Codes algébriques et géométriques, applications à la cryptographie et à l'information quantique

Alain Couvreur

Université de Paris

École doctorale de sciences mathématiques (ED 386)

Institut de Mathématiques de Jussieu – Paris rive gauche (UMR 7586)

Codes algébriques et géométriques, applications à la cryptographie et à l'information quantique

Par Alain Couvreur

Habilitation à diriger les recherches,
spécialité Mathématiques

Présentée et soutenue publiquement le 16 décembre 2019

Devant un jury composé de :

Peter Beelen	PR, Danmarks Tekniske Universitet	Rapporteur
Irene Bouw	PR, Universität Ulm	Examinatrice
Ronald Cramer	PR, CWI Amsterdam	Examinateur
Arnaud Durand	PR, Université Paris Diderot	Examinateur
Jean-François Mestre	PR, Université Paris Diderot	Rapporteur interne
Nicolas Sendrier	DR, Inria	Rapporteur
Jean–Pierre Tillich	DR, Inria	Examinateur
Damien Vergnaud	PR, Sorbonne Universités & IUF	Examinateur

Table des matières

I Codes géométriques **11**

1 Codes géométriques **13**
1.1 Historique . . . 13
1.1.1 Codes sur les courbes algébriques . . . 13
1.1.2 Codes sur les surfaces algébriques . . . 14
1.2 Construction et paramètres de codes à partir de variétés de dimension $\geqslant 2$ . . . 15
1.2.1 Dimension . . . 16
1.2.2 Distance minimale . . . 16
1.3 Une borne sur le nombre de points rationnels d'une variété projective . . . 18
1.3.1 L'approche de Serre pour les hypersurfaces . . . 18
1.3.2 Esquisse de preuve de la conjecture de Ghorpade et Lachaud . . . 19
1.3.3 Questions ouvertes sur l'optimalité de la borne . . . 20
1.4 Quelques exemples de bons codes à partir de surfaces rationnelles . . . 20
1.4.1 Un exemple illustratif . . . 20
1.4.2 Nouveaux codes à partir d'éclatés de $\mathbf{P}^2$ en des points irrationnels . . . 22
1.5 Quadriques et tordues de variétés de Segré . . . 24
1.5.1 Quadriques elliptiques : la géométrie ne peut pas tout . . . 24
1.5.2 Les codes BCH à la rescousse . . . 25
1.6 Codes anticanoniques à partir de surfaces de del Pezzo . . . 26
1.6.1 Surfaces de del Pezzo . . . 27
1.6.2 Exemples de codes . . . 27

II Produits d'espaces et de codes, de la combinatoire additive à la cryptanalyse **29**

2 Cryptographie à base de codes **31**
2.1 Histoire . . . 31
2.1.1 Présentation du schéma de chiffrement de McEliece . . . 31
2.1.2 Pourquoi faire de la cryptographie avec des codes ? . . . 33
2.1.3 L'appel du NIST . . . 33
2.1.4 Comment analyse-t-on la sécurité d'un schéma à la McEliece ? . . . 33
2.1.5 D'autres schémas de chiffrement à base de codes . . . 35
2.2 Codes algébriques pour la cryptographie . . . 35
2.2.1 Codes de Reed–Solomon généralisés . . . 35
2.2.2 Codes alternants, codes de Goppa classiques . . . 35
2.3 Exemples d'instanciations du schéma de McEliece . . . 37

2.3.1 Les différentes instanciations de McEliece dans la littérature . . . 37
2.3.2 Quelques exemples pour démarrer . . . 38
2.3.3 Le schéma original de McEliece . . . 38
2.3.4 Codes munis d'un groupe d'automorphisme non trivial . . . 39
2.4 Codes géométriques pour la cryptographie . . . 40
2.4.1 Codes à partir de courbes . . . 40
2.4.2 Sous-codes sur un sous-corps et opérateur de Cartier . . . 40

3 Produits de codes et application à la cryptanalyse 45
3.1 Le produit $\star$ de codes . . . 45
3.2 Distinguer les codes algébriques et géométriques de codes aléatoires . . . 46
3.2.1 Motivation, preuves de sécurité . . . 46
3.2.2 Rappel, codes raccourcis . . . 46
3.2.3 Le distingueur $\mathcal{C} \mapsto \mathcal{C}^2$ . . . 47
3.2.4 Codes de Reed–Solomon généralisés . . . 47
3.2.5 Codes alternants, codes de Goppa . . . 48
3.2.6 Codes géométriques . . . 48
3.3 Cryptanalyses basées sur le distingueur par carré . . . 49
3.3.1 Attaques de quelques schémas basés sur des codes GRS . . . 49
3.3.2 Attaques par filtration . . . 51
3.4 Une cryptanalyse sans distingueur par code carré, le schéma DAGS . . . 55
3.4.1 Structure de la clé publique dans DAGS . . . 55
3.4.2 Idées de l'attaque . . . 56
3.5 Des propositions résistantes . . . 57
3.5.1 BIG QUAKE . . . 57
3.5.2 Les travaux d'Élise Barelli . . . 58

4 Combinatoire additive et produits d'espaces vectoriels dans des corps de fonctions 59
4.1 Les théorèmes de Freiman en combinatoire additive . . . 59
4.2 Un analogue dans le contexte des corps de fonctions . . . 60
4.2.1 Résultats antérieurs . . . 60
4.2.2 Première contribution, une forme faible du théorème de Freiman . . . 61
4.3 Le cas des espaces de genre combinatoire 0 et 1 . . . 61

III Méthodes géométriques et combinatoires pour la construction de codes quantiques 65

5 Codes quantiques à partir de graphes 67
5.1 Quelques notions de calcul quantique . . . 67
5.1.1 Qubits et intrication . . . 68
5.1.2 Mesure quantique . . . 68
5.2 Codes quantiques . . . 68
5.2.1 Le groupe de Pauli . . . 68
5.2.2 Codes stabilisateurs . . . 69
5.2.3 Codes CSS . . . 70
5.2.4 Interprétation homologique des codes CSS . . . 72
5.3 Codes LDPC quantiques . . . 73
5.4 La construction de McKay, Mitchison, Shokrollahi . . . 73
5.5 Produits tensoriels itérés de complexes de chaînes et de codes CSS . . . 75
5.5.1 Produits tensoriels de complexes de chaînes . . . 75
5.5.2 Produits tensoriels de codes CSS . . . 76

5.6 Cryptographie à base de codes 81
5.7 Produits $\star$ d'espaces vectoriels et de codes 81
5.7.1 Freiman toujours 81
5.7.2 Extension aux codes géométriques et application au calcul multiparti 82
5.8 Codes géométriques 82
5.8.1 Nouvelles constructions 82
5.8.2 Constructions efficaces 82
5.8.3 Décodage 83
5.9 Et aussi... 83
5.9.1 Codes en métrique rang 83
5.9.2 Codes LDPC quantiques 83

Remerciements

On me l'avait dit : « le plus difficile dans la rédaction d'une habilitation, c'est de dépasser la phase de l'angoisse de la feuille blanche ». J'observe que la rédaction de la seule partie « remerciements » vérifie la même règle impitoyable. Je souhaite pourtant souligner que ce manuscrit n'aurait jamais vu le jour s'il n'y avait pas eu l'aide, le soutien et les encouragements de nombreux collègues et amis que je me dois d'honorer aujourd'hui.

Mes premiers mots iront à Peter Beelen et Nicolas Sendrier pour avoir accepté sans hésitation d'être rapporteurs de cette habilitation et à Jean-François Mestre pour avoir accepté d'en être le tuteur. Je tiens également à exprimer ma gratitude aux autres membres du jury : Irene Bouw, Ronald Cramer, Arnaud Durand, Jean-Pierre Tillich et Damien Vergnaud. C'est une grande fierté pour moi de pouvoir réunir pour ma soutenance des scientifique d'une telle qualité.

Depuis plus de 8 ans maintenant, j'ai le plaisir d'être membre de l'équipe Grace, dont je remercie les membres passés et présents et tout spécialement le chef, Daniel, qui nous fait partager au quotidien sa bonne humeur et sa passion pour les bandes dessinées, les oreilles de cochon et l'informatique. Merci également à Élise et Isabella, des doctorantes comme elles, on aimerait en avoir plus !

Au-delà des frontières de l'équipe, je salue tous mes collègues du LIX et du centre de recherche de Saclay qui, collectivement, contribuent au plaisir que j'ai à me rendre au travail malgré les conditions de transports (je ne remercierai pas transdev, même sous la torture). Un merci particulier à Sylvie Boldo qui m'a accordé sa confiance pour reprendre la responsabilité de la médiation scientifique à Saclay et à Magalie et Fanny qui m'accompagnent au mieux dans cette nouvelle tâche.

Ces dernières années ont été l'occasion de nombreuses collaborations, échanges et discussions. J'ai eu la chance de participer au projet ANR *Manta* et à ses retraites annuelles. J'en remercie tous les membres et « symathisants ». Une pensée particulière va à Marc Perret, celui par qui tout à commencé. Le revoir et continuer à travailler avec lui est un régal toujours renouvelé. Un grand merci également à Gilles Zémor pour nos discussions mathématiques régulières. Je ne me lasserai probablement jamais de ses explications, dont la fin se fait parfois attendre, mais sont toujours des plus éclairantes.

Un autre événement récurrent que je ne manquerais pour rien au monde est le groupe de travail de cryptographie à base de codes que Jean-Pierre organise consciencieusement depuis près de 5 ans. J'ai plaisir à le voir prendre de l'ampleur (le groupe de travail) et j'en remercie sincèrement tous les membres. Tout particulièrement Philippe Gaborit pour avoir assuré un excellent service d'assistance téléphonique du soir dans les dernières étapes de la préparation de BIG QUAKE. Ce groupe de travail est une occasion de plus pour moi de rendre visite aux collègues de l'équipe Secret... pardon *Cosmiq* à qui je transmets un merci collectif pour avoir su au fil des années conserver leur sens de l'accueil, leur tradition des mots fléchés digestifs et deux dictionnaires en lambeaux. Un merci tout particulier à Anne avec qui j'enseigne les codes et la crypto au MPRI depuis 6 ans maintenant, et grâce à qui les dictionnaires précités ont survécu au déménagement de Rocquencourt.

Pour finir, je tiens à remercier mes proches, mes amis et évidemment Gwenola et nos loulous sans qui la vie n'aurait pas la même saveur.

Introduction

Ce document se divise en trois parties résumant mes travaux de recherche dans les trois directions que j'ai suivies après ma thèse. Un fil conducteur connecte cestrois axes de recherche, un mot clé y est omniprésent : les codes correcteurs d'erreurs. J'aime également croire que l'on retrouve dans tous mes travaux mon goût prononcé pour les interactions entre mathématiques et informatique, pour l'algèbre, la géométrie mais également l'algorithmique et mon intérêt pour toutes ces problèmes soulevés par l'informatique et les technologies de la communication qui nourrissent les mathématiques de nouveaux problèmes.

Dans ce qui suit, chaque paragraphe présente un thème de recherche sur lequel j'ai travaillé et commence par la liste des publications issues de ces travaux.

Codes géométriques à partir de surfaces

Publications associées (par ordre chronologique) : [41, 47, 44, 30].

Une première partie concerne les codes géométriques, et en particulier les codes construits à partir de surfaces algébriques. Cet axe de recherche est celui qui se situe le plus dans la continuité de mes travaux de thèse. Dans cette première partie, je présente différentes constructions de codes admettant d'excellents paramètres et obtenus à partir de différents types de surfaces rationnelles : surfaces quadriques, surfaces de del Pezzo, etc... L'estimation de la distance minimale de tels codes pouvant se reformuler en termes d'estimation du nombre maximal de points rationnels d'une famille de variétés, le problème du comptage de points dans une famille de variétés est également abordé dans cette première partie en § 1.3.

Ces travaux ont notamment permis de découvrir de nouveaux codes [41, 30] dont les paramètres battaient les meilleurs codes référencés dans la base de données `codetables.de` [77].

Produits d'espaces et de codes et application à la cryptographie

Publications associées :

— Cryptographie : [48, 54, 51, 50, 56, 55, 52, 17, 49, 20] ;
— Codes de Goppa classiques et opérateur de Cartier : [43, 53] ;
— Produits d'espaces : [11].

Dans une seconde partie, je présente mes travaux en cryptographie basée sur les codes. Il s'agit d'un sujet auquel j'ai commencé à l'intéresser lorsque je suis arrivé à l'INRIA en 2011. Mes travaux dans le domaine se concentrent principalement sur la cryptanalyse de schémas basés sur des codes algébriques et géométriques. Ils on notamment mené à une attaque sur les codes de Goppa sauvages de degré d'extension 2 [53, 55] et sur les codes géométriques [51, 50, 52]. L'attaque sur les codes de Goppa a été la première attaque structurelle de complexité polynomiale sur des codes alternants de degré d'extension strictement supérieur à 1 : autrement dit des codes alternants qui ne sont **pas** des codes de Reed–Solomon généralisés. L'attaque sur les codes géométrique concerne les codes à partir de

courbes de genre quelconque alors que la seule attaque connue jusque là ne concernait que les codes à partir de courbes hyperelliptiques et de petit genre.

Cette partie très portée sur les attaques contient également un volet plus constructif : j'y présente aussi le système BIG QUAKE soumis à l'appel du NIST et auquel j'ai activement participé.

Du point de vue de la cryptanalyse, l'un des outils fondamentaux que j'ai utilisé à maintes reprises est une opération d'apparence totalement élémentaire : le produit $*$. C'est-à-dire, le produit de vecteurs coordonnées par coordonnées et les codes engendrés par de tels produits. Cette opération permet de lire en filigrane sur les codes et de récolter des informations sur les structures algébriques dissimulées derrière. Par ailleurs, cette notion de produits de codes est fortement connecté à des travaux récents consistant à transposer dans un contexte multiplicatif des résultats de combinatoire additive. J'ai mené un travail commun avec Christine Bachoc et Gilles Zémor et obtenu d'intéressants résultats qui pourraient mener à terme vers un analogue multiplicatif du théorème de Freiman. Je présente ce travail à la fin de cette seconde partie car, même s'il ne s'agit pas de cryptographie, le thème de ce travail est très proche des problématiques de produits de codes.

Codes LDPC quantiques

Publications associées : [46, 10].

Dans la dernière partie de document, je présente une autre direction de recherche, à savoir les codes quantiques dits *LDPC*, c'est-à-dire construits à partir de matrices creuses. Il s'agit d'un sujet auquel je me suis initié vers 2010 lorsque j'étais post–doctorant à l'institut de mathématiques de Bordeaux et que j'ai poursuivi plus récemment dans un travail en collaboration avec Benjamin Audoux.

Contenu du document

Tous les résultats présentés dans ce rapport ont donné lieu à des publications dans des conférences ou des journaux et sont accessibles sur ma page web ou sur ArXiv. Aussi, si je fais précisément référence à ces articles, il me semblait sans intérêt d'en reproduire le contenu ici. Mon approche à consisté à résumer ces travaux et si possible de donner un regard différent sur ces derniers. J'ai essayé de faire ressortir les résultats principaux et les points clé de leur démonstration, tout en omettant les détails techniques pour lesquels je renvoie le lecteur à mes articles.

Pour le reste et en vue d'avoir une cohérence globale, j'ai essayé (et ce n'était pas une mince affaire) d'harmoniser les notations sur l'ensemble du manuscrit. Cette harmonisation a un certain prix : les notations de ce manuscrit diffèrent souvent de celles des articles auxquels il fait référence. Par ailleurs certains choix de notations peuvent sembler surprenants mais il a fallu que je m'arrange entre les courbes, les codes, les codes quantiques, l'opérateur de Cartier et les complexes de chaînes pour ne pas désigner par la même lettre $\ll C \gg$ ces différents objets.

Première partie

Codes géométriques

Chapitre 1

Codes géométriques

Prérequis

La théorie des codes est omniprésente dans tout ce mémoire. Les codes correcteurs sont d'ailleurs probablement le seul fil conducteur reliant les différentes parties de ce dernier. Plutôt que d'en rappeler les rudiments ici, et parce qu'on n'est jamais aussi bien cité que par soi même, je renvoie le lecteur à mes notes de cours [45] en m'excusant d'avance auprès des plus grands adeptes de la francophonie : ces notes de cours sont en anglais.

1.1 Historique

1.1.1 Codes sur les courbes algébriques

Introduits à la fin des années 70 par V.D. Goppa [76], les codes géométriques ont été la source d'une recherche intense dans les décennies qui ont suivi. L'article originel de Goppa présentait une généralisation des codes de Goppa classiques comme code d'évaluation en un ensemble de points fixés de résidus de formes différentielles sur une courbe. Cet article de seulement deux pages, cité plusieurs milliers de fois dans la littérature introduit une construction de codes à partir de courbes algébriques et fournit une estimation de leurs paramètres : la dimension provenant du théorème de Riemann–Roch et la distance minimale étant une conséquence du fait que le degré d'un diviseur canonique est toujours égal à $2g-2$ où g désigne le genre de la courbe.

La construction de Goppa permet de dire que, étant donnée une courbe $\mathscr{X}$ projective lisse géométriquement connexe sur $\mathbf{F}_q$ et de genre g, on peut construire des codes de longueur n, dimension k et distance minimale d tels que

$$k + d \geqslant n + 1 - g.$$

Rappelons que, selon la célèbre borne de Singleton en théorie des codes, on a toujours

$$k + d \leqslant n + 1.$$

Autrement dit, les codes géométriques sur une courbe de genre g se situent dans le pire des cas "à g de l'optimal". D'un point de vue asymptotique — et c'est sans doute cet aspect remarquable qui fit la célébrité de ces codes géométriques — si une suite de courbes $(\mathscr{X}_s)_{s\in\mathbb{N}}$ dont la suite des genres $(g_s)_{s\in\mathbb{N}}$ est telle que le ratio $\frac{\sharp\mathscr{X}_s(\mathbf{F}_q)}{g_s}$ converge vers une constante $c > 0$, alors il existe une suite de codes $(\mathcal{C}_s)_{s\in\mathbb{N}}$ de paramètres $[n_s, k_s, d_s]$ telle que les ratios $R_s = \frac{k_s}{n_s}$ et $\delta_s = \frac{d_s}{n_s}$ convergent vers des constantes $(R, \delta) \in [0, 1]^2$ vérifiant

$$R + \delta \geqslant 1 - \frac{1}{c}\cdot$$

En 1982, Tsfasman, Vlăduţ et Zink [148] et indépendamment Ihara [86] prouvent l'existence de familles de courbes modulaires et de Shimura dont le nombre de points rationnels tend vers l'infini, le ratio $\frac{\mathscr{X}(\mathbf{F}_q)}{g(\mathscr{X})}$ tend vers $\sqrt{q}-1$ et ce pour tout q puissance paire d'un nombre premier. Un an plus tard, Drinfel'd et Vlăduţ [151] prouvent que la limite $\sqrt{q}-1$ est en fait optimale. Une quinzaine d'années plus tard, Garcia et Stichtenoth fournissent une construction plus « explicite » de telles familles de courbes à base de tours récursives de corps de fonctions [74].

Ainsi, si q est un carré, cela prouve l'existence d'une famille de codes dont les paramètres asymptotiques vérifient

$$R+\delta \geqslant 1+\frac{1}{\sqrt{q}-1}. \tag{1.1}$$

Cette inégalité prouve l'existence de familles de codes géométriques asymptotiquement bonnes (c'est-à-dire telles que $R>0$ et $\delta>0$) pour tout q carré $\geqslant 16$. Par ailleurs pour $q \geqslant 49$ et pour des valeurs médianes de R,δ, la minoration (1.1) est meilleure que la borne de Gilbert Varshamov. Autrement dit, certaines suites de codes géométriques ont un comportement asymptotique meilleur que des suites de codes aléatoires de mêmes longueur et dimension.

Outre leurs performances asymptotiques, les codes géométriques bénéficient d'algorithmes de décodage efficaces permettant de corriger une quantité d'erreur atteignant la moitié de leur distance *construite*[1] [135, 70]. Voir [83] pour une synthèse sur les algorithmes de décodage unique. On dispose de plus d'algorithmes de décodage en liste permettant de corriger des erreurs jusqu'à la borne de Johnson [78, 22].

Il est fréquent de dire que les codes géométriques soient vus comme une généralisation des codes de Reed–Solomon — qui ne sont rien d'autre que des codes géométriques sur une courbe de genre 0 — permettant, au prix d'une dégradation de la distance minimale, de s'affranchir de la contrainte que le code ne peut pas avoir une longueur dépassant la taille du corps de base. À ce titre, les codes géométriques apparaissent dans de nombreux pans de la littérature et pour de très diverses applications.

Enfin, en dehors des performances asymptotiques, les codes géométriques ont permis de construire un certain nombre des meilleurs codes connus répertoriés par exemple dans la base de données Code Tables [77]. Le lecteur découvrant le domaine pourra être rapidement lassé de voir régulièrement resurgir des courbes aux propriétés extrémales, telles les courbes Hermitiennes, de Suziki, de Giulietti et Korchmáros ou encore la quartique de Klein. Il n'en reste pas moins que ces courbes pouvant être jugées exceptionnelles ou pathologiques pour de nombreuses raisons n'en restent pas moins de remarquables usines à produire de bons codes.

1.1.2 Codes sur les surfaces algébriques

Si les codes géométriques à partir de courbes algébriques ont été sujets à de très nombreux développements et, alors que la définition de code géométrique s'étend aisément aux variétés de dimension quelconque, la littérature sur les codes provenant de variétés de dimension supérieure ou égale à 2 reste extrêmement restreinte. L'article de synthèse de John B. Little [98] écrit il y a une dizaine d'années donnait une présentation encyclopédique des travaux connus en 2008 sur le sujet.

Pourquoi regarder la dimension supérieure ?

En effet, c'est une question légitime dans la mesure où le contexte des courbes fournit de très bons codes en longueur finie, des suites de codes aux paramètres asymptotiques excellents, pour ne pas dire inespérés, ainsi que des algorithmes de décodage de complexité polynomiale. Pourquoi regarder la dimension supérieure ? Outre le pur et simple plaisir de travailler sur des objets géométriques plus riches, on peut donner les motivations suivantes :

1. On appelle *distance construite*, la minoration de la distance minimale donnée par la borne de Goppa. À noter que la détermination exacte de la distance minimale d'un code étant un problème algorithmiquement difficile, on ne dispose en général que de la donnée de cette distance construite. C'est la raison pour laquelle cette distance construite sert de référence pour le décodage.

(1) Pour la construction de codes *en longueur finie* sur un corps $\mathbf{F}_q$, la construction de codes de longueur de l'ordre de q^2 nécessitera de considérer une courbe dont le genre sera minoré par $cq\sqrt{q}$ pour une certaine constante $c > 0$. D'un autre côté une surface aussi élémentaire que $\mathbf{P}^2$ ou une quadrique lisse aura plus de q^2 points rationnels. Ainsi, on peut espérer que à corps de base fixé les variétés de dimension supérieures donnent facilement des codes plus longs. Si l'on inverse la vapeur on peut également dire qu'à longueur de code fixée, le fait de travailler avec des variétés de dimension supérieure permettra de construire des codes sur des corps plus petit, permettant un arithmétique plus simple et plus efficace.

(2) Les surfaces offrent une géométrie nettement plus riche qui ouvre des perspectives nouvelles. Par exemple, l'éclatement d'un point, qui est une opération triviale sur une courbe lisse, transforme une surface lisse en une autre qui aurait q point rationnels supplémentaires.

(3) La dernière décennie a vu l'avènement de nouvelles problématiques de codes, à savoir des codes bénéficiant de « bonnes propriétés locales ». Pour ce type de codes, on attend par exemple d'être capable de déduire à la valeur d'une coordonnée d'un vecteur du code à partir d'un petit nombre d'autres coordonnées de ce dernier. Pour cette problématique, les codes de Reed–Solomon sont relativement médiocres et les codes sur des courbes sont relativement inadaptés. *À contrario*, les codes construits à partir de variétés de dimension supérieure semblent bien mieux répondre à ce type de défi. Ce point avait déjà été observé en 2003 par Bouganis [32]. En effet partant par exemple d'un code sur une surface $\mathscr{X}$ et considérant une courbe $\mathscr{C}$ contenue dans $\mathscr{X}$, les points rationnels de $\mathscr{C}$ correspondent à un certains nombre de coordonnées des mots de code. La projection sur ces coordonnées fournit un morphisme d'un code à partir de la $\mathscr{X}$ vers un code à partir de $\mathscr{C}$. Via ce morphisme, on peut raisonnablement espérer qu'une coordonnée d'un mot correspondant à un point de $\mathscr{C}$ puisse se déduire des coordonnées correspondant aux autres points de la courbe. Aussi, avec une surface $\mathscr{X}$ qui aurait $q^2 + O(q\sqrt{q})$ points rationnels et une courbe $\mathscr{C}$ qui en aurait $q + O(\sqrt{q})$, on obtient un code de longueur $n = q^2 + O(q\sqrt{q})$ dans lequel une coordonnée d'un vecteur peut se déduire de la donnée de $O(\sqrt{n})$ autre coordonnées.

Le revers de la médaille et la raison pour laquelle les codes provenant de variétés de dimension supérieure ou égale à 2 n'a été que peu exploré dans le passé vient essentiellement de ce que la difficulté à estimer les paramètres de tels code est rapidement très élevée. Pour cette raison, on ne trouve que très peu de travaux sur le sujet dans la littérature et ces derniers se cantonnent à traiter le cas de surfaces de dimension de Kodaiara -1 ; des surfaces rationnelles ou réglées. Mes travaux ne font pas exception dans ce domaine.

1.2 Construction et paramètres de codes à partir de variétés de dimension $\geqslant 2$

La construction générale de codes à partir d'une variété algébrique, présentée pour la première fois dans [104] s'énonce comme suit. On se donne une variété projective lisse géométriquement connexe $\mathscr{X}$ définie sur $\mathbf{F}_q$, un diviseur G sur $\mathscr{X}$ et un n–uplet $\mathscr{P} = (P_1, \ldots, P_n) \in \mathscr{X}(\mathbf{F}_q)^n$ de points rationnels qui évitent le support de G. Le code $\mathcal{C}_L(\mathscr{X}, \mathscr{P}, G)$ est défini comme

$$\mathcal{C}_L(\mathscr{X}, \mathscr{P}, G) \stackrel{\text{def}}{=} \{(f(P_1), \ldots, f(P_n)) \mid f \in L(G)\}$$

où $L(G)$ désigne l'espace de Riemann–Roch associé à G.

Remarque 1.2.1. La contrainte selon laquelle les points d'évaluation doivent éviter le support de G semble nécessaire afin que l'on puisse donner un sens à l'évaluation. En réalité, on peut s'en affranchir quitte à modifier la définition d'évaluation ou à remplacer le diviseur par un diviseur linéairement équivalent en invoquant le *moving lemma* [131, III.1.3, Theorem 1]. Un tel changement de diviseur change le code mais pas sa classe d'isométrie : le nouveau code se déduit du premier par multiplication par une matrice diagonale inversible.

Il est bien connu qu'il existe par ailleurs une équivalence entre classes d'équivalence linéaire de diviseurs, classes d'isomorphismes de faisceaux inversibles et classes d'isomorphismes de fibrés en droites. De fait, de manière équivalente, on pourrait remplacer le diviseur par un faisceau inversible ou par un fibré en droites. Le code s'obtiendrait alors en évaluant les sections globales du fibré/faisceau en les points $P_1, \ldots, P_n$. C'est d'ailleurs ainsi que Manin et Vlăduţ définissent ces codes dans [104]. À noter que pour qu'une telle évaluation soit bien définie, il faut se donner en chaque point P_i un système de coordonnées de la fibre dans le cas d'un fibré en droites et un générateur des germes en P_i dans le cas d'un faisceau inversible. La définition du code $\mathcal{C} \stackrel{\text{def}}{=} \mathcal{C}_L(\mathscr{X}, \mathscr{P}, G)$ dépend d'un tel choix en chaque point et changer de coordonnées sur les fibres ou de générateur des germes donnera encore une fois un nouveau code $\mathcal{C}'$ qui se déduit de $\mathcal{C}$ par multiplication à droite par une matrice diagonale inversible. Autrement dit, toutes ces définitions sont équivalentes modulo l'action du groupe des matrices diagonales $n \times n$ inversibles.

1.2.1 Dimension

L'estimation de la dimension peut se faire via le théorème de Riemann–Roch. Dans le cas des codes à partir d'une courbe $\mathscr{X}$ d'un ensemble de n points rationnels $\mathscr{P}$ et d'un diviseur G, sous l'hypothèse que $n > \deg G$, le théorème de Riemann Roch donne directement une minoration de la dimension :

$$\dim \mathcal{C}_L(\mathscr{X}, \mathscr{P}, G) \geqslant \deg G + 1 - g.$$

Cette minoration est une égalité si $\deg G > 2g - 2$.

Pour les codes à partir de surfaces, le théorème de Riemann–Roch ne donne à priori qu'une minoration de $\dim H^0(\mathscr{X}, \mathscr{O}(G)) - \dim H^2(\mathscr{X}, \mathscr{O}(G))$. Une manière simple de se défaire de la dimension de $H^2(\mathscr{X}, \mathscr{O}(G))$ et suggérée par Bouganis reposant sur l'application directe du critère de Nakai Moishezon et du théorème de Riemann Roch. Voir par exemple [81, § V.1].

Notation 1.2.2. Dans ce qui suit, étant donnée une surface $\mathscr{X}$, et deux classes de diviseurs $A, B \in \mathrm{Pic}(\mathscr{X})$, on note $A \cdot B$ le produit d'intersection.

Lemme 1.2.3 ([32, Lemma 1])**.** *Soit $\mathscr{X}$ une surface projective lisse géométriquement connexe sur $\mathbf{F}_q$. Soient G un diviseur sur $\mathscr{X}$ et $\mathscr{P} = (P_1, \ldots, P_n)$ un n–uplet de points rationnels distincts. Si l'application d'évaluation*

$$ev : \left\{ \begin{array}{ccc} L(G) & \longrightarrow & \mathbf{F}_q^n \\ f & \longmapsto & (f(P_1), \ldots, f(P_n)) \end{array} \right.$$

est injective et qu'il existe un diviseur ample H sur $\mathscr{X}$ tel que $G \cdot H > K \cdot H$ alors

$$\dim \mathcal{C}_L(\mathscr{X}, \mathscr{P}, G) = \frac{G \cdot (G - K)}{2} + \chi(\mathscr{O}_{\mathscr{X}}).$$

où $\chi(\mathscr{O}_X)$ désigne la caractéristique d'Euler cohérente du faisceau structural.

Pour les codes provenant de variétés de dimension supérieure, dans la littérature, l'estimation de la dimension repose sur des pratiques plus « artisanales » consistant à considérer des variétés plongées dans un espace projectif $\mathbf{P}^r$ et à considérer l'évaluation de fonction dans $H^0(\mathbf{P}^r, \mathscr{O}(s))$ pour un certain $s > 0$ en les points de la variété.

1.2.2 Distance minimale

Nous abordons le premier point réellement délicat et celui sur lequel se sont essentiellement concentrés les rares chercheurs à s'être aventurés sur le terrain des codes sur les surfaces ou variétés de dimension supérieure. La distance minimale d'un code $\mathcal{C}_L(\mathscr{X}, \mathscr{P}, G)$ sur une variété $\mathscr{X}$ vérifie

$$d = n - \max_{\mathscr{C} \in |G|} |\{\sharp \mathscr{C}(\mathbf{F}_q) \cap \mathscr{P}\}|$$

où n désigne la longueur du code, i.e. le nombre d'éléments de $\mathscr{P}$ et $|G|$ désigne le *système linéaire* associé à G, i.e. l'ensemble des diviseurs positifs linéairement équivalents à G et définis sur $\mathbf{F}_q$.

Dans le cas où le n–uplet $\mathscr{P}$ contient tous les points rationnels de $\mathscr{X}$ on a alors

$$d = \sharp\mathscr{X}(\mathbf{F}_q) - \max_{\mathscr{C}\in|G|} \sharp\mathscr{C}(\mathbf{F}_q).$$

Autrement dit dans ce contexte, l'estimation de la distance minimale se ramène à estimer le nombre maximal de points rationnels d'un élément du système linéaire associé à G. On trouve ainsi dans la littérature différentes bornes génériques plus ou moins simples d'utilisation. Aubry déduit une borne inférieure sur la distance minimale d'un code à partir d'une surface d'une borne supérieure élémentaire sur le nombre de points rationnels d'une courbe projective [6], cette borne ne peut toutefois s'appliquer que si le diviseur G est très ample. Hansen [80], propose deux bornes, l'une mêlant comptage de points et produits d'intersection et nécessitant l'introduction d'une famille de courbes plongée dans la surface et recouvrant tous les points d'évaluation, la seconde fait intervenir la constante de Seshadri associée au diviseur et à l'ensemble des points d'évaluation.

On constate ainsi la marche qu'il y a à franchir lorsque l'on passe des courbes aux surfaces. Pour une courbe, une borne élémentaire sur la distance minimale de points est donnée par le degré du diviseur G. En dimension supérieure, les éléments du système linéaire sont des variétés de dimension $\geqslant 1$ pour lesquelles on doit trouver une borne uniforme sur le nombre de points rationnels.

Focalisons nous maintenant sur le cas où $\mathscr{X}$ serait une surface. Dans ce cas, l'estimation de la distance minimale se ramène à trouver une majoration uniforme sur le nombre de points rationnels de courbes appartenant à un système linéaire complet donné. Une autre difficulté vient de ce qu'un tel système linéaire peut contenir des courbes singulières et même un certain nombre de courbes réductibles. De plus, il est fréquent (mais pas systématique) que le nombre maximal de points rationnels soit atteint par les éléments réductibles du système linéaire. Aussi, pour obtenir une borne supérieure uniforme sur le nombre de points rationnels d'un élément de $|G|$, le calcul du genre arithmétique par la formule d'adjonction et l'application des bornes de Weil ne suffit pas, il faut également être capable de borner le nombre de composantes irréductibles d'une courbe dans ce système linéaire.

Nombre de points de variétés projectives équidimensionnelles et de degré fixé

Motivation Restons dans le contexte où l'on chercherait à minorer la distance minimale d'un code $\mathcal{C}_L(\mathscr{X}, \mathscr{P}, G)$, et donc à majorer le plus finement possible le nombre maximal de points rationnels d'un élément du système linéaire $|G|$. Supposons également que G est très ample, on dispose alors d'un plongement de

$$\psi_G : \mathscr{X} \hookrightarrow \mathbf{P}^{\dim L(G)-1}$$

via lequel le faisceau inversible $\mathscr{O}(G)$ s'identifie à $\psi_G^\star\mathscr{O}(1)$ et les éléments de $|G|$ à l'intersection de $\psi_G(\mathscr{X})$ avec un hyperplan de l'espace projectif ambiant. Dans ce contexte, les éléments de $|G|$ sont des sous-variétés de dimension $r-1$ et de degré G^r. L'estimation de la distance minimale d'un tel code se ramène donc à majorer le nombre de points rationnels de sous-variétés équidimensionnelles de degré fixé d'un espace projectif.

Dans la littérature, on peut distinguer trois approches pour estimer le nombre de points rationnels.

- Les bornes issues de raisonnement purement combinatoires, comme par exemple la borne établie par Serre [130] sur le nombre maximal de points rationnels d'une hypersurface projective.
- Les bornes de type Weil basées sur l'application de la formule des traces de Lefschetz ;
- Les bornes à la Stöhr et Voloch [140] qui s'appliquent principalement aux courbes lisses et consistent à compter le nombre de points géométriques P de la courbe tels que l'espace tangent en P contient l'image de P par le morphisme de Frobenius. Cette condition s'avère plus simple à géométriser que celle consistant à dénombrer les points fixes sous l'action du Frobenius et peut fournir des bornes remarquablement fines dans certains cas. Par exemple pour des courbes planes de degré $\delta \leqslant q$, les bornes les plus fines connues, dues à Homma et Kim [84] reposent sur une utilisation conjointe de la combinatoire et des bornes de Stöhr et Voloch.

Essentiellement, si l'on souhaite comparer les différents types de bornes, les bornes de Weil sont efficaces quand la taille du corps est grande devant les nombres de Betti de la variété. Par exemple dans le cas d'une courbe lisse, la borne de Weil

$$\sharp\mathscr{X}(\mathbf{F}_q) \leqslant q + 1 + 2g\sqrt{q},$$

où g désigne le genre de $\mathscr{X}$ donnera des résultats fins si q est grand devant g. À contrario, pour de petites valeurs de q les bornes à la Stöhr et Voloch et le bornes combinatoires sont en général meilleures. Par ailleurs, un intérêt des méthodes combinatoires est que la prise en compte du cas de variétés singulières ou même réductibles ne représente pas de difficulté supplémentaire.

1.3 Une borne sur le nombre de points rationnels d'une variété projective

Publication associée : [44].

Notation 1.3.1. Dans tout ce qui suit on se fixe un corps fini $\mathbf{F}_q$ et on notera π_r le nombre de points rationnels de $\mathbf{P}^r$. On ajoute à ce la la convention suivante, si $r < 0$ alors $\pi_r = 0$. Autrement dit

$$\pi_r \stackrel{\text{def}}{=} \begin{cases} \sharp\mathbf{P}^r(\mathbf{F}_q) = \frac{q^{r+1}-1}{q-1}. & \text{si} \qquad r \geqslant 0 \\ 0 & \text{sinon.} \end{cases}$$

Mes travaux sur le sujet ont été dans un premier temps motivés par la sortie sur ArXiv d'un article de Lachaud et Rolland [96] proposant une certaine diversité de bornes sur le nombre de points rationnels de variétés projective ainsi qu'un article plus ancien de Ghorpade et Lachaud [75]. Dans ces deux articles, le théorème suivant était conjecturé.

