2019-01489 - PhD Position F/M (BN19) Enumerating integral orbits of prehomogeneous representations

Type de contrat : CDD de la fonction publique
Niveau de diplôme exigé : Bac + 5 ou équivalent
Fonction : Doctorant

A propos du centre ou de la direction fonctionnelle

Team presentation

The LFANT team researches algorithms in number theory and arithmetic geometry. We cover all aspects from complexity theory over optimised implementations up to cryptologic applications.

Research themes

The LFANT team has the goal of making an inventory of the major number theoretic algorithms, with an emphasis on algebraic number theory and arithmetic geometry, and of carrying out complexity analyses. So far, most of these algorithms have been designed and tested over number fields of small degree and scale badly. A complexity analysis should naturally lead to improvements by identifying bottlenecks, systematically redesigning and incorporating modern asymptotically fast methods.

Reliability of the developed algorithms is a second long term goal of our team. Short of proving the Riemann hypothesis, this could be achieved through the design of specialised, slower algorithms not relying on any unproven assumptions. We would prefer, however, to augment the fastest unproven algorithms with the creation of independently verifiable certificates. Ideally, it should not take longer to check the certificate than to generate it.

All theoretical results are complemented by concrete reference implementations in Pari/Gp, which allow to determine and tune the thresholds where the asymptotic complexity kicks in and help to evaluate practical performances on problem instances provided by the research community. Another important source for algorithmic problems treated by the LFANT team is modern cryptology.

Indeed, the security of all practically relevant public key cryptosystems relies on the difficulty of some number theoretic problem; on the other hand, implementing the systems and finding secure parameters require efficient number theoretic algorithms.

Contexte et atouts du poste

Scientific Research context:

Manjul Bhargava [6, 7, 8, 10] has constructed very explicit parametrizations for rings of low rank with some additional algebraic structures. Although it is not yet fully understood why this happens, these arise naturally as integral orbits of prehomogeneous representations of algebraic groups. It is foreseen in [5] that these parametrizations should give rise to efficient algorithms to enumerate those integral orbits by increasing discriminant. A major application would be to enumerate quartic or quintic fields of type S_4 or S_5 respectively, of discriminant up to X. If possible in almost linear time in the output size, which Bhargava [9, 11] proved to be of the order of X.

More generally, Bhargava’s constructions have found an amazing number of applications when estimating average densities of algebraic structures ordered by “discriminant”. For instance the average size of Selmer groups, which allows to prove that a positive proportion of elliptic curves over Q have rank 1, or that (at least) about 2/3 of all elliptic curves over Q satisfy the Birch and Swinerton-Dyer conjecture.

Bhargava received the Fields medal in 2014 for these achievements [12].

Keywords:

Bhargava bijections, Computational number theory

Bibliography:

Mission confiée

The subject of the thesis is to realize Bhargava’s prediction that his bijections actually give rise to optimal algorithms, with complexity linear in the output size, to enumerate structures of bounded discriminant.

More precisely, to specify, implement and optimize explicit algorithms for some of the open cases in Bhargava’s list and prove they indeed run in essentially linear time. The parametrizations associated to quadratic and cubic rings are classical by now, see e.g., [1, 2]. The case of quartic rings (or fields) of bounded discriminant is of particular interest: the parameter space has dimension 12 and it is not at all obvious how to enumerate in \(O(X)\) linear time the integer points in Bhargava’s fundamental domain, even though its Euclidean volume is \(O(X)\). For instance partially fixing a number of coordinates within allowed bounds will not always give rise to a “full” integer point, and one must prove that we do not lose too much time partially enumerating those points. In fact, for the particular case of quartic fields of discriminant bounded by \(X\), Hunter’s method yields a simple algorithm with complexity \(O(X^{(3/2)})\); any algorithm in \(o(X^{(3/2)})\) will already be interesting, even if we do not reach the expected \(O(X)\).

