AIX-MARSEILLE UNIVERSITÉ
École Doctorale en Mathématiques et Informatique de Marseille
Institut de Mathématiques de Marseille (I2M)

Thèse présentée pour obtenir le grade universitaire de docteur

Discipline : Mathématiques

Elena Berardini

Algebraic geometry codes from surfaces over finite fields

Soutenue le 18 juin 2020 devant le jury composé de :

Peter BEELEN	Technical University of Denmark	Rapporteur
Marc HINDRY	Université Paris Diderot	Rapporteur
Iwan DUURSMA	University of Illinois	Examinateur
Massimo GIULIETTI	Università degli Studi di Perugia	Examinateur
Elisa LORENZO GARCÍA	Université de Rennes 1	Examinatrice
Serge VLĂDUŢ	Université d'Aix-Marseille	Examinateur
Yves AUBRY	Université de Toulon	Directeur de thèse
David KOHEL	Université d'Aix-Marseille	Directeur de thèse

One often meets his destiny
on the road he takes to avoid it.

Abstract

In this thesis we provide a theoretical study of algebraic geometry codes from surfaces defined over finite fields. We prove lower bounds for the minimum distance of codes over surfaces whose canonical divisor is either nef or anti-strictly nef and over surfaces without irreducible curves of small genus. We sharpen these lower bounds for surfaces whose arithmetic Picard number equals one, surfaces without curves with small self-intersection and fibered surfaces. Then we apply these bounds to surfaces embedded in $\mathbb{P}^3$. A special attention is given to codes constructed from abelian surfaces. In this context, we give a general bound on the minimum distance and we prove that this estimation can be sharpened under the assumption that the abelian surface does not contain absolutely irreducible curves of small genus. In this perspective we characterize all abelian surfaces which do not contain absolutely irreducible curves of genus up to 2. This approach naturally leads us to consider Weil restrictions of elliptic curves and abelian surfaces which do not admit a principal polarization.

Résumé

Nous proposons, dans cette thèse, une étude théorique des codes géométriques algébriques construits à partir de surfaces définies sur les corps finis. Nous prouvons des bornes inférieures pour la distance minimale des codes sur des surfaces dont le diviseur canonique est soit nef soit anti-strictement nef et sur des surfaces sans courbes irréductibles de petit genre. Nous améliorons ces bornes inférieures dans le cas des surfaces dont le nombre de Picard arithmétique est égal à un, des surfaces sans courbes de petite auto-intersection et des surfaces fibrées. Ensuite, nous appliquons ces bornes aux surfaces plongées dans $\mathbb{P}^3$. Une attention particulière est accordée aux codes construits à partir des surfaces abéliennes. Dans ce contexte, nous donnons une borne générale sur la distance minimale et nous démontrons que cette estimation peut être améliorée en supposant que la surface abélienne ne contient pas de courbes absolument irréductibles de petit genre. Dans cette optique nous caractérisons toutes les surfaces abéliennes qui ne contiennent pas de courbes absolument irréductibles de genre inférieur ou égal à 2. Cette approche nous conduit naturellement à considérer les restrictions de Weil de courbes elliptiques et les surfaces abéliennes qui n'admettent pas de polarisation principale.

Can we take a moment to celebrate Us?

Il arrive un moment avant la soutenance, quand on a fini de rédiger le manuscrit et on est dans l'attente des rapports de thèse, quand la date de la soutenance est fixée mais il est encore trop tôt pour s'occuper de la présentation, qu'on se rend compte que le moment de tirer les conclusions et écrire la partie la plus personnelle est arrivé, mais on n'est pas prêt. Parce qu'on n'est jamais prêt pour admettre qu'une époque s'est terminée et qu'il faut se regarder dans les yeux pour une dernière fois et se dire *au revoir*. Alors, avant de devenir pleurnicharde, allons-y...

Pour faire une thése, ça va sans dire, il faut avoir un directeur de thése. Et puisque je ne me contente jamais, j'en ai eu bien deux. Deux directeurs, deux projets, et comme le dirait David, le double du travail pour moi et la moitié pour eux.

Yves, notre aventure a commencé en 2016 avec ma preuve de l'amélioration de la borne de Weil par Serre au tableau. Puis, entre un stage de master, cinq conférences, deux road trips, quatre retraites, quelques soirées, une quantité non dénombrable de spritz et deux papiers, quatre annés sont volées. On a échangé sur les maths, la musique, les films, les séries, les livres, le sport, la vie... Tu as été *Monsieur Aubry*, puis mon directeur, mon Jedi Master et enfin, mon ami. Toujours à l' écoute, positif, présent sans être indiscret, tu as su me guider, m'enseigner des choses, faire fleurir des idées dans ma tête. Tu as pris une jeune étudiante qui écoutait sans trop parler, hésitante à participer ou à s'exprimer, tu l'as conduite à travers le monde de la recherche, dans des conférences, dans une ambiance dynamique et challengeant, et tu as obtenu une jeune chercheuse qui travaille avec ses collaborateurs plus experiencés sans crainte. On dit qu'on reste toujours l'étudiant de notre directeur de thèse, et dans mon cas, je serai toujours orgueilleuse de l'être.

David, je n'oublierai jamais toutes nos rencontres hebdomadaires d'où je suis sortie à chaque fois avec un sentiment différent : illuminée, confondue, motivée... Toujours j'ai été surprise par ta maîtrise, ta capacité de lier plusieurs sujets et passer d'un sujet à l'autre, comme si tu tenais dans ta tête le fil imaginaire qui lie la théorie des nombres et la géométrie algébrique. On dit qu'on finit pour ressembler à notre directeur de thèse, et si un jour je serai capable de retrouver un morceau de ce fil dans mes pensées mathématiques, j'en serai bien orgueilleuse. Merci pour ta patience infinie, pour tout ce que tu m'as enseigné et surtout pour ton soutien, en particulier pendant cette dernière période.

Juste après mes directeurs, un gros merci va à Marc Perret. Marc, tu m'as enseigné beaucoup des choses et bien plus que cela, tu as su croire en moi et à mes capacités, en sachant trouver parfois de l'interêt dans mes idées quand moi-même, je fatiguais à le trouver. Ton enthousiasme pour la géométrie algébrique, ta volonté d'aider les jeunes et ton honneté intellectuelle, font de toi une personne hors-norme.

On ne choisit pas forcement nos collaborateurs quand on est en thèse, et je peux donc affirmer d'avoir eu de la chance à travailler avec toi. Dans cette dernière période tu as pris à coeur mon futur, et ton aide, ton attention et ta disponibilité, m'ont vraiment touché. Merci.

I want to thank Marc Hindry and Peter Beelen for having accepted to be the referees of my thesis. You have done this work during an neither easy nor happy period of confinement. I hope reading my thesis has taken up a little of your time without boring you too much. I want to thank Iwan Duursma, Massimo Giulietti, Elisa Lorenzo García and Serge Vlăduţ for having accepted to be part of my jury.

Un gros remerciement va aux membres de l'équipe ATI. À Stéphane et Alexis qui gèrent l'équipe et le groupe avec savoir-faire. À Jessica, Corinne et Jean-Bruno, qui nous rendent la vie beaucoup plus facile. Merci à Stéphane, mon collègue du bureau à côté. Au début de ma thèse à Marseille, quand je pensais avoir désormais appris un peu de français après un an de master, parler avec toi, mon cher breton, c'était le plus dur. À la fin de mon parcours, je me retrouve même à t'avoir appris des tournures du français que tu ignorais ! Maintenant, c'est l'heure que tu commences à apprendre l'italien ! Merci à Samuele qui est arrivé recemment mais qui a déjà amené de la lumière dans notre team. L'équipe ATI a été ma maison pendant beaucoup de temps, et même en sachant que je l'aurais quittée un jour ou l'autre, je m'y suis liée comme si ça pouvait durer pour toujours : je suis contente de pouvoir la laisser dans les mains savantes d'un autre italien qui saura en prendre soin.

L'équipe ATI a été ma maison, je l'ai déjà dit, mais je ne serais peut être pas ici sans l'équipe LDP. Je suis arrivée à Marseille pour faire de la logique et bien que je me retrouve à partir après quatre ans de géométrie algébrique, théorie des nombres et théorie des codes, je reste très liée à cet autre domaine des mathématiques. Désolée de vous avoir trahis...

Je remercie mon autre coauteur, collègue et ami, Fabien Herbaut, pour avoir été toujours attentif, méticuleux et soucieux du détail : c'est ainsi qu'on fait grandir les nouvelles générations de chercheuses et chercheurs ! Tu es probablement caché quelque part dans la salle avec des faux moustaches et des lunettes noires : j'attend le moment où tu te lèveras de la chaise pour dire "C'est faux !".

Je veux remercier les porteurs du projet ANR Manta : grâce à vous, nous nous sommes régalé-e-s pendant quatre ans en faisant des belles mathématiques dans des endroits magnifiques ! Sans ce projet mon experience de thèse aurait été sûrement moins riche.

Je remercie aussi tou-te-s mes étudiant-e-s de l'Université d'Aix-Marseille : c'est aussi grâce à vous que je suis devenue une enseignante-chercheuse !

