Rapport à mi-vague de Xavier Caruso

Période : décembre 2015 — juin 2018

A. Rapport d'activités

1 Curriculum vitæ

Xavier Caruso
(né le 24 avril 1980 à Cannes)
IRMAR – Université Rennes 1
Campus de Beaulieu
35042 Rennes Cedex
Tél : 02 23 23 58 92
E-Mail : xavier.caruso@normalesup.org
Page web : http://xavier.toonywood.org/
Marié, deux enfants

Parcours scolaire et professionnel

2018 Promu directeur de recherche, 2ème classe (DR2)

2017–2021 Titulaire de la prime d'encadrement doctoral et de recherche (PEDR)

2011 Habilitation à diriger les recherches soutenue le 3 juin à l'université de Rennes 1 durant le jury composé de Laurent Berger, Christophe Breuil, Pierre Colmez, Jean-Marc Fontaine et Michael Rapoport.

2009–2010 Mobilité d'une année au laboratoire Poncelet à l'Université Indépendante de Moscou

2006– Chargé de recherche au CNRS affecté à l'Université de Rennes 1.

2005 Thèse sous la direction de Christophe Breuil intitulée *Conjecture de l'inertie modérée de Serre* et soutenue le 7 décembre devant le jury composé de Ahmed Abbes, Pierre Berthelot (rapporteur), Lawrence Breen, Christophe Breuil (directeur de thèse), Michel Raynaud. Autre rapporteur : Mark Kisin.

2003–2006 Moniteur à l'université Paris 13.

1999–2003 Élève de de l'École normale supérieure de Paris

Quelques responsabilités

2017– Membre fondateur et éditeur du journal *Annales Henri Lebesgue*

2012–2016 Membre élu du CoNRS (Comité National de la Recherche Scientifique)

2012–2016 Membre nommé du conseil de l'IRMAR (Institut de Recherche en Mathématiques de Rennes)

2009–2013 Coordinateur du projet ANR CETHop (Calculs effectifs en théorie de Hodge p-adique)

Divers

1997 Premier accessit au concours général de mathématiques.
Quatrième accessit au concours général de physique.
Participation aux olympiades internationales de mathématiques à Mar del Plata (Argentine). Obtention d'une *honourable mention*.

Langues : français (langue maternelle), anglais (parlé et écrit), russe (assez bonne connaissance)

2 Recherche scientifique

Ma recherche de ces cinq derniers semestres a été concentrée principalement sur deux thématiques : les polynômes de Ore et l'algorithmique des nombres et structures p-adiques.

2.1 Polynômes de Ore

Dans tout cette partie, la lettre K désigne un corps fixé muni d'un endomorphisme d'anneaux $\theta : K \to K$ et d'une θ-dérivation $\partial : K \to K$, c'est-à-dire d'une application additive vérifiant la loi de Leibniz tordue $\partial(ab) = \theta(a)\partial(b) + \partial(a)b$ (pour $a, b \in K$). À ces données, on associe l'anneau de Ore $K[X, \theta, \partial]$ défini comme suit. Ses éléments sont les expressions formelles de la forme :

$$a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \quad \text{avec} \quad n \in \mathbb{N},\ a_i \in K.$$

Celles-ci s'additionnent comme des polynômes classiques mais la loi de multiplication, non commutative en général, est régie par la règle $X \cdot a = \theta(a)X + \partial(a)$, valable pour tout $a \in K$. Cette règle, combinée à l'associativé et à la distributivité, suffit à décrire entièrement la loi de multiplication sur $K[X, \theta, \partial]$.

Les polynômes de Ore sont des outils qui apparaissent naturellement en algèbre semi-linéaire ou dans le cadre de l'étude algébrique des équations différentielles linéaires. Comprendre leur structure, d'une part, et apprendre à les manipuler efficacement, d'autre part, revêt ainsi une certaine importance dans ces domaines.

2.1.1 Multiplication rapide des polynômes de Ore

Référence :
[6] X. Caruso, J. Le Borgne, *Fast multiplication for skew polynomials*,

Un premier travail que j'ai effectué, en collaboration avec Jérémy Le Borgne, a été de mettre au point une algorithmique efficace pour la manipulation des polynômes de Ore dans le cas particulier où $\partial = 0$ et θ est d'ordre fini, noté r. Nous avions, de fait, déjà étudié ce type de questions dans un article antérieur mais les résultats que nous avions obtenus alors n'étaient valables que pour des polynômes de grand degré (à savoir, au moins de l'ordre de r^2). En réalité, nous n'étions pas conscients de cette limitation puisque, dans la situation que nous considérions, l'entier r était toujours petit. Elle nous est apparue lorsque nous avons lu un article de Wachter-Zeh et Puschinger qui traitait le cas où $d \simeq r$; l'article précisait en outre explicitement que ce cas échappait à nos méthodes et, par ailleurs, qu'il était pertinent pour les applications aux codes de Gabidulin (*cf* §2.1.2 ci-après).

Toutefois, en étudiant l'article de Wachter-Zeh et Puschinger, nous nous sommes rendus compte que leur résultat n'était pas optimal et que nous étions certainement capables de l'améliorer. Nous nous sommes donc penchés plus en détails sur la question.

Soit F le sous-corps de K formé par les points fixes de θ. La théorie de Galois nous apprend que K/F est une extension cyclique de degré r. L'algorithme que nous proposons avec Jérémy Le Borgne fait un usage décisif du morphisme d'évaluation défini comme suit :

$$\begin{array}{rccc} \text{ev} : & K[X, \theta, 0] & \longrightarrow & \text{End}_F(K) \\ & P(X) & \mapsto & P(\theta) \end{array}$$

On vérifie que c'est un morphisme d'anneaux qui induit un isomorphisme entre $K[X,\theta,0]/(X^r-1)$ et $\mathrm{End}_F(K)$. Qui plus est, il peut être évalué très efficacement dès lors que l'on dispose d'une base normale de K sur F. En effet, nous avons le lemme suivant.

