# Rapport à mi-vague de Xavier Caruso

## Période : décembre 2021 — juin 2024

# A. Rapport d'activité

## 1 Curriculum vitæ

Xavier Caruso
né le 24 avril 1980 à Cannes
IMB – Université de Bordeaux
351, cours de la Libération
33405 Talence
Tél : 05 40 00 21 59
E-Mail : xavier@caruso.ovh
Page web : http://xavier.caruso.ovh/
Marié, trois enfants

### Parcours scolaire et professionnel

**2023** Promu directeur de recherche, 1ème classe (DR1)

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

**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

**2022–** Directeur adjoint de l'IMB, responsable de la cellule informatique

**2022** Président du comité HCERES de l'I2M (Institut de Mathématiques de Marseille)

**2020–2023** Membre suppléant au CNU (Conseil National des Universités)

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

**2017–2023** 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)

# 2 RECHERCHE SCIENTIFIQUE

Durant ces cinq derniers semestres, mes activités de recherche se sont concentrées principalement sur les polynômes de Ore (un sujet sur lequel j'ai déjà beaucoup travaillé par le passé) et plusieurs de leurs applications : (1) à des problèmes d'algébricité et de transcendance, (2) à la théorie des codes correcteurs d'erreurs, et (3) à l'arithmétique des corps de fonctions, *via* les modules de Drinfeld. Si les deux premières avaient déjà retenu mon attention par le passé, l'étude des modules de Drinfeld est, pour moi, nouvelle. Par de nombreux aspects, elle a été l'occasion de faire le pont avec certaines problématiques et/ou constructions de la théorie de Hodge $p$-adique que j'avais étudiées il y a longtemps et qui m'étaient restées chères.

## Préambule : choix de cinq publications signficatives

Pour ce rapport, on me demande de procéder à un choix de cinq de mes publications (ou pré-publications, j'imagine). Je ne suis pas certain que cet exercice soit vraiment pertinent pour les mathématiciens et mathématiciennes, étant donné que nous avons tendance à publier moins d'articles que dans certaines autres disciplines et que, pour une majorité écrasante de cas, chaque article publié représente un véritable investissement. Ceci dit, comme j'ai plus de cinq publications sur la période, je me plie aux demandes de la direction et sélectionne les items suivants qui, à mon avis, sont représentatifs des domaines dans lequels je me suis le plus investi durant les cinq derniers semestres.

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

[4] X. Caruso, A. David, A. Mézard, *Combinatorics of Serre weights in the potentially Barsotti–Tate setting*

[7] E. Berardini, X. Caruso, *Algebraic geometry codes in the sum-rank metric*

[8] X. Caruso, Q. Gazda, *Computation of classical and $v$-adic $L$-series of $t$-motives*

[10] B. Adamczewski, A. Bostan, X. Caruso, *A sharper multivariate Christol's theorem with applications to diagonals and Hadamard products*

Dans la suite, j'évoque néanmoins la (quasi-)intégralité de ma recherche, sans me restreintre aux cinq articles précédents. La raison en est que j'aime présenter mon activité de recherche comme une aventure humaine, ponctuée par les rencontres qui influence le fil de ma pensée et mes thèmes de prédilection. Pour moi, ce rapport d'activité est le lieu idéal pour prendre ce recul sur les événements qui ont ponctué ma carrière de mathématicien, et donner une image vivante de la recherche en mathématiques [1].

## 2.1 Reminiscences

Je débute ce rapport d'activité par des travaux que j'avais déjà évoqués dans mes précédents rapports et que j'ai finalisés durant la période sous évaluation.

### 2.1.1 Espaces de déformations

*Références* :
[4] X. Caruso, A. David, A. Mézard, *Combinatorics of Serre weights in the potentially Barsotti–Tate setting*
[5] X. Caruso, A. David, A. Mézard, *Can we dream of a 1-adic Langlands correspondence ?*
[13] X. Caruso, A. David, A. Mézard, *Déformations potentiellement Barsotti-Tate*, librairie SAGEMATH (2022)

Le premier d'entre eux concerne ma collaboration suivie avec Agnès David et Ariane Mézard avec qui nous étudions certains espaces de déformations galoisiennes $p$-adiques, en lien avec la correspondance de Langlands $p$-adique et la conjecture de Breuil–Mézard. Plus précisément, nous considérons une extension finie non ramifiée $F$ de $\mathbb{Q}_p$, ainsi qu'un corps $p$-adique $E$ suffisamment gros. Nous nous intéressons aux déformations potentiellement Barsotti–Tate d'une représentation résiduelle $\bar{\rho} : G_F \to \mathrm{GL}_2(k_E)$ où $G_F$ désigne le groupe de Galois absolu de $F$ et $k_E$ est le corps résiduel de $E$. Ces déformations sont paramétrées par une donnée supplémentaire : le type galoisien $t$.

1. Tout en étant conscient, évidemment, que les membres du CoNRS ne sont pas les premiers à convaincre à ce sujet ; toutefois, je laisse aussi en libre accès mes rapports d'activité sur ma page web, espérant — sans doute très naïvement — pouvoir ainsi toucher occassionnellement d'autres personnes.

Pour calculer les anneaux de déformations correspondants $R(\bar{\rho}, t)$, nous suivons une méthode initiée par Kisin qui consiste à déformer, non pas des représentations galoisiennes, mais des modules de Breuil–Kisin, un objet d'algèbre semi-linéaire plus simple à manipuler. La première étape de la méthode consiste à déterminer la variété de Kisin $\mathcal{V}(\bar{\rho}, t)$ associée à la situation. Il s'agit d'un travail que nous avons réalisé en 2016 et, dans lequel, nous avons mis en évidence le rôle du *gène*, un objet combinatoire épuré qui décrit complètement la géométrie de la variété de Kisin. Dans le même travail, nous avons conjecturé que le même gène détermine également la fibre générique de l'anneau de déformations recherché, et avons proposé un candidat explicite pour ce dernier.

Nous nous sommes ensuite intéressés à la fibre spéciale. Cette dernière est une variété singulière qui, en vertu de la conjecture de Breuil–Mézard (qui est démontrée dans ce cadre), s'écrit comme une union de composantes indexée par un ensemble $\mathcal{D}(\bar{\rho}, t)$ de *poids de Serre* [2]. Dans [4], nous démontrons que le gène détermine $\mathcal{D}(\bar{\rho}, t)$ par une recette algorithmique entièrement explicite (que nous avons implémentée dans [13]), ce qui nous a amené à conjecturer qu'il détermine finalement aussi l'espace de déformations $R(\bar{\rho}, t)$ dans sa globalité. Nous allons en réalité plus loin en donnant des précisions importantes sur les énoncés (démontrés et conjecturaux) précédents. Tout d'abord, nous renforçons les liens entre gènes et variétés de Kisin, en démontrant que ces deux objets encodent exactement les mêmes informations pour peu que l'on munisse les variétés de Kisin de données supplémentaires : leur plongement canonique dans $(\mathbb{P}^1)^{[F:\mathbb{Q}_p]}$, d'une part, et leur stratification par le genre, d'autre part. Ceci nous permet de reformuler nos énoncés de manière plus intrinsèque en évitant toute mention du gène et, mieux encore, de mettre en évidence une structure multiplicative sur tous les objets concernés. Ainsi, la forme finale de notre conjecture s'énonce comme suit.

**Conjecture 1.** *Il existe un morphisme de monoïdes :*

$$R : \left\{ \begin{array}{c} \textit{variétés de Kisin} \\ \textit{plongées et stratifiées} \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \textit{$\mathcal{O}_E$-algèbres} \\ \textit{complètes et noethériennes} \end{array} \right\}$$

*tel que* $R(\bar{\rho}, t) \simeq R\big(\mathcal{V}(\bar{\rho}, t)\big)$ *pour tout* $\bar{\rho}, t$.

Une partie de la conjecture ci-dessus a été démontrée récémment par Le Hung, Mézard et Morra.

Une conséquence frappante de nos travaux est que le nombre premier $p$, bien que fixé depuis la première ligne de l'article et absolument nécessaire à la définition des objets, semble jouer un rôle secondaire, voire complètement figuratif : il n'intervient pas dans la définition du gène, il n'intervient aussi pratiquement pas dans nos recettes combinatoires, *etc.* Pour cette raison, nous en sommes venus à penser qu'il pourrait exister un dénominateur commun, indépendant de $p$, à la correspondance de Langlands $p$-adique ou, au moins, à certains de ses aspects. Nous avons rédigé l'article [5] (déposé sur arXiv un 1er avril) dans lequel nous faisons l'hypothèse de l'existence d'une correspondance de Langlands 1-adique qui serait ce mystérieux dénominateur commun. Nous donnons du crédit à cette hypothèse en interprétant le gène comme (le squelette d')une variété de Kisin 1-adique. Nous commençons également à développer dans *loc. cit.* une théorie galoisienne des extensions finies de $\mathbb{F}_1$ et de $\mathbb{Q}_1$, prémice indispensable, s'il en est, à la mise en place d'une correspondance de Langlands 1-adique, si elle existe.