Enfin, avant de quitter la partie académique des remerciements, je veux remercier l'un des créateurs de la Géométrie Algébrique moderne, Jean-Pierre Serre. J'ai eu l'honneur et le plaisir d'avoir Jean-Pierre Serre parmi les spectateurs de mon exposé au CIRM en 2019, lors de la conférence AGC^{2}T. À la fin de mon exposé, il m'a congratulé et a pris du temps pour échanger avec moi sur mon travail. Il m'a dit "Vous devriez faire de la géométrie algébrique aussi sans des applications aux codes", et une telle phrase dite de la part de l'un des plus grands géomètres algébristes au monde, peut renforcer grandement l'estime de soi. Je pense que l'un des rôles des grand-e-s mathématicien-ne-s comme Jean-Pierre Serre est de stimuler et d'encourager les jeunes chercheuses et chercheurs et, avec moi, il a superbement fait ce travail. Je ne l'oublierai jamais.

Une partie de ma première année de thèse à été consacrée au plus grand événement mathématique que la France ait jamais vu : la Tournée de π ! On ne peut pas expliquer l'emotion et la satisfaction de partir en Tournée à Paris, Lyon et Marseille, pour un projet qu'on a conçu et fait grandir avec ses ami-e-s. C'est une experience que je n'oublierai jamais et pour la quelle je dois tout d'abord remercier Joël, Anna et Guillaume, que dès mon arrivée à Marseille m'ont entraînée dans l'association Pi Day. La réalisation de ce projet et de la Tournée n'aurait quand même pu être aussi belle et amusante sans Paolo, Émilie, et tou-te-s les membres des équipes de Paris et de Lyon, ainsi que les actrices et les acteurs, les musicien-ne-s, les oratrices et les orateurs : un gros merci à vous tou-te-s !

En parlant d'association, un très gros merci va aussi à la team de l'association Café des Langues Luminy, dont j'ai eu l'honneur et le plaisir d'être la "presidenta" depuis sa naissance, il y a deux ans. Merci Guillaume, Claudio et Federico pour avoir aidé dans la creation de l'association et avoir accepté de faire partie du bureau. Merci aux vieux et aux nouveaux animateurs. Merci Tom, directeur du CIEL(L), pour ton soutien et ton enthousiasme : je n'oublierai jamais nos soirées karaoke ! Merci Jean-Michel, pour nous avoir toujours soutenu dans nos activités et nos événements. Enfin, merci Anna pour m'avoir entraînée dans ce monde qui m'a apporté beaucoup de belles emotions.

Le concept de *chez moi* est devenu pour moi très relatif pendant les dernières années. Je suis née et grandie dans l'une des plus belles villes au monde : Rome. Pendant beaucoup de temps je l'ai considerée ma seule ville et j'ai cru que je ne l'aurais jamais quittée. Cependant, quand je suis arrivée à Marseille, je n'ai pas eu peur ni je me suis sentie depaysée ou insecure. Sans m'en rendre compte et sans savoir comment et pourquoi, je me sentais déjà *chez moi*. Pas une seule fois j'ai eu l'impression d'être seule ou perdue, et cela a été possible grâce à la grande famille d'ami-e-s que j'ai trouvé ici. La liste des personnes que j'ai recontrées à Marseille est très longue et, comme toute personne qui s'est confronté avec la tâche d'écrire des remerciements, j'ai peur que j'oublierai quelqu'un. Donc, à toi qui lis ces longs remerciements, si tu as fait partie de mon entourage à Marseille, alors, avec tout mon cœur, MERCI !

Andrea, da quando ti conosco e finché sei rimasto a Marsiglia, ho sempre avuto un posto dove andare a sbroccare quando la vita da dottoranda colpiva troppo forte: il tuo ufficio. Sapere che c'era qualcuno sempre pronto ad arrivare a Luminy più tardi di me, a fare una pausa caffé dietro l'altra e ad ascoltarmi, mi ha sicuramente salvata dall'esaurimento nervoso da dottorato. Serena, grazie per aver visto in me una persona su cui si può fare affidamento. Abbiamo passato molto tempo insieme, abbiamo parlato di tante cose e forse a volte sono stata quella che ti ha detto le cose che non volevi sentirti dire. Sei stata una persona importante in questi anni marsigliesi, e ti voglio bene. Alejandro, realmente disfruté todas nuestras interacciones. Verte venir a mi oficina para hacer preguntas, y generalmente salir sin respuestas y con mas preguntas, es un hábito que extrañaré. Tu tranquilidad es algo raro, al principio difícil de entender para alguien que va a mil como yo, pero con el tiempo aprendí a apreciarla porque también me calma. Gracias por todos, y en particular por dejarme dar mis primeros pasos de bachata. Alberto, amigo, para mí siempre has sido una persona con la que puedo contar y por eso te extrañé mucho el año pasado. Estoy orgullosa de ser la tía de Rodrigol y muy feliz por tu nueva vida. Como siempre te he dicho, serás un padre fantástico! Diogo, gostei do tempo que passamos juntos, fazendo música, jogando poker ou tênis, assistindo filmes. Fiquei

muito emocionada e orgulhosa de estar presente no seu casamento com Marta e sou, como sempre, grande fã de Piccioncini. Labas Rasa! Unfortunately my Lithuanian stops here for the moment...It took a bit of time but I am very happy that at the end we found each other. I have really enjoyed the last period together in Marseille and I am proud to be your friend. I hope my thesis defense will not go bananas! Anna, sei la mia sorella accademica, e direi che il tuo ruolo l'hai svolto perfettamente, dal primo giorno in cui, a Roma, mi hai parlato della tuo dottorato, fino a quando mi hai inserito nel mondo marsigliese che già da tempo era la tua casa. Grazie al tuo aiuto e alla tua guida molte cose sono state più facili. Con la mia discussione, si chiude anche la nostra tesi di dottorato segreta, chissà forse un giorno la pubblicheremo! Guillaume, j'apprécie beaucoup ton esprit ouvert et la passion que tu sais mettre dans les choses. Je sais que je ne parle pas beaucoup de moi, et toi encore moins, mais les rares fois qu'on est arrivé à s'ouvrir, je les ai bien aimées. Merci pour ton amitié et pour avoir été mon meilleur enseignant de français. Joël, tu te donnes tout entier pour aider les amis, et je l'apprécie beaucoup. Tu as été très accueillant avec moi dès mon arrivée à Marseille et ton aide et ta disponibilité ont été très important pour moi. Sukran Lamia, pour ton amitié et pour n'avoir jamais fait manquer du reggaeton dans nos soirées ! Bastien et Leonardo, merci pour les pauses café et pour avoir participé à tenir vivante l'ambiance dans notre équipe. Vous allez bientôt prendre le relève des jeunes de l'équipe ATI : je compte sur vous !

Merci aussi à Afroditi, Federico, Federico (oui, il y en a deux !), Alessandro, Ante, Stefania, Santiago, Audrey, Matteo, Matteo (oui, encore deux !), Marianna, Davide, Claudio, Marta, Suzana, Claire, Davo, Guillaume K, Bob, Adam, Paolo, Paolo (toujours deux !), Mélodie, Marc, Firas, Lolita, Fifi, Christiana, Cairo, Hung, Nacho...

Enfin, merci ma chère Marseille, pour m'avoir accueillie. Pour toujours tu seras un autre *chez moi*. Tes ciels de Mistral me manquent déjà...

Ci sono gli amici nuovi, che sono stati la mia famiglia a Marsiglia in questi cinque anni, e ci sono gli amici di vecchia data, quelli che sono la mia famiglia da un tempo a volte così lungo che è difficile distinguerlo nella memoria.

Il gruppo Santa Subito, nato senza questo nome poco meno di 25 anni fa sul bagnasciuga di Santa Severa e che oggi si ritrova ad essere un gruppo Whatsapp fra Francia, Inghilterra, Italia, Belgio (Sud Africa a breve?). Giorgia, Giulia, Maila, le nostre videochiamate in quest'ultimo periodo hanno saputo darmi delle ore spensierate. Grazie di cuore, vi voglio bene!

Giorgia, i nostri scambi di audio infiniti sulla nostra vita hanno saputo tenerci sempre molto vicine. Sei sempre positiva, sempre motivante, e sempre orgogliosa di me, in un modo che mi risulta a volte così inaspettato che mi chiedo come faccio a meritarlo. Maila, le nostre video chiamate su Skype potrebbero non finire mai. C'è sempre qualcosa di cui discutere, qualcosa su cui riflettere, qualcosa da raccontarsi... D'altronde è sempre stato così e, senza troppo sforzo, posso pensare che resterà così per tutta la nostra vita. Siete le mie R.I.P., fra alti e bassi, e nonostante tutto ciò che potrà succedere e per quanto la vita potrà allontanarci fisicamente, so per certo che potrò sempre contare su di voi.

Care ragazze della Confraternita, da una relazione giorno per giorno a La Sapienza, che come minimo ha il merito di averci fatte incontrare, siamo passate a una relazione a distanza che a stento ci permette di vederci una volta l'anno. Ciononostante, poche ma buone, siamo sopravvissute, e i nostri incontri annuali nonché i nostri scambi

a distanza, mi riempiono sempre il cuore. Aspetto con gioia il nostro prossimo incontro, in qualsiasi parte del mondo sarà. Vi voglio bene!