Lemme 1. *Soit $(b_i)_{i\in\mathbb{Z}/r\mathbb{Z}}$ une base de K/F telle que $\theta(b_{i+1}) = b_i$ pour tout i. On considère $A(X) = a_0 + a_1X + \cdots + a_{r-1}X^{r-1} \in K[X,\theta,0]$ et on pose $c_i = A(\theta)(b_i)$ pour tout i.*

Alors la congruence suivante est vraie dans l'anneau des polynômes usuels $K[T]$:

$$\left(a_0 + \cdots + a_{r-1}T^{r-1}\right)\cdot\left(b_0 + \cdots + b_{r-1}T^{r-1}\right) = c_0 + \cdots + c_{r-1}T^{r-1} \pmod{T^r-1}.$$

Le lemme indique que calculer l'image d'un polynôme de Ore par le morphisme d'évaluation revient à effectuer une multiplication polynômiale dans l'anneau quotient $K[T]/(T^r-1)$, opération pour laquelle on dispose d'algorithmes efficaces. Pareillement, calculer l'image réciproque d'un élement de $\mathrm{End}_F(K)$ par ev revient à faire une division dans $K[T]/(T^r-1)$, ce qui peut également se faire de manière très efficace. Ces constatations permettent de ramener la multiplication de polynômes de Ore dont la somme des degrés est inférieure à r à la composition dans $\mathrm{End}_F(K)$, c'est-à-dire concrètement à la multiplication de matrices carrées de taille r à coefficients dans F. De cette manière, nous aboutissons à un algorithme de multiplication des polynômes de Ore de petits degrés dont le coût est $O(r^\omega)$ opérations dans F, où ω désigne l'exposant de la multiplication matricielle.

Pour passer aux degrés supérieurs, nous introduisons des versions twistées du morphisme d'évaluation. Précisément, étant donné un scalaire $\lambda \in K$, nous considérons l'application :

$$\begin{array}{rccc} \mathrm{ev}_\lambda : & K[X,\theta,0] & \longrightarrow & \mathrm{End}_F(K) \\ & P(X) & \mapsto & P(\lambda\,\theta) \end{array}$$

Il s'agit, à nouveau, d'un morphisme d'anneaux surjectif. Son noyau est l'idéal principal engendré par le polynôme $X^r - N_{K/F}(\lambda)$, de sorte que ev_λ induit un isomorphisme entre $K[X,\theta,0]/(X^r - N_{K/F}(\lambda))$ et $\mathrm{End}_F(K)$. Comme précédemment, il se trouve que celui-ci, ainsi que son inverse, sont calculables très efficacement. La multiplication dans $K[X,\theta,0]/(X^r - N_{K/F}(\lambda))$ se ramène ainsi à de la multiplication matricielle et a donc, elle aussi, un coût de $O(r^\omega)$ opérations dans F. Nous concluons enfin en utilisant une version du lemme chinois adaptée à nos besoin et démontrons, de cette manière, le théorème suivant.

Théorème 2. *Avec les notations et hypothèses précédentes, il existe un algorithme qui calcule le produit de deux polynômes de Ore de $K[X,\theta,0]$ de degré au plus d pour un coût de $\tilde{O}(dr^{\omega-1})$ opérations dans F, dès lors que $d \geqslant r$.*

Nous obtenons également des améliorations de ce résultats (qui ne sont malheureusement pas optimales) pour les polynômes de degré $d \ll r$.

Comme souvent, la multiplication est la brique de base à d'autres problèmes algorithmiques plus complexes. Ainsi, à partir du théorème 2, nous améliorons les complexités connues pour la division euclidienne des polynômes de Ore, le calcul du PGCD, la multi-évaluation et l'interpolation.

2.1.2 Codes de Gabidulin

Référence :

[21] X. Caruso, A. Durand, *Gabidulin codes with large length*

Dans les années 1980, Gabidulin imagina une nouvelle famille de codes correcteurs d'erreurs basée sur l'arithmétique des polynômes de Ore. Ces codes utilisent la métrique rang et, pour cette raison, sont particulièrement adaptés au codage réseau. Initialement, les codes de Gabidulin avaient été proposés dans le contexte des corps finis, où les polynômes de Ore s'effacent au profit des polynômes linéarisés. Récemment, toutefois, Robert a remis le travail de Gabidulin dans le cadre général des anneaux de Ore sans dérivation. Voici ce qui a constitué le point de départ de ma réflexion.

Comme précédemment, considérons un corps K muni d'un endomorphisme d'anneaux $\theta : K \to K$, supposé d'ordre fini r, et formons l'anneau des polynômes de Ore $K[X,\theta,0]$. Notons F le sous-corps de K

formé des points fixes de θ et considérons une base $(a_1, \dots, a_r)$ de K sur F. Soit, en outre, d un entier inférieur à r. Le code de Gabidulin associé à ces données est l'image de l'application :

$$\begin{array}{rcl} K[X,\theta,0]_{<d} & \longrightarrow & K^r \\ P(X) & \mapsto & \big(P(\theta)(a_1), \dots, P(\theta)(a_r)\big). \end{array} \tag{1}$$

où $K[X,\theta,0]_{<d}$ désigne l'espace vectoriel des polynômes de Ore de degré $< d$. Définissons le *poids rang* $w_{\mathrm{r}}(x)$ d'un vecteur $x = (x_1, \dots, x_r) \in K^r$ comme la dimension du F-espace vectoriel engendré par les coordonnées x_i, et la *distance rang* d_{r} sur K^r par $d_{\mathrm{r}}(x,y) = w_{\mathrm{r}}(x-y)$. On peut alors démontrer que la distance minimale du code de Gabidulin défini précédemment est $r - d + 1$; celle-ci atteint donc la borne de Singleton, propriété qui rend les codes de Gabidulin particulièrement intéressants. En plus de cela, les codes de Gabidulin admettent des algorithmes de codage et de décodage efficaces : le codage n'est autre qu'un problème de multi-évaluation (pour lequel nous avons obtenu des algorithmes efficaces, comme expliqué au §2.1.1), tandis que le décodage peut se réaliser à l'aide d'une variante de l'algorithme d'Euclide. En contrepartie, un des inconvénients des codes de Gabidulin est que leur dimension (qui est d) est nécessairement majorée par r. Autrement dit, construire de longs codes nécessite de travailler avec de grandes extensions, ce qui conduit souvent à des lenteurs algorithmiques.

