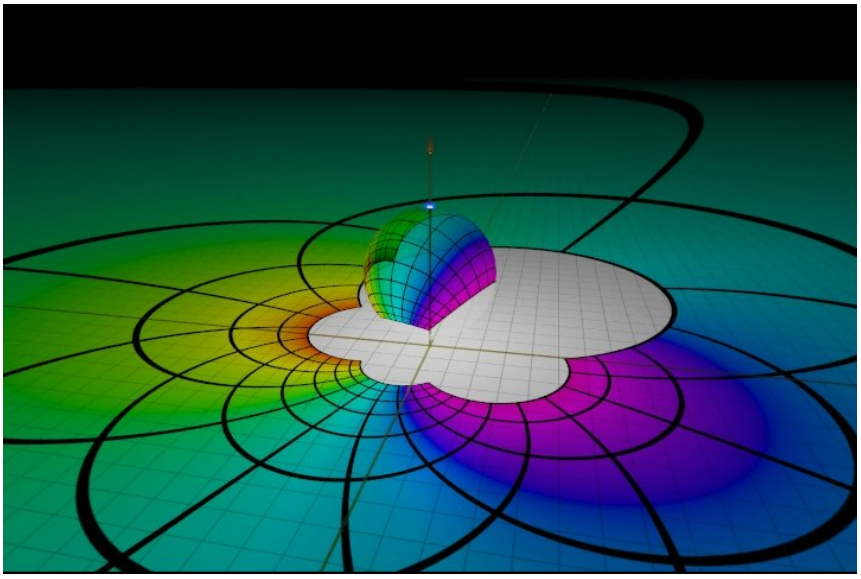
Journal du colloque des étudiants de premier cycle en mathématiques de l'Université Laval



Volume 5, Septembre 2011

UNIVERSITÉ LAVAL

Avant-propos

On peut sans aucun doute dire que l'été 2011 fut chargé pour les étudiants en mathématiques bénéficiant d'une bourse de recherche de premier cycle (BRPC) ou d'un projet de recherche subventionné par un professeur. En plus du traditionnel colloque de fin de stage donnant la chance aux étudiants de présenter leur travail, un séminaire hebdomadaire leur a permis d'assister à plus d'une quarantaine d'exposés donnés par leurs pairs tout au long de l'été. Finalement s'est aussi tenu au mois de juin le Congrès Canadien des Étudiants en Mathématiques. Environ 165 étudiants de partout au Canada ont alors convergé vers Québec pour donner et assister à des présentations portant sur divers sujets mathématiques.

Suite à l'initiative d'Alexandre St-Onge en 2006, les boursiers sont incités à écrire un article sur leur sujet de recherche de l'été. C'est ainsi que le journal du colloque des étudiants au premier cycle en est à sa cinquième édition. L'écriture d'articles est importante pour tout chercheur en mathématiques. Ce journal se veut donc une opportunité intéressante afin de se familiariser à l'écriture d'un article scientifique.

On ne peut passer sous silence l'appui des professeurs qui ont généreusement donné de leur temps, expérience et patience afin d'encadrer les étudiants dans leur travail. De même, rien de tout cela n'aurait été envisageable sans les bourses du CRSNG qui permettent aux étudiants d'être rémunérés pour faire de la recherche. Merci aussi à Dominique Maheux pour l'aide à la préparation de ce journal.

Bonne lecture !

Laurent Pelletier

Laurent Robert-Veillette

Table des matières

Journal du colloque des étudiants de 1er cycle en
mathématiques de l'Université Laval
Volume 4, Septembre 2010, 6-10

Homologie et cohomologie de $\ell^1(S)$

Laurent Robert-Veillette
sous la direction de Frédéric Gourdeau

Résumé

Sans entrer dans les détails et technicalités de l'homologie et de la cohomologie, cet article pose les bases théoriques permettant une introduction à ce sujet. Entre autre, nous introduirons la théorie des semi-groupes afin de travailler avec l'algèbre $\ell^1(S)$ composée des suites sommables indexées par les éléments d'un semi-groupe et nous parlerons brievement du rôle du produit tensoriel.

1 Introduction

Avant même de penser à introduire le réel sujet de cet article, il faut inévitablement passer par quelques définitions qui nous seront très utiles plus loin pour mieux comprendre le lien entre l'homologie et la cohomologie.

Définition 1 *Soit X, Y deux espaces vectoriels sur $\mathbb{C}$ normés*

1. *Un opérateur $T : X \to Y$ est linéaire si*
   $\forall x, z \in X$ et $\forall \alpha \in \mathbb{C}$, on a $T(\alpha x + z) = \alpha T(x) + T(z)$.
2. *Un opérateur $T : X \to Y$ est borné s'il existe*
   $N > 0$ tel que $\| Tx \|_Y \leq N \| x \|_X$.
3. *On appelle T une fonctionnelle linéaire lorsque c'est un opérateur linéaire de X vers le corps de base $\mathbb{C}$.*
4. *On appelle $X^* := \{T : X \to \mathbb{C} | \, T$ est linéaire et borné$\}$ le dual de X. On peut aussi le noter $BL(X, \mathbb{C})$.*

La définition la plus importante ici est évidemment celle du dual X^*. On va donc regarder plus en détails les opérateurs linéaires et bornés qui ont comme image le corps $\mathbb{C}$. Bien que la linéarité soit un concept familier, le fait d'être un opérateur borné n'est pas nécessairement intuitif. En fait, il est facile de montrer que dans le cas des opérateurs linéaires, il y a une équivalence entre « être borné » et « être continu ». On peut donc simplement penser au dual comme l'ensemble des fonctionelles linéaires et continues. Ce sont donc ces « jolies » fonctions qui nous intéresseront plus loin et avec lesquelles nous relierons l'homologie et la cohomologie.

2 Les semi-groupes

La théorie classique des structures algébriques se concentre habituellement sur les groupes, des objets ayant beaucoup de régularité. En comparaison, les semi-groupes font plutôt pitié. Par contre, on tente aujourd'hui d'explorer d'autres zones qui semblaient auparavant sans intérêt. Ayant plusieurs applications en informatique et en résolution d'équations différentielles, les semi-groupes font partie de ces nouvelles zones de recherche.

Définition 2 *Un semi-groupe S est un ensemble muni d'une loi de composition $\star$ associative. Autrement dit, $\forall a, b, c \in S \quad a \star (b \star c) = (a \star b) \star c$.*

Tout de suite, on voit qu'il y a un relâchement majeur par rapport aux axiomes des groupes. En effet, on n'exige ni la présence d'inverses, ni celle d'une unité. Les semi-groupes sont donc très généraux, car il n'y a quasiment aucune restriction quant aux éléments qui les composent.