Conjecture 1.3.2 (Ghorpade, Lachaud). Soit $\mathscr{X}$ une sous-variété projective de $\mathbf{P}^r_{\mathbf{F}_q}$ de dimension h et de degré δ. Alors,

$$\sharp\mathscr{X}(\mathbf{F}_q) \leqslant \delta(\pi_h - \pi_{2h-r}) + \pi_{2h-r}.$$

À noter que cette conjecture fournit une borne atteinte par certaines réunion de sous–variétés linéaires de $\mathbf{P}^r$. Plus précisément, si $2h < r$, les réunions de sous–variétés linéaires deux à deux disjointes dans $\mathbf{P}^r$, objets parfois appelés *partial spreads* en géométrie finie. Voir par exemple (la liste n'est pas exhaustive) [29, 88, 89, 109]. Si $2h \geqslant r$, les réunions de sous-variétés linéaires dont les intersections deux à deux sont toutes égales à une même sous-variété linéaire de dimension $2h - r$. Il n'est pas compliqué de se convaincre que, sous l'hypothèse où $\mathscr{X}$ serait une réunion de sous-variétés linéaires, alors le nombre de points rationnels de $\mathscr{X}$ ne peut dépasser la borne conjecturée par Ghorpade et Lachaud. La question restait de savoir si une variété de même dimension et degré pouvait avoir plus de points rationnels que toute réunion de sous-variétés linéaires.

1.3.1 L'approche de Serre pour les hypersurfaces

L'approche que j'ai utilisée consistait à essayer de reproduire la preuve de Serre dans [130] qui démontre cette conjecture dans le cas particulier des hypersurfaces projectives. Je redonne ici dans les grandes lignes les idées de la preuve de Serre. Il s'agissait de supposer l'existence d'un point rationnel P (dans le cas contraire, la borne est trivialement vérifiée) et de considérer le graphe biparti Γ dont l'ensemble des sommets $S_1 \cup S_2$ est défini par

$$S_1 \stackrel{\text{def}}{=} \mathscr{X}(\mathbf{F}_q) \setminus \{P\};$$
$$S_2 \stackrel{\text{def}}{=} \left\{\mathscr{H} \in \check{\mathbf{P}}^r(\mathbf{F}_q) \mid P \in \mathscr{H}\right\}$$

où $\check{\mathbf{P}}^r$ désigne l'espace projectif dual, dont les points rationnels sont en bijection avec les hyperplans de $\mathbf{P}^r$ définis sur $\mathbf{F}_q$. L'ensemble des arêtes est défini par les relations d'incidence naturelles :

$$E \stackrel{\text{def}}{=} \{(P, \mathscr{H}) \in S_1 \times S_2 \mid P \in \mathscr{H}\}.$$

La preuve de Serre se résume comme suit. On se donne une hypersurface $\mathscr{X}$ de degré d définie sur $\mathbf{F}_q$ dans $\mathbf{P}^r$.

(1) On fait l'hypothèse que $\mathscr{X}$ a un point rationnel qui n'est dans aucune composante irréductible de degré 1 de $\mathscr{X}$. Si un tel point n'existe pas, on est ramené au cas de compter les points rationnels d'une réunion d'hyperplans. Sinon, on se fixe un tel point P.

(2) On construit le graphe présenté ci-dessus et on en compte les arêtes de deux manières différentes :
   (a) Pour tout $Q \in S_1 = \mathscr{X}(\mathbf{F}_q) \setminus \{P\}$, le nombre d'arêtes incidentes à Q n'est autre que le nombre d'hyperplans contenant P et Q, à savoir π_{r-2} ;
   (b) Pour tout $\mathscr{H} \in S_2$, l'intersection $\mathscr{X} \cap \mathscr{H}$ est une hypersurface de degré d dans $\mathscr{H}$ et, par récurrence on en déduit que le nombre d'arêtes incidentes à $\mathscr{H}$ est majoré par $dq^{r-2} - \pi_{r-3}$.
   (c) On en déduit donc que l'ensemble des arêtes vérifie

$$\sharp S_1 \cdot \pi_{r-2} = \sharp E \leqslant \sharp S_2 \cdot (dq^{r-2} - \pi_{r-3}).$$

   De fait,

$$(\sharp \mathscr{X}(\mathbf{F}_q) - 1) \cdot \pi_{r-2} \leqslant \pi_{r-1} \cdot (dq^{r-2} - \pi_{r-3}).$$

   De cette dernière formule on peut déduire le résultat. Je revoie à Serre [130] pour plus de détails.

1.3.2 Esquisse de preuve de la conjecture de Ghorpade et Lachaud

Si l'on reprend point par point la preuve de Serre, on constate que la difficulté pour l'étendre au cas de sous-variétés équidimensionnelles va apparaître dans l'étape (2b) car si une section hyperplane d'une hypersurface ne contenant pas l'hyperplan donnera une nouvelle hypersurface, une section hyperplane d'une variété équidimensionnelle peut ne plus être équidimensionnelle dans le cas où certaines composantes irréductibles de notre variété seraient contenues dans l'hyperplan.

La solution que j'ai adoptée pour contourner cette difficulté a consisté à *charger* la récurrence, i.e. à démontrer une hypothèse plus forte pour laquelle l'étape d'hérédité d'une preuve par récurrence se démontrerait. J'ai donc démontré le résultat suivant, dont la conjecture de Ghorpade et Lachaud est un corollaire.

Théorème 1.3.3 ([44]). *Soit $\mathscr{X}$ un sous-schéma fermé de $\mathbf{P}^r$ et $\mathscr{X}_1, \ldots, \mathscr{X}_s$ ses composantes irréductibles. Soient $h_1, \ldots, h_s$ et $\delta_1, \cdots, \delta_s$ les dimensions et degrés respectifs de $\mathscr{X}_1, \ldots, \mathscr{X}_s$ et posons $D \stackrel{def}{=} \max\{h_i \mid 1 \leqslant i \leqslant s\}$, la dimension de $\mathscr{X}$*

$$\sharp \mathscr{X}(\mathbf{F}_q) \leqslant \left(\sum_{i=1}^{s} \delta_i (\pi_{h_i} - \pi_{2h_i - r}) \right) + \pi_{2D-r}.$$

Corollaire 1.3.4. *La conjecture de Ghorpade et Lachaud est vraie.*

La preuve du Théorème 1.3.3 se fait par récurrence sur la dimension maximale d'une composante $\mathbf{F}_q$–irréductible de $\mathscr{X}$ et dans le même esprit que la preuve de Serre par une méthode de double-comptage en considérant les intersections de $\mathscr{X}$ avec des hyperplans passant par un point rationnel fixé. Si tout hyperplan $\mathscr{H} \in \check{\mathbf{P}}^n(\mathbf{F}_q)$ ne contient aucune composante irréductible de $\mathscr{X}$, la preuve de Serre se généralise alors sans difficulté majeure. Il faut ensuite traiter séparément :

— le cas où $\mathscr{X}$ admet des composantes irréductibles de degré 1, autrement dit, des sous-variétés linéaires projectives ;
— le cas où $\mathscr{X}$ a des composantes irréductibles de degré > 1 qui sont contenues dans au moins un hyperplan défini sur $\mathbf{F}_q$.

1.3.3 Questions ouvertes sur l'optimalité de la borne

La borne supérieure obtenue pourrait être améliorée dans certains cas.

1. Si la borne dans le cas équidimensionnel est optimale en ce sens où elle est atteinte par les sous-variétés linéaires, il est possible que la borne générale ne le soit pas. En particulier, on peut démontrer que pour certaines suites de dimension des composantes irréductibles, aucun arrangement de sous-variétés linéaires n'a un nombre de points atteignant la borne du Theorème 1.3.3.
2. Dans sa preuve, Serre signale une amélioration de sa borne dans le cas où l'hypersurface $\mathscr{X} \subset \mathbf{P}^n$ n'est pas une réunion d'hyperplans à savoir

$$\sharp \mathscr{X}(\mathbf{F}_q) \leqslant \delta q^{n-1} + \pi_{n-2} - (q + 1 - \delta).$$

La question de savoir si une telle amélioration pourrait s'étendre au cas des variétés projectives quelconques reste ouverte.

1.4 Quelques exemples de bons codes à partir de surfaces rationnelles

Publication associée : [41].

Jusqu'à la fin de ce chapitre nous allons maintenant nous focaliser sur le cas de codes à partir de surfaces. Les travaux qui précèdent fournissent des méthodes d'estimation de la dimension et de la distance minimale. Toutefois, l'application de la borne obtenue en § 1.3 fournira une minoration de la distance minimale qui aura le mérite d'être générale mais sera souvent assez grossière dans la mesure où elle ne tiendra pas compte de la géométrie de la variété ambiante. Une part de la littérature sur les codes sur les surfaces ou variétés de dimension supérieure se focalise sur des classes de surfaces particulières et dont la géométrie est bien comprise afin d'obtenir des estimations fines des paramètres des codes ainsi construits.

Les codes associés au faisceau $\mathscr{O}(1)$ et $\mathscr{O}(2)$ sur des surfaces et hypersurfaces quadriques on été étudiés dans [7, 63, 64]. Les codes à partir de surfaces Hermitiennes ont été étudiés dans [37, 62]. Les surfaces et variétés toriques ont donné lieu à la construction et l'étude de codes dans [79, 126]. Des codes sur des surfaces cubiques ont été étudiés dans [161] et différentes surfaces rationnelles obtenues par des éclatements du plan on donné lieu à d'intéressantes constructions de codes [99, 57, 15]

Ces références amènent à l'observation suivante. Une piste intéressante pour construire de bons codes (en longueur finie) à partir de surfaces algébriques consiste à choisir des surfaces munies d'un diviseur dont le système linéaire complet associé ne contient que des courbes irréductibles ou à défaut des courbes dont le nombre de composantes irréductibles est borné. C'est l'approche suggérée par Zarzar [161] puis Voloch et Zarzar [152] suggérant d'aller chercher de bons codes parmi les surfaces dont le nombre de Picard arithmétique était petit.

Dans l'article [41], suivant cette approche, j'ai cherché à construire des surfaces rationnelles munies d'un diviseur G telles que le système linéaire $|G|$ ne contienne pas de courbe trop « friable », i.e. admettant beaucoup de composantes irréductibles. L'idée consistait à éclater des points fermés non rationnels de $\mathbf{P}^2$.

1.4.1 Un exemple illustratif

Partons de $\mathbf{P}^2$ muni du système linéaire $|\mathscr{O}(2)|$, i.e. le système linéaire des coniques planes. Dans tout ce qui suit, on choisira comme ensemble de points d'évaluation $\mathscr{P}$ l'ensemble de tous les points rationnels de la surface que l'on ordonnera de manière arbitraire. Rappelons que le choix de l'ordre n'a pas d'influence sur les paramètres du codes. Le code associé est un code de Reed–Muller projectif [95] de longueur $n = q^2 + q + 1$, de dimension $k = 6$ et de distance minimale $d = q^2 - q = n - 2q - 1$. L'estimation de la distance minimale vient de ce qu'une conique plane admet au plus $2q + 1$ points rationnels dans le cas où elle est une réunion de deux droites définies sur $\mathbf{F}_q$.

Éclatement de $\mathbf{P}^2$ en trois points rationnels

Considérons maintenant l'éclatement $\pi : \mathscr{X} \to \mathbf{P}^2$ de $\mathbf{P}^2$ en trois points rationnels P_1, P_2, P_3 que l'on munit du système linéaire $|\mathscr{O}_{\mathscr{X}}(-E_1 - E_2 - E_3) \otimes \pi^\star \mathscr{O}_{\mathbf{P}^2}(2)|$ où E_1, E_2, E_3 désigne les diviseurs exceptionnels. Les éléments de ce système linéaire sont de la forme $\pi^\star C - E_1 - E_2 - E_3$ où $\pi^\star C$ désigne le tiré en arrière d'une conique C contenant les points P_1, P_2, P_3. Le nouveau code obtenu est de longueur $q^2 + 4q + 1$ de dimension 3 : la dimension de l'espace des formes quadratique s'annulant en 3 points et de distance minimale $d = q^2 + q$. La distance minimale vient de ce que la conique plane obtenue par la réunion des droites $C = L_{12} \cup L_{13}$ où L_{ij} est la droite joignant les points P_i, P_j. La tirée en arrière de C est de la forme

$$\pi^\star C = \widetilde{L}_{12} + \widetilde{L}_{13} + 2E_1 + E_2 + E_3$$

où $\widetilde{L}_{ij}$ désigne la transformée stricte de L_{ij} par π. De fait, le système linéaire $|\mathscr{O}(-E_1 - E_2 - E_3) \otimes \pi^\star \mathscr{O}(2)|$ contient une courbe

$$\widetilde{L}_{12} + \widetilde{L}_{13} + E_1$$

admettant trois composantes irréductibles lisses de genre 0. Une telle courbe admet $3q + 1$ points rationnels, ce qui donne une distance minimale vérifiant

$$d \leqslant n - (3q + 1).$$

Une analyse plus poussée montre que cette inégalité est atteinte.

Éclatement de $\mathbf{P}^2$ en un point fermé de degré 3

Considérons maintenant une tordue de la surface considérée, à savoir l'éclatement de $\mathbf{P}^2$ en un point fermé de degré 3 non contenu dans une droite ou, de manière équivalente, en 3 points non alignés $P, P^\sigma, P^{\sigma^2}$ définis sur $\mathbf{F}_{q^3}$ et conjugués sous l'action de $\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)$. L'existence d'un tel point peut se faire via un procédé de comptage ou plus simplement en partant d'un point fermé de degré 3 de $\mathbf{P}^1$ et en considérant son image par le plongement de Veronese

$$\left\{ \begin{array}{ccc} \mathbf{P}^1 & \longrightarrow & \mathbf{P}^2 \\ (u:v) & \longmapsto & (u^2 : uv : v^2) \end{array} \right. .$$

Dans ce contexte, le code obtenu sera de même dimension que dans le cas précédent, à savoir 3, mais la longueur ne verra pas d'augmentation, i.e. restera à $q^2 + q + 1$ car les points éclatés ne sont pas rationnels. Enfin la distance minimale sera égale à $q^2 = n - (q + 1)$.

En conclusion, au prix d'une longueur n plus petite, on peut construire un code de même dimension avec une distance minimale telle que la différence $n - d$ est significativement plus petite. Plus précisément, en sacrifiant une partie de la longueur, on est passé de paramètres relatifs

$$R = \frac{k}{n} = \frac{3}{q^2 + 4q + 1} \qquad \delta = \frac{d}{n} = \frac{q^2 + q}{q^2 + 4q + 1}$$

à des paramètres relatifs

$$R = \frac{3}{q^2 + q + 1} \qquad \delta = \frac{q^2}{q^2 + q + 1}.$$

Autrement dit, les paramètres relatifs ont été améliorés. Cette observation a motivé certains de mes travaux. Pour les codes sur des courbes, la tentation naturelle pour chercher de bons codes a été d'aller chercher à les construire à partir de courbes dont le ratio nombre de points / genre était optimal ou proche de l'optimum. Pour les surfaces, les premiers travaux ont consisté à chercher des codes à partir d'une surface Hermitienne, cette dernière ayant en effet un grand nombre de point. Or lorsque l'on cherche des codes optimaux, il peut être préférable de chercher des surfaces ayant un moindre nombre de points rationnels mais telles qu'il existe un système linéaire complet de diviseurs dont les sections sont toutes irréductibles ou admettent dans le pire des cas qu'un « petit » nombre de composantes irréductibles. Dans le § 1.5 nous illustrons cette philosophie sur un cas d'apparence élémentaire, celui des quadriques de $\mathbf{P}^3$.

1.4.2 Nouveaux codes à partir d'éclatés de $\mathbf{P}^2$ en des points irrationnels

L'exemple qui précède du plan projectif éclaté en un point fermé de degré 3 permet de construire de très bons codes en considérant le faisceau

$$\mathscr{F}_i \stackrel{\text{def}}{=} \mathscr{O}_{\mathscr{X}}(-E) \otimes \pi^\star \mathscr{O}_{\mathbf{P}^2}(i)$$

où $\pi : \mathscr{X} \to \mathbf{P}^2$ désigne le morphisme d'éclatement et E désigne le diviseur exceptionnel dont le support est la réunion de trois droites conjuguées sous l'action de Galois. Ici encore, on prendra pour ensemble de points d'évaluation $\mathscr{P}$, l'ensemble de tous les points rationnels de $\mathscr{X}$ ordonnés de manière arbitraire.

Pour $i = 3, 4$ et 5 les codes obtenus sont excellents et ont parfois permis de dépasser les meilleurs paramètres connus jusque là. Plus précisément, pour $i = 3$, et pour tous les corps finis de cardinal inférieur ou égal à 9, les codes obtenus atteignaient les meilleurs paramètres connus comme en atteste le tableau 1.1. La dernière colonne de ce tableau donne la meilleure distance minimale référencée dans `codetables` avant la publication de mes travaux pour un code de même longueur et dimension. Les tableaux 1.2 et 1.3 traitent respectivement les cas $i = 4$ et 5. Les codes obtenus sur $\mathbf{F}_7$ pour $i = 4$ et sur $\mathbf{F}_9$ pour $i = 5$ battent un record.

Dans ce qui suit, nous expliquerons comment les paramètres sont évalués dans le cas $i = 3$, pour les autres cas et d'autres constructions de codes à partir de surfaces rationnelles, je renvoie le lecteur à [41].

Remarque 1.4.1. La surface obtenue est en fait une surface de del Pezzo de degré 6, nous reviendrons sur les surfaces de del Pezzo en § 1.6.1.

Remarque 1.4.2. Sachant que π induit une bijection entre les points rationnels de la surface $\mathscr{X}$ et ceux de $\mathbf{P}^2$, les codes $C(\mathscr{X}, \mathscr{P}, \mathscr{F}_i)$ peuvent être décrit de manière bien plus élémentaire. Il s'agit des sous-codes des codes de Reed–Muller projectifs de degré i provenant de l'évaluation de de formes homogènes de degré i s'annulant en un point fermé de degré 3.

q	n	k	d	Meilleur d jusque là
3	13	7	5	5
4	21	7	11	11
5	31	7	19	19
7	57	7	41	41
8	73	7	55	55
9	91	7	71	71

TABLE 1.1 – Parametres du code $C(\mathscr{X}, \mathscr{P}, \mathscr{F}_3)$.

q	n	k	d	Meilleur d jusque là
4	21	12	7	7
5	31	12	14	14
7	**57**	**12**	**34**	33
8	73	12	47	48
9	91	12	62	62

TABLE 1.2 – Paramètres du code $C(\mathscr{X}, \mathscr{P}, \mathscr{F}_4)$.

q	n	k	d	Meilleur d jusque là
5	31	18	9	9
7	57	18	27	27
8	73	18	39	40
9	**91**	**18**	**53**	52

TABLE 1.3 – Paramètres du code $C(\mathscr{X}, \mathscr{P}, \mathscr{F}_5)$.

Détermination des paramètres pour $i = 3$

Partant de la Remarque 1.4.2, la dimension du code s'obtient aisément, il s'agit de l'espace des formes de degré 3 s'annulant en 3 points géométriques. L'espace des formes cubiques ternaires est de dimension 10. On en déduit que le code obtenu est de dimension 7.

Pour la distance minimale, il s'agit de déterminer le nombre maximal de points rationnels d'une cubique contenant un point de degré 3 fixé. On distingue trois situations

(1) La cubique est irréductible ;

(2) La cubique est une réunion d'une droite et d'une conique plane C irréductible.

(3) La cubique est une réunion de trois droites.

La contrainte selon laquelle la cubique doit contenir un point fermé de degré 3 fait que le cas (3) nécessite que les trois droites soient définies sur $\mathbf{F}_{q^3}$ et conjuguées sous l'action de Galois. Une telle cubique n'a pas de point rationnels.

Pour le cas (1), la borne de Homma Kim [84] nous dit qu'une telle courbe a au plus $2q + 1$ points rationnels. Quant au cas (2), il peut donner des courbes à $2q + 2$ points rationnels dans le cas où la conique et la droite se coupent en des points non rationnels. Une telle configuration est possible dans la mesure où, une fois choisie une conique irréductible contenant le point fermé de degré 3, on est entièrement libre de positionner la droite comme on le souhaite. Cela fournit des paramètres de la forme

$$[q^2 + q + 1, 7, q^2 - q - 1].$$

À noter que la formule sur la distance minimale est exacte et non une minoration puisque le discours qui précède sur le cas (2) fournit des mots dont le poids atteint exactement cette valeur.

Constacyclicité des codes obtenus

En soumettant les nouveaux codes obtenus à `Codetables`, Markus Grassl me signala que ces codes, pour un certain choix d'ordre des points d'évaluation, étaient consta-cycliques. Autrement dit ils étaient globalement invariants par une isométrie pour la métrique de Hamming de la forme

$$\left\{ \begin{array}{ccc} \mathbf{F}_q^n & \longrightarrow & \mathbf{F}_q^n \\ (x_1, \ldots, x_n) & \longmapsto & (ax_2, x_3, \ldots, x_n, x_1) \end{array} \right.$$

pour un certain $a \in \mathbf{F}_q^\times$. Ce phénomène s'explique aisément puisque cet automorphisme du code, provient d'un automorphisme de la surface qui permute cycliquement tous ses points rationnels. Cet automorphisme provient d'un automorphisme linéaire de $\mathbf{P}^2$ qui laisse fixe les points géométriques $P, P^\sigma, P^{\sigma^2}$. On peut décrire l'automorphisme comme suit. On considère un générateur ζ du groupe multiplicatif $\mathbf{F}_{q^3}^\times$. L'application

$$\left\{ \begin{array}{ccc} \mathbf{F}_{q^3} & \longrightarrow & \mathbf{F}_{q^3} \\ x & \longmapsto & \zeta x \end{array} \right.$$

est $\mathbf{F}_q$–linéaire et peut être vue comme un automorphisme ψ $\mathbf{F}_q$–linéaire de $\mathbf{F}_q^3$ dont les valeurs propres sont $\zeta, \zeta^q, \zeta^{q^2}$ et admet trois vecteurs propres associés définis sur $\mathbf{F}_{q^3}$ et conjugués sous Galois. En

projectivisant on obtient un élément $\bar{\psi} \in \mathbf{PGL}(3, \mathbf{F}_q)$ qui induit un automorphisme de $\mathbf{P}^2$ fixant un point fermé de degré 3 correspondant à la réunion des 3 droites propres de ψ.

1.5 Quadriques et tordues de variétés de Segré

Publication associée : [47].

Une famille plus élémentaire de surfaces rationnelles lisses sont les quadriques de $\mathbf{P}^3$. Il en existe deux classes d'isomorphisme appelées quadriques *elliptiques* et *hyperboliques* qui — en caractéristique différente de 2 — correspondent aux formes quadratiques de rang 4 en quatre variables de discriminant -1 et 1. Pour le cas de la caractéristique 2, je renvoie à [82, § 15.3].

Le plongement de Segré de $\mathbf{P}^1 \times \mathbf{P}^1$ a pour image une quadrique hyperbolique, ce qui fait de cette surface une surface doublement réglée. La quadrique elliptique est une tordue quadratique de la quadrique hyperbolique.

La détermination de la distance minimale des codes sur ces surfaces associés au faisceau $\mathscr{O}(d)$ a été étudiée par Edoukou [63] pour les cas $d \leqslant 2$. Dans un travail commun avec Iwan Duursma [47], nous avons déterminé la distance minimale exacte de ces codes pour tout d. Le cas de la quadrique hyperbolique est somme toute élémentaire dans la mesure où le plongement de Segré nous montre que le code obtenu n'est autre qu'un produit tensoriel de deux codes sur $\mathbf{P}^1$, autrement dit de deux codes de Reed–Solomon généralisés. Or il est bien connu que les paramètres des produits tensoriels de codes sont les produits des paramètres des codes considérés. Ainsi pour une quadrique hyperbolique munie du faisceau $\mathscr{O}(d)$ on obtient les paramètres

$$[(q+1)^2, (d+1)^2, (q-d+1)^2].$$

Plus généralement, regardant cette surface comme $\mathbf{P}^1 \times \mathbf{P}^1$, on peut considérer le faisceau $\mathscr{O}(a, b)$ et obtenir des paramètres

$$[(q+1)^2, (a+1)(b+1), (q-a+1)(q-b+1)].$$

1.5.1 Quadriques elliptiques : la géométrie ne peut pas tout

Le cas des quadriques elliptiques est plus délicat. Une telle surface a q^2+1 points rationnels, ce qui nous fournit la longueur du code. La dimension s'obtient aisément, car la surface étant isomorphe sur $\mathbf{F}_{q^2}$ à $\mathbf{P}^1 \times \mathbf{P}^1$, la dimension du code est la même que dans le cas hyperbolique, autrement dit

$$k = (d+1)^2.$$

Pour la distance minimale, sa détermination se ramène à estimer le nombre maximal de points rationnels de l'intersection de la quadrique avec une surface de degré d transverse à cette dernière :

$$d = q^2 + 1 - \max\{\sharp C(\mathbf{F}_q),\ C \in |\mathscr{O}_{\mathscr{X}}(d)|\}.$$

La détermination de ce nombre maximal n'a rien d'évident, du moins nous ne sommes pas parvenus à l'estimer via des méthodes arithmétiques ou géométriques classiques. Il est connu que le groupe de Picard de cette surface est libre de rang 1 et engendré par $\mathscr{O}_{\mathscr{X}}(1)$. Autrement dit, tout diviseur est linéairement équivalent à un multiple entier d'une section plane.

Une section plane de cette surface est soit une conique lisse dans le cas où le plan n'est pas tangent à la quadrique, soit une réunion de deux droites définies sur $\mathbf{F}_{q^2}$ et conjuguées sous l'action de Galois dans le cas où le plan est tangent. Les sections planes donnant le plus grand nombre de points rationnels sont les coniques lisses qui ont $q+1$ points rationnels. On en déduit que l'intersection de $\mathscr{X}$ avec une réunion de d plans a au plus $d(q+1)$ points rationnels. La borne $d(q+1)$ peut être atteinte si ces d plans sont distincts, définis sur $\mathbf{F}_q$ et vérifient également les conditions suivantes.

— aucun de ces plans n'est tangent à $\mathscr{X}$;
— ils s'intersectent tous en une même droite L de l'espace ambiant ;
— l'intersection de L avec $\mathscr{X}$ n'a pas de points rationnels, autrement dit est un point fermé de degré 2.

Il est tentant de penser qu'une intersection de $\mathscr{X}$ avec une surface de degré d ne peut pas avoir plus de points rationnels qu'une réunion de sections planes deux-à-deux sans points rationnels communs et, ainsi d'espérer une borne du type

$$\max\{\sharp C(\mathbf{F}_q) \mid C \in |\mathscr{O}_{\mathscr{X}}(d)|\} = d(q+1). \tag{1.2}$$

Cette formule est effectivement exacte mais sa démonstration nécessite des arguments supplémentaires. Il n'y en effet pas de raison à priori pour que les courbes de $|\mathscr{O}_{\mathscr{X}}(d)|$ admettant le nombre maximal de points rationnels proviennent d'intersections de $\mathscr{X}$ avec une réunion de d plans. Nous avons d'ailleurs trouvé des exemples de courbes irréductibles provenant de l'intersection de $\mathscr{X}$ avec une surface cubique admettant ce nombre de points. L'irréductibilité entraîne qu'une telle courbe ne peut pas être l'intersection de $\mathscr{X}$ avec une réunion de 3 plans. Voir [47, Exemple 4.14] pour plus de détails.

1.5.2 Les codes BCH à la rescousse

Pour démontrer que le nombre maximal de point d'une intersection d'une quadrique elliptique $\mathscr{X}$ avec une surface de degré s vérifie bien (1.2), on peut dans un premier temps considérer les deux méthodes suivantes.

(1) considérer les composantes $\mathbf{F}_q$–irréducibles séparément, en estimer le genre arithmétique via la formule d'adjonction, puis, enfin en majorer le nombre de points via une borne sur le nombre de points de courbes singulières, comme par exemple [8, § 4.1].

(2) utiliser la rationalité de $\mathscr{X}$, considérer une paramétrisation $\mathbf{P}^2 \dashrightarrow \mathscr{X}$ et compter les points de la tirée en arrière d'une courbe qui sera alors une courbe plane de degré $2d$. Cette approche ayant entre autres l'intérêt que pour les courbes planes, on connaît des bornes [130, 143, 84] ne dépendant que du degré de cette courbe et qui, sur de petits corps s'avèrent bien plus fines que les bornes à la Weil.

Force est de constater qu'aucune de ces approches n'a été fructueuse pour parvenir à prouver (1.2). Je n'aurais pas la prétention de dire que la borne (1.2) ne peut s'obtenir par des méthodes de comptage habituelles, mais le fait est que nous n'y sommes pas parvenus de cette manière. De façon assez surprenante, ce sont des méthodes de théorie des codes qui nous ont permis de conclure. En effet, nous sommes parvenus à montrer que les codes $\mathcal{C}_L(\mathscr{X}, \mathscr{P}, \mathscr{O}_{\mathscr{X}}(d))$ étaient des codes BCH doublement étendus et pour lesquels la borne BCH fournit la distance minimale exacte. En inversant la vapeur, le résultat sur la distance minimale permet de démontrer (1.2).

La structure de code cyclique étendu de $\mathcal{C}_L(\mathscr{X}, \mathscr{P}, \mathscr{O}_{\mathscr{X}}(d))$ s'interprète géométriquement par le fait que $\mathscr{X}$ admet un automorphisme permutant cycliquement tous ses points rationnels sauf deux qu'elle laisse fixe. L'existence de cet automorphisme peut se comprendre de différentes manières en voici deux :

— On peut montrer que la variété $\mathscr{X}$ sur $\mathbf{F}_q$ est la restriction de Weil de $\mathbf{P}^1_{\mathbf{F}_{q^2}}$ sur $\mathbf{F}_q$. On constate par exemple que l'on a bien $\sharp\mathbf{P}^1(\mathbf{F}_{q^2}) = \sharp\mathscr{X}(\mathbf{F}_q)$. Par fonctorialité de la restriction de Weil, un $\mathbf{F}_{q^2}$–automorphisme de $\mathbf{P}^1$ induit un $\mathbf{F}_q$–automorphisme de $\mathscr{X}$. Si l'on considère l'automorphisme de $\mathbf{P}^1$ défini par

$$(u : v) \longmapsto (\zeta u : v)$$

où $\zeta \in \mathbf{F}_{q^2}^{\times}$ est un générateur du groupe multiplicatif, cet automorphisme permute cycliquement les éléments de $\mathbf{F}_{q^2}^{\times}$ et donc permute les $\mathbf{F}_{q^2}$–points de $\mathbf{P}^1$ en laissant fixes l'origine $(0 : 1)$ et le point à l'infini $(1 : 0)$.

— De manière plus explicite, si en prenant pour notre quadrique la surface d'équation

$$XT - Q(Y, Z) = 0$$

où Q est une forme homogène de degré 2 irréductible sur $\mathbf{F}_q$ qui se factorise sur $\mathbf{F}_{q^2}$ en

$$Q(Y, Z) = (Y - \zeta Z)(Y + \zeta^q Z)$$

où $\zeta \in \mathbf{F}_{q^2}$ est un générateur de l'extension $\mathbf{F}_{q^2}/\mathbf{F}_q$, l'automorphisme provient d'une homographie de $\mathbf{P}^3$ définie par la matrice

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -\mathrm{N}(\zeta) & -\mathrm{Tr}(\zeta) & 0 \\ 0 & 0 & 0 & \mathrm{N}(\zeta) \end{pmatrix}$$

où $\mathrm{N}(\zeta)$ et $\mathrm{Tr}(\zeta)$ désignent respectivement la norme et la trace de ζ dans $\mathbf{F}_{q^2}/\mathbf{F}_q$, à savoir, ζ^{q+1} et $\zeta + \zeta^q$. On vérifie en effet que

$$Q(-\mathrm{N}(\zeta)Z, Y - \mathrm{Tr}(\zeta)Z) = \mathrm{N}(\zeta) \cdot Q(Y, Z).$$

Soient $P = (1 : 0 : 0 : 0)$ et $Q = (0 : 0 : 0 : 1)$ les points fixes de l'automorphisme. L'existence de cet automorphisme permet de prouver que le code, $\mathcal{C}_L(\mathscr{X}, \mathscr{P}', \mathscr{O}_{\mathscr{X}}(d))$ où $\mathscr{P}' = \mathscr{X}(\mathbf{F}_q) \setminus \{P, Q\}$ est un code cyclique. On démontre ensuite [47, Theorem 4.10] qu'il s'agit en fait d'un code BCH, dont les paramètres avaient déjà été étudiés dans [61] où il était prouvé qu'un tel code avait pour paramètres

$$[q^2 - 1, (s+1)^2, q^2 - 1 - s(q+1)].$$

On en déduit alors les résultats suivants.

Théorème 1.5.1 ([47]). *Les paramètres du code $\mathcal{C}_L(\mathscr{X}, \mathscr{P}, \mathscr{O}_X(d))$ vérifient :*

$$[q^2 + 1, (s+1)^2, q^2 + 1 - s(q+1)].$$

Corollaire 1.5.2 ([47]). *La relation (1.2) est vraie.*

La géométrie ne peut pas tout Ce phénomène est assez intéressant à mon sens pour la raison suivante. Lorsque j'étais en thèse, je vendais souvent le discours selon lequel la théorie des codes porte des problèmes combinatoires et algorithmiques difficiles et que la théorie des codes géométriques permet la traduction de ces problèmes en des problèmes de type arithmétique ou géométrique. Par exemple l'estimation de la distance minimale de $\mathcal{C}_L(\mathscr{X}, \mathscr{P}, \mathscr{O}_{\mathscr{X}}(d))$ pouvant se reformuler en l'estimation de $\max\{\sharp C(\mathbf{F}_q) \mid C \in |\mathscr{O}_{\mathscr{X}}(d)|\}$. Ensuite, la puissance de la géométrie algébrique permettrait de résoudre tous les problèmes. Or ici, face à un problème d'apparence simple : majorer le nombre de points d'une courbe sur une quadrique, les techniques classiques de géométries ne nous ont pas permis d'obtenir un résultat assez fin là où des méthodes classiques de théorie des codes l'ont permis.

1.6 Codes anticanoniques à partir de surfaces de del Pezzo

Publication associéé : [30].

Un travail en collaboration avec des membres de l'ANR Manta (Régis Blache, Emmanuel Hallouin, David Madore, Jade Nardi, Matthieu Rambaud et Hugues Randriambololona) [30], a consisté à rechercher des surfaces de del Pezzo produisant de bons codes en passant au crible toutes les types de surfaces de del Pezzo sur $\mathbf{F}_q$ dont le nombre de Picard était égal à 1 et étudié les codes *anticanoniques*, autrement dit les codes $\mathcal{C}_L(\mathscr{X}, \mathscr{P}, -K_{\mathscr{X}})$ où $K_{\mathscr{X}}$ désigne la classe canonique. Cette approche, plus

systématique et bine moins artisanale que celle que j'avais adoptée dans [41] s'est montrés très fructueuse. Il s'agissait donc de classifier surfaces de del Pezzo en fonction de leur fonction Zeta, ou, de manière équivalente de l'action du Frobenius sur leur groupe de Picard géométrique. Ensuite, parmi celles qui avaient un groupe de Picard arithmétique de rang 1, on estimait les paramètres du code anticanonique associé, puis cherchait à donner une construction explicite d'un tel code.

1.6.1 Surfaces de del Pezzo

Une surface de del Pezzo est une surface $\mathscr{X}$ dont la classe anticanonique $-K_{\mathscr{X}}$ est ample. Sur un corps algébriquement clos, une telle surface est toujours isomorphe à un éclatement du plan en $9-d$ poins pour un certain $1 \leqslant d \leqslant 8$ appelé le *degré* de la surface. Dans le cas où $3 \leqslant d \leqslant 7$ la classe anticanonique est très ample et le plongement associé donne une surface de degré d dans $\mathbf{P}^d$. Par ailleurs, pour une telle surface, le Comme une telle surface $\mathscr{X}$ est rationnelle, $H^1_{\text{ét}}(\overline{\mathscr{X}}, \mathbf{Q}_\ell) = H^3_{\text{ét}}(\overline{\mathscr{X}}, \mathbf{Q}_\ell) = 0$, la fonction Zeta de la surface ne dépend donc que de l'action du Frobenius sur le $H^2_{\text{ét}}(\overline{\mathscr{X}}, \mathbf{Q}_\ell)$. Par ailleurs, d'après [103, Theorem 27.1] l'action du Frobenius sur le groupe de Picard géométrique permet de décrire entièrement l'arithmétique de la surface. Enfin, le fait que la surface soit $\overline{\mathbf{F}}_q$–isomorphe à un éclaté de $\mathbf{P}^2$ en un nombre fini de points fournit une description de $\mathrm{Pic}(\overline{\mathscr{X}})$ comme un groupe discret muni d'une forme bilinéaire symétrique : le produit d'intersection.

À un tel réseau, on associe un système de racines et un groupe de Weyl, l'action du Frobenius sur le Picard géométrique est alors associée à une classe de conjugaison dans un certain groupe de Weyl. La classification de ces classes de conjugaison, permet de définir des types de surfaces de del Pezzo et parmi ces derniers, d'identifier les types correspondant aux surfaces de del Pezzo de rang de Picard (arithmétique) égal à 1.

