographie et l'interaction, et explore les relations entre la complexité de communication classique et quantique.

L'échange d'idées et techniques entre le calcul quantique et probabiliste, dans les deux directions, est une caractéristique importante d'une part des recherches menées au sein du groupe.

### Algorithmique distribuée et graphes

Les recherches de l'équipe Algorithmique distribuée et graphes couvrent principalement les thématiques suivantes : algorithmique distribuée et algorithmique des graphes.

L'équipe possède en particulier une forte expertise en algorithmique pour les décompositions de graphes, et sur la conception et l'analyse d'algorithmes conçus pour des familles de graphes possédant des propriétés structurelles spécifiques telles qu'une métrique hyperbolique, une dimension doublante bornée, ou excluant un mineur. L'équipe couvre par ailleurs la plupart des thématiques de l'algorithmique distribuée, de la tolérance aux pannes (consensus, élection de leader, détecteurs de défaillance, etc.) au développement de protocoles distribués pour les réseaux (routage, étiquetage,



coloration, spanners, etc.).

Les domaines d'applications des travaux de l'équipe ont principalement trait à la conception de protocoles pour les réseaux pair-à-pair, et à l'analyse de différents types de réseaux sociaux (graphe du Web, petits mondes, etc.). Une partie des membres de l'équipe sont à ce titre membres du projet INRIA «GANG» dont l'objectif est le développement de méthodes algorithmiques pour la conception et le contrôle des réseaux à grande échelle.

### Automates et applications

Les recherches de l'équipe Automates et applications portent d'une part sur les questions fondamentales de la théorie des automates et d'autre part sur des questions algorithmiques issues de problèmes concrets. Les aspects fondamentaux concernent principalement les semigroupes, la combinatoire des mots, les liens avec la logique, la topologie, les jeux, etc. Un effort particulier a été fait ces dernières années sur les extensions de la notion d'automate : automates travaillant sur des mots infinis ou même transfinis, automates avec sortie, etc. En ce qui concerne les applications, l'équipe travaille sur des problèmes issus de la vérification des systèmes, de la modélisation des systèmes concurrents, sur les applications des automates à l'arithmétique des ordinateurs, sur des algorithmes spécialisés pour la reconnaissance automatique dans les séquences génétiques.

### Combinatoire

Les axes principaux de l'équipe Combinatoire du LIAFA sont la combinatoire énumérative, la combinatoire bijective et la combinatoire analytique.

En particulier, l'équipe possède une expertise sur les q-séries, les fonctions Mock-Théta, la génération aléatoire et exhaustive. Ses membres s'intéressent aux structures combinatoires issues de problèmes informatique, mathématique et/ou physique. L'équipe s'est spécialisée sur les objets tels que les partitions d'entiers, les permutations, les arbres, les cartes, les graphes et les polyominos. Sur ces thèmes, l'approche énumérative est privilégiée tout en sachant que les membres de l'équipe ont des interactions avec la théorie des nombres et la probabilité.

### Modélisation et vérification

Les activités de l'équipe Modélisation et vérification portent sur le développement d'approches algorithmiques pour la vérification de systèmes, des fondements théoriques aux outils de vérification innovants.

Les applications visées sont dans un spectre large comprenant les algorithmes distribués, les réseaux dynamiques de processus communicants, les systèmes temps-réel, les systèmes embarqués critiques, les programmes avec structures de données complexes, les programmes concurrents, etc.

Les approches adoptées sont généralement basées sur l'utilisation (1) de modèles formels pour la description à un certain niveau d'abstraction des comportements des systèmes étudiés, (2) de spécifications formelles pour la description des propriétés que doivent satisfaire ces systèmes, et (3) de méthodes algorithmiques soit pour établir la correction, soit pour détecter des comportements illicites, d'un système par rapport à sa spécification.

Les modèles et les formalismes de spécification sont de manière générale de type automate (finis, à piles/files, à horloges/compteurs, etc.) ou logique (temporelle, monadique de premier/second ordre, point fixe, etc.), et les problèmes de la vérification sont souvent ramenés à des problèmes de décision sur ces formalismes (accessibilité/langage vide pour les automates, satisfaisabilité pour les logiques, stratégies gagnantes pour les jeux, etc). Se pose alors la question de la décidabilité et de la complexité de ces problèmes, et celle de développer des techniques basées sur le calcul de (sur/sous) approximations raffinables pour résoudre ces problèmes de manière efficace.

L'équipe a des compétences dans les domaines de la vérification de systèmes infinis, systèmes temporisés et hybrides, logiques temporelles, jeux et model-checking, model-checking quantitatif, vérification de programmes.

### Preuves, Programmes et Systèmes

L'équipe Preuves, Programmes et Systèmes fédère les énergies de chercheurs, enseignants-chercheurs et doctorants issus de cultures différentes (informatique et mathématiques) pour travailler sur les thématiques des langages de programmation et des systèmes distribués, et de leurs fondements logiques et mathématiques. Dans cette perspective, l'équipe développe la théorie des systèmes de typage, des machines abstraites et des programmes concurrents et s'intéresse à la logique des programmes, à la sémantique des effets et des ressources dans les langages de programmation, etc. L'équipe élabore aussi des méthodes et des outils de modélisation des systèmes dans le domaine du logiciel libre. PPS est un acteur essentiel dans le domaine du développement des assistants à la preuve. Le projet de recherche est fondé sur la conviction que la logique (et plus particulièrement la théorie de la démonstration), mais aussi la théorie des catégories, et d'autres théories mathématiques comme l'homologie ou l'homotopie, ou les probabilités, ont un rôle essentiel à jouer pour élucider le sens des programmes, afin de les rendre plus sûrs, et qu'inversement l'informatique, comme la physique a pu l'être et continue de l'être, peut être une source dans laquelle la logique et d'autres domaines des mathématiques peuvent puiser pour se renouveler. L'équipe PPS comporte une équipe projet commune (EPC) de l'Inria,  $\pi^2$  et à un rôle moteur dans l'initiative de Recherche sur l'Informatique du Logiciel Libre, structure d'accueil commune à l'Inria, l'Université Paris Diderot et l'UPMC.