Exemples

1. L'exemple le plus simple et le plus intuitif d'un semi-groupe est l'ensemble des naturels $\mathbb{N}$ avec l'addition, le min ou le max.
2. Un semi-groupe très utile en informatique est celui généré par un ensemble ou alphabet avec l'opération de concaténation
3. Le semi-groupe qui jouera un rôle important pour nous, sera celui du type **régulier**. Celui-ci respecte la condition selon laquelle $\forall x \in S \quad \exists y \quad$ t.q. $xyx = x$. Il faut remarquer ici que xy joue le rôle d'une unité à gauche pour x. C'est cette propriété que nous utiliserons plus tard.

3 L'algèbre $\ell^1(S)$ et le produit tensoriel

Habituellement, l'analyste en herbe joue avec les suites indexées par les éléments de $\mathbb{N}$: $(x_1, x_2, x_3, \dots)$. Si on ajoute la condition que les éléments de ces suites soient sommables ($\sum_{i=1}^{\infty} |x_i| < \infty$), on se retrouve dans l'espace $\ell^1 = \ell^1(\mathbb{N})$. Nous allons généraliser légèrement cet espace en définissant l'algèbre qui suit :

Définition 3 $\ell^1(S) := \{(x_s)_{s\in S} | \sum_{s\in S} |x_s| < \infty\}$.
Ce sont les suites sommables indexées par les éléments d'un semi-groupe S. Munies de l'addition terme à terme et du produit de convolution, elles forment une algèbre.

Définition 4 *Le produit de convolution dans $\ell^1(S)$ est* $(f * g)(u) = \sum_{st=u} f(s)g(t)$.

On va vouloir faire des opérations sur les éléments de cette algèbre. Comme on ne peut pas calculer un par un les résultats d'une application sur chaque suite dans $\ell^1(S)$, on va vouloir se doter d'une sorte de base sur laquelle nous appliquerons nos calculs pour ensuite déduire le résultat pour l'espace global. Si on imagine que nos suites sont finies, il n'est pas difficile de se convaincre que les deltas de Kronecker ci-dessous font notre affaire :

$$\delta_s(t) := \begin{cases} 1 & \text{si } s = t \\ 0 & \text{sinon} \end{cases}$$

En fait, pour élargir le résultat au cas où il y a un nombre infini d'éléments non-nul dans notre suite, il suffit de compléter l'espace en ajoutant toutes les combinaisons linéaires de δ_s qui convergent par rapport à la norme 1. On a donc l'égalité suivante :

$$\ell^1(S) = \langle B \rangle^- := \{a | a = \lim_{\|\cdot\|_1} \sum_{finie} \lambda_s \delta_s\} \quad \text{où } \lambda_s \in \mathbb{C}$$

Ainsi, on pourra travailler sur l'ensemble des δ_s et prendre la limite pour obtenir un résultat global sur l'algèbre en entier. Comme nous allons aussi utiliser les algèbres $\ell^1(S \times S), \ell^1(S \times S \times S), \ldots$, nous voudrions un ensemble générateur semblable à celui en une dimension. Le choix naturel qui nous vient en tête est le suivant :

$$\delta_{s_1,\ldots,s_n}(t_1, \ldots, t_n) := \begin{cases} 1 & \text{si } s_i = t_i \quad \forall i \\ 0 & \text{sinon} \end{cases}$$

Par contre, nous préférerions manier des opérateurs linéaires ayant un seul argument. Si on emploie la fonction ci-dessus, nous devrons manipuler plusieurs variables à la fois. La solution existe et nous la trouverons à travers le produit tensoriel. Nous passerons très rapidement sur les buts et sur la théorie entourant celui-ci. C'est un outil essentiel pour quiconque désire linéariser des applications bilinéaires ou multilinéaires.

Le but est d'associer chaque couple (x, y) à un élément noté $x \otimes y$ qui englobera les propriétés bilinéaires des fonctions qui prennent (x, y) en argument. Pour X et Y deux espaces vectoriels, on choisit donc $x \otimes y \in BL(X^* \times Y^*, \mathbb{C})$ et on définit :

$$x \otimes y(f, g) := f(x)g(y) \quad \forall f \in X^* \quad \forall g \in Y^*$$
$$X \otimes Y := span\{x \otimes y | x \in X \quad y \in Y\}$$

Ce qu'il faut remarquer ici est que grâce aux propriétés des duaux dans lesquels se trouvent les fonctions f et g, le tenseur $x \otimes y$ possède toutes les propriétés de bilinéarité. Autrement dit, $x \otimes \alpha y + z \otimes y = \alpha(x+z) \otimes y$. La raison pour laquelle nous voulons utiliser un produit comme celui-ci est qu'il y a un isomorphisme isométrique entre $BL(X \times Y, \mathbb{C})$ et $BL(X \otimes Y, \mathbb{C})$. Dans le cas qui nous intéresse, il y a même un isomorphisme entre $\ell^1(S \times \cdots \times S)$ et $\ell^1(S)\hat{\otimes} \ldots \hat{\otimes}\ell^1(S)$.

Les chapeaux sur les symboles du produit tensoriel servent ici à noter que nous avons, un peu comme dans le cas à une dimension, complété l'espace selon la norme projective. Le lecteur est invité à consulter [2] pour plus de détails.

Il faut mentionner une dernière propriété plaisante du produit tensoriel. Si on a $\{x_i\}$ une base pour X et $\{y_j\}$ une base pour Y, alors on sait que $\{x_i \otimes y_j\}$ forme une base pour $X \otimes Y$. Donc, ce qu'il faut retenir, c'est que comme l'ensemble des δ_s engendre $\ell^1(S)$, nous pouvons effectuer tous nos calculs sur les tenseurs $\delta_{s_1} \otimes \delta_{s_2} \otimes \cdots \otimes \delta_{s_n}$ pour ensuite compléter l'espace et ainsi obtenir un résultat global pour $\ell^1(S \times \cdots \times S)$.

4 Homologie et cohomologie

Mais pour quels genre de calculs et pour quels genre de questions avons-nous besoin de développer tous ces outils ? Cette section tente d'en dresser un maigre portrait. Parlons d'abord du cas très précis d'homologie qui nous intéresse. On regarde de plus près la chaîne suivante :

$$\ldots \xrightarrow{d_3} \ell^1(S)\hat{\otimes}\ell^1(S)\hat{\otimes}\ell^1(S) \xrightarrow{d_2} \ell^1(S)\hat{\otimes}\ell^1(S) \xrightarrow{d_1} \ell^1(S)$$

Nous allons éviter d'expliciter les d_i, car ce n'est pas pertinent pour l'explication qui suit, mais il faut savoir que ce sont des fonctions linéaires, continues et respectant la condition $d_n d_{n+1} = 0$. Pour aboutir à la **co**homologie il faut en fait dualiser la chaîne ci-dessus. Le concept général est simple, mais on a besoin d'une définition.

