

RAPPORT DE MISSION AU CAMBODGE

PIERRE ARNOUX

Ce rapport rend compte de ma mission d'enseignement au Cambodge du 22 mars au 8 avril 2005, dans le cadre du projet de coopération scientifique inter-universitaire entre l'Académie Royale du Cambodge, l'Institut de Technologie du Cambodge, le CIMPA et les universités de Paris VI et de la Méditerranée, projet soutenu par l'AUF.

J'ai donné un cours intensif de mathématiques discrètes, cours un peu particulier puisqu'il était destiné à la fois aux étudiants du master de mathématiques de l'Académie Royale du Cambodge, et aux étudiants de 3ème et 4ème année du département GIC (Génie Informatique et Communications) de l'Institut de Technologie du Cambodge.

J'ai profité de ce séjour pour rencontrer diverses personnes, et voir quelles suites peuvent être données au travail actuel.

Ce rapport fait suite à celui de Michel Jambu, auquel je renvoie pour le cadre général du PCSI.

1. DÉROULEMENT DU COURS DE MATHÉMATIQUES DISCRÈTES

Ce cours prévu sur 60 heures faisait suite à des cours plus restreints (environ 24 heures) donnés les années précédentes à l'ITC, en cryptographie et en théorie des graphes. Son but était de donner des bases dans divers domaines des mathématiques très utilisés, en particulier en informatique (théorie des codes, cryptographie, théorie des graphes); on trouvera en annexe le programme du cours. Il est à souligner qu'une bonne partie de l'enseignement a consisté en travaux pratiques sur ordinateurs.

Le public de ce cours était constitué d'une part de 35 étudiants de master de l'Académie Royale du Cambodge, et d'autre part de deux promotions d'étudiants du département GIC de l'ITC, qui ont suivi chacune la moitié du cours (13 étudiants pour la promotion I4, et 17 pour la promotion I3). Les cours ont eu lieu dans les locaux de l'ITC, qui a mis à disposition une salle d'ordinateurs équipée du logiciel MuPad.

L'intérêt de ce cours est double, et particulièrement adapté au public visé : il s'agit à la fois de donner des connaissances techniques sur des domaines en plein expansion (en particulier, techniques mathématiques liées à la transmission de données) et très nécessaires pour des ingénieurs en informatique, et aussi de donner un autre regard sur les connaissances mathématiques, en particulier en algèbre linéaire : les étudiants ont souvent eu une formation sérieuse dans ce domaine, mais sans aucune mention des applications possibles, ce qui est nuisible pour de futurs enseignants et chercheurs tout autant que pour de futurs ingénieurs.

Ce cours a aussi donné aux étudiants une initiation à un logiciel de calcul formel, le logiciel MuPad, développé par l'université de Paderborn. Il s'agit de l'un des grands logiciels standard de calculs, qui présente le grand intérêt d'être gratuit pour les enseignants et les chercheurs : il peut être téléchargé directement depuis le site mupad.de. Les étudiants pourront donc, dans la mesure où ils ont accès à un ordinateur, continuer à l'utiliser par la suite.

Le cours s'est déroulé en réalité sur 55 heures, pour des raisons d'emploi du temps. Les étudiants, qui n'avaient jamais rencontré ce genre de mathématiques (groupes et corps finis, graphes) ont été très attentifs; comme dans le cours précédent de géométrie, ils ont rédigé le cours par groupe de 4 dans le but de constituer un polycopié.

Je dois cependant dire que, malgré le sérieux des étudiants, l'efficacité de l'enseignement a été plus faible que les autres années. La raison en est claire : la taille du public (plus de 50 personnes) m'a forcé à faire cours 3 heures le matin en amphi, et une heure et demi l'après-midi seulement en salle d'ordinateurs, à 3 étudiants par ordinateur, alors que les années précédentes le cours avait lieu presque entièrement en cours intégré, en salle d'ordinateurs. L'enseignement en a évidemment souffert, comme j'ai pu le vérifier en corrigeant l'examen partiel des élèves de l'ITC. Je considère que c'est accidentel : il est normal qu'il y ait un public élevé l'année de mise en place du master, et le public devrait être plus restreint si le cours est mis en place de façon récurrente, comme prévu ci-dessous.