Des codes de Gabidulin de grande longueur. Une extension des codes de Gabidulin, qui m'est apparue naturelle après le travail du §2.1.1, consiste à remplacer le morphisme d'évaluation ev par les morphismes ev_λ, c'est-à-dire l'application (1) par :

$$\begin{array}{rcl} K[X,\theta,0]_{<d} & \longrightarrow & K^r \times \cdots \times K^r = K^{rm} \\ P(X) & \mapsto & \big(P(\lambda_j\theta)(a_i)\big)_{1\leqslant i\leqslant r, 1\leqslant j\leqslant m} \end{array} \tag{2}$$

où les λ_j $(1 \leqslant j \leqslant m)$ sont des éléments fixés de K et $(a_1, \dots, a_r)$ est, comme précédemment, une base de K sur F. L'idée est séduisante car cette construction permet *a priori* d'envisager des codes de longueur dépassant largement r.

Dans ce contexte généralisé, il se trouve que la distance pertinente sur K^{rm} est un mélange entre la distance rang introduite précédemment et la distance de Hamming, classique en théorie du codage. Pour des éléments $x_{i,j} \in K$, elle est définie par :

$$w_{\mathrm{rH}}\big((x_{i,j})_{1\leqslant i\leqslant r, 1\leqslant j\leqslant m}\big) = \sum_{j=1}^{m} \dim_F \left(Fx_{1,j} + \cdots + Fx_{r,j}\right)$$

où la somme d'espaces vectoriels $Fx_{1,j} + \cdots + Fx_{r,j}$ est calculée dans l'espace ambiant K. Avec cette définition, lorsque $r = 1$, on retombe sur les codes de Reed–Salomon traditionnels. Sans hypothèse sur r, je démontre le théorème suivant qui indique, une nouvelle fois, que les codes définis ci-dessus atteignent la borne de Singleton.

Théorème 3. *On suppose que $d \leqslant mr$ et que les $N_{K/F}(\lambda_i)$ sont deux à deux disjoints.*
Alors la distance minimale du code défini par l'application (2) est $mr - d + 1$.

De plus, j'obtiens des algorithmes de codage et de décodage des codes de Gabidulin généralisés qui conservent la même efficacité que dans le cas classique.

Des codes de Gabidulin avec dérivation. À la suite de ce travail, j'ai proposé à un étudiant de M2, Amaury Durand, d'étudier le cas des anneaux de Ore généraux $K[X,\theta,\partial]$ où la θ-dérivation ∂ est possiblement non nulle. Pour ce faire, la première étape a été de comprendre quel était le bon analogue des morphismes d'évaluation. À cet effet, nous avons remarqué qu'afin que l'application $P(X) \mapsto P(f)$ soit un morphisme d'anneaux, il faut et il suffit que l'application $f : K \to K$ vérifie l'axiome :

$$\forall a, b \in K, \quad f(ab) = \theta(a)f(b) + f(a)b$$

c'est-à-dire, dans le langage de Ore, que f soit un pseudo-endomorphisme de K. La classification de telles applications est un exercice facile, dont la conclusion est résumée par le lemme suivant.

Lemme 4. *Avec les notations précédentes, les pseudo-endomorphismes de K sont les applications de la forme $\partial + \lambda\theta$ avec $\lambda \in K$.*

Ce résultat nous a conduit à considérer les applications d'évaluation ev_λ ainsi définies :

$$\begin{array}{rccc} \mathrm{ev}_\lambda : & K[X,\theta,\partial] & \longrightarrow & \mathrm{End}_F(K) \\ & P(X) & \mapsto & P(\partial + \lambda\theta) \end{array}$$

où F est maintenant défini comme le sous-corps de K formé des éléments x tels que $\theta(x) = x$ et $\partial(x) = 0$. (Notons que lorsque $\theta \neq \mathrm{id}$, la seconde condition est impliquée par la première.) Étant donnés des scalaires $\lambda_1, \dots, \lambda_m \in K$ et une base $(a_1, \dots, a_r)$ de K sur F, nous avons ensuite défini le code de Gabidulin généralisé comme l'image de l'application :

$$\begin{array}{ccc} K[X,\theta,\partial]_{<d} & \longrightarrow & K^r \times \cdots \times K^r = K^{rm} \\ P(X) & \mapsto & \big(P(\partial + \lambda_j\theta)(a_i)\big)_{1\leqslant i\leqslant r, 1\leqslant j\leqslant m}. \end{array} \tag{3}$$

Enfin, nous avons démontré une extension du théorème 3 à ce cadre (bien que l'hypothèse sur les λ_j soit plus délicate à exprimer), et avons proposé des algorithmes de codage et de décodage efficaces.

Vers les codes de Gabidulin géométriques. Les constructions (2) et (3) que je viens de présenter peuvent être vues comme une mise en famille des codes de Gabidulin, la famille étant indexée par le paramètre λ variant dans K. Géométriquement, cela correspond à des codes de Gabidulin définis sur la droite affine là où les codes de Gabidulin traditionnels n'étaient définis que sur un point.

Afin d'aller plus loin dans cette direction, il me semble intéressant, à l'instar de ce qui se fait pour les codes de Reed–Solomon, de chercher à définir — puis à étudier — des codes de Gabidulin sur des objets géométriques plus généraux que la droite affine, en commençant par les courbes algébriques.

J'ai proposé à Amaury Durand de travailler en thèse sur ce sujet. Malheureusement, nous n'avons pour le moment pas obtenu de financement. Par conséquent, la thèse ne pourra donc pas débuter en septembre 2018. Un report à septembre 2019 semble toutefois tout à fait envisageable.

