Rapport à vague de Xavier Caruso

Période : décembre 2015 — décembre 2020

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, trois enfants

Parcours scolaire et professionnel

2018– Directeur de recherche au CNRS, affecté à l'IMB (Bordeaux)

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

2006–2018 Chargé de recherche au CNRS, affecté à l'IRMAR (Rennes)

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

2020– Membre nommé du CNU

2018–2022 Membre nommé du conseil de l'IMB

2018–2022 Coordinateur du projet ANR CLap–CLap (Correspondance de Langlands p-adique : une approche constructive et algorithmique)

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

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

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)

2 RECHERCHE SCIENTIFIQUE

Mes travaux de recherche de ces cinq dernières années ont touché plusieurs thématiques, plus ou moins directement reliées entre elles. Le fil directeur de mes recherches reste toutefois toujours centré sur l'étude algorithmique des objets les plus courants rencontrés en théorie de Hodge p-adique. Parmi ceux-ci, on peut citer bien sûr les représentations galoisiennes p-adiques, mais aussi les φ-modules (ou, de manière équivalente, les applications semi-linéaires par rapport au Frobenius) et les équations différentielles p-adiques que j'approche généralement *via* la théorie des polynômes non commutatifs de Ore.

Régulièrement, toutefois, je m'autorise de petites escapades soit vers la théorie des codes correcteurs d'erreurs (qui, pour la partie que je regarde, utilise abondamment les polynômes de Ore), soit vers les probabilités (dont l'étude est intéressante pour analyser le comportement en moyenne de certaines algorithmes).

2.1 Polynômes de Ore

Dans tout cette partie, la lettre K désigne un corps fixé muni d'un morphisme d'anneaux $\theta : K \to K$. À ces données, on associe l'anneau de Ore $K[X;\theta]$ 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 $X \cdot a = \theta(a)X$, 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 $K[X;\theta]$.

Les éléments de $K[X;\theta]$ sont souvent appelés *polynômes tordus* ou *polynômes de Ore*. Ils interviennent naturellement comme polynômes d'opérateurs d'applications semi-linéaires et sont, à ce titre, étroitement reliés à la réduction des endomorphismes semi-linéaires d'un espace vectoriel sur K.

2.1.1 Multiplication rapide des polynômes tordus

Référence :
[4] 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 tordus dans le cas particulier où 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.

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 :

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

On vérifie que c'est un morphisme d'anneaux qui induit un isomorphisme entre $K[X;\theta]/(X^r-1)$ 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 $A(X) = a_0 + a_1X + \cdots + a_{r-1}X^{r-1} \in K[X;\theta]$ 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 tordus 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 :

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

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 $K[X;\theta]/(X^r-N_{K/F}(\lambda))$ et $\mathrm{End}_F(K)$. Comme précédemment, il se trouve que celui-ci, ainsi que son inverse, sont calculables très efficacement. La multiplication dans $K[X;\theta]/(X^r-N_{K/F}(\lambda))$ 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 tordus de $K[X;\theta]$ 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 résultat (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 tordus, le calcul du PGCD, la multi-évaluation et l'interpolation. Comme conséquence directe, nous en déduisons des algorithmes efficaces pour le codage et le décodage des codes de Gabidulin.

2.1.2 Une théorie des résidus pour les polynômes tordus

Référence :

[17] X. Caruso, *Residues of skew rational functions and linearized Goppa codes*

Dans le cadre classique, les polynômes présentent en même temps une saveur algébrique et une saveur analytique puisqu'ils définissent des fonctions d'une variable qui peuvent être dérivées, intégrées, *etc.*

Loin d'être disjoints, ces deux aspects sont complémentaires et il arrive souvent qu'une argumentation mettant en œuvre des outils algébriques ait des conséquences analytiques et *vice versa*. En particulier, la théorie des résidus apparaît classiquement comme un outil extrêmement puissant pour l'étude des formes différentielles aussi bien en géométrie analytique qu'en géométrie algébrique. Dans le cadre des polynômes tordus, il est naturel d'espérer que de telles situations se reproduisent. Toutefois, la théorie analytique des polynômes tordus n'a, semble-t-il, pas réellement été développée jusqu'à présent. J'ai donc décidé de m'atteler à la tâche en me focalisant, pour commencer, sur la théorie des résidus pour laquelle j'avais une application en vue aux codes de Reed–Solomon linéarisés.

Comme au §2.1.1, je me place sous l'hypothèse que l'automorphisme θ est d'ordre fini r et j'appelle F le sous-corps de K fixé par θ. Je considère également l'élément central $Y = X^r$ et j'introduis la dérivation $\partial = \frac{d}{dY}$ sur $k[X^{\pm 1};\theta]$ definie comme suit :

$$\partial\Big(\sum_i a_i X^i\Big) = r^{-1} \cdot \sum_i i a_i X^{i-r}.$$

Comme on le constate, cette dérivation n'est définie que lorsque r est premier avec p ; dans la suite, je ferai cette hypothèse pour simplifier l'exposition (pour le cas général, je renvoie à mon article [17]). La puissance p-ième de ∂ s'annule, mais il est possible de définir ses puissances divisées $\partial^{[n]}$ pour tout $n \in \mathbb{N}$ de manière explicite comme suit :

$$\partial^{[n]}\Big(\sum_i a_i X^i\Big) = r^{-n} \cdot \sum_i \frac{i(i-r)\cdots(i-(n-1)r)}{n!}\, a_i X^{i-rn}$$

la division par $n!$ ne posant pas de problème car le numérateur est lui-même multiple de $n!$. À partir de là, je définis le développement de Taylor d'un polynôme tordu $f \in K[X;\theta]$ au voisinage d'un point $z \in F$, $z \neq 0$, par :

$$\mathrm{TS}_z(f) = \sum_{n=0}^{\infty} \partial^{[n]}(f)_{|Y=z}\, T^n \;\in\; \big(K[X^{\pm 1};\theta]/(Y-z)\big)[[T]] \simeq \big(K[X;\theta]/(Y-z)\big)[[T]]$$

où la notation « $Y=z$ » en indice signifie simplement que l'on considère l'image de l'élément dans l'anneau quotient $K[X^{\pm 1};\theta]/(Y-z)$. Je démontre ensuite les propriétés attendues d'un développement de Taylor, en particulier que l'application TS_z est un homomorphisme d'anneaux.

Le fait que Frac $K[X;\theta]$ soit isomorphe à $F(Y) \otimes_{F[Y]} K[X;\theta]$ entraîne facilement que TS_z s'etend en un morphisme d'anneaux Frac $K[X;\theta] \to \big(K[X;\theta]/(Y-z)\big)((T))$ que je note encore TS_z. Je peux ainsi définir le résidu de f en z comme le coefficient en T^{-1} dans son développement de Taylor ; je le noterai dans la suite $\mathrm{sres}_z(f)$. En étendant les scalaires, je définis pareillement $\mathrm{sres}_z(f)$ pour toute valeur z non nulle dans une clôture séparable F^{sep} de F. Il s'agit alors d'un élément de l'anneau quotient :

$$\frac{F^{\mathrm{sep}} \otimes_F K[X;\theta]}{Y - z}.$$

Comparer les résidus d'une même fonction f pour différentes valeurs de z paraît délicat car ceux-ci ne vivent pas dans le même anneau. Afin de palier à cette difficulté, je remarque que $\mathrm{sres}_z(f)$ peut toujours être écrit comme un polynôme tordu de degré au plus r à coefficient dans $F^{\mathrm{sep}} \otimes_F K$. Pour $j \in \{0,\dots,r-1\}$, je définis ainsi $\mathrm{sres}_{z,j}(f) \in F^{\mathrm{sep}} \otimes_F K$ comme le coefficient en X^j de $\mathrm{sres}_z(f)$. Par des manipulations *ad hoc*, je définis également les $\mathrm{sres}_{0,j}(f)$ et $\mathrm{sres}_{\infty,j}(f)$ et je démontre enfin le théorème suivant qui est un analogue tordu de la formule des résidus.

Théorème 3. *1. Pour tout $f \in$ Frac $K[X;\theta]$, on a $\sum_{z\in F^{\mathrm{sep}}} \mathrm{sres}_{z,0}(f) = 0$.*

2. Pour tout $f \in$ Frac $K[X;\theta]$ ayant uniquement des pôles simples et pour tout $j \in \{1,\dots,r-1\}$, on a $\sum_{z\in F^{\mathrm{sep}}} \mathrm{sres}_{z,j}(f) = 0$.

Dans [17], je démontre également une formule de changement de variables qui spécifie comment les résidus sont modifiés lorsqu'on fait agir sur f un endomorphisme de K-algèbres de Frac $K[X;\theta]$. Cette formule étant assez technique, je ne la reproduis pas dans ce rapport et me contente de renvoyer celles et ceux qui souhaitent à en savoir davantage à mon article.