1.6.2 Exemples de codes

Les meilleurs exemples viennent d'une surfaces de del Pezzo de degré 5 obtenue à partir de $\mathbf{P}^2$ en éclatant un point fermé de degré 5 non contenu dans une droite et en contractant la transformée stricte de l'unique conique plane le contenant. Le tableau 1.6.2 fournit les paramètres des codes anticanoniques provenant de telles surfaces pour différents corps de base. Sur les corps $\mathbf{F}_8$ et $\mathbf{F}_9$ les paramètres obtenus battent les meilleurs codes connus jusque là.

q	3	4	5	7	8	9
$[n,k,d]$	$[10,6,3]$	$[17,6,8]$	$[26,6,16]$	$[50,6,37]$	$[\mathbf{65},\mathbf{6},\mathbf{51}]$	$[\mathbf{82},\mathbf{6},\mathbf{66}]$

TABLE 1.4 – Paramètres de codes à partir d'une surface de del Pezzo de degré 5

Deuxième partie

Produits d'espaces et de codes, de la combinatoire additive à la cryptanalyse

Chapitre 2

Cryptographie à base de codes

2.1 Histoire

L'histoire de la cryptographie à base de codes commence à la fin des années 70, très peu de temps après l'introduction de la cryptographie à clé publique par Whitfield Diffie et Martin Hellman. Tout commence avec un résultat dû à Berlekamp, McEliece et Van Tilborg.

Théorème 2.1.1 (Berlekamp, McEliece, Van Tilborg [25])**.** *Le problème suivant est NP-complet.*

> **Problème du décodage borné.** *Étant donnés un code $\mathcal{C} \subseteq \mathbf{F}_{q^n}$, un vecteur $\boldsymbol{y} \in \mathbf{F}_q^n$ et un entier $0 \leqslant t \leqslant n$. Décider s'il existe $\boldsymbol{c} \in \mathcal{C}$ tel que*
>
> $$d_H(\boldsymbol{c}, \boldsymbol{y}) \leqslant t,$$
>
> *où $d_H(\cdot, \cdot)$ désigne la distance de Hamming.*

La difficulté du problème du décodage borné encourage McEliece à proposer dans la foulée un schéma de chiffrement dont la sécurité reposerait sur la difficulté de ce problème [108].

2.1.1 Présentation du schéma de chiffrement de McEliece

Nous donnons ici une présentation générale du schéma de chiffrement de McEliece. Des exemples particuliers d'instanciation de ce schéma seront donnés plus loin en § 2.3.

Le schéma de McEliece est un schéma de chiffrement à clé publique. Pour l'instancier, il faut se donner une famille de codes $\mathcal{F}$ pour laquelle on dispose d'un algorithme de décodage efficace $\mathcal{D}$. Par « efficace » on entend que sa complexité doit être polynomiale en la longueur du code considéré. On introduit également un ensemble $\mathcal{S}$, qui sera l'ensemble des clés secrètes, tel que à tout $s \in \mathcal{S}$ on associe un code $\mathcal{C}(s) \in \mathcal{F}$. Autrement dit, on dispose d'une fonction surjective :

$$\mathcal{C} : \mathcal{S} \longrightarrow \mathcal{F} \tag{2.1}$$

Enfin, l'algorithme de décodage prendra parmi ses entrées le secret s. Autrement dit, on souhaite que le décodage soit facile si l'on connaît s et difficile si on l'ignore.

Clé secrète. Un élément $s \in \mathcal{S}$;

Clé publique. Un couple $(\boldsymbol{G}_{\text{pub}}, t)$ où $\boldsymbol{G}_{\text{pub}}$ est une matrice génératrice du code $\mathcal{C}(s)$, que l'on appellera *code public*, et t est le nombre d'erreurs maximal que l'algorithme $\mathcal{D}$ peut corriger.

Chiffrement. Le message clair est un vecteur $\boldsymbol{m} \in \mathbf{F}_q^k$ et le chiffré

$$\boldsymbol{y} \stackrel{\text{def}}{=} \boldsymbol{m}\boldsymbol{G} + \boldsymbol{e}$$

où $\boldsymbol{e}$ est une variable aléatoire de loi uniforme à valeur dans les vecteurs de poids de Hamming t.

Déchiffrement On applique l'algorithme de décodage :

$$\mathcal{D}(s, \boldsymbol{y}) = \boldsymbol{m}.$$

Remarque 2.1.2. Insistons sur le fait qu'il ne s'agit que d'une primitive cryptographique qui ne peut pas être utilisée en l'état. Afin d'avoir un niveau de sécurité au moins du type IND–CPA, une conversion sémantiquement sûre est nécessaire. Voir [118] pour plus de détails.

Remarque 2.1.3. Notons que la fonction 2.1 n'est pas injective en général, elle ne le sera pas pour tous les exemples de codes algébriques ou géométriques que nous regarderons par la suite. Aussi, une attaque pourra consister à chercher, non pas s mais un élément $s \in \mathcal{S}$ tel que $\mathcal{C}(s')$ est égal à $\mathcal{C}(s)$.

Cette présentation met bien en évidence les difficultés à la mise en place d'un tel système. La difficulté d'un problème du décodage borné nous dit qu'un attaquant qui connaîtrait le chiffré $\boldsymbol{y}$ aura des difficultés à en déduire le clair si le code $\mathcal{C}$ était un code quelconque. Toutefois, pour que le système soit utilisable, il faut que l'on soit dispose d'un algorithme de décodage efficace pour le code $\mathcal{C}$, or, pour un code pris au hasard, il n'existe pas de tel algorithme. Aussi toute la difficulté réside dans le choix d'une bonne famille de codes. Cette famille doit vérifier les propriétés suivantes :

- L'ensemble $\mathcal{S}$ doit contenir suffisamment d'éléments pour qu'une attaque par recherche exhaustive soit hors de portée ;
- La famille $\mathcal{F}$ doit disposer d'un algorithme de décodage efficace (de complexité polynomiale en n) permettant de corriger t erreurs et ce seulement si l'on dispose de l'élément s permettant de construire le code ;
- Enfin, et c'est là l'aspect le plus délicat, il ne faut pas que l'on puisse déduire la clé secrète s à partir de la seule connaissance du code $\mathcal{C}(s)$. Autrement dit, il faut une famille de codes disposant d'un algorithme de décodage et donc d'une structure particulière mais qui soient indistinguables de codes aléatoires.

La présentation usuelle du schéma de McEliece dans la littérature La présentation faite du schéma de McEliece peut sembler différente de celle que l'on voit classiquement dans la littérature. Une présentation plus classique consiste à dire que la clé secrète est la donnée de

- une matrice génératrice $\boldsymbol{G}_{\text{sec}}$ « structurée » d'un code $\mathcal{C}$;
- une matrice inversible $\boldsymbol{S} \in \mathbf{GL}_k(\mathbf{F}_q)$;
- une matrice de permutation $\boldsymbol{P} \in \mathfrak{M}_n(\mathbf{F}_q)$

La clé publique est alors la donnée d'un entier t et de la matrice

$$\boldsymbol{G}_{\text{pub}} \stackrel{\text{def}}{=} \boldsymbol{S}\boldsymbol{G}_{\text{sec}}\boldsymbol{P}.$$

Je pense que cette présentation, qui est la présentation historique proposée par McEliece dans son article [108], est à proscrire car elle mène à un certain nombre de contresens. Déjà, parce que pour beaucoup de familles considérées, si un code $\mathcal{C} \in \mathcal{F}$, alors son image par une permutation des coordonnées sera aussi dans la famille $\mathcal{F}$. Autrement dit, le groupe symétrique $\mathfrak{S}_n$ agit sur $\mathcal{F}$. Par conséquent, le fait de spécifier la permutation $\boldsymbol{P}$ dans la présentation du système revient à supposer que toute orbite de $\mathcal{F}$ pour l'action de $\mathfrak{S}_n$ aurait un représentant canonique, ce qui est faux pour l'écrasante majorité des familles de codes considérées pour instancier le schéma. De plus, la présence de la matrice $\boldsymbol{S}$ laisse penser qu'un code dispose d'une matrice génératrice canonique et que la connaissance de cette dernière suffirait à déduire un algorithme de décodage. Ce dernier point est faux pour beaucoup familles de codes et au mieux discutable pour les autres.

En § 2.3, nous présenterons des attaques pour différentes instanciations du schéma de McEliece, i.e. pour différents choix de familles de codes et nous verrons que l'attaque ne consiste jamais « à retrouver les matrices $\boldsymbol{S}$ et $\boldsymbol{P}$ » mais plutôt à retrouver un secret $s' \in \mathcal{S}$ (qui n'est pas unique en général) et tel que le code public soit égal à $\mathcal{C}(s')$.

2.1.2 Pourquoi faire de la cryptographie avec des codes ?

La proposition originelle de McEliece reposait sur la famille des codes de Goppa binaires que nous présenterons en § 2.2.2. Il proposait dans son article l'utilisation de codes de paramètres $[1024, 524, 101]$ pour lesquels on sait efficacement corriger 50 erreurs. La clé publique sera donc une matrice génératrice d'un tel code. On peut se contenter d'en publier une matrice systématique, *i.e.* sous forme échelonnée réduite ce qui donne une matrice de taille 500×524, soit $32,75$ kilo-octets (kB). Cette taille de clé prohibitive si l'on compare avec RSA ou un schéma de chiffrement basé sur les courbes elliptiques. Pour cette raison, le schéma de McEliece, et plus généralement, la cryptographie basée sur les codes a longtemps été considérée comme un sujet théorique mais sans possible application pratique.

Les choses ont considérablement évolué dans les deux dernières décennies pour deux raisons. La première est que de nouvelles propositions ont permis une réduction très significative des tailles de clés. La proposition la plus offensive dans ce domaine vient des codes MDPC (*Moderate Parity Check Codes*) quasi–cycliques (QC-MDPC) [113], fournissent une sécurité de 128bits [1] avec des clés de taille $\approx 1{,}27$ kilo-octets. La seconde est que la cryptographie basée sur les codes dispose d'atouts que n'ont pas les schémas basés sur des problèmes de théorie algorithmique des nombres comme la factorisation ou le problème du logarithme discret. D'abord, le schéma de McEliece permet un chiffrement et un déchiffrement rapide. Ensuite, la montée en puissance de l'informatique quantique et la menace grandissante de l'arrivée d'un ordinateur quantique qui, comme l'a prouvé Shor dans [132] pourrait efficacement résoudre des problèmes de théorie algorithmique des nombres tel la factorisation d'entiers ou le problème du logarithme discret, encourage à se tourner vers de nouveaux schémas de chiffrement que l'on estime *post quantiques*. La cryptographie à base de codes tout comme la cryptographie à base de réseaux apparaît alors comme une alternative pertinente.

2.1.3 L'appel du NIST

Un événement représentatif de l'intérêt croissant pour la cryptographie post quantique est l'appel émis par le NIST en 2016 pour standardiser de nouveaux systèmes de chiffrement, signature ou échange de clés résistant à un ordinateur quantique. Sur les 64 soumissions complètes reçues par le NIST, 19 étaient basées sur les codes. J'ai moi-même porté la soumission BIG QUAKE [17] que je présenterai en § 3.5.1.

2.1.4 Comment analyse-t-on la sécurité d'un schéma à la McEliece ?

En § 2.3, je présenterai différents choix de familles de codes et discuterai leur sécurité. Il est donc naturel de se demander comment on estime la sécurité d'un schéma à la McEliece. On distinguera deux types d'attaques :

— Les *attaques sur les messages* consistant à décrypter un message chiffré à partir de la connaissance du code public ;

— Les *attaques sur la clé* ou *attaques structurelles* qui consistent à retrouver un secret $s' \in \mathcal{S}$ tel que le code public $\mathcal{C}_{\text{pub}} = \mathcal{C}(s')$.

1. On dira que la sécurité d'un schéma est estimée à x bits, si la meilleure attaque connue coûterait à l'attaquant plus de 2^x opérations élémentaires. À l'heure actuelle, on considère que nos capacités de calculs ne peuvent dépasser 2^{80} à 2^{90} opérations élémentaires. Actuellement, les attentes standards pour un schéma de chiffrement sont d'assurer une sécurité supérieure à 128 bits. Dans le récent appel du NIST évoqué en § 2.1.3, trois niveaux de sécurité différents étaient attendus : 128, 192 et 256 bits de sécurité.

C'est la raison pour laquelle lorsque l'on discutera la sécurité d'une famille de codes, on traitera séparément la question de la sécurité des messages et celle de la sécurité des clés. Mis à part dans le cas des codes QC–MDPC, ces deux problèmes sont en général très différents et requièrent des analyses distinctes. La *sécurité* d'un schéma sera définie comme le minimum de la sécurité des clés et des messages. Autrement dit le coût minimal d'une attaque parmi toutes les attaques sur les messages et toutes les attaques structurelles connues.

Attaques sur les messages

Les attaques sur les messages reposent sur des algorithmes de décodage *génériques*, c'est-à-dire des algorithmes permettant de corriger des erreurs pour n'importe quel code. De tels algorithmes ont une complexité exponentielle et partent tous d'une même idée : l'algorithme de Prange [120], également appelé *décodage par ensemble d'information*. L'idée de l'algorithme de Prange s'explique comme suit.

— On dispose d'un code $\mathcal{C}_{\text{pub}} \subseteq \mathbf{F}_q^n$ décrit par une matrice génératrice $\boldsymbol{G}_{\text{pub}}$ et d'un vecteur $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$ dont le poids de Hamming vérifie $\mathrm{w_H}(\boldsymbol{e}) \leqslant t$.

— On tire au hasard un ensemble $\mathcal{I} \subseteq \{1, \dots, n\}$ de cardinal k. Tel que le mineur $k \times k$ de $\boldsymbol{G}_{\text{pub}}$ correspondant aux colonnes indicées par $\mathcal{I}$ soit non nul.

— Supposons que $\mathcal{I}$ soit tel que le support de l'erreur évite $\mathcal{I}$, autrement dit, pour tout $i \in \mathcal{I}$, $\boldsymbol{e}_i = 0$. Alors, le vecteur $\boldsymbol{y}_{\mathcal{I}}$ obtenu en par projection sur les coordonnées dont l'indice est dans $\mathcal{I}$ vérifie $\boldsymbol{y}_{\mathcal{I}} = \boldsymbol{c}_{\mathcal{I}}$, de plus, par hypothèse sur la matrice $\boldsymbol{G}_{\text{pub}}$ et l'ensemble $\mathcal{I}$, $\boldsymbol{c}$ est entièrement déterminé par sa projection $\boldsymbol{c}_{\mathcal{I}}$, on peut donc déduire $\boldsymbol{c}$ de $\boldsymbol{c}_{\mathcal{I}}$ par un simple procédé d'élimination Gaussienne. On vérifie que le vecteur obtenu $\boldsymbol{c}$ est proche de $\boldsymbol{y}$ pour la métrique de Hamming, si c'est le cas, le décodage a réussi.

— Si $\mathcal{I}$ n'évite pas le support de l'erreur, on calculera un mot $\boldsymbol{c}' \in \mathcal{C}_{\text{pub}}$ qui sera loin de $\boldsymbol{y}$, on en déduit que l'on a échoué et on recommence avec un autre $\mathcal{I}$.

La complexité moyenne de cet algorithme dépend de la probabilité de trouver un bon ensemble $\mathcal{I}$ évitant le support de l'erreur :

$$\mathbb{P}\left(\forall i \in \mathcal{I}, \boldsymbol{e}_i = 0\right) = \frac{\binom{n-t}{k}}{\binom{n}{k}}$$

On en déduit une complexité moyenne en $O\left(\frac{\binom{n}{k}}{\binom{n-t}{k}} n^\omega\right)$, où ω désigne l'exposant de l'algèbre linéaire (disons que $\omega = 3$). On montre aisément que, dans le cas où k et t dépendent linéairement de n, alors l'algorithme est de complexité exponentielle en n.

Des améliorations de l'algorithme de Prange reposant sur des principes classiques d'algorithmique : compromis temps/mémoire, paradoxe des anniversaires etc... permettent d'obtenir une complexité, certes toujours exponentielle mais significativement meilleure que celle de Prange. De telles améliorations sont proposées dans [137, 60, 97, 35, 106, 21, 107].

Remarque 2.1.4. Il est important de noter que les attaques sur les messages sont génériques en ce sens qu'elles peuvent être appliquées en l'état à n'importe quel code.

Remarque 2.1.5. Signalons que, dans le cas où le code disposerait d'un groupe d'automorphismes non trivial G, alors l'algorithme [129] permet de diviser la complexité d'un algrotihme de décodage générique par $\sqrt{|G|}$. Ce gain reste mineur comparé au coût de tels algorithmes.

Attaques structurelles

À la différence des attaques sur les messages, les attaques sur les clés sont très spécifiques de la famille de codes $\mathcal{F}$ choisie pour instancier le schéma de chiffrement. Nous en présenterons un certain nombre en § 3.3.

2.1.5 D'autres schémas de chiffrement à base de codes

Avant de rentrer dans le vif du sujet, il est important de signaler que la cryptographie basée sur les codes ne se limite pas au chiffrement et au schéma de McEliece. Dans les dernières années, d'autres paradigmes très prometteurs, inspirés des travaux d'Alekhnovich [5] ont émergé, tels que les schémas HELEN [59], HQC [2] ou son analogue en métrique rang RQC [3].

2.2 Codes algébriques pour la cryptographie

Nous avons déjà présenté dans le chapitre 1 les codes géométriques, dans ce qui suit nous allons présenter d'autres familles de codes. En un sens toutes ces familles sont reliées de près ou de loin à des codes géométriques, mais disposent en général d'une présentation plus élémentaire et permettant d'éviter toute considération de géométrie algébrique.

2.2.1 Codes de Reed–Solomon généralisés

Une fois n'est pas coutume, je renvoie ici le lecteur à mes notes de cours [45] pour plus de détails sur les définitions et résultats énoncés ci-dessous.

Notation 2.2.1. Soit k un entier positif, on note $\mathbf{F}_q[X]_{<k}$ l'espace vectoriel des polynômes de degré strictement inférieur à k.

Les codes de Reed–Solomon généralisés notés GRS (pour *Generalised Reed–Solomon codes*) ne sont rien d'autre que des codes géométriques construits à partir de la droite projective. Une définition plus élémentaire s'obtient comme suit.

Définition 2.2.2 (Codes de Reed–Solomon Généralisés)**.** Soient $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbf{F}_q^n$ un vecteur dont les coordonnées sont deux à deux distinctes. Soit $\boldsymbol{y} \in \mathbf{F}_q^n$ un vecteur dont tous les coefficients sont non nuls. Soit $k \leqslant n$ un entier, alors le *code de Reed–Solomon généralisé* associé au couple $(\boldsymbol{x}, \boldsymbol{y})$ est défini par

$$\mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y}) \stackrel{\text{def}}{=} \{(y_1 f(x_1), \ldots, y_n f(x_n)) \mid f \in \mathbf{F}_q[X]_{<k}\}\,.$$

Les vecteurs $\boldsymbol{x}, \boldsymbol{y}$ sont respectivement appelés *support* et *multiplieur* du code. Dans le cas où $\boldsymbol{y} = (1, \ldots, 1)$, le code est un code de Reed–Solomon et est noté $\mathbf{RS}_k(\boldsymbol{x})$.

Remarque 2.2.3. Notons que pour un code de Reed–Solomon généralisé, le support et le multiplieur ne sont pas uniques. Par exemple, remplacer $\boldsymbol{x}$ par son image par une application affine fournira le même code.

Les codes de Reed–Solomon généralisés bénéficient d'algorithmes de décodage efficace permettant de corriger jusqu'à $t = \left\lfloor \frac{n-k}{2} \right\rfloor$ erreurs en $O(n^2)$ opérations dans $\mathbf{F}_q$, via l'algorithme d'Euclide. L'arithmétique rapide permet même de les décoder en temps quasi-linéaire.

Par ailleurs, ces codes sont la brique de base pour construire une large famille de codes appelés *codes alternants*.

2.2.2 Codes alternants, codes de Goppa classiques

La notion de sous-code sur un sous-corps

La notion de sous-code sur un sous-corps est une notion, certes relativement élémentaire, mais d'un intérêt fondamental, à la fois en théorie des codes algébriques mais également pour leurs applications à la cryptographie à base de codes. En particulier, il est important de signaler qu'une quantité de constructions de codes algébriques s'interprète en termes de sous-codes sur un sous-corps de codes GRS, c'est le cas des codes de Goppa classiques, des codes BCH, des codes de Srivastava, etc... Voir [102, Chap. 12] pour plus de détails.

Définition 2.2.4. Soit $\mathcal{C} \subseteq \mathbf{F}_{q^m}^n$ un code. Son *sous-code sur le sous-corps* $\mathbf{F}_q$ n'est autre que

$$\mathcal{C} \cap \mathbf{F}_q^n.$$

Son *code trace* est défini par

$$\mathrm{Tr}(\mathcal{C}) \stackrel{\text{def}}{=} \{(\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(c_1), \ldots, \mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(c_n)) \mid \boldsymbol{c} = (c_1, \ldots, c_n) \in \mathcal{C}\}.$$

Selon un célèbre théorème dû à Delsarte [58], pour tout $\mathcal{C} \subseteq \mathbf{F}_{q^m}^n$, on a

$$(\mathcal{C} \cap \mathbf{F}_q^n)^\perp = \mathrm{Tr}(\mathcal{C}^\perp)$$

et les paramètres de $\mathcal{C} \cap \mathbf{F}_q^n$ se déduisent de ceux de $\mathcal{C}$ comme suit.

Proposition 2.2.5. *Soit $\mathcal{C} \subseteq \mathbf{F}_{q^m}^n$ un code de paramètres $[n, k, d]_{q^m}$, alors le code $\mathcal{C} \cap \mathbf{F}_q^n$ a pour paramètres $[n, \geqslant n - m(n-k), \geqslant d]$.*

Pour les dimensions et distances minimales d'un sous-code sur un sous-corps, on ne dispose que de bornes inférieures. Pour un code aléatoire, la borne inférieure sur la dimension est atteinte avec une probabilité qui tend vers 1 quand $k \to \infty$ pour la distance minimale, la borne inférieure fournie est loin de la vraie distance minimale dans le cas typique. Il est en particulier connu (voir par exemple [149, Theorem 9.4.1]) que certains codes alternants, i.e. les sous-codes sur un sous-corps de codes GRS atteignaient la borne de Gilbert Varshamov, qui s'avère être bien au-dessus de la borne fournie par la proposition 2.2.5. Un résultat similaire est prouvé par Voss et Stichtenoth pour les sous-codes sur des sous-corps de codes géométriques [153].

Toutefois, en cryptographie basée sur les codes, la notion de distance minimale importe peu. Le paramètre important est en réalité le nombre d'erreurs que saura corriger notre algorithme de décodage. Sur ce point il est important de noter que si l'on dispose d'un algorithme de décodage permettant de corriger t erreurs pour un code $\mathcal{C} \subseteq \mathbf{F}_{q^m}^n$, alors le même algorithme permettra de corriger t erreurs pour le code $\mathcal{C} \cap \mathbf{F}_q^n$.

Codes alternants

Définition 2.2.6 (Code alternant)**.** Soient $\boldsymbol{x}, \boldsymbol{y} \in \mathbf{F}_{q^m}^n$ un support et un multiplieur. Soit r un entier. On définit le code alternant $\mathcal{A}_{r,q}(\boldsymbol{x}, \boldsymbol{y})$ par

$$\mathcal{A}_{r,q}(\boldsymbol{x}, \boldsymbol{y}) \stackrel{\text{def}}{=} \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^\perp \cap \mathbf{F}_q^n.$$

L'entier r est appelé *degré* du code alternant. L'entier m est appelé son *degré d'extension*.

Remarque 2.2.7. Rappelons que $\mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^\perp = \mathbf{GRS}_{n-r}(\boldsymbol{x}, \boldsymbol{y}^\perp)$ où $\boldsymbol{y}^\perp$ est un autre multiplieur qui s'exprime en fonction de $\boldsymbol{x}$ et $\boldsymbol{y}$. L'expression explicite de $\boldsymbol{y}^\perp$ est donnée dans [45, Thm 6.6]. Aussi, un code alternant n'est autre qu'un sous-code sur un sous-corps d'un code GRS, le fait de le définir via un GRS dual dans la définition n'est qu'une convention qui s'avèrera utile dans certaines situations.

D'après les résultats qui précédent ainsi que les propriétés des codes GRS, un code alternant de longueur n et de degré r et de degré d'extension m a des paramètres de la forme

$$[n, \geqslant n - mr, \geqslant r + 1]. \tag{2.2}$$

Un tel code bénéficie de plus d'un algorithme corrigeant $\lfloor \frac{r}{2} \rfloor$ erreurs en temps polynomial.

Codes de Goppa classiques

Les codes de Goppa classiques, sont des cas particuliers de codes alternants qui bénéficient d'un algorithme pouvant corriger jusqu'à deux fois plus d'erreurs.

Définition 2.2.8 (Code de Goppa classique)**.** Soit $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbf{F}_{q^m}^n$ un support et $g \in \mathbf{F}_{q^m}[X]$ un polynôme tel que $g(x_i) \neq 0$ pour tout $i \in \{1, \ldots, n\}$. Le code de Goppa classique associé à $(\boldsymbol{x}, g)$ est défini par

$$\mathcal{G}_q(\boldsymbol{x}, g) \stackrel{\text{def}}{=} \mathcal{A}_{\deg(g),q}(\boldsymbol{x}, g(\boldsymbol{x})^{-1})$$

où $g(\boldsymbol{x})^{-1}$ désigne le vecteur $(g(x_1)^{-1}, \ldots, g(x_n)^{-1})$.

Attention ! Notons ici une ambiguïté dans la terminologie qui peut perturber. Les codes géométriques ont été découverts par Goppa et sont parfois appelés « codes de Goppa ». **Les codes de Goppa classiques définis précédemment ne sont pas des codes géométriques sur $\mathbf{P}^1$** mais des sous-codes sur des sous-corps de certains codes géométriques sur $\mathbf{P}^1$. Afin d'éviter toute confusion, je parlerai pour les codes construits à partir de courbes de *codes géométriques* , dédiant le terme « code de Goppa » aux codes de Goppa classiques de la Définition 2.2.8.

L'intérêt des codes de Goppa classiques réside dans l'énoncé suivant.

Théorème 2.2.9 ([142])**.** *Soit $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbf{F}_{q^m}^n$ un support et $g \in \mathbf{F}_{q^m}[X]$ un polynôme tel que $g(x_i) \neq 0$ pour tout $i \in \{1, \ldots, n\}$. Si g est sans facteur carré, alors*

$$\mathcal{G}_q\left(\boldsymbol{x}, g^{q-1}\right) = \mathcal{G}_q\left(\boldsymbol{x}, g^q\right).$$

Selon le théorème 2.2.9, de tels codes de Goppa ont donc des paramètres de la forme

$$[n, \geqslant n - m(q-1)\deg g, \geqslant q \deg g + 1]_q. \tag{2.3}$$

En particulier pour $q = 2$, on obtient des paramètres de la forme

$$[n, \geqslant n - \deg g, \geqslant 2\deg g + 1] \tag{2.4}$$

et pour un tel code, on peut corriger jusqu'à $\deg g$ erreurs, soit 2 fois plus que pour un code alternant de même dimension.

2.3 Exemples d'instanciations du schéma de McEliece

2.3.1 Les différentes instanciations de McEliece dans la littérature

On distingue deux grandes familles de codes utilisées pour instancier le schéma de McEliece, je parlerai de constructions *algébriques* et de constructions *probabilistes*. Dans les constructions algébriques, on trouve les codes construits par évaluation de polynômes, tels les codes de Reed–Solomon généralisés, les codes de Goppa classiques, les codes géométriques ou encore les codes de Reed–Muller.

Dans les constructions *probabilistes*, on trouvera essentiellement la famille des codes dits MDPC (*Moderate Density Parity Check*). Mon travail s'est principalement concentré sur les constructions algébriques. Une présentation chronologique des principaux résultats sur les schéma de chiffrement à la McEliece est donnée page 43.

2.3.2 Quelques exemples pour démarrer

Maintenant que nous disposons de familles de codes, reprenons la présentation générique du schéma de McEliece en § 2.1.1 et donnons quelques exemples concrets, en particulier pour l'ensemble des secrets $\mathcal{S}$.

Codes GRS On se fixe un corps fini $\mathbf{F}_q$ et des entiers n, k tels que $q \geqslant n \geqslant k$ (ces données sont donc publiques). L'ensemble $\mathcal{S}$ est l'ensemble des couples $(\boldsymbol{x}, \boldsymbol{y}) \in (\mathbf{F}_q^n)^2$ tels que $\boldsymbol{x}$ est un support (i.e. ses coordonnées sont distinctes) et $\boldsymbol{y}$ un multiplieur (i.e. ses coordonnées sont toutes non nulles). Étant donnée une clé secrète $s = (\boldsymbol{x}, \boldsymbol{y})$, on lui associera le code $\mathcal{C}(s) = \mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y})$. Une clé publique associée sera de la forme $(\boldsymbol{G}_{\text{pub}}, t)$ où $\boldsymbol{G}_{\text{pub}}$ est une matrice génératrice de $\mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y})$ et $t = \lfloor \frac{n-k}{2} \rfloor$.

Notons que cet exemple d'utilisation est à proscrire puisqu'il est la cible d'une attaque très efficace due à Sidelnikov et Shestakov [134].

Codes de Goppa binaires On se fixe des entiers m, n, r (ces données sont donc publiques). L'ensemble $\mathcal{S}$ est l'ensemble des couples $(\boldsymbol{x}, g) \in \mathbf{F}_{2^m}^n \times \mathbf{F}_{2^m}[X]$ où $\boldsymbol{x}$ est un support et g un polynôme de degré r sans facteur carré et sans racine parmi les coefficients de $\boldsymbol{x}$. Cette famille de codes a donné lieu aux soumissions du NIST Classic McEliece [26] et NTS KEM [4].

Codes de Goppa q–aires On peut évidemment étendre la proposition qui précède au cas de codes de Goppa q–aires. De telles propositions ont été faites par exemple dans [27, 28]

Codes géométriques On se fixe une courbe $\mathscr{X}$ de genre g, un entier $n \leqslant \sharp\mathscr{X}(\mathbf{F}_q)$ et un entier m tel que $m > 2g - 2$ et $m + 1 - g < n$. L'ensemble $\mathcal{S}$ est l'ensemble des couples $(\mathscr{P}, G)$ où $\mathscr{P}$ est un n–uplet ordonné de points distincts $(P_1, \ldots, P_n) \in \mathscr{X}(\mathbf{F}_q)$ et G un diviseur de degré m.

À noter que nous faisons le choix ici de rendre la courbe publique, un autre choix pourrait être fait et la seule référence sur le sujet [87] n'est pas claire sur ce point.

Codes QC–MDPC Les codes QC–MDPC ont été introduits dans [113]. Ce sont des codes binaires de longueur n qui sont noyau d'une matrice dont le poids des lignes est en $O(\sqrt{n})$ ils sont munis d'un algorithme probabiliste de complexité linéaire en n permettant de corriger de l'ordre de $O(\sqrt{n})$ erreurs. Il a également été récemment prouvé dans [146] que ce même algorithme pouvait corriger tout motif d'erreur de poids $O\left(\frac{\sqrt{n}\log\log n}{\log n}\right)$ sans échouer. En termes de correction d'erreurs ils sont en réalité peu performants comparé à des codes LDPC (poids des lignes en $O(\log n)$), ils sont par contre particulièrement intéressants, leur version quasi–cyclique permet de proposer un schéma de chiffrement avec des clés publique de $1,25$ à $2,7$ kilo-octets pour 128 bits de sécurité ce qui est fortement concurrentiel pour des schéma de cryptographie post–quantiques. Les codes MDPC ont donné lieu aux soumissions au NIST BIKE [1] et QC–MDPC KEM [160].

2.3.3 Le schéma original de McEliece

La proposition originelle de McEliece [108] reposait sur des codes de Goppa binaires. La clé secrète est donc un couple $(\boldsymbol{x}, g) \in \mathbf{F}_{2^m}^n \times \mathbf{F}_{2^m}[X]$ et la clé publique associée est le couple $(\boldsymbol{G}, t)$ où $\boldsymbol{G}$ est une matrice génératrice du code $\mathcal{G}_q(\boldsymbol{x}, g)$ et t le nombre d'erreurs que l'on peut corriger, à savoir $t = \deg g$.

Sécurité des messages.

McEliece suggérait les paramètres suivants, un degré d'extension 10 et un polynôme de Goppa de degré 50. Cela donne pour la clé publique un code de paramètres $[1024, 524, \geqslant 101]_2$ pour lequel on peut corriger 50 erreurs. Pour ce code, McEliece garantit un niveau de sécurité supérieur à 65 bits. En réalité, en 1978, le seul algorithme de décodage générique existant était celui de Prange dont le coût moyen pour un tel code serait plutôt de 2^{80} opérations. Si l'on considère les algorithmes existants aujourd'hui, un algorithme tel que BJMM [21] permettrait de décrypter des messages en $\approx 2^{48}$ opérations. Dans le cadre de l'appel du NIST, la soumission *Classic McEliece* [26] se base exactement sur la proposition

originale de McEliece. Pour garantir une sécurité de 128 bits les auteurs y proposent une clé publique de 261 kilo-octets.

Sécurité des clés

Pour la sécurité de la clé on peut s'intéresser au cas d'une recherche exhaustive sur les clés secrètes à savoir sur les couples $(\boldsymbol{x}, g)$. Si l'on se contente de dénombrer les polynômes irréductibles, on a $\approx \frac{2^{10 \cdot 50}}{50} \approx 2^{494}$ tels polynômes.

Cet exemple est assez significatif du schéma de McEliece basé sur les codes de Goppa binaire, on observe un décalage conséquent entre le coût de la meilleure attaque sur les messages et celui de la meilleure attaque sur la clé. Nous y reviendrons un peu plus loin.

Taille de clé

On suppose que la clé publique est une matrice mise sous forme *systématique*, autrement dit sous forme échelonnée réduite en supposant que les k premières colonnes sont indépendantes. Dans cette situation si le code public est de paramètres $[n, k]$, la clé publique sera une matrice $\boldsymbol{A}$ de taille $k \times (n-k)$ telle que $(\boldsymbol{I}_k \mid \boldsymbol{A})$ est une matrice génératrice du code public. Ainsi on aura une taille de clé de $k(n-k)\log_2(q)$ bits, soit pour la proposition originale de McEliece, une clé d'environ $32,7$ kilo-octets. Les paramètres proposés pour classic McEliece donnent des clés de 1 à 1,3 méga-octet pour 256 bits de sécurité. On voit là le principal défaut de McEliece, la taille considérable des clés publiques.

Par conséquent, pendant longtemps, la cryptographie basée sur les codes était jugée comme un domaine purement théorique et sans application pratique envisageable. Deux phénomènes ont changé la donne : tout d'abord, la montée de la « menace quantique », qui a encouragé à réfléchir à de nouvelles alternatives en cryptographie à clé publique. Fait qui a entre autres motivé l'appel émis par le NIST en 2017 pour de nouvelles primitives cryptographiques pouvant résister à l'ordinateur quantique. Ensuite, des propositions nouvelles et nettement plus compétitives ont vu le jour. Citons par exemple les codes MDPC quasi-cycliques [113] utilisés dans la soumission BIKE [2] [1] au NIST permettent une sécurité estimée à 128 bits pour des clés publiques d'$1,27$ à $2,5$ kilo octets.

2.3.4 Codes munis d'un groupe d'automorphisme non trivial

Comme expliqué précédemment, le défaut majeur des schémas de chiffrement basés sur les codes est la taille de la clé publique. Pour pallier cette faiblesse, une solution, suggérée par Gaborit [72] en 2005 consiste à utiliser comme code public un code muni d'un groupe d'automorphisme G non trivial. Ainsi, au lieu de publier une base du code public, il suffit de s'en donner une famille génératrice pour sa structure de $\mathbf{F}_q[G]$–module. Si le code est $\mathbf{F}_q[G]$–libre, une telle approche permet de diviser la taille de la clé par $\sharp G$.

Les codes GRS sont des codes géométriques sur $\mathbf{P}^1$ et les codes alternants des sous-codes sur des sous-corps de ces derniers. Le groupe projectif $\mathbf{PGL}_2$ agit sur $\mathbf{P}^1$ et, de cette action, on peut déduire des codes GRS ou alternants munis d'automorphismes non triviaux. Si l'on considère un automorphisme $\sigma \in \mathbf{PGL}_2(\mathbf{F}_q)$ et un support $\boldsymbol{x}$ dont l'ensemble des coefficients est globalement invariant par σ, l'homographie σ induit alors une permutation $\bar{\sigma}$ sur les coefficients de $\boldsymbol{x}$. Si les coefficients de $\boldsymbol{y}$ sont constants sur toute orbite pour $\bar{\sigma}$, alors, $\bar{\sigma}$ induit une isométrie de $\mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y})$ pour tout $k > 0$ et de $\mathcal{A}_{r,q}(\boldsymbol{x}, \boldsymbol{y})$ pour tout $r > 0$. Pour un code de Goppa classique $\mathcal{G}_q(\boldsymbol{x}, g)$, tout automorphisme $\sigma \in \mathbf{PGL}_2(\mathbf{F}_q)$ qui laisse les coefficients de $\boldsymbol{x}$ globalement invariants et tel que $g \circ \sigma = g$ induit une isométrie du code de Goppa.

2. Bit flIpping Key Encapsulation.

2.4 Codes géométriques pour la cryptographie

2.4.1 Codes à partir de courbes

En 1996, Janwa et Moreno [87] proposent trois schémas de chiffrement basés sur les codes géométriques. La clé publique pouvant être

(i) un code géométrique à partir d'une courbe ;

(ii) un sous-code sur un sous-corps d'un code géométrique ;

(iii) un code géométrique concaténé avec un bon code défini sur un sous-corps.

L'article de Janwa et Moreno ne propose pas de paramètres spécifiques et ne produit pas d'analyse de sécurité du schéma. Il reste d'ailleurs flou sur la définition de la clé secrète. En particulier le fait que la courbe soit publique ou gardée secrète n'y est pas discuté. Dans ce qui suit nous verrons que, pour les schémas que nous sommes parvenus à attaquer, la connaissance préalable d'un modèle de la courbe n'est pas nécessaire.