Pour tenir compte de la diversité du public, le cours a eu lieu à la fois en français et en anglais; les étudiants de l'ITC ont suivi une scolarité essentiellement en français, alors que certains des étudiants de l'ARC ont un niveau en français trop faible pour pouvoir suivre un cours seulement dans cette langue. J'ai donc fait attention à donner la terminologie dans les deux langues, et l'examen pour les étudiants de l'ARC sera distribué en deux versions.

Comme l'a déjà noté Michel Jambu, il faut relever le manque de documents; il faudrait prévoir l'envoi d'une série de livres sur les mathématiques discrètes, en français et en anglais. Je donne une première liste à la fin du rapport.

2. PROJET DE DÉVELOPPEMENT POUR LES MATHÉMATIQUES DISCRÈTES

Ce cours, dont le projet avait été discuté les années précédentes avec Mr Protin, Mr Krey et les membres du département GIC, pourrait devenir un cours permanent du département GIC. Il serait souhaitable, pour une meilleure intégration dans le cursus de l'ITC, que sa durée soit réduite à 48 heures.

Plusieurs enseignants du département GIC et du tronc commun sont intéressés à reprendre ce cours; le plus efficace serait probablement que je le refasse encore une fois l'an prochain en tandem avec un enseignant de l'ITC, pour mettre au point le polycopié et une batterie d'exercices. Le public devrait être composé d'une promotion complète du département GIC, soit environ 15 personnes, et d'une dizaine d'étudiants de l'ARC, de façon à ne pas dépasser 30 personnes, pour pouvoir faire entièrement le cours dans une salle informatique. Si le public devait dépasser ce chiffre, une solution serait à long terme de faire plusieurs groupes, ce qui ne posera pas de problèmes si le cours est fait par des enseignants cambodgien (il est plus difficile, pour des raisons matérielles, de scinder en plusieurs groupes un cours intensif fait au cours d'une mission de 3 semaines).

Il serait éminemment souhaitable de pouvoir ensuite donner un cours plus avancé, en particulier sur les codes, qui ont de nombreuses applications industrielles; c'est un domaine dans lequel on peut facilement concevoir une poursuite d'études en 3ème cycle, avec master et thèse.

S'il est possible d'obtenir une bourse, je connais des laboratoires français qui seraient capables de recevoir un étudiant en thèse sur ce genre de sujet et de le soutenir efficacement.

3. PERSONNES RENCONTRÉES ET PERSPECTIVES DE COOPÉRATION

J'ai longuement parlé avec Mr Chan Roath, de l'Académie Royale du Cambodge, qui a assisté au cours dans la mesure où ses lourdes charges lui en laissaient le temps. Sa venue en France est prévue à l'automne prochain.

J'ai aussi beaucoup parlé avec les gens de l'ITC, Mr Ludovic Protin, et les membres du département GIC, en particulier son directeur, Mr Sopheap Seng, et Mr May Madeth; je tiens à les remercier de leur aide pendant ce séjour. J'espère pouvoir continuer à collaborer avec eux pour la mise au point du cours de tronc commun, et la mise au point de notes de cours adaptées.

J'ai rencontré Mr Ilf Eddine Bencheikh, responsable de l'AUF au Cambodge, et Monsieur Louis Arzac, attaché de coopération à l'ambassade de France à Phnom-Penh, avec lesquels j'ai parlé des possibilités de développement de la coopération.

Par contre, je dois souligner que je n'ai rencontré personne de l'Université; l'URPP est totalement absente de ce programme de coopération, ce qui pose un gros problème, déjà évoqué dans le rapport de Michel Jambu. Ce problème a deux causes: d'une part, la faiblesse de leur revenu semble contraindre les enseignants de l'université à avoir de nombreuses activités annexes, qui freinent leur investissement dans la recherche et l'enseignement. D'autre part, le niveau de la plupart des enseignants est faible (licence), et ne leur permet peut-être pas de participer à un travail de ce type. Si l'on veut que le programme actuel porte ses fruits, il faudra trouver le moyen d'intégrer à l'université des enseignants qui aient le désir et les possibilités d'augmenter le niveau des cours distribués.