### 2.1.2 Polynômes $p$-adiques aléatoires

*Référence* :

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

Dans un autre registre, je me suis intéressé aux racines des polynômes aléatoires à coefficients dans $\mathbb{Z}_p$. Un des intérêts de travailler dans le monde $p$-adique est que, contrairement à $\mathbb{R}$, le corps $\mathbb{Q}_p$ admet toute une panoplie d'extensions algébriques, et donc autant d'endroits intéressants où chercher les solutions d'équations polynomiales. Dans tout ce qui suit, $\bar{\mathbb{Q}}_p$ désigne une clôture algébrique fixée de $\mathbb{Q}_p$.

Suivant une méthode, classique dans le cas réel, je m'intéresse au nombre moyen de racines : étant donnés une extension finie $E$ de $\mathbb{Q}_p$ incluse dans $\bar{\mathbb{Q}}_p$ et un ouvert $U$ de $E$, je note $Z_n(U)$ l'espérance du nombre de zéros dans $U$ d'un polynôme aléatoire [3] de degré $n$. Je démontre alors le théorème suivant.

2. Ce sont des représentations irréductibles de $\mathrm{GL}_2(k_F)$.
3. Les coefficients sont tirés de manière indépendante selon la mesure de Haar sur $\mathbb{Z}_p$

**Théorème 2.** *Il existe une famille de fonctions $\rho_{K,n} : K \to \mathbb{R}^+$ indexées par les sous-extensions finies $K \subset \bar{\mathbb{Q}}_p$ telles que, pour tout $E$ et $U$ comme précédemment, on ait :*

$$Z_n(U) = \sum_{K \subset E} \int_{U \cap K} \rho_{K,n}(x) dx. \tag{1}$$

*De plus, en notant $r = [K{:}\mathbb{Q}_p]$, les fonctions $\rho_{K,n}$ vérifient les propriétés suivantes.*

1. (Annulation) *Si $\mathbb{Q}_p[x] \neq K$ ou $n < r$, alors $\rho_{K,n}(x) = 0$.*
2. (Continuité) *Les fonctions $\rho_{K,n}$ sont continues sur $K$.*
3. (Invariance par isomorphisme) *Étant donnés une deuxième extension finie $L$ de $\mathbb{Q}_p$ et un isomorphisme $\sigma : K \to L$, on a $\rho_{K,n}(x) = \rho_{L,n}\big(\sigma(x)\big)$.*
4. (Transformation par homographie) *Pour $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}_p)$, on a :*
$$\rho_{K,n}\left(\frac{ax+b}{cx+d}\right) = \|cx+d\|^{2r} \cdot \rho_{K,n}(x).$$
5. (Monotonie) *On a $\rho_{K,n}(x) \leqslant \rho_{K,n+1}(x)$ et l'inégalité est stricte si et seulement si $\mathbb{Q}_p[x] = K$ et $r \leqslant n < 2r-1$.*
6. (Formules pour les degrés extrémaux) *Si $\mathbb{Q}_p[x] = K$ et $x \in \mathcal{O}_K$ (anneau des entiers de $K$), alors*
$$\begin{aligned} \rho_{K,r}(x) &= |D_K|_p \cdot \frac{1}{\mathrm{Card}\big(\mathcal{O}_K/\mathbb{Z}_p[x]\big)} \cdot \frac{q^{r+1}-q^r}{q^{r+1}-1} \\ \text{pour } n \geqslant 2r-1, \quad \rho_{K,n}(x) &= |D_K|_p \cdot \int_{\mathbb{Z}_p[x]} |t|_p^r \, dt \end{aligned} \tag{2}$$
*où $D_K$ est le discriminant de $K$ et $|\cdot|_p$ est la norme $p$-adique normalisée par $|p|_p = 1/p$.*

Les fonctions $\rho_{K,n}$ donnent ainsi la densité de présence d'une racine « nouvelle », c'est-à-dire une racine qui n'appartient à aucun sous-corps strict ou, de manière équivalente, qui engendre le corps $K$ sur $\mathbb{Q}_p$. Les propriétés énumérées dans le théorème 2 nous apprennent plusieurs choses : la formule (1) nous enseigne que les racines se concentrent le long des sous-extensions, tandis que les formules explicites (2) indiquent que le nombre moyen de racines nouvelles dans une extension donnée est directement lié à la norme de son discriminant : *grosso modo*, il faut s'attendre à une racine nouvelle environ dans chaque extension non ramifiée, à $\frac{1}{p}$ racine nouvelle dans une extension modérément ramifiée et encore moins que cela dans les extensions sauvagement ramifiées.

Enfin, je démontre une généralisation du théorème 2 au cas où $E$ est une algèbre finie étale, c'est-à-dire un produit d'extensions finis de $\mathbb{Q}_p$. Ce cas est intéressant pour plusieurs raisons. Premièrement, il donne les clés pour calculer, au delà de l'espérance, les moments d'ordre supérieur du nombre de zéros d'un polynôme aléatoire $p$-adique. C'est ainsi que j'ai pu mettre en évidence un phénomène (classique dans le cas de $\mathbb{R}$) de répulsion des racines. Deuxièmement, il permet d'énoncer une formule sommatoire que je trouve particulièrement élégante :

**Théorème 3.** *Pour une algèbre finie étale $E$, on note $\rho_n(E) = \int_E \rho_{E,n}(x)dx$ le nombre moyen de racines nouvelles dans $E$ d'un polynôme aléatoire $p$-adique de degré $n$. Pour tous entiers $n$ et $r$ avec $n \geqslant r$, on a :*

$$\sum_{E \in \text{Ét}_r} \frac{\rho_n(E)}{\mathrm{Card}\ \mathrm{Aut}(E)} = 1$$

*où $\text{Ét}_r$ désigne l'ensemble des algèbres étales de degré $r$ sur $\mathbb{Q}_p$ modulo isomorphisme.*

Lorsque $r = 1$, il n'y a qu'une algèbre étale de degré 1, à savoir $\mathbb{Q}_p$ lui-même ; ainsi la formule précédente dit qu'un polynôme $p$-adique a en moyenne une racine dans $\mathbb{Q}_p$. Le théorème 3 généralise cet énoncé simple et frappant aux extensions de degré supérieur : il dit qu'un polynôme $p$-adique de degré au moins $r$ a en moyenne $r$ racines nouvelles dans les algèbres étales de degré $r$. On prendra garde au fait que ce résultat ne vaut pas du tout si l'on se restreint aux extensions de degré $r$. Par exemple, pour $r = 2$, on pourra retenir qu'il y a en moyenne à peu près une racine nouvelle dans $\mathbb{Q}_{p^2}$ et une autre dans $\mathbb{Q}_p \times \mathbb{Q}_p$ ; aucune de ces deux moyennes n'est exactement 1 mais les écarts se compensent parfaitement de sorte que la somme vaille exactement 2.

### 2.1.3 Un théorème de Christol multivarié

*Référence* :

[10] B. Adamczewski, A. Bostan, X. Caruso, *A sharper multivariate Christol's theorem with applications to diagonals and Hadamard products*

L'origine du travail que je vais présenter maintenant remonte à un article publié en 2019 où mes co-auteurs, Alin Bostan, Gilles Christol et Philippe Dumas, et moi-même proposions un nouvel algorithme pour calculer rapidement le coefficient $a_N$ d'une série $f(x) = \sum a_n x^n \in \mathbb{F}_p((x))$ algébrique sur $\mathbb{F}_p(x)$. Pour ce faire, mettant au point une nouvelle méthode, nous démontrions une version effective d'un célèbre théorème de Christol reliant algébricité d'une série formelle sur $\mathbb{F}_p$ et $p$-automaticité de la suite de ses coefficients.

Suite à la publication de cet article, 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. Rapidement, nous nous sommes rendus compte que c'était bel et bien le cas et nous avons finalement entâmé une collaboration à trois (impliquant Alin, Boris et moi-même) pour rédiger la démonstration et étudier les conséquences de ce nouveau résultat. Le théorème clé que nous démontrons s'énonce comme suit.

**Théorème 4.** *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 :*

$$\begin{array}{rccc} S_{\underline{r}} : & \mathbb{F}_p[[\underline{t}]] & \longrightarrow & \mathbb{F}_p[[\underline{t}]] \\ & \sum a_{\underline{i}} t^{\underline{i}} & \mapsto & \sum a_{p\underline{i}+\underline{r}} t^{\underline{i}} \end{array}$$

*pour $\underline{r}$ variant dans $\{0, 1, \dots, p-1\}^n$.*

Le théorème ci-dessus permet d'apporter de nouveaux éclairages sur plusieurs constructions classiques de la théorie : diagonales de fractions rationelles, produits d'Hadamard de séries algébriques, *etc.* Dans tous les cas, il permet d'améliorer de manière spectaculaire (passant souvent d'une tour d'exponentielles à une expression polynômiale) les bornes existantes sur la complexité du résultat de ces constructions.