Concernant les trois propositions de Janwa et Moreno, notons que l'on peut d'office écarter la suggestion (iii) basée sur les codes concaténés. En effet, un travail de Sendrier [128] prouve que l'opération de concaténation n'ajoute pas de sécurité supplémentaire. Autrement dit, la version (iii) ne peut pas être plus sûre que la version (i).

Quant aux deux autres propositions, la proposition (i) a été l'objet d'une attaque en temps polynomial dans le cas de codes provenant de courbes de genre 1 par Minder [110], cette attaque fut ensuite étendue aux codes à partir de courbes hyperelliptiques par Faure et Minder [69] avec une complexité exponentielle en le genre de la courbe. Dans un travail commun avec Irene Márquez–Corbella et Ruud Pellikaan [52], nous avons conçu une attaque nouvelle permettant d'attaquer le système (i) en temps polynomial et ce quelque soit le genre de la courbe considéré. Nous donnerons quelques détails sur cette attaque en § 3.3.2.

Pour finir, le cas (ii) que l'on peut voir comme une généralisation de la proposition historique de McEliece, résiste encore à toutes les attaques connues. Ce sujet a d'ailleurs été l'objet d'une part des travaux de thèse d'Élise Barelli [19].

2.4.2 Sous-codes sur un sous-corps et opérateur de Cartier

Les sous-codes sur un sous-corps de codes géométriques étant évoqués dans le paragraphe précédent, terminons ce chapitre en rappelant quelques éléments sur ces codes qui somme toute ont été peu étudiés dans la littérature. Essentiellement, un résultat analogue au Théorème 2.2.9 a été démontré par Katsman et Tsfasman [90] et indépendemment par Wirtz [159]. Essentiellement, ils prouvent le résultats suivants. Le premier peut être vu comme une généralisation aux codes géométriques du théorème 2.2.9.

Théorème 2.4.1 ([159, Theorem 2])**.** *Soit $\mathscr{X}$ une courbe de genre g définie sur $\mathbf{F}_{q^m}$, $\mathscr{P}$ un ensemble de points rationnels et G, G_1 deux diviseurs positifs tels que $\deg G_1 > 2g-2$ et $G \geqslant qG_1$. Soit G_U le diviseur réduit défini comme la somme des places telles que $v_P(G) \equiv q-1 \mod q$. Alors*

$$\mathcal{C}_\Omega(\mathscr{X}, \mathscr{P}, G) \cap \mathbf{F}_q^n = \mathcal{C}_\Omega(\mathscr{X}, \mathscr{P}, G + G_U) \cap \mathbf{F}_q^n.$$

Le second du à Katsman et Tsfasman ne fournit pas d'égalité entre des codes mais montre que, sous certaines conditions, les sous-codes sur un sous-corps de codes géométriques ont une dimension strictement supérieure à la borne générique (2.2). Une version sensiblement plus générale de leur résultat figure dans dans le livre de Stichtenoth [139]. Cette inégalité se base sur un résultat de [138].

Théorème 2.4.2 ([138, Theorem 4])**.** *Soit $\mathscr{X}$ une courbe sur $\mathbf{F}_{q^m}$ de genre g. Soient $\mathscr{P}$ un ensemble de points rationnels et G, G_1 des diviseurs tels que $G \geqslant qG_1$. Alors*

$$\dim \mathcal{C}_\Omega(\mathscr{X}, \mathscr{P}, G) \cap \mathbf{F}_q^n \geqslant \begin{cases} n-1-m(h^0(G)-h^0(G_1)) & \text{si} \quad G \geqslant 0 \\ n-m(h^0(G)-h^0(G_1)) & \text{sinon.} \end{cases}$$

Dans [43], je propose une construction alternative de codes à partir de courbes et définis sur un sous-corps du corps de définition de la courbe. Cette construction est basée sur l'opérateur de Cartier : un opérateur sur les formes différentielles rationnelles qui a pour noyau les différentielles exactes et pour points fixes les différentielles logarithmiques. On le note

$$\mathbf{Car} : \Omega_{\mathbf{F}_{q^m}(\mathscr{X})/\mathbf{F}_{q^m}} \to \Omega_{\mathbf{F}_{q^m}(\mathscr{X})/\mathbf{F}_{q^m}}.$$

L'idée est qu'en un point rationnel P, le résidu d'une forme différentielle logarithmique $\frac{dt}{t}$ est dans le sous-corps premier $\mathbf{F}_p$ et n'est autre que la classe modulo p de la valuation de t en P. Aussi, le code obtenu en se restreignant aux résidus de différentielles logarithmiques est inclus dans le sous-code sur un sous-corps d'un code géométrique.

Par ailleurs, on peut être intéressé par des codes dont le corps de base n'est pas un corps premier. Le cas échéant on considère des formes différentielles fixées par un certain itéré de l'opérateur de Cartier. Plus précisément, si on travaille sur un corps $\mathbf{F}_{q^m}$ où $q = p^s$ avec p premier, on définit

$$\mathbf{Car}_q : \begin{cases} \Omega_{\mathbf{F}_{q^m}(\mathscr{X})/\mathbf{F}_{q^m}} & \longrightarrow & \Omega_{\mathbf{F}_{q^m}(\mathscr{X})/\mathbf{F}_{q^m}} \\ \omega & \longmapsto & \underbrace{\mathbf{Car} \circ \cdots \circ \mathbf{Car}}_{s \text{ fois}}(\omega) \end{cases}$$

L'indice 'q' signifie que les formes différentielles invariantes par $\mathbf{Car}_q$ ont leur résidus en les places rationnelles à valeurs dans $\mathbf{F}_q$.

Définition 2.4.3. Soit $\mathscr{X}$ une courbe sur $\mathbf{F}_{q^m}$, soient $\mathscr{P}$ un ensemble ordonné de points et G un diviseur sur $\mathscr{X}$, on définit le code $\mathrm{Car}_q(\mathscr{X}, \mathscr{P}, G)$ par

$$\mathrm{Car}_q(\mathscr{X}, \mathscr{P}, G) \stackrel{\text{def}}{=} \left\{ (\mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_n}(\omega)) \mid \omega \in \Omega(G - D_{\mathscr{P}})^{\mathbf{Car}_q} \right\},$$

où $D_{\mathscr{P}} \stackrel{\text{def}}{=} \sum_{P \in \mathscr{P}} P$, $\mathrm{res}_{P_i}(\cdot)$ désigne le résidu en P_i et $\Omega(G - D_{\mathscr{P}})^{\mathbf{Car}}$ désigne l'ensemble des formes différentielles fixes par l'opérateur $\mathbf{Car}_q$.

On démontre aisément que

$$\mathrm{Car}_q(\mathscr{X}, \mathscr{P}, G) \subseteq \mathcal{C}_\Omega(\mathscr{X}, \mathscr{P}, G) \cap \mathbf{F}_q^n.$$

Il y a de plus égalité dès lors qu'il existe un diviseur G_1 tel que $G \geqslant qG_1$ et $\deg G_1 > 2g - 2$. En effet, d'après [43, Theorem 5.1] la codimension de $\mathrm{Car}_q(\mathscr{X}, \mathscr{P}, G)$ dans $\mathcal{C}_\Omega(\mathscr{X}, \mathscr{P}, G) \cap \mathbf{F}_q^n$ est majorée par $mh^1(G_1)$ où m désigne le degré d'extension $\mathbf{F}_{q^m}/\mathbf{F}_q$. Pour une courbe de genre nul, on peut montrer que l'inclusion est toujours une égalité. En ce sens, les codes de Cartier sont une autre généralisation des codes de Goppa classiques sensiblement différente des sous-codes sur un sous-corps de codes géométriques. Cette généralisation est quelque part plus naturelle dans la mesure où le principal intérêt des codes de Goppa est le Théorème 2.2.9 qui, dans le cas binaire donne une minoration de la distance minimale deux fois plus élevée que celle d'un code alternant de même dimension. Un tel résultat s'étend au sous-code sur un sous-corps de codes géométriques, comme l'a montré Wirtz (Théorème 2.4.1) mais sous certaines conditions de degré dont on peut s'affranchir en utilisant les codes de Cartier comme ne atteste le résultat ci-dessous.

Théorème 2.4.4 ([43, Theorem 4.4])**.** *Soit $\mathscr{X}$ une courbe de genre g sur $\mathbf{F}_{q^m}$. Soient $\mathscr{P}$ un ensemble de points rationnels de $\mathscr{X}$ et G un diviseur de $\mathscr{X}$. Soit G_U le diviseur réduit obtenu comme la somme des places telles que $v_P(G) \geqslant 0$ et $v_P(G) \equiv -1 \mod q$. Alors,*

$$\mathrm{Car}_q(\mathscr{X}, \mathscr{P}, G) = \mathrm{Car}_q(\mathscr{X}, \mathscr{P}, G + G_U).$$

Enfin, l'utilisation de l'opérateur de Cartier permet une analyse plus fine de la dimension de ces codes, même dans le cas où le code de Cartier et le sous-code sur un sous corps coïncident.

Théorème 2.4.5 ([43, Theorem 6.3 & Corollary 6.5]). *Soit $\mathscr{X}$ une courbe de genre q sur $\mathbf{F}_{q^m}$. Soient $\mathscr{P}$ un ensemble de points rationnels de $\mathscr{X}$ et G un diviseur de la forme $G = qG_0 - G_-$ où G_0, G_- sont deux diviseurs positifs à supports disjoints. Soit s le nombre de places supportant G_-, alors*

$$\dim \mathrm{Car}_q(\mathscr{X}, \mathscr{P}, G) \geqslant n - 1 + s - m(q-1)\deg G_0 - h^1(G);$$
$$\dim \mathcal{C}_\Omega(\mathscr{X}, \mathscr{P}, G) \geqslant n - 1 + s - m(q-1)\deg G_0.$$

En comparaison, le théorème 2.4.2 donne pour le sous-code sur un sous-corps une minoration en

$$\dim \mathcal{C}_\Omega(\mathscr{X}, \mathscr{P}, G) \geqslant n - m(q-1)\deg G_0$$

qui est donc moins bonne dès lors que $s > 1$. Même si ce résultat ne concerne pas directement les codes de Cartier il est obtenu grâce à une comparaison fine entre ces codes et les sous-codes sur un sous-corps de codes différentiels.

Présentation chronologique de l'histoire du chiffrement à la McEliece en métrique de Hamming

Légende

- Les attaques figurent en rouge.
- Les propositions en noir. À côté des proposition figure
  - le symbole [A] si elle a été totalement attaquée ;
  - le symbole [PA] si elle a été partiellement attaquée.

1978 — Berlekamp, McEliece et Van Tilborg [25] prouvent que le problème du décodage borné est NP–complet (théorème 2.1.1).
— McEliece [108] propose un schéma de chiffrement à base de codes. Propose de l'instancier avec des codes de Goppa binaires.

1986 Niederreiter [115] propose une version duale du schéma de McEliece et donne un exemple d'instanciation basé sur les codes GRS. [A].

1992 Sidelnikov et Shestakov [134] proposent une attaque polynomiale sur les codes GRS.

1994 Sidelnikov [133] propose l'utilisation des codes de Reed–Muller binaires. [A]

1996 Janwa et Moreno [87] proposent
— les codes géométriques [A] ;
— leurs sous–codes sur un sous–corps.

2005 — Gaborit [72] propose d'utiliser des codes quasi–cycliques pour réduire la taille de la clé publique. Il suggère une instanciation à base de sous–codes de codes BCH binaires. [A]
— Berger et Loidreau [24] proposent d'utiliser des sous-codes de petite codimension de codes GRS. [A]

2007 Minder et Shokrollahi [111] proposent une attaque de complexité sous–exponentielle sur les codes de Reed–Muller.

2008 Faure et Minder [69] proposent une attaque sur les codes géométriques provenant de courbes hyperelliptiques de petit genre (essentiellement, $g \leqslant 2$).

2009 Berger, Cayrel, Gaborit, Otmani [23] proposent les codes alternants quasi–cycliques. [PA]

2010 — Berstein, Lange, Peters [27] proposent des codes de Goppa q–aires « sauvages ». [PA]
— Deux attaques sur des codes quasi–cycliques :
  — Otmani, Tillich et Dallot [117] ;
  — Faugère, Otmani, Perret et Tillich [67].
— Wieschebrink [158] propose une attaque de complexité polynomiale sur le schéma de Berger Loidreau (sous–codes de codes GRS) à l'aide du produit $\star$.

2011 Faugère, Gautier–Umaña, Otmani, Perret, Tillich [65] proposent un distingueur de complexité polynomiale pour les codes alternants de haut rendement.

2012 Misoczki, Tillich, Sendrier, Barreto [113] proposent les codes MDPC et MDPC quasi–cycliques.

2014 — Couvreur, Márquez–Corbella et Pellikaan [51] proposent une attaque polynomiale sur les codes géométriques à partir de courbes de genre quelconque.
— Couvreur, Otmani, Tillich [53] proposent une attaque polynomiale sur les codes de Goppa q–aires avec $m = 2$.
— Faugère, Perret, de Portzamparc [68] proposent une attaque alternative sur certains codes de Goppa vérifiant $m = 2$ ou 3 et définis sur des corps non premiers.

Novembre 2017 Démarrage de l'appel du NIST pour les schémas cryptographiques post quantiques.

Remarque 2.4.6. La présentation chronologique qui précède n'est évidemment pas exhaustive. Je me suis contenté de présenter quelques dates qui, à mon sens représentent des ≪ points forts ≫ de l'histoire du chiffrement de McEliece. À noter également que je me suis concentré sur les propositions en métrique de Hamming. L'utilisation de la métrique rang est une autre histoire, tout aussi riche, que je n'aborde pas dans ce document.

Chapitre 3

Produits de codes et application à la cryptanalyse

La notion de *produit* $\star$ de code codes, parfois aussi appelé *produit de Schur* est une notion d'apparence élémentaire dont la diversité des applications est à la fois remarquable et déconcertante. On voit apparaître cette opération dans des travaux de Pellikaan sur le décodage [119]. Elle apparaît également dans des problèmes de construction de réseaux euclidiens, dans des protocoles de transfert inconscient et dans le domaine du calcul multiparti. Je renvoie le lecteur à [121] pour plus de détails sur ces différentes applications. Enfin, ce produit $\star$ est une opération fondamentale en cryptanalyse, il s'avère être un outil d'une remarquable efficacité pour distinguer des codes algébriques de codes aléatoires et pour retrouver la structure de tels codes. Notons que l'introduction de cette opération pour analyser la structure de codes algébriques ou géométrique est très naturelle. Rappelons tout d'abord que le produit $\star$ de vecteurs de $\mathbf{F}_q^n$ n'est autre que le produit coordonnées par coordonnées :

$$(a_1, \ldots, a_n) \star (b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n).$$

Cette opération n'est rien d'autre que la loi de multiplication de l'anneau produit $\mathbf{F}_q^n$. Or, les codes que nous considérons sont des codes d'évaluation, il sont donc l'image d'une application de la forme

$$\mathrm{ev} : \left\{ \begin{array}{ccc} V & \longrightarrow & \mathbf{F}_q^n \\ f & \longmapsto & (\varphi_1(f), \ldots, \varphi_n(f)) \end{array} \right. ,$$

où V est un espace de dimension finie de fonctions contenu dans une $\mathbf{F}_q$–algèbre A, et $\varphi_1, \ldots, \varphi_n$ sont des formes linéaires *d'évaluation* sur A, i.e. des morphismes d'**algèbre** $A \longrightarrow \mathbf{F}_q$. Ainsi, ev est un morphisme d'anneau de A dans $\mathbf{F}_q^n$ muni du produit $\star$.

Un code d'évaluation porte de manière naturelle la structure d'espace vectoriel de V qui provient de celle de A, l'introduction du produit $\star$ permet d'importer dans le monde des codes la structure multiplicative dont est naturellement munie l'algèbre A.

3.1 Le produit $\star$ de codes

Étant donnés deux codes $\mathcal{A}$ et $\mathcal{B} \subseteq \mathbf{F}_q^n$, le produit $\star$ de $\mathcal{A}$ et $\mathcal{B}$ est défini par

$$\mathcal{A} \star \mathcal{B} \stackrel{\text{def}}{=} \langle \boldsymbol{a} \star \boldsymbol{b} \mid \boldsymbol{a} \in \mathcal{A}, \boldsymbol{b} \in \mathcal{B} \rangle.$$

Insistons bien sur ce point, il s'agit d'un code **linéaire**, c'est donc l'espace vectoriel engendré par les produits $\boldsymbol{a} \star \boldsymbol{b}$ et pas seulement l'ensemble de ces produits.

Une fort intéressante application de cette opération pour la cryptanalyse de codes algébriques, vient de ce que cette opération d'apparence élémentaire permet souvent de distinguer des codes d'évaluation de codes aléatoires. En effet, étant donnés deux codes, on a

$$\dim \mathcal{A} \star \mathcal{B} \leqslant \min \left\{ n,\ \dim \mathcal{A} \cdot \dim \mathcal{B} - \binom{\dim \mathcal{A} \cap \mathcal{B}}{2} \right\}.$$

En particulier, dans le cas $\mathcal{A} = \mathcal{B}$, on note $\mathcal{A}^2 \stackrel{\text{def}}{=} \mathcal{A} \star \mathcal{A}$ et

$$\dim \mathcal{A}^2 \leqslant \min \left\{ n,\ \binom{\dim \mathcal{A} + 1}{2} \right\}. \tag{3.1}$$

Il est prouvé dans [36] que la borne supérieure (3.1) est atteinte dans le cas typique :

Théorème 3.1.1 (Cascudo, Cramer, Mirandola, Zémor 2015)**.** *Il existe des constantes $c, \tilde{c} \in \mathbf{R}_+$ dépendant de q telles que si $n : \mathbb{N} \to \mathbb{N}$ vérifie*

$$\forall k \in \mathbb{N}, \quad , k \leqslant n(k) \leqslant c \cdot \binom{k+1}{2},$$

alors, pour k suffisamment grand,

$$\mathbb{P}(\mathcal{C}^2 = \mathbf{F}_q^n) \geqslant 1 - 2^{\tilde{c}k},$$

où $\mathcal{C}$ désigne une variable aléatoire de loi uniforme à valeur dans l'ensemble des codes de dimension k dans $\mathbf{F}_q^n$

En substance ce théorème affirme que le carré d'un code aléatoire de dimension k tel que $n \leqslant \binom{k+1}{2}$ est égal à $\mathbf{F}_q^n$ avec une probabilité très proche de 1. Par ailleurs, un argument de poinçonnage permet de déduire des résultats de [36] le fait suivant : si $\binom{k+1}{2} \leqslant n$ alors pour tout entier $\ell > 0$

$$\mathbf{P}\left(\dim \mathcal{C}^2 \leqslant \binom{k+1}{2} - \ell \right) = O(q^{-\ell}).$$

3.2 Distinguer les codes algébriques et géométriques de codes aléatoires

3.2.1 Motivation, preuves de sécurité

La sécurité sémantique d'un schéma de chiffrement à la McEliece se démontre selon le principe suivant. On fait l'hypothèse qu'une variable aléatoire uniforme à valeurs dans la famille $\mathcal{F}$ est calculatoirement indistinguable d'une variable aléatoire uniforme à valeurs dans l'ensemble des codes $[n, k]$. Autrement dit, on suppose qu'il n'existe pas d'algorithme de complexité polynomiale décidant si un code est dans $\mathcal{F}$ avec une probabilité de succès significativement supérieure à $1/2$. Sous cette hypothèse, on peut montrer qu'attaquer un tel système est au moins aussi difficile que de résoudre le problème de décodage borné, qui rappelons le est NP–complet (voir Théorème 2.1.1).

Ainsi, la sécurité repose essentiellement sur cette hypothèse d'instinguabilité.

3.2.2 Rappel, codes raccourcis

Rappelons que l'on appelle *raccourci* d'un code $\mathcal{C} \subset \mathbf{F}_q^n$ sur un ensemble $\mathcal{I} \subseteq \{1, \ldots, n\}$, le code

$$\mathcal{S}_{\mathcal{I}}(\mathcal{C}) \stackrel{\text{def}}{=} \{ \boldsymbol{c} \in \mathcal{C} \mid \forall i \in \mathcal{I},\ c_i = 0 \}.$$

Remarque 3.2.1. La définition qui précède diffère sensiblement de celle que l'on trouve dans la littérature. En effet, le code ainsi décrit admet un certain nombre de coordonnées toujours nulles, il est habituel dans la littérature de les supprimer et d'en déduire un code de longueur $n - |\mathcal{I}|$. J'ai préféré conserver ces positions nulles dans la définition car, on aura parfois à faire des produits $\star$ entre un code raccourci et un code qui ne l'est pas, or le produit $\star$ n'est bien défini que pour deux codes de même longueur.

Notons que le Théorème 3.1.1 admet le corollaire suivant.

Corollaire 3.2.2. *Soit $\mathcal{C} \subseteq \mathbf{F}_q^n$ une variable aléatoire de loi uniforme à valeurs dans l'ensemble des codes $[n, k]$. Soit $\mathcal{I} \subseteq \{1, \dots, n\}$. Alors l'événement*

$$\dim \mathcal{S}_{\mathcal{I}}(\mathcal{C})^2 = \min\left\{n - |\mathcal{I}|, \binom{\dim \mathcal{S}_{\mathcal{I}}(\mathcal{C}) + 1}{2}\right\},$$

a une probabilité qui tend vers 1 quand k tend vers l'infini.

3.2.3 Le distingueur $\mathcal{C} \mapsto \mathcal{C}^2$

Le comportement des codes vis-à-vis de l'opération $\mathcal{C} \mapsto \mathcal{C}^2$ permet de distinguer un certain nombre de codes algébriques et géométriques de codes aléatoires. Si l'existence d'un tel distingueur rend impossible toute preuve de sécurité, elle ne fournit pas une attaque en l'état. Toutefois, dans la quasi-totalité des situations pratiques où le produit $\star$ nous a permis de distinguer la famille des clés publiques de codes aléatoires, nous sommes parvenus à construire une attaque efficace produisant les éléments secrets nécessaires au déchiffrement.

Aussi, il est fondamental lorsque l'on propose une famille de codes pour la cryptographie de vérifier que les codes considérés ont le même comportement que des codes aléatoires en respect au produit $\star$. On attend donc que pour presque tout code $\mathcal{C}$ de cette famille et presque toute partie $\mathcal{I}$ de $\{1, \dots, n\}$, les dimensions de $\mathcal{C}^2, (\mathcal{C}^\perp)^2, \mathcal{S}_{\mathcal{I}}(\mathcal{C})^2, \mathcal{S}_{\mathcal{I}}\left(\mathcal{C}^\perp\right)^2$ soient les mêmes que celles de codes aléatoires de même paramètres. Notons que l'on ne peut pas effectuer en temps polynomial un tel test qui nécessiterait d'énumérer toutes les parties de $\{1, \dots, n\}$. On peut toutefois calculer la dimension de $\mathcal{S}_{\mathcal{I}}(\mathcal{C})$ pour un certain nombre d'ensembles $\mathcal{I}$ de cardinal fixé tirés au hasard. Une série de manipulations permettant de tester la distinguabilité d'un code est suggérée en § 3.3.2.

3.2.4 Codes de Reed–Solomon généralisés

Contrairement aux codes aléatoires dont la dimension du carré atteint la valeur $\min\left(n, \binom{k+1}{2}\right)$, les codes de Reed–Solomon généralisés, tout comme les codes géométriques admettent des comportements très différents vis-à-vis de l'opération $\mathcal{C} \mapsto \mathcal{C}^2$. En effet, on vérifie aisément que

$$\mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y})^2 = \mathbf{GRS}_{2k-1}(\boldsymbol{x}, \boldsymbol{y} \star \boldsymbol{y}).$$

Et plus généralement, on a le résultat suivant.

Proposition 3.2.3. *Pour tous $u, v \leqslant n$, tout support $\boldsymbol{x} \in \mathbf{F}_q^n$ et tout couple de multiplieurs $\boldsymbol{y}_1, \boldsymbol{y}_2 \in (\mathbf{F}_q^\times)^n$, on a*

$$\mathbf{GRS}_u(\boldsymbol{x}, \boldsymbol{y}_1) \star \mathbf{GRS}_v(\boldsymbol{x}, \boldsymbol{y}_2) = \mathbf{GRS}_{u+v}(\boldsymbol{x}, \boldsymbol{y}_1 \star \boldsymbol{y}_2).$$

Autrement dit, pour les codes de Reed–Solomon généralisés, $\dim \mathcal{C}^2$ est linéaire en $\dim \mathcal{C}$ alors qu'elle est quadratique pour un code aléatoire. Cette observation nous fournit un distingueur très simple pour les codes de Reed–Solomon généralisés.

À noter que tous les codes GRS sont ainsi distinguables de codes aléatoires. En effet, pour les codes de dimension $k \leqslant n/2$, on aura $\dim \mathcal{C}^2 = 2 \dim \mathcal{C} - 1 < \min\left(n, \binom{k+1}{n}\right)$. Si maintenant $k > n/2$, alors, $\mathcal{C}^2 = \mathbf{F}_q^n$ pour un GRS comme pour un code aléatoire. Mais dans ce cas, on peut considérer le code dual $\mathcal{C}^\perp$ qui est également un code GRS et dont le carré sera de dimension strictement plus petite que celle du carré d'un code aléatoire de même longueur et dimension.

3.2.5 Codes alternants, codes de Goppa

En l'état, l'opération $\mathcal{C} \mapsto \mathcal{C}^2$ ne permet pas de distinguer un code alternant d'un code aléatoire sauf dans les cas suivants :

(i) Si le code est de rendement proche de 1, alors son dual a un carré de dimension sensiblement plus petite que celle d'un code aléatoire ; Ce distingueur a été identifié paru Faugère, Gautier, Otmani, Perret et Tillich dans [65]. Il a ensuite été reformulé en termes de produit $\star$ dans [105]. Dans [65], il est prouvé que le rendement critique au delà duquel les codes alternants sont distinguables de codes aléatoires est asymptotiquement équivalent à

$$R_{\text{crit}} = 1 - \sqrt{\frac{2m \log q}{q^m \log m}}(1 + \circ(1)).$$

À noter que ce distingueur n'a à l'heure actuelle pas donné lieu à une attaque : on ne sait pas tirer partie de ce distingueur pour retrouver les couple $(\boldsymbol{x}, \boldsymbol{y})$ tel que notre code soit égal à $\mathcal{A}_{r,q}(\boldsymbol{x}, \boldsymbol{y})$.

(ii) Pour les codes de Goppa q-aires de degré d'extension 2 et de rendement petit.

Le cas (ii) il a donné lieu à l'attaque [54, 55] dont je reparlerai un peu plus loin en § 3.3.2. Il repose sur le fait que la dimension des codes de Goppa dans le cas $m = 2$ qui est sensiblement supérieure à l'estimation générale donnée dans (2.3) et (2.4) comme expliqué dans l'énoncé suivant qui est une conséquence de [53, Theorem 1].

Théorème 3.2.4. *Soient $\boldsymbol{x} \in \mathbf{F}_{q^2}^n$ un support et $g \in \mathbf{F}_{q^2}[X]$ un polynôme sans racines dans $\mathbf{F}_{q^2}$ et de degré t, alors*

$$\mathcal{G}_q(\boldsymbol{x}, g^q) = \mathcal{G}_q\left(\boldsymbol{x}, g^{q+1}\right).$$

De plus, un tel code a pour paramètres

$$[n, \geqslant n - 2t(q+1) + t(t-2), \geqslant t(q+1) + 1]_q.$$

Ce gain de dimension permet de distinguer certains raccourcis de tels codes de Goppa de codes aléatoires. Plus précisément :

Théorème 3.2.5 ([55, Theorem 15])**.** *Soit $\mathcal{C} = \mathcal{G}_q\left(\boldsymbol{x}, g^{q-1}\right)$ où g est de degré $t < q$ et sans facteur carré. Si l'inégalité suivante est vérifiée*

$$\binom{t(t+2)+1}{2} > 2t(q+1) - 2,$$

alors il existe un intervalle non vide d'entiers $\{a_-, \ldots, a_+\} \subseteq \{1, \ldots, n\}$ tel que pour tout $\mathcal{I} \subseteq \{1, \ldots, n\}$ tel que $\sharp\mathcal{I} \in \{a_-, \ldots, a_+\}$, la dimension de $\mathcal{S}_{\mathcal{I}}(\mathcal{C})^2$ est strictement inférieure à celle de presque tout code aléatoire de mêmes longueur et dimension (voir la valeur donnée dans le Corollaire 3.2.2). De plus,

1. *$a_- = n - 2t(q+1)$;*
2. *a_+ est le plus grand entier tel que*

$$\binom{n - a_+ + t(t-2q)+1}{2} > 3(n - a_+) - 4t(q+1) - 2.$$

3.2.6 Codes géométriques

De manière très similaire aux codes de Reed–Solomon, les codes géométriques sont aisément distinguables de codes aléatoires. Le comportement de leur carré pour le produit $\star$ se déduit directement d'un résultat dû à Mumford.

Théorème 3.2.6 (Mumford, [114, Theorem 6]). *Soit $\mathscr{X}$ une courbe lisse de genre g. Soient A, B deux diviseurs sur $\mathscr{X}$ tels que* $\deg A \geqslant 2g$ *et* $\deg B \geqslant 2g+1$. *Alors*

$$L(A) \cdot L(B) \stackrel{def}{=} \langle fg \mid f \in L(A),\ g \in L(G) \rangle = L(A+B).$$

Notons que l'inclusion

$$L(A) \cdot L(B) \subseteq L(A+B)$$

est vraie pour tout couple de diviseurs (A, B). Seule l'inclusion réciproque est réellement délicate à prouver. Ensuite, il est important de signaler que les conditions sur le degré des diviseurs sont des conditions nécessaires mais en aucun cas suffisantes.

De façon immédiate, on déduit du Théorème 3.2.6 que si $\deg A \geqslant 2g$ et $\deg B \geqslant 2g+1$, alors

$$\mathcal{C}_L(\mathscr{X}, \mathscr{P}, A) \star \mathcal{C}_L(\mathscr{X}, \mathscr{P}, B) = \mathcal{C}_L(\mathscr{X}, \mathscr{P}, A+B).$$

Ici encore, l'inclusion vers la droite est vérifiée pour tout couple de diviseurs, sans condition de degré. On en déduit en particulier qu'un code $\mathcal{C}_L(\mathscr{X}, \mathscr{P}, G)$ associé à un diviseur G tel que $\deg G > 2g$ est distinguable d'un code aléatoire dès lors que

$$2\deg G + 1 - g < \min\left\{n, \binom{\deg G + 2 - g}{2}\right\}.$$

Un calcul rapide permet de vérifier que si $\deg G \geqslant 2g+1$, alors on a toujours $2\deg G + 1 - g < \binom{\deg G + 2 - g}{2}$, de fait, un tel code est distinguable d'un code aléatoire si

$$2g + 1 \leqslant \deg G < \frac{n+g-1}{2}.$$

Par dualité, il le sera également si

$$2g + 1 \leqslant 2g - 2 - \deg G + n \leqslant \frac{n+g-1}{2}.$$

En définitive, tout code associé à un diviseur vérifiant

$$2g + 1 \leqslant \deg G \leqslant n - 3$$

est distinguable d'un code aléatoire. Cela correspond à des codes dont la dimension vérifie

$$g + 2 \leqslant k \leqslant n - (g+2).$$

Insistons encore une fois sur le fait qu'il s'agit d'une condition suffisante qui n'est en aucun cas nécessaire.

3.3 Cryptanalyses basées sur le distingueur par carré

Dans cette section, nous présentons quelques résultats de cryptanalyse obtenus dans les articles [48, 56, 55, 52, 49].

3.3.1 Attaques de quelques schémas basés sur des codes GRS

Publications associées : [48, 56, 49].

Présentation de quelques schémas basés sur des codes GRS

La critique récurrente relative à la taille des clés dans le schéma de McEliece a motivé la recherche de propositions alternatives en vue de réduire cette taille de clés. Pour ce faire, une tentation naturelle est d'aller chercher des codes pour lesquels on sait corriger un plus grand nombre d'erreurs que les codes de Goppa. C'est par exemple le cas des codes GRS, mais ces derniers ont fait l'objet d'une attaque en temps polynomial présentée par Sidelnikov et Shestakov en 1992 [134]. Notons d'ailleurs que les résultats du paragraphe précédent montrent que de tels codes sont aisément distinguables de codes aléatoires via l'opération $\mathcal{C} \mapsto \mathcal{C}^2$. Suite à cela des variantes du schéma basées sur des codes « proches » de codes GRS ont été proposées :

- Dans [24], Berger et Loidreau proposent de considérer des sous-codes aléatoires de codes GRS de petite codimension.
- Dans [157], Wieschebrink, propose de prendre un code admettant une matrice génératrice construite à partir d'une matrice génératrice de code GRS à laquelle on a ajouté des colonnes aléatoires en des positions aléatoires.
- Dans [14], les auteurs proposent comme clé publique une matrice $\boldsymbol{G}_{\text{pub}} = \boldsymbol{G}_{\text{sec}}(\boldsymbol{P} + \boldsymbol{T})^{-1}$ où $\boldsymbol{G}_{\text{sec}}$ est une matrice génératrice de code GRS, $\boldsymbol{P}$ est une matrice dont les lignes sont de poids « petit » et $\boldsymbol{T}$ est une matrice de « petit » rang. Les paramètres pratiques suggérés consistent à prendre $\boldsymbol{T}$ de rang 1 et $\boldsymbol{P}$ avec des lignes de poids 1 et 2.
- Dans [154, 155], Y. Wang propose un système nommé RLCE (Random Linear Code Encryption) consistant à prendre comme clé publique une matrice $\boldsymbol{G}$ obtenue comme suit. On part d'une matrice d'un code GRS, on sélectionne un certain nombre w de colonnes et on remplace chacune de ces colonnes C par deux colonnes $aC + bR$ et $cC + dR$ où R est une colonne aléatoire et $a, b, c, d \in \mathbf{F}_q$ vérifient $ad - bc \neq 0$.

Remarque 3.3.1. Pour les schémas décrits ci-dessus, la description de la clé secrète et de l'algorithme de déchiffrement nécessitent quelques détails supplémentaires que j'omets, je renvoie le lecteur aux références pour plus de détails.

Attaques

À ma connaissance, le premier à avoir utilisé le produit $\star$ pour la cryptanalyse est Wieschebrink qui utilise cette opération dans [158] pour attaquer la proposition de Berger et Loidreau [24]. Le principe est simple, si la clé publique est un code $\mathcal{C}$ de codimension ℓ dans un code $\mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y})$, alors avec une probabilité élevée, $\mathcal{C}^2$ sera égal à $\mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y})^2 = \mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y} \star \boldsymbol{y})$. Cette dernière affirmation est une heuristique que l'expérimentation pratique a rendu très convaincante. Si $2k - 1 < n$, alors le code $\mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y} \star \boldsymbol{y})$ n'est pas $\mathbf{F}_q^n$ tout entier et l'attaque de Sidelnikov Shestakov [134] permet de retrouver $\boldsymbol{x}$ et $\boldsymbol{y} \star \boldsymbol{y}$, en déduire $\boldsymbol{y}$ est relativement aisé (surtout en caractéristique paire !).

Dans le cas où $2k-1 \geqslant n$, c'est à dire dans le cas où le code GRS ambiant est de rendement supérieur à $1/2$, on peut se ramener au cas précédent en procédant à un raccourcissement en a positions avec a vérifiant

$$2(k-a) - 1 < n - a \quad \Longrightarrow \quad a \geqslant 2k - n.$$

Dans ce cas, pour tout $\mathcal{I} \subseteq \{1, \ldots, n\}$ tel que $|\mathcal{I}| = a$, alors

$$\mathcal{S}_{\mathcal{I}}(\mathcal{C}) \subseteq \mathcal{S}_{\mathcal{I}}(\mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y}))$$

et le raccourci d'un code GRS étant un code GRS on a

$$\dim \mathcal{S}_{\mathcal{I}}(\mathcal{C})^2 \leqslant 2(k-a) + 1$$

cette dernière propriété permet de distinguer $\mathcal{C}$ d'un code aléatoire.

Dans [48], nous avons attaqué différents schémas à la McEliece utilisant des codes construits à partir de codes GRS. Ces attaques reposent essentiellement sur le distingueur fourni par la fonction $\mathcal{C} \mapsto \mathcal{C}^2$. Par exemple, le système de Wieschebrink [157] dont la clé publique $\boldsymbol{G}_{\text{pub}}$ est une matrice $k \times n + \ell$

obtenue à partir d'une matrice génératrice $k \times n$ de code GRS dans laquelle on a introduit des colonnes aléatoires en des positions aléatoires. On observe que le code public $\mathcal{C}_{\text{pub}}$ de matrice génératrice $\boldsymbol{G}_{\text{pub}}$ vérifie la propriété avec une probabilité très proche de 1 :

$$\dim {\mathcal{C}_{\text{pub}}}^2 = \min\{n, 2k-1+\ell\}.$$

Dans le cas où $2k-1+\ell < n$, on peut alors identifier les colonnes aléatoires comme suit. Pour tout $i \in \{1, \ldots, n+\ell\}$, on considère le code $\mathcal{C}_i$, *poinçonné* en la position i, i.e. le code obtenu en supprimant la i–ème colonne d'une matrice génératrice de $\mathcal{C}_{\text{pub}}$. On vérifie alors que

$$\dim \mathcal{C}_i^2 = \begin{cases} 2k-1-(\ell-1) & \text{si la } i-\text{ème colonne est aléatoire;} \\ 2k-1-\ell & \text{sinon.} \end{cases}$$

Une fois les positions des colonnes aléatoires retrouvées le système est cassé. Ici encore, on parvient à s'affranchir de la condition $2k-1+\ell < n$ en procédant à un raccourcissement adéquat.

