Sur le calcul des solutions d'un système linéaire Diophantien

Sylvain Lombardy

On se propose de présenter certains algorithmes permettant la résolutions des systèmes linéraires diophantiens. Les solutions de tels systèmes étant des ensembles rationnels non ambigus, on étudiera des algorithmes donnant les solutions, d'une part sous la forme de solutions minimales, d'autre part sous la forme d'expresions rationnelles non ambiguës, et on comparera la taille du résultat.

1 Les solutions d'un système linéaire sont rationnelles

Si $\mathbb{N}^d$ est muni de l'ordre produit, tout ensemble d'éléments de $\mathbb{N}^d$ deux à deux incomparables est fini. Les solutions d'un système $A.x = C$ est un ensemble $F + G^*$, où F est l'ensemble des solutions minimales et G l'ensemble des solutions non nulles minimales du système homogène associé. Ces ensembles sont finis car composés d'éléments incomparables.

Tout ensemble rationnel de $\mathbb{N}^d$ est non ambigu [4], c'est-à-dire union disjointe finie d'ensembles $F_i \oplus G_i^*$, où G_i^* est librement engendré.

2 Bornes sur les solutions minimales

On peut borner la taille des solutions d'un système linéaire homogène [5]; si x est une solution minimale de $A.x = 0$,

$$\|x\|_1 \leq \mathcal{B} = (1 + \max_{1 \leq i \leq k} \sum_{1 \leq j \leq d} |a_{ij}|)^k .$$

Ainsi, pour résoudre un tel système, un premier algorithme consiste à explorer l'ensemble borné par $\mathcal{B}$.

D'autre part, on peut ramener la résolution d'un système quelconque à celle d'un système linéaire.

3 Recherche des solutions minimales

La plupart des algorithmes sont axés sur la recherche des solutions minimales de $A.x = 0$:

L'**algorithme du gradient** [2] est une exploration de $\mathbb{N}^d$ à partir des vecteurs de la base canonique $(e_i)_{i \in [1,d]}$. Le principe est de n'incrémenter la *ième* coordonnée que si $(Ax).(Ae_i) < 0$.

L'**algorithme "Lexicographique"**[5] utilise les bases de Gröbner d'une famille de polynôme issue de A. On obtient ainsi un système de réécriture appliqué à la solution nulle.

L'**algorithme algébrique** [3] est basé sur le calcul de mineurs de A. Contrairement aux précédents, il n'est pas fondé sur la recherche à l'intérieur d'un ensemble borné.

4 L'algorithme de décomposition

Cet algorithme basé sur des décompositions successives de $\mathbb{N}^d$ permet d'obtenir la solution d'un système linéaire sous forme d'une expression non ambiguë.

Il est inspiré de la preuve de la non ambiguïté des ensembles rationnels de $\mathbb{N}^d$ [4].

Une solution $y \neq 0$ de $A.x = 0$ induit une partition de l'ensemble E_y des points non supérieurs à y en sous-ensembles de dimension $d - 1$. Ainsi, par récurrence, si S_y est une expression non ambiguë des solutions incluses dans E_y, $S_y \oplus y^*$ est une expression non ambiguë.

S'il n'y a pas de solution non nulle à $A.x = 0$, on montre que le nombre de solutions du système est fini.

Pour disposer d'un algorithme, il faut être capable de trouver une solution d'un système homogène ainsi que l'ensemble des solutions minimales d'un système. Pour cela, on peut utiliser les algorithmes précédents ou résoudre les équations les unes après les autres, ce que permet la forme particulière des expressions obtenues.

Cette dernière méthode est en fait un autre point de vue de l'algorithme donnant des solutions "paramétriques" non ambiguës [1].

Remarque

Ces algorithmes s'étendent à la résolution de systèmes comportant des inéquations. Dans ce cas, pour obtenir des solutions non ambiguës, il semble que la seule solution soit de résoudre les inéquations les unes après les autres.

4.1 Comparaisons

$A.x = 0$	Algorithme du gradient	Solutions minimales	Algorithme par décomposition	Solutions particulières
$\begin{pmatrix} 0 & 0 & 0 & 0 & -2 & 1 & 1 \\ 6 & -1 & -5 & 0 & 0 & 0 & 0 \\ -6 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$	$4,27s$	95	$0,43s$	768
$\begin{pmatrix} -5 & -2 & 1 & -1 & 1 \\ 9 & 62 & -5 & -3 & 101 \\ 56 & -34 & -11 & 67 & 98 \end{pmatrix}$	$1067,97s$	7	$352,56s$	66635
$(13, 17, 23, -19, -11, -15)x = 7$	$2,71s$	$(89, 182)$	$1053,57s$	602861

La taille des solutions est donnée, pour une description ambiguë, par l'ensemble des solutions minimales (engendrant le réseau des solutions), et pour une description non ambiguë par le nombre de solutions particulières obtenues (le nombre de générateurs de chaque réseau étant inférieur à $d - k$, où d est le nombre d'inconnues et k le nombre d'équations indépendantes.

On voit que les performances de l'algorithme non ambigu sont limitées. La taille de sa sortie devient rapidement très importante devant celle d'un algorithme classique, lorsque les coefficients ou le nombre d'équations croissent.

Références

[1] H. Abdulrab and M. Maksimenko, General solution of systems of linear diophantine equations and inequations, 6th Int. Conf on Rewriting Techn. and Appl., Lect. Notes in Comp. Science, Vol.914 (1995), 339-351.

[2] E. Contejean and H. Devie, An efficient incremental algorithm for solving systems of diophantine equations, *Information and Computation*, Vol.113 (1994).

[3] E. Domenjoud, Solving systems of linear diophantine equations: an algebraic approch, *Proc. 16th Math. Foundations of Comp. Science*, Lect. Notes in Comp. Science, Vol.520 (1991), 141-150.

[4] S. Eilenberg and M.P. Schützenberger, Rational sets in commutative monoids, *Journal of Algebra*, Vol.13,No 2 (1969), 173-191.

[5] L. Pottier, Minimal solutions of linear diophantine systems: bounds and algorithms,*Proc. of the Int. Congress on Rewriting tech. and appl.*, Lect. Notes in Comp. Science, Vol.488 (1989), 162-173.