2.1.3 Rédaction de notes de cours

Référence :

[2] X. Caruso, *Polynômes de Ore en une variable*

Au printemps 2017, j'ai donné un cours d'école doctorale sur les polynômes de Ore, avec un regard particulier sur la structure d'algèbre d'Azumaya sous-jacente. J'ai rédigé, par la suite, des notes de cours étendues (complétant largement ce que j'ai eu le temps de traiter à l'oral), qui atteignent à présent une petite centaine de pages.

Avant de proposer ces notes pour publication, j'ai le projet d'y ajouter encore deux parties : l'une portant sur le théorème de structure de Jacobson des modules de type fini sur les anneaux de Ore et l'autre portant sur les application des polynômes de Ore à la théorie des codes correcteurs d'erreurs (*cf* §2.1.2).

2.2 Algorithmique p-adique

Ma recherche de ces cinq derniers semestres a été également largement occupée par l'étude du suivi de la précision dans le monde p-adique et la programmation d'outils offrant un suivi de précision très fin. Ces travaux apparaissent comme la suite logique de travaux antérieurs que j'avais réalisés avec David Roe et Tristan Vaccon et que j'avais présentés dans mon dernier rapport d'activités.

2.2.1 Précision sur le polynôme caractéristique

Référence :

[5] X. Caruso, D. Roe, T. Vaccon, *Characteristic polynomials of p-adic matrices*

Tout d'abord, poursuivant nos travaux sur l'algèbre linéaire p-adique (présentés dans mon dernier rapport d'activités), nous nous sommes intéressés, David Roe, Tristan Vaccon et moi-même, à la précision

optimale sur le polynôme caractéristique d'une matrice dont les coefficients ne sont pas connus de manière exacte. À la lumière de la théorie que nous avons développés, la question posée revient à estimer la différentielle de l'application

$$\begin{array}{rccc} \chi & : M_n(\mathbb{Q}_p) & \longrightarrow & \mathbb{Q}_p[X] \\ & M & \mapsto & \det(X\mathrm{I}_n - M) \end{array}$$

Un calcul classique montre que la différentielle de χ au point M, notée $d\chi_M$, est donnée par la formule $d\chi_M(dM) = \mathrm{Tr}\big(\mathrm{Adj}(X\mathrm{I}_n - M) \cdot dM\big)$ où Adj désigne la matrice adjointe, c'est-à-dire la transposée de la matrice des cofacteurs.

Nous proposons un premier algorithme pour le calcul de $\mathrm{Adj}(X\mathrm{I}_n - M)$, qui repose sur l'obtention d'une forme de Hessenberg de la matrice M. Cet algorithme a une complexité cubique en n et n'effectue pas de division dans $\mathbb{Q}_p$. La complexité cubique est à la fois satisfaisante par certains aspects mais aussi difficilement acceptable par d'autres. En effet, elle est satisfaisante car elle paraît optimale puisque la taille de la sortie est, elle-même, cubique en n. En contrepartie, le calcul du polynôme caractéristique ne coûte que $O(n^\omega)$ opérations dans $\mathbb{Q}_p$, ce qui signifie que le goulot d'étrangement, avec cette approche, devient le calcul de la précision — et pas celui de la réponse elle-même.

Pour palier à cet écueil, nous avons montré que la matrice $\mathrm{Adj}(X\mathrm{I}_n - M)$ pouvait être représentée sous une forme compacte ne faisant intervenir que $O(n^2)$ coefficients. Précisément, nous démontrons que, dès lors que M admet un vecteur cyclique, il existe deux matrices $P, Q \in \mathrm{GL}_n(\mathbb{Z}_p)$ et un polynôme $\alpha \in \mathbb{Q}_p[X]$ tels que :

$$\mathrm{Adj}(X\mathrm{I}_n - M) = \alpha \cdot P \cdot \begin{pmatrix} 1 & X & \cdots & X^{n-1} \\ X & X^2 & \cdots & X^n \\ \vdots & \vdots & & \vdots \\ X^{n-1} & X^n & \cdots & X^{2n-2} \end{pmatrix} \cdot Q \mod \chi_M.$$

De plus, les matrices P et Q s'obtiennent à partir de la forme normale de Frobenius de M, pour laquelle on dispose d'algorithmes de calcul rapides en $O(n^\omega)$. *In fine*, nous obtenons un algorithme de calcul de la précision optimale sur le polynôme caractéristique qui ne coûte que $O(n^\omega)$ opérations dans $\mathbb{Q}_p$ (mais effectue des divisions) et n'est donc pas plus cher que le calcul du polynôme caractéristique lui-même.

Nous avons appliqué nos résultats pour tester la stabilité numérique des méthodes traditionnelles de calcul du polynôme caractéristique avec des matrices aléatoires sur $\mathbb{Q}_p$, dont les coefficients ont des ordres de grandeur variables. Il ressort de notre étude que la plupart d'entre elles sont fortement instables numériquement. Par exemple, pour des matrices de taille 8, la perte de précision relative optimale est en moyenne de $3{,}17$ chiffres significatifs, là où les algorithmes usuels affichent une perte pouvant aller jusqu'à 200 chiffres.

Dans le cas du calcul du déterminant (plus simple), le calcul préliminaire d'une forme normale de Smith de M permet de concevoir des algorithmes stables qui affichent une perte de précision générique proche de l'optimal. Peut-on adapter ces techniques pour le polynôme caractéristique ? Il s'agit d'une question qui reste ouverte sur laquelle nous aimerions revenir prochainement.

2.2.2 Le package ZpL

Références :

[9] X. Caruso, D. Roe, T. Vaccon, *ZpL : a p-adic precision package*

[14] X. Caruso, D. Roe, J. Rüth, *ZpL : a p-adic precision package*, librairie SageMath (2018)

Comme rappelé brièvement au §2.2.1 ci-dessus, dans notre premier travail avec David Roe et Tristan Vaccon, nous proposions d'utiliser des méthodes différentielles pour réaliser le suivi de précision p-adique. Précisément, nous proposions de modéliser la précision sur un d-uplet de variables p-adiques par un $\mathbb{Z}_p$-réseau dans $\mathbb{Q}_p^d$ et, de faire évoluer le réseau de précision, au fur et à mesure des calculs, en appliquant la différentielle des opérations effectuées.