Des stratégies similaires quoique nettement plus techniques nous ont permis d'attaquer dans [56] le système BBCRS [14]. De même, une attaque du système RLCE [154, 155] basée sur des principes similaires est présentée dans [49].

3.3.2 Attaques par filtration

Si l'existence d'un distingueur rend caduque tout espoir de preuve de sécurité, une attaque ne s'en déduit pas toujours de manière immédiate. La conception d'une attaque à partir d'un distingueur peut être un travail relativement délicat. Rappelons d'ailleurs que les codes de Goppa de haut rendement sont distinguables de codes aléatoires mais qu'à l'heure actuelle aucune attaque sur de tels codes n'est connue.

Pour les codes d'évaluation, tels que les codes de Reed–Solomon, les codes géométriques et certains codes de Goppa (ceux dont le degré d'extension est égal à 2), nous avons développé un paradigme d'attaque reposant sur le produit $\star$ que nous avons appelé *attaque par filtration*. Elle repose sur le fait que la clé publique $\mathcal{C}_{\text{pub}}$ est un code appartenant à une famille de codes $\mathcal{F}$ et qui s'inscrit dans une filtration

$$\mathcal{C}_{\text{pub}} = \mathcal{C}_0 \supseteq \mathcal{C}_1 \supseteq \cdots \supseteq \mathcal{C}_i \supseteq \cdots$$

où les codes $\mathcal{C}_j$ sont des codes de la même famille et vérifiant des propriétés multiplicatives du type

$$\mathcal{C}_i \star \mathcal{C}_j \subseteq \mathcal{C}_{i+j}.$$

De telles filtrations existent naturellement lorsque les codes sont des codes d'évaluation de fonctions appartenant à une algèbre graduée comme par exemple une algèbre de polynômes.

De façon très schématique, le principe d'une attaque par filtration est, comme son nom l'indique de calculer des termes successifs d'une telle filtration jusqu'à obtenir un code « plus petit » sur lequel une attaque, par exemple basée sur une recherche exhaustive, sera aisée.

Le cas des codes GRS

L'exemple le plus simple de codes pour présenter les attaques par filtration reste les codes GRS. Si la structure d'un code GRS se retrouve aisément à partir d'une matrice génératrice comme l'ont montré Sidelnikov et Shestakov dans [134], l'attaque qui suit est d'un type totalement différent et se généralise naturellement à des familles de codes qui restent hors de d'atteinte d'une généralisation de l'attaque de Sidelnikov et Shestakov. L'attaque qui suit est présentée de manière plus détaillée dans [48, § 5]. Dans un premier temps, introduisons un objet qui nous sera utile dans ce qui suit.

Définition 3.3.2. Soient $\mathcal{A}, \mathcal{B} \subseteq \mathbf{F}_q^n$ deux codes. Le *conducteur de $\mathcal{A}$ dans $\mathcal{B}$* est le plus grand code $\mathcal{X}$ tel que $\mathcal{A} \star \mathcal{X} \subseteq \mathcal{B}$. Autrement dit

$$\mathbf{Cond}(\mathcal{A}, \mathcal{B}) \stackrel{\text{def}}{=} \{\boldsymbol{x} \in \mathbf{F}_q^n \mid \boldsymbol{x} \star \mathcal{A} \subseteq \mathcal{B}\}.$$

Notons que le calcul d'un conducteur se réduit à la résolution d'un système linéaire. On peut même donner une description explicite de ce code [52, Lemma 7]

$$\mathbf{Cond}(\mathcal{A}, \mathcal{B}) = (\mathcal{A} \star \mathcal{B}^{\perp})^{\perp}.$$

Lemme 3.3.3 ([48, Proposition 5] et [52, § VI.B.4])**.** *Le calcul du conducteur d'un code de longueur n à valeurs dans un autre peut s'effectuer de manière déterministe en $O(n^4)$ opérations. Un algorithme probabiliste permet d'effectuer ce calcul en $O(n^3)$ opérations.*

Remarque 3.3.4. Si la terminologie *conducteur* n'y est pas utilisée, on trouve une opération similaire dans les travaux de Khuri–Makdisi [91, 92] pour faire des calculs explicites sur des jacobiennes de courbes. Les considérations de complexité du lemme 3.3.3 figurent d'ailleurs dans [92].

Procédons maintenant à la description de l'attaque.

Terme 0 de la filtration Partons de la donnée d'un code $\mathcal{C}_0 = \mathcal{C}_{\text{pub}} \stackrel{\text{def}}{=} \mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y})$ pour lequel on suppose que $k < n/2$ (dans le cas contraire, il suffit de considérer le code dual). Ce code s'obtient par évaluation d'éléments de l'espace de polynômes

$$\mathbf{F}_q[X]_{<k} \stackrel{\text{def}}{=} \{f \in \mathbf{F}_q[X] \mid \deg f < k\}.$$

Terme 1 de la filtration La 2–transitivité du groupe affine sur la droite affine nous permet de faire l'hypothèse que $\boldsymbol{x}_1 = 0$ et $\boldsymbol{x}_2 = 1$. Considérons maintenant le code raccourci en la première coordonnée, i.e. le sous-code des vecteurs dont la première coordonnée est nulle :

$$\mathcal{C}_1 \stackrel{\text{def}}{=} \mathcal{S}_{\{1\}}(\mathcal{C}_{\text{pub}}).$$

Il correspond à l'évaluation de polynômes dans l'idéal engendré par X et plus précisément des polynômes appartenant à l'espace $X\mathbf{F}_q[X]_{<k-1}$. Ce code se calcule aisément par élimination Gaussienne.

Terme 2 de la filtration Le prochain terme que nous cherchons correspond à l'espace $X^2\mathbf{F}_q[X]_{<k-2}$, autrement dit les polynômes nuls en 0 avec multiplicité 2. On pourrait penser que la notion d'annulation avec multiplicité ne peut se lire sur le code et pourtant, le code que l'on recherche vérifie la propriété suivante :

$$\mathcal{C}_2 \star \mathcal{C}_0 = \mathcal{C}_1^2.$$

En effet, il suffit de vérifier que cette relation est vérifiée par les espaces de polynômes. Comme les codes $\mathcal{C}_0$ et $\mathcal{C}_1$ sont connus, on peut calculer $\mathcal{C}_2$ comme le conducteur de $\mathcal{C}_0$ dans $\mathcal{C}_1^2$:

$$\mathcal{C}_2 = \{\boldsymbol{c} \in \mathcal{C}_1 \mid \boldsymbol{x} \star \mathcal{C}_0 \subseteq \mathcal{C}_1^2\} = \mathbf{Cond}(\mathcal{C}_0, \mathcal{C}_1^2).$$

Et ensuite ? Le procédé qui précède permet de calculer l'intégralité de la filtration jusqu'à obtenir le code $\mathcal{C}_{k-1}$ de dimension 1 correspondant à l'évaluation des polynômes de la forme cX^{k-1} pour $c \in \mathbf{F}_q$. Autrement dit, on obtient la droite engendrée par $\boldsymbol{x}^{\star(k-1)} \star \boldsymbol{y}$.

Si l'on considère maintenant le code $\mathcal{C}_{k-2}$ et que l'on le raccourcit en la seconde position (on rappelle que $x_2 = 1$), on obtient un autre code de dimension 1 correspondant à l'évaluation de polynômes de la forme $cX^{k-2}(X-1)$, autrement dit le code obtenu est la droite engendrée par $\boldsymbol{x}^{\star(k-2)} \star (\boldsymbol{x} - \mathbf{1}) \star \boldsymbol{y}$, où $\mathbf{1} \stackrel{\text{def}}{=} (1, \ldots, 1)$.

La division coordonnées par coordonnées (en supprimant les coordonnées nulles) d'un vecteur de $\langle \boldsymbol{x}^{\star(k-2)} \star (\boldsymbol{x} - \mathbf{1}) \star \boldsymbol{y} \rangle$ par un vecteur de $\langle \boldsymbol{x}^{\star(k-1)} \star \boldsymbol{y} \rangle$, nous permet d'éliminer $\boldsymbol{y}$ et d'obtenir la droite engendrée par le vecteur $(\boldsymbol{x} - \mathbf{1}) \star \boldsymbol{x}^{\star(-1)}$ dont les coordonnées sont les évaluations de l'homographie $\boldsymbol{x} \mapsto \frac{x-1}{x}$. On déduit aisément de ce vecteur le vecteur $\boldsymbol{x}$ puis le calcul de $\boldsymbol{y}$ s'en déduit aisément.

Conclusion Cette attaque permet donc de retrouver la structure d'un code GRS à partir de la seule donnée d'une matrice génératrice. On peut montrer que la complexité de cette attaque est en $O(n^5)$ soit un coût plus conséquent que l'attaque de Sidelnikov et Shestakov dont la complexité est en $O(n^3)$. Toutefois, elle présente un intérêt fondamental : à la différence de l'attaque de Sidelnikov et Shestakov, notre attaque ne repose pas sur le calcul de mots de poids minimal. Or, si pour les codes GRS, le calcul de mots de poids minimal est élémentaire et se réduit à une simple élimination Gaussienne, la détermination de mots de poids minimal peut devenir bien plus complexe pour d'autres familles de codes.

Deux exemples permettent d'illustrer ce dernier point :

— Le schéma de Sidelnikov [133] prenant comme clé publiques des codes de Reed–Muller a été cassé par Minder et Shokrollahi [111] via une attaque « à la Sidelnikov Shestakov ». L'étape de calcul de mots de poids minimal rend la complexité d'une telle attaque sous-exponentielle. Plus tard, Chizhov et Borodin [38] produisent une attaque sur les codes de Reed–Muller basée sur le produit $\star$ qui, elle, est de complexité polynomiale.

— Les premières attaques sur les codes géométriques sont dûes à Minder [110] et Faure Minder [69]. Il s'agit là encore d'attaques « à la Sidelnikov Shestakov ». L'étape de calcul de mots de poids minimal est alors de complexité exponentielle en le genre de la courbe, la portée d'une telle attaque reste donc réduite au cas de code à partir de courbes de genre 1 et 2. L'attaque par filtration que nous avons produit avec Márquez–Corbella et Pellikaan [52] a une complexité polynomiale et indépendante du genre de la courbe.

Les codes de Goppa sauvages sur des extensions quadratiques

Publications associées : [53, 55].

L'attaque sur les codes de Goppa sauvages sur des extensions quadratiques repose tout d'abord sur un distingueur qui passe *in extremis*. Pour comprendre ce point, considérons tout d'abord un code alternant de degré d'extension 2. On se donne donc un support et un multiplieur $\boldsymbol{x}, \boldsymbol{y} \in \mathbf{F}_{q^2}^n$ et on considère le code $\mathcal{A}_{r,q}(\boldsymbol{x}, \boldsymbol{y})$. Ce code est contenu dans un code GRS de dimension $n-r$ et a une dimension $\geqslant n-2r$. Dans la situation typique la dimension du code est exactement $n-2r$. Pour avoir $n-2r>0$ la dimension du GRS ambiant est $n-r>n/2$ et donc le carré du GRS ambiant est égal à $\mathbf{F}_{q^2}^n$. En pratique, on observe que le carré d'un code alternant remplit également l'espace ambiant dès lors que sa dimension k vérifie $\binom{k+1}{2} \geqslant n$. Un tel code étant contenu dans un code GRS, on est tenté de le raccourcir, de manière à raccourcir le GRS ambiant, jusqu'à ce que le rendement du GRS ambiant devienne inférieur à $1/2$ et que son carré le rende distinguable d'un code aléatoire. Toutefois, si l'on raccourcit le GRS ambiant de a positions de manière à ce que $n-r-a<(n-a)/2$, il faut prendre $a \geqslant n-2r$ et donc, raccourcir ainsi notre code alternant donnera un code nul.

Le fait que les codes de Goppa soient distinguables repose sur le fait que ces codes ont en fait une dimension plus élevée que la dimension typique $n-2r$ du fait des Théorèmes 3.2.4 et 3.2.5.

Fort de ce distingueur, on peut ensuite procéder au calcul d'une filtration associée aux espaces de polynômes s'annulant en 0 avec des multiplicités croissantes.

$$\mathcal{C}_0 = \mathcal{G}_q(\boldsymbol{x}, g) \supseteq \mathcal{C}_1 \supseteq \mathcal{C}_2 \supseteq \cdots$$

Comme signalé en § 3.2.5, le distingueur ne s'applique qu'à des raccourcis de $\mathcal{C}_0 = \mathcal{C}_{\text{pub}}$. Ainsi, chaque terme de la filtration se calculera par « recollements successifs » : connaissant les termes $\mathcal{C}_0, \ldots, \mathcal{C}_{r-1}$ de la filtration, on calcule d'abord un certain nombre de raccourcis de $\mathcal{C}_r$ puis on en calcule la somme pour obtenir le code $\mathcal{C}_r$ recherché.

On calcule cette filtration jusqu'au terme $\mathcal{C}_{q+1}$. À ce stade, on remarque la chose suivante. Le code $\mathcal{C}_{\text{pub}}$ est un code de Goppa, donc à fortiori un code de la forme $\mathbf{GRS}_{n-r}(\boldsymbol{x}, \boldsymbol{z}) \cap \mathbf{F}_q^n$ qui correspond aux évaluations de l'espace $\mathbf{F}_q[X]_{<n-r}$. Le code $\mathcal{C}_{q+1}$ correspond aux évaluations des polynômes de l'espace $X^{q+1}\mathbf{F}_q[X]_{<n-r-(q+1)}$. Autrement dit, c'est le code

$$\left(\boldsymbol{x}^{\star(q+1)} \star \mathbf{GRS}_{n-r-(q+1)}(\boldsymbol{x}, \boldsymbol{z})\right) \cap \mathbf{F}_q^n.$$

On note ensuite que $\boldsymbol{x}^{\star(q+1)}$ a ses coordonnées dans $\mathbf{F}_q^n$ car $\boldsymbol{x}$ a ses coordonnées dans $\mathbf{F}_{q^2}$ et que l'application $x \mapsto x^{q+1}$ n'est autre que la norme de $\mathbf{F}_{q^2}/\mathbf{F}_q$. De fait, le conducteur $\mathbf{Cond}(\mathcal{C}_{q+1}, \mathcal{C}_{\text{pub}})$ contient de manière évidente le mot $\mathbf{1}$ mais également le mot $\boldsymbol{x}^{\star(-q-1)}$ ainsi que d'autres éléments que l'on sait expliciter (voir [55] pour plus de détails). Un travail relativement technique permet d'extraire $\boldsymbol{x}^{q+1}$ puis d'en déduire $\boldsymbol{x}$.

Cette attaque permet de calculer en moins d'une heure la clé secrète associée à une clé publique dont la sécurité était estimée à 128 bits dans [27].

Les codes géométriques

Publications associées : [51, 50, 52].

Les codes géométriques sont bien plus simples à distinguer de codes aléatoires que les codes alternants. Pour ces derniers on peut également monter une attaque par filtration. Partant de

$$\mathcal{C}_0 = \mathcal{C}_{\text{pub}} = \mathcal{C}_L(\mathscr{X}, \mathscr{P}, G)$$

et en notant P le premier élément de $\mathscr{P}$, on calcule le raccourci de notre code en cette première position :

$$\mathcal{C}_1 = \mathcal{S}_{\{1\}}(\mathcal{C}_0) = \mathcal{C}_L(\mathscr{X}, \mathscr{P}, G - P)$$

puis la filtration que l'on calculera ne sera rien d'autre que la suite des codes

$$\mathcal{C}_i \stackrel{\text{def}}{=} \mathcal{C}_L(\mathscr{X}, \mathscr{P}, G - iP).$$

De plus, lorsque l'on dispose de cette filtration, par des calculs de conducteurs on peut en déduire les codes $\mathcal{C}_L(\mathscr{X}, \mathscr{P} \setminus \{P\}, jP)$ car :

$$\mathcal{C}_L(\mathscr{X}, \mathscr{P} \setminus \{P\}, jP) = \mathbf{Cond}(\mathcal{C}_L(\mathscr{X}, \mathscr{P} \setminus \{P\}, G - jP), \mathcal{C}_L(\mathscr{X}, \mathscr{P} \setminus \{P\}, G))$$

dès lors que j et $\deg G - j$ sont assez grands.

Dans [55] nous détaillons une procédure pour calculer l'intégralité de ces deux filtrations. Il s'avère que la connaissance de telles filtrations fournit ce que l'on appelle dans la littérature des *error correcting arrays* ou encore *well behaving sequences* auxquels sont associés des algorithmes de décodage permettant de corriger de tels codes jusqu'à la moitié de leur distance construite sans avoir besoin d'une quelconque information sur la courbe $\mathscr{X}$.

Ainsi, la connaissance d'une telle filtration permet de déchiffrer les messages avec la même efficacité que le destinataire légitime. Nous avons de plus montré qu'une alternative « à la Berger Loidreau » consistant à prendre pour clé publique un sous-code aléatoire de petite codimension d'un code géométrique n'était pas sûre dans la mesure où l'on est capable, via des calculs de codes carrés et de conducteurs de retrouver le code géométrique ambiant puis de lui appliquer l'attaque par filtration décrite ci-dessus.

L'importance du distingueur

Terminons ce paragraphe sur les attaques par filtration en insistant sur un point. Ce type d'attaque n'est possible que si le code de départ (resp. l'un de ses raccourcis en a positions) a un carré de dimension strictement inférieure à $\min\left\{n, \binom{k+1}{2}\right\}$ (resp. à $\min\left\{n-a, \binom{k-a+1}{2}\right\}$), sans une telle propriété aucun calcul de filtration n'est possible. C'est la difficulté que nous avons rencontré pour attaquer le schéma DAGS abordé en § 3.4.

Tester le distingueur ou s'en prémunir

Terminons cette section en présentant une série de tests à appliquer à une famille de codes afin de vérifier l'existence ou non d'un distingueur par produit $\star$ sur cette famille. Considérons une famille $\mathcal{F}$ de codes de longueur n et de dimension k, si l'un des tests suivant échoue la famille est distinguable de codes aléatoires. Les tests consistent à se fixer deux entiers N, N' et vérifier les propriétés suivantes.

(1) Pour N éléments $\mathcal{C}$ tirés aléatoirement dans $\mathcal{F}$, la propriété suivante doit êtré vérifiée par tous sauf une proportion négligeable d'entre eux [1] :

$$\dim \mathcal{C}^2 = \min\left(n, \binom{k+1}{2}\right);$$

et

$$\dim \left(\mathcal{C}^\perp\right)^2 = \min\left(n, \binom{(n-k)+1}{2}\right);$$

(2) Pour tout $a < k$, tirer aléatoirement N éléments $\mathcal{C} \in \mathcal{F}$. Pour chacun de ces $\mathcal{C}$, tirer aléatoirement un ensemble $\mathcal{I} \subset \{1, \ldots, n\}$ tels que $|\mathcal{I}| = a$ et vérifier que la propriété suivante est vérifiée par tous les codes $\mathcal{C}$ sauf peut-être une proportion négligeable d'entre eux :

$$\dim \mathcal{S}_\mathcal{I}(\mathcal{C}) = \min\left(n - |I|, \binom{\dim \mathcal{S}_\mathcal{I}(\mathcal{C})}{2}\right);$$

et

$$\dim \mathcal{S}_\mathcal{I}\left(\mathcal{C}^\perp\right) = \min\left(n - |I|, \binom{\dim \mathcal{S}_\mathcal{I}\left(\mathcal{C}^\perp\right)}{2}\right).$$

Une famille de codes qui échoue aux tests ci-dessus est distinguable de code aléatoire et ne peut pas être proposée pour le schéma de McEliece.

3.4 Une cryptanalyse sans distingueur par code carré, le schéma DAGS

Publication associée : [20].

Pour terminer, présentons un travail de cryptanalyse d'un style sensiblement différent effectué en collaboration avec Élise Barelli. Dans cette attaque, le produit $\star$ reste omniprésent, mais les codes concernés sont indistinguables de codes aléatoires via l'opération $\mathcal{C} \mapsto \mathcal{C}^2$. Le schéma attaqué s'appelle DAGS [16] et a compté parmi les schémas soumis au NIST.

DAGS utilise comme clé publique des codes alternants de degré d'extension 2 et munis d'un groupe d'automorphisme non trivial. Le fait d'utiliser des codes alternants de petit degré d'extension et muni d'un grand groupe d'automorphisme permettait des tailles de clés publiques extrêmement offensives : de l'ordre de 10 kilo-octets pour 128 bits de sécurité.

Comme signalé précédemment, les codes publics, tout comme leurs raccourcis avaient des carrés qui se comportaient comme le carré de codes aléatoires muni du même groupe d'automorphisme. Ainsi, le procédé d'attaque par distingueur et filtration présenté précédemment ne peut s'appliquer directement.

3.4.1 Structure de la clé publique dans DAGS

Il s'agit d'un code $\mathcal{A}_{r,q}(\boldsymbol{x}, \boldsymbol{y})$ de degré d'extension 2 et muni d'un groupe de permutations isomorphe à $(\mathbb{Z}/2\mathbb{Z})^\gamma$. L'action de groupe vient de l'action d'un groupe de translations sur la droite affine qui laisse l'ensemble des coefficients du support $\boldsymbol{x}$ globalement invariant. Rappelons qu'en caractéristique 2 les translations sont involutives ce qui explique que le groupe soit de 2–torsion. Pour donner quelques ordres de grandeur, les paramètres proposés dans la soumission originale de DAGS sont présentés dans le tableau 3.1.

1. On attend que pour N essais la propriété soit vérifiée par au moins $N(1 - 2^{-\Omega(n)})$ d'entre eux.

Name	q	m	n	k	γ	Taille de clé	Sécurité estimée
DAGS_1	2^5	2	832	416	4	6,8 ko	128 bits
DAGS_3	2^6	2	1216	512	5	8,5 ko	192 bits
DAGS_5	2^6	2	2112	704	6	11,6 ko	256 bits

TABLE 3.1 – Paramètres initialement proposés dans DAGS.

3.4.2 Idées de l'attaque

L'attaque ne repose plus sur un calcul de filtration qui serait hors de portée faute de distingueur via l'application $\mathcal{C} \mapsto \mathcal{C}^2$. Le produit $\star$ va tout de même jouer un rôle central via le calcul de conducteurs. Rappelons qu'étant donnés deux codes $\mathcal{A}$ et $\mathcal{B}$, le *conducteur* de $\mathcal{A}$ dans $\mathcal{B}$ est le code

$$\mathbf{Cond}(\mathcal{A}, \mathcal{B}) \stackrel{\text{def}}{=} \left\{ \boldsymbol{x} \in \mathbf{F}_q^n \mid \boldsymbol{x} \star \mathcal{A} \subseteq \mathcal{B} \right\}.$$

Autrement dit, c'est le plus grand code $\mathcal{X}$ tel que $\mathcal{X} \star \mathcal{A} \subseteq \mathcal{B}$. Pour comprendre l'utilité d'un tel objet, commençons par un exemple très simple. Supposons que l'on connaisse les deux codes $\mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y})$ et $\mathbf{GRS}_{k-1}(\boldsymbol{x}, \boldsymbol{y})$, on peut alors montrer que

$$\mathbf{Cond}(\mathbf{GRS}_{k-1}(\boldsymbol{x}, \boldsymbol{y}), \mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y})) = \mathbf{RS}_2(\boldsymbol{x}).$$

Le point important ici est que le calcul de conducteur nous fournit un nouveau code qui ne dépend que de $\boldsymbol{x}$. Autrement dit, on s'est débarrassés de $\boldsymbol{y}$. Partant de ce code, déduire $\boldsymbol{x}$ est une tâche relativement élémentaire.

Cette idée élémentaire n'est pas directement adaptable au cas d'un code alternant $\mathcal{A}_{r,q}(\boldsymbol{x}, \boldsymbol{y})$ pour deux raisons. Déjà parce qu'on ne connaît que le code $\mathcal{A}_{r,q}(\boldsymbol{x}, \boldsymbol{y}) = \mathbf{GRS}_{n-r}(\boldsymbol{x}, \boldsymbol{y}^\perp)$ et pas le code $\mathcal{A}_{r+1,q}(\boldsymbol{x}, \boldsymbol{y}) = \mathbf{GRS}_{n-r-1}(\boldsymbol{x}, \boldsymbol{y}^\perp)$. Ensuite, quand bien même on connaîtrait un tel sous-code, on aurait quelque chose de la forme :

$$\mathbf{Cond}(\mathcal{A}_{r+1,q}(\boldsymbol{x}, \boldsymbol{y}), \mathcal{A}_{r,q}(\boldsymbol{x}, \boldsymbol{y})) \subseteq \mathbf{RS}_2(\boldsymbol{x}) \cap \mathbf{F}_q^n$$

et on vérifie expérimentalement que cette inclusion est presque toujours une égalité. Or le code $\mathbf{RS}_2(\boldsymbol{x})$ est le code de dimension 2 engendré par les vecteurs $\mathbf{1}$ et $\boldsymbol{x}$. Donc, dès lors que $\boldsymbol{x}$ a au moins un coefficient dans $\mathbf{F}_{q^2} \setminus \mathbf{F}_q$, ce qui arrive dès que $n > q$, on a $\mathbf{RS}_2(\boldsymbol{x}) \cap \mathbf{F}_q^n = \langle \mathbf{1} \rangle$. De fait, un tel procédé ne donne aucune information sur $\boldsymbol{x}$.

Il faut donc rechercher un sous-code $\mathcal{A}_{r+s,q}(\boldsymbol{x}, \boldsymbol{y})$ correspondant à des polynômes de plus petit degré tel que $\mathbf{Cond}(\mathcal{A}_{r+s,q}(\boldsymbol{x}, \boldsymbol{y}), \mathcal{A}_{r,q}(\boldsymbol{x}, \boldsymbol{y}))$ qui est typiquement égal à $\mathbf{RS}_{s+1}(\boldsymbol{x}) \cap \mathbf{F}_q^n$ soit différent de $\langle \mathbf{1} \rangle$ et contienne des informations sur $\boldsymbol{x}$. Un bon choix est $s = q$. Pour cette dernière, valeur le code $\mathbf{RS}_{q+1}(\boldsymbol{x})$ contient le vecteur à coefficients dans $\mathbf{F}_q$: $\boldsymbol{x}^{\star q} + \boldsymbol{x}$ obtenu par évaluation de la trace coordonnée par coordonnée.

Reste la question de savoir comment trouver le code $\mathcal{A}_{r+q,q}(\boldsymbol{x}, \boldsymbol{y})$. On peut procéder à une recherche exhaustive sur tous les sous-codes de $\mathcal{A}_{r,q}(\boldsymbol{x}, \boldsymbol{y})$ de la bonne codimension, à savoir $2r$ et pour chacun de ces codes $\mathcal{Y}$ calculer $\mathbf{Cond}(\mathcal{Y}, \mathcal{A}_{r,q}(\boldsymbol{x}, \boldsymbol{y}))$ qui sera trivial sauf dans le cas où $\mathcal{Y}$ est le code recherché. Ce procédé reste bien trop coûteux du fait du nombre prohibitif de sous-codes de codimension $2q$ de notre code public. En effet, le nombre de codes à énumérer serait en $O(q^{2q(\dim \mathcal{C}_{\text{pub}} - 2q)})$ ce qui pour les paramètres DAGS_1 donnerait un nombre d'itérations de l'ordre de 2^{112640} ce qui est évidemment hors de portée.

C'est là que le groupe d'automorphisme entre dans le jeu car ce dernier, accompagné d'une astuce de raccourcissement permet de réduire drastiquement la complexité d'une telle recherche. En effet, le fait qu'un groupe de permutations $\mathcal{G}$ agisse sur le code public permet de calculer le sous-code invariant

$$\mathcal{A}_{r,q}(\boldsymbol{x}, \boldsymbol{y})^{\mathcal{G}} \stackrel{\text{def}}{=} \{ \boldsymbol{c} \in \mathcal{A}_{r,q}(\boldsymbol{x}, \boldsymbol{y}) \mid \forall \sigma \in \mathcal{G},\ \sigma(\boldsymbol{c}) = \boldsymbol{c} \}. \tag{3.2}$$

On va alors chercher le sous-code $\mathcal{A}_{r+q,q}(\boldsymbol{x},\boldsymbol{y})^{\mathcal{G}}$ de $\mathcal{A}_{r,q}(\boldsymbol{x},\boldsymbol{y})^{\mathcal{G}}$ le nombre d'itérations tombe alors à $O\left(q^{\frac{2q}{\sharp\mathcal{G}}\cdot\frac{\dim \mathcal{C}_{\text{pub}}-2q}{\sharp\mathcal{G}}}\right)$, soit, pour les paramètres `DAGS_1` un nombre d'itérations de l'ordre de 2^{440} ; l'exposant de la complexité a été divisé par $\sharp\mathcal{G}$. Enfin, une simple astuce de raccourcissement permet de faire tomber ce nombre d'itérations à $O\left(q^{\frac{4q}{\sharp\mathcal{G}}}\right)$ soit de l'ordre de 2^{40} itérations pour l'exemple en cours. Une itération consistant en le calcul d'un conducteur, ce qui se réduit essentiellement à la résolution d'un système linéaire dont on on a évalué le coût à environ 2^{30} opérations (voir lemme 3.3.3). Ce qui fournit un coût d'attaque de l'ordre de 2^{70} opérations , ce qui est bien en dessous des 128 bits de sécurités estimés par les auteurs

Nous avons proposé deux approches pour trouver ce code $\mathcal{A}_{r+q,q}(\boldsymbol{x},\boldsymbol{y})^{\mathcal{G}}$. La première est partiellement décrite ci-dessus et est basée sur une énumération de sous-codes et sa complexité est décrite dans le Tableau 3.2. La seconde, consiste à calculer une base de ce code en résolvant un système d'équations

Name	**Niveau de sécurité estimé**	**Coût de l'attaque**
`DAGS_1`	128 bits	$\approx 2^{70}$
`DAGS_3`	192 bits	$\approx 2^{80}$
`DAGS_5`	256 bits	$\approx 2^{58}$

TABLE 3.2 – Coût de la première version de l'attaque

quadratiques. Nous ne sommes pas parvenus à analyser la complexité théorique de cette méthode mais les résultats expérimentaux obtenus à l'aide du logiciel `Magma` [31] étaient assez concluants, permettant en particulier de casser des clés publiques d'une sécurité estimée à 256 bits en moins d'une minute !

3.5 Des propositions résistantes

La littérature en cryptographie basée sur les codes fourmille de propositions qui ont donné lieu à des attaques peu de temps après leur publication. Il serait pourtant erroné de penser que la cryptographie à base de codes et en particulier à base de codes algébriques n'est pas sûre. Malgré une littérature de cryptanalyse fournie, un certain nombre de familles de codes restent hors de portée de toutes les méthodes d'attaque connues.

En particulier, les codes alternants et de Goppa de degré d'extension élevé, en particulier les codes alternants et de Goppa binaires n'ont fait l'objet d'aucune attaque de complexité polynomiale ou même sous–exponentielle en plus de quarante ans d'existence.

Concernant les codes géométriques, si nous avons montré qu'ils n'étaient pas sûrs, leurs sous-codes sur un sous-corps restent hors d'atteinte du distingueur $\mathcal{C} \mapsto \mathcal{C}^2$ et hors d'atteinte de toute attaque connue. Notons d'ailleurs qu'une telle famille n'est autre qu'une généralisation des codes de Goppa classiques, ces derniers correspondant au cas des courbes de genre 0.

Je termine ce chapitre en signalant mes contributions à des propositions et non des attaques.

3.5.1 BIG QUAKE

Publication associée : [17].

Dans le cadre de l'appel lancé par le NIST en 2016 pour des primitives cryptographiques post quantiques, nous avons proposé un schéma nommé BIG QUAKE [17] (BInary Goppa QUAsi–cyclic Key Encapsulation). Cette soumission, n'a pas été retenue au second tour, mais n'a par ailleurs fait l'objet d'aucune attaque et reste selon moi un schéma solide permettant une alternative à *Classic McEliece* [26] avec des clés plus légères (une taille environ divisée par 10 pour une sécurité équivalente).

Cette proposition repose sur l'utilisation de codes de Goppa binaires quasi–cycliques, i.e. munis d'un groupe d'automorphismes cyclique. La motivation de cette proposition était la suivante :

— Les codes de Goppa binaires comptent parmi les rares familles de codes pour lesquels on ne connaît aucune attaque polynomiale ou même sous-exponentielle. Ils étaient dans la proposition historique de McEliece et résistent donc à toutes les attaques depuis plus de 40 ans.
— Si l'on analyse les attaques (exponentielles) existantes, on constate que les attaques sur les clés sont bien plus coûteuses que les attaques sur les messages.
— Le fait d'ajouter une structure quasi–cyclique réduit le coût des attaques sur les clés mais son influence sur les attaques sur les messages reste très limitée. En effet :
  - Élise Barelli a montré dans [18] que la structure d'un code alternant (resp. de Goppa) quasi–cyclique se déduit aisément de celle de son sous-code invariant défini en (3.2). On peut montrer que ce sous-code invariant (après suppression des colonnes redondantes dans la matrice génératrice) est également un code alternant (resp. de Goppa) dont la longueur et le degré ont été divisés par l'ordre du groupe. Ce fait avait d'ailleurs déjà déjà utilisé dans [67, 66] pour attaquer des systèmes basés sur des codes alternants quasi–cycliques dont le groupe d'automorphismes était trop grand.
  - Concernant les attaques sur les messages, autrement dit les algorithmes de décodage génériques, on ne sait pas réduire significativement la complexité de tels algorithmes lorsque l'on se restreint au cas de codes quasi–cycliques ou plus généralement aux codes admettant un groupe d'automorphismes $\mathcal{G}$ non trivial. La meilleure amélioration connue est celle de Sendrier [129] permettant de diviser la complexité par un facteur $\sqrt{\sharp\mathcal{G}}$, cette complexité restant exponentielle et de même exposant.

Le second point motive donc l'approche suivante. Choisir la taille du groupe d'automorphismes $\mathcal{G}$ (isomorphe à $\mathbb{Z}/\ell\mathbb{Z}$ dans notre cas) de manière à ce que la sécurité des clés, bien que significativement diminuée, reste supérieure à celle des messages, qui elle n'est que peu impactée par l'ajout d'une structure quasi–cyclique de manière à ce que le niveau de sécurité globale reste du même ordre que pour un McEliece classiques à base de codes de Goppa binaires. La taille des clés est essentiellement divisée par l'ordre du groupe. Les choix les plus offensifs de ℓ que nous avons faits étaient $\ell = 19$. Des paramètres de BIG QUAKE sont présentés dans le tableau 3.5.1.

Table 3.3 – Paramètres de BIG QUAKE

Sécurité (bits)	Longueur	Dimension	ℓ	Taille de clés (Ko)
128	3510	2418	13	25389
192	7410	4674	19	84132
256	10070	6650	19	149625

3.5.2 Les travaux d'Élise Barelli

Dans sa thèse de doctorat [19], Élise Barelli a proposé l'utilisation de sous-codes sur un sous-corps de codes géométriques à partir de courbes munies d'un automorphisme. Son approche semble très prometteuse. En particulier elle montre que, le fait de considérer des codes à partir de courbes de genre $g \neq 0$ ajoute une difficulté supplémentaire : en genre 0 la classe d'équivalence linéaire d'un diviseur ne dépend que de son degré. En genre supérieur, à degré fixé, le nombre de classes d'équivalence, n'est autre que le nombre d'éléments du groupe $\mathrm{Pic}^0(\mathscr{X})$. Ainsi, par rapport au cas des codes de Goppa classiques, pour des codes à partir de courbes, le coût d'une recherche exhaustive sera multiplié par un facteur $O(q^g)$ correspondant au nombre de points de la Jacobienne de la courbe.

Chapitre 4

Combinatoire additive et produits d'espaces vectoriels dans des corps de fonctions

Publication associée : [11].

L'étude de produits de codes et l'analyse de codes dont le carré est de dimension strictement plus petite que celui de codes aléatoires m'ont amené vers l'étude d'un problème plus théorique : la classification de sous-espaces S de dimension finie dans une algèbre A sur un corps k et tels que la dimension de

$$S^2 \stackrel{\text{def}}{=} \langle ab \mid a, b \in S \rangle$$

est « petite ». Ce problème n'est pas sans rappeler un problème classique de combinatoire additive consistant à classifier les sous-ensembles A d'un groupe abélien G tels que le cardinal de $A + A \stackrel{\text{def}}{=} \{a + b \mid a, b \in A\}$ est « petit ».

4.1 Les théorèmes de Freiman en combinatoire additive

Afin d'établir les liens existants entre les problèmes de produits d'espaces et la combinatoire additive, commençons par rappeler quelques résultats classiques de ce dernier domaine. Les résultats qui suivent peuvent être trouvés dans le livre de Tao et Vu [145].

Si on se donne deux parties finies A, B d'un groupe abélien G, on définit

$$A + B \stackrel{\text{def}}{=} \{a + b \mid a \in A, b \in B\}.$$

De manière évidente $\sharp(A + B) \leqslant \sharp A \cdot \sharp B$, ce qui va nous intéresser sont les cas où $\sharp(A + B)$ est le plus petit possible. Notons que si $A = B$ et que A est un sous-groupe de G alors $A + A = A$.

Si l'on s'intéresse au cas du groupe $G = \mathbb{Z}$ qui n'a pas de sous-groupe fini on a une minoration meilleure, parfois appelée inégalité de Cauchy Davenport.

Proposition 4.1.1. *Soient A, B deux parties finies de $\mathbb{Z}$ telles que $\sharp A, \sharp B \geqslant 2$, alors :*

$$\sharp(A + B) \geqslant \sharp A + \sharp B - 1 \tag{4.1}$$

et l'égalité est atteinte si et seulement si A et B sont deux progressions arithmétiques de même raison.