Pour ce qui concerne les applications, à partir du théorème 3, j'obtiens une description en termes de résidus des duaux des codes de Reed–Solomon linéarisés (qui sont une généralisation des codes de Gabidulin introduite récemment par Martinez-Peñas). J'en déduis, en particulier, que la classe des codes de Reed–Solomon linéarisés est stable par dualité, ce qui répond à une question posée par Martinez-Peñas dans son article.

2.1.3 Séries algébriques en caractéristique positive

Références :

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

[23] B. Adamczewski, A. Bostan, X. Caruso, G. Christol, R. Yassawi, *A sharp quantitative version of multivariate Christol's theorem, and applications*

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 l'observation suivante : si

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

est une série algébrique sur $\mathbb{F}_p(t)$, alors la famille des $\big(f(t)^{p^n}\big)_{n\geqslant 0}$ est nécessairement liée, ce qui signifie qu'il existe $P \in \mathbb{F}_p(t)[X;\mathrm{Frob}]$ (où Frob : $x \mapsto x^p$ est le Frobenius) tel que $P(\mathrm{Frob})(f) = 0$. Autrement dit, f est annulé par un polynôme tordu. On déduit de cette observation le fameux théorème de Christol qui affirme que la suite des coefficients de f, *i.e.* la suite des a_n, 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. En particulier, on en déduit 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 introduisons les opérateurs de section S_r ($0 \leqslant r < p$) définis par :

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

et nous démontrons le théorème suivant qui peut être considéré comme une version *effective* du théorème de Christol.

Théorème 4 (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*

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

est stable par les opérateurs de section S_r.

L'idée de remplacer le Frobenius par les opérateurs de section et de construire un espace de dimension finie sur k stable par ces derniers est classique dans ce domaine. L'originalité de notre résultat est, d'une part, sa forme entièrement explicite et, d'autre part, l'absence totale d'hypothèse sur f ; en particulier, nous ne supposons pas la lissité de la courbe $E(t,y) = 0$, contrairement à d'autres résultats de ce type que l'on trouve dans la littérature.

Forts du théorème 4, 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 4. 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 4 assure que l'on a une écriture :

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

avec $\deg b_i(t) < h$. On peut voir l'équation (1) 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 $f(t)$ est connue 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.

Suite à ce travail, nous avons été contactés par Boris Adamczewski et Reem Yassawi qui nous ont demandé si nous pensions que nos méthodes s'étendaient à un contexte multivarié. Comme nous n'avions jusqu'alors pas réfléchi à cette question, nous avons entâmé une collaboration sur le sujet. Les premiers résultats que nous avons obtenus sont très encourageants puisque nous nous sommes rendus compte très rapidement que le théorème 4, ainsi que sa démonstration, s'étendent *verbatim* à des fonctions à plusieurs variables.

Théorème 5. *On note $\underline{t} = (t_1, \dots, t_n)$. Soit $f(\underline{t}) \in \mathbb{F}_p[[\underline{t}]]$ une série entière en n variables. On suppose qu'il existe un polynôme irréductible $E(\underline{t}, y) \in \mathbb{F}_p[\underline{t}, y]$ tel que $E(\underline{t}, f(\underline{t})) = 0$. Soient $h_i = \deg_{t_i} E$ et $d = \deg_y E$. Alors le $\mathbb{F}_p$-espace vectoriel*

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

est stable par les opérateurs de section $S_{\underline{r}}$ pour $\underline{r}$ variant dans $\{0, 1, \dots, p-1\}^n$.

Au delà des applications algorithmiques, le théorème 5 fournit un nouvel angle d'attaque à l'étude des diagonales de fonctions algébriques. Rappelons que si $f(\underline{t}) = \sum_{\underline{i}} a_{\underline{i}} \underline{t}^{\underline{i}}$ est une série entière multivariée à coefficients dans un anneau A, sa diagonale est définie par :

$$\mathrm{Diag}(f) = \sum_{i=0}^{\infty} a_{i,\dots,i} x^i \in A[[x]].$$

Lorsque A est un corps fini, un théorème de Furstenberg affirme que $\mathrm{Diag}(f)$ est algébrique sur $A[\underline{t}]$ dès lors que f l'est. Cette conclusion n'est toutefois plus valable lorsque A est un corps de caractéristique nulle, typiquement $A = \mathbb{Q}$. Malgré tout, partant d'une fonction algébrique $f \in \mathbb{Q}[[\underline{t}]]$, la réduction de f modulo p a un sens pour presque tout nombre premier p, et nous pouvons nous intéresser au degré d'algébricité $d_p(f)$ de $g_p = \mathrm{Diag}(f) \bmod p$ sur $\mathbb{F}_p(x)$. Faisant suite à de nombreux autres travaux, Adamczewski et Bell ont montré en 2013 que $d_p(f) \in O(p^H)$ où H est une constante faramineuse (une tour d'exponentielles en d et en les h_i dont la taille croît au moins linéairement avec le nombre de variables) qu'il est, de plus, difficile d'expliciter à cause d'un procédé de résolution des singularités qui apparaît dans la construction. En comparaison, grâce au théorème 5, nous démontrons que $H = (h_1 + 1) \cdots (h_n + 1) \cdot (d + 1)$ convient dans tous les cas.

Mieux encore, le polynôme annulateur de g_p que nous construisons est obtenu à partir d'un polynôme de Ore de degré H, indépendant de p. Ceci implique en particulier que, pour presque tout nombre premier p, le groupe de Galois du corps de décomposition de g_p, noté G_p, apparaît comme un sous-groupe de $\mathrm{GL}_H(\mathbb{F}_p)$ (défini à conjugaison près). À ce stade, il est naturel de se demander s'il n'existerait pas un sous-groupe $G \subset \mathrm{GL}_H(\mathbb{Q})$ dont G_p serait, à conjugaison près, la réduction modulo p pour presque tout p. De surcroît, un tel groupe G, s'il existe, pourrait être lié au groupe de Galois de l'*équation différentielle* satisfaite par $\mathrm{Diag}(f)$. Ces questions semblent entièrement nouvelles mais, malheureusement, pour le moment, nous ne savons pas encore y apporter de réponses satisfaisantes, fussent-elles partielles.

2.2 Le projet CLap–CLap

Depuis septembre 2018, je suis coordinateur du projet ANR CLap–CLap (« Correspondance de Langlands p-adique : une approche constructive et algorithmique ») qui vise, en particulier, à développer des outils

algorithmiques pour manipuler les principaux objets qui interviennent dans le correspondance de Langlands p-adique avec l'espoir, à terme, d'avoir une meilleure vision de ce que pourrait être cette correspondance qui, au délà de $\mathrm{GL}_2(\mathbb{Q}_p)$, reste encore bien mystérieuse.

2.2.1 Espaces de déformations galoisiennes et poids de Serre

Références :
[9] X. Caruso, A. David, A. Mézard, *Un calcul d'anneaux de déformations potentiellement Barsotti–Tate*
[2] X. Caruso, A. David, A. Mézard, *Variétés de Kisin stratifiées et déformations potentiellement Barsotti–Tate*
[22] X. Caruso, A. David, A. Mézard, *Combinatorics of Serre weights in the potentially Barsotti–Tate setting : the non generic case*
[29] X. Caruso, *Espaces de déformations potentiellement Barsotti–Tate*, librairie SAGEMATH

S'il existe effectivement une correspondance de Langlands p-adique mettant en relation, d'une part, les représentations galoisiennes d'un corps p-adique F et, d'autre part, les représentations du groupe réductif $\mathrm{GL}_n(F)$, on s'attend à ce que celle-ci se retrouve au niveau des espaces de déformations. Un énoncé précis dans cette direction est la conjecture de Breuil–Mézard qui prédit que la géométrie de la fibre spéciale de certains espaces de déformations galoisiennes est dictée par la théorie des $\bar{\mathbb{F}}_p$-représentations du groupe réductif correspondant.