Quelles perspectives peut-on proposer pour la suite?

3.1. Mise en place du cours de mathématiques discrètes. Dans un premier temps, je voudrais achever la mise en place de ce cours; il suffirait de le refaire une fois pour former plusieurs enseignants capables de le reprendre, ce qui est l'un des buts de ce programme AUF. Il y a au moins 3 personnes à l'ITC qui ont la volonté et la capacité de reprendre ce cours.

3.2. Poursuite d'études dans le domaine. Le cours que j'ai donné est un cours de base, qui donne le vocabulaire et les concepts fondamentaux (calcul modulo p , corps finis, espaces vectoriels sur les corps finis, etc...); il n'est évidemment pas possible d'arriver en 60 heures à un niveau master 2 en partant du début. Il serait donc souhaitable de compléter par un cours plus spécialisé, ce que de nombreuses personnes peuvent faire.

Dans un deuxième temps, il sera nécessaire de former des étudiants au niveau 3ème cycle, en vue des applications informatiques et à la transmission de données. plusieurs laboratoires en France travaillent dans ce domaine en lien avec l'industrie, et pourraient accueillir un étudiant en thèse, venant de l'ITC ou de l'ARC. Il est donc très souhaitable de pouvoir obtenir une ou plusieurs bourses de thèse dans ce domaine.

3.3. Formation pédagogique de base. Il est important que la formation mathématique ne fonctionne pas en circuit fermé, coupée du reste de la société, c'est pourquoi il est important qu'une partie des diplômés s'intègre dans l'industrie, comme nous venons de le proposer.

Cependant, il faut aussi constituer un appareil d'enseignement et de recherche efficace. Sans cela, la formation de base restera inadaptée, et la formation supérieure devra être effectuée à l'étranger. Il faut donc aussi penser à former les futurs enseignants, chercheurs et

cadres supérieurs du système éducatif, et il est important qu'ils n'aient pas une vue étroite de l'enseignement mathématique (qui, comme dans tous les pays du monde, restera une part importante de l'enseignement primaire et secondaire).

Dans ce but, je pense qu'il serait très souhaitable de proposer à quelques étudiants choisis de suivre en France une formation aux concours de recrutement (agrégation), en particulier pour les enseignants des filières francophones. Cela aurait, pour un coût modeste, un triple avantage : tout d'abord, leur permettre d'élargir leurs connaissances de base en mathématiques (la formation cambodgienne est solide, mais trop étroite); ensuite, améliorer leur niveau en français, ce qui est particulièrement souhaitable pour les enseignants des filières francophones; enfin, pour les meilleurs, donner une base au niveau master, permettant une poursuite d'étude en thèse.

4. PROGRAMME DU COURS

Le cours sera fait en utilisant un logiciel de calcul formel (mupad).

Le but de ce cours est d'aborder les notions mathématiques les plus utilisées dans divers domaines informatiques, en particulier : cryptographie, codes correcteurs, graphes, automates. On restera à un niveau élémentaire, tout en donnant aux étudiants les bases conceptuelles permettant de poursuivre l'étude. On essaiera de donner des algorithmes explicites dans chaque domaine; l'examen portera en particulier sur l'application de ces algorithmes. C'est pour cela qu'une composante sur machine est nécessaire.

4.1. Fondements : théorie des ensembles.

4.1.1. *Vocabulaire de théorie des ensembles.*

Listes, opérations sur les listes.

Ensembles.

Opérateurs de création d'ensembles :

- sous-ensembles
- intersection, réunion, différence symétrique, complémentaire; lien avec le calcul propositionnel.
- ensemble des parties
- produit cartésien

Exercices.

4.1.2. *Relations, fonctions).*

Relation entre un ensemble E et un ensemble F , vue comme une partie de $E \times F$.