Définition 5 *Pour une fonction $\Psi : X \to Y$, on pose la fonction duale $\Psi^* : Y^* \to X^*$ qu'on définit par $(\Psi^* g)(x) := g(\Psi(x)) \quad \forall g \in Y^* \quad \forall x \in X$.*
Comme on connait Ψ et g, la valeur de Ψ^* est bien définie en chaque x.

On voudrait donc trouver la fonction duale des d_i. Pour cela, il faut connaître les duaux de $\ell^1(S)\hat{\otimes} \ldots \hat{\otimes}\ell^1(S)$. Nous allons développer l'intuition pour le cas de dimension 2, mais cela se généralise facilement.

Affirmation 1 : Il y a un isomorphisme isométrique entre $(\ell^1(S)\hat{\otimes}\ell^1(S))^*$ et $BL(\ell^1(S) \times \ell^1(S), \mathbb{C})$.
Intuition : La propriété fondamentale du produit tensoriel nous dit qu'il y a un isomorphisme isométrique entre $BL(\ell^1(S) \otimes \ell^1(S), \mathbb{C})$ et $BL(\ell^1(S) \times \ell^1(S), \mathbb{C})$.

Si $\phi(x,y) \leftrightarrow F_\phi(x \otimes y)$, alors il suffit de prendre l'extension de F_ϕ dans l'espace complété pour avoir l'isomorphisme recherché.

Affirmation 2 : Il y a un isomorphisme isométrique entre $BL(\ell^1(S) \times \ell^1(S), \mathbb{C})$ et $BL(\ell^1(S), (\ell^1(S))^*)$.
Intuition : Si on se donne un opérateur $\phi \in BL(\ell^1(S) \times \ell^1(S), \mathbb{C})$, on peut l'associer à un opérateur $T_\phi \in BL(\ell^1(S), (\ell^1(S))^*)$ ainsi : $(T_\phi(x))(y) := \phi(x,y)$. C'est cette identification qui nous permet de mettre en évidence l'isomorphisme.

De ces deux affirmations, on conclut qu'il existe un isomorphisme entre le dual de $\ell^1(S)\hat{\otimes}\ell^1(S)$ et $BL(\ell^1(S), (\ell^1(S))^*)$. Donc lorsqu'on parle de cohomologie comme la dualisation de l'homologie, c'est parce qu'on renverse les chaînes en prenant les duaux autant des opérateurs que des algèbres. On obtient alors la **co**-chaîne ci-dessous.

$$\ldots \overset{d_3^*}{\leftarrow} BL(\ell^1(S) \times \ell^1(S), (\ell^1(S))^*) \overset{d_2^*}{\leftarrow} BL(\ell^1(S), (\ell^1(S))^*) \overset{d_1^*}{\leftarrow} \ell^\infty(S)$$

C'est ainsi que la cohomologie est obtenue à partir des notions d'homologie.

5 Conclusion

Toute cette théorie a servi à comprendre un problème plus calculatoire que je ne décrirai pas ici. Nous avons obtenu une condition suffisante sur un semi-groupe S pour la *H-unitality* de $\ell^1(S)$. La preuve du résultat est assez calculatoire et plutôt ennuyante. C'est pourquoi j'ai choisi de me concentrer sur la partie théorique du projet plutôt que de remplir des pages entières de calculs. Le but de cet article n'était clairement pas de donner de preuves rigoureuses, mais plutôt de donner une intuition et un contexte très général au lecteur sur l'homologie et la cohomologie de $\ell^1(S)$.

Références

[1] Béla Bollobás. *Linear analysis*. Cambridge University Press, Cambridge, second edition, 1999. An introductory course.

[2] Frank F. Bonsall and John Duncan. *Complete normed algebras*. Springer-Verlag, New York, 1973. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 80.

[3] Yemon Choi, Frédéric Gourdeau, and Micheal C. White. Simplicial cohomology of band semigroup algebras. *Proc. Royal Soc. Edinburgh Sect. A*, Juillet 2011.

[4] John M. Howie. *Fundamentals of semigroup theory*, volume 12 of *London Mathematical Society Monographs. New Series*. The Clarendon Press Oxford University Press, New York, 1995. Oxford Science Publications.

Journal du colloque des étudiants de 1er cycle en
mathématiques de l'Université Laval
Volume 5, Septembre 2011, 7-11

Parallélisation de la méthode des éléments finis

Christian Tye Gingras
sous la direction d'André Fortin

Résumé

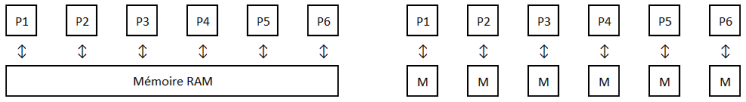
Cet été, mon stage au Groupe Interdisciplinaire de Recherche en Éléments Finis (GIREF) portait sur la parallélisation du code de MEF++, la librairie de classes permettant le calcul par éléments finis. La parallélisation rend possible l'exécution de programmes faisant usage de plusieurs processeurs de manière simultanée. Ainsi, en divisant la tâche sur plusieurs processeurs, il devient possible de résoudre des problèmes de grande taille qui, sur un seul processeur, exigeraient plusieurs jours et même plusieurs semaines de calculs. Le travail de parallélisation du code de MEF++ remonte à plusieurs années. Plusieurs classes étaient donc devenues désuètes. La première étape importante de mon travail consistait à remettre à jour ces classes déjà existantes, mais dont le fonctionnement devait être amélioré, et la deuxième étape, à parcourir le code de plusieurs classes couramment utilisées en séquentiel (sur un seul processeur) afin de rendre l'exécution parallèle plus efficace. Ce travail avait pour but de rendre possible l'utilisation du super-ordinateur Colosse, et ainsi de pouvoir exécuter du code en utilisant jusqu'à 256 processeurs.

1 Notions de base

1.1 Architecture

Afin de programmer de manière efficace en parallèle, il faut tenir compte de l'architecture du système utilisé. Il existe un grand nombre d'architectures plus ou moins complexes, mais nous pouvons les diviser en deux groupes principaux, c'est-à-dire l'architecture à mémoire partagée et l'architecture à mémoire distribuée.

L'architecture à mémoire partagée permet à tous les processeurs d'avoir accès à la même mémoire et, par le fait même, aux mêmes variables. Sans entrer dans les détails, mentionnons simplement que cette architecture est moins intéressante que



(a) Mémoire partagée (b) Mémoire distribuée

FIG. 1 – Architectures

la seconde, étant donné que le nombre de processeurs utilisables y est généralement limité. Cela peut suffire amplement pour la plupart des applications courantes, mais pas dans le contexte du calcul de haute performance.

L'architecture à mémoire distribuée alloue à chaque processeur une quantité de mémoire qui lui est propre. Il devient nécessaire, pour faire travailler conjointement toutes les unités de calcul, de les faire communiquer entre elles grâce à des fonctions spéciales appartenant à des librairies de passage de messages. Les librairies MPI (Message Passing Interface) sont sans doute les plus connues. C'est d'ailleurs ce type de librairie qui a été utilisé au GIREF. La caractéristique intéressante de cette architecture est qu'il n'y a pas de limite au nombre de processeurs utilisables.