Avec l'espoir d'aller au delà d'un énoncé portant uniquement sur la fibre spéciale, nous avons entrepris avec Agnès David et Ariane Mézard de calculer explicitement certains espaces de déformations galoisiennes. Précisément, nous considérons une extension non ramifiée F de $\mathbb{Q}_p$ de degré f. Nous notons par G_F le groupe de Galois absolu de F et par I_F son sous-groupe d'inertie. Étant donnés un caractère $\psi : \mathrm{Gal}(\bar{\mathbb{Q}}_p/F) \to \mathbb{Z}_p^\times$, une représentation $\bar\rho : \mathrm{Gal}(\bar{\mathbb{Q}}_p/F) \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$ et un type galoisien modérément ramifié $\mathrm{t} : I_F \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$, nous nous sommes donné comme objectif de calculer l'espace de déformation $R^\psi(\bar\rho, \mathrm{t})$ paramétrisant les représentations galoisiennes potentiellement Barsotti–Tate $G_F \to \mathrm{GL}_2(\bar{\mathbb{Z}}_p)$ de déterminant ψ, de type galoisien t, et se réduisant (à conjugaison près) sur $\bar\rho$ modulo l'idéal maximal. Dans les articles [9] et [2] (qui correspondent à des travaux publiés pendant la période d'évaluation, mais réalisés antérieurement), nous avons donné une description *conjecturale* de $R^\psi(\bar\rho, \mathrm{t})$; cette description est géométrique et entièrement explicite : elle s'obtient à partir de la variété $(\mathbb{P}^1)^f$ par une succession d'éclatements et de complétés formels, qui est dictée par un invariant combinatoire $\mathbb{G}(\bar\rho, \mathrm{t})$ associé au couple $(\bar\rho, \mathrm{t})$ que nous avons appelé le *gène*.

Afin de tester nos conjectures, nous avons ensuite voulu vérifier la compatibilité de celles-ci avec la conjecture de Breuil–Mézard. Ce travail, qui nous paraissait initialement n'être guère plus qu'un exercice, s'est en réalité révélé bien plus ardu, mais aussi bien plus fructueux, que nous ne l'avions imaginé. En effet, comme je le disais précédemment, la conjecture de Breuil–Mézard relie la fibre spéciale des espaces de déformations galoisiennes à des données provenant de la théorie des représentations des groupes réductifs. Dans le cadre dans lequel nous nous sommes placés, ces données sont incarnées par la notion de *poids de Serre*. En guise de préliminaire, nous devions donc relier ces poids de Serre au gène que nous avions défini dans [2]. C'est le travail que nous avons accompli dans l'article [22] (dont la rédaction n'est pas encore entièrement finalisée).

De manière plus précise, nous formulons une recette entièrement combinatoire qui permet d'obtenir l'ensemble des poids de Serre $S(\bar\rho, \mathrm{t})$ correspondant au couple $(\bar\rho, \mathrm{t})$ à partir du $\mathbb{G}(\bar\rho, \mathrm{t})$. Il serait trop long (et sans doute peu intéressant) de la recopier *in extenso* dans ce rapport d'activités. Plus importantes sont les conséquences de nos résultats qui impliquent, en particulier, que $S(\bar\rho, \mathrm{t})$ ne dépend que de $\mathbb{G}(\bar\rho, \mathrm{t})$. Ceci n'était pas du tout évident *a priori* et vient conforter les conjectures de [2] qui, elles-mêmes, prédisent que l'anneau de déformations $R^\psi(\bar\rho, \mathrm{t})$ ne devrait dépendre que de $\mathbb{G}(\bar\rho, \mathrm{t})$. Mieux encore, il résulte de notre description que $S(\bar\rho, \mathrm{t})$ s'écrit comme un produit cartésien indexé par certaines sous-parties du gène de la même manière que les conjectures de [2] prédisent que $R^\psi(\bar\rho, \mathrm{t})$ devrait s'écrire comme produit tensoriel d'anneaux plus petits.

En complément de cela, nos méthodes conduisent à des algorithmes rapides (de complexité quasi-optimale) pour lister ou compter les éléments de $S(\bar\rho, \mathrm{t})$ et permettent ainsi de mettre en place toute une algorithmique des poids de Serre dans ce contexte. J'ai implementé un *package* SAGEMATH [29] (que je n'ai pas encore rendu public, mais qui devrait l'être très prochainement) reprenant tous ces algorithmes et offrant ainsi à l'utilisateur des outils efficaces pour manipuler les $\bar{\mathbb{F}}_p$-représentations de G_F, les types

galoisiens et les poids de Serre qui leur correspondent. Ces outils, nous ayant été particulièrement utiles pour l'élaboration de notre article, j'espère qu'ils pourront également servir à d'autres collègues qui travaillent sur des questions connexes.

J'aimerais conclure ce paragraphe sur une note plus spéculative. En effet, je voudrais souligner que, selon moi, le fait que le gène gouverne entièrement la combinatoire des poids de Serre et donc, par ricochet, la géométrie de la fibre spéciale des espaces de déformations galoisiennes est tout à fait remarquable étant donné que le gène, lui-même, est défini indépendemment du nombre premier p avec lequel on travaille (pourvu que $p \geqslant 3$). Cela semble indiquer que, au moins dans le cas que nous considérons, la correspondance de Langlands p-adique est, en quelque sorte, « uniforme en p ». Cette question de l'uniformité vis-à-vis de p est, à ma connaissance, nouvelle dans ce contexte, et me paraît tout à fait intéressante. J'aimerais pouvoir la creuser davantage dans les années à venir.

2.2.2 Bases de Gröbner pour les algèbres de Tate

Références :

[13] X. Caruso, T. Vaccon, T. Verron, *Gröbner bases over Tate algebras*

[14] X. Caruso, T. Vaccon, T. Verron, *Signature-based algorithms for Gröbner bases over Tate algebras*

[19] X. Caruso, T. Vaccon, T. Verron, *On FGLM algorithm with Tate algebras*

[27] X. Caruso, T. Verron, *Bases de Gröbner sur les algèbres de Tate*, librairie SAGEMATH

Les constructions que l'on rencontre communément en théorie de Hodge p-adique peuvent très souvent être interprétées de manière naturelle dans le langage de la géométrie p-adique, lorsqu'elles ne sont pas directement basées sur celle-ci. Typiquement, les conjectures de [2] que j'ai mentionées dans la paragraphe précédent sont énoncées dans ce langage mais, au delà de ça, la plupart des constructions géométriques que l'on est amené à effectuer dans ces domaines sortent souvent du cadre de la géométrie algébrique classique pour se placer dans celui de la géométrie formelle, de la géométrie rigide voire, plus récemment, avec les travaux de Scholze et al., de la géométrie de Huber, de la géométrie perfectoïde, prismatique, *etc.* Un autre exemple où la géométrie p-adique est omniprésente est celui de l'étude des équations différentielles p-adiques où le cadre naturel pour énoncer les théorèmes est celui de la géométrie de Berkovitch.

Pour ces raisons, il m'a semblé important de développer l'algorithmique des variétés rigides p-adiques, en commençant par les briques de bases qui sont la manipulation sur machine des algèbres de Tate et de leurs idéaux. Je rappelle brièvement qu'étant donnée une extension finie K de $\mathbb{Q}_p$, l'algèbre de Tate $K\{\underline{X}\}$ (avec $\underline{X} = (X_1, \dots, X_n)$) est, par définition, constituée des séries $\sum_{\underline{i} \in \mathbb{N}^n} a_{\underline{i}} \underline{X}^{\underline{i}}$ où les $(a_{\underline{i}})_{\underline{i} \in \mathbb{N}^n}$ forment une suite d'éléments de K qui converge vers 0 lorsque $|\underline{i}|$ tend vers l'infini. Géométriquement, les séries de Tate correspondent aux fonctions analytiques sur le disque unité fermé. Classiquement, l'outil standard pour la manipulation algorithmique des idéaux dans les anneaux de polynômes est la théorie des bases de Gröbner. C'est ainsi qu'il m'est apparu naturel d'essayer d'en développer un analogue dans le cadre des algèbres de Tate. Pour ce projet, j'ai proposé à Tristan Vaccon et Thibaut Verron de collaborer avec moi. Nous avons, pour le moment, rédigé trois articles sur le sujet [13, 14, 19] (dont je vais présenter brièvement le contenu dans la suite) et réalisé une implémentation dans le logiciel SAGEMATH [27] qui est disponible dans la distribution standard depuis la version 8.5.

Dans le cadre polynomial, la notion fondamentale pour élaborer une théorie des bases de Gröbner est celle d'*ordre monomial* qui conduit à définir le *terme de tête* d'un polynôme, puis à l'utiliser pour effectuer les divisions. Étendre cette notion au cas des séries de Tate pose d'emblée des difficultés étant donné qu'une série est composée d'une infinité de monômes dont les degrés ne sauraient être bornés. Dans ces conditions, quel pourrait être le terme de tête ? La solution à ce problème nous est, malgré tout, apparue rapidement : il suffit d'incorporer la valuation des coefficients dans la définition de l'ordre.

Définition 6. Soient $a\underline{X}^{\underline{i}}$ et $b\underline{X}^{\underline{j}}$ deux termes (avec $a, b \in K$ et $\underline{i}, \underline{j} \in \mathbb{N}^n$). On dit que $a\underline{X}^{\underline{i}} < b\underline{X}^{\underline{j}}$ si $\mathrm{val}_p(a) > \mathrm{val}_p(b)$ ou si $\mathrm{val}_p(a) = \mathrm{val}_p(b)$ et $\underline{i} < \underline{j}$.

