PSFPN : Implantation efficace de l'Algorithme de Berlekamp – Massey

Encadrants : Jean-Charles Faugère et Jérémy Berthomieu
Adresse de contact :
jean-charles.faugere@inria.fr, jeremy.berthomieu@lip6.fr

Nombre d'étudiants : 2.

Description :

Dimension 1**.**

L'algorithme de Berlekamp – Massey, introduit par Berlekamp en 1968 [Ber68] et Massey en 1969 [Mas69], est un algorithme fondamental en Calcul Formel. Il permet par exemple de calculer efficacement le polynôme minimal d'une matrice ou d'interpoler un polynôme creux. En Théorie des Codes correcteurs, il permet de corriger les erreurs de transmission des codes BCH [Hoc59, BC60] (utilisés entre autres dans les CD, les SSD ou encore certains codes-barres bidimensionnels).

Étant donnée une table $\mathbf{u} = (u_0, \ldots, u_{d-1})$ à coefficients dans un corps $\mathbb{K}$, l'algorithme de Berlekamp – Massey retourne la relation de récurrence à coefficients constants de plus petit ordre vérifiée par $\mathbf{u}$.

Deux modélisations classiques du problème du calcul de relation de récurrence existent.

— La première, *via* l'algèbre linéaire, nous permet assez facilement de montrer que la complexité de l'algorithme de Berlekamp – Massey est en $O(d^3)$ opérations dans $\mathbb{K}$.

— La seconde, *via* des polynômes, nous assure que cette complexité est en fait en $O(d^2)$, voire en $O(\mathsf{M}(d)\log d)$.

Le premier objectif de ce projet est de faire le lien entre ces deux modélisations et de les implémenter efficacement en `C`.

Ensuite, nous nous intéresserons au calcul efficace *en ligne* de la relation de récurrence. Dans la version en ligne, nous supposons que les coefficients $u_0, \ldots, u_{d-1}$ de $\mathbf{u}$ ne sont plus connus d'un coup mais au fur et à mesure. Le but est de calculer la relation de récurrence satisfaite par $\mathbf{u}_{<k} = (u_0, \ldots, u_{k-1})$ puis de la mettre à jour efficacement dès que u_k nous est donné afin de déterminer celle de $\mathbf{u}_{<k+1}$. Un second objectif de ce projet sera alors d'implémenter efficacement en `C` la version en ligne de l'algorithme de Berlekamp – Massey.

Dimension $n > 1$**.**

Le problème du calcul des relations de récurrence d'une suite à plusieurs indices trouve des applications en Calcul Formel [FM11], en Combinatoire [BMP00] et en Théorie des Codes correcteurs [Sak90].

En 1990, Sakata [Sak90] a proposé l'algorithme de Berlekamp – Massey – Sakata généralisant celui de Berlekamp – Massey aux suites à n indices.

En 2015, l'algorithme Scalar-FGLM [BBF15] a été proposé afin de calculer aussi les relations de récurrence d'une suite à plusieurs indices.

Si le temps le permet, nous étudierons soit l'algorithme de Berlekamp – Massey – Sakata, soit une version en ligne de l'algorithme Scalar-FGLM.

Références

[Ber68] Berlekamp, E., 1968. Nonbinary BCH decoding. IEEE Trans. Inform. Theory 14 (2), 242–242.

[BBF15] Berthomieu, J., Boyer, B., Faugère, J.-Ch., 2015. Linear Algebra for Computing Gröbner Bases of Linear Recursive Multidimensional Sequences. In : Proc. of the 40th ISSAC. ACM, pp. 61–68.

[BC60] Bose, R. C., Ray-Chaudhuri, D. K., 1960, On A Class of Error Correcting Binary Group Codes. Information and Control 3 (1), 68–79.

[BMP00] Bousquet-Mélou, M., Petkovšek, M., 2000. Linear recurrences with constant coefficients : the multivariate case. Discrete Math. 225 (1–3), 51 – 75, FPSAC'98.

[FM11] Faugère, J.-Ch., Mou, C., 2011. Fast Algorithm for Change of Ordering of Zero-dimensional Gröbner Bases with Sparse Multiplication Matrices. In : Proc. of the 36th ISSAC. ACM, pp. 115–122.

[Hoc59] Hocquenghem, A., 1959, Codes correcteurs d'erreurs. Chiffres (in French) (Paris) 2, 147–156

[Mas69] Massey, J. L., 1969. Shift-register synthesis and BCH decoding. IEEE Trans. Inform. Theory IT-15, 122–127.

[Sak90] Sakata, S., 1990. Extension of the Berlekamp-Massey algorithm to N Dimensions. Inform. and Comput. 84 (2), 207–239.