1.2 Speedup et loi d'Amdahl

Le speedup est la mesure de l'efficacité d'un code à utiliser plusieurs processeurs. Posons

- T_s le temps d'exécution d'un programme avec un seul coeur ;
- T_p le temps d'exécution du même programme avec plusieurs coeurs.

On définit le speedup (accélération) comme étant

$$Speedup = T_s/T_p \tag{1}$$

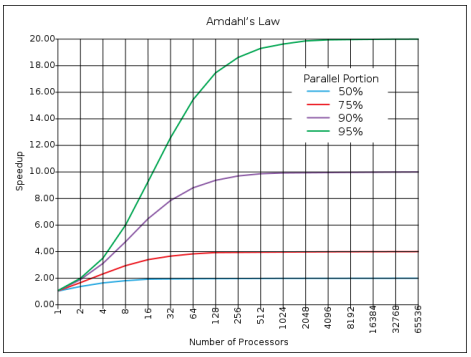


FIG. 2 – Loi d'Amdahl

Il serait logique de penser qu'utiliser n cœurs permet d'accélérer l'exécution du code par un facteur n. En pratique, il est bien rare d'avoir une telle accélération, car en général, un programme parallèle est parsemé de sections séquentielles. Cela signifie que certaines portions de code ne peuvent être exécutées qu'avec un seul processeur. La loi d'Amdahl formule de manière empirique ce phénomène.

Posons s la proportion du code pouvant être parallélisée. Alors

$$Speedup \leq \frac{1}{1-s} \tag{2}$$

La loi d'Amdahl impose donc une borne supérieure à l'accélération. La figure 2 montre l'évolution du speedup en fonction du nombre de processeurs utilisés et ce, pour plusieurs degrés de parallélisme du code.

Le coût de communication est un autre facteur dont il faut tenir compte dans un code efficace. Les communications amènent généralement les processeurs à devoir se synchroniser et à s'attendre mutuellement, en plus du délai de communication. C'est pourquoi il faut limiter au maximum leur utilisation.

2 Classes de communications du GIREF

2.1 Communications point-à-point

Pendant la première moitié de mon stage, l'essentiel de mon travail consistait à manipuler les fonctions de la librairie MPI, et ce, dans le cadre des classes destinées au calcul parallèle dans MEF++. Cette librairie offre, de base, plusieurs fonctions de communication pour les calculs parallèles. Deux familles distinguent ces fonctions selon le nombre de cœurs impliqués dans la communication, c'est-à-dire les communications point-à-point et globales.

La famille des communications point-à-point est la plus couramment utilisée au GIREF. Ces fonctions permettent à deux processeurs d'échanger des informations sous la forme de tableaux de données. Un appel typique à ce genre de communication prend la forme d'un couple de fonctions d'envoi et de réception, respectivement invoquées par le processus source et le processus cible. Ces communications peuvent être blocantes (MPI_Send et MPI_Recv) ou non blocantes (MPI_ISend MPI_IRecv). Avec l'usage des communications bloquantes, les processeurs doivent s'attendre et exécuter simultanément les appels d'envoi et de réception. Par contre, les appels non bloquants permettent de continuer l'exécution du code sans avoir à attendre que l'autre processeur ait appelé la fonction correspondante. La fonction MPI_Wait permet alors de bloquer jusqu'à ce que la communication se termine et permet de s'assurer que la valeur est bien transférée. Les appels non bloquants sont plus intéressants et permettent plus de flexibilité, étant donné qu'il est possible d'éviter, dans une certaine mesure, les délais de synchronisation entre les processeurs.

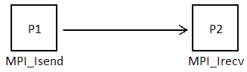


FIG. 3 – Communication point-à-point

2.2 Communications Globales

Les communications globales offertes par MPI regroupent des fonctions variées, dont les fonctions suivantes :

- MPI_Broadcast : Un processus envoie les mêmes données à tous les processus ;
- MPI_Scatter : Un processus envoie des données différentes à tous les processus ;
- MPI_Gather : Tous les processus envoient une donnée à un processus cible ;
- MPI_Alltoall : Tous les processus partagent leur donnée à tous les autres processus.

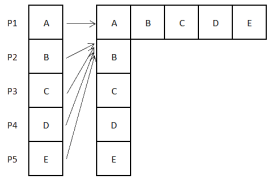


FIG. 4 – Communication globale (Gather)

Toutes ces fonctions sont bloquantes et relativement difficiles à manipuler. C'est pourquoi elles font l'objet d'une implémentation maison au GIREF sous la forme de classes C++. L'objectif de mon travail était de travailler avec les communications point-à-point non bloquantes de manière à éviter autant que possible l'attente entre les processeurs dans les classes déjà existantes. En repoussant l'appel à la fonction MPI_Wait au maximum, les communications ont davantage de temps pour se compléter en arrière-plan, et on perd ainsi moins de temps en attente inutile.

3 Assemblage des matrices

3.1 Description

La deuxième partie de mon stage consistait à améliorer le speedup de la partie dite d'assemblage dans la méthode des éléments finis. L'assemblage englobe entre autres la préparation des matrices et des vecteurs qui serviront à la résolution de systèmes linéaires. Ces matrices et vecteurs dépendent du maillage et des conditions limites qui sont appliquées sur le domaine où l'on veut résoudre un système

d'équations différentielles. En parallèle, les matrices et vecteurs sont divisés entre les processeurs, ce qui nécessite quelques communications.

L'assemblage est un algorithme théoriquement hautement parallélisable. Nous devrions donc pouvoir utiliser chacun de nos processeurs avec une efficacité de presque 100%. Cependant, le code du GIREF avait été écrit principalement pour bien fonctionner en séquentiel sans égard à l'efficacité en parallèle. Je me suis donc concentré sur l'élimination des appels inutiles aux communications et sur la mise en place de mécanismes facilitant la bonne utilisation de celles-ci.

3.2 Résultats

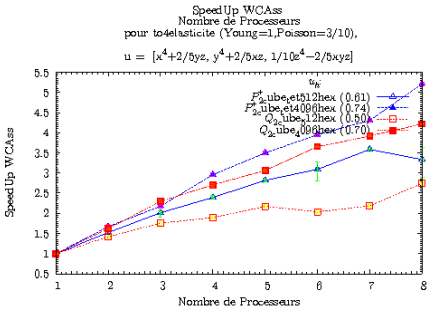


FIG. 5 – Performances en assemblage

Voici les performances que nous avons obtenues jusqu'à maintenant dans l'assemblage. On observe un bon speedup, tout particulièrement pour les problèmes plus gros. Cependant, on n'atteint pas encore le speedup optimal étant donné la nécessité de communiquer de l'information lors de l'application de certains types de conditions aux limites.