La définition ci-dessus dépend du choix d'un ordre sur $\mathbb{N}^n$. Comme dans la théorie classique, nous choisissons un ordre monomial, c'est-à-dire un ordre bien fondé qui prolonge l'ordre (partiel) naturel sur $\mathbb{N}^n$ et qui est compatible à l'addition. L'ordre lexicographique, par exemple, convient. Toutefois, ce n'est

pas celui qui conduit aux calculs les plus efficaces en pratique et on préfèrera souvent choisir un ordre dit *gradué*, c'est-à-dire qui compare en priorité le degré total des monômes.

La condition de convergence qui apparaît dans la définition des algèbres de Tate assure qu'une série de Tate $f = \sum_{\underline{i} \in \mathbb{N}^n} a_{\underline{i}} \underline{X}^{\underline{i}}$ n'admet qu'un nombre fini de monômes pour lesquels $\mathrm{val}_p(a_{\underline{i}})$ est minimal. Ainsi, le terme de tête de f est bien défini ; nous le noterons $\mathrm{LT}(f)$ dans la suite. Ceci étant posé, la définition d'une base de Gröbner est identique à celle que l'on utilise dans le cas classique.

Définition 7. Soit I un idéal de $K\{\underline{X}\}$. Une *base de Gröbner* de I est une famille finie $(g_1, \dots, g_s)$ d'élements de I telle que, pour tout $f \in I$, il existe un indice i tel que $\mathrm{LT}(f)$ soit divisible par $\mathrm{LT}(g_i)$.

Une autre conséquence importante de l'existence d'un terme de tête est la possibilité d'énoncer (et de démontrer) un théorème de « division euclidienne » (que l'on appelle généralement *réduction*) pour les séries de Tate.

Théorème 8. *Soient $f, g_1, \dots, g_s \in K\{\underline{X}\}$. Il existe $q_1, \dots, q_s, r \in K\{\underline{X}\}$ tels que $f = q_1 g_1 + \cdots + q_s g_s + r$ et pour tout indice i, aucun terme de r n'est divisible par $\mathrm{LT}(g_i)$.*

Forts de ces constructions, les théorèmes classiques de la théorie s'étendent à présent sans difficulté majeure au cas des algèbres de Tate. Le théorème suivant donne un aperçu des principaux résultats de notre premier article [13].

Théorème 9. *Pour un idéal I de $K\{\underline{X}\}$, les assertions suivantes sont vraies :*

(1) I admet une base de Gröbner $(g_1, \dots, g_s)$, que l'on peut calculer par un algorithme de type Buchberger,

(2) une série de Tate f appartient à I si et seulement si le reste de la réduction de f par $(g_1, \dots, g_s)$ est nul.

Dans [13], nous traitons également le cas d'algèbres de Tate définies par des conditions de convergence plus générales qui indiquent que la fonction associée converge non pas sur la boule unité, mais sur un polydisque de rayons arbitraires. Lorsque ces rayons sont dans $p^{\mathbb{Z}}$, il est possible de se ramener à $K\{\underline{X}\}$ par un simple changement de variables ; cependant, pour des rayons généraux, des arguments supplémentaires sont nécessaires si l'on souhaite éviter d'avoir à travailler dans une extension (ce qui est toujours coûteux en temps de calcul).

Après ce premier travail, nous avons voulu aller plus loin et voir dans quelle mesure les algorithmes *rapides* dans le cadre polynomial pouvaient s'étendre au cas des séries de Tate. Parmi les algorithmes rapides en question, le plus célèbre est sans doute l'algorithme F5 de Faugère. Sa particularité est qu'il est capable de détecter en amont une quantité importante de réductions inutiles (dans le sens où elles n'apportent aucune information supplémentaire) et ainsi gagne beaucoup de temps en ne les effectuant simplement pas. Dans l'article [14], nous montrons qu'il est possible d'adapter cette stratégie de détection aux idéaux de $K\{\underline{X}\}$, aboutissant ainsi, comme dans le cas polynomial, à une accéleration significative des temps de calcul. Nous proposons, en réalité, deux approches différentes qui conduisent à deux algorithmes différents que nous avons appelés *PoTe* (pour « *Po*sition over *Te*rm ») et *VaPoTe* (pour « *Va*luation over *Po*sition over *Te*rm »). Chacun d'eux a ses avantages et ses inconvénients : le premier est incrémental et permet ainsi facilement d'ajouter un générateur à un idéal, tandis que le second, qui privilégie la valuation, est plus stable numériquement et plus adapté à une gestion fine de la précision (et aussi, souvent, un peu plus rapide).

Enfin, dans l'article [19] que nous avons terminé de rédiger très récemment, nous avons cherché à étendre l'algorithme FGLM qui permet, dans le cas classique, d'effectuer rapidement des changements d'ordre monomiaux dans le cas des idéaux de dimension nulle (*i.e.* des idéaux I pour lesquels le quotient $K[\underline{X}]/I$ est de dimension de Krull 0 ou, ce qui revient au même, de dimension finie comme espace vectoriel sur K). Les algorithmes de changement d'ordre sont intéressants car, comme je l'ai mentionné précédemment, il est souvent nettement plus rapide pour les calculs de choisir un ordre gradué ; cependant, dans certaines situations (par exemple, pour le calcul d'intersections d'idéaux), il est souhaitable, voire nécessaire, de travailler avec d'autres ordres, typiquement lexicographiques. Nous avons démontré que la stratégie générale de FGLM s'étend au cas des algèbres de Tate et conduit à des algorithmes de complexité comparable. Mieux encore, nos algorithmes ne permettent pas uniquement d'effectuer un changement d'ordre, mais également un changement sur les rayons du polydisque de convergence. Cette fonctionnalité supplémentaire nous a semblé particulièrement intéressante pour plusieurs raisons. D'une part, poussée

à son terme, elle donne un théorème de *factorisation par les pentes* des idéaux I de dimension nulle de $K\{\underline{X}\}$ qui permet notamment de déterminer, grâce à un calcul d'algèbre linéaire pure, la valuation des points de la variété $V(I)$ associée. D'autre part, elle fournit les bases qui devraient nous permettre *in fine* de travailler avec des ordres plus généraux que ceux de la définition 6 ne mettant en avant la valuation de manière aussi nette et ressemblant ainsi encore davantage à des ordres gradués pour lesquels on peut espérer que l'algorithmique sous-jacente soit encore plus performante.

2.2.3 Calcul d'isogénies sur les 2-adiques

Référence :

[18] X. Caruso, E. Eid, R. Lercier, *Fast computation of elliptic curve isogenies in characteristic two*

Une source particulièrement intéressante de représentations galoisiennes p-adiques est donnée par la construction du module de Tate : partant d'une courbe elliptique E (ou, plus généralement, d'une variété abélienne) définie sur un corps de caractéristique différente de p, son module de Tate $T_p(E)$ est la limite projective du groupe de ses points de p^n-torsion, qui est naturellement un $\mathbb{Z}_p$-module libre sur lequel Galois agit. Les isogénies rationnelles de E induisent des endomorphismes $\mathbb{Z}_p$-linéaires de E qui commutent à l'action galoisienne. Ainsi, il est souvent commode de développer l'algorithmique des représentations galoisiennes à travers le miroir des courbes elliptiques et des isogénies qui sont, à l'évidence, des objets qui se prêtent beaucoup plus facilement à la manipulation sur machine.

Bien entendu, la question du calcul d'isogénies entre courbes elliptiques a déjà été abondamment traitée dans la littérature. Parmi les nombreuses stratégies qui ont été proposées, on trouve la méthode d'Elkies qui ramène le calcul d'isogénies à la résolution d'une équation différentielle non linéaire. En effet, si E_1 (resp. E_2) est la courbe d'équation $y^2 = x^3 + a_1x + a_0$ (resp. $y^2 = x^3 + b_1x + b_0$), Elkies démontre qu'une isogénie $I : E_1 \to E_2$ est nécessairement de la forme $I : (x, y) \mapsto \big(f(x), cyf'(x)\big)$ où la fonction f vérifie :

$$c^2 \cdot \big(x^3 + a_1x + a_0\big) \cdot f'(x)^2 = f(x)^3 + b_1f(x) + b_0 \tag{2}$$

et où c désigne la constante par laquelle l'isogénie I agit sur la différentielle invariante $\frac{dx}{y}$. De plus, on sait que si I est de degré ℓ, alors f est une fraction rationnelle dont le numérateur et le dénominateur sont de degré au plus ℓ. En pratique, on peut alors résoudre formellement l'équation différentielle (2) au voisinage du point à l'infini à précision suffisante grâce à une itération de Newton, puis retrouver la fonction f en utilisant des approximants de Hermite–Padé. On obtient, ce faisant, un algorithme de calcul d'isogénies de complexité quasi-linéaire en le degré ℓ.

