

École doctorale : École doctorale de mathématiques et informatique
de Bordeaux, ED-39

Unité de recherche : Institut de Mathématiques (IMB)
- Université Bordeaux 1 et CNRS, UMR 5251

Équipe : Théorie des nombres

Localisation : Institut de Mathématiques de Bordeaux

Directrice : Christine Bachoc

Courriel : `bachoc@math.u-bordeaux1.fr`

Sujet : Combinatorial optimization and coding theory

Description :

En théorie des codes correcteurs d'erreurs, on rencontre de nombreux problèmes d'optimisation. Typiquement, on cherche à estimer le cardinal maximal d'un ensemble de "mots" soumis à certaines contraintes, où les "mots" appartiennent à un certain espace métrique. Les espaces intervenant en théorie des codes se sont beaucoup diversifiés mais ont pour caractéristique commune de posséder un gros groupe d'isométries. Dans le cas classique des codes sur un alphabet q -aire de distance minimale fixée, on sait depuis les travaux de Philippe Delsarte dans les années 70 estimer leur cardinal par la valeur optimale d'un programme linéaire, et cette approche a été généralisée avec succès dans les années 80 au cas des espaces compacts 2-points homogènes.

Plus récemment, plusieurs travaux ont montré l'intérêt de méthodes de programmation mathématique plus générales, en particulier la programmation semidéfinie positive, pour soit améliorer des résultats antérieurs ([5], [6]) soit traiter des espaces et/ou des contraintes plus généraux ([1], [2], [3], [4]). L'exploitation des symétries de l'espace sous-jacent et en particulier les outils de l'analyse harmonique s'avèrent déterminants. Les résultats obtenus sont prometteurs mais sont encore loins de ceux issus de la méthode de program-

mation linéaire, en particulier en ce qui concerne l'analyse asymptotique des bornes obtenues.

Cette thèse contribuera à développer ces méthodes, par exemple relativement aux sujets suivants : le décodage en liste, les codes quantiques, ou encore les pseudo-distances de k mots. Elle se déroulera au sein du groupe de recherche *Codes, cryptographie et réseaux* de l'IMB, et bénéficiera de la collaboration que ce groupe développe avec des membres de l'équipe *Optimization* de l'Université TU Delft et de CWI Amsterdam. Elle pourra contribuer à développer des échanges avec le groupe *Recherche opérationnelle* de l'IMB.

Connaissances et compétences : Une connaissance préalable de l'un des domaines suivants : codes correcteurs d'erreurs, programmation mathématique, représentations linéaires des groupes finis est souhaitée.

Description :

In the theory of error correcting codes, many problems of optimization are encountered. Typically, one tries to estimate the maximal number of elements of a set of “words” subject to some constraints, where the “words” belong to some specific metric space. The metric spaces of interest in coding theory are more and more numerous but usually have a large group of symmetries. In the classical case of codes over a q -ary alphabet with given minimal Hamming distance, we know after Philippe Delsarte work in the seventies how to estimate their size from the optimal value of a linear program. This work was successfully generalized to the compact 2-point homogeneous spaces in the eighties.

More recently, several results have shown the relevants of more general methods in mathematical programming, in particular of semidefinite programming, in order to strengthen the older estimates ([5], [6]), or to treat new spaces or constraints ([1], [2], [3], [4]). Taking advantage of the symmetries of the underlying space and exploiting tools from harmonic analysis have shown to be crucial. The results obtained so fare with these ideas are very promising but are far from the level of achievements that the linear programming method has reached, especially in the asymptotic range.

This thesis will contribute to the development of these methods, for example in one of the following directions : applications to list decoding problems, quantum codes, or the study of pseudo-distances of k words. It will take place in the research group *Codes, cryptographie et réseaux* of IMB, and will

benefit of the collaboration that this group develops with members of the group *Optimization* in TU Delft and CWI Amsterdam. It will help develop interactions with the research group *Recherche opérationnelle* of IMB.

Preliminary knowledge : A preliminary knowledge of one of the following topics is expected from the candidates : error correcting codes, mathematical programming, group representations.

Références

- [1] C. Bachoc, *Linear programming bounds for codes in Grassmannian spaces*, IEEE Trans. Inf. Th. **52-5** (2006), 2111-2125.
- [2] C. Bachoc, F. Vallentin, *New upper bounds for kissing numbers from semidefinite programming*, J. Amer. Math. Soc. 21 (2008), 909-924.
- [3] C. Bachoc, F. Vallentin, *Semidefinite programming, multivariate orthogonal polynomials, and codes in spherical caps*, special issue in the honor of Eichii Bannai, European Journal of Combinatorics **30** (2009), 625-637.
- [4] A. Barg, P. Purkayastha, *Bounds on ordered codes and orthogonal arrays*, Moscow Math. Journal, no. 2 (2009)
- [5] A. Schrijver, *New code upper bounds from the Terwilliger algebra and semidefinite programming*, IEEE Trans. Inform. Theory **51** (2005), 2859–2866.
- [6] D.C. Gijswijt, A. Schrijver, H. Tanaka, *New upper bounds for nonbinary codes*, J. Combin. Theory Ser. A **13** (2006), 1717–1731.