L'idée d'implémenter cette approche était présente dès nos premières publications, en 2014. Toutefois, s'investir dans cette direction demandait du travail et le bénéfice escompté n'était pas évident *a priori*. En effet, le maintien du réseau de précision est coûteux, à la fois en taille et en temps, et il me semblait alors absolument déraisonnable de travailler en arrière plan avec des matrices 100×100 (servant à modéliser la

précision) lorsque l'utilisateur ne manipule que des matrices 10×10. J'ai toutefois franchi le pas une nuit de l'été 2017, alors que je participais à des SAGEDAYS sur les nombres p-adiques à l'université de Vermont, aux États-Unis. C'est alors que j'ai produit une première version de ce qui deviendra le package ZpL.

À mon étonnement, les premiers résultats ont été plutôt encourageants. Alors que je ne pensais être capable de manipuler au maximum une poignée de variables, mon implémentation (qui n'était pourtant pas du tout optimisée) parvenait à calculer le polynôme caractéristique d'une matrice 8×8 en un temps raisonnable, et produisait bien sûr — c'était le but de la manœuvre — un résultat optimalement précis. Avec l'aide de David Roe et de Julian Rüth, j'ai repris et peaufiné mon implémentation qui est, maintenant, intégrée au logiciel de calcul formel SAGEMATH. Une démonstration des possibilités de notre package est disponible en ligne à cette adresse :

http://xavier.toonywood.org/softwares/ZpL-demo.html

Les temps de calcul ne sont pas encore satisfaisants. Il reste encore un gros travail d'optimisation à faire, que nous prévoyons de réaliser à l'automne prochain.

En complémement de cela, avec David Roe et Tristan Vaccon, nous avons entâmé une étude théorique systématique des algorithmes sous-jacents au package ZpL. Nous avons montré que son impact sur la complexité est au plus quadratique, et généralement plus faible que cela pour des algorithmes sous-optimaux.

2.2.3 Rédaction de notes de cours

Référence :

[1] X. Caruso, *Computations with p-adic numbers*

J'ai été invité, en janvier 2017, à donner un cours aux *Journées Nationales de Calcul Formel* sur le calcul numérique p-adique. À cette occasion, il m'a été demandé de rédiger des notes de cours. Ces notes sont disponibles sur HAL/arXiv, ainsi que sur ma page web mais, bien que déjà relativement fournies (plus de 80 pages), je ne les ai pas encore soumises à publication car je voudrais les compléter pour en faire un livre de référence sur le sujet, qui pourrait être coécrit avec David Roe et Tristan Vaccon.

2.3 Miscallenous

2.3.1 Ensembles de Kakeya p-adiques

Référence :

[12] X. Caruso, *Almost all non-archimedean Kakeya sets have measure zero*

De manière plus anecdotique, je me suis également intéressé, pendant l'été 2016, aux ensembles de Kakeya p-adiques aléatoires. Rappelons que, dans le cas réel, un ensemble de Kakeya est un sous-ensemble de $\mathbb{R}^d$ balayé par une aiguille de longueur 1 qui tourne de manière continue sur elle-même en passant par toutes les directions de l'espace. Besikovitch a démontré au début du 20ème siècle qu'il existe des ensembles de Kakeya de mesure arbitrairement petite. Les ensembles de Kakeya, qui sont ensuite restés un moment dans l'oubli, connaissent une seconde jeunesse depuis plusieurs décennies en raison des liens étroits qu'ils entretiennent avec certaines problèmes centraux en analyse harmonique.

En particulier, la question de Kakeya a été posée sur d'autres corps ; le cas le plus célèbre est probablement celui des corps finis [1] mais le cas des corps non archimédiens a également été évoqué par Ellenberg, Oberlin et Tao. Dans le cas de $\mathbb{Q}_p$, la question peut se formuler ainsi : existe-t-il une fonction *continue* $f : \mathbb{S}^{d-1}(\mathbb{Q}_p) \to \mathbb{Q}_p^d$ (où $\mathbb{S}^{d-1}(\mathbb{Q}_p)$ est la sphère unité de $\mathbb{Q}_p^d$ pour la norme infinie) pour laquelle l'ensemble

$$K(f) = \big\{ta + f(a) \ : \ a \in \mathbb{S}^{d-1}(\mathbb{Q}_p),\, t \in \mathbb{Z}_p\big\}$$

soit de mesure nulle. Dummit et Hablicsek ont apporté une réponse positive en exhibant une fonction f particulière répondant à la question. De mon côté, j'ai considéré la question sous un angle probabilisite et ai obtenu le théorème suivant.

1. Sur les corps finis, la question se formule ainsi : existe-t-il une constante c_d pour laquelle tout sous-ensemble de $\mathbb{F}_q^d$ contenant une droite affine dans chaque direction a au moins $c_d q^d$ éléments. Dans un article célèbre, Dvir a apporté une réponse affirmative à cette question (avec $c_d = \frac{1}{d!}$) grâce à ce que l'on appelle désormais la *méthode polynômiale*.