Tout ceci fonctionne parfaitement sur un corps exact de caractéristique nulle mais des problèmes surviennent dès lors que l'on travaille en caractéristique $p > 0$ (à cause des divisions par p qui interviennent dans la formule d'itération de Newton) ou sur les p-adiques (à cause de possibles instabilités numériques). Dans le cadre p-adique, Vaccon et Lairez ont montré que, *lorsque p est impair*, les pertes cumulées de précision sont d'au plus $\log \ell + O(1)$ chiffres significatifs. Ce résultat est entièrement satisfaisant mais il laisse, malheureusement, de côté le cas $p = 2$ qui est important pour les applications. Or, des expériences numériques montrent que, sur les 2-adiques, une interprétation naïve de la formule d'itération de Newton conduit à des pertes de précision affolantes qui sont de l'ordre de ℓ chiffres significatifs.

Avec Reynald Lercier et Elie Eid, nous avons donc décidé d'attaquer à bras le corps ce cas restant, souvent négligeamment délaissé [1], de la caractéristique résiduelle 2. Dans cette situation, il est préférable d'utiliser des équations de Weierstrass de la forme $y^2 + xy = x^3 + a_1x^2 + a_2$. Avec le changement de variables $t = x^{-1}$ et le changement de fonctions $z(t) = f(x)^{-1}$, l'équation différentielle à résoudre prend la forme :

$$c^2 \cdot \Big(4t + (4a_1{+}1)t^2 + 4a_2t^4\Big) \cdot z'(t)^2 = 4z(t) + (4b_1{+}1)z(t)^2 + 4b_2z(t)^4. \tag{3}$$

Contrairement au cas de la caractéristique résiduelle impaire, l'équation différentielle (3) a le mauvais goût de faire apparaître deux singularités dans le disque unité. En effet, le polygone de Newton de $4t + (4a_1{+}1)t^2 + 4a_2t^4$ indique que ce polynôme a, en plus de la racine $t = 0$, une seconde racine de valuation 2, et donc de norme $\frac{1}{4}$. La présence de ces singularités fait sortir l'équation différentielle (3) du cadre habituel d'étude (si tant est qu'il y en ait un pour les équations non linéaires) et nous oblige ainsi à

1. Par moi-même également, dans d'autres contextes.

reprendre entièrement le travail à son commencement. Néanmoins, nous parvenons à mettre en place les rouages d'une méthode de type perturbation : nous montrons qu'une petite modification des coefficients de (3) (c'est-à-dire des polynômes $4t + (4a_1{+}1)t^2 + 4a_2t^4$ et $4t + (4b_1{+}1)t^2 + 4b_2t^4$) n'induit qu'une petite modification de ses solutions et, en particulier, n'en modifie pas le rayon de convergence. Ce résultat théorique est la clé qui conduit à un algorithme stable de résolution numérique de (3). Précisément, nous démontrons le théorème suivant qui a une portée légèrement plus large que la famille d'équations différentielles considérée jusqu'à présent.

Théorème 10. *Il existe un algorithme qui prend en entrée :*
- *deux entiers strictement positifs n et N,*
- *deux entiers 2-adiques a et b inversibles dans $\mathbb{Z}_2$,*
- *deux séries entières $u, v \in \mathbb{Z}_2[[t]]$ telles que $u(0)$ soit inversible dans $\mathbb{Z}_2$*

et, dans le cas où l'équation différentielle suivante en z

$$t(t{-}4a)\, u(t)^2\, z'^2 = z\,(z{-}4b)\, v(z)^2$$

admet une unique solution dans $t{\cdot}\mathbb{Z}_2[[t]]$, calcule cette solution modulo $(2^N, t^n)$ pour un coût de $\tilde{O}(n)$ opérations dans $\mathbb{Z}_2$ à précision $O(2^M)$ avec $M = \max(N, 3) + \lfloor \log_2(n) \rfloor + 2$.

Comme corollaire, nous déduisons un algorithme efficace de calcul d'isogénies sur les corps 2-adiques et, également, sur les corps finis de caractéristique 2 en utilisant des relevés canoniques. Ces algorithmes ont été implémentés par mon collègue Reynald Lercier en MAGMA ; ils sont très efficaces en pratique et permettent de calculer en une poignée de secondes des isogénies de degré $\approx 10^6$ sur le corps fini $\mathbb{F}_2$.

2.3 Algorithmique sur les nombres p-adiques

Ma recherche de ces cinq dernières années a été également 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 un précédent rapport d'activités.

2.3.1 Précision sur le polynôme caractéristique

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

Tout d'abord, poursuivant nos travaux sur l'algèbre linéaire p-adique, 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 envisageons de revenir tantôt.

2.3.2 Le package ZpL

Références :
[8] X. Caruso, D. Roe, T. Vaccon, *ZpL : a p-adic precision package*
[25] X. Caruso, D. Roe, J. Rüth, *ZpL : a p-adic precision package*, librairie SageMath

Comme rappelé brièvement au §2.3.1 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 espérons pouvoir réaliser dans un futur pas trop éloigné.

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.

2.3.3 Évaluation rapide de quelques fonctions p-adiques

Références :
[24] X. Caruso, *Algorithmes rapides pour le calcul du logarithme et de l'exponentielle p-adique*, librairie SAGEMATH
[20] X. Caruso, M. Mezzarobba, T. Vaccon, N. Takayama, *Fast evaluation of some p-adic transcendental functions*

Dans le cas des nombres réels, il existe des stratégies très efficaces pour évaluer en un point donné un grand nombre de fonctions transcendantes élémentaires (logarithme, exponentielle, *etc.*) et spéciales (fonction ζ, fonction Γ, fonctions hypergéométriques, *etc.*) qui permettent de calculer des millions de chiffres significatifs en quelques secondes à peine. Toutefois, les analogues p-adiques de ces méthodes n'avaient, jusqu'à présent, pas été étudiées de manière systématique.

Avec Marc Mezzarobba, Tristan Vaccon et Nobuki Takayama, nous avons récemment entrepris de combler cette lacune de la littérature en montrant comment étendre les méthodes de type *scindage binaire* et *bit-burst* dans le monde p-adique [20]. Le cadre que nous avons considéré est celui de l'évaluation en un point rationnel d'une fonction f qui est solution d'une équation différentielle de la forme :

$$a_r(x)f^{(r)}(x) + a_{r-1}(x)f^{(r-1)}(x) + \cdots + a_1(x)f'(x) + a_0(x)f(x) = 0 \tag{4}$$

Nous supposons que les $a_i(x)$ sont des *polynômes* à coefficients *rationnels* et que la fonction f est définie sur un domaine D, qui est une boule ouverte de $\mathbb{Q}_p$ (ou, plus généralement, d'une extension finie de $\mathbb{Q}_p$) contenant 0. Nous démontrons le théorème suivant.

Théorème 11. *Il existe un algorithme qui prend en entrée l'équation différentielle (4), $f(0), f'(0), \dots, f^{(r-1)}(0)$ et un point $x_0 \in D$ et calcule, sous l'hypothèse que la fonction a_r ne s'annule pas sur $D\backslash\{0\}$, la valeur $f(x_0)$ en un temps qui croît de manière quasi-linéaire en la précision de la sortie.*

Comme corollaire immédiat, nous obtenons des algorithmes efficaces pour le calcul du logarithme et de l'exponentielle p-adiques, que j'ai implémentés dans SAGEMATH et qui sont disponibles dans la distribution standard du logiciel depuis la version 8.0. Par ailleurs, le fait que nous autorisons la fonction a_r à s'annuler en 0 est important pour les applications car de nombreuses fonctions spéciales p-adiques d'intérêt nécessitent cette hypothèse affaiblie. Il en va ainsi notamment des fonctions hypergéométriques p-adiques (solutions de $x(x-1)y'' + \big(c-(a+b+1)z\big)y' - aby = 0$) ou des fonctions de Bessel p-adiques (solutions de $x^2y'' + xy' + (x^2-\alpha^2)y = 0$).