As new insight is gained about these situations, interesting side projects about suitable asymptotic enumeration should become tractable, for instance the density of quartic fields with Galois closure \(A_4\) is unknown but expected to be of the order of \(X^{(1/2)}}^{10\log(X)}\) by Malle’s conjecture [14]; any improvement on the known \(O(X^{(5/6)}}^{+\varepsilon})\) estimate would be worthwhile. The density of non-quartic fields with Galois closure \(S_4\), for instance normal fields of degree 15 years ago the density of quartic fields with normal closure \(S_4\). (See [13, 4] for the analogous but simpler statement for sextic \(S_3\)-fields vs. cubic \(S_3\)-fields.)

Principales activités

Main activities:
- Design quasi-optimal algorithms for Number Theory
- Develop efficient code for PARI/GP and/or SageMath

Compétences

Masters in mathematics, with an emphasis on number theory, and a strong interest for effective computation and algorithmic issues; or Masters in computer science with strong background in computational number theory.

More precisely, the subject requires a good understanding of basic algebraic number theory (working knowledge of class field theory), a working knowledge of analytic number theory (as required by algorithm analysis and average estimates of arithmetic functions) and the ability to program within standard number theoretic frameworks, e.g., SageMath and PARI/GP.

A working knowledge of basic algebraic geometry will also be useful: algebraic curves, elliptic curves.

The ability to program in C or C++ and a working knowledge of parallel computation techniques (e.g., POSIX threads or MPI) will also be appreciated.

Avantages

- Subsidized meals
- Partial reimbursement of public transport costs
- Possibility of teleworking (after 6 months of employment) and flexible organization of working hours
- Professional equipment available (videocabling, loan of computer equipment, etc.)
- Social, cultural and sports events and activities
- Access to vocational training
- Social security coverage

Rémunération

1982€ / month (before tax) during the first 2 years, 2085€ / month (before tax) during the third year.

Informations générales

- **Thème/Domaine** : Algorithmique, calcul formel et cryptologie
- **Ville** : Talence
- **Centre Inria** : CRI Bordeaux - Sud-Ouest
- **Date de prise de fonction souhaitée** : 2019-09-02
- **Durée de contrat** : 3 ans
- **Date limite pour postuler** : 2019-04-14

Contacts

- **Equipe Inria** : LFANT
- **Directeur de thèse** :
  Belabas Karim / karim.belabas@inria.fr
A propos d’Inria

Inria, l’institut national de recherche dédié aux sciences du numérique, promeut l’excellence scientifique et le transfert pour avoir le plus grand impact. Il emploie 2400 personnes. Ses 200 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3000 scientifiques pour relever les défis des sciences informatiques et mathématiques, souvent à l’interface d’autres disciplines. Inria travaille avec de nombreuses entreprises et a accompagné la création de plus de 160 start-up. L’institut s’efforce ainsi de répondre aux enjeux de la transformation numérique de la science, de la société et de l’économie.

Consignes pour postuler

Thank you to send :

- CV
- Cover letter
- Master marks and ranking
- Support letter(s)

Sécurité défense :

Ce poste est susceptible d’être affecté dans une zone à régime restrictif (ZRR), telle que définie dans le décret n°2011-1425 relatif à la protection du potentiel scientifique et technique de la nation (PPST). L’autorisation d’accès à une zone est délivrée par le chef d’établissement, après avis ministériel favorable, tel que défini dans l’arrêté du 03 juillet 2012, relatif à la PPST. Un avis ministériel défavorable pour un poste affecté dans une ZRR aurait pour conséquence l’annulation du recrutement.

Politique de recrutement :

Dans le cadre de sa politique diversité, tous les postes Inria sont accessibles aux personnes en situation de handicap.

Attention: Les candidatures doivent être déposées en ligne sur le site Inria. Le traitement des candidatures adressées par d'autres canaux n'est pas garanti.