Théorème 5. *Pour presque toute fonction 1-lipschitzienne $f : \mathbb{S}^{d-1}(\mathbb{Q}_p) \to \mathbb{Z}_p^d$, l'ensemble $K(f)$ est de mesure nulle.*

La démonstration du théorème 5 repose sur des arguments combinatoires. En effet, la condition « 1-lipschitzien » permet de se ramener directement à des ensembles de Kakeya sur $\mathbb{Z}/p^n\mathbb{Z}$ et ainsi à des structures finies. La suite de la démonstration consiste à estimer le cardinal moyen d'un ensemble d'un Kakeya modulo p^n. Ceux-ci s'écrivant par définition comme une union de segments, j'utilise la formule d'inclusion-exclusion et me retrouve ainsi à déterminer le cardinal moyen de l'intersection de k segments aléatoires dans $\mathbb{Z}/p^n\mathbb{Z}$. La question devient alors un problème d'arithmétique que je résous par des méthodes usuelles de congruences. Mettant tout ensemble, j'obtiens une formule *exacte* pour le cardinal moyen d'un ensemble d'un Kakeya sur $\mathbb{Z}/p^n\mathbb{Z}$, et j'observe que celle-ci converge vers 0 lorsque n tend vers l'infini. J'en déduis que la mesure d'un ensemble de Kakeya p-adique est nulle en moyenne et, par suite, nulle presque surement.

2.3.2 Séries algébriques en caractéristique positive

Référence :
[10] A. Bostan, X. Caruso, G. Christol, P. Dumas, *Fast coefficient computation for algebraic power series in positive characteristic*

En collaboration avec Alin Bostan, Gilles Christol et Philippe Dumas, nous nous sommes intéressés au calcul efficace du N-ième coefficient d'une série algébrique en caractéristique positive. L'origine de cette question est un théorème de Christol qui affirme que si la série

$$f(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_N t^N + \cdots \in \mathbb{F}_p[[t]]$$

est algébrique sur $\mathbb{F}_p(t)$, alors la suite de ces coefficients est p-automatique. *Grosso modo*, cela signifie qu'il existe un automate qui lit l'écriture de N en base p et « produit » le coefficient a_N. Adoptant un point de vue plus algébrique, la conclusion du théorème de Christol peut se reformuler comme suit : il existe un $\mathbb{F}_p$-espace vectoriel de dimension finie qui contient f et qui est stable par les opérateurs de section S_r ($0 \leqslant r < p$) définis par :

$$S_r\big(a_0 + a_1 t + a_2 t^2 + \cdots\big) = a_r + a_{r+p} t + a_{r+2p} t^2 + \cdots$$

Quelle que soit la formulation, il résulte du théorème de Christol qu'il existe un algorithme de complexité $O(\log N)$ qui calcule a_N. Toutefois, la dépendance de la complexité d'un tel algorithme en fonction des autres paramètres qui entrent en jeu — le nombre premier p, le degré du polynôme minimal de $f(t)$, la hauteur de $f(t)$ — n'est pas claire.

Nous avons souhaité comprendre cette dépendance et, si possible, l'améliorer. Pour cela, nous avons démontré une version *effective* du théorème de Christol qui exhibe un espace de confinement explicite et facilement calculable.

Théorème 6 (Version effective du théorème de Christol)**.** *Soit $f(t) \in \mathbb{F}_p[[t]]$ une série entière. On suppose qu'il existe un polynôme irréductible $E(t, y) \in \mathbb{F}_p[t, y]$ tel que $E(t, f(t)) = 0$. Soient $h = \deg_t E$ et $d = \deg_y E$. Alors le $\mathbb{F}_p$-espace vectoriel*

$$\left\{ \sum_{i=0}^{d-1} a_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))} \quad \text{avec} \quad a_i(t) \in \mathbb{F}_p[t],\ \deg a_i(t) < h \right\}$$

est stable par les opérateurs de section S_r.

Forts de ce résultat, l'idée pour calculer efficacement le N-ième coefficient du développement de $f(t)$ est simple. On écrit la décomposition de N en base p, à savoir $N = N_0 + N_1 p + \cdots + N_\ell p^\ell$, puis on remarque que a_N est la coefficient constant de

$$S_{N_\ell} \circ \cdots \circ S_{N_1} \circ S_{N_0}(f(t)).$$

En outre, chaque valeur intermédiaire $S_{N_i} \circ \cdots \circ S_{N_0}(f(t))$ vit dans l'espace de confinement donné par le théorème 6. Il suffit donc d'expliquer comment calculer l'image par S_r d'un élément de la forme $\sum_{i=0}^{d-1} a_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t,f(t))}$ avec $\deg a_i(t) < h$. Or le théorème 6 assure que l'on a une écriture :

$$S_r\left(\sum_{i=0}^{d-1} a_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t,f(t))}\right) = \sum_{i=0}^{d-1} b_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t,f(t))} \tag{4}$$

avec $\deg b_i(t) < h$. On peut voir l'équation (4) comme un système linéaire (structuré) en les coefficients de $b_i(t)$, système que l'on peut résoudre dès lors que l'on connaît la série $f(t)$ à précision suffisamment grande. Une étude plus précise montre que les $2dhp$ premiers coefficients de $f(t)$ sont suffisants. Déroulant cette idée, on aboutit à un algorithme de complexité $\tilde{O}(d^2hp) + O(d^2h^2 \log N)$ pour le calcul de a_N.

La complexité obtenue vis-à-vis des paramètres d, h et N est entièrement satisfaisante. Elle l'est par contre moins pour ce qui concerne la variable p ; en effet, le paramètre pertinent est $\log p$, ce qui signifie que notre algorithme a une complexité exponentielle vis-à-vis de p. Dans le même article, Alin Bostan, Gilles Christol, Philippe Dumas et moi-même proposons un second algorithme de calcul de a_N qui combine des méthodes p-adiques et des méthodes d'équations différentielles. Celui-ci reste polynômial en d et h (avec des exposants plus élévés que précédemment) et a une complexité quasi-linéaire en $\sqrt{p}$ (ce qui est, semble-t-il, le mieux que l'on puisse espérer avec la technologie actuelle).