Ale, vicinissime sui banchi di scuola o lontanissime con chilometri di distanza che ci separano, certe cose non cambiano: esci dalla mia testa, amica! Dalla fine del liceo ad oggi siamo state in grado di rincorrerci per tutta l'Europa senza perderci: sono venuta a Potiers, tu mi hai raggiunta a Marsiglia, ho fatto una scappata a Milano, tu sicuramente verrai a Parigi... perché sono anni che per noi *le distanze non contano.* Ti voglio bene!

Se c'è una cosa che mi è mancata negli anni marsigliesi, sono le riunioni familiari. Ogni volta che c'è stato un pranzo, una cena, una festa a cui non ho potuto partecipare, ho vissuto un senso di mancanza e nostalgia. Per questo ogni volta che sono tornata ho cercato sempre di ricreare quell'atmosfera persa, correndo da una parte all'altra di Roma per poter vedere tutte e tutti. Non sempre è stato possibile purtroppo, e certe occasioni non ritornano, ma ringrazio tutta la mia famiglia e gli amici di famiglia che mi hanno accolta ad ogni mio ritorno, che mi hanno sostenuta a distanza, e tutte le persone che hanno preso un aereo e sono venute a conoscere la mia nuova casa.

Occorre notevole ardimento per andare via di casa ma molto di più per lasciar andare via di casa. Papà, grazie per essere sempre così orgoglioso di me. Da te cerco sempre di imparare a mantenere la calma in ogni situazione, perché per quanto possa essere pesante o semplicemente noioso l'ostacolo da superare, tutto si può risolvere e prima si inizia, prima si finisce. Mamma, grazie per sapermi inaspettatamente calmare dalle mie ansie. Penso che senza il tuo esempio non sarei potuta diventare la donna forte ed indipendente che cerco di essere ogni giorno.

Teresa, sei arrivata in un momento della mia vita incasinato: un dottorato iniziato da poco che non andava proprio benissimo, una storia che non era riuscita a sopravvivere alla distanza, e una vita lontana da dov'eri tu, Roma. Ciononostante testarda - incosciente? - innamorata, hai deciso che io ero la tua strada e non mi hai più mollata. Più di tutti hai saputo starmi vicina, provando a capire un mondo, quello della ricerca, sconosciuto ed incomprensibile per molti. Sei stata il mio posto sicuro quando troppe ansie e insicurezze mi assalivano, e nel cedere un po' della mia indipendenza, ho vinto una nuova grande sicurezza. Grazie per tutto e tanto altro ancora. *Non posso prevedere dove saremo un domani, posso solo sperare che sarò fra la tue mani...*

Finally, I must thank the person who made all this possible, which I often thank too little or nothing at all. It's about me, from the five-years-ago me who decided to quit Rome and leave for an unknown Marseille, until the last-few-months me that managed to get to the end of this path and get out of it with a written thesis and a post-doc for next year. The Covid-19 pandemic has greatly changed my last months of doctorate and my expectations for this defense and for the party that will follow. I wish it hadn't happened to me, or at least I wish it hadn't happened in this period. But as Gandalf taught us *"So do all who live to see such times, but that is not for them to decide. All we have to decide is what to do with the time that is given to us".* And for now, I can say that I spent it right.

Rendez-vous à Paris,
Elena - X

Contents

Introduction

In 1981 the pop group ABBA published their eighth album, The Visitors. Besides personal tastes [1] this album marked an important historical event: The Visitors was the first record to be pressed on the new Compact-Disc format. At that time, the compact disc digital audio system, or just CD, was an innovative transmission system that essentially brought sound from the studio into the living room. The data was physically written on the medium, thus imperfections on the disc, like fingerprints or scratches, could produce errors in the recovered data, that is in the music output. Nevertheless, we all know by personal experience that we were able to listen to our favourite CD even if it was not in its best shape. How was it possible? We should thank error correcting codes. Indeed, the reconstitution of the record in presence of imperfections was made possible by a family of error correcting codes, namely *the Reed-Solomon codes*. In all respect, we can say that without error correcting codes digital audio would not have been feasible. The Reed-Solomon codes were used after CDs for DVDs, Blu-Rays and so on. However, recording of music and videos is just one example of the many applications of these codes. For instance, they were and are used by the NASA in space missions to receive information from the rovers launched to Mars, Jupiter and Saturn. For further reading on the many applications of the Reed-Solomon codes, we recommend [57].

Generally speaking, whenever there is a transmission or storage of data, we want to detect any error (noise) added to the data and be able to recover the original information. An error correcting code is a tool for encoding data with the ability to retrieve the correct information in case the encoded data is somehow corrupted.

At this point, one could ask what mathematics, especially algebraic geometry, has to do with these useful tools. Some error correcting codes can be constructed using algebraic geometry's objects, and for that reason, they are called algebraic geometry codes. For instance, the above mentioned Reed-Solomon codes can be viewed as algebraic geometry codes.

Algebraic geometry and algebraic geometry codes are the two main characters of this thesis.

The year 1981 was a good one not only for the ABBA, but also for mathematics. In the same year in fact, the Russian mathematician Valery Denisovich Goppa introduced the idea of constructing error correcting codes using algebraic curves ([16]). His idea was to evaluate spaces of functions over points on curves. These spaces were the Riemann-Roch spaces, and the points were rational points on curves: two objects that algebraic geometers had studied for years. The importance of these codes became clear one year later. Until then, the common belief in coding theory

1. But if you have never listen to *One of Us* you are missing something in your sentimental education.

was that no code could exceed the asymptotic Gilbert-Varshamov bound. In 1982 this turned out to be false as Tsfasman, Vlăduţ and Zink were able to combine Goppa codes and deep results from algebraic geometry to construct a sequence of error correcting codes which beat the Gilbert-Varshamov bound ([51]).

Since then, algebraic geometry codes over curves have been largely studied. Many families of curves have been considered in order to construct good codes, for instance Hermitian curves ([60], [40], [50], [59]), Castle curves ([39], [41]), Suzuki curves ([20]) and Giulietti-Korchmáros curves ([7]). Starting from 1986 lot of work on codes from curves was also devoted to decoding methods ([43], [9], [8]). At last but not least, Goppa codes over curves were and are still studied for application to the McEliece public-key cryptographic system ([35]). Even though Goppa construction holds on varieties of dimension higher than one, the literature is less abundant in this context. However, one can consult [32] for a survey of Little and [21] for an extensive use of intersection theory involving the Seshadri constant proposed by S. H. Hansen. Some work has also been undertaken in the direction of surfaces. Rational surfaces yielding to good codes were constructed by Couvreur in [12] from some blow-ups of the plane and by Blache *et al.* in [10] from Del Pezzo surfaces. Codes from cubic surfaces were studied by Voloch and Zarzar in [55], from toric surfaces by J. P. Hansen in [19], from Hirzebruch surfaces by Nardi in [42], from ruled surfaces by Aubry in [1] and from abelian surfaces by Haloui in [18], in the specific case of simple Jacobians of genus 2 curves. Furthermore Voloch and Zarzar ([55], [61]) and Little and Schenck ([30]) have studied surfaces whose arithmetic Picard number is one.

In this thesis...

The main purpose of this thesis is to provide a study of the minimum distance $d(X, G, S)$ of the algebraic geometry code $\mathcal{C}(X, G, S)$ (defined in Section 2.2) constructed from an algebraic surface X defined over a finite field, a set S of rational points on X and a rational effective ample divisor G on X avoiding S. In what follows we offer a detailed outline of this thesis.

Chapter 1 and 2 provide a general introduction to algebraic surfaces and to algebraic geometry codes. In the first chapter we treat general definitions and basic results on algebraic varieties of any dimension, then we move to dimension two in order to state and prove some results from intersection theory. In the second chapter we introduce evaluation codes, we prove the bounds for the dimension and the minimum distance of the classical Goppa codes, i.e. evaluation codes from algebraic curves, and we begin the study of codes from algebraic surfaces. For this last purpose, at the end of Chapter 2, we recall and prove some upper bounds for the number of rational points on curves on smooth surfaces.

In Chapter 3, we study the minimum distance of codes from algebraic surfaces trying to keep our study as generic as possible, with the aim to point out which surfaces are more suitable for constructing good codes. We prove in Section 3.1 lower bounds for the minimum distance $d(X, G, S)$ of the code $\mathcal{C}(X, G, S)$, under some specific assumptions on the geometry of the surface itself. Two quite wide families of surfaces are studied. The first one is that of surfaces whose canonical divisor is either nef or anti-strictly nef. The second one consists of surfaces which do not contain irreducible curves of low genus. We obtain the following theorem,

where we denote, as in the whole thesis, the finite field with q elements by $\mathbb{F}_q$ and the virtual arithmetic genus of a divisor D by π_D, and where we set $m := \lfloor 2\sqrt{q} \rfloor$.

