Introduction

Un certain nombre de méthodes algorithmiques pour la résolution formelle d'équations algébriques sont devenues classiques et appartiennent au patrimoine de base du Calcul Formel. Parmi celles-ci, les algorithmes de bases standard et la méthode de Wu Wen-Tsün, occupent une place privilégiée. L'application de ces méthodes au cas des systèmes d'équations différentielles ordinaires ou aux dérivées partielles est beaucoup plus récente, bien que la méthode de Wu ne soit qu'un cas particulier de la théorie développée par Ritt en algèbre différentielle.

Les problèmes de complexité liés à ces algorithmes se présentent sous deux aspects différents : d'une part évaluer la complexité intrinsèque d'un problème dans le pire des cas, d'autre part isoler un certain nombre de cas particuliers non triviaux pour lesquels la complexité est acceptable. De telles études concourent soit au développement d'algorithmes plus performants, soit à un meilleur emploi des algorithmes existants, en se restreignant aux cas où ils peuvent se montrer efficaces.

La preuve de bornes de complexité requiert un appareillage théorique fin, et fournit en retour un éclairage nouveau sur la structure algébrique des objets calculés. En effet, l'expérience acquise montre une corrélation nette entre une bonne complexité et des propriétés algébriques simples.

Cette thèse tente, modestement, de se placer dans cette problématique, en proposant une étude transversale d'un problème ayant des applications pratiques, principalement en modélisation, sous le nom de *problème de l'identifiabilité structurelle globale*. D'un point de vue algébrique, il s'agit de tester si une fraction rationnelle appartient à un sous-corps du corps des fractions en n variables. On s'intéressera particulièrement au problème de tester si $k(f_1, \ldots, f_m) = k(x_1, \ldots, x_n)$. Un problème similaire est de tester si un polynôme appartient à une sous-algèbre de type fini de $k[x_1, \ldots, x_n]$.

Dans les deux cas, on pourra ramener le problème de multiples manières à la résolution d'un, ou de plusieurs systèmes d'équations algébriques, qui seront résolus soit par les algorithmes de base standard, soit par la méthode Wu–Ritt. Dans le cas polynomial, on dispose en outre d'une méthode intrinsèque, utilisant les algorithmes de bases canoniques, récemment introduits par Kapur et Madlener, et indépendamment par Robbiano et Sweedler.

Le problème de l'identifiabilité se résume de la manière suivante. On modélise un processus par une structure, décrite par un système d'équations différentielles, dépendant de fonctions de commande décrivant l'action de l'expérimentateur et d'un certain nombre de paramètres internes, qui sont des constantes physiques a priori inconnues. Des mesures, dépendant continûment de l'état du système sont effectuées. On les décrit de manière abstraite par des fonctions des variables d'état. Le problème est alors de savoir si, à partir d'une série d'expériences en nombre arbitrairement grand, on pourra déterminer de manière univoque les paramètres internes, sous l'hypothèse que ceux-ci sont génériques. En d'autres termes, il s'agit de vérifier que l'application qui associe à un n-uplet de paramètres le comportement entrée-sortie du système est injective sur un ouvert dense.

Un premier problème est de manipuler le comportement entrée-sortie. Des techniques classiques permettent de lui substituer une application polynomiale f équivalente, appelée résumé exhaustif. On teste alors que $k(f_1, \ldots, f_n) = k(x_1, \ldots, x_n)$, ce qui ramène au problème algébrique décrit ci-dessus. Nos travaux dans ce domaine se sont très largement inspirés des résultats antérieurs obtenus par LECOURTIER, RAKSANYI et WALTER au Laboratoire des Signaux et Systèmes à Supélec.

On introduira une mise en œuvre plus fine des techniques de résolution algébrique, qui permet un gain d'efficacité notable. Surtout, on étendra le calcul d'un résumé exhaustif à des structures non linéaires quelconques, sous quelques réserves de généricité, en employant les techniques d'algèbre différentielle, qui sont actuellement d'un emploi croissant en automatique, par exemple dans les travaux de Michel FLIESS.

Ce mémoire se compose de trois parties distinctes, d'un volume inégal, qui marquent les étapes conceptuelles de ce travail. La première donne des résultats théoriques préliminaires, regroupés en deux chapitres. Le premier est une introduction à l'algèbre différentielle, qui m'a paru indispensable pour fixer les notations et énoncer les propriétés de base utiles pour la suite. Le second traite des applications rationnelles et polynomiales, tant dans le cas algébrique que dans le cas différentiel. On y a réuni un certain nombre de résultats d'algèbre, difficiles, et qui auront leur importance pour l'algorithmique et l'étude de complexité.

Citons un théorème, prouvé par GABBER qui permet de majorer le degré de l'inverse d'un application birationnelle $f : \mathbf{A}^n \mapsto \mathbf{A}^n$ par $(\deg f)^{n-1}$. On donnera une version différente, qui se montre plus fine dans certains cas, et surtout un analogue dans le cas différentiel, permettant de borner l'ordre def^{-1} par $n \operatorname{ord} f$.

Le dernier paragraphe décrit des techniques permettant de ramener l'étude d'un sous-corps de $k(x_1, \ldots, x_n)$ ou d'une sous-algèbre à celle d'un idéal associé. La première utilise le graphe de l'application rationnelle associée à un ensemble de générateurs. Il s'agit donc d'une technique très classique et qui a déjà été beaucoup utilisée pour des applications effectives par VAN DEN ESSEN, SHANNON et SWEEDLER, etc. Une technique différente, moins connue, utilise une "section générique" du graphe. Elle apparaît chez RITT au cours de la démonstration d'un analogue différentiel du théorème de Lüroth. Les méthodes de LECOURTIER et RAKSANYI en sont assez proches, et je n'ai eu qu'à en préciser la signification géométrique.

