Approximation polynomiale efficace en machine

Nicolas BRISEBARRE, Pascaline, CNRS-LIP, ENS Lyon - Lyon
Sylvain CHEVILLARD, Factas, Centre Inria Université Côte d'Azur - Sophia Antipolis
Guillaume HANROT, Cryptolab - Lyon
Tom HUBRECHT, Pascaline, ENS Lyon, LIP - Lyon
Serge TORRES, LIP, ENS Lyon - Lyon

Quand on implante des fonctions élémentaires en machine, on utilise presque toujours des approximations polynomiales. Dans la plupart des cas, le polynôme qui approche le mieux (pour une norme et un intervalle donnés) une fonction a des coefficients qui ne sont pas exactement représentables sur un nombre fini de bits, une contrainte pourtant incontournable pour pouvoir les utiliser en machine.
Nous présenterons une méthode heuristique utilisant l'algorithmique des réseaux euclidiens et notamment l'algorithme LLL qui permet de produire une très bonne (voire la meilleure) approximation polynomiale sous cette contrainte quand la norme considérée est la norme sup. Des techniques similaires fonctionnent pour la norme L^2.
[Travaux en collaboration avec Chevillard, Hanrot, Hubrecht et Torres]

Contact : `https://perso.ens-lyon.fr/nicolas.brisebarre/`