Ci-dessous, je présente rapidement le cas des diagonales de fractions rationnelles qui, à mon avis, présente un intérêt particulier. Rappelons pour commencer 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 $g_p = \mathrm{Diag}(f)$ mod $p$ sur $\mathbb{F}_p(x)$. Cette question a été abordée par Deligne dans le cas des fonctions bivariées : dans ce cas, il a démontré que $d_p(f) \in O(p^H)$ pour une certaine constante $H$. En 2013, Adamczewski et Bell ont démontré que cette estimation vaut encore pour les fonctions algébriques en un nombre quelconque de variables ; toutefois, la constante $H$ qu'ils obtiennent est faramineuse, c'est une tour d'exponentielles en $d$ et en les $h_i$ dont la taille croît au moins linéairement avec le nombre de variables ! En comparaison, grâce au théorème 4, nous démontrons que $H = (h_1 + 1) \cdots (h_n + 1) \cdot (d + 1)$ convient dans tous les cas.

La situation est en réalité encore meilleure car il suit de notre démonstration que, pour presque tout $p$, la diagonale $g_p$ admet un polynôme annulateur de la forme

$$P(X) = c_0(t) \cdot X + c_1(t) \cdot X^q + c_2(t) \cdot X^{q^2} + \cdots + c_H(t) \cdot X^{q^H} \qquad (c_i(t) \in \mathbb{F}_p(\underline{t}))$$

ce qui, à son tour, implique que 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 m'a paru naturel de se poser la question de l'uniformité en $p$ : le plus naïvement possible, on peut se demander s'il existe un sous-groupe $G \subset \mathrm{GL}_H(\mathbb{Z})$ tel que $G_p$ soit la réduction modulo $p$ de $G$ pour presque tout $p$. J'ai proposé ce sujet de recherche à un étudiant de Vienne, Florian Fürnsinn, avec qui nous avons commencé à étudier des exemples. Calculer les groupes de Galois $G_p$ n'est pas une tâche aisée mais nous avons réussi à la mener (presque) à terme dans certaines situations simples. Suffisamment, en tout cas, pour nous rendre compte que, malheureusement, la conjecture naïve formulée précédemment est fausse.

Ne nous décourangeant cependant pas, nous avons invité Daniel Vargas-Montoya à rejoindre le projet et nous nous sommes concentrés, pour commencer, sur les fonctions hypergéométriques (qui, à vrai dire, ne sont pas définies comme des diagonales mais pour lesquelles on s'attend néanmoins à avoir des résultats similaires). Nos premiers calculs sont encourageants : nous avons réussi à déterminer une panoplie de groupes de Galois $G_p$, et avons remarqué de nombreux motifs qui paraissent en accord avec une dépendance contrôlée vis-à-vis de $p$. Plusieurs subtilités apparaissent toutefois et, bien que nous sentons que nous nous approchons du but, la formumation d'une conjecture générale dans la veine de ce que nous recherchons nous échappe encore. Ce travail me tient véritablement à cœur et j'espère y revenir avec de bonnes nouvelles dans mon prochain rapport d'activité.

## 2.2 Codes en métrique somme-rang

Faisant également suite à des travaux antérieurs mentionnés dans mes précédents rapports d'activité, j'ai continué à m'intéresser aux codes correcteurs d'erreurs en métrique somme-rang que j'étudie généralement *via* l'angle des polynômes de Ore.

### 2.2.1 Duaux des codes de Reed–Solomon linéarisés

*Référence* :
[3] X. Caruso, A. Durand, *Duals of linearized Reed-Solomon codes*

Je rappelle brièvement que si $K$ est un anneau muni d'un endomorphisme $\sigma : K \to K$ (resp. d'une dérivation $\delta : K \to K$) l'anneau des polynômes de Ore $K[X;\sigma]$ (resp. $K[X;\delta]$) est l'ensemble des polynômes $\sum a_i X^i$ muni de l'addition usuelle et de la multiplication déduite de la règle

$$Xa = \sigma(a)X \quad (\text{resp. } Xa = aX + \delta(a))$$

valable pour tout $a \in K$. En remplaçant les polynômes usuels par des polynômes de Ore dans la construction classique de Reed–Solomon (qui consiste, rappelons-le brièvement, à évaluer des polynômes de degré $k$ en un $n$ points avec $n > k$), on peut définir des codes intéressants. Pour ce faire, un préliminaire incontournable est de disposer d'une bonne notion d'évaluation des polynômes de Ore. Malheureusement, remplacer simplement la variable $X$ par une valeur scalaire $\alpha \in K$ n'est pas satisfaisant car l'application $K[X;\sigma] \to K$ (resp. $K[X;\delta] \to K$) qui s'en déduit n'est pas un morphisme d'anneaux. Pour conserver cette propriété essentielle, il faut au contraire évaluer en certains endomorphismes particuliers, à savoir ceux de la forme $c\theta$ (resp. $\delta + c\cdot\mathrm{id}$) pour $c$ variant dans $K$. On obtient, ce faisant, des morphismes d'évaluation

$$\begin{array}{rccc} \varepsilon_c : & K[X;\sigma] & \longrightarrow & \mathrm{End}_F(K) \\ & f(x) & \mapsto & f(c\theta) \end{array} \qquad \text{resp.} \qquad \begin{array}{rccc} \varepsilon_c : & K[X;\delta] & \longrightarrow & \mathrm{End}_F(K) \\ & f(x) & \mapsto & f(\delta + c\cdot\mathrm{id}) \end{array}$$

où $F$ est le sous-anneau des points fixes par $\theta$ (resp. le sous-anneau des constantes de $\delta$). Lorsque $K$ est un corps et $F$ est un sous-corps d'indice fini, l'espace d'arrivée des morphismes $\varepsilon_c$ est isomorphe à une algèbre de matrices. De surcroît, on dispose d'une formule qui borne le « nombre de zéros » d'un polynôme de Ore $f$ en fonction de son degré :

$$\sum_{c \in K^{\mathrm{nr}}/\sim} \dim_F \ker \varepsilon_c(f) \leqslant \deg f \tag{3}$$

où $K^{\mathrm{nr}}$ est un sous-ensemble de $K$ évitant au plus un point et $\sim$ est une relation d'équivalence sur $K^{\mathrm{nr}}$. Lorsque $K = \mathbb{F}_q$ est un corps fini et $\theta$ est le morphisme de Frobenius (de sorte que $F = \mathbb{F}_p$), on

a simplement $K^{\mathrm{nr}} = K\backslash\{0\}$ et deux éléments sont équivalents si et seulement s'ils ont la même norme sur $\mathbb{F}_p$.

En combinant les $\varepsilon_c$ pour différentes valeurs de $c$, on obtient des morphismes de multi-évaluation à partir desquels on définit des codes intéressants : le code de Reed–Solomon linéarisé associé aux paramètres $k \in \mathbb{N}$ et $\underline{c} = (c_1, \dots, c_n) \in (K^{\mathrm{nr}})^n$ est l'image du sous-espace des polynômes de Ore de degré strictement inférieur à $k$ par l'application $\varepsilon_{\underline{c}} = (\varepsilon_{c_1}, \dots, \varepsilon_{c_n})$. Lorsque les $c_i$ sont deux à deux non équivalents, Martinez-Peñas démontre que les codes ainsi obtenus possèdent d'excellents paramètres pour la métrique somme-rang ; précisément, ils atteignent la borne de Singleton.

Dans l'article [3] co-écrit avec mon ancien étudiant, Amaury Durand, nous nous intéressons aux duaux des codes de Reed–Solomon linéarisés dans le cas, déjà mentionné précédemment, où $K$ est un corps et $F$ est un sous-corps d'indice fini. En nous inspirant du cas classique, nous démontrons que ces duaux s'interprètent comme des codes « de Goppa » obtenus, non pas en évaluant des polynômes, mais en prenant des résidus de formes différentielles. Un préliminaire important que nous réalisons en partie [4] dans *loc. cit.* est la mise au point d'une théorie des résidus pour les polynômes de Ore. Une conséquence notable de nos résultats est que le dual d'un code de Reed–Solomon linéarisé est encore un code de Reed–Solomon linéarisé. Ceci répond affirmativement à une question de Kschischang et Martinez-Peñas.

### 2.2.2 Construction de nouveaux codes

*Références* :
[7] E. Berardini, X. Caruso, *Algebraic geometry codes in the sum-rank metric*
[12] E. Berardini, X. Caruso, *Reed-Muller codes in the sum-rank metric*

**Génèse.** Dans le cas classique, une généralisation bien connue des codes de Reed–Solomon est la famille des codes AG (pour *Algebraic Geometry*) où l'évaluation des polynômes est remplacée par l'évaluation de fonctions regulières sur une courbe algébrique. La condition sur le degré est alors remplacée par une condition de type Riemann–Roch, et est encodée par un diviseur sur la courbe.

