

Sujet de thèse - PhD Subject

Frédérique Bassino (LIPN, Paris 13)
Frederique.Bassino@lipn.univ-paris13.fr

Pascal Weil (LaBRI)
pascal.weil@labri.fr

Génération aléatoire et propriétés génériques des sous-groupes du groupe libre

Mots-clés : génération aléatoire, groupes libres

Le développement de la théorie algorithmique des groupes infinis (groupes libres, groupes finiment présentés) a conduit naturellement à l'analyse de la complexité (pire des cas, en moyenne, générique) de ces algorithmes. Parallèlement, l'étude statistique des propriétés des éléments et des sous-groupes des groupes infinis s'est développée, et des algorithmes de génération aléatoire ont été proposés. Une partie des résultats obtenus est utilisée pour le développement de nouveaux systèmes cryptographiques, utilisant des groupes non commutatifs infinis.

Dans ce cadre, on dispose de deux approches fort différentes de la distribution des sous-groupes finiment engendrés du groupe libre, qui mettent en lumière des propriétés très distinctes des sous-groupes : l'une utilise la représentation des sous-groupes par des graphes finis (graphes de Stallings), et l'autre est basée sur la génération uniforme d'un k -uplet de mots indépendants qui engendrent le sous- groupe (k fixé). Ce ne sont pas les seules distributions "naturelles" et l'objectif de la thèse proposée est d'explorer une autre famille de distributions : pour engendrer un mot de longueur au plus n , on commence par choisir la longueur de ce mot selon une distribution μ préalablement fixée, puis on choisit uniformément un mot de cette longueur; on répète cette opération k fois pour engendrer un k -uplet. La richesse de cette méthode réside dans la flexibilité qu'offre le choix de la distribution μ , qui peut être choisie selon une loi de Poisson, de Bernoulli, de Gauss, etc. On s'attachera à calculer l'espérance de certains invariants des sous-groupes engendrés comme le rang, ou la fréquence (généricité, négligibilité) de certaines propriétés (indice fini, mal-normalité, etc) en fonction de μ . On pourra aussi voir le k -uplet engendré, non plus comme un ensemble de générateurs d'un sous-groupe, mais comme un ensemble de relateurs définissant un groupe finiment présenté et on étudiera alors la fréquence de certaines propriétés comme la petite cancellation.

L'étude pourra ensuite être étendue dans plusieurs directions. On pourra rechercher des problèmes génériquement difficiles (par exemple, NP-hard sur un ensemble générique d'instances); de tels problèmes peuvent être utilisés pour le développement de systèmes cryptographiques. On pourra aussi étudier l'extension de ces problématiques statistiques à l'étude des sous- groupes de groupes finiment présentés, et notamment des groupes hyperboliques ou des groupes partiellement commutatifs libres (right- angled Artin groups).

Cette étude, si elle met en jeu un peu de théorie des groupes et de probabilités, repose essentiellement sur des méthodes combinatoires (combinatoire des mots, combinatoire analytique en particulier).

Random generation and generic properties of subgroups of free groups

Keywords: random generation, free groups

The development of the algorithmic theory of infinite groups (free groups, finitely presented groups) led naturally to the analysis of the complexity (worst-case, average-case, generic) of these algorithms. At the same time, the study of the statistical properties of elements and subgroups of infinite groups also developed, and random generation algorithms were proposed. Part of the results obtained in this direction can be used to develop new cryptographic schemes, based on the properties of infinite non-commutative groups.

In this context, we have two very different approaches of the distribution of the finitely generated subgroups of a free group, which put the emphasis on very distinct properties of free groups. One uses the representation of subgroups by finite graphs (Stallings graphs), the other is based on the uniform generation of a k -tuple of independent words which generate the subgroup (k is fixed). These are not the only "natural" distributions, and the objective of the proposed thesis is to explore another family of distributions: to generate a word of length at most n , one first chooses the length of that word according to a distribution μ , fixed in advance, and one then chooses uniformly at random a word of that length; the operation is repeated k times to generate a k -tuple. The interest of this method lies in the flexibility afforded by the choice of the distribution μ , which can be chosen according to a Poisson, a Bernoulli, a Gaussian, etc, law. We will want to compute the expected value, in terms of μ , of certain invariants (e.g. the rank) of the subgroup generated, and the frequency (genericity, negligibility) of certain properties (e.g. finite index, malnormality, etc). We will also view the k -tuple generated as the set of relators in a finite presentation (and not anymore as the set of generators of a subgroup) and we will study the frequency of properties such as small cancellation.

This study can be extended in several directions. One can for instance try to identify generically difficult problems (eg NP-hard on a generic set of instances); such problems can be used to develop cryptographic systems. One can also study the extension of the statistical approach described above to the study of the subgroups of finitely presented groups, and in particular of hyperbolic groups and free partially commutative groups (right-angled Artin groups).

This research topic requires a modicum of group theory and of probabilities, but it relies mostly on combinatorial methods (combinatorics on words and analytic combinatorics in particular).

References

- [1] F. Bassino, A. Martino, C. Nicaud, E. Ventura, P. Weil. Statistical properties of subgroups of free groups, 28 pages, January 2010. submitted. Available at <http://www-lipn.univ-paris13.fr/~bassino/publications/rsa2010.pdf>
- [2] F. Bassino, C. Nicaud, P. Weil. Random generation of finitely generated subgroups of a free group, *International Journal of Algebra and Computation* 18 (2008) 1-31. Available at <http://www-lipn.univ-paris13.fr/~bassino/publications/BNW.pdf>
- [3] F. Bassino, A. Martino, C. Nicaud, E. Ventura, P. Weil. On distributions of subgroups of free groups, In *the SIAM Workshop on Analytic Algorithmics and Combinatorics (ANALCO'10)*. Austin, Texas. January 2010. pp. 82–89. 2010. Available at <http://www.siam.org/proceedings/analco/2010/analco10.php>.
- [4] A. Myasnikov, V. Shpilrain, A. Ushakov. Group-based cryptography, *Advanced Courses of the CRM Barcelona*, Birkhäuser 2008.