Theorem. *(Theorem 3.1.2 and Theorem 3.1.4) Let X be an absolutely irreducible smooth projective algebraic surface defined over $\mathbb{F}_q$ whose canonical divisor is denoted by K_X. Consider a set S of rational points on X, a rational effective ample divisor H avoiding S, and a positive integer r. In order to compare the following bounds, we set*

$$d^*(X, rH, S) := \#S - rH^2(q + 1 + m) - m(\pi_{rH} - 1).$$

1) (i) If K_X is nef, then

$$d(X, rH, S) \geqslant d^*(X, rH, S).$$

(ii) If $-K_X$ is strictly nef, then

$$d(X, rH, S) \geqslant d^*(X, rH, S) + mr(\pi_H - 1).$$

2) If there exists an integer $\ell > 0$ such that any $\mathbb{F}_q$-irreducible curve lying on X and defined over $\mathbb{F}_q$ has arithmetic genus strictly greater than ℓ, then

$$d(X, rH, S) \geqslant d^*(X, rH, S) + \left(rH^2 - \frac{\pi_{rH} - 1}{\ell} \right) (q + 1 + m).$$

Inside both families, adding some extra geometric assumptions on the surface yields in Section 3.2 to some improvements for these lower bounds. This is the case for surfaces whose arithmetic Picard number is one, for surfaces without irreducible curves defined over $\mathbb{F}_q$ with small self-intersection, so as for fibered surfaces. In particular, Theorems 3.2.8 and 3.2.9 (that hold for fibered surfaces $X \to B$) improve the bounds of Theorems 3.1.2 and 3.1.4 (that hold for the whole wide families). Indeed, the bound on the minimum distance $d(X, G, S)$ is increased by the non-negative *defect* $\delta(B) = q + 1 + mg_B - \#B(\mathbb{F}_q)$ of the base curve B. Finally in Section 3.3 we specify our bounds to the case of surfaces of degree $d \geqslant 3$ embedded in $\mathbb{P}^3$.

The results we present in Chapter 3 appear in a joint paper with Y. Aubry, F. Herbaut and M. Perret ([6]) accepted for publication in Contemporary Mathematics of the AMS.

The aim of Chapter 4 is to study codes from abelian surfaces defined over finite fields. First, in Section 4.1, we discuss the parameters of codes from abelian surfaces and we give a lower bound on the minimum distance of these codes using results from Chapter 3. Secondly, in Section 4.2, we sharpen our lower bound in the case of codes from abelian surfaces which do not contain absolutely irreducible curves defined over $\mathbb{F}_q$ of arithmetic genus less than or equal to a fixed integer ℓ . We summarise our results in the following theorem.

Theorem. *(Theorem 4.1.2 and Theorem 4.2.3) Let A be an abelian surface defined over $\mathbb{F}_q$ of trace $\mathrm{Tr}(A)$. Consider a set S of rational points on A, a rational effective ample divisor H on A avoiding S, and a positive integer r. Then the minimum distance $d(A, rH, S)$ of the code $\mathcal{C}(A, rH, S)$ satisfies*

$$d(A, rH, S) \geqslant \#S(\mathbb{F}_q) - rH^2(q + 1 - \mathrm{Tr}(A) + m) - mr^2 \frac{H^2}{2}. \qquad (1)$$

Moreover, if A is simple and contains no absolutely irreducible curves of arithmetic genus less than or equal to ℓ, for some positive integer ℓ, then

$$d(A, rH, S) \geqslant \#S(\mathbb{F}_q) - \max\left(\left\lfloor r\sqrt{\frac{H^2}{2}}\right\rfloor(\ell-1), \varphi(1), \varphi\left(\left\lfloor r\sqrt{\frac{H^2}{2\ell}}\right\rfloor\right)\right), \qquad (2)$$

where

$$\varphi(x) := m\left(r\sqrt{\frac{H^2}{2}} - x\sqrt{\ell}\right)^2 + 2m\sqrt{\ell}\left(r\sqrt{\frac{H^2}{2}} - x\sqrt{\ell}\right) + x\left(q+1-\mathrm{Tr}(A)+(\ell-1)\left(m-\sqrt{\ell}\right)\right) + r\sqrt{\frac{H^2}{2}}(\ell-1).$$

If A is simple then we can take $\ell = 1$ and the lower bound (2) is nothing but Haloui's one stated in [18] only in the case of simple Jacobian surfaces $\mathrm{Jac}(C)$ with the choice $H = C$ (see Remark 4.2.4). However, it holds here also for simple Weil restrictions of elliptic curves on a quadratic extension and for abelian surfaces which do not admit a principal polarization.

It is worth to notice that the lower bound (2) is better for large ℓ (at least for q sufficiently large and $1 < r < \sqrt{q}$, see Remark 4.2.5). In particular the bound obtained for $\ell = 2$ improves the one obtained for $\ell = 1$. This leads us to investigate in Section 4.3 the case of abelian surfaces with no absolutely irreducible curves of genus 1 nor 2, which are necessarily Weil restrictions of elliptic curves or not principally polarizable abelian surfaces, from the classification we give in Subsection 1.4.3. The following proposition lists all situations for which we can apply bound (2) with $\ell = 2$.

Proposition. *(Proposition 4.3.2 and Proposition 4.3.3) The bound on the minimum distance (2) of the previous theorem holds when taking $\ell = 2$ in the two following cases.*

1. *Let A be an abelian surface defined over $\mathbb{F}_q$ which does not admit a principal polarization. Then A does not contain absolutely irreducible curves of arithmetic genus 0, 1 nor 2.*
2. *Let q be a power of a prime p. Let E be an elliptic curve defined over $\mathbb{F}_{q^2}$ of Weil polynomial $f_{E/\mathbb{F}_{q^2}}(t) = t^2 - \mathrm{Tr}(E/\mathbb{F}_{q^2})t + q^2$. Let A be the $\mathbb{F}_{q^2}/\mathbb{F}_q$-Weil restriction of the elliptic curve E. Then A does not contain absolutely irreducible curves defined over $\mathbb{F}_q$ of arithmetic genus 0, 1 nor 2 if and only if one of the following cases holds:*
   - *(i)* $\mathrm{Tr}(E/\mathbb{F}_{q^2}) = 2q - 1$;
   - *(ii)* $p > 2$ *and* $\mathrm{Tr}(E/\mathbb{F}_{q^2}) = 2q - 2$;
   - *(iii)* $p \equiv 11 \mod 12$ *or* $p = 3$, q *is a square and* $\mathrm{Tr}(E/\mathbb{F}_{q^2}) = q$;
   - *(iv)* $p = 2$, q *is nonsquare and* $\mathrm{Tr}(E/\mathbb{F}_{q^2}) = q$;
   - *(v)* $q = 2$ *or* $q = 3$ *and* $\mathrm{Tr}(E/\mathbb{F}_{q^2}) = 2q$.

Finally, in Section 4.4, we make explicit the terms that appear in the lower bounds obtained for the minimum distance.

The results we present in Chapter 4 appear in a joint paper with Y. Aubry, F. Herbaut and M. Perret ([5]) submitted to an international review.

Characterising surfaces that yield good codes seems to be a complex question. It is not the goal of this thesis to produce good codes: we aim to give theoretical bounds on the minimum distance of algebraic geometry codes on general surfaces. However, one can derive from our work one or two heuristics. Indeed, Theorem 3.1.4 and Theorem 4.2.3 suggest to look for surfaces with no curves of small genus and fibered surfaces provide natural examples of such surfaces (see Theorem 3.2.9) as well as abelian surfaces from Proposition 4.3.2 and Proposition 4.3.3.

Chapter 1

Algebraic surfaces over finite fields

When thinking about algebraic surfaces the very first reference one has in mind is Chapter V of Hartshorne's famous volume Algebraic Geometry ([22]), which is in fact the main source of inspiration here, as long as Shafarevich's Basic Algebraic Geometry 1 ([47]), Hindry and Silverman's Diophantine Geometry ([23]) and Silverman's Arithmetic of Elliptic Curves ([49]). Far from the richness and completeness of the yellow books, this chapter is conceived to recall the definitions and some known results on algebraic surfaces. Our aim is to state here all the properties we shall use later, in order for this thesis to be, as far as possible, self-contained.

This chapter is structured as follows. We give the basic definitions in the context of algebraic projective varieties in Section 1.1. In Section 1.2, we introduce the notion of divisor and the Riemann-Roch space. In Section 1.3 we focus on algebraic surfaces, we introduce intersection theory over surfaces and recall some results in this context. In particular we prove the useful corollary of the Hodge index theorem (Lemma 1.3.6) which is one of the key tools in the proofs of our main theorems. Finally, Section 1.4 is devoted to abelian surfaces, a family of algebraic surfaces that will be the main character of Chapter 4. Here the leading reference will be Milne's Abelian Varieties ([36]).

1.1 Algebraic projective varieties

In this section we work over a perfect field k whose algebraic closure is denoted by $\overline{k}$. Nevertheless, the field we have in mind in this thesis is the finite field $\mathbb{F}_q$ with q elements, where q is the power of a prime p.

For further details on this first part we refer to [47] and [22] for when $k = \overline{k}$ is an algebraically closed field and to [23] and [49] for the reader interested in possibly non algebraically closed field.