Depuis plusieurs années déjà, me trottait dans la tête cette idée d'étendre la construction des codes AG dans le cadre des polynômes de Ore. Après un temps de maturation déraisonnablement long, j'ai finalement réalisé que, dans le cas des codes de Reed–Solomon linéarisés, la courbe sous-jacente était la droite projective sur le sous-corps $F$, et non sur le corps $K$ lui-même ! En effet, bien qu'il semblerait *a priori* que les points d'évaluation $c\theta$ soient indexés par $c \in K$, deux paramètres $c$ conduisent à des évaluations équivalentes dès lors qu'ils sont équivalents au sens de la relation $\sim$ introduite précédemment. Dans le cas où $K = \mathbb{F}_q$ et $\theta = \mathrm{Frob}$, les points d'évaluation sont donc en correspondance avec les éléments de $\mathbb{F}_p^\star$, et non pas ceux de $\mathbb{F}_q$. De surcroit, au niveau des anneaux, $\mathbb{P}^1_F$ est incarnée par le *centre* de $K[X;\theta]$, qui n'est autre que $F[X^r]$ avec $r = [K{:}F]$.

Après cetté révélation, j'ai compris que la clé consistait à présenter l'anneau des polynômes de Ore $K[X;\theta]$ en faisant intervenir explicitement la variable $X^r$ :

$$K[X;\theta] = K[X^r][T;\theta]/(T^r - X^r).$$

Dans le cas général, il s'agirait donc de considérer une courbe projective lisse $\mathcal{C}$ définie sur le sous-corps $F$ et de travailler avec l'anneau quotient $K(\mathcal{C})[T;\theta]/(T^r - x)$ où $K(\mathcal{C})$ est le corps des fonctions de $K \otimes_F \mathcal{C}$ et $x$ désigne un élément fixé de $F(\mathcal{C})$. J'en étais à ce point de ma réflexion lorsque j'ai discuté pour la première fois avec Elena Berardini qui s'intéressait à la même question. C'est ainsi que nous avons commencé à collaborer. Il restait évidemment encore beaucoup de travail à réaliser : définir des morphismes d'évaluation, définir les espaces de Riemann–Roch adéquats et démontrer un théorème de Riemann–Roch, estimer la taille des zéros d'un polynôme de Ore dans la veine de la formule (3), *etc.* J'ai invité une première fois Elena à Bordeaux et, au bout d'une semaine à peine, nous avions suffisamment dégrossi toutes ces questions pour être tout à fait confiants sur l'issue de projet.

**Les codes LAG.** Nous considérons le cadre suivant légèrement plus général que ce qui précède : nous nous donnons un revêtement de courbes projectives lisses $\varpi : \mathcal{C}' \to \mathcal{C}$ sur un corps de base $k$ et nous

4. Plus précisément, nous traitons le cas d'une dérivation, celui d'un endomorphisme ayant déjà été considéré dans un travail antérieur, que j'avais présenté dans mon rapport d'activité précédent.

supposons que $\varpi$ est génériquement galoisien de groupe de Galois cyclique d'ordre $r$, engendré par un automorphisme $\theta$. Soit $K = k(\mathcal{C}')$ et $F = k(\mathcal{C})$ ; *via* $\varpi$, le corps $K$ apparaît ainsi comme une extension cyclique de $F$ de degré $r$. Nous choisissons également un élément $x \in F$ et formons le quotient

$$\mathcal{D} = K[T;\theta]/(T^r - x)$$

qui est une algèbre centrale simple sur $F$. Les morphismes d'évaluation sont définis pour chaque place $\mathfrak{p}$ de la courbe $\mathcal{C}$ où la fonction $x$ n'a ni zéro, ni pôle. En effet, à ces places, l'algèbre $\mathcal{D}$ est triviale dans le sens où son complété en $\mathfrak{p}$ est isomorphe à une algèbre de matrices. Réduisant modulo $\mathfrak{p}$, nous obtenons un morphisme $\varepsilon_\mathfrak{p} : \mathcal{O}_{\mathcal{D},\mathfrak{p}} \to M_r(k(\mathfrak{p}))$ où $\mathcal{O}_{\mathcal{D},\mathfrak{p}}$ désigne l'anneau de valuation de $\mathcal{D}$ à la place $\mathfrak{p}$ et $k(\mathfrak{p})$ est le corps résiduel de $\mathcal{C}$ à cette même place.

Ensuite, à chaque diviseur $E = \sum_{\mathfrak{p}' \in \mathcal{C}'} n_{\mathfrak{p}'}\mathfrak{p}'$ sur $\mathcal{C}'$ (où les $n_{\mathfrak{p}'}$ peuvent éventuellement être des nombres rationnels avec des dénominateurs contrôlés en fonction de la ramification à la place $\mathfrak{p}'$), nous associons l'espace de Riemann–Roch

$$\Lambda(E) = \bigoplus_{i=0}^{r-1} \mathcal{L}_{\mathcal{C}'}\Big( \sum_{\mathfrak{p}'} \big\lfloor n_{\mathfrak{p}'} + \tfrac{i}{r} e_{\mathfrak{p}'} \cdot v_{\varpi(\mathfrak{p}')}(x) \big\rfloor \cdot \mathfrak{p}' \Big) \cdot T^i \subset \mathcal{D}$$

où $e_{\mathfrak{p}'}$ désigne l'indice de ramification à la place $\mathfrak{p}'$ et $\mathcal{L}_{\mathcal{C}'}$ fait référence à l'espace de Riemann–Roch classique sur $\mathcal{C}'$. Nous démontrons le théorème suivant, analogue dans notre contexte de l'inégalité de Riemann[5].

**Théorème 5.** *Pour tout diviseur $E$ comme ci-dessus, on a :*

$$\dim_k \Lambda(E) \geqslant r \cdot \deg(E) - r \cdot (g_{\mathcal{C}'} - 1) - \frac{r^2}{2} \sum_{\mathfrak{p} \in \mathcal{C}} \frac{b_\mathfrak{p} - 1}{b_\mathfrak{p} e_\mathfrak{p}} \deg(\mathfrak{p})$$

*où $g_{\mathcal{C}'}$ est le genre de la courbe $\mathcal{C}'$ et $b_\mathfrak{p} = \frac{r}{\operatorname{pgcd}(r, e_\mathfrak{p} v_\mathfrak{p}(x))}$.*

Enfin, pour obtenir un équivalent de l'estimation (3), nous utilisons un outil classique de la théorie des algèbres centrales simples : la norme réduite. Rappelons brièvement qu'il s'agit d'une fonction multiplicative qui associe à chaque élément de l'algèbre un élement de son centre. Dans notre situation, nous récupérons ainsi une application $N_{\mathrm{rd}} : \mathcal{D} \to k(\mathcal{C})$. Pour toute place $\mathfrak{p}$ de $\mathcal{C}$ pour laquelle $\varepsilon_\mathfrak{p}$ est défini, et pour toute fonction $f \in \mathcal{O}_{\mathcal{D},\mathfrak{p}}$, nous démontrons l'inégalité :

$$\dim_F \ker \varepsilon_\mathfrak{p}(f) \leqslant \operatorname{ord}_\mathfrak{p} N_{\mathrm{rd}}(f) \tag{4}$$

dans laquelle $\operatorname{ord}_\mathfrak{p}$ désigne l'ordre d'annulation en $\mathfrak{p}$. Ceci nous permet de ramener l'estimation de la taille des zéros d'un élément $f \in \mathcal{D}$ à celui de sa norme réduite $N_{\mathrm{rd}}(f)$, qui est simplement une fonction rationnelle sur une courbe algébrique et pour laquelle les techniques usuelles s'appliquent.

Tous ces ingrédients étant mis en place, nous suivons finalement la construction classique des codes AG pour définir les codes AG linéarisés (que nous appelons codes LAG) et estimons leurs paramètres. Comme dans le cas classique, ils atteignent la borne de Singleton à un défaut près qui est contrôlé, ici, par le genre de la courbe $\mathcal{C}'$ et la ramification du revêtement $\varpi$ ; précisément, il vaut

$$g_{\mathcal{C}'} + \frac{r}{2} \sum_{\mathfrak{p} \in \mathcal{C}} \frac{b_\mathfrak{p} - 1}{b_\mathfrak{p} e_\mathfrak{p}} \deg(\mathfrak{p}).$$

Pour conclure, nous remarquons que ce défaut est minimal lorsque le revêtement $\varpi : \mathcal{C}' \to \mathcal{C}$ est isotrivial, c'est-à-dire lorsque $\mathcal{C}' = \ell \otimes_k \mathcal{C}$ où $\ell/k$ est une extension cyclique d'ordre $r$.

**Les codes LRM.** Après ce premier travail, Elena a obtenu un poste de chaire de professeur junior CNRS et a rejoint notre équipe à Bordeaux. Nous avons donc naturellement poursuivi notre collaboration avec, d'une part, l'encadrement de la thèse de Fabrice Drain (voir aussi §5) et, d'autre part, la rédaction d'un nouvel article [12] sur les codes de Reed–Muller linéarisés.