Dans le monde p-adique, il arrive régulièrement qu'un procédé de « renormalisation » permette d'augmenter le rayon de convergence des fonctions considérées. L'exemple le plus simple de ce phénomène est incarné par l'exponentielle d'Artin–Hasse, qui est définie par l'égalité :

$$\mathrm{AH}(x) = \exp\left(x + \frac{x^p}{p} + \frac{x^{p^2}}{p^2} + \cdots\right).$$

Il se trouve que lorsque l'on développe formellement l'expression de droite, on obtient une série à coefficients dans $\mathbb{Z}_p$; autrement dit, toutes les divisions par p au dénominateur disparaissent. La fonction AH converge ainsi sur la boule unité ouverte d'une clôture algébrique $\bar{\mathbb{Q}}_p$ de $\mathbb{Q}_p$ alors que la fonction exponentielle, elle-même, ne converge sur la boule de rayon $p^{-\frac{1}{p-1}} < 1$. Ainsi, si l'on souhaite évaluer AH en un point de norme proche de 1, il n'est pas possible de simplement évaluer l'argument puis d'appliquer la fonction $\exp$. En outre, il n'est pas possible non plus d'utiliser le théorème 11 car AH n'est solution d'aucune équation différentielle simple à coefficients *polynomiaux*. Dans [20], nous proposons toutefois un algorihme rapide d'évaluation de l'exponentielle de Artin–Hasse qui utilise un procédé différent basé sur une itération de Newton.

Un autre exemple intéressant de surconvergence est donné par la fonction hypergéométrique de Dwork $\mathcal{F}_{\frac{1}{2},\frac{1}{2}}$ qui interpole le quotient :

$$\frac{{}_2F_1\big(\frac{1}{2},\frac{1}{2};1;x\big)}{{}_2F_1\big(\frac{1}{2},\frac{1}{2};1;x^p\big)}$$

sur le disque ouvert de rayon 1 mais qui définit une fonction analytique (dans le sens de Krasner) sur le disque *fermé* de rayon 1. Ainsi, calculer les valeurs de $\mathcal{F}_{\frac{1}{2},\frac{1}{2}}$ en un point du cercle unité s'avère particulièrement difficile. Dans un travail récent, Asakura a montré que ces valeurs spéciales apparaissent

dans la cohomologie d'une certaine fibration et en a déduit un algorithme de calcul de $\mathcal{F}_{\frac{1}{2},\frac{1}{2}}(x)$ de complexité polynomiale en la précision. Dans notre article [20], nous allons plus loin dans cette direction en montrant comment utiliser la connexion de Gauss–Manin sur la fibration d'Asakura pour se ramener à une situation où le théorème 11 s'applique. Ce faisant, nous obtenons finalement un algorithme de complexité quasi-linéaire pour l'évaluation de la fonction hypergéométrique de Dwork en tout point du disque unité fermé.

2.4 Un soupçon de probabilités

En complément des applications arithmétiques évidentes, les nombres p-adiques offrent aussi un terrain de jeu idéal pour pratiquer les probabilités. En effet, l'anneau $\mathbb{Z}_p$ est naturellement muni d'une mesure de probabilité, qui n'est autre que sa mesure de Haar : selon elle, tirer un nombre aléatoire p-adique revient à tirer indépendamment chacun de ses chiffres selon une loi uniforme sur l'ensemble fini $\{0, 1, \dots, p-1\}$. Ainsi de nombreuses questions qui ont reçu énormément d'attention sur les nombres réels admettent souvent des analogues p-adiques qui n'ont, en général, pas été autant étudié, loin de là.

2.4.1 Polynômes aléatoires p-adiques

Référence :
[16] X. Caruso, *Where are the zeroes of a random p-adic polynomial ?*

Un exemple frappant est l'étude des polynômes aléatoires : alors que, pour ce qui concerne les polynômes aléatoires réels (ou complexes), la littérature foisonne, peu de travaux ont été entrepris vers l'étude des polynômes aléatoires p-adiques. Par exemple, s'il fait plus ou moins partie du folklore [2] qu'un polynôme aléatoire de degré $d \geqslant 0$ à coefficients dans $\mathbb{Z}_p$ a en moyenne une racine de $\mathbb{Q}_p$ (ceci indépendamment de p et de d), il semble que des questions plus précises sur la répartition des racines ou sur le comptage de celles-ci dans des corps plus gros n'aient jamais été abordées sérieusement. Pourtant, le cadre p-adique paraît immensément plus riche que le cadre réel étant donné que $\bar{\mathbb{Q}}_p$ vis-à-vis de $\mathbb{Q}_p$ est bien plus gros que $\mathbb{C}$ ne l'est vis-à-vis de $\mathbb{R}$.

Pour mes premiers pas en probabilités [3], je me suis donné pour objectif d'explorer cette question et je n'ai finalement pas été déçu des petites pépites que j'ai pû découvrir. Pour les énoncer de manière précise, j'ai besoin d'introduire quelques notations supplémentaires. Je note $|\cdot|_p$ la norme p-adique sur $\mathbb{Q}_p$, normalisée par $|p|_p = p^{-1}$. Je fixe une clôture algébrique $\bar{\mathbb{Q}}_p$ de $\mathbb{Q}_p$ et j'appelle $\mathcal{E}$ l'ensemble des extensions finies de $\mathbb{Q}_p$ incluses dans $\bar{\mathbb{Q}}_p$. Pour tout $L \in \mathcal{E}$, le discrimant de $L/\mathbb{Q}_p$ est un idéal de $\mathbb{Z}_p$; je note δ_L la norme p-adique d'un de ses générateurs.

Théorème 12. *Il existe une famille de nombre réels $(Z_{L,d})_{L\in\mathcal{E},d\in\mathbb{N}}$ vérifiant les propriétés suivantes :*

(i) pour $K \in \mathcal{E}$, le nombre moyen de racines d'un polynôme aléatoire de degré d à coefficients dans $\mathbb{Z}_p$ est égal à la somme des $Z_{L,d}$ pour $L \in \mathcal{E}$, $L \subset K$.

(ii) pour $L \in \mathcal{E}$, on a :

$$\begin{aligned} Z_{L,d} &= 0 && \text{si } d < [L:\mathbb{Q}_p] \\ Z_{L,d} &= \delta_L \cdot \big(1 + O\big(p^{-f/2}\big)\big) && \text{si } d \geqslant [L:\mathbb{Q}_p] \end{aligned}$$

où f est le degré résiduel de l'extension $L/\mathbb{Q}_p$ et où la constante cachée dans le $O(-)$ est une constante absolue.

Le théorème 12 nous dit donc que les racines d'un polynôme aléatoire de degré d à coefficients dans $\mathbb{Z}_p$ ont tendance à se repartir le long des extensions de $\mathbb{Q}_p$ qui sont de degré au plus d (évidemment !) et peu ramifiés. En particulier, une version légèrement raffinée de ce théorème indique qu'un polynôme aléatoire de degré d comme précédemment a, en moyenne :

- exactement une racine dans $\mathbb{Q}_p$,
- $1 - \frac{1}{p} + O\big(\frac{1}{p^2}\big)$ racine supplémentaire dans $\mathbb{Q}_{p^2}$,
- $1 + O\big(\frac{1}{p^2}\big)$ racine supplémentaire dans $\mathbb{Q}_{p^n}$ pour $3 \leqslant n \leqslant d-1$,
- $1 - \frac{1}{p} + O\big(\frac{1}{p^2}\big)$ racine supplémentaire dans $\mathbb{Q}_{p^d}$.

2. Ce résultat, apparemment, a été redécouvert ces dernières années de façon indépendante par, au moins, deux autres collègues.
3. Pas tout à fait, mais presque...

On en déduit qu'un tel polynôme a, en moyenne, $d - \frac{2}{p} + O\big(\frac{1}{p^2}\big)$ racines dans l'extension maximale non ramifiée de $\mathbb{Q}_p$. Par conséquence, il en a, toujours en moyenne, $\frac{2}{p} + O\big(\frac{1}{p^2}\big)$ à l'extérieur de cette extension. À partir du théorème 12, il est également possible d'estimer le nombre moyen de racines d'un polynôme aléatoire qui n'appartiennent pas à l'extension maximale modérément ramifiée de $\mathbb{Q}_p$; en ordre de grandeur, on en trouve $p^{-p+2} + O\big(p^{-p+1}\big)$.

2.4.2 Ensembles de Kakeya p-adiques

Référence :

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

Pendant l'été 2016, je me suis également intéressé 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 [4] 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.

Théorème 13. *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 13 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.

2.5 Rédaction de notes de cours

Durant les cinq dernières années, j'ai été amené à rédiger plusieurs notes de cours sur plusieurs sujets qui, mis ensemble, donnent finalement un aperçu assez complet de mes thématiques de recherche privilégiées.

2.5.1 Polynômes de Ore

Référence :

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

4. 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*.

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.

2.5.2 Calcul avec les nombres p-adiques

Référence :
[7] 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, qui sont à présent publiés dans la collection *Les cours du CIRM*.

