

MASTER 1- CRYPTIS
Projet d'Initiation à la Recherche

Soit K un corps commutatif, $K[X]$ l'algèbre des polynômes à coefficients dans K et $K[[X]]$ l'algèbre des séries formelles à coefficients dans K .

Suites polynomialement récurrentes

Soit $u = (u_n)$ une suite d'éléments de K . On dit que u est une suite P -récurrente s'il existe $h \in \mathbb{N}^*$ et des polynômes P_0, \dots, P_h dans $K[X]$ tels que

$$\forall n \in \mathbb{N}, \quad P_h(n)u_{n+h} + P_{h-1}(n)u_{n+h-1} + \dots + P_0(n)u_n = 0.$$

On désigne par $\mathcal{J}(K)$ l'ensemble de ces suites.

Séries différentiellement finies

Soit $f(X)$ un élément de $K[[X]]$. On désigne, pour $n \in \mathbb{N}$, par $f^{(n)}(X)$ la dérivée formelle n -ième de f . On dit que f est D -finie (différentiellement finie) ou D -finie s'il existe $h \in \mathbb{N}^*$ et des polynômes P_0, \dots, P_h dans $K[X]$ tels que

$$P_h(X)f^{(h)}(X) + P_{h-1}(X)f^{(h-1)}(X) + \dots + P_0(X)f^{(0)}(X) = 0.$$

On désigne par $\mathcal{D}(K)$, l'ensemble de telles séries.

Travail à faire

L'objet de ce mémoire est de se familiariser avec les propriétés algébriques des ensembles $\mathcal{J}(K)$ et $\mathcal{D}(K)$ et de mettre en œuvre certains algorithmes les concernant. Après avoir fait le lien entre $\mathcal{J}(K)$ et $\mathcal{D}(K)$ ainsi que la relation de ces ensembles avec l'ensemble des séries algébriques, le travail consistera à traiter une bonne partie des points suivants :

- étudier la structure de $\mathcal{J}(K)$ (resp. $\mathcal{D}(K)$), muni de l'addition usuelle et du produit de Hadamard ou de Cauchy,
- calculer, dans le cas de la caractéristique non nulle, la période d'un élément unitaire de $\mathcal{J}(K)$ et de produire un programme permettant de calculer cette période sur machine,
- déterminer, connaissant les relations de récurrence, de deux éléments de $\mathcal{J}(K)$, une relation non triviale vérifiée par leur produit de Hadamard ou de Cauchy.

Références

- [1] A. BOSTAN, F. Chyzak, B. Salvy, *D-finitude : algorithmes et applications*, algo.inria.fr/EJCIM07/EJCIM07-LN.pdf
- [2] A. NECER, *Séries formelles et produit de Hadamard*, Journal de Théorie des nombres de Bordeaux, tome 9, n°2 (1997) p. 319–335.
- [3] R. P. STANLEY, *Finite Power series*, European Journal of Combinatorics, 1 (1980), p. 175–188.