5. Un théorème de Riemann–Roch avec un terme correctif supplémentaire conduisant à une égalité est, en réalité, certainement possible (et probablement nécessaire pour de futurs développements). Toutefois, l'inégalité de Riemann était suffisante pour ce qui nous occupe ici et nous devons avouer que nous avons été paresseux...

Dans le cas classique, les codes de Reed–Muller sont une autre généralisation très connue des codes de Reed–Solomon ; cette fois-ci, au lieu de remplacer les polynômes usuels par des fonctions sur une courbe algébrique, on les remplace par des polynômes multivariés. Il semble donc tout à fait naturel d'étudier une extension possible des codes de Reed–Muller à la métrique somme-rang et, après un voyage en Inde où elle a rencontré Sudhir Ghorpade (un collègue qui a beaucoup travaillé sur les codes de Reed–Muller), Elena m'a proposé de la suivre dans ce projet de recherche.

Cette fois-ci, la stratégie était claire : il s'agissait de développer la théorie des polynômes de Ore multivariés en suivant pas à pas les étapes que nous avions mises en évidence dans notre travail sur les codes LAG. Nous avons choisi de nous restreindre au cas où le corps de base $k$ est fini pour deux raisons : d'une part, c'est certainement la situation qui a le plus grand potentiel d'avoir des applications concrètes et, d'autre part, c'est un cas que plusieurs auteurs avaient précédemment jugé inadapté au cadre multivarié, étant donné que le groupe de Galois d'un corps fini est nécessairement cyclique (donc engendré par un seul élement). Malgré cela, nous ne nous sommes pas découragés et avons entrepris l'étude de l'algèbre de polynômes de Ore

$$\mathbb{F}_q[X_1, \dots, X_n; \theta_1, \dots, \theta_n]$$

avec $\theta_i = \mathrm{Frob}^{e_i}$. Dans l'anneau ci-dessus, les variables $X_i$ commutent entre elles et chacune d'elle commute avec les scalaires selon la loi de Ore $X_i a = \theta_i(a) X_i$. Nous déroulons toute la théorie dans ce cadre : nous définissons les morphismes d'évaluation, introduisons un analogue des espaces de Riemann–Roch (qui sont, cette fois-ci, paramétrés par des sous-ensembles convexes de $\mathbb{Z}^n$ correspondant aux exposants retenus), estimons leur dimension et, en nous appuyant sur la norme réduite, démontrons un analogue des estimations (3) et (4). Par certains aspects, les démonstrations sont plus techniques — en particulier car elles font intevenir des arguments de géométrie convexe (notamment le théorème d'Ehrhart) — mais le cheminement de la méthode est entièrement parallèle au cas des codes LAG.

*In fine*, nous définissons des codes LRM associés aux données suivantes : un uplet d'exposants $\underline{e} = (e_1, \dots, e_n) \in \mathbb{Z}^n$ et un sous-ensemble convexe compact $E$ de $\mathbb{R}^n$. Nous calculons les paramètres de nos codes et montrons qu'ils vérifient des estimations analogues à ce que l'on a classiquement pour les codes de Reed–Muller. De même que dans le cas des codes LAG, nous montrons que les paramètres optimaux sont atteints dans un cas extrêmement particulier, à savoir celui où $\underline{e} = (0, \dots, 0, 1)$ et $E$ est le simplexe engendré par les vecteurs $e_1, \dots, e_{n-1}, re_n$, où $r = [\mathbb{F}_q{:}\mathbb{F}_p]$ et $(e_1, \dots, e_n)$ est la base canonique de $\mathbb{R}^n$.

Nous concluons notre article en établissant un lien entre codes LRM et codes LAG. Précisément, sous certaines conditions, nous montrons que les premiers se plongent dans les seconds, avec une perte contrôlée sur la distance minimale. Cette propriété est intéressante car elle permet de ramener le décodage des codes LRM à celui des codes LAG, un sujet sur lequel nous sommes en train de travailler actuellement avec Elena et notre étudiant Fabrice.

## 2.3 Modules de Drinfeld

Un autre domaine de recherche dans lequel je me suis résolument engagé depuis un peu plus d'une année est l'arithmétique des corps de fonctions incarnée, pour ce qui me concerne, par la théorie des modules de Drinfeld. Étant donnée la proximité de ces derniers avec les polynômes de Ore, il était en fait étonnant que je ne m'y sois pas intéressé plus tôt. Il m'aura fallu un alignement des planètes assez exceptionnel pour finalement me forcer à franchir le pas.

Tout a commencé en 2022 lorsque j'ai assisté à un exposé d'Antoine Leudière présentant sommairement le sujet ainsi qu'une application possible à la cryptographie qu'il avait récemment développée avec l'un de ses directeurs de thèse, Pierre-Jean Spaenlehauer. En parallèle de cela, Olivier Fouquet m'avait proposé de participer au projet ANR PadLEfAn sur les fonctions $L$ et, en particulier, leur calcul effectif. Ce projet comportait également un aspect « corps de fonctions », en lien avec les séries $L$ des modules de Drinfeld. J'étais à l'époque étranger à ce domaine de recherche mais, pour des raisons administratives, je me suis retrouvé rattaché au nœud de Caen, aux côtés de collègues spécialistes des corps de fonctions. Tous ces signaux m'ont finalement convaincu que je devais aussi moi-même m'intéresser au sujet.

### 2.3.1 Polynôme caractéristique du Frobenius

*Références* :
[6] D. Ayotte, X. Caruso, A. Leudière, J. Musleh, *Drinfeld modules in SageMath*
[11] X. Caruso, A. Leudière, *Algorithms for computing norms and characteristic polynomials on general Drinfeld modules*
[14] D. Ayotte, X. Caruso, A. Leudière, J. Musleh, *Modules de Drinfeld*, librairie SAGEMATH

Ma première aventure en recherche dans ce domaine a été menée aux côtés d'Antoine. À la suite de son travail avec Pierre-Jean, il s'intéressait au calcul efficace du polynôme caractéristique du Frobenius d'un module de Drinfeld sur un corps fini. Après qu'il ait évoqué cette question lors de son exposé de 2022, j'ai tout de suite entrevu une nouvelle piste qui me semblait naturelle au vu de mon expérience passée avec les polynômes de Ore. En revanche, pour Antoine, cette approche était entièrement nouvelle et c'est ainsi que nous avons commencé à collaborer. Rapidement, je l'ai invité à Bordeaux et, après une rencontre fructueuse d'une semaine à peine, nous avions posé les bases de ce qui allait devenir deux nouveaux algorithmes compétitifs pour le calcul du polynôme caractéristique du Frobenius.

Ces algorithmes sont décrits dans la prépublication [11]. Avant de les présenter sommairement dans ce rapport d'activité, j'ai besoin de rappeler quelques définitions. On se donne un corps fini $\mathbb{F}_q$ ainsi qu'une extension $\mathbb{F}_{q^n}$ de celui-ci. Dans ce contexte, un module de Drinfeld est, par définition, un morphisme d'anneaux $\phi : A \to \mathbb{F}_{q^n}[\tau;\theta]$ où $A = \mathbb{F}_q[t]$ et $\theta$ est le Frobenius $x \mapsto x^q$. Étant donné que $\phi$ est un morphisme d'anneaux, il est entièrement déterminé par son image sur le générateur $t$, qui est généralement notée $\phi_t$. Plus généralement, pour un élement $a \in A$, on écrit $\phi_a$ pour $\phi(a)$. À un module de Drinfeld $\phi$, on peut associer des points de torsion et des modules de Tate : pour $a \in A$, on définit la $a$-torsion de $\phi$, notée $\phi[a]$, comme le noyau de $\phi_a(\theta)$ agissant sur $\bar{\mathbb{F}}_q$ (où $\theta$ est prolongé à $\bar{\mathbb{F}}_q$ en conservant la même formule $x \mapsto x^q$) et, pour un polynôme irréductible $\mathfrak{p} \in A$, on pose

$$T_{\mathfrak{p}}(\phi) = \varprojlim_{n\in\mathbb{N}} \phi[\mathfrak{p}^n].$$

Lorsque $\mathfrak{p}$ n'est pas dans le noyau du morphisme structurel $\phi$ mod $\tau : A \to \mathbb{F}_{q^n}$, on démontre que $T_{\mathfrak{p}}(\phi)$ est un module libre sur le complété $A_{\mathfrak{p}}$ dont le rang est égal au degré du polynôme $\phi_t$.

