Conversions simultanées entre représentation classique et modulaire à l'aide d'algèbre linéaire

Javad Doliskani Pascal Giorgi Romain Lebreton
Éric Schost

Le système modulaire de représentation des entiers est très utilisé, notamment de par sa capacité à réduire des calculs sur de grandes valeurs à des calculs menés en parallèle sur des nombres de taille choisie. Nous présentons un nouvel algorithme de conversion de représentation d'entiers entre le système positionnel classique et le système modulaire. Cet algorithme ramène le gros des calculs de conversion à de l'algèbre linéaire sur des mots machines.

Notre algorithme est naturellement conçu pour convertir simultanément un certain nombre d'entiers. Dans ce cas, sa complexité théorique améliore celle des méthodes naïves sans toutefois atteindre la quasi-linéarité des algorithmes rapides. Mais c'est en pratique que notre algorithme tire le mieux son épingle du jeu : parce qu'il bénéficie des implémentations optimisées d'algèbre linéaire, notre programme fournit le meilleur temps de calcul des algorithmes de conversions pour une large plage intermédiaire de taille de matrice et d'entiers.

La principale application de notre algorithme est la multiplication de matrices à coefficients entiers. Nos expériences montrent des améliorations de temps de calculs pour une large plage intermédiaire de taille de matrice et d'entiers.