3 Enseignement, formation et diffusion de la culture scientifique

Enseignement et formation

Cours dispensés

Voici, par ordre chronologique, la liste des cours que j'ai donnés au cours des cinq derniers semestres

Analyse, probabilités et informatique avec les nombres p-adiques (niveau D) : il s'agit d'un corps d'école doctorale ; j'y ai tout d'abord introduit les nombres p-adiques, puis j'ai présenté quelques résultats les concernant en essayant de rester le plus en dehors de la théorie des nombres : j'ai traité la théorie des fonctions continues (resp. dérivables) d'une variable p-adique, j'ai mentionné quelques résultats sur les matrices et les polynômes p-adiques aléatoires puis j'ai étudié la stabilité numérique de quelques algorithmes p-adiques (*e.g.* élimination de Gauss) ;

Arithmétique (niveau L1) : il s'agit d'un cours d'introduction à la logique mathématique (connecteurs logiques, quantificateurs, *etc.*), aux ensembles, aux fonctions, puis aux congruences ;

Polynômes de Ore (niveau D) : il s'agit d'un cours d'école doctorale ; j'y ai introduit les polynômes de Ore (*cf* §2.1) et ai montré comment ceux-ci étaient liés à l'algèbre linéaire *via* la notion d'algèbre d'Azumaya ; une fois ces faits établis, dans un deuxième temps, j'ai entâmé une étude fine des propriétés de factorisation des polynômes de Ore ;

Mathématiques pour les informaticiens (niveau L3) : il s'agit d'un cours, à forte composante mathématique, dispensé aux étudiants en informatique en première année de l'ENS de Rennes ; j'ai choisi de traiter les algorithmes de multiplication rapide des entiers et les polynômes, les corps finis puis quelques brides de la théorie des codes correcteurs d'erreurs ;

Codes géométriques (niveau D) : il s'agit d'un cours d'école doctorale dont l'objectif était de présenter la théorie des codes géométriques telle qu'elle apparaît dans le livre de Tsfasman, Vlăduţ et Nogin ; le cours comprenait une partie importante de rappels, d'une part, sur les codes correcteurs d'erreurs et, d'autre part, sur la théorie des courbes algébriques.

Encadrement de stages

Durant les cinq derniers semestres, j'ai également encadré, à tous les niveaux, plusieurs stages de découverte des mathématiques ou de recherche. En voici la liste.

Fanny Serre (niveau L2) : le sujet proposé était l'étude des courbes elliptiques ; sans véritablement rentrer dans les démonstrations, nous avons d'abord exploré les courbes elliptiques complexes puis, dans un second temps, les propriétés arithmétiques des courbes elliptiques définies sur les corps de nombres ;

Dorian Berger (niveau L3) : le sujet du stage était la correspondance entre les revêtements ramifiés de la sphère de Riemann, d'une part, et les extensions finies de $\mathbb{C}(t)$, d'autre part ; cela nous a permis ensuite d'étudier les corps de nombres à la lumière de cette correspondance ;

Huu Phuoc Le (niveau M1) : le sujet du stage était de réaliser une implémentation efficace des entiers 2-adiques sur machine, en essayant de tirer profit, autant que possible, des flottants ;

Amaury Durand (niveau M2) : le sujet du stage était d'étendre la théorie des codes de Gabidulin au cas où l'anneau de Ore sous-jacent est défini par une dérivation non triviale ; je renvoie au §2.1.2 pour de nombreux compléments concernant les résultats obtenus lors de ce stage.

Organisation de séminaires et d'événements

Séminaire de l'équipe « Géométrie et algèbre effectives »

À la rentrée de septembre 2015, les équipes de géométrie à l'IRMAR ont été réorganisées et, en particulier, a été créée l'équipe de *Géométrie et algèbre effectives*.

J'ai demandé mon rattachement à 50% à cette nouvelle équipe (qui m'a été accordé) et me suis proposé pour coorganiser le séminaire de l'équipe. J'ai accompli cette tâche pendant deux ans, au côté de Delphine Boucher puis, pendant un an, au côté d'Élisa Lorenzo-García.

Les 5 minutes Lebesgue

Depuis novembre 2015, je suis le cofondateur et le coorganisateur avec San Vũ Ngọc, Benoît Grébert et Baptiste Chantraine du séminaire hebdomadaire « Les 5 minutes Lebesgue ». Il s'agit d'un séminaire d'un genre particulier puisque les exposés ne durent que cinq minutes mais sont filmés puis mis en ligne sur le site du CHL et sur YouTube. Depuis le début de lancement, 76 vidéos ont été réalisées et mises en ligne. Épisodiquement, ces vidéos sont relayées sur la revue en ligne *Images des mathématiques*.

Je me suis, moi-même, essayé deux fois à l'exercice en donnant un exposé dans ce cadre sur les nombres p-adiques et un autre où je présente, en duo avec Vincent Duchêne, deux jeux mathématiques.

Le forum des mathématiques vivantes

Le *Forum des mathématiques vivantes* est une manifestement biannuelle qui a lieu dans certaines villes de France et est coordonnée à l'échelle nationale par la CFEM (Commission Française pour l'Enseignement des Mathématiques).

En 2017, notre laboratoire, en collaboration avec le rectorat et l'IREM, a organisé cette manifestation à Rennes. Au programme, nous avions le projection du film *Pourquoi j'ai détesté les maths*, de nombreux ateliers et conférences en centre-ville, une troupe de théâtre qui a évoqué des questionnements autour de l'égalité homme-femme, *etc.*

Je me suis moi-même impliqué dans l'organisation de cet événement d'ampleur. J'ai réalisé le site web `http://rennes.forum-maths-vivantes.fr/` et ai tenu, le jour venu, le stand des *5 minutes Lebesgue* sur la place Hoche à Rennes.

MATh.en.JEANS

En 2017 et en 2018, j'ai encadré plusieurs groupes d'élèves de collège et du lycée du centre scolaire Saint Mangloire à Dol de Bretagne. Les sujets que j'ai proposés étaient *Le paradoxe des anniversaires*, *Le problème des huit dames sur un jeu d'échecs*, *L'aiguille de Kakeya*, *Retrouver une fraction à partir de son écriture décimale*.

Après avoir travaillé une année (voire plus) sur le sujet, les élèves sont venus présenter leurs découvertes au congrès MATh.en.JEANS à Nantes. Globalement, je garde un très bon souvenir de cette expérience ; j'ai

trouvé les élèves (pour la plupart) motivés et dynamiques et il était toujours très intéressant d'échanger nos points de vue. L'étape de restitution a également toujours été très réussi, ai-je trouvé.