Un morphisme entre deux modules de Drinfeld $\phi$ et $\psi$ est, par définition, un polynôme de Ore $u \in \mathbb{F}_{q^n}[\tau;\theta]$ tel que $u\phi_t = \psi_t u$. Tout morphisme induit une application $A_{\mathfrak{p}}$-linéaire $T_{\mathfrak{p}}(u) : T_{\mathfrak{p}}(\phi) \to T_{\mathfrak{p}}(\psi)$ au niveau des modules de Tate, et on définit le polynôme caractéristique de $u$ comme celui de $T_{\mathfrak{p}}(u)$ ; on vérifie qu'il ne dépend pas de $\mathfrak{p}$ et est à coefficients dans $A$. Un endomorphisme particulièrement intéressant d'un module de Drinfeld $\phi$ est son endomorphisme de Frobenius, qui est défini par $u = \tau^n$. En effet, on peut démontrer, par exemple, que son polynôme caractéristique détermine de manière unique la classe d'isogénie[6] de $\phi$. Être capable de calculer ce polynôme caractéristique revêt donc un enjeu important.

Le résultat dont j'avais eu l'intuition à la fin de l'exposé d'Antoine de 2022 est le théorème 6 ci-après. Avant de l'énoncer, je rappelle que l'on dispose d'une application de norme réduite $N_{\mathrm{rd}}$ qui, dans le cas présent, applique l'anneau des polynôme de Ore $\mathbb{F}_{q^n}[\tau;\theta]$ dans son centre $\mathbb{F}_q[\tau^n]$. Plus généralement, il existe aussi une fonction « polynôme caractéristique réduit » : si $x$ est une variable auxiliaire (qui commute avec les scalaires et avec $\tau$), elle est définie par $\chi_{\mathrm{rd}}(f) = N_{\mathrm{rd}}(x - f) \in \mathbb{F}_q[\tau^n, x]$ pour tout $f \in \mathbb{F}_{q^n}[\tau;\theta]$.

**Théorème 6.** *Soit $\phi : A \to \mathbb{F}_{q^n}[\tau;\theta]$ un module de Drinfeld. Soit $\pi(t,x) \in A[x]$ le polynôme caractéristique du Frobenius de $\phi$ et soit $\chi(\tau^n, x) \in \mathbb{F}_q[\tau^n, x]$ le polynôme caractéristique réduit du polynôme de Ore $\phi_t$. Alors*

$$\pi(t,x) = \chi(x,t).$$

Nous étions contents de démontrer ce théorème mais, après la mise en ligne de notre article sur arXiv, Mihran Papikian nous a signalé que cet énoncé était « bien connu » ; en tout cas, il pouvait être facilement déduit de la combinaison de trois propositions dispersées dans le livre de 500 pages qu'il venait de publier. Je rends donc à Mihran ce qui lui appartient, mais demeure néanmoins satisfait d'avoir réussi à reconstruire ce joli résultat. Quoi qu'il en soit, le théorème 6 donne une première méthode pour calculer efficacement le polynôme caractéristique de l'endomorphisme de Frobenius d'un module de Drinfeld puisque l'on dispose, par ailleurs, d'algorithmes efficaces pour le calcul d'une norme réduite.

6. Une isogénie est, par définition, un morphisme non nul.

Mieux encore, le chemin vers la démonstration du théorème 6 nous a permis, à Antoine et à moi-même, de découvrir et d'approfondir la théorie des motifs d'Anderson, un autre point saillant de l'arithmétique des corps de fonctions. Si $\phi : A \to \mathbb{F}_{q^n}[\tau;\theta]$ est un module de Drinfeld, son motif d'Anderson $\mathbf{M}(\phi)$ n'est autre que $\mathbb{F}_{q^n}[\tau;\theta]$ muni des structures supplémentaires suivantes :
(a) une action de $A$ donnée par $\phi$ : le résultat de l'action d'un polynôme $a \in A$ sur $f \in \mathbb{F}_{q^n}[\tau;\theta]$ est $f\phi_a$,
(b) une action de $\mathbb{F}_{q^n}$ donnée par multiplication à gauche,
(c) un endomorphisme $\tau_{\mathbf{M}(\phi)} : \mathbf{M}(\phi) \to \mathbf{M}(\phi)$ donné par la multiplication à gauche par $\tau$.

On retiendra en particulier que $\mathbf{M}(\phi)$ hérite d'une structure de module sur $A \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n} \simeq \mathbb{F}_{q^n}[t]$. Si $\phi_t$ est un polynôme de Ore de degré $r$, il se trouve que $\mathbf{M}(\phi)$ est libre de rang $r$ sur $\mathbb{F}_{q^n}[t]$, une base étant donnée par la famille $(1, \tau, \ldots, \tau^{r-1})$. En contrepartie, on prendra garde au fait que $\tau_{\mathbf{M}(\phi)}$ est bien $A$-linéaire, mais qu'il est *semi-linéaire* par rapport à $\mathbb{F}_{q^n}$ : il vérifie $\tau_{\mathbf{M}(\phi)}(\lambda x) = \lambda^q \, \tau_{\mathbf{M}(\phi)}(x)$ pour $\lambda \in \mathbb{F}_{q^n}$ et $x \in \mathbf{M}(\phi)$.

Un morphisme $u : \phi \to \psi$ entre modules de Drinfeld induit un morphisme dans le sens opposé $\mathbf{M}(u) : \mathbf{M}(\psi) \to \mathbf{M}(\phi)$ au niveau des motifs d'Anderson ; ce dernier est donné par la multiplication par $u$ à droite, il est $\mathbb{F}_{q^n}[t]$-linéaire et commute à l'action de $\tau$. Comme $\mathbf{M}(\phi)$ et $\mathbf{M}(\psi)$ sont libres et équipés de bases canoniques, on peut, sans ambiguité, considérer la matrice de $\mathbf{M}(u)$. Dans le cas d'un endomorphisme, on démontre que le polynôme caractéristique de cette dernière est égal au polynôme caractéristique de $u$ tel que nous l'avons défini précédemment (en regardant l'action sur le module de Tate). Cette interprétation donne lieu à un deuxième algorithme pour le calcul du polynôme caractéristique du Frobenius d'un module de Drinfeld.

Dans [11], Antoine et moi-même étudions en détails les deux algorithmes dont je viens de présenter les rouages. En particulier, nous calculons leur complexité et constatons que chacun d'eux surpasse l'autre dans des régimes différents : lorsque $n$ est grand par rapport à $r$, le premier algorithme, qui se base sur le théorème 6 est beaucoup plus performant, alors que le contraire se produit lorsque $n \ll r$. Nous étendons aussi nos résultats à des modules de Drinfeld plus généraux où l'anneau $A = \mathbb{F}_q[t]$ est remplacé par l'anneau des fonctions regulières en dehors d'un point sur une courbe projective lisse, géométriquement connexe, définie sur $\mathbb{F}_q$.

Enfin, avec l'aide supplémentaire de David Ayotte et Joseph Musleh, nous avons implémenté nos algorithmes, et plus généralement toute une bibliothèque pour la manipulation des modules de Drinfeld (sur $\mathbb{F}_q[t]$), dans le logiciel SAGEMATH [14]. Outre ce dont je viens de discuter, cette bibliothèque inclut des fonctionnalités dans le cadre des modules de Drinfeld dits de caractéristique nulle, c'est-à-dire pour lesquels le corps $\mathbb{F}_{q^n}$ est remplacé par $\mathrm{Frac}(A)$ ou l'une de ses extensions ; dans ce cadre, nous avons implémenté des méthodes pour le calcul du logarithme et de l'exponentielle, des $j$-invariants, des formes modulaires de Drinfeld, *etc.* L'article [6] présente en quelques pages les réalisations les plus importantes de notre implémentation. Ce travail a été extrêmement bien accueilli par la communauté : nous avons reçu des messages de félications et d'encouragement de plusieurs grands noms du domaine, y compris Ernst-Ulrich Gekeler.

### 2.3.2 Motifs d'Anderson et séries $L$

*Références* :
[8] X. Caruso, Q. Gazda, *Computation of classical and $v$-adic $L$-series of $t$-motives*
[15] X. Caruso, *Motifs d'Anderson*, librairie SAGEMATH

Outre Ernst-Ulrich, j'ai également été contacté par Quentin Gazda qui était, lui aussi, très content de voir une implémentation des modules de Drinfeld, et souhaitait l'utiliser pour tester des conjectures. En réalité, Quentin était principalement intéressé par le calcul des séries $L$, quelque chose que nous n'avions pas implémenté et qui, pour être tout à fait honnête, m'était inconnu à l'époque.