Un théorème du à Kneser permet de généraliser l'inégalité (4.1) au cas où la somme $A + B$ est périodique, i.e. dans le cas où il existe $g \in G$ tel que $A + B + g = A + B$. Une telle situation est possible dans le cas où G admet des sous-groupes finis.

Théorème 4.1.2 (Kneser [94]). *Soient A, B deux parties finies d'un groupe G, alors*

$$\sharp(A+B) \geqslant \sharp A + \sharp B - \sharp\{u \in G \mid u + A + B = A + B\}$$

À noter que l'inégalité (4.1) se déduit immédiatement du théorème de Kneser car le seul élément $u \in \mathbb{Z}$ tel que $u + A + B = A + B$ est 0.

Enfin, on dispose d'un résultat plus général dû à Freiman et parfois appelé *Théorème* $3k-4$ *de Freiman.*

Théorème 4.1.3 (Freiman). *Soit A une partie finie de $\mathbb{Z}$ telle que $\sharp(A+A) \leqslant 3\sharp A - 4$, alors A est contenu dans une progression arithmétique de longueur inférieure ou égale à $\sharp(A+A) - \sharp A + 1$.*

Corollaire 4.1.4. *Soit A une partie finie de $\mathbb{Z}$ telle que $\sharp(A+A) = 2\sharp A - 1$, alors A est une progression arithmétique.*

Un autre énoncé dû à Freiman nous sera utile dans ce qui suit.

Théorème 4.1.5 (Lemme de Freiman). *Soit A une partie finie de $\mathbf{R}^d$ telle que $\sharp(A+A) \leqslant 3\sharp A - 4$, alors A engendre un espace affine de dimension 1.*

4.2 Un analogue dans le contexte des corps de fonctions

Ce qui nous intéresse est d'étudier les analogies entre le contexte additif et le contexte multiplicatif. On se donne un corps de base K et un corps F qui est une K–algèbre de type fini de degré de transcendance d sur K. On se donne également $S \subseteq F$ un K–espace vectoriel de dimension finie et on va s'intéresser à l'espace

$$S^2 = \{ab \mid a, b \in S\}.$$

Attirons l'attention sur le fait que, à la différence du cas additif, S^2 n'est pas l'ensemble des produits de deux éléments de S mais bien **l'espace engendré** par ces produits. C'est d'ailleurs précisément ce point qui rend difficile la transposition au contexte multiplicatif de certains résultats en théorie additive.

4.2.1 Résultats antérieurs

Le contexte multiplicatif a été bien moins étudié que le contexte additif. Toutefois, on dispose des résultats récents dans la littérature. Tout d'abord un analogue du théorème de Kneser.

Théorème 4.2.1 (Hou, Leung, Xiang [85]). *Soit L un corps de type fini séparable sur un corps K. Soient A, B deux sous–K–espaces de dimension finie de L de dimensions $\geqslant 2$, alors*

$$\dim AB \geqslant \dim A + \dim B - \dim \mathit{Stab}(AB)$$

où

$$\mathit{Stab}(AB) \stackrel{def}{=} \langle s \in L \mid s \cdot AB \subseteq AB \rangle.$$

Ce résultat a été généralisé aux extensions quelconques, éventuellement inséparables dans [13].

Notons dans l'énoncé précédent que $\mathrm{Stab}(AB) \stackrel{\text{def}}{=} \langle s \in L \mid s \cdot AB \subseteq AB \rangle$ est une sous–K–algèbre de L, autrement dit une extension de K. De plus, cette extension est finie. En effet, il suffit de prendre $u \in AB \setminus \{0\}$ et de noter que $\mathrm{Stab}(AB) \cdot u \subseteq AB$ et $\dim \mathrm{Stab}(AB) \cdot u = \dim \mathrm{Stab}(AB) \leqslant \dim AB$. De fait, si K est algébriquement clos dans L, alors pour tout sous-espace de dimension finie $S \subseteq L$ on aura $\mathrm{Stab}(S) = K$.

4.2.2 Première contribution, une forme faible du théorème de Freiman

Notre but est de classifier les espaces S dont le carré est de petite dimension. Dans le contexte additif et dans le groupe $\mathbb{Z}$, les progressions arithmétiques fournissent les parties finies A telles que $A+A$ est le plus petit possible, à savoir $2\sharp A-1$. De façon similaire, les espaces vectoriels S admettant une base en progression géométrique, i.e. de la forme $a, ax, ax^2, \dots, ax^{n-1}$ ont également un carré de petite dimension, à savoir $2\dim S-1$.

Des analogues multiplicatifs du Corollaire 4.1.4 affirmant que les espaces vérifiant $\dim S^2 = 2\dim 2-1$ ont une base en progression géométrique ont été démontrés dans le cas où K, F sont des corps finis [12].

Notre premier objectif est évidemment de tirer au maximum parti des résultats existants et donc de se ramener à des problèmes additifs. Un outil fondamental pour cela est la notion de valuation. Dans le cas d'un corps de fonction de dimension 1 sur un corps K algébriquement clos, toutes les valuations sont à valeurs dans $\mathbb{Z}$ et de corps résiduel égal à K. Cependant, dans notre contexte le corps de fonctions ambiant n'est pas à priori de degré de transcendance 1 à priori. Notre premier résultat montre que si $\dim S^2 \leqslant 3\dim S-4$, et que $1 \in S$, alors le sous-corps $K(S) \subseteq F$ engendré par les éléments de S est de degré de transcendance 1 sur K.

Théorème 4.2.2 ([11, Theorem 4.2])**.** *Soit K un corps parfait et L une extension de type fini de K telle que K soit algébriquement clos dans L. Soit $S \subseteq L$ un K–espace de dimension finie tel que $1 \in S$ et S engendre L sur K. Si*

$$\dim S^2 \leqslant 3\dim S-4,$$

alors le degré de transcendance de L sur K est égal à 1.

Ainsi, sans perte de généralité, on supposera dorénavant que F est un corps de fonctions de degré de transcendance 1.

4.3 Le cas des espaces de genre combinatoire 0 et 1

Définition 4.3.1. Soit S un sous–K–espace vectoriel de dimension finie n de L. Le *genre combinatoire* de S est l'entier γ vérifiant

$$\dim S^2 = 2\dim S-1+\gamma.$$

Ainsi, les espaces admettant une base en progression géométrique $1, x, x^2, \dots, x^{n-1}$ sont de genre combinatoire nul. On note par ailleurs que de tels espaces engendrent sur K le corps $K(x)$, autrement dit, sont contenus dans un corps de fonctions de genre nul.

D'autres exemples sont donnés par les espaces de Riemann–Roch de corps de fonctions. Notons que, si l'on se donne un diviseur A d'un corps de fonctions L de genre g, alors $L(A)^2 \subseteq L(2A)$ et un théorème dû à Mumford nous donne une condition suffisante d'égalité.

Théorème 4.3.2 (Mumford [114, Theorem 6])**.** *Soient A, B deux diviseurs d'un corps de fonctions de genre g tels que $\deg A \geqslant 2g$ et $\deg B \geqslant 2g+1$, alors*

$$L(A)L(B) = L(A+B).$$

Ainsi, tout espace de Riemann Roch $L(A) \subseteq L$ tel que $\deg A > 2g$ vérifie

$$\dim L(A)^2 = 2\dim A+1-g = 2(\dim A+1-g)-1+g = 2\dim L(A)-1+g.$$

Autrement dit, un tel espace est de genre combinatoire g.

Notons enfin que si l'on prend un sous-espace S de codimension ℓ dans un espace de Riemann Roch $L(A)$ avec $\deg A > 2g$ et tel que $S^2 = L(2A)$ (une telle situation est facile à obtenir d'un sous-code aléatoire dès lors que $\binom{\dim S+1}{2} > \dim L(2A)$), alors

$$\dim S^2 = 2\dim L(A)-1+g = 2\dim S-1+(g+2\ell).$$

Autrement dit, le genre combinatoire de l'espace est supérieur à celui du corps de fonctions ambiant.

Ces différents exemples motivent une question : est-ce que tout espace S de genre combinatoire γ est contenu dans un corps de fonction de genre

$$g \leqslant \gamma.$$

Le résultat que nous avons obtenu concerne les espaces de genre combinatoire 1.

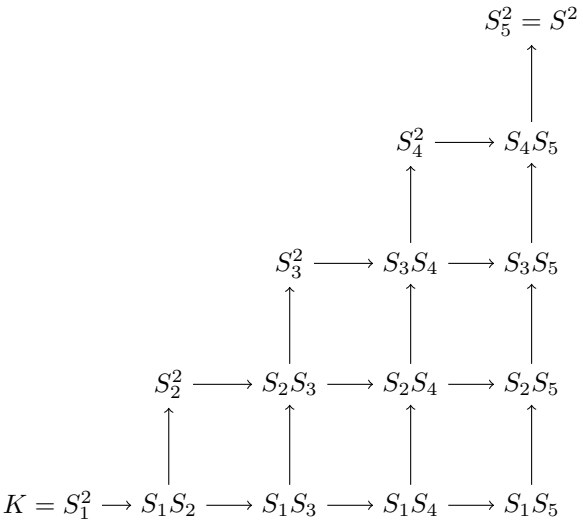
Théorème 4.3.3 ([11, Theorem 6.3])**.** *Soit K un corps parfait et L un corps de fonctions de degré de transcendance 1 sur K dans lequel K est algébriquement clos. Soit $S \subseteq L$ un K–espace vectoriel de dimension finie tel que $1 \in S$ et S engendre L sur K. Si S est de genre combinatoire 1, alors, L est de genre 0 ou 1. De plus*

- *Si L est de genre 1, alors $S = L(D)$ pour un certain diviseur D de degré n ;*
- *Si L est de genre 0, alors S est de codimension 1 dans un espace $L(D)$ pour un diviseur D de degré n.*

Dans les grandes lignes, la démonstration de ce résultat se fait comme suit. On se fixe une valuation discrète v sur L et on en déduit une filtration

$$\{0\} = S_0 \subseteq S_1 \subseteq \cdots \subseteq S_n = S.$$

On note $1 = x_1, \ldots, x_n$ la base filtrée associée à ce drapeau. On considère ensuite, le treillis d'espaces suivants, en prenant l'exemple $n = 5$.



Lemme 4.3.4. *Dans le graphe orienté ci-dessus, tout chemin de S_1^2 à S^2 correspond à une suite d'inclusions d'espaces vectoriels toutes de codimension 1 sauf une qui est de codimension 2.*

Démonstration. Un argument de valuation permet de voir que toutes les inclusions sont strictes donc de codimension au moins 1. Un chemin de S_1^2 à S^2 est de longueur $2n-2$ alors que $\dim S^2 - \dim S_1^2 = 2n-1$, ce qui donne le résultat attendu. □

De fait, sur un chemin donné, la codimension d'une arête est 1 sauf pour une seule telle arête. On démontre ensuite le lemme suivant.

Lemme 4.3.5. $L = K(S_3)$.

Démonstration. Pour tout $i \geqslant 1$,

$$S_{i-1}S_i = S_{i-1}^2 + S_{i-1}x_i.$$

Comme $\dim S_{i-1}S_i - \dim S_{i-1}^2 \leqslant 2$, dès lors que $i \geqslant 4$, alors $x_iS_{i-1} \cap S_{i-1}^2 \neq \{0\}$ et donc $x_i \in K(S_{i-1})$. □

Autrement dit, en rappelant que l'on a noté $x_1, \ldots, x_n$ notre base filtrée de S pour la valuation v et que $x_1 = 1$, alors

$$L = K(x_2, x_3).$$

Avec ces données, on a les clés en main pour montrer que le corps de fonctions L est de genre au plus 1. En effet, on distingue deux cas

— Si $dim S_2S_3 = 4$ alors, comme S_2S_3 est engendré par $1, x_2, x_3, x_2^2, x_2x_3$, il existe une relation linéaire entre ces monômes qui nous fournit une équation de conique, donc de courbe de genre 0.

— Si $\dim S_2S_3 = 5$, alors d'après le lemme 4.3.4, $\dim S_3S_4 = 7$ et cet espace est engendré par neuf générateurs :

$$1, x_2, x_3, x_4, x_2^2, x_2x_3, x_2, x_4, x_3^2, x_3x_4.$$

On en déduit l'existence de deux relations quadratiques indépendantes

$$x_4L_1(x_2, x_3) = Q_1(x_2, x_3)$$
$$x_4L_2(x_2, x_3) = Q_2(x_2, x_3)$$

où L_1, L_2 sont des polynômes de degré 1 et Q_1, Q_2 de degré 2. L'élimination de x_4 permet d'en déduire une équation cubique irréductible reliant x_2 et x_3. Une telle courbe est de genre 1 si elle est lisse et 0 sinon.

La fin de la preuve, sur la structure de S (espace de Riemann Roch ou sous-espace de codimension 1 d'un tel espace) requiert une analyse plus poussée pour laquelle je renvoie à [11].

Troisième partie

Méthodes géométriques et combinatoires pour la construction de codes quantiques

Chapitre 5

Codes quantiques à partir de graphes

Dans cette dernière partie je présente un autre aspect de mes travaux. Il concerne encore les codes mais cette fois-ci les codes quantiques et plus précisément les codes LDPC quantiques.

En codage classique, les codes LDPC (*Low Density Parity Check*) sont des codes qui sont noyau d'une matrice creuse. Plus précisément, une suite de codes $(\mathcal{C}_s)_s$ est dite LDPC si la suite des longueurs n_s tend vers l'infini et que pour tout s, $\mathcal{C}_s$ est le noyau d'une matrice $\boldsymbol{H}_s$ telle que le poids de chaque ligne de $\boldsymbol{H}_s$ soit en $O(\log(n_s))$. Historiquement, les codes LDPC ont été introduits par Gallager [73] dans sa thèse de doctorat dans les années 60. À cette époque son travail avait été vu comme purement théorique, ils ont connu un regain d'intérêt dans les années 90 après l'article [101] de McKay et Neal qui présente des résultats expérimentaux sur la performance de tels codes. Expérimentations qui n'étaient pas possibles dans les années 60 du fait de capacités de calcul limitées. Une preuve théorique du fait que des codes LDPC *irréguliers* atteignent la capacité de Shannon si leur graphe de Tanner [144] est acyclique est fournie dans [122]. Pour plus de détails sur le sujet, je renvoie le lecteur à [123].

Pour les codes LDPC classiques, on distingue deux type de constructions, les constructions combinatoires provenant de structures d'incidence discrètes telles que les designs, la géométrie finie etc... et les constructions probabilistes. Pour des codes de grande longueur les constructions probabilistes s'avèrent être imbattables, restreignant l'intérêt des constructions combinatoires au cas de longueurs moyennes ($1000 < n < 10000$). *À contrario*, pour les codes quantiques, nous verrons que l'approche probabiliste ne peut pas fournir les familles de codes les plus intéressantes, il est donc nécessaire de se tourner vers des constructions à base d'objets structurés issus de la combinatoire, la géométrie ou la topologie.

Ma contribution dans ce domaine s'est faite en deux temps. J'ai tout d'abord produit une construction de codes LDPC classiques à partir de méthodes géométriques [42]. J'ai ensuite travaillé sur les codes LDPC quantiques. En collaboration avec N. Delfosse et G. Zémor, j'ai étudié les paramètres de codes dont la construction avait été proposée par Shokrollahi et. al. [100]. Enfin, en collaboration avec B. Audoux, nous avons étudié le comportement des paramètres de codes quantiques construits par produits tensoriels itérés [10]. Dans ce qui suit, je vais présenter mes travaux sur les codes quantiques. Une rapide introduction au calcul quantique et aux codes associés s'impose donc.

5.1 Quelques notions de calcul quantique

Dans cette section je donne quelques éléments du modèle de calcul quantique. N'étant pas physicien et de culture limitée dans le domaine, je resterai délibérément flou sur les interprétations et explications physiques des phénomènes décrits. Le but de cette section est de fournir les éléments minimaux pour comprendre le principe du modèle de calcul quantique et avoir assez d'éléments pour comprendre ce qui amène à la définition de code quantique. Pour plus de détails sur le calcul quantique, je revoie le

lecteur au livre [116] et à l'article introductif [124].

5.1.1 Qubits et intrication

Un bit quantique ou *qubit* est la donnée d'un vecteur unitaire dans l'espace de Hilbert $\mathcal{H} \stackrel{\text{def}}{=} \mathbf{C}^2$. On note

$$|0\rangle \stackrel{\text{def}}{=} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \text{et} \qquad |1\rangle \stackrel{\text{def}}{=} \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Aussi, un qubit n'est autre qu'un vecteur de la forme $\alpha\,|0\rangle + \beta\,|1\rangle$ où $|\alpha|^2 + |\beta|^2 = 1$. Un tel objet décrit l'état quantique d'une particule isolée. La première différence majeure entre les théories de l'information classique et quantique est que, si l'on considère n particules, leur état ne sera pas décrit comme dans le cas classique par le produit cartésien de n copies de $\mathcal{H}$ mais par le produit tensoriel $\mathcal{H}^{\otimes n}$. Aussi, l'état quantique de n particules sera décrit par un élément de norme Hermitienne 1 dans $\mathcal{H}^{\otimes n}$ autrement dit par un élément de la forme

$$\sum_{\boldsymbol{u} \in \{0,1\}^n} \alpha_{\boldsymbol{u}}\,|u_1\rangle \otimes \cdots \otimes |u_n\rangle \qquad \text{tel que} \qquad \sum_{\boldsymbol{u} \in \{0,1\}^n} |\alpha_{\boldsymbol{u}}|^2 = 1.$$

Pour alléger les notations, on note $|u_1 \cdots u_n\rangle \stackrel{\text{def}}{=} |u_1\rangle \otimes \cdots \otimes |u_n\rangle$. Notons qu'un élément d'un produit tensoriel n'est pas toujours un tenseur élémentaire mais une combinaison de tels tenseurs. Aussi, l'état quantique d'un n–uplet de particules n'est pas toujours un produit d'état de particules élémentaires. On parle alors d'*états quantiques intriqués*. Ce phénomène d'intrication quantique est sans doute ce qui amène la remarquable richesse du calcul quantique.

5.1.2 Mesure quantique

La seconde particularité de la physique quantique est que l'on ne peut pas observer l'état d'une particule ou d'un ensemble de particules sans modifier ce dernier. Mesurer un qubit $q = \alpha\,|0\rangle + \beta\,|1\rangle$ renverra 0 avec probabilité $|\alpha|^2$ et 1 avec probabilité $|\beta|^2$. Le second effet de la mesure est que le qubit sera transformé en $|0\rangle$ dans le cas où l'opération de mesure a renvoyé 0 et en $|1\rangle$ sinon. Plus généralement, la mesure d'un état quantique se fait en respect à une décomposition dans une somme directe orthogonale. Si $\mathcal{H}^{\otimes n}$ se décompose en une somme directe orthogonale d'espaces de même dimensions

$$\mathcal{H}^{\otimes n} = \bigoplus_{i \in I}^{\perp} H_i$$

on lui associe une mesure quantique qui, étant donné un état $a \in \mathcal{H}^{\otimes n}$ se décomposant en $a = \sum_{i \in I} \alpha_i e_i$ telle que $\sum_i |\alpha_i|^2 = 1$, alors la mesure de a renverra i avec probabilité $|\alpha_i|^2$ et transformera l'état a en e_i.

5.2 Codes quantiques

L'interaction d'une particule ou d'un système de particules avec son environnement provoque des modifications de son état. C'est ce qui motive la nécessité d'avoir des codes correcteurs quantiques.

5.2.1 Le groupe de Pauli

On va se baser sur un modèle d'erreur sans mémoire, i.e. telle que les erreurs sur deux qubits distincts sont indépendantes. On définit les opérateurs de Pauli :

$$I \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X \stackrel{\text{def}}{=} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{et} \quad Y \stackrel{\text{def}}{=} \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$$

et le groupe de Pauli comme le groupe de matrices

$$\mathcal{P} \stackrel{\text{def}}{=} \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}.$$

Deux éléments du groupe de Pauli commutent ou anticommutent, i.e. vérifient toujours

$$AB = BA \qquad \text{ou} \qquad -BA.$$

Une erreur sur un qubit sera une combinaison linéaire de ces opérateurs. Un tel modèle d'erreurs est continu. Toutefois, si l'on part d'un qubit $q \in \{|0\rangle, |1\rangle\}$, que q subit une erreur

$$E = aI + bX + cY + dZ \quad \text{telle que} \quad |a|^2 + |b|^2 + |c|^2 + |d|^2 = 1,$$

alors, lorsque l'on mesurera le qubit Eq, il sera transformé en le qubit q avec probabilité $|a|^2$ en Xq avec probabilité $|b|^2$, etc... Aussi, même si les erreurs survenant sur nos qubits sont des opérateurs appartenant au groupe unitaire, la combinaison des erreurs du canal et de la mesure quantique peut être décrite comme un modèle d'erreurs discret. Dans ce contexte, le canal de décohérence quantique de probabilité p est un modèle d'erreurs indépendantes sur les qubits telles que I est appliqué sur un qubit avec probabilité $1-p$ et X, Y, Z lui sont appliquées avec probabilité $\frac{p}{3}$. Le canal que l'on vient de décrire est souvent présenté comme l'analogue quantique du canal binaire symétrique.

5.2.2 Codes stabilisateurs

Dans le cas de n qubits, on considère l'action du groupe

$$\mathcal{P}_n \stackrel{\text{def}}{=} \{a \cdot E_1 \otimes \cdots \otimes E_n \mid a \in \{\pm 1, \pm i\},\ E_i \in \{1, X, Y, Z\}\},$$

sur nos n qubits. On munit le groupe $\mathcal{P}_n$ d'une fonction de poids. Le *poids* d'un élément $a \cdot E_1 \otimes \cdots \otimes E_n$ étant le nombre d'éléments E_i qui diffèrent de I.

Lemme 5.2.1. *Le groupe $\mathcal{P}_n/\{\pm 1, \pm i\}$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^n$.*

Définition des codes stabilisateurs

Définition 5.2.2. À un sous-groupe commutatif $\mathcal{G} \subseteq \mathcal{P}_n$ ne contenant pas $-(I \otimes \cdots \otimes I)$, on associe le *code stabilisateur* $\mathscr{C}_\mathcal{G} \subseteq \mathcal{H}^{\otimes n}$ défini comme le sous-espace des éléments fixes par $\mathcal{G}$:

$$\mathscr{C}_\mathcal{G} \stackrel{\text{def}}{=} \{x \in \mathcal{H}^{\otimes n} \mid \forall \sigma \in \mathcal{G},\ \sigma(x) = x\}.$$

La *longueur* de $\mathscr{C}_\mathcal{G}$ est n et sa *dimension* est l'entier k tel que le plus petit système de générateurs de $\mathcal{G}$ soit de cardinal $n-k$.

Remarque 5.2.3. Notons ici une confusion à éviter. La dimension d'un code quantique n'est **pas** sa dimension en tant que $\mathbf{C}$–espace vectoriel. En effet, $\dim_\mathbf{C} \mathscr{C}_\mathcal{G} = 2^k$. Il faut voir la dimension d'un code quantique comme le nombre de qubits qu'il peut encoder. De même que la longueur n'est pas la dimension de l'espace de Hilbert ambiant mais bien le nombre de qubits utilisés pour encoder k qubits d'information.

Lemme 5.2.4. *Soit $N(\mathcal{G})$ le sous-groupe de $\mathcal{P}_n$ des éléments qui commutent avec tout élément de $\mathcal{G}$. Alors $\mathscr{C}_\mathcal{G}$ est stable par $\sigma \in \mathcal{P}_n$ si et seulement si $\sigma \in N(\mathcal{G})$.*

Démonstration. Si σ commute avec tout élément de $\mathcal{G}$, alors pour tout $x \in \mathscr{C}_\mathcal{G}$ et pour tout $\gamma \in \mathcal{G}$,

$$\gamma(\sigma(x)) = \sigma\gamma(x) = \sigma(x).$$

Réciproquement, supposons qu'il existe $\gamma \in \mathcal{G}$ tel que σ ne commute pas avec γ. Le cas échéant, les deux éléments anticommutent et pour tout $x \in \mathscr{C}_\mathcal{G}$, on a

$$\gamma(\sigma(x)) = -\sigma(\gamma(x)) = -\sigma(x).$$

Aussi, pour tout $x \setminus \{0\}$, $\sigma(x) \notin \mathscr{C}_\mathcal{G}$. □

Mesure du syndrome

Si $\mathcal{G} \subseteq \mathcal{P}_n$ ne contient pas $-(I \otimes \cdots \otimes I)$, il ne contient pas non plus $\pm i(I \otimes \cdots \otimes I)$ et est donc isomorphe à son image dans $\mathcal{P}_n/\{\pm 1, \pm i\}$. De ce fait, d'après le lemme 5.2.1, le groupe $\mathcal{G}$ est isomorphe à un sous-groupe de $(\mathbb{Z}/2\mathbb{Z})^n$, qui, rappelons le, est un $\mathbb{Z}/2\mathbb{Z}$–espace vectoriel. S'il est engendré par $S_1, \ldots, S_{n-k}$ et que ces générateurs sont linéairement indépendants (sur $\mathbb{Z}/2\mathbb{Z}$), alors, le code $\mathscr{C}_\mathcal{G}$ est de dimension 2^k. Par ailleurs, on définit pour tout $\boldsymbol{u} \in \{0,1\}^{n-k}$ le sous-espace de $\mathcal{H}^{\otimes n}$

$$\mathscr{C}(\boldsymbol{u}) \stackrel{\text{def}}{=} \{x \in \mathcal{H}^{\otimes n} \mid \forall i \in \{1, \ldots, n-k\},\ S_i x = (-1)^{u_i} x\}.$$

On démontre aisément que l'espace $\mathcal{H}$ se décompose en la somme directe orthogonale suivante :

$$\mathcal{H}^{\otimes n} = \bigoplus_{\boldsymbol{u} \in \{0,1\}^n}^{\perp} \mathscr{C}(\boldsymbol{u}).$$

À cette décomposition, on associe une mesure quantique. Ainsi si $x \in \mathscr{C}_\mathcal{G}$ subit une erreur $E = a \cdot E_1 \otimes \cdots \otimes E_n \in \mathcal{P}_n$, la mesure du syndrome permet de détecter la présence d'erreur si E anticommute avec au moins un élément de $\mathcal{G}$.

En conclusion, étant donné un mot $\boldsymbol{c} \in \mathscr{C}_\mathcal{G}$, un tel mot peut subir trois types d'erreurs $E = E_1 \otimes \cdots \otimes E_n \in \mathcal{P}^{\otimes n}$:

— Une erreur qui ne fait rien, à savoir une erreur $E \in \mathcal{G}$;
— Une erreur détectable, à savoir une erreur E qui ne commute pas avec tout élément de $\mathcal{G}$;
— Une erreur indétectable, à savoir une erreur de $N(\mathcal{G}) \setminus \mathcal{G}$.

Il est donc fondamental que les erreurs indétectables, i.e. les éléments de $N(\mathcal{G}) \setminus \mathcal{G}$ correspondent à des erreurs rares. Dans le contexte du canal de décohérence quantique, les erreurs rares sont celles de poids élevé, autrement dit, on attend d'un bon code stabilisateur que le poids minimal de $N(\mathcal{G}) \setminus \mathcal{G}$ soit le plus élevé possible. Ce poids minimal est appelé *distance minimale du code quantique*.

Remarque 5.2.5. Faisons ici un premier lien avec les codes classiques. Si l'on considère des codes binaires et que notre modèle d'erreurs est le canal binaire symétrique, les motifs d'erreur indétectables sont les motifs d'erreur qui sont égaux à un mot de code. Aussi, la distance minimale d'un code classique, peut également être vue comme le poids minimal d'une erreur indétectable. La différence entre les codes classiques et les codes quantiques réside dans le fait que pour les codes quantiques, il existe des motifs d'erreurs qui ne font rien. Une notion qui n'a pas d'analogue pour les codes classiques.

5.2.3 Codes CSS

Une classe particulièrement étudiée de codes quantiques est la famille des codes CSS (pour Calderbank, Shor et Steane) [34, 136]. Il s'agit d'une sous-classe des codes stabilisateurs dont le groupe de stabilisateurs admet un système de générateurs qui se décompose en deux sous-ensembles :

— un ensemble de générateurs « en X », i.e. de générateurs de la forme $E_1 \otimes \cdots \otimes E_n$ avec $E_i \in \{I, X\}$;
— un ensemble de générateurs « en Z », i.e. de la forme $E_1 \otimes \cdots \otimes E_n$ avec $E_i \in \{I, Z\}$.

Notons que les générateurs en X (resp. en Z) commutent entre eux. Aussi, pour vérifier la propriété de commutativité de $\mathcal{G}$, il suffit de vérifier que les générateurs en X et en Z commutent entre eux. À un tel système de générateurs, on peut associer deux matrices $\boldsymbol{H}_X, \boldsymbol{H}_Z$ à coefficients dans $\mathbf{F}_2$. Les lignes de $\boldsymbol{H}_X$ (resp. de $\boldsymbol{H}_Z$) sont en correspondance avec les générateurs en X de la façon suivante. Si le i–ème générateur en X est

$$E_i^X = E_{i,1}^X \otimes \cdots \otimes E_{i,n}^X$$

on lui fait correspondre la i-ème ligne de $\boldsymbol{H}_X$ de manière à ce que le coefficient (i,j) de $\boldsymbol{H}_X$ soit

$$h_{ij}^X = \begin{cases} 1 & \text{si} \quad E_{ij}^X = X \\ 0 & \text{si} \quad E_{ij}^X = I. \end{cases}$$

Lemme 5.2.6. *Les stabilisateurs en X commutent avec les stabilisateurs en Z si et seulement si*

$$\boldsymbol{H}_X \cdot {}^t\boldsymbol{H}_Z = 0.$$

Démonstration. Rappelons que $XZ = -ZX$ et que, de manière évidente, I commute à X et Z. Aussi, étant donnés un stabilisateur $E^X = E_1^X \otimes \cdots \otimes E_n^X$ avec $E_i^X \in \{I, X\}$ et un stabilisateur $E^Z = E_1^Z \otimes \cdots \otimes E_n^Z$ avec $E_i^Z \in \{I, Z\}$, on a

$$E^X \cdot E^Z = (-1)^w E^Z \cdot E^X$$

où w est le nombre de positions en lesquelles E^X a un X et E^Z à un Z. La parité de ce nombre de positions n'est autre que la forme bilinéaire canonique sur $\mathbf{F}_2$ appliquée au couple des lignes correspondantes de $\boldsymbol{H}_X, \boldsymbol{H}_Z$.

Aussi, si $\boldsymbol{H}_X \cdot {}^t\boldsymbol{H}_Z = 0$, alors les lignes de $\boldsymbol{H}_X$ sont orthogonales à celles de $\boldsymbol{H}_Z$ et d'après ce qui précède, cette dernière assertion est équivalente au fait que les générateurs en X commutent aux générateurs en Z. □

Un code CSS est donc décrit par deux matrices $\boldsymbol{H}_X, \boldsymbol{H}_Z$ à coefficients dans $\mathbf{F}_2$ telles que

$$\boldsymbol{H}_X \cdot {}^t\boldsymbol{H}_Z = 0.$$

Si on note $\mathcal{C}_X, \mathcal{C}_Z$ les codes binaires (classiques) de matrices de contrôle respectives $\boldsymbol{H}_X$ et $\boldsymbol{H}_Z$ alors, la donnée d'un code CSS est équivalente à la donnée de deux codes classiques $\mathcal{C}_X, \mathcal{C}_Z$ tels que

$$\mathcal{C}_Z \subseteq \mathcal{C}_X^{\perp}.$$

Proposition 5.2.7. *Les paramètres d'un code CSS $\mathscr{C}$ sont notés $[[n, k, d]]$ où n désigne sa longueur, k désigne sa dimension, qui vérifie*

$$k = n - Rk(\boldsymbol{H}_X) - Rk(\boldsymbol{H}_Z) = \dim \mathcal{C}_X + \dim \mathcal{C}_Z - n.$$

Enfin, sa distance minimale est égale à

$$d = \min(d^X, d^Z) \qquad où \qquad \begin{cases} d^X \overset{def}{=} \min\{w_H(\boldsymbol{c}) \mid \boldsymbol{c} \in \mathcal{C}_X \setminus \mathcal{C}_Z^{\perp}\} \\ d^Z \overset{def}{=} \min\{w_H(\boldsymbol{c}) \mid \boldsymbol{c} \in \mathcal{C}_Z \setminus \mathcal{C}_X^{\perp}\}. \end{cases}$$

Interprétons rapidement les résultats ci-dessus. La formule concernant la dimension est naturelle. Le terme $\mathrm{Rk}(\boldsymbol{H}_X) + \mathrm{Rk}(\boldsymbol{H}_Z)$ correspond au nombre de stabilisateurs indépendants. Concernant la distance minimale, la quantité d^X correspond au poids minimal d'une erreur qui commute avec tout stabilisateur en X sans être un stabilisateur en Z et réciproquement pour d^Z.

Remarque 5.2.8. Pour un code CSS, on dispose toujours de la minoration suivante pour la distance minimale.

$$d \geqslant \min(d(C_X), d(C_Z)).$$

Dans le cas où cette quantité n'est pas atteinte, on parle de code CSS *dégénéré*. Notons que la terminologie *dégénéré* peut être trompeuse en ce sens où elle laisse penser qu'il s'agit des éléments que l'on cherche à éviter. En réalité c'est le contraire, nous verrons en particulier que pour les codes LDPC quantiques, seuls les codes dégénérés nous permettent d'espérer obtenir des distances minimales croissant plus vite que $\log n$. Le cas des codes dégénérés est donc précisément celui qui nous intéressera dans ce qui suit.

5.2.4 Interprétation homologique des codes CSS

L'algèbre homologique, utilisée à un niveau certes très élémentaire, s'avère être un outil intéressant pour décrire et étudier les propriétés de codes CSS. Commençons par fournir une définition de code CSS via un complexe de chaînes. Si l'on se donne un complexe de chaînes que l'on va centrer en 0 (simple convention) :

$$\cdots \longrightarrow C_{-1} \xrightarrow{\partial_{-1}} C_0 \xrightarrow{\partial_0} C_1 \longrightarrow \cdots$$

où les C_i sont des espaces vectoriels de dimension finie sur $\mathbf{F}_2$ et chaque C_i est muni d'une base $\mathcal{B}_i$. On introduit également le complexe dual :

$$\cdots \longleftarrow C_{-1}^\vee \xleftarrow{\partial_{-1}^*} C_0^\vee \xleftarrow{\partial_0^*} C_1^\vee \longleftarrow \cdots$$

Chaque $C_i^\vee$ est muni de la base duale $\mathcal{B}_i^*$ associée à $\mathcal{B}_i$. La donnée d'un complexe de chaînes nous fournit naturellement un code CSS dont la matrice $\boldsymbol{H}_X$ est la matrice représentant ∂_{-1}^* dans les bases $\mathcal{B}_0^*, \mathcal{B}_{-1}^*$ et $\boldsymbol{H}_Z$ est la matrice représentant ∂_0 dans les bases $\mathcal{B}_0, \mathcal{B}_1$. De fait, la matrice ${}^t\boldsymbol{H}_X$ représente ∂_{-1} dans les bases $\mathcal{B}_{-1}, \mathcal{B}_0$. De fait, la propriété de complexe de chaînes $\partial_0 \circ \partial_{-1} = 0$ se traduit par

$${}^t\boldsymbol{H}_X \cdot \boldsymbol{H}_Z = 0,$$

on retrouve ainsi la propriété attendue.

Proposition 5.2.9. *À un complexe de chaînes :*

$$C_\bullet : \qquad \cdots \longrightarrow C_{-1} \xrightarrow{\partial_{-1}} C_0 \xrightarrow{\partial_0} C_1 \longrightarrow \cdots$$

on associe naturelle un code CSS de longueur $n = \dim C_0$, dont la dimension est la dimension du groupe d'homologie $H_0(C_\bullet) \overset{def}{=} \ker \partial_0 / Im\, \partial_{-1}$. Sa distance minimale est le minimum des quantités suivantes :

$$d^Z = \min\{w_H(x) \in C_0 \mid x \in \ker \partial_0 \setminus Im\, \partial_{-1}\}, \qquad d^X = \min\{w_H(x) \in C_0^\vee \mid x \in \ker \partial_{-1}^* \setminus Im\, \partial_0^*\},$$

où les poids sont calculés en respect à la décomposition dans la base $\mathcal{B}_0$ (resp. $\mathcal{B}_0^*$).

Autrement dit, d^Z désigne le poids minimal d'un représentant de classe d'un élément non nul de l'homologie et d^X désigne le poids minimal d'un représentant de classe d'un élément non nul de la cohomologie. Ce point de vue homologique des codes quantiques a encouragé l'introduction de méthodes issues de la topologie algébrique pour la construction de codes quantiques comme on le verra un peu plus loin.

Notons qu'un complexe de chaînes de longueur 2 est une donnée suffisante pour décrire un code quantique. Dans ce qui suit, nous nous intéresserons particulièrement au cas de complexes *courts* et/ou *réduits* selon la définition suivante.

Définition 5.2.10. Un complexe *court* est un complexe de chaînes dont les seuls termes non nuls sont en degré $-1, 0, 1$. Autrement dit, il est de la forme

$$0 \longrightarrow C_{-1} \xrightarrow{\partial_{-1}} C_0 \xrightarrow{\partial_0} C_1 \longrightarrow 0\ .$$

Un tel complexe est dit *réduit* si de plus son H_{-1} et son H_1 sont nuls. Autrement dit, ∂_{-1} est injective et ∂_0 est surjective.