La seconde partie traite des méthodes algorithmiques. Elles concernent principalement les méthodes de résolution de systèmes algébriques ou algébriques différentiels, qui permettent de mettre en action les traductions en termes d'idéaux décrites au chapitre II.

Le troisième chapitre débute par la description d'un "cadre général" pour les bases standard, mettant en relief les liens conceptuels qui unissent bases standard d'idéaux, bases canoniques et bases standard d'idéaux différentiels. Ce formalisme tient compte du fait que les bases standard généralisées à d'autres structures sont en général infinies (bases canoniques de sous-algèbres) et que l'ensemble des syzygies peut être lui-même infini (bases standard d'idéaux différentiels). On donne ensuite des algorithmes de résolution utilisant les bases standard classiques, rappelant la méthode du graphe et décrivant la méthode de section générique. On donne des bornes de complexité, simplement exponentielles, reposant soit sur le théorème de Gabber, soit sur le nullstellensatz effectif.

Le dernier paragraphe décrit les bases canoniques de sous-algèbres qui apparaissent clairement comme une généralisation des bases standard. On s'attachera surtout aux problèmes de finitude, conjecturant que la base canonique d'une sous-algèbre intégralement close et de type fini est finie, et aux applications aux automorphismes de $k[x_1, \ldots, x_n]$. On dispose dans ce cas d'une borne du même ordre, et même meilleure, ce que confirme l'expérience, qu'avec les méthodes utilisant un idéal associé.

Quelques relations entre bases canoniques et bases standard sont également présentées, comme une généralisation des bases standard aux idéaux d'une sous-algèbre, apparaissant comme un cas particulier d'une généralisation précédente de Sweedler et une méthode effective pour obtenir un système de générateurs de l'idéal des relations entre les éléments d'un base canonique, qui est une base standard pour un ordre bien choisi.

Le quatrième chapitre aborde les méthodes de résolution dans le cadre différentiel, commençant par une généralisation des bases standard, reprenant une notion précédemment introduite par Giuseppa Carra' Ferro. Précisons qu'elle est distincte de la théorie des bases standard de $\mathcal{D}$-modules. On y donne une procédure qui converge vers la base standard, sans qu'on soit sûr de pouvoir l'atteindre puisqu'elle est en général infinie. Dans quelques cas particuliers on peut néanmoins l'employer avec certitude, par exemple pour des idéaux isobares, où l'on retrouve les propriétés des bases standard d'idéaux homogènes. Dans le cas général, il faut disposer de bornes sur l'ordre de dérivation.

L'analogue différentiel du théorème de Gabber nous en fournit une, qui débouche sur une méthode algorithmique.

On décrit ensuite un algorithme de construction d'ensembles caractéristiques. Il faut noter qu'en général on ne sait pas construire l'ensemble caractéristique d'un idéal, fût-il premier, mais seulement un système d'ensembles caractéristiques dont certains — on ignore lesquels — définissent les composantes irréductibles de l'idéal. Cela suppose en outre de pouvoir factoriser des polynômes après plusieurs extensions algébriques du corps de base. Ne considérant que des idéaux premiers, j'ai pu remédier à cet inconvénient par une méthode qui suppose qu'on sait déjà tester l'appartenance à l'idéal, et nécessitant uniquement des décompositions sans facteur multiple.

Si l'on connaît déjà un ensemble caractéristique de l'idéal premier $\mathcal{I}$, le test d'appartenance nécessaire s'en déduit aisément et l'on peut alors tester qu'une application rationnelle $f : V(\mathcal{I}) \mapsto \mathbf{A}^m$ admet un inverse à gauche rationnel. Dans la mesure où les idéaux différentiels ne sont pas tous de type fini, et qu'il faut bien les définir par quelque chose, ce n'est pas une trop grande limitation que de le faire par un ensemble caractéristique, dont la connaissance est en général nécessaire, pour s'assurer au préalable que l'idéal est premier.

La dernière partie ne comporte, elle, qu'un chapitre décrivant les applications. Il commence par un rappel de quelques notions fondamentales et des résultats de LECOURTIER, RAKSANYI et WALTER. On donne ensuite une méthode originale pour le calcul des résumés exhaustifs dans le cas non-linéaire et des exemples d'applications. Cette méthode utilise l'élimination préalable des variables d'état, par un calcul d'ensemble caractéristique. N'ayant pas encore achevé l'implantation de cet algorithme, on ne pourra donner que des exemples susceptibles d'être calculés à la main, à titre d'illustration.

Par des méthodes reposant sur des techniques classiques de calculs de résumés exhaustifs, on donne un exemple résolu en 4 min. par Scratchpad II sur IBM 4381, alors que le programme de Raksanyi échoue par saturation de la mémoire après près d'une journée de calcul. Ce gain de temps ne peut s'expliquer uniquement par la puissance de l'ordinateur. Le calcul des bases standard est lent en Scratchpad II qui ne dispose en outre, dans cette configuration, que de 4M de mémoire disponible pour les calculs.

On trouvera en appendice le code Scratchpad II permettant de traiter les structures linéaires stationnaires, ainsi qu'une implantation d'un algorithme de construction de bases canoniques.