C'est alors que Quentin, sans se décourager le moins du monde, a endossé son costume de professeur et m'a patiemment expliqué de quoi il retournait. On part d'un module de Drinfeld en caractéristique nulle $\phi : A \to A[\tau;\theta]$ où $A = \mathbb{F}_q[t]$ et $\theta$ est toujours l'application $x \mapsto x^q$. À un tel $\phi$, il est impossible d'associer un endomorphisme de Frobenius étant donné que $\theta$ n'est pas d'ordre fini sur $A$. En revanche, pour tout polynôme irréductible $\mathfrak{p} \in A$, on peut réduire $\phi$ modulo $\mathfrak{p}$ et obtenir ainsi un autre module de Drinfeld $\phi_\mathfrak{p} : A \to (A/\mathfrak{p})[\tau;\theta]$. L'intérêt de cette manipulation est qu'à présent, $A/\mathfrak{p}$ est une extension finie de $\mathbb{F}_q$, et on peut considérer le polynôme caractéristique $\chi_\mathfrak{p}(x)$ du Frobenius de $\phi_\mathfrak{p}$. La série $L$ de $\phi$ est obtenue en

mettant ensemble tous ces polynômes caractéristiques comme suit :

$$L(\phi;x) = \prod_{\mathfrak{p}} \frac{\chi_{\mathfrak{p}}(0)}{\chi_{\mathfrak{p}}(x^{\deg \mathfrak{p}})}. \tag{5}$$

Du fait qu'il n'y a qu'un nombre de polynômes de degré majoré par une constante donnée, on déduit que la série $L(\phi;x)$ converge dans $\mathrm{Frac}(A)[[x]]$. En réalité, de même que dans le cas plus classique des corps de nombres, ce ne sont pas réellement les coefficients de $L(\phi;x)$ qui sont les plus intéressants, mais plutôt les valeurs prises par la fonction $L(\phi;-)$ (ou ses dérivées) en certains points particuliers. C'est pour cette raison que l'on considère souvent $L(\phi;x)$ comme une série à coefficients dans $K_\infty = \mathbb{F}_q((\frac{1}{t}))$, le complété de $\mathrm{Frac}(A)$ en la place à l'infini. Pareillement, il existe une variante $\mathfrak{p}$-adique des constructions précédentes : on définit

$$L(\phi;x) = \prod_{\mathfrak{q}\neq\mathfrak{p}} \frac{\chi_{\mathfrak{q}}(0)}{\chi_{\mathfrak{q}}(x^{\deg \mathfrak{q}})} \tag{6}$$

que l'on considère comme une série à coefficients dans $K_{\mathfrak{p}}$, le complété de $\mathrm{Frac}(A)$ en la place $\mathfrak{p}$. L'intérêt d'omettre $\mathfrak{p}$ dans le produit définissant $L_{\mathfrak{p}}(\phi;x)$ est technique : il autorise une écriture plus harmonieuse de la formule des traces d'Anderson dont je reparlerai rapidement ci-après et permet *in fine* d'obtenir de meilleures propriétés de convergence.

La question de Quentin était donc de calculer explicitement les séries $L(\phi;x)$ et $L_{\mathfrak{p}}(\phi;x)$. J'ai rapidement compris qu'il allait être très coûteux de calculer indépendamment chacun des facteurs locaux $\chi_{\mathfrak{p}}$ puis de les injecter dans la formule (5). En effet, il y a environ $q^n/n$ polynômes irréductibles de degré $n$ sur $\mathbb{F}_q$, ce qui signifie que l'on devra calculer autant de polynômes caractéristiques de Frobenius pour déterminer la série $L$ à précision $O(x^n)$. L'algorithme qui en résulterait serait donc *exponentiel* en la précision. Heureusement, Quentin avait une autre méthode à proposer, basée sur une formule très célèbre dans le domaine : la formule des traces d'Anderson. Celle-ci permet de réécrire les produits infinis (5) et (6) comme le « polynôme caractéristique » d'un unique opérateur $\tau^\star$ défini, en quelques mots, comme le dual de $\tau_{\mathbf{M}(\phi)^\vee}$ agissant sur le dual du motif d'Anderson de $\mathbf{M}(\phi)$. Donner les définitions précises m'amènerait trop loin pour ce rapport d'activité mais je voudrais néanmoins signaler une difficulté importante : l'espace sur lequel agit $\tau^\star$ n'est pas de dimension finie et définir le polynôme caractéristique de $\tau^\star$ n'est donc pas immédiat. La solution consiste, d'une part, à raisonner par approximations successives et, d'autre part, une fois qu'on s'est ramené à une précision fixée, à travailler avec la notion de *nucleus*, un sous-espace de dimension finie possédant les bonnes propriétés pour permettre le calcul du polynôme caractéristique approché.

Dans [8], nous rendons entièrement explicite toute cette démarche en construisant notamment des bases sympathiques des nucleus sus-mentionnés, et en exprimant les matrices de $\tau^\star$ dans ces bases. Ceci nous permet d'obtenir en fin de compte un algorithme de complexité *quasi-linéaire* en la précision pour le calcul des séries $L(\phi;x)$ et $L_{\mathfrak{p}}(\phi;x)$. Bien entendu, en comparaison de la complexité exponentielle de la méthode naïve, il s'agit d'une amélioration considérable. En outre, notre algorithme ne fonctionne pas uniquement dans le cadre des modules de Drinfeld, mais dans celui beaucoup plus général des motifs d'Anderson. Parce qu'elle autorise twists et produits tensoriels, cette généralité est particulièrement intéressante, et conduit à une variété de séries $L$ bien plus grande dans laquelle il est plus naturel — et souvent plus pertinent — de formuler des théorèmes et des conjectures.

Tous nos algorithmes ont été implémentés par mes soins dans le logiciel SageMath [15]. Bien que, tout à fait fonctionnelle, cette implémentation n'est pas encore à un stade de maturatité optimal et, en particulier, elle n'est pas encore prête pour être intégrée à la distribution standard de SageMath. J'espère avoir le temps, dans les prochains mois, de la compléter pour la rendre accessible et facile d'utilisation à toute la communauté.

Pour conclure, j'aimerais signaler que, de manière inattendue, notre démarche et notre algorithme nous ont permis d'obtenir de nouveaux résultats théoriques sur les séries $L$. Typiquement, nous démontrons que $L(\phi;x)$ et $L_{\mathfrak{p}}(\phi;x)$ ont un rayon de convergence infini et donnons des estimations très fines sur la vitesse de convergence de ces séries (qui s'avère être extrêmement rapide). Nous formulons également une conjecture :

**Conjecture 7.** *L'ordre d'annulation en $x{=}1$ de la série $L$ $\mathfrak{p}$-adique d'un motif d'Anderson fixé ne dépend pas du polynôme $\mathfrak{p}$.*

Avec Quentin, nous avons déjà des pistes sérieuses pour démontrer cette conjecture. J'espère qu'elles seront fructueuses et pouvoir les présenter dans mon prochain rapport d'activité.

# 3 Enseignement, formation et diffusion de la culture scientifique

## Enseignement et formation

**Cours dispensés.** Depuis mon arrivée à Bordeaux, en 2018, je donne un cours d'informatique quantique, commun aux masters AGTN (*Algèbre, Géométrie et Théorie des Nombres*) et CSI (*Cryptologie et Sécurité Informatique*). L'objectif du cours est de présenter le paradigme de l'ordinateur quantique ainsi que l'algorithme de factorisation des entiers en temps polynomial, dû à Shor.

**Encadrement de stages.** En 2024, j'ai encadré le stage de M2 de Chiara Mandatelli, intitulé « *Classification of rank 1 Drinfeld modules over an arbitrary function field* ».

## Organisation de séminaires et d'événements

En 2022 et 2023, j'ai co-organisé avec mes collègues du LaBRI (Laboratoire Bordeaux de Recherche en Informatique) des SageDays d'une semaine à la réserve ornithologique du Teich. Ces deux rencontres ont été un franc succès et nous aimerions pouvoir les reconduire chaque année.

## Activités de diffusion

Avec ma collègue Chantal Menini, nous avons été, entre 2018 et 2023, chargés de mission diffusion par le laboratoire. Je me suis investi, à ce titre, dans plusieurs chantiers. Le premier a été la réorganisation interne de la diffusion à l'IMB. En particulier, nous avons créé une équipe au sein de l'IMB et obtenu un budget propre récurrent du laboratoire.

À côté de cela, j'ai mis en place un partenariat durable avec le FabLab de l'IUT de l'université de Bordeaux. Dans ce cadre, je conçois et réalise régulièrement des objets ou des petits applications illustrant des points de mathématiques.

Actuellement, avec un collègue du FabLab, Pierre Grangé-Praderas, nous travaillons sur une exposition artistique autour des mathématiques, intitulée « Théorèmes ». Cette exposition regroupe 14 tableaux que nous allons faire tirer très prochainement. En attendant, une version numérique est disponible à https://xavier.caruso.ovh/diffusion/theoremes/ (faites glisser pour voir tous les tableaux). En complément de cela, nous préparons des textes ainsi que des vidéos et/ou des podcasts explicatifs. Notre objectif est de pouvoir être exposés, et de rencontrer le public lors de performances [7], aussi bien dans des écoles, des lieux de culture scientifique que dans des lieux de culture artistique.

Enfin, j'interviens régulièrement dans des collèges et des lycées, j'encadre des ateliers MATh.en.JEANS, je participe au dispositif « Regards de géomètre », à la fête de la science et j'anime des stands dans des manifestations grand public (*e.g.* « Les échappées inattendues »).

