Stage de M2
Exploration des codes à redondance optimale

Lieu : Université de Montpellier, Laboratoire LIRMM
Équipe d'accueil : équipe ECO (`http://www.lirmm.fr/eco/`)
Encadrants : Bruno Grenet (`Bruno.Grenet@lirmm.fr`)
Romain Lebreton (`Romain.Lebreton@lirmm.fr`)

Les codes correcteurs d'erreurs sont issus du domaine des télécommunications et sont indispensables pour garantir l'intégrité de données (stockage, calcul distribué). Ils sont aussi utilisés en théorie de la complexité ou dans le domaine de la cryptographie. Un défi dans ce domaine consiste à trouver le meilleur compromis entre le ratio R du code (ratio entre la taille des messages avant et après encodage) et la proportion d'erreurs qu'il peut corriger. La théorie de l'information permet de montrer que le décodage en temps polynomial est impossible dès que la proportion d'erreur dépasse $(1 - R)$.

Il a fallu attendre 2008 pour que la première construction de code approchant cette borne soit proposée [1], basée sur les codes de Reed-Solomon (qui consistent à évaluer un polynôme sur plus de points que son degré afin d'introduire de la redondance). Au lieu de considérer chaque évalué comme une lettre du mot de code, ces évalués sont regroupés en des m-uplets consécutifs qui sont vus comme des lettres sur un alphabet plus grand. Seules deux autres constructions de codes approchant la borne optimale ont été proposées depuis [2], basées sur l'évaluation non seulement du polynôme mais aussi de ces dérivées.

L'objectif du stage que nous proposons est d'explorer ces codes à redondance optimale pour mieux les comprendre, afin de pouvoir à terme proposer de l'algorithmique efficace pour les manipuler.

Contenu du stage Un but du stage serait d'étudier la possibilité de plonger les quelques constructions existantes de codes à redondance optimale dans un cadre général unificateur. En effet, les m-uplets d'évalués successifs dans les codes repliés présentent une similarité avec une notion de dérivation appelée q-dérivation. Exploiter cette similarité permettrait de définir un cadre général basé sur une notion abstraite de dérivation.

À plus long terme, l'objectif est d'arriver à améliorer les complexités des algorithmes de décodage pour ces codes, ainsi que fournir des implantations de ces algorithmes.

1. V. GURUSWAMI et A. RUDRA. « Explicit codes achieving list decoding capacity : Error-correction with optimal redundancy ». Dans : *Information Theory, IEEE Transactions on* 54.1 (2008), p. 135–150.

2. V. GURUSWAMI et C. WANG. « Linear-algebraic list decoding for variants of Reed–Solomon codes ». Dans : *Information Theory, IEEE Transactions on* 59.6 (2013), p. 3257–3268, S. KOPPARTY. « List-Decoding Multiplicity Codes ». Dans : *Theory of Computing* 11.5 (2015), p. 149–182. DOI : `10.4086/toc.2015.v011a005`.