Bases de Gröbner d'idéaux invariants sous un groupe abélien fini dans le cas non-modulaire.

Jean-Charles Faugère, Jules Svartz
Équipe Polsys – INRIA Paris-Rocquencourt/UPMC/LIP 6

La résolution de systèmes polynomiaux présentant des symétries est un problème naturel qui apparaît dans plusieurs contextes provenant d'applications (cryptographie, robotique, biologie, physique, codes correcteurs d'erreurs...) Malheureusement, la résolution de ces systèmes avec les algorithmes usuels de calcul de bases de Gröbner ne tient pas compte de ces symétries. Lorsque toutes les équations du système polynomial sont individuellement invariantes sous l'action d'un groupe, plusieurs approches peuvent-être envisagées pour tenir compte de cette action et accélérer le processus de résolution (théorie des invariants, bases de Gröbner SAGBI). Ces approches ont en commun de travailler dans l'algèbre $\mathbb{K}[x_1,\dots,x_n]^G$ des polynômes de $\mathbb{K}[x_1,\dots,x_n]$ invariants sous l'action du groupe. Dans le cas général d'un système polynomial présentant des symétries, le cadre algébrique sous-jacent étant celui d'un ideal I globalement invariant sous l'action d'un groupe, ces approches ne peuvent être utilisées.

Dans cet exposé, nous proposons des variantes des algorithmes usuels de calcul de bases de Gröbner (F_4, F_5, FGLM) dans le cas où l'idéal I est globalement invariant sous l'action d'un groupe fini G supposé *abélien*. Sous l'hypothèse de non-modularité (la caractéristique du corps $\mathbb{K}$ ne divise pas le cardinal du groupe G), le problème se ramène à celui du calcul de base de Gröbner d'un ideal $I_{\mathscr{D}}$ globalement invariant sous l'action d'un groupe $G_{\mathscr{D}}$ constitué de matrices diagonales (nous dirons que l'idéal est $G_{\mathscr{D}}$-stable). Cette action permet d'introduire une graduation sur l'algèbre $\mathbb{K}[x_1,\dots,x_n]$ indexée sur le groupe $G_{\mathscr{D}}$ et dont chacune des composantes est engendrée par des monômes. Nous introduisons ensuite le concept de $G_{\mathscr{D}}$-degré et de polynôme $G_{\mathscr{D}}$-homogène et montrons que les notions d'idéal $G_{\mathscr{D}}$-stable et d'idéal $G_{\mathscr{D}}$-homogène coïncident.

Une fois observé que la propriété de $G_{\mathscr{D}}$-homogénéité est préservée par le calcul de S-polynômes et de formes normales, il est facile de montrer que les matrices intervenant dans les versions matricielles des algorithmes usuels de calcul de bases de Gröbner peuvent-être partitionnées en sous-matrices de taille divisée par un facteur approximativement $|G_{\mathscr{D}}|$. De plus, les matrices intervenant dans l'algorithme F_5 peuvent être construites en parallèle, nous en déduisons donc un gain théorique d'un facteur $|G|^{\omega}$ dans l'algorithme F_5 et $|G|^2$ dans l'algorithme FGLM.

L'analyse de complexité passe par une étude assymptotique de la série de Hilbert associée à l'algèbre des invariants sous un groupe diagonal, et nous verrons qu'avec cette approche, certains problèmes deviennent résolubles en temps polynomial en la taille de l'entrée. D'une manière générale, cette approche permet de résoudre certains problèmes provenant d'applications jusque là inatteignables.