Fonction et graphe d'une fonction.

Vocabulaire des fonctions : injection, surjection, bijection.

Cas particulier des ensembles finis.

Fonction f^{-1} de $\mathcal{P}(F)$ dans $\mathcal{P}(E)$

4.1.3. *Relations d'ordre.*

Vocabulaire des relations d'ordre : majorant, minorant, plus grand élément (ou maximum), borne supérieure, élément maximal.

Exemples de relations d'ordre : relation d'ordre usuelle sur les nombres, inclusion, divisibilité.

Union, PPCM, vus comme borne supérieure.

4.1.4. *Relations d'équivalence.*

Définition, classes d'équivalence. Partition d'un ensemble.

Clôture transitive d'une relation symétrique.

Le dernier constructeur d'ensembles : ensemble quotient.

Exemples : construction des entiers relatifs, des rationnels, des entiers modulo n , des angles.

4.1.5. *Combinatoire, dénombrements.*

Coefficients binomiaux; formule d'inclusion-exclusion.

4.1.6. *Calcul propositionnel.*

Vrai, faux, variables propositionnelles, opérateurs Not, Or, And, Xor. Formules propositionnelles. Relation avec la théorie des ensembles.

Expression dans $\mathbb{Z}/2\mathbb{Z}$.

4.2. **Groupes et cryptographie.**

4.2.1. *Introduction à la cryptographie.*

4.2.2. *Les groupes $\mathbb{Z}/n\mathbb{Z}$.*

Définition, propriétés de base, calcul modulo n .

4.2.3. *Le petit théorème de Fermat et ses généralisations.*

4.2.4. *La méthode RSA : théorie et pratique.*

4.2.5. *Quelques autres applications des groupes.*

4.3. **Algèbre linéaire et codes correcteurs.**

4.3.1. *Exemples de problèmes linéaires et rappels d'algèbre linéaire.*

Equations linéaires, suites récurrentes linéaires, équations différentielles linéaires.

Méthode du pivot, vue de façon algorithmique.

A traiter en détail; on insistera sur le fait qu'il est rare qu'on ait un algorithme complet et efficace permettant de traiter une aussi large classe de problèmes.

Vocabulaire de l'algèbre linéaire : Espaces vectoriels, bases, applications linéaires, matrices. Equations cartésiennes et paramétriques.

Produit de matrices et composition d'applications linéaires. Calcul de puissances de matrices : le cas des matrices diagonales. Le problème de la diagonalisation. Exemples simples.

4.3.2. *Codes correcteurs et autres applications.*

Distance de Hamming, code détecteur et correcteur, borne de Hamming.

Codes correcteurs d'erreur linéaires : codes de Hamming. Matrice génératrice, matrice de contrôle, syndrome.

Codes polynomiaux et codes cycliques; utilisation de polynômes irréductibles à coefficient dans un corps fini.

Exemples de problèmes linéaires à coefficients dans un corps fini (jeu Lights Out).

Calcul effectif sur machine.

4.4. **Théorie des graphes.** Introduction à la théorie des graphes.

Vocabulaire : arêtes, sommets, degrés, chaînes, cycles, et applications élémentaires. Représentation sur machine : matrice d'incidence et matrice d'adjacence.

Etude de diverses classes de problèmes, avec quelques algorithmes de solution :

- problèmes de chemin eulérien, et théorème d'Euler.
- problèmes de comptage de chemin et matrice d'adjacence.
- problèmes de flots et de tension, et matrice d'incidence.
- problèmes de calculs de plus court chemin et algorithme de Dijkstra.
- problèmes de coloriage et algorithme de Welsh et Powell.

5. QUELQUES LIVRES DE BASE

Demazure, *Cours d'algèbre*

Graham, Knuth, Patashnik, *Concrete Mathematics*

Hardy, Wright, *An introduction to the theory of numbers*

Koblitz, *A course in number theory and cryptography*

Vélu, *Méthodes mathématiques pour l'informatique*

Zémor, *Cours de cryptographie*

UNIVERSITÉ DE LA MÉDITERRANÉE