1.1.1 Basic definitions

The affine space $\mathbb{A}^n(\overline{k})$ or just $\mathbb{A}^n$ is the set of n-tuples $(a_1, \ldots, a_n)$ with coordinates in $\overline{k}$. The rational points on $\mathbb{A}^n$ are the n-tuples with coordinates in k. We classically define the projective space $\mathbb{P}^n(\overline{k})$ ($\mathbb{P}^n$ for short) to be the set of equivalence classes of points in $\mathbb{A}^{n+1} \setminus \{0\}$ under the equivalence relation given by $(a_0, \ldots, a_n) \sim (\lambda a_0, \ldots, \lambda a_n)$ for every $\lambda \in \overline{k} \setminus \{0\}$. We denote the equivalence

class of a point P by $(a_0 : \ldots : a_n)$ and we call $(a_0, \ldots, a_n)$ a set of homogeneous coordinates for the point P. Note that $\mathbb{P}^n$ contains many copies of $\mathbb{A}^n$.

A rational point on $\mathbb{P}^n$ is a class of a point $(a_0 : \ldots : a_n)$ that admits at least one set of homogeneous coordinates in $\mathbb{A}^{n+1}(k)$ or, equivalently, has one $a_j \neq 0$ such that $a_i/a_j \in k$ for every $i = 1 \ldots, n$. With an abuse of notation the set of rational points on $\mathbb{P}^n$ can be defined as

$$\mathbb{P}^n(k) \coloneqq \{(a_0 : \ldots : a_n) \in \mathbb{P}^n \mid a_i \in k \ \forall i\}.$$

The notion of algebraic variety is normally introduced on the affine space and can then be naturally extended to the projective space. In this section we focus on basic definitions on projective algebraic varieties and we refer the reader to the books cited at the beginning of this chapter for an introduction to affine algebraic varieties. Anyway the following definitions can be read as definitions in the context of affine varieties by replacing $\mathbb{P}^n$ by $\mathbb{A}^n$, $\overline{k}[x_0, \ldots, x_n]$ by $\overline{k}[x_1, \ldots, x_n]$, and by dropping the hypothesis of homogeneity on the polynomials and on the ideals. We recall also that any affine variety can be uniquely identified with a projective variety, namely its projective closure (see for instance [49, I §2]).

An *homogeneous ideal* $I \subset \overline{k}[x_0, \ldots, x_n]$ is an ideal that is generated by *homogeneous polynomials*, that are polynomials f such that

$$f(\lambda x_0, \ldots, \lambda x_n) = \lambda^{\deg f} f(x_0, \ldots, x_n) \quad \text{for every } \lambda \in \overline{k}.$$

A projective algebraic set X is a subset of $\mathbb{P}^n$ which consists of all points at which a certain finite number of homogeneous polynomials with coefficient in $\overline{k}$ vanish. Formally this means that there exists an homogeneous ideal $I \subset \overline{k}[x_0, \ldots, x_n]$ such that

$$X = Z(I) \coloneqq \{P \in \mathbb{P}^n \mid f(P) = 0 \text{ for every homogeneous } f \in I\}.$$

Note that the property of f to be zero at P depends only on the equivalence class of P, thus the previous set is well-defined.

The Zariski topology is defined on $\mathbb{P}^n$ by taking the open sets to be the complements of algebraic sets.

For an algebraic set $X \subset \mathbb{P}^n$ we define its (homogeneous) ideal to be

$$I(X) \coloneqq \{f \in \overline{k}[x_0, \ldots, x_n] \mid f \text{ is homogeneous and } f(P) = 0 \ \forall P \in X\}.$$

If $I(X)$ can be generated by homogeneous polynomials with coefficients in k, we say that X is defined over k. If this is the case, then the set of rational points on X is

$$X(k) = X \cap \mathbb{P}^n(k).$$

If X is defined over k and $I(X) \cap k[x_0, \ldots, x_n]$ is a prime ideal of $k[x_0, \ldots, x_n]$, we say that X is irreducible over k or *k-irreducible*. If X is irreducible over $\overline{k}$, that is if $I(X)$ is a prime ideal of $\overline{k}[x_0, \ldots, x_n]$, then we say that X is *absolutely irreducible* or equivalently geometrically irreducible.

Definition 1.1.1. An *algebraic projective variety* X over k is an algebraic k-irreducible set of $\mathbb{P}^n$.

1.1.2 Regular and rational functions

Let X be a projective variety defined over k. The (homogeneous) *coordinate ring* of X is defined by $k[X] \coloneqq k[x_0, \ldots, x_n]/I(X)$.

A function $f : X \to k$ is regular at a point $P \in X$ if there exists an open affine subset $U \subset X$ containing P such that over U we have $f = h/g$ for $h, g \in k[x_0, \ldots, x_n]$ two homogeneous polynomials of same degree with g non zero on U (in particular $g(P) \neq 0$). Note that since h and g are homogeneous and of the same degree, h/g is well defined on the projective space (wherever g is non-zero). A function regular at every points on X is called a *regular function*. The ring of all regular functions on X is denoted by $\mathcal{O}_X$. The *function field* of X, denoted by $k(X)$, is defined to be the set of couples (f, U) where f is a regular function on a non-empty open set U, under the relation that $(f_1, U_1) = (f_2, U_2)$ if $f_1 = f_2$ on $U_1 \cap U_2$. An element in $k(X)$ is called a *rational function*. Observe that $k(X)$ is a field. We define in the same way the function field $\overline{k}(X)$ considering regular functions from X to $\overline{k}$.

Definition 1.1.2. The dimension of an algebraic variety X is the transcendence degree of $\overline{k}(X)$ over $\overline{k}$. Varieties of dimension one are called *curves* while varieties of dimension two are called *surfaces*. If $X' \subset X$ is an algebraic subvariety of X then the quantity $\dim(X) - \dim(X')$ is called the codimension of X' (in X).

1.1.3 Local rings

For any point P on X we can consider the set of rational functions that are *regular* or defined at P, that is

$$\mathcal{O}_{P,X} = \left\{ f = \frac{h}{g} \in \overline{k}(X) \;\middle|\; g(P) \neq 0 \right\}.$$

One can easily see that $\mathcal{O}_{P,X}$ is in fact the localization of $\mathcal{O}_X$ at the (maximal) ideal

$$\mathcal{M}_P = \{ f \in \mathcal{O}_X \mid f(P) = 0 \}.$$

$\mathcal{O}_{P,X}$ is called the *local ring* of X at P. The ideal $\mathcal{M}_P$ allows to characterise singular points on X as follows.

Definition 1.1.3. Let X be a projective algebraic variety. We say that X is *non-singular* at a point P if $\dim_{\overline{k}} \mathcal{M}_P/\mathcal{M}_P^2 = \dim X$. If X is nonsingular at any P then we say that X is nonsingular or *smooth*. Otherwise X is called *singular*.

1.1.4 Maps between varieties

So far we have defined algebraic varieties and their function fields. Now we introduce maps between algebraic varieties. In what follows, when we do not explicitly specify the embedding of the variety, the definitions and results are valid for both affine and projective varieties.

Definition 1.1.4. Let X and X' be two varieties. A map $\varphi : X \to X'$ is a *morphism* if it is continuous and for every function f regular on an open set $U \subset X'$ the composition $f \circ \varphi$ is regular on $\varphi^{-1}(U)$. A map between varieties is *regular* at a point if it is a morphism on an open neighbourhood of the point.

Note that the image of a projective variety by a morphism is a projective variety (see [23, A.1.2]).

Definition 1.1.5. Let $\varphi : X \to X'$ be a regular map. For $P \in X'$ we define the *fiber* of φ over P to be $\varphi^{-1}(P)$.

It can be shown (see [47, Th.1.25]) that if X and X' are of dimension n and m respectively and if φ is surjective, then $m \leqslant n$ and for any $P \in X'$ and for any component F of the fiber $\varphi^{-1}(P)$ we have $\dim F \geqslant n - m$.

Definition 1.1.6. A *rational map* $\varphi : X \to X'$ is an equivalence class of pairs (U, φ_U) where φ_U is a morphism of a non-empty set of $U \subset X$ to X'. Two pairs (U, φ_U) and (V, φ_V) are equivalent if $\varphi_U = \varphi_V$ on $U \cap V$. A rational map φ is *dominant* if $\varphi(U)$ is dense in X' for some (and hence every) non-empty open set $U \subset X$ on which φ is a morphism.

Any morphism $\varphi : X \to X'$ between affine varieties induces an homomorphism from $k[X']$ to $k[X]$. We say that φ is finite if $k[X]$ is finitely generated as a $k[X']$-module.

Definition 1.1.7. A morphism $\varphi : X \to X'$ between projective varieties is *finite* if for every affine open subset $U \subset X'$, the set $\varphi^{-1}(U)$ is affine and the restriction map $\varphi : \varphi^{-1}(U) \to U$ is finite.

Any dominant rational map $\varphi : X \to X'$ induces a map $\varphi^* : k(X') \to k(X)$ ([22, I §4]). If φ is finite its *degree* is defined to be $\deg \varphi := [k(X) : \varphi^* k(X')]$.