Références

[1] Parizeau, Marc, *Architecture Matérielle*. [en ligne]. http ://wcours.gel.ulaval.ca/2011/h/GIF4104/default/5notes/2-ArchitectureMaterielle.pdf [page consultée le 23 août].

[2] Parizeau, Marc, *Programmation par passage de message*. [en ligne]. http ://wcours.gel.ulaval.ca/2011/h/GIF4104/default/5notes/5-ProgMultiprocessus.pdf [page consultée le 23 août].

Journal du colloque des étudiants de 1er cycle en
mathématiques de l'Université Laval
Volume 5, Septembre 2011, 13-17

La théorie des corps de classe

Laurent Pelletier
sous la direction de Hugo Chapdelaine

Résumé

La théorie des corps de classe est une branche de la théorie des nombres s'intéressant aux extensions abéliennes des corps de nombres. On développe ici les outils nécessaires à la compréhension de la question qui m'a occuppée cet été, soit la construction d'extensions abéliennes reliées à un groupe d'idéaux.

1 Introduction

On se place dans un corps de nombres K, une extension finie des rationnels. Un objet très important de ce corps de nombres est son anneau des entiers, l'ensemble de tous les éléments de K qui sont racines d'un polynôme unitaire à coefficients entiers. On note cet anneau $\mathcal{O}_K$. Parallèlement à l'écriture de K comme $\mathbb{Q}$-espace-vectoriel, $\mathcal{O}_K$ est un $\mathbb{Z}$-module libre de rang $n = [K : \mathbb{Q}]$.

L'anneau des entiers possède plusieurs propriétés indépendantes du corps choisi. Bien que ce ne soit pas en général un anneau principal comme $\mathbb{Z}$, il possède toujours les trois propriétés suivantes :

1. Idéaux premiers non nuls sont maximaux
2. Noethérien
3. Intégralement clos

Un anneau intègre qui possède ces trois propriétés est appelé domaine de Dedekind. Ce sont les propriétés nécessaires pour assurer la factorisation des idéaux en produit d'idéaux premiers (pas toujours principaux). Ce qui nous intéresse à présent est le comportement de ces idéaux premiers lors d'une extension de corps. On considère une extension de corps L/K et un idéal premier $\mathfrak{p}$ de K. $\mathcal{O}_K$ est noethérien donc $\mathfrak{p}$ est généré par un ensemble fini d'éléments. On veut étudier l'anneau engendré par ces éléments mais cette fois dans l'extension L. Le schéma suivant représente bien la situation :

$$\begin{array}{ccccc} L & \supseteq & \mathcal{O}_L & ? \\ | & & | & | \\ K & \supseteq & \mathcal{O}_K & \mathfrak{p} \end{array}$$

La question est la suivante : $\wp$ est-il toujours un idéal premier lorsque vu dans L ? Sinon, à quoi ressemble sa factorisation ?

Définition 1. *La norme d'un idéal $I \leq A$ est la cardinalité du quotient A/I. $N(I) = \#(A/I)$.*

Résultat 1. *Soit I un idéal de A et $I = \prod_{i=1}^{r} \wp_i^{e_i}$ sa factorisation en idéaux premiers. Alors $N(I) = \prod_{i=1}^{r} N(\wp_i)^{e_i}$*

Si on prend L/K de degré n avec $K = \mathbb{Q}$, p un nombre premier et $a_1, a_2, ..., a_n$ une base de $\mathcal{O}_L$ comme $\mathbb{Z}$-module, on remarque que :

$$p\mathcal{O}_L = a_1 p\mathbb{Z} + ... + a_n p\mathbb{Z}$$

Donc $N((p)) = p^n$ où n est le degré de l'extension $L/\mathbb{Q}$. De ce résultat, on peut déduire qu'il y a au maximum n idéaux premiers de $\mathcal{O}_L$ au-dessus de (p) et que ceux-ci ont tous une norme d'une puissance de p. Ce résultat est aussi vrai dans le cas où on choisit un autre corps de base. Ainsi, si l'extension L/K est de degré n, un idéal premier de K se factorise en un maximum de n idéaux premiers lorsque vu dans L.

Résultat 2. *Soit L/K une extension galoisienne, $\mathfrak{p}$ un idéal premier de K et $\mathfrak{p} = \prod_{i=1}^{r} \wp_i^{e_i}$ sa factorisation en idéaux premiers. Alors $N(\wp_i) = N(\wp_j)$ et $e_i = e_j$ $\forall i, j$*

La véracité du résultat 2 découle du fait que le groupe des auomorphismes de l'extension galoisienne agit de façon transitive sur les idéaux premiers au-dessus de $\mathfrak{p}$. À partir de maintenant, on dira qu'un idéal premier $\mathfrak{p}$ de K est ramifié dans L si $e > 1$ dans sa factorisation. À l'opposé, on dira que cet idéal se déploie complement si le nombre d'idéaux premiers dans la factorisation est égal au degré de l'extension.

Résultat 3. *Soit $I \leq \mathcal{O}_K$. Alors $N(I) < \infty$*

Démonstration. Soit $n = [K : \mathbb{Q}]$. On choisit $\alpha \in I$. C'est un entier algébrique, donc il existe $f(x) = b_0 + b_1 x + ... + b_r x^r$ tel que $f(\alpha) = b_0 + b_1\alpha + ... + b_r(\alpha)^r = 0$. Ainsi, $b_0 = -(b_1\alpha + ... + b_r\alpha^r) \in I$ car $\alpha \in I$. On a donc $b_0 \in \mathbb{Z}$ et si $b_0 = 0$ on divise par α. $(b_0) \subseteq I$ et alors $N((b_0)) \geq N(I)$. Mais $N((b_0)) = b_0^n$ ce qui implique que $N(I) < \infty$ □

En utilisant le fait que tout les idéaux premiers non nuls de l'anneau des entiers sont maximaux, on trouve que le quotient de $\mathcal{O}_K$ par un idéal premier est un corps fini. Ce résultat est cohérent avec le cas $K = \mathbb{Q}$ puisqu'on sait que les corps finis ont tous une cardinalité d'une puissance d'un nombre premier.

