Retour oral de modélisation 2023 - Brian Flanagan

Textes au choix : Corps finis, algèbre linéaire (C46) et Polynômes, géométrie (C100)
Note : 16.25

Le contenu du texte :

J'ai choisi le premier texte (C46). Il traitait d'une génération mathématique de suites aléatoires. Il donnait l'exemple de la méthode de Monte-Carlo ou de la complétion de messages RSA courts par du bruit (trop faciles à décoder sinon) pour justifier l'intérêt d'avoir des suites aléatoire à disposition. On se concentre dans la suite sur une génération mathématique, non basée sur des phénomène naturels.

L'idée de base pour générer des suites aléatoires est de considérer des suites récurrentes de la forme $u_{k+1} = f(u_k)$ sur un ensemble fini. On remarque que par principe des tiroirs, de telles suites sont nécessairement péiodiques à partir d'un certain rang. Le but du texte est alors de trouver des suites de période la plus grande possible. On se place dans le cadre des suites récurrentes polynomiales, puis récurrentes linéaires.

On traite d'abord rapidement le cas des suites récurrentes polynomiales sur $\mathbb{Z}/p\mathbb{Z}$. Ici la période est nécessairement au plus p. On peut en dire un peu plus dans le cas des suites définies par $f(x) = ax + b$ en fonction de a et b.

On s'intéresse ensuite, pour augmenter la période, à des suites récurrentes linéaires sur $(\mathbb{Z}/p\mathbb{Z})^n$, c'est-à-dire définies par une fonction de la forme $f(x) = Ax + b$, avec b un vecteur et A une matrice. Après quelques justifications, on se place dans la cas où $b = 0$ et où A n'admet pas 1 comme valeur propre. La période est alors majorée par $p^n - 1$.

Le gros théorème du texte consiste alors à démontrer que si A admet une valeur propre λ (dans $\mathbb{L}$ la clôture algébrique de $\mathbb{F}_p$) d'ordre $p^d - 1$ (avec $d \leqslant n$) dans le groupe $\mathbb{L}^*$, alors il existe un vecteur $x_0 \in \mathbb{F}_p^n$ qui définit une suite de période au moins $p^d - 1$.

Jusque là, les preuves étaient à peu près complètes, mais pas celle de ce résultat. L'idée de la preuve est de considérer y_0 un vecteur propre dans $\mathbb{F}_{p^d}$ associé à λ est de considérer $y_i = y_0^{p^i}$ pour $i = 1, \dots, d-1$ (où la puissance p est appliquée à chaque composante de y_0). Au final, on considère x_0 la somme des y_i pour $i = 0, \dots, d-1$. Le texte affirmait qu'un tel x_0 convenait et rien de plus. Il y avait donc plusieurs lacunes à combler : pourquoi x_0 est dans $\mathbb{F}_p^n$ (le mettre à la puissance p), pourquoi il définit une suite d'ordre au moins $p^d - 1$ (pour cela il fallait un peu travailler, en remarquant que les y_i étaient des vecteurs propres de A pour des valeurs propres distinctes).

Ainsi, pour déterminer si une matrice peut définir une suite de période au moins $p^n - 1$, il est suffisant de trouver une valeur propre d'ordre $p^n - 1$ dans $\mathbb{L}^*$. Le texte tâche donc ensuite d'étudier différentes façons de calculer le polynôme caractéristique d'une matrice.

Le texte présente d'abord deux méthodes jugées peu efficaces, l'une par réduction de Gauss et l'autre par interpolation. Le cas des matrices compagnon est ensuite présenté et ici le calcul du polynôme caractéristique est presque immédiat. On remarque alors que dès que le polynôme caractéristique est irréductible, la matrice est compagnon. On essaye donc de se placer dans ce cas.