Du point de vue des codes quantiques. Un code CSS représenté par un couple de matrices $(\boldsymbol{H}_X, \boldsymbol{H}_Z)$ donne naturellement un complexe de chaînes court

$$0 \longrightarrow C_{-1} = \mathbf{F}_2^{n_{-1}} \xrightarrow{{}^t\boldsymbol{H}_X} C_0 = \mathbf{F}_2^{n_0} \xrightarrow{\boldsymbol{H}_Z} C_1 = \mathbf{F}_2^{n_1} \longrightarrow 0$$

où n_{-1} désigne le nombre de lignes de $\boldsymbol{H}_X$, n_1 celui de $\boldsymbol{H}_Z$ et n_0 désigne le nombre de colonnes de ces deux matrices. Le complexe sera réduit si et seulement si les matrices $\boldsymbol{H}_X, \boldsymbol{H}_Z$ sont toutes deux de rang plein.

Remarque 5.2.11. Attention ! Dans ce qui précède et contrairement à l'usage établi en théorie des codes, la notation $\ll\ A \xrightarrow{\boldsymbol{A}} B \gg$ décrit une application $x \mapsto \boldsymbol{A}x$ où x est vu comme un vecteur colonne. C'est la convention que j'adopterai dans tout ce qui suit lorsque je souhaiterais rendre explicites les différentielles dans des complexes de chaînes.

5.3 Codes LDPC quantiques

Un code CSS est dit *LDPC* s'il peut être décrit par un couple de matrices $(\boldsymbol{H}_X, \boldsymbol{H}_Z)$ toutes deux creuses. Plus précisément, une suite $(\mathscr{C}^{(s)})$ de codes CSS dont la suite (n_s) des longueurs tend vers l'infini est dite LDPC si chaque terme de la suite peut être décrit par un couple de matrices $(\boldsymbol{H}_X^{(s)}, \boldsymbol{H}_Z^{(s)})$ dont les poids des lignes sont en $O(\log(n_s))$.

Rappelons qu'en codage classique, les codes LDPC sont ceux qui admettent une matrice de contrôle dont les lignes sont de poids $O(\log n)$. Un tel code LDPC classique tiré au hasard a une distance $\geqslant \alpha n$ pour une certaine constante positive α [73] et bénéficie d'algorithmes de décodages rapides et dont les performances permettent d'approcher de très près la limite théorique de Shannon [122]. Pour les codes quantiques la situation est loin d'être aussi agréable pour les raisons suivantes.

- S'il est aisé de générer une matrice creuse de manière aléatoire, la construction d'un couple de matrices creuses $(\boldsymbol{H}_X, \boldsymbol{H}_Z)$ vérifiant ${}^t\boldsymbol{H}_X \cdot \boldsymbol{H}_Z = 0$ ne peut se faire par génération aléatoire.
- Si l'on veut produire des codes CSS LDPC quantiques de distance minimale linéaire en la longueur (i.e. tels que $d \geqslant \alpha n$ pour $\alpha > 0$), le code CSS doit être dégénéré (c.f. Remarque 5.2.8). En effet, dans le cas non dégénéré, la distance minimale est bornée par le poids minimal des lignes des matrices $\boldsymbol{H}_X, \boldsymbol{H}_Z$, autrement dit, pour les codes CSS non dégénérés, on ne peut pas espérer mieux qu'une distance minimale en $O(\log n)$.

Ainsi, si un code LDPC classique tiré au hasard a une distance minimale linéaire en la longueur avec une probabilité proche de 1, dans le cas quantique, la meilleure construction, due à Freedman, Meyer et Luo [71] fournit des codes LDPC quantiques dont la distance minimale est en $\Omega(\sqrt{n\sqrt{\log n}})$ mais dont la dimension est égale à 1. Si l'on demande que la dimension soit non bornée, la meilleure construction connue est due à Tillich et Zémor [147] qui fournissent des familles de codes CSS LDPC dont la dimension est en $\Omega(n)$ et la distance minimale en $\Omega(\sqrt{n})$.

L'existence de familles de codes LDPC quantiques dont la distance minimale soit en $\Omega(n^\beta)$ avec $\beta > \frac{1}{2}$ reste un problème totalement ouvert. À noter qu'en relaxant significativement la contrainte sur le poids des lignes, Bravyi et Hastings [33] parviennent à construire des codes CSS dont les poids des lignes des matrices $\boldsymbol{H}_X, \boldsymbol{H}_Z$ sont en $O(\sqrt{n})$ et dont la dimension est en $\Omega(n)$.

Comme précisé, ci-dessus, pour produire des codes quantiques LDPC, on ne peut pas se baser sur la génération aléatoire. Par ailleurs, l'étude des paramètres (dimension, distance minimale) encourage l'importation de constructions issues d'autres branches de mathématiques, en particulier la topologie algébrique pour construire nos codes. L'approche topologique a été initiée par Kitaev qui dans [93] produit une famille de codes construits à partir de complexes de chaînes provenant de pavages du tore de dimension 2. La famille de codes obtenue est de dimension 2 (c'est la dimension du premier groupe d'homologie du tore), et de distance minimale $\Omega(\sqrt{n})$.

5.4 La construction de McKay, Mitchison, Shokrollahi

Publication associée : [46].

Dans [100], les auteurs proposent la construction de codes CSS symétriques (i.e. tels que $\mathcal{C}_X = \mathcal{C}_Z$, autrement dit $\boldsymbol{H}_X = \boldsymbol{H}_Z$). On considère un groupe fini Γ muni d'un ensemble de générateurs S stable par inversion. On considère alors le graphe de Cayley $\mathfrak{G}(\Gamma, S)$ dont les sommets sont les éléments de Γ

et une arête entre deux sommets g, g' existe s'il existe $s \in S$ tel que $g' = gs$. Notons que la propriété $\ll S$ est stable par inversion $\gg$ fait que le graphe est non orienté. On note $\boldsymbol{H}(\Gamma, S)$ la matrice d'adjacence du graphe. Le but est de créer un code CSS symétrique. On cherche donc à ce que ${}^t\boldsymbol{H}(\Gamma, S) \cdot \boldsymbol{H}(\Gamma, S) = 0$.

Proposition 5.4.1 ([46, Proposition II.1])**.** *La matrice $\boldsymbol{H}(\Gamma, S)$ d'adjacence de $\mathfrak{G}(\Gamma, S)$ vérifie*

$$ {}^t\boldsymbol{H}(\Gamma, S) \cdot \boldsymbol{H}(\Gamma, S) = 0 $$

si et seulement si les conditions suivantes sont vérifiées

(i) $\sharp S$ est pair ;

(ii) Pour tout $g \in G$, il existe un nombre pair de manières d'écrire $g = st^{-1}$ avec $(s, t) \in S^2$.

Nous allons nous focaliser sur le cas où le groupe G est $\mathbf{F}_2^n$ et où S est une famille génératrice de cet espace vectoriel telle que $\sharp S = O(n)$. Il s'agit d'un contexte particulièrement agréable car, si le groupe est $\mathbf{F}_2^n$, les conditions de la Proposition 5.4.1 se ramènent simplement au fait que $\sharp S$ soit pair. En effet, comme tous les éléments sont de 2–torsion, la condition (ii) revient à dire que tout élément $x \in \mathbf{F}_2^n$ a un nombre pair d'écritures $x = s + t$ avec $s, t \in S$. Cette condition est assurée pour tout $x \neq 0$ du fait de la commutativité de $\mathbf{F}_2^n$ et pour $x = 0$ car dans ce cas il ne pourra s'écrire que $0 = s + s$ et la parité de $\sharp S$ assure la parité du nombre de telles écritures.

De cette manière, on peut construire des codes CSS de paramètres $[[N, K, D]]$ où $N = 2^n$ et $K = N - 2\mathrm{Rk}(\boldsymbol{H}(\Gamma, S))$. Un tel code est LDPC : le poids d'une ligne est égal à $\sharp S = O(n) = O(\log N)$. La difficulté est d'en estimer les paramètres K, D. Sur ce point nous sommes parvenus aux résultats suivants.

Théorème 5.4.2 ([46, Theorem V.1])**.** *Soit S une famille de vecteurs dans $\mathbf{F}_2^n$ telle que $\sharp S$ est pair et strictement positif et telle que S contienne les vecteurs de la base canonique de $\mathbf{F}_2^n$. Soit $H \in \mathfrak{M}_{n \times \sharp S}(\mathbf{F}_2)$ une matrice dont les colonnes sont les éléments de S. Soit C le code* **classique** *de longueur $\sharp S$ admettant H pour matrice de contrôle. Alors la distance minimale D du code CSS associé vérifie*

$$ D \geqslant \frac{1}{640} d n^2, $$

où d désigne la distance minimale du code classique C.

Dans un premier temps, on montre que, pour tout m pair, si $S = \mathcal{B}_m$ est la base canonique de $\mathbf{F}_2^m$, alors la dimension du code quantique associé est nulle. Autrement dit

$$ \ker \boldsymbol{H}(\mathbf{F}_2^m, \mathcal{B}_m) = \mathrm{Im}\, \boldsymbol{H}(\mathbf{F}_2^m, \mathcal{B}_m). \tag{5.1} $$

Ensuite on va considérer le revêtement du graphe de Cayley $\mathfrak{G}(\mathbf{F}_2^n, S)$:

$$ \mathfrak{G}(\mathbf{F}_2^{\sharp S}, \mathcal{B}_{\sharp S}) \longrightarrow \mathfrak{G}(\mathbf{F}_2^n, S) \tag{5.2} $$

où $\mathcal{B}_{\sharp S}$ désigne la base canonique de $\mathbf{F}_2^{\sharp S}$. Le degré de ce revêtement est égal à $2^{\sharp S - n}$. De plus, ce revêtement se trivialise au–dessus de toute boule de rayon inférieur ou égal à $\lfloor \frac{d-1}{2} \rfloor$, où d désigne la distance minimale du code classique C. C'est à dire que l'image réciproque d'une telle boule par le revêtement est isomorphe à la réunion disjointe de $2^{\sharp S - n}$ copies de cette boule.

Considérons un mot $\boldsymbol{c} \in \ker \boldsymbol{H}(\mathbf{F}_2^m, S)$. À un tel mot on fait naturellement correspondre un ensemble de sommets de $\mathfrak{G}(\mathbf{F}_2^m, S)$. L'argument de trivialisation locale du revêtement (5.2) permet de montrer que si cet ensemble de sommets est contenu dans une boule de rayon $\lfloor \frac{d-1}{2} \rfloor$, alors $\boldsymbol{c} \in \mathrm{Im}\, \boldsymbol{H}(\mathbf{F}_2^m, S)$. En quelques mots, on montre que si l'ensemble de sommets est contenu dans une telle boule, alors on peut le relever en un ensemble de sommets dans $\mathfrak{G}(\mathbf{F}_2^{\sharp S}, \mathcal{B}_{\sharp S})$ auquel correspondra un mot de $\ker \boldsymbol{H}(\mathbf{F}_2^{\sharp S}, \mathcal{B}_{\sharp S})$, or, d'après (5.1), un tel mot sera dans $\mathrm{Im}\, \boldsymbol{H}(\mathbf{F}_2^{\sharp S}, \mathcal{B}_{\sharp S})$. Pour finir, un argument d'isomorphisme local de graphe permet d'en déduire que $\boldsymbol{c} \in \mathrm{Im}\, \boldsymbol{H}(\mathbf{F}_2^m, S)$.

Par conséquent, un mot non trivial du code CSS associé à $(\mathbf{F}_2^m, S)$, i.e. un vecteur de $\ker \boldsymbol{H}(\mathbf{F}_2^m, S) \setminus \operatorname{Im} \boldsymbol{H}(\mathbf{F}_2^m, S)$ ne peut être contenu dans une boule de rayon $\lfloor \frac{d-1}{2} \rfloor$. Des arguments combinatoires permettent de déduire de ce fait que son poids est minoré par $\frac{1}{640} dn^2$.

On montre ainsi que les codes considérés ont une distance minimale en $\Omega(\log^2 N)$ où $N = 2^m$ désigne leur longueur alors que le poids des lignes de $\boldsymbol{H}(\mathbf{F}_2^m, S)$ est en $O(\log N)$. En particulier de tels codes quantiques sont dégénérés. Notons enfin que la borne inférieure $\Omega(\log^2 N)$ est très pessimiste. En particulier, dans le cas où le code classique associé est le code de répétition. Autrement dit, dans le cas où m est impair et $S = \mathcal{B}_m \cup \{(1, \ldots, 1)\}$ où $\mathcal{B}_m$ désigne la base canonique de $\mathbf{F}_2^m$, nous avons obtenu les paramètres exacts de ces codes par des procédés algébriques pour lesquels je revoie le lecteur à [46].

Théorème 5.4.3. *Le code CSS associé au couple $(\mathbf{F}_2^m, S)$ où m est impair et $S = \mathcal{B}_m \cup \{(1, \ldots, 1)\}$ ($\mathcal{B}_m$ désigne la base canonique de $\mathbf{F}_2^m$) a pour paramètres*

$$[[N = 2^m, K = 2^{\frac{m+1}{2}}, D = 2^{\frac{m-1}{2}}]].$$

Autrement dit, la famille des codes CSS associée aux codes classiques de répétition donne des codes de longueur N dont les dimensions et distances minimales sont en $\Omega(\sqrt{N})$.

5.5 Produits tensoriels itérés de complexes de chaînes et de codes CSS

Publication associée : [10].

Dans cette dernière section, je présente les résultats d'un travail en collaboration avec Benjamin Audoux [10]. Le travail était motivé par une construction figurant dans [9] : une construction de codes quantiques basés sur l'homologie de Khovanov [150] de nœuds et d'entrelacs. Il s'avère que certaines constructions itératives figurant dans cet article pouvaient s'obtenir par puissances tensorielles itérées d'un certain complexe de chaînes.

5.5.1 Produits tensoriels de complexes de chaînes

Rappelons que, étant donnés deux complexes de chaînes $C_\bullet, D_\bullet$:

$$\cdots \xrightarrow{\partial} C_{i-1} \xrightarrow{\partial} C_i \xrightarrow{\partial} C_{i+1} \xrightarrow{\partial} \cdots \quad \text{et} \quad \cdots \longrightarrow D_{i-1} \xrightarrow{\partial} D_i \xrightarrow{\partial} D_{i+1} \xrightarrow{\partial} \cdots$$

où les C_i et les D_i sont des $\mathbf{F}_2$–espaces vectoriels de dimension finie, on définit le complexe $(C \otimes D)_\bullet$ comme le complexe défini en degré k par

$$(C \otimes D)_k \stackrel{\text{def}}{=} \bigoplus_{i+j=k} C_i \otimes D_j$$

et dont la différentielle est définie par

$$\partial : \left\{ \begin{array}{ccc} C_i \otimes D_j & \longrightarrow & C_{i+1} \otimes D_j \oplus C_i \otimes D_{j+1} \\ c_i \otimes d_j & \longmapsto & \partial(c_i) \otimes d_j + c_i \otimes \partial(d_j) \end{array} \right.$$

et prolongée par linéarité.

Remarque 5.5.1. Notons que dans tout ce qui suit les complexes de chaînes sont définis sur $\mathbf{F}_2$, ce qui simplifie l'expression de la différentielle pour les produits tensoriels dans la mesure où l'on n'a pas besoin de se soucier des signes.

5.5.2 Produits tensoriels de codes CSS

De la notion de produit tensoriel de complexes de chaînes, on dérive plusieurs notions de produit tensoriel de codes quantiques. Nous allons commencer par une définition naturelle puis allons la modifier sensiblement afin d'en améliorer les performances.

La définition la plus naturelle consiste, partant de deux codes CSS $\mathscr{C}, \mathscr{D}$ décrits par des couples de matrices $(\boldsymbol{H}_X^{\mathscr{C}}, \boldsymbol{H}_Z^{\mathscr{C}})$ et $(\boldsymbol{H}_X^{\mathscr{D}}, \boldsymbol{H}_Z^{\mathscr{D}})$, à considérer les complexes de chaînes

$$C_{-1} \xrightarrow{{}^t\boldsymbol{H}_X^{\mathscr{C}}} C_0 \xrightarrow{\boldsymbol{H}_Z^{\mathscr{C}}} C_1 \qquad \text{et} \qquad D_{-1} \xrightarrow{{}^t\boldsymbol{H}_X^{\mathscr{D}}} D_0 \xrightarrow{\boldsymbol{H}_Z^{\mathscr{D}}} D_1.$$

On considère ensuite le produit tensoriel de ces derniers et, comme la partie qui nous intéresse est l'homologie en degré 0, on se focalise sur les termes de degrés $-1, 0$ et 1.

$$\begin{array}{c} C_{-1} \otimes D_0 \oplus C_0 \otimes D_{-1} \\ \Big\downarrow {}^t\boldsymbol{H}_X^{\mathscr{C}\otimes\mathscr{D}} \\ C_{-1} \otimes D_1 \oplus C_0 \otimes D_0 \oplus C_1 \otimes D_{-1} \\ \Big\downarrow \boldsymbol{H}_Z^{\mathscr{C}\otimes\mathscr{D}} \\ C_0 \otimes D_1 \oplus C_1 \otimes D_0. \end{array} \tag{5.3}$$

où les matrices $\boldsymbol{H}_X^{\mathscr{C}\otimes\mathscr{D}}, \boldsymbol{H}_Z^{\mathscr{C}\otimes\mathscr{D}}$ ont les représentations par blocs suivantes

$$\boldsymbol{H}_X^{\mathscr{C}\otimes\mathscr{D}} \stackrel{\text{def}}{=} \begin{pmatrix} \boldsymbol{I}_{C_{-1}} \otimes {}^t\boldsymbol{H}_Z^{\mathscr{D}} & \boldsymbol{H}_X^{\mathscr{C}} \otimes \boldsymbol{I}_{D_0} & (0) \\ (0) & \boldsymbol{I}_{C_0} \otimes \boldsymbol{H}_X^{\mathscr{D}} & {}^t\boldsymbol{H}_Z^{\mathscr{C}} \otimes \boldsymbol{I}_{D_{-1}} \end{pmatrix}$$

$$\boldsymbol{H}_Z^{\mathscr{C}\otimes\mathscr{D}} \stackrel{\text{def}}{=} \begin{pmatrix} {}^t\boldsymbol{H}_X^{\mathscr{C}} \otimes \boldsymbol{I}_{D_1} & \boldsymbol{I}_{C_0} \otimes \boldsymbol{H}_Z^{\mathscr{D}} & (0) \\ (0) & \boldsymbol{H}_Z^{\mathscr{C}} \otimes \boldsymbol{I}_{D_0} & \boldsymbol{I}_{C_1} \otimes {}^t\boldsymbol{H}_X^{\mathscr{D}} \end{pmatrix}.$$

Le code $\mathscr{C} \otimes \mathscr{D}$ est alors défini par le couple de matrices $(\boldsymbol{H}_X^{\mathscr{C}\otimes\mathscr{D}}, \boldsymbol{H}_Z^{\mathscr{C}\otimes\mathscr{D}})$.

Remarque 5.5.2. Notons que si l'on prend les matrices $\boldsymbol{H}_X^{\mathscr{C}}, \boldsymbol{H}_X^{\mathscr{D}}, \boldsymbol{H}_Z^{\mathscr{C}}, \boldsymbol{H}_Z^{\mathscr{D}}$ de rang plein alors les complexes de chaînes associés sont réduits (voir § 5.2.4), mais les matrices $\boldsymbol{H}_X^{\mathscr{C}\otimes\mathscr{D}}, \boldsymbol{H}_Z^{\mathscr{C}\otimes\mathscr{D}}$ ne le seront pas. Dans l'article [10] nous donnons un procédé non canonique de réduction du complexe consistant essentiellement à supprimer les lignes redondantes de ces matrices afin de pallier de problème. Ce procédé permet entre autre de mieux contrôler la croissance des paramètres lorsque l'on considère la suite des puissances tensorielles itérées d'un code CSS. Je renvoie le lecteur à l'article pour ce point technique.

Commençons par un énoncé élémentaire sur les paramètres d'un tel produit tensoriel.

Proposition 5.5.3. *Soient $\mathscr{C}, \mathscr{D}$ deux codes CSS décrits par des couples de matrices $(\boldsymbol{H}_X^{\mathscr{C}}, \boldsymbol{H}_Z^{\mathscr{C}})$ et $(\boldsymbol{H}_X^{\mathscr{D}}, \boldsymbol{H}_Z^{\mathscr{D}})$ et de paramètres respectifs $[[n_{\mathscr{C}}, k_{\mathscr{C}}, d_{\mathscr{C}}]]$ et $[[n_{\mathscr{D}}, k_{\mathscr{D}}, d_{\mathscr{D}}]]$. Notons*

$$0 \longrightarrow C_{-1} \xrightarrow{{}^t\boldsymbol{H}_X^{\mathscr{C}}} C_0 \xrightarrow{\boldsymbol{H}_Z^{\mathscr{C}}} C_1 \longrightarrow 0 \quad \text{et} \quad 0 \longrightarrow D_{-1} \xrightarrow{{}^t\boldsymbol{H}_X^{\mathscr{D}}} D_0 \xrightarrow{\boldsymbol{H}_Z^{\mathscr{D}}} D_1 \longrightarrow 0$$

les complexes de chaînes associés. Alors les paramètres du code CSS $\mathscr{C} \otimes \mathscr{D}$ vérifient :

$$\begin{aligned} n_{\mathscr{C}\otimes\mathscr{D}} &= n_{\mathscr{C}} n_{\mathscr{D}} + \dim C_{-1} \dim D_1 + \dim C_1 \dim D_{-1}, \\ k_{\mathscr{C}\otimes\mathscr{D}} &= k_{\mathscr{C}} k_{\mathscr{D}}. \end{aligned}$$

Démonstration. Le formule pour la longueur se déduit de la description du produit tensoriel (5.3). Quant à la formule pour la dimension, c'est une conséquence directe de la formule de Künneth [156, Theoreme 3.6.3]. □

Un résultat sur la distance minimale

L'estimation de la distance minimale est un point bien plus délicat, pour lequel nous avons obtenu le résultat suivant pour lequel nous devons tout d'abord introduire une définition.

Définition 5.5.4. Étant donné un ensemble de vecteurs $\Omega \subseteq \mathbf{F}_2^n$, on définit

$$\mathrm{Rec}(\Omega) \stackrel{\text{def}}{=} \max_{i=1}^{n} \sharp\{v \in \Omega \mid v_i \neq 0\}.$$

Autrement dit, si Ω est l'ensemble des lignes d'une matrice, $\mathrm{Rec}(\Omega)$ est le poids de Hamming maximal d'une colonne de cette matrice.

Théorème 5.5.5 ([10, Theorem 2.8])**.** *Soit $\mathscr{C}$ un code CSS décrit par un couple de matrices $(\boldsymbol{H}_X, \boldsymbol{H}_Z)$ toutes deux de rang plein. Notons*

$$C_\bullet : \qquad 0 \longrightarrow C_{-1} \xrightarrow{{}^t\boldsymbol{H}_X^{\mathscr{C}}} C_0 \xrightarrow{\boldsymbol{H}_Z^{\mathscr{C}}} C_1 \longrightarrow 0$$

le complexe de chaînes associé. Soient $g_1, \ldots, g_k$ et $g_1^*, \ldots, g_k^*$ des familles de vecteurs respectivement dans $\ker \boldsymbol{H}_Z^{\mathscr{C}}$ et $\ker \boldsymbol{H}_X^{\mathscr{C}}$ tels que les classes d'homologies $[g_1], \ldots, [g_k]$ (resp. les classes de cohomologie $[g_1^*], \ldots, [g_k]^*$) forment une base de $H_0(C_\bullet)$ (resp. de $H^0(C_\bullet)$) et que

$$\forall 1 \leqslant i, j \leqslant k, \qquad \langle g_i, g_j^* \rangle = \delta_{ij}.$$

Si pour tout $1 \leqslant j_0 \leqslant k$, il existe $\Omega_{j_0} \subseteq [g_{j_0}^*] = g_{j_0}^* + Im\,{}^t\boldsymbol{H}_Z^{\mathscr{C}}$ et $\Omega_{j_0}^* \subseteq [g_{j_0}] = g_{j_0} + Im\,{}^t\boldsymbol{H}_X^{\mathscr{C}}$ telles que

(i) $\sharp\Omega_{j_0}, \sharp\Omega_{j_0}^* \geqslant N$;

(ii) $\mathrm{Rec}(\Omega_{j_0}), \mathrm{Rec}(\Omega'_{j_0}) \leqslant K$,

alors pour tout code CSS $\mathscr{D}$, la distance minimale de $\mathscr{C} \otimes \mathscr{D}$ vérifie

$$d_{\mathscr{C}\otimes\mathscr{D}} \geqslant \left\lceil \frac{N}{K} d_{\mathscr{D}} \right\rceil.$$

Remarque 5.5.6. En réalité l'énoncé qui précède peut donner séparément des bornes inférieures sur $d^X_{\mathscr{C}\otimes\mathscr{D}}$ et $d^Z_{\mathscr{C}\otimes\mathscr{D}}$ à savoir

$$d^Z_{\mathscr{C}\otimes\mathscr{D}} \geqslant \left\lceil \frac{\min_j\{\sharp\Omega_j\}}{\max_j\{\mathrm{Rec}(\Omega_j)\}} d^Z_{\mathscr{D}} \right\rceil, \qquad d^X_{\mathscr{C}\otimes\mathscr{D}} \geqslant \left\lceil \frac{\min_j\{\sharp\Omega'_j\}}{\max_j\{\mathrm{Rec}(\Omega^*_j)\}} d^X_{\mathscr{D}} \right\rceil. \tag{5.4}$$

Remarque 5.5.7. Dans [10], l'énoncé est formulé en termes des codes classiques $\mathcal{C}_1, \mathcal{C}_2$ tels que $\mathcal{C}_2 \subseteq \mathcal{C}_1^\perp$ décrivant $\mathscr{C}$. J'ai choisi de le reformuler ainsi pour être plus cohérent avec les notations introduites dans ce chapitre et d'éviter certaines confusions de notations. Afin de reconnecter avec les notations de l'article, il faut comprendre que

$$\mathcal{C}_1 = \left(\ker \boldsymbol{H}_Z^{\mathscr{C}}\right)^\perp = \mathrm{Im}\,{}^t\boldsymbol{H}_Z^{\mathscr{C}}$$
$$\mathcal{C}_2 = \mathrm{Im}\,{}^t\boldsymbol{H}_X^{\mathscr{C}} = \left(\ker \boldsymbol{H}_X^{\mathscr{C}}\right)^\perp.$$

Conséquences

Le théorème 5.5.5 est d'apparence technique et semble difficile à appliquer. On peut toutefois en énoncer un certain nombre de conséquences intéressantes.

Corollaire 5.5.8. *Pour tout couple de codes quantiques $\mathscr{C}, \mathscr{D}$, décrits par des couples de matrices de rang plein, on a*

$$d_{\mathscr{C}\otimes\mathscr{D}} \geqslant \max(d_{\mathscr{C}}, d_{\mathscr{D}}).$$

Démonstration. On applique le théorème 5.5.5 dans le cas où $N = K = 1$ en prenant dans chaque classe de (co)homologie $[g_j]$ (resp. $[g_j^*]$) un représentant arbitraire. □

On peut même aller plus loin.

Proposition 5.5.9. *Pour toute paire de codes quantiques binaires $\mathscr{C}, \mathscr{D}$ décrits par des couples de matrices de rang pleins tels qu'aucune de ces matrices n'admet de colonne de 0, alors*

$$d_{\mathscr{C}\otimes\mathscr{D}} \geqslant 2\max(d_{\mathscr{C}}, d_{\mathscr{D}}).$$

Démonstration. L'idée ici est de prendre pour les Ω_{j_0} (resp. Ω'_{j_0}) toute la classe d'homologie (resp. cohomologie) de g_{j_0} (resp. de g'_{j_0}). Le fait que l'on soit sur $\mathbf{F}_2$ fait que ces classes de cohomologie sont des espaces affines et, par conséquent si une matrice a pour lignes l'ensemble des vecteurs d'un tel espace affine, alors le poids de chaque colonne est égal à la moitié de la longueur de la colonne. En effet, une telle colonne décrit l'ensemble des évaluations possibles de la forme linéaire de projection sur la j_0–ème coordonnée restreinte à l'espace affine $[g_{j_0}] = g_{j_0} + \operatorname{Im} {}^t\boldsymbol{H}_X^{\mathscr{C}}$. Ces évaluations ne peuvent être toutes égales à 0 ou toutes égales à 1 par hypothèse sur $\boldsymbol{H}_X$. Ainsi, par linéarité de l'application, le nombre de 1 est donc égal au nombre de 0 et donc, en prenant $N = [g_{j_0}]$ et $K = \frac{N}{2}$, on obtient le résultat attendu. □

Ce dernier résultat est particulièrement intéressant pour la raison suivante. Si on considère un code CSS $\mathscr{C}$ et que l'on en considère la suite des puissances tensorielles $\mathscr{C}^{\otimes 2}, \mathscr{C}^{\otimes 3}, \ldots$. On vérifie la longueur de la suite $\mathscr{C}^{\otimes n}$ croît plus vite que n_0^n où n_0 est la longueur de $\mathscr{C}$. Par ailleurs, on peut vérifier que le poids des lignes des matrices correspondantes croît en $O(n)$. Autrement dit, cette suite de codes CSS est LDPC. De plus sa distance minimale est minorée par 2^n. Autrement dit, même si $\mathscr{C}$ n'est pas un code dégénéré, à partir d'un certain rang les codes $\mathscr{C}^{\otimes n}$ le sont.

La construction de Tillich Zémor revisitée

La construction de Tillich–Zémor [147] peut se ré-interpréter en termes de produits tensoriels de deux complexes relativement simples. En effet, prenons deux codes LDPC classiques de matrices de contrôle $\boldsymbol{H}_1, \boldsymbol{H}_2$. Considérons les complexes

$$C_\bullet : \quad 0 \longrightarrow C_0 \xrightarrow{\boldsymbol{H}_1} C_1 \qquad \text{et} \qquad D_\bullet : \quad D_{-1} \xrightarrow{{}^t\boldsymbol{H}_2} D_0 \longrightarrow 0\,. \tag{5.5}$$

Ces complexes fournissent des codes CSS triviaux mais leur produit tensoriel fournit un code CSS de longueur

$$N = \dim C_0 \dim D_0 + \dim C_1 \dim D_{-1} = n_1 n_2 + (n_1 - k_1)(n_2 - k_2)$$

et dont la dimension est

$$K = k_1 k_2.$$

Par ailleurs, les codes CSS triviaux associés à $C_\bullet, D_\bullet$ ont des couples de distances (d^X, d^Z) respectivement égaux à $(1, d_1)$ et $(d_2, 1)$. La remarque 5.5.6 permet alors de montrer que le code CSS associé au produit tensoriel des deux complexes triviaux a pour couple de distances $(\geqslant d_1, \geqslant d_2)$, sa distance minimale est donc minorée par $\min(d_1, d_2)$. Si l'on prend des codes LDPC aléatoires, leur distance est en $\Omega(n)$ avec une probabilité proche de 1. On obtient ainsi l'existence de codes CSS LDPC de longueur N, dimension $\Omega(N)$ et distance minimale $\Omega(\sqrt{N})$.

Des exemples

Dans [10] nous proposons trois familles de codes LDPC quantiques obtenues par puissances tensorielles itérées pour lesquelles nous sommes parvenus à appliquer le théorème 5.5.5.

— Une construction à partir de codes de Reed–Muller binaires

— Une construction à partir de codes binaires cycliques

— Une construction à partir de géométrie finie.

Pour chacune de ces constructions, on peut extraire des familles de codes quantiques dont la distance minimale est en $\Omega(n^{1/2-\varepsilon})$ pour tout $\varepsilon > 0$.

Dans ce qui suit, j'ai choisi de vous présenter l'exemple basée sur de la géométrique finie. Ce n'est pas celui qui donne les meilleurs paramètres, la construction à base de codes de Reed–Muller donne des codes dont la dimension tend vers l'infini alors que les codes que je vais présenter sont tous de dimension 1.

Codes à partir de géométrie finie Soit $q = 2^s$ pour un certain $s > 0$. On considère le plan projectif $\mathbf{P}^2(\mathbf{F}_q)$ dont on numérote les éléments arbitrairement de 1 à q^2+q+1. Ainsi, l'espace $\mathbf{F}_2^{q^2+q+1}$ est en bijection avec l'ensemble des parties de $\mathbf{P}^2(\mathbf{F}_q)$ et, afin de simplifier les notations, on pourra s'autoriser à dire qu'un point $P \in \mathbf{P}^2(\mathbf{F}_q)$ appartient à un vecteur $\boldsymbol{v} \in \mathbf{F}_2^{q^2+q+1}$ pour dire que $\boldsymbol{v}$ a un 1 à la position correspondant à P.

Dans ce contexte, on introduit deux codes classiques de longueur q^2+q+1 :

— $\mathcal{C}_{\text{droites}}$ engendré par les droites de $\mathbf{P}^2(\mathbf{F}_q)$;

— $\mathcal{C}_{\text{cartes}}$ engendré par les cartes affines, autrement dit les complémentaires des droites de $\mathbf{P}^2(\mathbf{F}_q)$.

Lemme 5.5.10. *On a* $\mathcal{C}_{\text{cartes}} \subseteq \mathcal{C}_{\text{droites}}^{\perp}$.

Démonstration. Il suffit de vérifier que $\langle \boldsymbol{d}, \boldsymbol{c}\rangle = 0$ pour toute droite $\boldsymbol{d}$ et toute carte affine $\boldsymbol{c}$. Notons qu'un tel produit est égal au cardinal de l'intersection de $\boldsymbol{c}$ et $\boldsymbol{d}$ modulo 2. Or une telle intersection est soit vide, soit égale à une droite affine dont le cardinal est pair. □

Un tel couple de codes donne donc un code CSS $\mathscr{C}$ en considérant un couple de matrices $(\boldsymbol{H}_X, \boldsymbol{H}_Z)$ telles que $\boldsymbol{H}_Z$ est une matrice de parité de $\mathcal{C}_{\text{droites}}$ et $\boldsymbol{H}_X$ une matrice génératrice de $\mathcal{C}_{\text{cartes}}$. Par ailleurs, on peut prouver que pour toute droite L de $\mathbf{P}^2(\mathbf{F}_q)$

$$\mathcal{C}_{\text{droites}} = \mathcal{C}_{\text{cartes}} \oplus \langle L \rangle.$$

De fait, le code CSS associé est de dimension 1 et, voyant $\mathcal{C}_{\text{droites}}$ comme l'espace des cycles $\ker \partial$ et $\mathcal{C}_{\text{cartes}}$ comme l'espace des bords, alors, l'ensemble Ω des droites de $\mathbf{P}^2(\mathbf{F}_q)$ est un sous-ensemble de l'unique classe d'homologie non-triviale. Il vérifie

$$\sharp\Omega = q^2+q+1 \qquad \text{et} \qquad \operatorname{Rec}(\Omega) = q+1.$$

En effet, si les droites de $\mathbf{P}^2(\mathbf{F}_q)$ forment les lignes d'une matrice, le poids d'une colonne n'est autre que le nombre de points passant par une droite donnée qui n'est autre que $q+1$. En utilisant le théorème 5.5.5 ainsi que la remarque 5.5.6, on en déduit que

$$d^Z_{\mathscr{C}^{\otimes n}} \geqslant \left\lceil \frac{q^2+q+1}{q+1} \right\rceil^n.$$

Enfin, on montre que l'on peut obtenir la même minoration pour la distance en X pour la simple raison que la cohomologie correspond au quotient $\mathcal{C}_{\text{cartes}}^{\perp}/\mathcal{C}_{\text{droites}}^{\perp}$ or, $\Omega \subseteq \mathcal{C}_{\text{cartes}}^{\perp} \setminus \mathcal{C}_{\text{droites}}^{\perp}$. En effet, on a déjà signalé qu'une droite est bien orthogonale à toute carte affine mais une droite n'est orthogonale à aucune droite.

Une analyse fine du comportement de la longueur des puissances tensorielles itérées améliorée via un processus de réduction du complexe de chaînes à chaque étape permet de produire des familles de codes CSS LDPC dont les paramètres vérifient :

$$\left[\!\left[K\left(q^2+q+1+q'\right)^n,\ 1,\ \geqslant \left(\frac{q^2+q+1}{q+1}\right)^n \right]\!\right]$$

pour des constantes K, q' ne dépendent que de q. On a une distance minimale en $\circ(\sqrt{N})$ où N désigne la longueur. Toutefois, en faisant tendre q vers l'infini, on peut montrer que l'on peut obtenir une distance minimale en $\Omega(n^{1/2-\varepsilon})$ et ce pour tout $\varepsilon > 0$.

Conclusion et perspectives

Mes principales sources d'intérêt sont l'arithmétique, la géométrique algébrique effective le codage et la cryptographie. Ce sont ces thèmes que je souhaite continuer d'explorer dans les années à venir. Voici plus précisément quelques sujets ouverts que j'espère trouver le temps d'étudier dans le futur.

5.6 Cryptographie à base de codes

Mon but est de rester sur le qui-vive et de suivre l'actualité dans ce domaine. Continuer à rechercher des méthodes de cryptanalyse efficace car je suis convaincu que l'on ne comprend jamais aussi bien un schéma cryptographique que lorsque l'on a cherché à l'attaquer.

Sur l'utilisation du produit $\star$, de nouvelles attaques pourraient voir le jour dans les prochaines années. Cette opération d'apparence simple s'est avérée être un outil redoutable pour attaquer des propositions à base de codes algébriques. Parmi ces dernières une résiste encore et toujours à l'envahisseur : les codes alternants de haut rendement, qui sont pourtant distinguables de codes aléatoires grâce au produit $\star$ mais aucun algorithme efficace n'a été développé à partir de ce distingueur. À noter qu'un tel algorithme donnerait lieu à une attaque sur le schéma de signature de Courtois Finiasz et Sendrier [40]. Par ailleurs même si les codes de Goppa utilisés dans le schéma de McEliece standard sont de bien plus bas rendement que ceux qui sont distinguables, un tel algorithme représenterait tout de même une avancée significative dans l'analyse de la sécurité du schéma de McEliece historique.