1.2 Divisors

Let X be a smooth projective variety defined over k. A *divisor* on X is a formal sum of irreducible subvarieties of codimension 1 in X with assigned multiplicities. Usually we write $D = \sum_i n_i D_i$ where the n_i are integers and the D_i are k-irreducible subvarieties defined over k of codimension 1 in X. We allow the D_i's to be singular. Note that an irreducible subvariety of codimension 1, $C \subset X$, is also a divisor, sometime called a prime divisor. If all the n_i equal 0, we write $D = 0$. If all $n_i \geqslant 0$ then we say that D is *effective* and we write $D \geqslant 0$. The support of D, denoted by $\mathrm{Supp}(D)$, is the set of the irreducible varieties D_i's which appear in the decomposition of D with a non-zero coefficient. We denote by $\mathrm{Div}(X)$ the set of divisors on X. It is a free abelian group generated by the irreducible subvarieties of codimension 1 in X.

1.2.1 Principal divisors and the Picard group

Let $k(X)$ be the function field of X. To any function $f \in k(X)$ we can associate its divisor, denoted by (f). As to do so, we associate to any non zero function f an integer $\mathrm{ord}_C(f)$, for $C \subset X$ a prime divisor, as follows. Let $U \subset X$ be an open set intersecting C. Let $\mathcal{O}_C$ be the set of rational functions on X that are defined on U, then $\mathcal{O}_C$ is a discrete valuation ring (see for exemple [37, 8.b]). We let ord_C be the associated valuation. This depends only on C and not on U. For any $f \in k(X)$ we can write $f = h/g$ with $h, g \in \mathcal{O}_C$ and define $\mathrm{ord}_C(f) = \mathrm{ord}_C(h) - \mathrm{ord}_C(g)$. One

can think of $\mathrm{ord}_C(f)$ as the measure of the order of zero or pole of f along C. In particular if $\mathrm{ord}_C(f) = m > 0$, we say that f has a zero of order m along C, while if $\mathrm{ord}_C(f) = -m < 0$, we say that f has a pole of order m along C. One can prove that $ord_C(f)$ is not zero only for finitely many C. Thus we can write

$$(f) = \sum_{C \subset X} \mathrm{ord}_C(f) C.$$

We can also write (f) as

$$(f) = (f)_0 - (f)_\infty = \sum_{\substack{C \subset X \\ \mathrm{ord}_C(f) > 0}} \mathrm{ord}_C(f) C - \sum_{\substack{C \subset X \\ \mathrm{ord}_C(f) < 0}} -\mathrm{ord}_C(f) C$$

where $(f)_0$ and $(f)_\infty$ are the effectif divisor of zeroes and of poles of f, respectively. It is easy to see that the definition of (f) agrees with the general one we gave for divisors on X. Divisors associated to rational functions on X are called *principal divisors*. The set of principal divisors $\mathrm{Princ}(X)$ is a subgroup of $\mathrm{Div}(X)$. The quotient is the *Picard group* $\mathrm{Pic}(X)$. Two divisors on X are said to be *linearly equivalent* if they belong to the same class in $\mathrm{Pic}(X)$, that is if their difference is a principal divisor. We sometime write $[D]$ to denote the class of the divisor D in $\mathrm{Pic}(X)$.

1.2.2 The Riemann-Roch Space

For any divisor D on X we can consider the set

$$L(D) = \{f \in k(X) \setminus \{0\} \mid (f) + D \geqslant 0\} \cup \{0\}.$$

$L(D)$ together with the usual operations on functions is a k-vector space, called the *Riemann-Roch space* associated to D. Indeed, if we write $D = \sum_i n_i D_i$, the condition $(f) + D \geqslant 0$ is equivalent to say $\mathrm{ord}_{D_i}(f) \geqslant -n_i$ and $\mathrm{ord}_C(f) \geqslant 0$ for any $C \neq D_i$. By the standard properties of valuations, that are $\mathrm{ord}_C(f_1 f_2) = \mathrm{ord}_C(f_1) + \mathrm{ord}_C(f_2)$ and $\mathrm{ord}_C(f_1 + f_2) \geqslant \min\{\mathrm{ord}_C(f_1), \mathrm{ord}_C(f_2)\}$ if $f_1 + f_2 \neq 0$, we easily get that $L(D)$ is a k-vector space. The Riemann-Roch space $L(D)$ is a finite dimensional space, but we are not going to prove it. Its dimension is denoted by $\ell(D)$.

One of the interesting feature of the Riemann-Roch space $L(D)$ is that, if $\ell(D) \geqslant 1$, it allows to define a rational map from the variety to the projective space of dimension $\ell(D) - 1$. Indeed, let D be a divisor on X and let $\{f_0, \ldots, f_{\ell-1}\}$ be a basis of $L(D)$, for $\ell = \ell(D)$. Then we can define the following map

$$\begin{aligned} \varphi_D : \quad & X \longrightarrow \mathbb{P}^{\ell-1} \\ & P \longmapsto (f_0(P) : \ldots : f_{\ell-1}(P)). \end{aligned}$$

Definition 1.2.1 (Ample and very ample divisors)**.** If the map φ_D is an embedding of X in $\mathbb{P}^{\ell-1}$ then we say that D is *very ample*. Moreover, we say that a divisor H on X is *ample* if rH is very ample for some $r > 0$.

1.2.3 Differential forms and the canonical divisor

In this subsection we define the canonical divisor of an algebraic variety. For the reader who is more interested in the theory of algebraic geometry codes, it suffices to know that the canonical divisor is one of the most important birational invariant of a variety. As a matter of fact, one of the bounds on the minimum distance of codes that we prove in this thesis depends on some characterization of the canonical divisor.

In order to define the canonical divisor properly but without writing a course on differential forms, we take the assumption that the reader is familiar with differential forms and we refer to [47, III,§5] for more details on this topic.

Let n denotes the dimension of X. For an integer $r \geqslant 1$, let $\Omega^r[X]$ be the $k[X]$-module of all differential r-forms on X. An element $\omega \in \Omega^r[X]$ can be written in a neighbourhood U of any point in the form

$$\omega = \sum_{1 \leqslant i_1 \leqslant \cdots \leqslant i_r \leqslant n} g_{i_1 \ldots i_r} df_{i_1} \wedge \cdots \wedge df_{i_r},$$

for $g_{i_1 \ldots i_r}, f_{i_1} \ldots f_{i_r}$ regular functions on U. Introducing the equivalence relation $(\omega, U) \sim (\omega', U')$ if $\omega = \omega'$ on $U \cap U'$ allows to define a *rational differential r-form* to be an equivalence class under this relation. The set of these classes is denoted by $\Omega^r(X)$. It is a vector space over $k(X)$ of dimension $\binom{n}{r}$.

Let us consider a differential n-form ω on X. In some neighbourhood U of a point $P \in X$, we can write $\omega = g du_1 \wedge \cdots \wedge du_n$. If we cover X with open sets U_i such that $\omega = g_i du_{i,1} \wedge \cdots \wedge du_{i,n}$, we get on $U_i \cap U_j$

$$g_j = g_i \mathbf{J}\left(\frac{u_{i,1}, \ldots, u_{i,n}}{u_{j1}, \ldots, u_{j,n}}\right)$$

where $\mathbf{J}$ denotes the Jacobian determinant. The system of functions g_i on U_i defines a divisor called the divisor of ω and denoted by (ω). It satisfies the following property:

$$(f\omega) = (f) + (\omega) \text{ for every } f \in k(X). \tag{1.1}$$

Note that $\Omega^n(X)$ is a vector space of dimension $1 = \binom{n}{n}$ over $k(X)$. Therefore by property (1.1) all the $\omega \in \Omega^n(X)$ are linearly equivalent and thus belong to the same class in $\mathrm{Div}(X)$.

Definition 1.2.2. The divisor class (ω) is called the *canonical class* or simply the *canonical divisor* of X. It is denoted by K_X. We call $-K_X$ the *anti-canonical divisor*.

1.3 Intersection theory on algebraic surfaces

So far we have worked with varieties of any dimension since basic definitions on algebraic varieties can be stated without difficulty in the general setting. Now, in order to introduce intersection theory, we focus on the varieties we are interested in. Therefore, with all the previous definitions in mind, we consider X to be a projective, smooth, absolutely irreducible algebraic variety of dimension 2 defined over $k = \mathbb{F}_q$. We call X an algebraic surface or simply a *surface*.

Intersection theory has almost become a mainstream tool to study codes over surfaces (see [1], [21], [55], [61], [30]) and it is also central in our proofs. We recall in this section the few results of intersection theory on surfaces we need and we refer the reader to [22, §V] for the proofs of the theorems and other further details. Even though we have a unique intersection theory on varieties of any dimension, the Hodge index inequality - on which relies most of the bounds for the minimum distance we are going to prove in this thesis - is no longer valid for varieties of dimension 3 or more. For the reader interested in intersection theory on varieties of any dimension we recommend [28], where one can also find a generalised form of the Hodge index inequality (Theorem 1.6.1).

1.3.1 The intersection pairing

First of all we need to define the notion of intersection of two divisors on X. The subvarieties of codimension 1 in a surface are curves, thus divisors on X are formal sums of curves. Let $C, C' \subset X$ be irreducible curves on X. If $P \in C \cap C'$ is a point of intersection of C and C', we say that C and C' meet transversally at P if their local equations generate the maximal ideal $\mathcal{M}_P$ of $\mathcal{O}_{P,X}$. If C and C' meet everywhere transversally, we naturally want to define their intersection number to be the number of points of $C \cap C'$. This definition can be extended to all divisors on X as shown in the following theorem.