4 Transfert technologique, relations industrielles et valorisation

5 Encadrement, animation et management de la recherche

Projets ANR

Le projet CLap–CLap

Cela fait trois années consécutives que je soumets, en tant que coordinateur, un projet ANR intitulé « Correspondance de Langlands p-adique : une approche constructive et algorithmique » (CLap–CLap). Ce projet regroupe une vingtaine de chercheurs sur quatre sites : Bordeaux, Lyon, Paris et Rennes.

Les retours de l'ANR sont très aléatoires.

Activités éditoriales

Les Annales Henri Lebesgue

Nous le savons, les problèmatiques de l'édition scientifique occupent une place de plus en plus importante dans les inquiétudes de la communauté mathématique. De nombreux collègues ont signé l'appel de Jussieu pour la science ouverte et la bibliodiversité ; le conseil scientifique du CNRS a diffusé un certain nombre de recommandations à propos du droit d'auteur, de l'archivage, *etc.* ; plusieurs universités ont résilié leur abonnement Springer.

Dans le périmètre du centre Henri Lebesgue, nous sommes également très sensibles à ces préoccupations et, afin d'apporter notre contribution au combat contre les éditeurs commerciaux, nous avons très récemment lancé une nouvelle revue aux pratiques « vertueuses » : les Annales Henri Lebesgue. Cette revue est généraliste (mathématiques pures et appliquées) et purement électronique. Elle est entièrement gratuite pour l'auteur et le lecteur. Elle est dirigée par des collègues, qui ont pour uniques objectifs la diffusion, la valorisation et l'archivage des travaux mathématiques.

À titre personnel, je suis éditeur des Annales Henri Lebesgue et également coordinateur du pôle géométrie de la revue. Depuis septembre 2017, je me suis énormément investi pour que cette revue puisse naître et prospérer dans les meilleures conditions ; en particulier, je suis l'un des principaux auteurs du site web `annales.lebesgue.fr`, je suis coauteur d'un article d'annonce paru dans la *Gazette des Mathématiciens* et j'ai réalisé un clip publicitaire de 4 minutes pour faire la promotion de la revue.

Je ne peux donc que vous encourager à y soumettre vos meilleurs articles `:-)`.

Ma bibliographie des cinq derniers semestres

Notes de cours écrites pendant les 5 derniers semestres

[1] X. Caruso, *Computations with p-adic numbers*, notes de cours (2017), 83 pages

[2] X. Caruso, *Polynômes de Ore en une variable*, notes de cours (2017), 92 pages

Articles de recherche publiés pendant les 5 derniers semestres

[3] X. Caruso, D. Roe, T. Vaccon, *Division and slope factorization of p-adic polynomials*, proceddings de la conférence ISSAC 2016

[4] X. Caruso, A. David, A. Mézard, *Variétés de Kisin stratifiées et déformations potentiellement Barsotti–Tate*, J. Inst. Math. Jussieu (2016), https://doi.org/10.1017/S1474748016000232

[5] X. Caruso, D. Roe, T. Vaccon, *Characteristic polynomials of p-adic matrices*, proceddings de la conférence ISSAC 2017

[6] X. Caruso, J. Le Borgne, *Fast multiplication for skew polynomials*, proceddings de la conférence ISSAC 2017

[7] X. Caruso, J. Le Borgne, *A new faster algorithm for factoring skew polynomials over finite fields*, J. Symbolic Comput. **79** (2017), 411–443

[8] X. Caruso, *Numerical stability of Euclidean algorithm over ultrametric fields*, J. Number Theor. Bordeaux **29** (2017), 503–534

[9] X. Caruso, D. Roe, T. Vaccon, *ZpL : a p-adic precision package*, proceddings de la conférence ISSAC 2018

[10] A. Bostan, X. Caruso, G. Christol, P. Dumas, *Fast coefficient computation for algebraic power series in positive characteristic*, proceddings de la conférence ANTS 2018

[11] X. Caruso, A. David, A. Mézard, *Un calcul d'anneaux de déformations potentiellement Barsotti–Tate*, Trans. Amer. Math. Soc. **370** (2018), 6041–6096

[12] X. Caruso, *Almost all non-archimedean Kakeya sets have measure zero*, à paraître à Confluentes Math.

Logiciels écrits pendant les 5 derniers semestres

[13] X. Caruso, *Algorithmes rapides pour le calcul du logarithme et de l'exponentielle p-adique*, librairie SageMath (2017), https://trac.sagemath.org/ticket/23043 et https://trac.sagemath.org/ticket/23235, $\sim$ 500 lignes

[14] X. Caruso, D. Roe, J. Rüth, *ZpL : a p-adic precision package*, librairie SageMath (2018), https://trac.sagemath.org/ticket/23505, $\sim$ 2000 lignes

Articles publicitaires écrits pendant les 5 derniers semestres

[15] X. Caruso, *Mathematic Park*, Gazette des Mathématiciens **148** (2016)

[16] X. Caruso, B. Grébert, X. Lachambre, S. Vũ Ngọc, *Les 5 minutes Lebesgue*, Gazette des Mathématiciens **151** (2017)

[17] D. Cerveau, X. Caruso, S. Gouëzel, X. Lachambre, N. Raymond, S. Vũ Ngọc, *Les annales Henri Lebesgue*, Gazette des Mathématiciens **155** (2018)

[18] X. Caruso, *Les annales Henri Lebesgue*, vidéo de promotion du journal (2018),
version française : https://annales.lebesgue.fr/video/promoAHL-fr.mp4
version anglaise : https://annales.lebesgue.fr/video/promoAHL-en.mp4

Quelques travaux en cours

[19] X. Caruso, *Slope factorization of Ore polynomials*, en préparation

[20] X. Caruso, *Zeros of random p-adic polynomials*, en préparation

[21] X. Caruso, A. Durand, *Gabidulin codes with large length*, en préparation