Le texte présente enfin un test qui permet de tester si une matrice peut donner une suite de période maximale. On montre d'abord qu'un polynôme de degré n dans $\mathbb{F}_p$ qui admet une racine d'ordre $p^n - 1$ dans $\mathbb{L}^*$ est nécessairement irréductible (c'est le polynôme minimal de ses racines sur $\mathbb{F}_p$!). On a donc eu raison de considérer précédemment le cas des matrices compagnon. Un second résultat donne un test permettant de vérifier si une matrice peut donner une suite de période maximale. Pour qu'un polynôme P de degré n admette une racine d'ordre $p^n - 1$, il faut et il suffit que X^{p^n-1} soit congru à 1 modulo $P(X)$ et que pour tout diviseur d de $p^n - 1$, $X^d - 1$ et $P(X)$ soient premiers entre eux. La preuve est

esquissée, il suffit de considérer un facteur irréductible Q de P et de calculer l'ordre de la projection de X dans $\mathbb{F}_p[X]/Q(X)$ (qui est un sous-corps de $\mathbb{L}$).

Le texte se terminait par une rapide évaluation heuristique du nombre de polynômes irréductibles de degré n ayant une racine d'ordre $p^n - 1$.

Ma présentation :

J'ai fait une présentation de 30 minutes au total (sur 35), mais le jury n'a pas eu l'air de m'en avoir tenu rigueur. J'ai présenté grosso modo ce dont j'ai parlé au dessus. Le texte suggérait de justifier l'utilisation du hasard dans le cadre du RSA, ce que j'ai fait en introduction, mais je crois que j'ai un peu raconté n'importe quoi (mais le jury n'a pas tiqué). Au niveau du code, j'ai calculé quelques périodes associées à des polynômes aléatoires de degré 2 et $p-2$ sur $\mathbb{Z}/p\mathbb{Z}$ (avec un histogramme des périodes pour un degré donné). J'ai également appliqué l'algorithme de fin du texte à une matrice donnée par l'énoncé. J'ai confronté le temps de calcul de polynômes caractéristique par Gauss, par interpolation et par la commande de Sage pour des petites dimensions.

Interraction avec le jury :

Beaucoup de questions sur le code, d'estimation de complexité (j'avais également glissé quelques calculs de complexité dans ma présentation), quelques demandes d'explicitation d'algorithmes de mon code. Par exemple, j'avais fait un algorithme naïf pour calculer la période d'une suite récurrente sur un ensemble de taille n (en $O(n^2)$), on m'a demandé si on ne pouvait pas faire mieux en utilisant la structure de $\mathbb{F}_p$ par exemple et je n'ai pas su quoi dire. Pour la complexité, on m'a demandé d'estimer celle de cet algorithme que je viens de citer, ainsi que de revenir sur les complexités des méthodes de calcul du polynôme caractéristique que j'avais citées, et à la fin on m'a demandé d'estimer celle de l'algorithme décrit à la fin du texte (et donc le coût de divisions euclidiennes).

On m'a demandé de ré-expliquer quelques petits points de ma présentation, mais pas énormément (surtout les preuves sur lesquelles j'étais passé rapidement). On est revenu rapidement sur le RSA, mais ils voulaient juste que je relise ce que j'avais écrit (en l'occurence que pour envoyer un message x pour la clé publique (n, e), on envoit un message $x + n * c$ où c est un bruit aléatoire... sauf que puisque l'on regarde modulo n, on n'envoit en fait pas le bruit... donc ça ne marche pas mais ils ne semblent pas l'avoir remarqué).

J'ai également eu un certain nombre de questions sur $\mathbb{F}_p$ et ses extensions, notamment sur les polynômes minimaux.

On m'a également demandé comment on pouvait trouver un germe x_0 qui donne une suite de période maximale une fois qu'on a identifié une matrice A. Il s'agit de reprendre la preuve et de construire y_0 en quotientant $\mathbb{F}_p[X]$.

Attitude du jury :

Jury sympathique, l'une n'a pas parlé du tout. Globalement ils étaient encourageants et aidants, mais je n'ai pas rencontré de grosses difficultés.

Organisation :

Une membre du jury m'a rappelé les modalités de l'épreuve de façon très détaillée, notamment le fait qu'il ne fallait pas faire référence au texte et faire comme si le jury ne le connaissait pas (avec cependant la possibilité de citer un théorème ou une formule du texte pour ne pas avoir à ré-écrire l'énoncé entier). La pièce comportait un grand tableau à craie ainsi qu'un écran à dérouler au milieu du tableau (un membre du jury allumait et éteignait le vidéoprojecteur lorsque je déroulait l'écran).