PSFPN : Algorithme de Berlekamp – Massey pour les codes correcteurs

Encadrant : Jérémy Berthomieu
Adresse de contact : jeremy.berthomieu@lip6.fr

Nombre d'étudiants : 2.

Description :

Étant donné un message représenté sous la forme d'un vecteur de $\mathbb{F}_q^k$, où $\mathbb{F}_q$ est un corps fini, la théorie des codes correcteurs permet d'anticiper les erreurs apparaissant au cours de sa transmission en y ajoutant de la redondance. En général, on considère alors les messages comme des vecteurs (dits *mots du code*) d'un sous-espace vectoriel C de $\mathbb{F}_q^n$ de dimension $k \leq n$. Après transmission du message, il *suffit* alors de trouver le vecteur de C le plus proche de celui reçu pour corriger les erreurs de transmission.

Dans ce projet, on souhaite étudier les codes BCH [Hoc59, BC60], utilisés entre autres dans les CD, DVD, SSD ou encore certains codes-barres bidimensionnels.

L'algorithme de Berlekamp – Massey, introduit par Berlekamp en 1968 [Ber68] et par Massey en 1969 [Mas69], permet de corriger les erreurs pour des codes BCH. Nous proposons d'étudier les deux versions classiques de l'algorithme : la version algèbre linéaire et la version polynomiale proche de l'algorithme d'Euclide.

Grâce à une modélisation du problème *via* l'algèbre linéaire, on peut montrer assez facilement que la complexité du décodage est en $O(n^3)$ opérations dans $\mathbb{F}_q$. On cherchera comment améliorer cette complexité afin d'obtenir une meilleure complexité en n.

Si une suite $\mathbf{u} = (u_i)_{i\in\mathbb{N}}$ est solution d'une relation de récurrence linéaire à coefficients constants, par exemple $u_{i+2} - u_{i+1} - u_i = 0,\ \forall\, i \in \mathbb{N}$, alors l'algorithme de Berlekamp – Massey permet de retrouver cette relation à partir des premiers termes de la suite. Une généralisation de cet algorithme pour les suites à deux indices a été proposée par Sakata en 1988 [Sak88], puis pour les suites avec plus d'indices ultérieurement [Sak90]. Si le temps le permet, on étudiera son algorithme dit de Berlekamp – Massey – Sakata. Il permet à son tour de décoder une généralisation des codes BCH.

Références

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

[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.

[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.

[Sak88] Sakata, S., 1988. Finding a minimal set of linear recurring relations capable of generating a given finite two-dimensional array. J. Symbolic Comput. 5 (3), 321–337.

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