Theorem 1.3.1. *Let D, D' be any two divisors on X. There is a unique symmetric bilinear paring*

$$\begin{array}{ccc} \mathrm{Div}(X) \times \mathrm{Div}(X) & \longrightarrow & \mathbb{Z} \\ (D, D') & \longmapsto & D.D' \end{array}$$

such that

1. *if D and D' are prime divisors that meet everywhere transversally, then $D.D' = \#(D \cap D')$;*
2. *if $D \sim D'$ then $D.D'' = D'.D''$ for any $D'' \in \mathrm{Div}(X)$.*

Notation 1. We denote the self-intersection of a divisor $D.D$ by D^2.

Example 1.3.2. Let $X = \mathbb{P}^2$. We have $\mathrm{Pic}(X) = \mathbb{Z}$. Pick the class of a line L as a generator for $\mathrm{Pic}(X)$. Any curve on X is then linearly equivalent to dL, d being the degree of the curve. Since lines are linearly equivalent to each other and since two lines intersect transversally in one point, we have $L^2 = 1$. So if $C \sim nL$ and $C' \sim mL$ are two prime divisors, we have $C.C' = nm$. By linearity of the intersection pairing, this gives the intersection on all X.

Definition 1.3.3 (Nef and strictly-nef divisors)**.** A divisor D on X is said to be *nef* (respectively *strictly nef*) if $D.C \geqslant 0$ (respectively $D.C > 0$) for any irreducible curve C on X. A divisor D is said to be *anti-nef* if $-D$ is nef.

1.3.2 The Néron-Severi and the numerical groups

We have already defined the linear equivalence between divisors and the Picard group $\mathrm{Pic}(X)$. We are now going to define the coarser *algebraic equivalence*.

Let C be an irreducible curve. For any point $Q \in C$ we can define an embedding $i_Q : X \hookrightarrow X \times C$ by $P \mapsto (P, Q)$. If $D \in \mathrm{Div}(X \times C)$ is such that $X \times Q \not\subset \mathrm{Supp}(D)$, then $i_Q^*(D)$ defines a pullback divisor on X. We define an algebraic family of divisors on X to be a map $f : C \to \mathrm{Div}(X)$ such that there exists a divisor $D \in \mathrm{Div}(X \times C)$ for which the pullback $i_Q^*(D)$ is defined for every $Q \in C$ and $i_Q^*(D) = f(Q)$. For a definition of algebraic families in term of effective divisors flat over C one can consult [22, §III, 9.8.5]. We say that two divisors D, D' on X are algebraically equivalent if there are two points $Q, Q' \in C$ such that $f(Q) = D$ and $f(Q') = D'$. The *Néron-Severi group* of X, denoted by $\mathrm{NS}(X)$, is obtained by considering the group of divisors on X modulo the algebraic equivalence. It was proved by Severi (in characteristic 0) and by Néron (in the general case) that for a smooth projective variety X, $\mathrm{NS}(X)$ is finitely generated. Its rank is called the arithmetic Picard number of X, or *Picard number* for short.

A divisor D on X is said to be *numerically equivalent* to zero, which we denote by $D \equiv 0$, if the intersection product $C.D$ is zero for all curves C on X. This gives the coarsest equivalence relation on divisors on X and we denote the group of divisors modulo numerical equivalence by $\mathrm{Num}(X)$. The group $\mathrm{Num}(X)$ is the quotient of $\mathrm{NS}(X)$ by its torsion subgroup, thus it is also finitely generated and, by construction, it is torsion free.

1.3.3 Classical results of intersection theory

Let us emphasize four classical results of intersection theory that we will use in this thesis.

The first one is (a generalisation of) the *adjunction formula* (see [22, §V, Exercise 1.3]). For any $\mathbb{F}_q$-irreducible curve C on X of arithmetic genus π_C, we have

$$C.(C + K_X) = 2\pi_C - 2 \tag{1.2}$$

where K_X is the canonical divisor of X. This formula allows to define the virtual arithmetic genus π_D of any divisor D on X: $\pi_D \coloneqq D.(D + K_X)/2 + 1$.

The second one is a simple outcome of Bézout's theorem in projective spaces (and the trivial part of the Nakai-Moishezon criterion). It ensures that for any ample divisor H on X and for any irreducible curve C on X, we have $H^2 > 0$ and $H.C > 0$.

The third one is the Riemann-Roch theorem for algebraic surfaces which gives a formula to compute the dimension of the Riemann-Roch space $L(D)$ (introduced in Subsection 1.2.2) where D is a divisor on a surface X. We refer the reader to [22, V, §1, Th. 1.6] for a proof of Riemann-Roch theorem over algebraically closed field. The statement follows (non trivially) on any field where X and D are defined.

Theorem 1.3.4 (Riemann-Roch)**.** *Let D be any divisor on the surface X. Then we have*

$$\ell(D) - s(D) + \ell(K_X - D) = \frac{1}{2} D.(D - K_X) + 1 + p_a(X),$$

where $p_a(X)$ is the arithmetic genus of X, and $s(D)$ is the so-called superabundance *of D in X.*

We shall use this theorem to give an estimation of the dimension of our codes in the next chapter.

Finally the last result we recall is the *Hodge index theorem*, from which we can derive one useful inequality.

Theorem 1.3.5 (Hodge Index Theorem)**.** *Let $H \in \mathrm{Div}(X)$ be an ample divisor and let $D \in \mathrm{Div}(X)$ be a divisor non numerically equivalent to 0 and such that $D.H = 0$. Then $D^2 < 0$.*

We refer the reader to [22, V,§1, Th. 1.9] for a prove of the Hodge index theorem and an explication of its name.

From this theorem one can derive a well-known inequality which links the intersection number of two divisors with the product of their self-intersections. This is sometimes called an *Hodge index inequality* and it is central in our proofs.

Lemma 1.3.6. *Let H be an ample divisor on X and D be any divisor on X. We have*

$$H^2D^2 \leqslant (H.D)^2, \tag{1.3}$$

with equality if and only if D and H are numerically proportional.

Proof. For any divisor $D \in \mathrm{Div}(X)$, consider the projection $\widehat{D}$ of D on the orthogonal $< H >^{\perp}$ in the Néron-Severi space,

$$\widehat{D} = D - \frac{H.D}{H^2}H.$$

Since H is ample, the Hodge index theorem gives that the intersection pairing is negative definite on $< H >^{\perp}$. Thus $\widehat{D}.\widehat{D} \leqslant 0$ with equality if and only if $\widehat{D} \equiv 0$. Hence $\left(D - \frac{H.D}{H^2}H\right).\left(D - \frac{H.D}{H^2}H\right) \leqslant 0$, that is, after some cancellation, $H^2D^2 \leqslant (H.D)^2$ with equality if and only if $D \equiv \frac{H.D}{H^2}H$.

□

1.4 Abelian Surfaces

In this section we discuss some properties of abelian varieties of dimension 2, that are *abelian surfaces*. We recall here all the results we shall need in Chapter 4 to study codes from abelian surfaces. We state basic definitions for abelian varieties of any dimension, then we give some results on the classification of abelian surfaces. We will use these last results in order to classify abelian surfaces which do not contain absolutely irreducible curves of low genus in Section 4.3. In this section we skip most of the details and we refer the reader to our main reference, Milne's Abelian Varieties ([36]), for an exhaustive introduction to abelian varieties. One can also consult [27] and [38].

1.4.1 Basic definitions

A *group variety* over a field k is a variety X defined over k together with two regular maps

$$m : X \times X \to X,\ i : X \to X,$$

and a point $e \in X(k)$ such that multiplication by m and inverse by i define a group structure on $X(\overline{k})$ with identity element e.

Definition 1.4.1. An *abelian variety* A is a connected and complete group variety.

It can be shown, but we will not do it, that the group law of an abelian variety is commutative and that an abelian variety is smooth. The first example of abelian varieties are elliptic curves, that are those of dimension one. Indeed, one can consider abelian varieties as higher-dimensional analogues of elliptic curves.

Definition 1.4.2. We say that an abelian variety A is *simple* if it does not contain non-zero proper sub-varieties, that is if there does not exist an abelian variety A' with $0 \subsetneq A' \subsetneq A$. Otherwise we say that A is *split*.

Note that the previous definition depends on the ground field k. Indeed, for any extension K of k if A is simple over k, or k-simple, it needs not to be simple over K. In particular, if A is simple over $\overline{k}$ we say that it is absolutely simple.

1.4.2 Isogeny classes and the Weil polynomial

Let A, A' be two abelian varieties and let $\varphi : A \to A'$ be an homomorphism. The *kernel* of φ is defined to be the fiber of φ over 0.

Proposition 1.4.3. *Let $\varphi : A \to A'$ be an homomorphism of abelian varieties. The following are equivalent:*

1. *φ is surjective and $\dim(A) = \dim(A')$;*
2. *$\ker(\varphi)$ is finite and $\dim(A) = \dim(A')$;*
3. *φ is finite, flat and surjective.*

Definition 1.4.4 (Isogeny)**.** We call an *isogeny* an homomorphism $\varphi : A \to A'$ satisfying the conditions in Proposition 1.4.3. The degree of an isogeny is its degree as a regular map, that is $\deg \varphi := [k(A) : \varphi^* k(A')]$.