2.5.3 Anneaux de périodes p-adiques

Référence :
[12] X. Caruso, *An introduction to p-adic period rings*

Suite à l'école d'été que j'ai co-organisée en 2014 avec Christophe Mourougane sur les théories de Hodge classique et p-adique, la rédaction d'un volume de *Panoramas et Synthèses* sur la partie p-adique a été initiée. J'ai contribué à la rédaction de ce volume par un article de survol sur les anneaux de périodes p-adiques de Fontaine. En guise d'introduction, j'étudie les propriétés de l'anneau de périodes $\mathbb{C}_p$ et je présente la théorie afférente des $\mathbb{C}_p$-représentations p-adiques dûe à Tate et à Sen. J'en viens ensuite aux anneaux de périodes B_{cris} et B_{dR} qui sont plus compliqués à définir et à étudier, mais qui permettent d'accéder à des propriétés beaucoup plus fines des représentations galoisiennes p-adiques.

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 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 ;

Informatique quantique (niveau M2) : il s'agit d'un cours dispensé dans le cadre du master de cryptographie de l'université de Bordeaux ; l'objectif du cours est de présenter le formalisme de l'informatique quantique, puis l'algorithme de factorisation de Shor ; j'ai donné ce cours en 2019 et en 2020, et il est prévu que je le réitère les années à venir ;

Mathématique, science et société (niveau L2) : il s'agit d'un cours où les étudiantes et les étudiants sont invités à préparer un exposé sur un sujet de leur choix montrant comment les mathématiques interviennent dans des questions de société.

Encadrement de stages

Durant les dix 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 ;

Adrien Chaud (niveau L1) : le sujet de ce stage pratique était la conception et la réalisation au FabLab de l'IUT de Gradignan d'un brachistochrone ; le travail réalisé a été, par la suite, présenté à une manifestation grand public organisée par la délégation régionale du CNRS pour fêter les 80 ans de l'insititut ;

Béranger Seguin (niveau M2) : le sujet du stage était de comprendre et de restituer les principaux résultats de la théorie des espaces de déformations galoisiennes de Mazur ;

Reem Chaalan (niveau M2) : le sujet du stage était d'étudier les algorithmes de décodage des codes de Gabidulin généralisés, puis à chercher à les accélérer dans le cas où le corps de base n'est pas un corps fini, en mettant en œuvre la théorie des sous-résultants de polynômes tordus ;

Raoul Hallopeau (niveau M2) : le sujet du stage était, dans un premier temps, de présenter un aperçu historique sur le développement de la cohomologie depuis les premiers résultats d'Euler et, dans un second temps, d'étudier la théorie des catégories dérivées ;

Raphaël Pagès (niveau M2) : le sujet du stage (coencadré avec A. Bostan) était de concevoir un algorithme rapide pour le calcul de multiples p-courbures d'un opérateur différentiel défini sur $\mathbb{Z}[t]$; ce travail a donné lieu à une prépublication qui a été soumise récemment à la conférence ISSAC.

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.

Séminaire de l'équipe LFANT

À mon arrivée à Bordeaux, j'ai été naturellement intégré à l'équipe projet INRIA LFANT (« Lithe and fast algorithmic number theory »). Depuis septembre 2019, j'assure avec mon collègue Aurel Page, l'organisation du séminaire de l'équipe. Comme beaucoup de séminaires, celui-ci se déroule désormais en ligne depuis l'arrivée de la pandémie.

Les 5 minutes Lebesgue

De novembre 2015 à juin 2018, j'ai été cofondateur et 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. Pendant que j'étais organisateur, 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.

3.1 Diffusion des mathématiques

Bien que je n'arrive pas à y consacrer autant de temps que je le souhaterais (comme toujours), la diffusion des mathématiques auprès de tous les publics m'a toujours très intéressée et j'essaie regulièrement d'y apporter ma contribution.

En janvier 2019 (juste après mon arrivée à l'IMB), j'ai accepté d'endosser le rôle, conjointement avec ma collègue Chantal Ménini, de chargé de mission pour la diffusion à l'IMB, qui m'a été proposé par la direction.

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

Depuis 2017, j'encadre régulièrement des groupes d'élèves de collège et de lycée dans le cadre de MATh.en.JEANS. 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*.

Réalisation d'applications web

Durant la période sous évaluation, j'ai réalisé plusieurs petites applications en ligne illustrant chacune, de manière ludique et/ou pédagogique, des propriétés étonnantes de certains objets mathématiques. Précisément, voici la liste de mes réalisations.

Une course qui permet de se rendre compte qu'en présence d'un gradient d'indice de réfraction, le chemin le plus rapide pour aller d'un point à un autre n'est pas la ligne droite (*cf* http://xavier.toonywood.org/popularization/applets/fastest/). Cette application est à mettre en parallèle avec le brachistochrone que nous avons fabriqué avec Adrien Chaud.

Deux promenades en 3D sur des surfaces plates de genre 1 (*cf* https://diffusion.math.u-bordeaux.fr/embed/walks/genus1.html) et de genre 2 (*cf* https://diffusion.math.u-bordeaux.fr/embed/walks/genus2.html) ; la métrique sur le surface de genre 2 présente une singularité (la fontaine) qui est à l'origine de phénomènes déroutants. J'ai récemment entâmé une collaboration avec le PIRVI pour améliorer le rendu de ces promenades et en réaliser d'autres, notamment dans un espace hyperbolique.

Une variante du célèbre jeu de 2048 avec la suite de Fibonacci (*cf* https://diffusion.math.u-bordeaux.fr/embed/987). Au délà la suite de Fibonacci, quelques études mathématiques à partir de ce jeu conduisent naturellement à explorer les fractions continues et les mots sturmiens.

Un article, écrit sous forme de dialogue, sur les pavages de l'hexagone régulier et le théorème du cercle arctique (*cf* https://diffusion.math.u-bordeaux.fr/tilehexa) ; le visuel de cet article a été proposé à un concours organisé par la délégation régionale du CNRS pour affichage sur la façade de son bâtiment pendant une année entière, mais n'a malheureusement pas été retenu.

4 Transfert technologique, relations industrielles et valorisation

5 Encadrement, animation et management de la recherche

Direction de thèses

La thèse de Elie Eid. Avec Reynald Lercier, j'encadre depuis septembre 2018 la thèse de Elie Eid. Elle porte sur la conception d'algorithmes rapides pour le calcul d'isogénies sur des corps de caractéristique 2 ou sur des extensions du corps des nombres 2-adiques $\mathbb{Q}_2$. Les méthodes employées consistent à passer par la résolution d'une équation différentielle 2-adique. La rédaction du manuscript de thèse est en cours de finalisation et la soutenance de la thèse est prévue pour le mois de juin 2021.

La thèse de Amaury Durand. J'encadre depuis septembre 2019 la thèse de Amaury Durand. Initialement, l'objectif de la thèse était de définir et d'étudier un analogue géométrique des codes de Gabidulin. Toutefois, à cause de problèmes personnels rencontrés par Amaury, je ne suis pas sûr que cet objectif pourra être tenu. Actuellement, Amaury a déjà effectué un premier travail dans lequel il étend les résultats de mon article [17] aux polynômes de Ore différentiels. J'espère que ce travail pourra être rédigé et soumis dans les meilleurs délais.

La thèse de Raphaël Pagès. Avec Alin Bostan, j'encadre depuis septembre 2020 la thèse de Raphaël Pagès dont l'objectif est de concevoir des algorithmes efficaces pour la factorisation des opérateurs différentiels en caractéristique positive.

Projets de recherche

Le projet CLap–CLap

Depuis septembre 2018, je suis le principal coordinateur du 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. À ce titre, j'ai organisé une première rencontre de lancement du projet et une conférence internationale dans le cadre du semestre thématique *Correspondances* du Centre Henri Lebesgue.

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. Tout au cours de l'année 2018, 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.

B. Objectifs

Au début de ma carrière, je prenais toujours un plaisir certain à écrire des projets de recherche : j'aimais poser mon regard au loin, dresser de grandes lignes droites pour atteindre ce que j'avais cru entrevoir, j'aimais me convaincre que la recherche était un long fleuve tranquille et qu'il était certain que, à quelques broutilles près qu'il ne resterait plus qu'à régler, le monde mathématique que je m'étais imaginé était conforme à la réalité. J'étais confiant, bien trop confiant, également dans la facilité avec laquelle j'arriverai à régler ces broutilles ou, dans le pire des cas, à persévérer sans relâche jusqu'à y parvenir. Finalement, je crois que ce que je trouvais attirant dans la rédaction des projets de recherche était la possibilité qui m'était offerte de pouvoir énoncer des théorèmes (ou disons, plutôt des questions) et d'en omettre les démonstrations.