# 4 Transfert technologique, relations industrielles et valorisation

# 5 Encadrement, animation et management de la recherche

## Étudiants en thèse

**Raphaël Pagès.** Entre 2020 et 2024, j'ai encadré avec Alin Bostan la thèse de Raphaël Pagès. Les prinicipales réalisations de la thèse sont la conception d'un algorithme efficace de calcul des $p$-courbures

7. Ce sont des sortes d'exposés sur une œuvre artistique.

d'un opérateur différentiel à coefficients dans $\mathbb{Q}(t)$ et l'étude théorique et algorthmique de la factorisation des opérateurs différentiels en caractéristique positive.

Raphaël a soutenu sa thèse en février 2024. À partir de la rentrée prochaine (septembre 2024), il sera postdoctorant à Linz.

**Fabrice Drain.** Depuis septembre 2023, j'encadre avec Elena Berardini la thèse de Fabrice Drain. Fabrice a un profil particulier car il a travaillé dans le privé pendant plus de 10 ans avant de décider de se réorienter vers la recherche en mathématiques. L'objet d'étude de la thèse de Fabrice est le codage en métrique somme-rang. Pour le moment, il s'intéresse au décodage des codes LAG que nous avons introduits récemment avec Elena.

## Projets de recherche

**CLap–CLap.** Entre 2018 et 2023, j'ai été le principal porteur du projet ANR CLap–CLap. L'ambition initiale du projet était de rapprocher deux communautés, celle des théoriciens des nombres et celle des algorithmiciens, autour de la thématique de la correspondance de Langlands $p$-adique. Malheureusement, cet objectif n'a pas été atteint en partie en raison de la pandémie ; dans ces circonstances, je n'ai pas eu le courage d'organiser les rencontres qui auraient été nécessaires à faire émerger des collaborations et la mayonnaise n'a finalement pas vraiment pris. Ceci étant dit, les membres du projet ont toutes et tous été très actifs et ont produit une excellente recherche tout au long des quatre années et demie.

**Barracuda.** Depuis 2021, je suis sympathisant du projet ANR Barracuda [8], dont l'objectif est l'étude des codes correcteurs d'erreurs *via* des méthodes algébriques.

À noter que le terme de « sympathisant » n'est pas officiel : administrativement, je ne suis pas membre du projet, point final. Le fait est, en réalité, qu'il y avait trop de membres dans le projet et qu'au moment de la soumission, il a été nécessaire de faire des choix. Je me suis alors porté volontaire pour être retiré de la liste officielle des membres. Cependant, j'assiste régulièrement aux rencontres (appelées « retraites ») organisées par le projet et participe activement aux activités de recherche menées dans ce cadre : les résultats que j'ai présentés dans le §2.2 rentrent tous parfaitement dans les thématiques de Barracuda.

**PadLEfAn.** Comme je l'ai expliqué en introduction du §2.3, je suis membre, depuis 2023, du projet ANR PadLEFan qui s'intéresse à l'arithmétique des fonctions $L$ ainsi qu'à leur calcul effectif, avec deux déclinaisons : une première sur les corps des nombres, une deuxième sur les corps de fonctions. Bien que j'avais été initialement contacté par travailler sur les aspects « corps de nombres », il ne fait plus aucun doute aujourd'hui que je me suis résolument engagé sur les aspects « corps de fonctions ».

**Un projet avec l'Autriche.** Depuis 2023, je suis le porteur français d'un projet PHC Amadeus de collaboration avec l'Autriche, qui regroupe cinq membres. L'objectif scientifique est de travailler sur l'uniformité vis-à-vis des groupes des réductions modulo $p$ des diagonales de fractions rationnelles (voir §2.1.3 pour plus de détails). Le projet finance les déplacements de ses membres français en Autriche, et réciproquement de ses membres autrichiens de France.

## Mon rôle de directeur adjoint

Depuis avril 2022, je suis directeur adjoint de l'IMB, en charge de la cellule informatique. Je suis responsable, à ce titre, d'une équipe de sept personnes (bientôt huit), je réalise les entretiens professionnels de trois d'entre elles et je les soutiens dans leurs demandes de promotion.

Au niveau du laboratoire, je fais le lien entre la direction et la cellule informatique ; en particulier, je prends en charge les dossiers afférents. Pour donner une idée, depuis 2022, les plus gros chantiers sur lesquels j'ai été amené à intervenir ont été : refonte de la fiche de poste d'un des agents pour le rendre plus conforme à ses aspirations et suivi de son travail, déménagement de nos serveurs dans une salle commune de l'université, conception et déploiement d'un nouveau logiciel pour la saisie des séminaires, rédaction

8. https://barracuda.inria.fr/fr/

d'une charte de sobriété informatique pour les membres de l'IMB, réorganisation des listes de diffusion, refonte complète de notre page web (en cours)...

Ces responsabilités impliquent des réunions hebdomadaires (en moyenne 4h par semaine), la participation au conseil de laboratoire et au conseil scientifique, ainsi qu'une forte disponibilité en cas de besoin.

## Autres responsabilités

J'ai été membre suppléant de la section 25 du CNU entre 2020 et 2023. En moyenne, je participais environ à deux sessions sur trois.

De 2018 à 2022, j'ai été également membre de conseil de département SIN (une structure qui chapeaute quatre laboratoires de recherche). Le conseil se réunit tous les trois mois environ. Après chaque conseil, je rédigeais un compte-rendu informel pour les collègues de l'IMB.

Je participe régulièrement à des comités de sélection, en moyenne deux par an.

En 2022, j'ai été jury pour le prix de thèse du laboratoire Blaise Pascal.

En 2022, j'ai présidé le comité HCERES qui a évalué l'I2M. En plus de la visite du site, le président a la charge d'organiser les réunions préparatoires du comité et de rédiger le partie générale du rapport.

En 2023, j'ai été membre du comité HCERES qui a évalué le LAGA.

## MA BIBLIOGRAPHIE DES CINQ DERNIERS SEMESTRES

*Articles de recherche publiés pendant les 5 derniers semestres*

[1] X. Caruso, *Where are the zeroes of a random p-adic polynomial ?*, Forum of Mathematics, Sigma **10** (2022), 1–41

[2] X. Caruso, T. Vaccon, T. Verron, *On Polynomial Ideals And Overconvergence In Tate Algebras*, proceddings de la conférence ISSAC 2022

[3] X. Caruso, A. Durand, *Duals of linearized Reed-Solomon codes*, Designs, Codes and Cryptography **91** (2023), 241–271

[4] X. Caruso, A. David, A. Mézard, *Combinatorics of Serre weights in the potentially Barsotti–Tate setting*, Moscow Journal of Combinatorics and Number Theory **12** (2023), 1–56

[5] X. Caruso, A. David, A. Mézard, *Can we dream of a 1-adic Langlands correspondence ?*, Mathematics Going Forward. Lecture Notes in Math. **2313** (2023), 537–560

[6] D. Ayotte, X. Caruso, A. Leudière, J. Musleh, *Drinfeld modules in SageMath*, ACM Communications in Computer Algebra **57** (2023), 65–71

[7] E. Berardini, X. Caruso, *Algebraic geometry codes in the sum-rank metric*, IEEE Transactions on Information Theory **70** (2024), 3345–3356

[8] X. Caruso, Q. Gazda, *Computation of classical and $v$-adic $L$-series of $t$-motives*, proceedings de la conférence ANTS XVI (2024), 21 pages

[9] A. Bostan, X. Caruso, J. Roques, *Algebraic solutions of linear differential equations : an arithmetic approach*, à paraître au Bulletin of American Mathematical Society, 52 pages

*Prépublications écrites pendant les 5 derniers semestres*

[10] B. Adamczewski, A. Bostan, X. Caruso, *A sharper multivariate Christol's theorem with applications to diagonals and Hadamard products*, prépublication (2023), 32 pages

[11] X. Caruso, A. Leudière, *Algorithms for computing norms and characteristic polynomials on general Drinfeld modules*, prépublication (2023), 43 pages

[12] E. Berardini, X. Caruso, *Reed-Muller codes in the sum-rank metric*, prépublication (2024), 28 pages

*Logiciels écrits pendant les 5 derniers semestres*

[13] X. Caruso, A. David, A. Mézard, *Déformations potentiellement Barsotti-Tate*, librairie SAGEMATH (2022), https://plmlab.math.cnrs.fr/caruso/pbtdef, $\sim$ 3000 lignes

[14] D. Ayotte, X. Caruso, A. Leudière, J. Musleh, *Modules de Drinfeld*, librairie SAGEMATH (2023), https://github.com/sagemath/sage/pull/35026, https://github.com/sagemath/sage/pull/35057, https://github.com/sagemath/sage/pull/35260, https://github.com/sagemath/sage/pull/35269 et https://github.com/sagemath/sage/pull/35527, $\sim$ 5000 lignes

[15] X. Caruso, *Motifs d'Anderson*, librairie SAGEMATH (2024), https://trac.sagemath.org/ticket/23043 et https://plmlab.math.cnrs.fr/caruso/anderson-motives, $\sim$ 1000 lignes