2 Extensions de corps finis et Frobenius

Soit L/K une extension galoisienne de corps de nombres. On prend $\mathfrak{p}$ un idéal premier de K et $\mathfrak{q}$ un idéal premier de L au-dessus de $\mathfrak{p}$ (dans sa factorisation). On considère l'extension galoisienne de corps finis $\kappa_\mathfrak{q}/\kappa_\mathfrak{p}$ de degré f où $\kappa_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$ et $\kappa_\mathfrak{q} = \mathcal{O}_K/\mathfrak{q}$. On peut s'attendre à ce que le groupe de Galois de cette extension s'apparente fortement au sous-groupe de $Gal(L/K)$ qui laisse fixe l'idéal $\mathfrak{q}$. On définit le groupe de décomposition et d'inertie de l'idéal $\mathfrak{q}$.

$$D(\mathfrak{q}) = \{\sigma \in Gal(L/K) | \sigma\mathfrak{q} = \mathfrak{q}\}$$

$$I(\mathfrak{q}) = \{\sigma \in Gal(L/K) | \sigma \text{ est réduit à l'identité sur } \kappa_\mathfrak{q}\}$$

On a la suite exacte suivante :

$$1 \longrightarrow I(\mathfrak{q}) \longrightarrow D(\mathfrak{q}) \longrightarrow Gal(\kappa_\mathfrak{q}/\kappa_\mathfrak{p}) \longrightarrow 1$$

Il est maintenant temps d'introduire l'endomorphisme de Frobenius, un outil important dans l'étude des corps finis.

$$Frob_\mathfrak{p} : x \longrightarrow x^{\#\kappa_\mathfrak{p}} \pmod{\mathfrak{q}}$$

On remarque que le Frobenius fixe tous les éléments de $\kappa_\mathfrak{p}$. Le fait que le groupe multiplicatif d'un corps fini soit cyclique nous affirme aussi que l'ordre du Frobenius dans $Gal(\kappa_\mathfrak{q}/\kappa_\mathfrak{p})$ est égal au degré de l'extension. On peut ainsi montrer que $Gal(\kappa_\mathfrak{q}/\kappa_\mathfrak{p})$ est cyclique avec $Frob_\mathfrak{p}$ comme générateur.

$$[\kappa_\mathfrak{q} : \kappa_\mathfrak{p}] = \#\left(Frob_\mathfrak{p}\right)$$

Il est important de remarquer que le choix de $\mathfrak{q}$ au-dessus de $\mathfrak{p}$ est sans importance du fait que l'extension est galoisienne. De plus, si $\#\left(Frob_{\mathfrak{p}}\right) = 1$ et que $\mathfrak{p}$ est non ramifié, on sait en utilisant le résultat 2 que $\mathfrak{p}$ se déploie complètement dans l'extension.

3 Théorie des corps de classe

Théorème (Kronecker-Weber)**.** *Toute extension abélienne (groupe de galois abélien) des rationnels est contenue dans $\mathbb{Q}(\zeta_m)$ pour un certain m et ζ_m une racine primitive m-ième de l'unité.*

En étudiant les corps cyclotomiques [Ireland and Rosen, 1990], on remarque que les seuls idéaux premiers de $\mathbb{Z}$ qui se déploient complètement sont ceux de la forme $p\mathbb{Z}$ avec $p \equiv 1 \pmod{m}$. Ainsi, ces idéaux se déploient complètement dans tous les sous-corps de $\mathbb{Q}(\zeta_m)$. Pour s'en convaincre, on procède par contradiction en supposant qu'un tel idéal $p\mathbb{Z}$ ne se déploie pas complètement dans un sous corps de $\mathbb{Q}(\zeta_m)$ de degré $n|\phi(m)$. Conséquement, $p\mathbb{Z}$ doit se diviser en $r < n$ idéaux premiers dans le sous-corps. À leur tour, ces facteurs ne peuvent se diviser en plus de $\phi(m)/n$ idéaux dans $\mathbb{Q}(\zeta_m)$ et donc $p\mathbb{Z}$ a au plus $r\phi(m)/n < n\phi(m)/n = \phi(m)$ facteurs dans $\mathbb{Q}(\zeta_m)$, ce qui contredit le fait que $p\mathbb{Z}$ se déploie complètement dans $\mathbb{Q}(\zeta_m)$.

Réciproquement, pour une certaine extension des rationnels, le fait de trouver un m tel que tous les idéaux de la forme $p\mathbb{Z}$ avec $p \equiv 1 \pmod{m}$ se déploient nous affirme que cette extension est un sous-corps de $\mathbb{Q}(\zeta_m)$. Il est à noter que m est divisible par tous les idéaux ramifiés dans l'extension.

On voudrait étudier le même phénomène avec des corps de base différents mais pour ce faire, il faudra faire intervenir certaines nouvelles notions. On définit tout d'abord un module de congruence comme un produit $m = m_0 m_\infty$ de places finies (l'idéal m_0) et de places réelles (ensemble de plongements réels). De cette façon, on traite les idéaux premiers divisant m_0 comme des valuations de façon analogue à la valuation p-adique des rationnels. On dit alors qu'un idéal est conguent à 1 modulo m si il existe $(\alpha) = I$ avec $\nu_{\wp_i}(\alpha - 1) \geq \nu_{\wp_i}(m_0)\ \forall p_i | m_0$ et α positif à toutes les places réelles de m_∞.

On note I^m l'ensemble des idéaux fractionnaires copremiers à m et P_m les idéaux principaux congruents à 1 en modulo m. Le corps dont les seuls idéaux qui se déploient complètement sont ceux de P_m est appelé corps de rayon (par rapport à m et au corps de base K). Il n'est pas étonnant à ce point que les corps cyclotomiques soient les corps de rayon associés au corps $\mathbb{Q}$.

L'application suivante, appelée application d'Artin, est nécessaire à la compréhension des corps de classe et très utilisée afin de les construire.

$$(., L/K) : I^m \to Gal(L/K) : a = \prod_{p|a} p^{\nu_p(a)} \mapsto \prod_{p|a} Frob_p^{\nu_p(a)}$$

On remarque que dans le cas des corps de rayon, le noyau de l'application d'Artin est réduit à P_m. Mais en choisissant un sous-groupe H de I^m qui contient P_m, on peut construire un corps qu'on appelle corps de classe L associé à H.

$$Gal(L/K) \cong I^m/H$$

Il s'agit du théorème d'existence des corps de classe. La réciproque est aussi vraie, dans le sens où à chaque sous-corps du corps de rayon est associé un groupe d'idéaux H. Le problème dans le cas général est qu'il n'existe toujours pas de système comme celui des racines de l'unité pour construire les corps de rayon. Une conjecture de Stark propose l'existence d'éléments particuliers dans les corps de nombres qui génèreraient les corps de rayon. Cette conjecture a été améliorée par Dasgupta qui propose même une formule pour ces éléments. La question est toujours ouverte aujourd'hui...

Références

[Cohen and Stevenhagen, 2008] Cohen, H. and Stevenhagen, P. (2008). Computational class field theory. In *Algorithmic number theory : lattices, number fields, curves and cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, pages 497–534. Cambridge Univ. Press, Cambridge.

[Fieker, 2001] Fieker, C. (2001). Computing class fields via the Artin map. *Math. Comp.*, 70(235) :1293–1303 (electronic).

[Ireland and Rosen, 1990] Ireland, K. and Rosen, M. (1990). *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition.