Quinze années plus tard, après avoir rédigé presque autant de projets de recherche, je dois avouer que mon enthousiasme de jeunesse s'est adouci. Le destin s'est joué de moi comme il se doit, les grands projets que j'avais élaborés n'ont, en réalité, généralement pas réussi à depasser le stade de la pré-maturation [5] et, jusqu'à présent, le principal moteur de ma recherche a été les rencontres aléatoires qu'il m'a été donné de faire, ainsi que quelques idées nouvelles qui, presque systématiquement, se sont introduites dans mon esprit sans que je ne m'y attende véritablement, presque par surprise, dirais-je. Non pas, comprenons-nous bien, que les projets que j'avais rédigés étaient voués à l'échec — je continue de croire que plusieurs d'entre eux ont un potentiel certain — mais plutôt que, le moment venu, j'ai été attiré par d'autres chemins qui m'ont semblé mieux résonner avec ce que j'avais réellement envie de faire. Ces nouveaux chemins qui, bien qu'initialement semblaient très proches de mes objectifs, s'en sont éloignés progressivement et m'ont finalement conduit vers de nouveaux horizons.

Bref, je dois bien admettre que je ne suis pas de ceux qui veulent, ni même qui peuvent, maintenir un cap sur le long terme ; non, je suis de ceux qui s'arrêtent quelque temps sur une idée qu'ils affectionnent, puis s'en vont papillonner ailleurs. Cela ne m'empêche pas cependant, je pense, de conserver une cohérence forte dans mes activités de recherche. Simplement, j'aime aborder une même problématique par différents angles, différents points de vue qui, souvent, m'arrivent soudainement et, parfois, repartent tout aussi brutalement.

C'est ainsi que l'exercice qui consiste à écrire un nouveau projet de recherche *pour les cinq années à venir* me paraît bien difficile, pour ne pas dire hors de portée. Bien entendu, j'ai plusieurs pistes de recherche que j'ai envie d'explorer (voire que j'ai déjà commencé à explorer) *en ce moment*, mais je ne saurais dire avec quelle intensité elles continueront à m'animer dans quelques mois (lorsque vous lirez ce rapport) et, encore moins, dans un an ou deux.

Malgré tout, voici un aperçu rapide de mes projets actuels. Les deux premiers concernent des questions d'uniformité en p, alors que les trois derniers portent sur la théorie des équations différentielles p-adiques, deux sujets qui me questionnent particulièrement ces temps-ci.

1. (*cf* §2.1.3) Comprendre les liens entre le groupe de Galois différentiel de la diagonale d'une fraction rationnelle et le groupe de Galois algébrique de ses réductions modulo p. À première vue, il me semble que le formalisme tannakien (déjà utilisé par Katz pour énoncer sa conjecture rafinée sur la p-courbure) puisse être une piste intéressante.
2. (*cf* §2.2.1) Au-délà de l'exemple des déformations potentiellement Barsotti–Tate de dimension 2, mieux comprendre la dépendance vis-à-vis de p de la géométrie des espaces de déformations galoisiennes et/ou des poids de Serre. Dans cette direction, une idée folle pourrait être d'envisager une correspondance de Langlands 1-adique (sur l'anneau des vecteurs de Witt du fameux corps à 1 élément) qui fournerait, par extension des scalaires, (une partie de) la correspondance de Langlands p-adique pour (presque) tout p.
3. (*cf* §2.2.2) Développer encore davantage la théorie des bases de Gröbner sur les algèbres de Tate (notamment en systématisant l'utilisation de l'arithmétique détendue de van der Hoeven et al.) afin d'arriver enfin à traiter en pratique des exemples de taille significative. Utiliser ces algorithmes

5. Comme on le dit, ai-je appris récemment, dans le domaine de l'innovation...

comme primitives pour proposer une implémentation des variétés rigides et des opérations courantes sur celles-ci (jusqu'à inclure, si les obstacles ne sont pas trop grands, le calcul de la cohomologie).

4. (*cf* §2.2.3) Étudier de manière systématique, les équations différentielles p-adiques non linéaires et leurs déformations ; en particulier, j'aimerais obtenir un théorème qui relie les variations des rayons de convergence d'une équation non linéaire à ceux de l'équation linéaire obtenue par perturbation au premier ordre. Dans la même direction, je me demande dans quelle mesure les résultats classiques sur le comportement des rayons de convergence dans le cadre linéaire s'étendent au cadre non linéaire.
5. (*cf* §2.3.3) Progresser sur l'évaluation rapide des fonctions spéciales p-adiques ; en particulier, nos algorithmes actuels ont une mauvaise complexité en p lorsque les équations différentielles sous-jacentes proviennent de la commutation du Frobenius à la connexion de Gauss–Manin ; pouvoir surmonter cette difficulté me paraît une question importante (sur laquelle, à vrai dire, je n'ai malheureusement que peu d'idées). Également, pouvoir traiter de façon systématique le cas des fonctions renormalisées de Dwork me paraît intéressant mais, à nouveau, je n'ai pas vraiment de piste pour le moment.
6. Finaliser mon implémentation de l'algorithmique détendue en SageMath [6] et l'utiliser pour implémenter des algorithmes efficaces de factorisation des opérateurs différentiels sur $\mathbb{Q}_p(t)$ puis, dans un second temps, utiliser ces algorithmes pour calculer les rayons de convergence des équations différentielles p-adiques (linéaires, voire non linéaires).

6. Voir https://trac.sagemath.org/ticket/31108

MA BIBLIOGRAPHIE DES DIX DERNIERS SEMESTRES

Articles de recherche

Articles publiés pendant les 10 derniers semestres

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

[2] 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

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

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

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

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

[7] X. Caruso, *Computations with p-adic numbers*, Les cours du CIRM **5**, cours II (2017), 1–75

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

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

[10] X. Caruso, *Almost all non-archimedean Kakeya sets have measure zero*, Confluentes Math. **10** (2018), 3–40

[11] A. Bostan, X. Caruso, G. Christol, P. Dumas, *Fast coefficient computation for algebraic power series in positive characteristic*, The Open Book Series **2** (2019), 119–135

[12] X. Caruso, *An introduction to p-adic period rings*, Panoramas et Synthèses **54** (2019), 19–92

[13] X. Caruso, T. Vaccon, T. Verron, *Gröbner bases over Tate algebras*, proceddings de la conférence ISSAC 2019

[14] X. Caruso, T. Vaccon, T. Verron, *Signature-based algorithms for Gröbner bases over Tate algebras*, proceddings de la conférence ISSAC 2020

Prépublications rédigées pendant les 10 derniers semestres

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

[16] X. Caruso, *Where are the zeroes of a random p-adic polynomial ?*, notes d'exposé (2018), 6 pages

[17] X. Caruso, *Residues of skew rational functions and linearized Goppa codes*, prépublication (2019), 51 pages

[18] X. Caruso, E. Eid, R. Lercier, *Fast computation of elliptic curve isogenies in characteristic two*, prépublication (2020), 30 pages

[19] X. Caruso, T. Vaccon, T. Verron, *On FGLM algorithm with Tate algebras*, prépublication (2021), 8 pages

[20] X. Caruso, M. Mezzarobba, T. Vaccon, N. Takayama, *Fast evaluation of some p-adic transcendental functions*, prépublication (2021), 8 pages

Quelques travaux en cours

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

[22] X. Caruso, A. David, A. Mézard, *Combinatorics of Serre weights in the potentially Barsotti–Tate setting : the non generic case*, en préparation

[23] B. Adamczewski, A. Bostan, X. Caruso, G. Christol, R. Yassawi, *A sharp quantitative version of multivariate Christol's theorem, and applications*, en préparation

Production logicielle

Logiciels écrits pendant les 10 derniers semestres

[24] 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

[25] X. Caruso, D. Roe, J. Rüth, *ZpL : a p-adic precision package*, librairie SAGEMATH (2018), https://trac.sagemath.org/ticket/23505, $\sim$ 5000 lignes

[26] X. Caruso, *Un cadre général pour les extensions d'anneaux*, librairie SAGEMATH (2019), https://trac.sagemath.org/ticket/21413, $\sim$ 6000 lignes

[27] X. Caruso, T. Verron, *Bases de Gröbner sur les algèbres de Tate*, librairie SageMath (2020), https://trac.sagemath.org/ticket/26195 et https://trac.sagemath.org/ticket/28777 $\sim$ 6000 lignes

[28] X. Caruso, *Anneaux de polynômes de Ore et corps des fractions*, librairie SageMath (2020), https://trac.sagemath.org/ticket/21264, https://trac.sagemath.org/ticket/29629 et https://trac.sagemath.org/ticket/29678, $\sim$ 5000 lignes

[29] X. Caruso, *Espaces de déformations potentiellement Barsotti–Tate*, librairie SageMath (2020) $\sim$ 4000 lignes

Autres articles

Articles publicitaires écrits pendant les 10 derniers semestres

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

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

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

[33] 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