Séquences pseudo-aléatoires et récurrences linéaires à coefficients polynomiaux

1 Objet et durée de la proposition

Il s'agit d' écrire (en un an environ) un logiciel d'exploration et d'étude de génération de séquences pseudo-aléatoires définies par des récurrences linéaires à coefficients polynomiaux sur un corps fini. Ce logiciel devra être interactif et basé sur la bibliothèque Σ^{it}[1] développée dans projet Café.

La programmation pourra être effectuée par un stagiaire d'école ingénieur (ESSI ou DESS Toulon), ou par un visiteur courte durée (post-doc).

2 Equipes participantes

Sont impliquées une équipe INRIA Sophia, une équipe de l'I3S, et une équipe de l'Université de Toulon et du Var.

INRIA: Café (Manuel Bronstein[2] – DR INRIA)

I3S: RECIFE (Patrick Solé – DR CNRS)

Toulon: SIS (Alexis Bonnecaze[3] – MdC)

3 Description Scientifique

Motivation

Les récurrences linéaires à coefficients **constants** sur des corps finis sont un objet central dans plusieurs domaines applicatifs :

1. Cryptographie (chiffrement à flot [3])
2. Traitement du Signal (accés multiple à division par codage: CDMA)

[1] `http://www.inria.fr/cafe/Manuel.Bronstein/sumit`
[2] `http://www.inria.fr/cafe/Manuel.Bronstein/`
[3] `http://www.univ-tln.fr/~bonnecaz/`

3. Codes Correcteurs (codes cycliques, CRC [5])

Par contre la théorie des récurrences linéaires à coefficients **polynomiaux** sur des corps finis est encore dans l'enfance. Son étude nécessite donc de nombreuses expériences numériques pour déterminer les propriétés des séquences générées. Dans tous les trois applications précitées il s'agit d'engendrer de manière déterministe une suite qui imite le hasard. Les mesures de pseudo–aléa sont essentiellement de deux sortes :

- algorithmiques (complexité d'engendrement),
- statistique (faible corrélation).

Une mesure du premier type est la **complexité linéaire** d'une séquence. C' est la profondeur de la plus courte récurrence linéaire à coefficients constants qui engendre une suite supposée périodique. Un algorithme fondamental de calcul de cette quantité est l'algorithme de **Berlekamp Massey [2]**. Un raffinement est le **profil de complexité** qui est la courbe d' évolution de la complexité linéaire de la séquence observée sur un intervalle $[0, t]$ en fonction du temps t. L'application principale est le point 1 plus haut.

Une mesure du second type est **l'autocorrélation** qui est essentiellement le produit scalaire de la séquence (convenablement complexifiée par l'usage d 'un caractère additif du corps fini ambiant) avec une version décalée circulairement d'elle -même. Suivant la nature de cette copie on parle de corrélation **périodique, apériodique, Doppler**. Les applications de cette mesure sont les points 2 et 3 plus haut.

Objectifs

L'objectif principal du projet est d'implémenter en caractéristique finie de manière conviviale un algorithme de génération de la famille de séquences particulières en question. Un but plus ambitieux est de construire des modules d'analyse applicables à des familles de séquences générales. En particulier une implémentation robuste de l'algorithme de Berlekamp–Massey est une étape essentielle. Plus facile de mise en oeuvre mais toute aussi importante au niveau des applications est un module d' évaluation de corrélation.

Synergies

L' équipe du projet CAFÉ a une grande expérience de l'étude des récurrences linéaires à coefficients polynômiaux en *caractéristique zéro*, car de telles récurrences apparaissent naturellement dans la résolution en séries formelles d'équation différentielles linéaires (c'était aussi le sujet de la thèse de R. Bomboy, soutenue en septembre 2001).

P. Solé a une grande expérience de la conception de suites pseudo-aléatoires par la théorie des codes cycliques. Certaines des suites sur les anneaux qu' il a considérées dans les années 80 [6] sont maintenant implémentées dans le standard de téléphonie mobile UMTS.

A. Bonnecaze a effectué des calculs préliminaires sur certaines suites générées par des récurrences à coefficients polynomiaux et enseigne l'algorithme de Berlekamp–Massey en DESS.

4 Ressources demandées

On demande 4 mois de stage ingénieur, soit 30kF au tarif T3 (2001).

References

[1] M. Bronstein: *Computer Algebra Algorithms for Linear Ordinary Differential and Difference Equations*, in Proceedings of 3ECM, Birkhäuser, in press.

[2] R.E. Blahut: *Decoding of Cyclic Codes and Codes on Curves*, Chapter 19 of *Handbook of Coding Theory*, V. Pless, W.C. Huffman, Eds, North Holland (1998).

[3] T. Cusick, C. Ding, A. Renvall: *Stream Ciphers and Number Theory*, North Holland (1998).

[4] V. Kumar, T. Helleseth: Chapter 21 of *Handbook of Coding Theory*, V. Pless, W.C. Huffman, Eds, North Holland (1998).

[5] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error Correcting Codes*, North Holland (1977).

[6] P. Solé: *A quaternary cyclic code, and quadriphases sequences with low correlation properties*, pp. 193-201, dans *Coding Theory and its Applications*, éditeurs G. Cohen, J. Wolfmann, Springer LNCS 388 (1988).