[Murty and Esmonde, 2005] Murty, M. R. and Esmonde, J. (2005). *Problems in algebraic number theory*, volume 190 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition.

Journal du colloque des étudiants de 1er cycle en
mathématiques de l'Université Laval
Volume 5, Septembre 2011, 19-23

Pseudospectres super-identiques

Andréa Deschênes
sous la direction de Jérémie Rostand

Résumé

Pour une matrice $A \in M_N(\mathbb{C})$, on note par $s_1(A), ..., s_n(A)$ ses valeurs singulières, de la plus grande à la plus petite. Deux matrices $A, B \in M_N(\mathbb{C})$ possèdent des pseudopectres super-identiques si pour chaque $z \in \mathbb{C}$ et chaque $k \in 1, ..., n$ on a $s_k(A - zI) = s_k(B - zI)$. Il a été démontré dans [2] que pour tout polynôme p et toute paire de matrices $A, B \in M_N(\mathbb{C})$ ayant des pseudospectres super-identiques, les inégalités suivantes tiennent : $\frac{1}{\sqrt{n}} \leq \frac{||p(A)||}{||p(B)||} \leq \sqrt{n}$. À ce jour, tous les exemples connus satisfont l'inégalité $\frac{1}{\sqrt{2}} \leq \frac{||p(A)||}{||p(B)||} \leq \sqrt{2}$. L'objectif de ce projet était de vérifier l'optimalité de la borne $\sqrt{n}$.

1 Introduction à la matière

Dans de nombreux domaines en lien avec les mathématiques appliquées, on s'intéresse à l'estimation de $||A^n||$, où $A \in M_N(\mathbb{C})$ (la norme utilisée sera toujours la norme euclidienne qui est définie par $||A|| := \sup_{|x|=1} |Ax|$ où $|x| := \left(\sum_{i=1}^{N} |x_i|^2\right)^{1/2}$ et où $x \in \mathbb{C}^N$). Cependant, il arrive que cette quantité ne puisse être évaluée numériquement. Le spectre de la matrice A nous donne alors des informations très pertinentes sur le comportement de la norme de ses puissances à long terme grâce à la formule $\lim_{n\to\infty} ||A^n||^{1/n} = \rho(A)$ que l'on retrouve dans [3].

Par contre, le spectre ne nous donne pas d'information sur le comportement de la norme des puissances à plus court terme. Il devient alors nécessaire d'utiliser un outil plus puissant, le pseudospectre. Ce dernier donne davantage de renseignements sur plusieurs aspects du comportement d'une matrice, d'où son utilité. Pour définir le pseudospectre d'une matrice, il est tout d'abord indispensable de définir ses valeurs singulières.

Définition 1 *Toute matrice complexe $A \in M_N(\mathbb{C})$ peut s'écrire sous la forme $A = V\Lambda W^*$ où $V, W \in M_N(\mathbb{C})$ sont unitaires et $\Lambda \in M_N(\mathbb{C})$ est une matrice diagonale avec des entrées positives. Ces entrées sont les valeurs singulières $s_k(A)$, où $k = 1, ..., N$ (voir [1, page 205]).*

Dans la définition précédente, la matrice W^* correspond à la matrice transconjuguée de W qui est définie dans [1, page 6] par $W^* = \overline{W}^t$ où $\overline{W}$ est la matrice conjuguée composante par composante de W. Comme la définition des valeurs singulières écrite ci-haut est assez difficile à utiliser en pratique, on préfère souvent se référer au résultat tiré de [2] qui dit que les valeurs singulières de A sont égales aux racines carrées positives des valeurs propres de AA^*. De plus, il est important de préciser qu'en ordonnant les valeurs singulières pour que $s_1(A) \geq s_2(A) \geq ... \geq s_N(A)$, on obtient

$$s_1(A) = ||A|| \text{ et } s_N(A) = 1/||A^{-1}||.$$

Ce résultat se montrera utile dans la définition du pseudospectre.

Définition 2 *Le ϵ-pseudospectre de A, $A \in M_N(\mathbb{C})$, est défini par $\sigma_\epsilon(A) := \{z \in \mathbb{C} : ||(A - zI)^{-1}|| > 1/\epsilon\} = \{z \in \mathbb{C} : s_N(A - zI) < \epsilon\}$ avec la convention que $||(A - zI)^{-1}|| = \infty$ si $z \in \sigma(A)$. Ainsi $\sigma_\epsilon(A) \to \sigma(A)$ quand $\epsilon \to 0$ (voir [2]).*

Pour comparer adéquatement le comportement des normes des puissances de deux matrices, on peut comparer leurs pseudospectres. Il existe plusieurs méthodes de comparaison. On peut en premier lieu vérifier si les matrices ont des pseudospectres identiques. Comme mentionné dans [2], deux matrices $A, B \in M_N(\mathbb{C})$ possèdent des pseudospectres identiques si $||(A - zI)^{-1}|| = ||(B - zI)^{-1}||$, $\forall z \in \mathbb{C}$, autrement dit si $s_N(A - zI) = s_N(B - zI)$, $\forall z \in \mathbb{C}$. On trouve alors le théorème suivant :

Théorème 1 *Soient $A, B \in M_N(\mathbb{C})$ possédant des pseudospectres identiques. Alors, $1/2 \leq ||A||/||B|| \leq 2$ (voir [2]).*

Cependant, même si deux matrices ont des pseudospectres identiques, les normes de leurs puissances plus élevées ne possèdent pas nécessairement de lien entre elles. Comme on voudrait obtenir un résultat plus puissant encore, on s'intéresse donc aux matrices qui ont des pseudospectres super-identiques. Deux matrices $A, B \in M_N(\mathbb{C})$ possèdent des pseudospectres super-identiques si $s_k(A - zI) = s_k(B - zI)$ où $z \in \mathbb{C}$ et $k = 1, ..., N$, comme énoncé dans [2]. Le théorème qui en découle est alors beaucoup plus intéressant.

Théorème 2 *Soient $A, B \in M_N(\mathbb{C})$ possédant des pseudospectres super-identiques. Alors, pour tout polynôme $p(z)$, $1/\sqrt{N} \leq ||p(A)||/||p(B)|| \leq \sqrt{N}$ (voir [2]).*

2 Description du projet

La problématique à la base de ce projet était que, malgré le théorème précédent, tous les exemples connus satisfaisaient en fait l'inégalité $\frac{1}{\sqrt{2}} \leq \frac{||p(A)||}{||p(B)||} \leq \sqrt{2}$. L'objectif du projet était donc d'améliorer la borne $\sqrt{N}$, peut-être en la remplaçant par une borne indépendante de N, ou de montrer son optimalité par des exemples.