5.7 Produits $\star$ d'espaces vectoriels et de codes

5.7.1 Freiman toujours

De manière évidente, les travaux menés sur la version multiplicative du théorème de Freiman ne sont qu'un début. L'analogie avec le théorème de Freiman dans le cas additif encourage à établir la conjecture suivante :

Conjecture 5.7.1. Soit K un corps parfait et F une extension de type fini de K. Soit $S \subseteq F$ un K–espace vectoriel de dimension finie tel que $1 \in S$ et que S engendre F sur K et

$$\dim S^2 = 2 \dim S - 1 + \gamma \qquad \text{avec} \qquad \gamma \leqslant \dim S - 3,$$

alors F est de degré de transcendance 1 sur K, de genre $\leqslant \gamma$ et S est contenu dans un espace de Riemann Roch.

Dans le chapitre 4, on a démontré le résultat sur le degré de transcendance et la conjecture dans le cas $\gamma \leqslant 1$. Aller plus loin dans la démonstration de cette conjecture reste un objectif. À noter également que, si nous ne sommes pas parvenus à démontrer nos résultats dans le cas où K n'est pas parfait, nous n'avons pas non plus trouvé de contre-exemple dans ce cas. Le problème reste donc largement ouvert dans le cas d'un corps de base quelconque.

Deux autre directions pourraient également être explorées. La première concerne le cas non symétrique, à savoir la classification des couples d'espaces S, T tels que $\dim ST = \dim S + \dim T - 1 + \gamma$. La seconde consiste à étudier les généralisations en degré de transcendance supérieure. Par exemple, la classification des espaces S dans un corps de degré de transcendance 2 vérifiant

$$\dim S^2 = 3 \dim S - 3 + \eta$$

pour de petites valeurs de η serait intéressante.

5.7.2 Extension aux codes géométriques et application au calcul multiparti

Au delà des espaces de dimension finie dans des corps de fonctions, je suis bien sûr tenté de revenir aux codes, i.e. à des problèmes de combinatoire « multiplicative » dans l'anneau produit $\mathbf{F}_q^n$. La question des codes vérifiant

$$\dim \mathcal{C} \star \mathcal{C} = 2 \dim \mathcal{C} - 1$$

a été traitée dans [112] et l'étude de codes de genre combinatoire supérieur serait intéressante. On pourrait espérer montrer que, sauf cas dégénérés a bien identifier, tous les codes de genre combinatoire suffisamment petit de courbes de genre inférieur au genre combinatoire du code. Par ailleurs il serait intéressant de savoir si un système d'équations de la courbe peut s'obtenir à partir de la seule connaissance des codes $\mathcal{C}$ et $\mathcal{C}^2$. En effet, considérons la suite exacte naturelle

$$0 \longrightarrow I_2 \longrightarrow S^2\mathcal{C} \longrightarrow C \star C \longrightarrow 0$$

où $S^2\mathcal{C}$ désigne le produit symétrique $\mathcal{C} \otimes \mathcal{C}/\langle \boldsymbol{a} \otimes \boldsymbol{b} - \boldsymbol{b} \otimes \boldsymbol{a} \mid \boldsymbol{a}, \boldsymbol{b} \in \mathcal{C} \rangle$ et I_2 désigne le noyau du morphisme canonique $S^2\mathcal{C} \to \mathcal{C} \star \mathcal{C}$. Le noyau I_2 décrit l'espace de formes quadratiques en $\dim \mathcal{C}$ variables s'annulant en les colonnes d'une matrice génératrice de $\mathcal{C}$, et, dans le cas où $\mathcal{C}$ est un code géométrique provenant d'une courbe $\mathscr{X}$, alors, sous certaines hypothèses sur le degré du diviseur, l'intersection des quadriques associées aux éléments de I_2 est une variété contenant un modèle de $\mathscr{X}$. Une question qui reste assez largement ouverte est : sous quelles conditions cette variété est égale à $\mathscr{X}$? Par ailleurs, dans les cas de non–égalité, à quoi correspondent les autres points de la variété ?

Concluons cette section en remarquant que la recherche et la classification de codes dont le carré est de petite dimension aurait d'intéressantes retombées dans le domaine du partage de secret sécurisé et du calcul multiparti dans lequel ce type de codes est particulièrement recherché.

5.8 Codes géométriques

5.8.1 Nouvelles constructions

Dans la continuité des travaux effectués durant ma thèse et mes post docs puis de ceux effectués plus récemment avec les collègues de l'ANR Manta, la construction et l'étude de codes provenant de surfaces algébriques et variétés de dimension supérieure reste un centre d'intérêt pour moi.

J'aimerais en particulier analyser les performances de ce type d'objets par rapport à des problématiques plus modernes de codage comme les codes localement recouvrables ou les codes localement décodables qui ont émergé dans la dernière décennie et représentent aujourd'hui un domaine de recherche très actif avec de nombreuses applications au stockage de données distribuées.

5.8.2 Constructions efficaces

Si Tsfasman Vlăduţ et Zink ont prouvé l'existence de codes géométriques dépassant la borne de Gilbert Varshamov, la question de la construction efficace de tels codes reste un problème largement ouvert. En collaboration avec les membres de l'équipe Max (calcul formel) du LIX, nous avons pour projet d'avancer dans cette direction : développer des algorithmes rapides pour calculer des bases de codes et/ou d'espaces de Riemann Roch sur des courbes provenant de tours récursives.

5.8.3 Décodage

Mon intérêt pour les aspects algorithmiques du codage algébrique et géométrique a toujours été conséquent et je souhaite avancer dans la compréhension des algorithmes récents tels que le *Power decoding* [127, 125], un algorithme de décodage des codes Reed–Solomon et des codes géométriques qui peut corriger autant d'erreurs qu'avec les algorithmes de Sudan et Guruswami Sudan [141, 78] mais peut échouer avec une faible probabilité. Toutefois, les considérations sur la probabilité d'échec restent heuristiques et la classification des cas d'échec reste un problème ouvert. La thèse d'Isabella Panaccione qui a démarré en octobre 2018 porte entre autre sur cette question.

5.9 Et aussi...

Pour conclure, je cite quelques directions de recherche que j'estime plus « exploratoires ».

5.9.1 Codes en métrique rang

Dans les dernières années, j'ai éprouvé un intérêt croissant pour les codes en métrique rang et leurs applications à la cryptographie et au *network coding*. Si mes contributions dans le domaine se limitent à la publication [39] j'espère y contribuer de manière plus significative à l'avenir. J'ai déjà investi beaucoup d'énergie, en vain pour le moment sur deux questions sur lesquelles je ne désespère pas de pouvoir donner un jour des éléments de réponses. Peut-on construire d'autres familles de codes algébriques que les codes de Gabidulin ? Si les codes de Reed–Solomon ont leur analogue en métrique rang, qu'en est-il des codes de Reed–Muller ou des codes géométriques ? et enfin : existe-t-il un algorithme de décodage probabiliste polynomial permettant de corriger plus de $\left\lfloor \frac{d-1}{2} \right\rfloor$ erreurs pour des codes de Gabidulin de distance minimale d ?

5.9.2 Codes LDPC quantiques

Ici, une vaste question que tous les spécialistes du domaine se posent : existe-t-il des codes LDPC quantiques dont la distance minimale est meilleure que $\widetilde{O}(\sqrt{n})$? J'avoue n'avoir en définitive aucune intuition concernant la réponse la plus plausible mais ce domaine mêlant codage, combinatoire, topologie et algèbre homologique continue à me fasciner et là aussi, je ne désespère pas de pouvoir en dire plus un jour.

Bibliographie

[1] C. Aguilar Melchor, N. Aragon, P. Barreto, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, S. Gueron, T. Güneysu, R. Misoczki, E. Persichetti, N. Sendrier, J.-P. Tillich, and G. Zémor. BIKE. First round submission to the NIST post-quantum cryptography call, Nov. 2017.

[2] C. Aguilar Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J. Deneuville, P. Gaborit, E. Persichetti, and G. Zémor. HQC, Nov. 2017. NIST Round 1 submission for Post-Quantum Cryptography.

[3] C. Aguilar Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, and G. Zémor. Rank quasi cyclic (RQC). First round submission to the NIST post-quantum cryptography call, Nov. 2017.

[4] M. Albrecht, C. Cid, K. G. Paterson, C. J. Tjhai, and M. Tomlinson. NTS-KEM. First round submission to the NIST post-quantum cryptography call, Dec. 2017.

[5] M. Alekhnovich. More on average case vs approximation complexity. *Computational Complexity*, 20(4) :755–786, 2011.

[6] Y. Aubry. Algebraic geometric codes on surfaces. Unpublished, available on the author's webpage, 1992.

[7] Y. Aubry. Reed-Muller codes associated to projective algebraic varieties. In *Coding theory and algebraic geometry (Luminy, 1991)*, volume 1518 of *Lecture Notes in Math.*, pages 4–17. Springer, Berlin, 1992.

[8] Y. Aubry and M. Perret. Coverings of singular curves over finite fields. *Manuscripta Math.*, 88(1) :467–478, 1995.

[9] B. Audoux. An application of Khovanov homology to quantum codes. *Ann. Inst. Henri Poincaré D, Comb. Phys. Interact.*, 1(2) :185–223, 2014.

[10] B. Audoux and A. Couvreur. On tensor products of CSS codes. To appear in Annales de l'Institut Henri Poincaré D, Combinatorics, Physics and their interactions. ArXiv :1512.07081., 2019.

[11] C. Bachoc, A. Couvreur, and G. Zémor. Towards a function field version of Freiman's theorem. *Algebraic Combin.*, 1(4) :501–521, 2018.

[12] C. Bachoc, C. Serra, and G. Zémor. An analogue of Vosper's theorem for extension fields. *Math. Proc. Philos. Soc.*, 163 :423–452, 2017.

[13] C. Bachoc, O. Serra, and G. Zémor. Revisiting Kneser's theorem for field extensions. To appear in Combinatorica, ArXiv :math/1510.01354, 2015.

[14] M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, and D. Schipani. Enhanced public key security for the McEliece cryptosystem. *J. Cryptology*, 29(1) :1–27, 2016.

[15] E. Ballico. Codes coming from a blowing up of the plane. *Afr. Mat.*, 24(1) :93–96, 2013.

[16] G. Banegas, P. S. Barreto, B. O. Boidje, P.-L. Cayrel, G. N. Dione, K. Gaj, C. T. Gueye, R. Haeussler, J. B. Klamti, O. N'diaye, D. T. Nguyen, E. Persichetti, and J. E. Ricardini. DAGS : Key encapsulation for dyadic GS codes. `https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/submissions/DAGS.zip`, Nov. 2017. First round submission to the NIST post-quantum cryptography call.

[17] M. Bardet, É. Barelli, O. Blazy, R. Canto Torres, A. Couvreur, P. Gaborit, A. Otmani, N. Sendrier, and J.-P. Tillich. BIG QUAKE. `https://bigquake.inria.fr`, Nov. 2017. NIST Round 1 submission for Post-Quantum Cryptography.

[18] E. Barelli. On the security of some compact keys for McEliece scheme. In *WCC Workshop on Coding and Cryptography*, Sept. 2017.

[19] E. Barelli. *On the security of short McEliece keys from algebraic and algebraic geometry codes with automorphisms*. PhD thesis, École Polytechnique X ; Université Paris Saclay, 2018.

[20] E. Barelli and A. Couvreur. An efficient structural attack on NIST submission DAGS. In T. Peyrin and S. Galbraith, editors, *Advances in Cryptology - ASIACRYPT'18*, volume 11272 of *LNCS*, pages 93–118. Springer, Dec. 2018.

[21] A. Becker, A. Joux, A. May, and A. Meurer. Decoding random binary linear codes in $2^{n/20}$: How $1 + 1 = 0$ improves information set decoding. In *Advances in Cryptology - EUROCRYPT 2012*, LNCS. Springer, 2012.

[22] P. Beelen and T. Høholdt. *The Decoding of Algebraic Geometry Codes*, volume 5, pages 49–98. World Scientific, 2008.

[23] T. P. Berger, P.-L. Cayrel, P. Gaborit, and A. Otmani. Reducing key length of the McEliece cryptosystem. In B. Preneel, editor, *Progress in Cryptology - AFRICACRYPT 2009*, volume 5580 of *LNCS*, pages 77–97, Gammarth, Tunisia, June 21-25 2009.

[24] T. P. Berger and P. Loidreau. How to mask the structure of codes for a cryptographic use. *Des. Codes Cryptogr.*, 35(1) :63–79, 2005.

[25] E. Berlekamp, R. McEliece, and H. van Tilborg. On the inherent intractability of certain coding problems. *IEEE Trans. Inform. Theory*, 24(3) :384–386, May 1978.

[26] D. J. Bernstein, T. Chou, T. Lange, I. von Maurich, R. Niederhagen, E. Persichetti, C. Peters, P. Schwabe, N. Sendrier, J. Szefer, and W. Wen. Classic McEliece : conservative code-based cryptography. `https://classic.mceliece.org`, Nov. 2017. First round submission to the NIST post-quantum cryptography call.

[27] D. J. Bernstein, T. Lange, and C. Peters. Wild McEliece. In A. Biryukov, G. Gong, and D. R. Stinson, editors, *Selected Areas in Cryptography*, volume 6544 of *LNCS*, pages 143–158, 2010.

[28] D. J. Bernstein, T. Lange, and C. Peters. Wild McEliece Incognito. In B.-Y. Yang, editor, *Post-Quantum Cryptography 2011*, volume 7071 of *LNCS*, pages 244–254. Springer Berlin Heidelberg, 2011.

[29] A. Beutelspacher. Blocking sets and partial spreads in finite projective spaces. *Geom. Dedicata*, 9(4) :425–449, 1980.

[30] R. Blache, A. Couvreur, E. Hallouin, D. Madore, J. Nardi, M. Rambaud, and H. Randriam. Anticanonical codes from del Pezzo surfaces with Picard rank one. ArXiv :1903.09397, Mar. 2019.

[31] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I : The user language. *J. Symbolic Comput.*, 24(3/4) :235–265, 1997.

[32] T. Bouganis. Error correcting codes over algebraic surfaces. In *Applied algebra, algebraic algorithms and error-correcting codes (Toulouse, 2003)*, volume 2643 of *Lecture Notes in Comput. Sci.*, pages 169–179. Springer, Berlin, 2003.

[33] S. Bravyi and M. B. Hastings. Homological product codes. In *Proceedings of the 46th annual ACM symposium on theory of computing, STOC '14. New York, NY, USA, May 31– June 04, 2014*, pages 273–282. ACM, 2014.

[34] R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54 :1098 :1098–1105, 1996.

[35] A. Canteaut and F. Chabaud. A new algorithm for finding minimum-weight words in a linear code : Application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511. *IEEE Trans. Inform. Theory*, 44(1) :367–378, 1998.

[36] I. Cascudo, R. Cramer, D. Mirandola, and G. Zémor. Squares of random linear codes. *IEEE Trans. Inform. Theory*, 61(3) :1159–1173, March 2015.

[37] I. M. Chakravarti. The generalized Goppa codes and related discrete designs from Hermitian surfaces in $PG(3, s^2)$. In G. Cohen and P. Godlewski, editors, *Coding Theory and Applications*, pages 116–124, Berlin, Heidelberg, 1988. Springer.

[38] I. V. Chizhov and M. A. Borodin. Effective attack on the McEliece cryptosystem based on Reed-Muller codes. *Discrete Math. Appl.*, 24(5) :273–280, 2014.

[39] D. Coggia and A. Couvreur. On the security of a Loidreau's rank metric code based encryption scheme. In *WCC 2019 - Workshop on Coding Theory and Cryptography*, Saint Jacut de la mer, France, Mar. 2019.

[40] N. Courtois, M. Finiasz, and N. Sendrier. How to achieve a McEliece-based digital signature scheme. In *Advances in Cryptology - ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 157–174, Gold Coast, Australia, 2001. Springer.

[41] A. Couvreur. Construction of rational surfaces yielding good codes. *Finite Fields Appl.*, 17(5) :424–441, Sept. 2011.

[42] A. Couvreur. Incidence structures from the blown–up plane and LDPC codes. *IEEE Trans. Inform. Theory*, 57(7) :4401–4416, July 2011.

[43] A. Couvreur. Codes and the Cartier Operator. *Proc. Amer. Math. Soc.*, 142 :1983–1996, Mar. 2014.

[44] A. Couvreur. An upper bound on the number of rational points of arbitrary projective varieties over finite fields. *Proc. Amer. Math. Soc.*, 144 :3671–3685, 2016.

[45] A. Couvreur. Introduction to coding theory, 2018. Notes de cours, disponibles sur le site : `http://www.lix.polytechnique.fr/~alain.couvreur/doc_ens/lecture_notes.pdf`.

[46] A. Couvreur, N. Delfosse, and G. Zémor. A construction of quantum LDPC codes from cayley graphs. *IEEE Trans. Inform. Theory*, 59(9) :6087–6098, Sep. 2013.

[47] A. Couvreur and I. Duursma. Evaluation codes from smooth quadric surfaces and twisted Segre varieties. *Des. Codes Cryptogr.*, 66(1) :291–303, Jan 2013.

[48] A. Couvreur, P. Gaborit, V. Gauthier-Umaña, A. Otmani, and J.-P. Tillich. Distinguisher-based attacks on public-key cryptosystems using Reed-Solomon codes. *Des. Codes Cryptogr.*, 73(2) :641–666, 2014.

[49] A. Couvreur, M. Lequesne, and J.-P. Tillich. Recovering short secret keys of RLCE in polynomial time. Preprint, 2018. arXiv :1805.11489, to appear in PQCrypto 2019.

[50] A. Couvreur, I. Márquez-Corbella, and R. Pellikaan. Cryptanalysis of public-key cryptosystems that use subcodes of algebraic geometry codes, 2014. Presented at the 4th International Castle Meeting on Coding Theory and Applications (4ICMCTA). Palmela (Portugal).

[51] A. Couvreur, I. Márquez-Corbella, and R. Pellikaan. A polynomial time attack against algebraic geometry code based public key cryptosystems. In *Proc. IEEE Int. Symposium Inf. Theory - ISIT 2014*, pages 1446–1450, June 2014.

[52] A. Couvreur, I. Márquez-Corbella, and R. Pellikaan. Cryptanalysis of McEliece cryptosystem based on algebraic geometry codes and their subcodes. *IEEE Trans. Inform. Theory*, 63(8) :5404–5418, Aug 2017.

[53] A. Couvreur, A. Otmani, and J.-P. Tillich. New identities relating wild Goppa codes. *Finite Fields Appl.*, 29 :178–197, 2014.

[54] A. Couvreur, A. Otmani, and J.-P. Tillich. Polynomial time attack on wild McEliece over quadratic extensions. In P. Q. Nguyen and E. Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 17–39. Springer Berlin Heidelberg, 2014.

[55] A. Couvreur, A. Otmani, and J.-P. Tillich. Polynomial time attack on wild McEliece over quadratic extensions. *IEEE Trans. Inform. Theory*, 63(1) :404–427, Jan 2017.

[56] A. Couvreur, A. Otmani, J.-P. Tillich, and V. Gauthier-Umaña. A polynomial-time attack on the BBCRS scheme. In J. Katz, editor, *Public-Key Cryptography - PKC 2015*, volume 9020 of *LNCS*, pages 175–193. Springer, 2015.

[57] J. Davis. Algebraic geometric codes on anticanonical surfaces. *J. Pure Appl. Algebra*, 215(4) :496 – 510, 2011.

[58] P. Delsarte. On subfield subcodes of modified Reed-Solomon codes. *IEEE Trans. Inform. Theory*, 21(5) :575–576, 1975.

[59] A. Duc and S. Vaudenay. HELEN : A public-key cryptosystem based on the LPN and the decisional minimal distance problems. In *Progress in Cryptology - AFRICACRYPT 2013*, volume 7918 of *LNCS*, pages 107–126. Springer, 2013.

[60] I. Dumer. Two decoding algorithms for linear codes. *Probl. Inf. Transm.*, 25(1) :17–23, 1989.

[61] I. M. Duursma and R. Pellikaan. A symmetric Roos bound for linear codes. *J. Combin. Theory Ser. A*, 113(8) :1677–1688, 2006.

[62] F. A. B. Edoukou. Codes defined by forms of degree 2 on Hermitian surfaces and Sørensen's conjecture. *Finite Fields Appl.*, 13(3) :616–627, 2007.

[63] F. A. B. Edoukou. Codes defined by forms of degree 2 on quadric surfaces. *IEEE Trans. Inform. Theory*, 54(2) :860–864, 2008.

[64] F. A. B. Edoukou. Codes defined by forms of degree 2 on quadrics in $\mathbb{P}^4(\mathbb{F}_q)$. In G. Lachaud, C. Ritzenthaler, and M. A. Tsfasman, editors, *Arithmetic, Geometry, Cryptography and Coding Theory*, volume 487 of *Contemp. Math.* Amer. Math. Soc., 2009.

[65] J.-C. Faugère, V. Gauthier, A. Otmani, L. Perret, and J.-P. Tillich. A distinguisher for high rate McEliece cryptosystems. In *Proc. IEEE Inf. Theory Workshop- ITW 2011*, pages 282–286, Paraty, Brasil, Oct. 2011.

[66] J.-C. Faugère, A. Otmani, L. Perret, F. de Portzamparc, and J.-P. Tillich. Folding alternant and Goppa Codes with non-trivial automorphism groups. *IEEE Trans. Inform. Theory*, 62(1) :184–198, 2016.

[67] J.-C. Faugère, A. Otmani, L. Perret, and J.-P. Tillich. Algebraic cryptanalysis of McEliece variants with compact keys. In *Advances in Cryptology - EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 279–298, 2010.

[68] J.-C. Faugère, L. Perret, and F. de Portzamparc. Algebraic attack against variants of McEliece with Goppa polynomial of a special form. In *Advances in Cryptology - ASIACRYPT 2014*, volume 8873 of *LNCS*, pages 21–41, Kaoshiung, Taiwan, R.O.C., Dec. 2014. Springer.

[69] C. Faure and L. Minder. Cryptanalysis of the McEliece cryptosystem over hyperelliptic curves. In *Proceedings of the eleventh International Workshop on Algebraic and Combinatorial Coding Theory*, pages 99–107, Pamporovo, Bulgaria, June 2008.

[70] G. Feng and T. R. N. Rao. Decoding algebraic-geometric codes up to the designed minimum distance. *IEEE Trans. Inform. Theory*, 39(1) :37–45, Jan 1993.

[71] M. H. Freedman, D. A. Meyer, and F. Luo. Z_2-systolic freedom and quantum codes. In *Mathematics of quantum computation*, Comput. Math. Ser., pages 287–320. Chapman & Hall/CRC, Boca Raton, FL, 2002.

[72] P. Gaborit. Shorter keys for code based cryptography. In *Proceedings of the 2005 International Workshop on Coding and Cryptography (WCC 2005)*, pages 81–91, Bergen, Norway, Mar. 2005.

[73] R. G. Gallager. *Low Density Parity Check Codes*. M.I.T. Press, Cambridge, Massachusetts, 1963.

[74] A. Garcia and H. Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlăduţ bound. *Invent. Math.*, 121 :211–222, 1995.

[75] S. R. Ghorpade and G. Lachaud. Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields. *Mosc. Math. J.*, 2(3) :589–631, 2002.

[76] V. D. Goppa. Codes on algebraic curves. *Dokl. Akad. Nauk SSSR*, 259(6) :1289–1290, 1981.

[77] M. Grassl. Bounds on the minimum distance of linear codes and quantum codes. Online available at `http://www.codetables.de`, 2007. Accessed on 2019-01-29.

[78] V. Guruswami and M. Sudan. Improved decoding of Reed-Solomon and algebraic-geometry codes. *IEEE Trans. Inform. Theory*, 45(6) :1757–1767, 1999.

[79] J. P. Hansen. Toric surfaces and error-correcting codes. In *Coding theory, cryptography and related areas (Guanajuato, 1998)*, pages 132–142. Springer, Berlin, 2000.

[80] S. H. Hansen. Error-correcting codes from higher-dimensional varieties. *Finite Fields Appl.*, 7(4) :531–552, 2001.

[81] R. Hartshorne. *Algebraic geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1977.

[82] J. Hirschfeld. *Finite Projective Spaces of Three Dimensions*. Oxford mathematical monographs. Clarendon Press, 1985.

[83] T. Høholdt and R. Pellikaan. On the decoding of algebraic-geometric codes. *IEEE Trans. Inform. Theory*, 41(6, part 1) :1589–1614, 1995.

[84] M. Homma and S. J. Kim. Sziklai's conjecture on the number of points of a plane curve over a finite field III. *Finite Fields and Their Applications*, In Press, Corrected Proof :–, 2010.

[85] X. Hou, K. H. Leung, and Q. Xiang. A generalization of an addition theorem of Kneser. *J. Number Theory*, 97 :1–9, 2002.

[86] Y. Ihara. Some remarks on the number of rational points of algebratic curves over finite fields. *J. Math. Sci. Univ. Tokyo*, 28(3) :721–724, feb 1982.

[87] H. Janwa and O. Moreno. McEliece public key cryptosystems using algebraic-geometric codes. *Des. Codes Cryptogr.*, 8(3) :293–307, 1996.

[88] D. Jungnickel. Maximal partial spreads and translation nets of small deficiency. *J. Algebra*, 90(1) :119 – 132, 1984.

[89] D. Jungnickel. Maximal partial spreads and transversal-free translation nets. *J. Combin. Theory Ser. A*, 62(1) :66 – 92, 1993.

[90] G. L. Katsman and M. A. Tsfasman. A remark on algebraic geometric codes. In *Representation theory, group rings, and coding theory*, volume 93 of *Contemp. Math.*, pages 197–199. Amer. Math. Soc., Providence, RI, 1989.

[91] K. Khuri-Makdisi. Linear algebra algorithms for divisors on an algebraic curve. *Math. Comp.*, 73(245) :333–357 (electronic), 2004.

[92] K. Khuri-Makdisi. Asymptotically fast group operations on Jacobians of general curves. *Math. Comp.*, 76(260) :2213–2239 (electronic), 2007.

[93] A. Y. Kitaev. Fault-tolerant quantum computation by anyons. *Ann. Physics*, 303(1) :2–30, 2003.

[94] M. Kneser. Summenmengen in lokalkompakten abelesche Gruppen. *Math. Z.*, 66 :88–110, 1956.

[95] G. Lachaud. Projective Reed-Muller codes. In *Coding theory and applications (Cachan, 1986)*, volume 311 of *Lecture Notes in Comput. Sci.*, pages 125–129. Springer, Berlin, 1988.

[96] G. Lachaud and R. Rolland. On the number of points of algebraic sets over finite fields. *J. Pure Appl. Algebra*, 219 :5117–5136, 2015.

[97] P. J. Lee and E. F. Brickell. An observation on the security of McEliece's public-key cryptosystem. In *Advances in Cryptology - EUROCRYPT'88*, volume 330 of *LNCS*, pages 275–280. Springer, 1988.

[98] J. B. Little. Algebraic geometry codes from higher-dimensional varieties. In E. Martinez-moro and D. Ruano, editors, *Advances in Algebraic Geometry codes*, chapter 7, pages 257–293. World Scientific Publishing Co., Inc., 2008.

[99] C. C. Lomont. *Error correcting codes on algebraic surfaces.* PhD thesis, University of Purdue, 2003. ArXiv :0309123v1.

[100] D. J. MacKay, G. Mitchison, and A. Shokrollahi. More sparse-graph codes for quantum error-correction, 2007.

[101] D. J. MacKay and R. M. Neal. Near shannon limit performance of low density parity check codes. *Electronics Letters*, 32 :1645–1646, 1996.

[102] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes.* North–Holland, Amsterdam, fifth edition, 1986.

[103] Y. I. Manin. *Cubic forms*, volume 4 of *North-Holland Mathematical Library.* North-Holland Publishing Co., Amsterdam, second edition, 1986. Algebra, geometry, arithmetic, Translated from the Russian by M. Hazewinkel.

[104] Y. I. Manin and S. G. Vlăduts. Linear codes and modular curves. In *Current problems in mathematics, Vol. 25*, Itogi Nauki i Tekhniki, pages 209–257. Akad. Nauk SSSR Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1984.

[105] I. Márquez-Corbella and R. Pellikaan. Error-correcting pairs for a public-key cryptosystem. CBC 2012, Code-based Cryptography Workshop, 2012. Available on `http://www.win.tue.nl/~ruudp/paper/59.pdf`.

[106] A. May, A. Meurer, and E. Thomae. Decoding random linear codes in $O(2^{0.054n})$. In D. H. Lee and X. Wang, editors, *Advances in Cryptology - ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 107–124. Springer, 2011.

[107] A. May and I. Ozerov. On computing nearest neighbors with applications to decoding of binary linear codes. In E. Oswald and M. Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015*, volume 9056 of *LNCS*, pages 203–228. Springer, 2015.

[108] R. J. McEliece. *A Public-Key System Based on Algebraic Coding Theory*, pages 114–116. Jet Propulsion Lab, 1978. DSN Progress Report 44.

[109] K. Metsch and L. Storme. Partial t-spreads in $PG(2t+1, q)$. *Des. Codes Cryptogr.*, 18(1-3) :199–216, 1999.

[110] L. Minder. *Cryptography based on error correcting codes.* PhD thesis, Ecole Polytechnique Fédérale de Lausanne, 2007.

[111] L. Minder and A. Shokrollahi. Cryptanalysis of the Sidelnikov cryptosystem. In *Advances in Cryptology - EUROCRYPT 2007*, volume 4515 of *LNCS*, pages 347–360, Barcelona, Spain, 2007.

[112] D. Mirandola and G. Zémor. Critical pairs for the product Singleton bound. *IEEE Trans. Inform. Theory*, 61(9) :4928–4937, 2015.

[113] R. Misoczki, J.-P. Tillich, N. Sendrier, and P. S. L. M. Barreto. MDPC-McEliece : New McEliece variants from moderate density parity-check codes. In *Proc. IEEE Int. Symposium Inf. Theory - ISIT*, pages 2069–2073, 2013.

[114] D. Mumford. Varieties defined by quadratic equations. In *Questions on algebraic varieties, C.I.M.E., III Ciclo, Varenna, 1969*, pages 29–100. Edizioni Cremonese, Rome, 1970.

[115] H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, 15(2) :159–166, 1986.

[116] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge University Press. xxxi, Cambridge, 10th anniversary editions edition, 2010.

[117] A. Otmani, J.-P. Tillich, and L. Dallot. Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes. *Special Issues of Mathematics in Computer Science*, 3(2) :129–140, Jan. 2010.

[118] R. Overbeck and N. Sendrier. Code-based cryptography. In D. J. Bernstein, J. Buchmann, and E. Dahmen, editors, *Post-quantum cryptography*, pages 95–145. Springer, 2009.

[119] R. Pellikaan. On decoding linear codes by error correcting pairs. Preprint Technical University Eindhoven, 1988.

[120] E. Prange. The use of information sets in decoding cyclic codes. *IRE Transactions on Information Theory*, 8(5) :5–9, 1962.

[121] H. Randriambololona. On products and powers of linear codes under componentwise multiplication. In *Algorithmic arithmetic, geometry, and coding theory*, volume 637 of *Contemp. Math.*, pages 3–78. Amer. Math. Soc., Providence, RI, 2015.

[122] T. Richardson, A. Shokrollahi, and R. Urbanke. Design of capacity-approaching irregular low-density parity check codes. *IEEE Trans. Inform. Theory*, 47 :619–637, Feb. 2001.

[123] T. Richardson and R. Urbanke. *Modern Coding Theory*. Cambridge University Press, 2008.

[124] E. Rieffel and W. Polak. An introduction to quantum computation for non–physicists. ArXiv :quant-ph/9809016v2, 2000.

[125] J. Rosenkilde. Power decoding Reed-Solomon codes up to the Johnson radius. *Advances in Mathematics of Communications*, 12(1) :81–106, 2018.

[126] D. Ruano. On the parameters of r-dimensional toric codes. *Finite Fields Appl.*, 13(4) :962–976, 2007.

[127] G. Schmidt, V. Sidorenko, and M. Bossert. Decoding reed-solomon codes beyond half the minimum distance using shift-register synthesis. In *2006 IEEE International Symposium on Information Theory*, pages 459–463, 2006.

[128] N. Sendrier. On the structure of a randomly permuted concatenated code. In *EUROCODE'94*, pages 169–173, 1994.

[129] N. Sendrier. Decoding one out of many. In *Post-Quantum Cryptography 2011*, volume 7071 of *LNCS*, pages 51–67, 2011.

[130] J.-P. Serre. Lettre à M. Tsfasman. *Astérisque*, 198-200 :351–353, 1991. Journées Arithmétiques, 1989 (Luminy).

[131] I. R. Shafarevich. *Basic algebraic geometry. 1*. Springer-Verlag, Berlin, second edition, 1994.

[132] P. W. Shor. Algorithms for quantum computation : Discrete logarithms and factoring. In S. Goldwasser, editor, *FOCS*, pages 124–134, 1994.

[133] V. M. Sidelnikov. A public-key cryptosytem based on Reed-Muller codes. *Discrete Math. Appl.*, 4(3) :191–207, 1994.

[134] V. M. Sidelnikov and S. Shestakov. On the insecurity of cryptosystems based on generalized Reed-Solomon codes. *Discrete Math. Appl.*, 1(4) :439–444, 1992.

[135] A. N. Skorobogatov and S. G. Vlăduţ. On the decoding of algebraic-geometric codes. *IEEE Trans. Inform. Theory*, 36(5) :1051–1060, Sep. 1990.

[136] A. Steane. Multiple particle interference and quantum error correction. *Proc. Roy. Soc. Lond. A*, 452 :2551 :2551–2577, 1996.

[137] J. Stern. A method for finding codewords of small weight. In G. D. Cohen and J. Wolfmann, editors, *Coding Theory and Applications*, volume 388 of *LNCS*, pages 106–113. Springer, 1988.

[138] H. Stichtenoth. On the dimension of subfield subcodes. *IEEE Trans. Inform. Theory*, 36(1) :90–93, 1990.

[139] H. Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[140] K.-O. Stöhr and J. F. Voloch. Weierstrass points and curves over finite fields. *Proc. London Math. Soc*, pages 1–19, 1986.

[141] M. Sudan. Decoding of Reed Solomon codes beyond the error-correction bound. *J. Complexity*, 13(1) :180–193, 1997.

[142] Y. Sugiyama, M. Kasahara, S. Hirasawa, and T. Namekawa. Further results on Goppa codes and their applications to constructing efficient binary codes. *IEEE Trans. Inform. Theory*, 22 :518–526, 1976.

[143] P. Sziklai. A bound on the number of points of a plane curve. *Finite Fields Appl.*, 14(1) :41–43, 2008.

[144] R. M. Tanner. A recursive approach to low complexity codes. *IEEE Trans. Inform. Theory*, 27(5) :533–547, 1981.

[145] T. Tao and V. Vu. *Additive combinatorics*, volume 105 of *Cambridge Stud. Adv. Math.* Cambridge University Press, Cambridge, 2006.

[146] J.-P. Tillich. The decoding failure probability of MDPC codes. preprint, Sept. 2018. arXiv :1801.04668.

[147] J.-P. Tillich and G. Zémor. Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength. *IEEE Trans. Inform. Theory*, 60(2) :1193–1202, 2014.

[148] M. A. Tsfasman, S. G. Vlăduts, and T. Zink. Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. *Mathematische Nachrichten*, 109(1) :21–28, 1982.

[149] J. H. van Lint. *Introduction to Coding Theory*. Springer-Verlag, Berlin, Heidelberg, 1982.

[150] O. Viro. Remarks on definition of khovanov homology. ArXiv :math/0202199, 2002.

[151] S. G. Vlăduţ and V. G. Drinfel'd. Number of points of an algebraic curve. *Funct. Anal. Appl.*, 17(1) :53–54, Jan 1983.

[152] J. F. Voloch and M. Zarzar. Algebraic geometric codes on surfaces. In *Arithmetics, geometry, and coding theory (AGCT 2005)*, volume 21 of *Sémin. Congr.*, pages 211–216. Soc. Math. France, Paris, 2010.

[153] C. Voss and H. Stichtenoth. Asymptotically good families of subfield subcodes of geometric Goppa codes. *Geometriae Dedicata*, 33(1) :111–116, Jan 1990.

[154] Y. Wang. Quantum resistant random linear code based public key encryption scheme RLCE. In *Proc. IEEE Int. Symposium Inf. Theory - ISIT 2016*, pages 2519–2523, Barcelona, Spain, July 2016. IEEE.

[155] Y. Wang. RLCE–KEM. `http://quantumca.org`, 2017. First round submission to the NIST post-quantum cryptography call.

[156] C. A. Weibel. *An introduction to homological algebra*, volume 38 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1994.

[157] C. Wieschebrink. Two NP-complete problems in coding theory with an application in code based cryptography. In *Proc. IEEE Int. Symposium Inf. Theory - ISIT*, pages 1733–1737, 2006.

[158] C. Wieschebrink. Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes. In *Post-Quantum Cryptography 2010*, volume 6061 of *LNCS*, pages 61–72. Springer, 2010.

[159] M. Wirtz. On the parameters of Goppa codes. *IEEE Trans. Inform. Theory*, 34(5, part 2) :1341–1343, 1988. Coding techniques and coding theory.

[160] A. Yamada, E. Eaton, K. Kalach, P. Lafrance, and A. Parent. QC-MDPC KEM. First round submission to the NIST post-quantum cryptography call, Nov. 2017.

[161] M. Zarzar. Error-correcting codes on low rank surfaces. *Finite Fields Appl.*, 13(4) :727–737, 2007.