

Algorithmes détendus pour les bases d'ordre et leur impact aux méthodes de Wiedemann par blocs

Romain Lebreton

Les bases d'ordre sont un outil fondamental de l'algèbre linéaire à coefficients polynomiaux. Si l'algorithme de Wiedemann par blocs peut aujourd'hui traiter de grands problèmes d'algèbre linéaire creuse, c'est en bonne partie grâce à l'apport des algorithmes rapides de bases d'ordre.

Toutefois, les algorithmes actuels souffrent de deux défauts : ils ne sont pas conçus pour permettre de la terminaison anticipée et ils nécessitent de connaître plus de coefficients de l'entrée que strictement nécessaire.

Dans cet exposé, nous proposons un algorithme en-ligne pour les bases d'ordre qui permet à la fois la mise en place aisée de terminaison anticipée et de ne nécessiter qu'une connaissance minimale de l'entrée tout en gardant une complexité quasi-optimale. L'utilisation de notre algorithme au sein des méthodes de Wiedemann par blocs mène à une amélioration des performances d'un facteur constant. Travail en collaboration avec Pascal Giorgi.