Jusqu'au début de l'été, l'exemple trouvé par Maxime Fortier-Bourque et décrit dans [4] était celui qui permettait d'obtenir la plus grande valeur pour le rapport $||A^2||/||B^2||$. À l'infini, la solution générale qu'il avait trouvée donnait :

$$A := \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & \to \infty \\ 0 & 0 & 0 & 0 \end{pmatrix}, B := \begin{pmatrix} 0 & \sqrt{2} & 0 & 1 \\ 0 & 0 & \to \infty & 0 \\ 0 & 0 & 0 & \sqrt{2} \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Alors, A et B ont des pseudospectres super-identiques et $||A^2||/||B^2|| \to \sqrt{2}$.

Pour atteindre l'objectif de ce projet d'été, il fallait commencer par trouver des paires de matrices ayant des pseudospectres super-identiques. Cependant, on sait que deux matrices ont des pseudospectres super-identiques si elles respectent une certaine condition pour une infinité de $z \in \mathbb{C}$. Les théorèmes suivants, tirés tous les deux de [2], permettent donc de remplacer cette condition infinie par un nombre fini de conditions à respecter. Ces conditions varient selon la dimension des matrices.

Théorème 3 *Soient $A, B \in M_3(\mathbb{C})$. A et B possèdent des pseudospectres super-identiques si et seulement si :*

$$\begin{cases} tr(A^i) = tr(B^i) \text{ où } i = 1, 2, 3 \\ tr(A^i A^{*j}) = tr(B^i B^{*j}) \text{ où } 1 \leq i \leq j \leq 2 \end{cases}$$

Théorème 4 *Soient $A, B \in M_4(\mathbb{C})$. A et B possèdent des pseudospectres super-identiques si et seulement si :*

$$\begin{cases} tr(A^i) = tr(B^i) \text{ où } i = 1, 2, 3, 4 \\ tr(A^i A^{*j}) = tr(B^i B^{*j}) \text{ où } 1 \leq i \leq j \leq 3 \\ tr(AA^*AA^*) = tr(BB^*BB^*) \end{cases}$$

En fait, pour tenter de trouver une paire de matrices possédant des pseudospectres super-identiques et dont le rapport des normes des carrés est plus grand que $\sqrt{2}$, la méthode peut être la suivante. Tout d'abord, il faut choisir une certaine forme

de matrices. Pour simplifier le problème afin que le logiciel Maple utilisé nous ressorte des solutions intéressantes, il faut poser certaines conditions sur la forme des matrices. Dans ce cas, on voulait qu'elles soient réelles et triangulaires supérieures en plus de posséder une diagonale nulle. Certaines des entrées restantes devaient également être nulles.

Ensuite, il faut résoudre le système d'équations qui est déterminé à partir des conditions équivalentes posées précédemment. Les solutions suggérées par le logiciel Maple n'étant pas toutes pertinentes, il faut faire un classement pour éliminer certaines solutions triviales donnant toujours un rapport de 1.

Puis, en fixant des valeurs aléatoires pour les variables indépendantes de la solution, on parvient à calculer le rapport $||A^2||/||B^2||$. Dans le cas où ce rapport est différent de 1, il faut faire des simulations pour en trouver les bornes inférieure et supérieure dans le but éventuellement de trouver un rapport supérieur à $\sqrt{2}$.

3 Résultats des expérimentations

Les expérimentations pour les matrices 4x4 n'ont pas été aussi fructueuses que prévu. Il existe relativement peu de matrices 4x4 possédant la forme décrite précédemment, et aucune de celles testées n'ont donné un rapport différent de 1, exceptés les multiples de la paire de matrices mentionnée plus tôt et trouvée par Maxime Fortier-Bourque.

Ce manque de solutions intéressantes pour ce qui est des matrices 4x4 nous a amené à faire davantage de recherche du côté des matrices 5x5. Comme aucun théorème n'avait été écrit concernant les conditions équivalentes aux pseudospectres super-identiques pour les matrices 5x5, il a fallu s'attarder un peu sur le sujet. La démonstration faisant appel aux identités de Frobenius et de Newton, les développements deviennent facilement très complexes. Cependant, en poursuivant dans le même ordre d'idée que pour les matrices 3x3 et 4x4, il a été possible de trouver le théorème suivant, mais sans le prouver. Ce théorème s'est avéré toujours vrai pour les matrices 5x5 réelles.

Théorème 5 *Soient $A, B \in M_5(\mathbb{C})$. A et B possèdent des pseudospectres super-identiques si et seulement si :*

$$\begin{cases} tr(A^i) = tr(B^i) \text{ où } i = 1,2,3,4,5 \\ tr(A^i A^{*j}) = tr(B^i B^{*j}) \text{ où } 1 \leq i \leq j \leq 4 \\ tr(AA^*AA^*) = tr(BB^*BB^*) \\ tr(A^2A^*AA^*) = tr(B^2B^*BB^*) \\ tr(AA^*AA^*AA^*) = tr(BB^*BB^*BB^*) \end{cases}$$

Il a alors été possible de trouver trois paires de matrices toutes assez similaires pour lesquelles le rapport $||A^2||/||B^2||$ ne donnait pas 1. Voici une de ces paires de matrices :

$$A := \begin{pmatrix} 0 & \to\infty & 0 & 0 & 1 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} B := \begin{pmatrix} 0 & -\sqrt{2} & \sqrt{2} & 0 & 1 \\ 0 & 0 & 0 & \to\infty & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \sqrt{2} \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Alors, A et B ont des pseudospectres super-identiques et $||A^2||/||B^2|| \to \sqrt{2}$. C'est également vrai pour les deux cas qui ne sont pas retranscrits ici. On remarque une certaine ressemblance avec les matrices de Maxime Fortier-Bourque mentionnées plus tôt.

4 Conclusion du projet

En conclusion, étant régulièrement limité par le logiciel Maple, il n'a pas été possible de trouver des paires de matrices dont le rapport des normes des carrés était supérieur à $\sqrt{2}$, ce qui aurait éventuellement pu montrer que la borne $\sqrt{N}$ était optimale. Cependant, il a été possible de trouver trois nouveaux cas intéressants pour les matrices 5x5 dont les rapports limites donnaient $\sqrt{2}$.

Dans de futures recherches, on pourrait tenter des tests avec des matrices complexes et des matrices ayant des entrées non nulles sur la diagonale. Il pourrait également être intéressant de poursuivre les recherches avec les matrices de dimension supérieure. Il serait peut-être même possible de démontrer que la borne supérieure $\sqrt{N}$ peut être ramenée à $\sqrt{2}$, au moins dans le cas des matrices réelles.

Références

[1] Roger A. Horn et Charles R.Johnson. *Matrix Analysis*, Cambridge University Press, 1985.

[2] Thomas Ransford. *Pseudospectra and matrix behaviour*, Banach Center Publications, 2010.

[3] Thomas Ransford. *On Pseudospectra and Power Growth*, Society for Industrial and Applied Mathematics, 2007.

[4] Maxime Fortier-Bourque et Thomas Ransford. *Super-identical pseudospectra*, London Mathematical Society, 2009.