Remark 1.4.5. The first example of an isogeny is the multiplication map $[n]_A : A \to A$ given by $a \mapsto na = a + \cdots + a$. For any integer n not divisible by the characteristic of k, we define the n-torsion group of A to be $A[n] := \ker([n]_A)$.

We recall that for a prime ℓ different from the characteristic of k, the *Tate module* of A is defined by

$$T_\ell A := \varprojlim A[\ell^n].$$

An element in $T_\ell A$ is an infinite sequence $(a_1, \dots, a_n \dots)$ such that $\ell a_1 = 0$, that is $a_1 \in A[\ell]$, and $\ell a_n = a_{n-1}$, thus $a_n \in A[\ell^n]$.

Proposition 1.4.6. *Let $\varphi : A \to A'$ be an isogeny of degree d. Then there exists another isogeny $\widehat{\varphi} : A' \to A$ of degree d such that $\varphi \circ \widehat{\varphi} = [d]_A$ and $\widehat{\varphi} \circ \varphi = [d]_{A'}$.*

If there exists an isogeny $A \to A'$ we write $A \sim A'$. From the previous proposition this is an equivalence relation. In order to characterize isogeny classes of abelian varieties, let us remark that if A is a simple abelian variety then every abelian variety isogenous to A is simple and thus it makes sense to talk about simple isogeny classes of abelian varieties. This is a consequence of the following theorem.

Theorem 1.4.7 (Poincaré Splitting Theorem)**.** *Let A be an abelian variety defined over k and let B be an abelian sub-variety of A. Then there exists an abelian sub-variety C of A such that the map $(x, y) \mapsto x + y$ gives an isogeny between $B \times C$ and A.*

The Weil polynomial of an abelian variety defined over $k = \mathbb{F}_q$ is the characteristic polynomial of the Frobenius endomorphism acting on its Tate module (note that it is independent of the prime ℓ). Weil proved that its roots are complex numbers of modulus $\sqrt{q}$, and they are called q-Weil numbers. The Honda-Tate theorem gives a bijection between simple abelian varieties up to isogenies and Weil numbers up to conjugacy. Since if A is split then its Weil polynomial is equal to the product of the Weil polynomials of its sub-varieties, the Honda-Tate theorem implies that the isogeny class of an abelian variety over a finite field is completely determined by its Weil polynomial.

When A is two-dimensional its Weil polynomial has the shape

$$f_A(t) = t^4 - \mathrm{Tr}(A)t^3 + bt^2 - q\,\mathrm{Tr}(A)t + q^2. \tag{1.4}$$

By Weil theorem one has $f_A(t) = (t-\omega_1)(t-\overline{\omega}_1)(t-\omega_2)(t-\overline{\omega}_2)$ where the ω_i's are complex numbers of modulus $\sqrt{q}$.

Definition 1.4.8. The number $\mathrm{Tr}(A) = \omega_1 + \overline{\omega}_1 + \omega_2 + \overline{\omega}_2$ is called the *trace of* A.

Isogeny classes of abelian surfaces will play an important role in Section 4.3 where we characterize abelian surfaces which do not contain absolutely irreducible curves of genus up to 2.

1.4.3 A classification of abelian surfaces

We need to introduce (principally) polarized abelian varieties. As to do so, let $\widehat{A}$ denotes the dual abelian variety of A (see [36, I §8] for a definition). For $P \in A$ and D a divisor on A, we write D_P for the translation of D by P, that is $D_P := D + P$. For any divisor on A we can thus define an homomorphism $\lambda_D : A \to \mathrm{Pic}(A)$ given by $P \mapsto [D_P - D]$. Note that when D is ample, λ_D is an isogeny (see [38, §8]).

Definition 1.4.9. An isogeny $\lambda : A \to \widehat{A}$ is called a *polarization* if over $\overline{k}$ it is equal to λ_H for some ample divisor H on A seen as a variety over $\overline{k}$. Moreover, if λ is of degree one we call it a *principal polarization* and the couple (A, λ) is called a *principally polarized abelian variety*.

From now on, we focus on abelian surfaces. While from the *geometric* point of view (i.e. over an algebraically closed field) a principally polarized abelian surface is isomorphic either to the Jacobian of a curve of genus 2 or to the product of two elliptic curves, the landscape turns to be richer from the *arithmetic* point of view. Indeed Weil proved the following theorem that classifies principally polarized abelian surfaces. We give it here in the form presented in [24].

Theorem 1.4.10 (Weil)**.** *Let (A, λ) be a principally polarized abelian surface defined over a field k. Then (A, λ) is either*

1. *the polarized Jacobian of a genus 2 curve;*
2. *the product of two polarized elliptic curves;*
3. *the Weil restriction of a polarized elliptic curve over a quadratic extension of k.*

Outside of principal polarized abelian surfaces, one can also consider abelian surfaces which do not admit a principal polarization. Non-principally polarized isogeny class of abelian surfaces are completely characterized by the following theorem, proved in [25, Th.1].

Theorem 1.4.11 (Howe, Maisner, Nart, Ritzenthaler, 2008, [25])**.** *An isogeny class of abelian surfaces defined over* $\mathbb{F}_q$ *with Weil polynomial* $f(t) = t^4+at^3+bt^2+qat+q^2$ *is not principally polarizable if and only if the following three conditions are satisfied:*

1. $a^2 - b = q$;
2. $b < 0$;
3. *all prime divisors of* b *are congruent to* $1 \mod 3$.

Chapter 2

Algebraic geometry codes

Error correcting codes are a powerful method to encode, store and transmit data with the capacity to detect and correct the errors that can occur during the storage and the transmission. Within these codes are the linear codes, which can be viewed from a mathematical point of view as vector spaces. Linear codes can be constructed using objects from algebraic geometry, and those codes are called algebraic geometry codes, or AG codes for short. Linear codes are characterised mainly by three parameters: their *length*, *dimension*, and *minimum distance*. This chapter is concerned with the construction of AG codes from algebraic surfaces and with the study of their parameters, with special regard to the minimum distance. After a brief introduction to linear codes in Section 2.1, we recall in Section 2.2 the construction of evaluation codes from algebraic varieties and we discuss the parameters of codes over curves, called Goppa codes. In Section 2.3 we begin the study of codes from surfaces and we prove the key Lemma 2.3.1 from which several lower bounds for the minimum distance of our codes will follow. In the optic of using Lemma 2.3.1, we need to bound the number of rational points on the curves that appear in the decomposition of divisors on surfaces. Thus in Section 2.4 we prove some upper bounds for the number of rational points on curves. Some of these bounds are general and well-known, while other are less known and can be proved using the fact that the curve is embedded in a smooth surface.

For a good introduction to the theory of algebraic geometry codes we refer the reader to [52] and [53]. One can also consult [13] and [29]. For an interesting study of codes from varieties of dimension 2 or more, one should address to [32] and [21]. Finally we cannot avoid to mention what is considered the Holy Bible of Error Correcting Codes, MacWilliams and Sloane's Theory of Error Correcting Codes ([33] and [34]), at which everyone interested in codes should take a look.

2.1 The parameters of a linear code

Let $\mathbb{F}_q^n$ be the n-dimensional vector space over $\mathbb{F}_q$. A *linear code* $\mathcal{C}$ of length n over the alphabet $\mathbb{F}_q$ can be thought of as a vector subspace of $\mathbb{F}_q^n$. An element of the code $\mathcal{C}$ is called a codeword and it is nothing more than a vector $c = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$. The *length* of the code corresponds to the length of every codeword while the *dimension* of the code is its dimension as a $\mathbb{F}_q$-vector space. The number of non-zero coordinates of a codeword c is called the *Hamming weight* of c and it is denoted by $\omega(c) := \#\{\ i \mid c_i \neq 0\}$. This quantity can be interpreted as the distance of the

codeword c from the zero-vector (that is itself a codeword) and allows to define the minimum distance of a code $\mathcal{C}$.

Definition 2.1.1. Let 0 denotes the zero-codeword of a code $\mathcal{C}$. The minimum distance of the code $\mathcal{C}$ is

$$d_{\mathcal{C}} \coloneqq \min_{c \in \mathcal{C} \setminus \{0\}} \{\omega(c)\}.$$

The dimension of a code is linked to its rate of transmission while the minimum distance is linked to the capacity of error detection and error correction. Indeed, it is well-known that a $[n, k, d]$-code, i.e. a linear code of length n, dimension k and minimum distance d, can detect $d-1$ errors and correct $\lfloor \frac{d-1}{2} \rfloor$ of them. Therefore it would be great to have codes with dimension and minimum distance as large as possible. Unfortunately, you cannot eat the cake and have it, and this proverb finds its correspondent in coding theory in the following proposition, known as the Singleton Bound.

Proposition 2.1.2 (Singleton Bound)**.** *Let $\mathcal{C}$ be a $[n, k, d]$-code. Then we have*

$$k + d \leqslant n + 1. \tag{2.1}$$

The Singleton Bound allows to give the following definition.

Definition 2.1.3. A $[n, k, d]$-code whose parameters satisfy $k + d = n + 1$ is called a *maximum distance separable code* or MDS code for short.

In this thesis we will discuss briefly the dimension of our codes, and we will focus on the minimum distance. For the reasons explained above, when we talk about bounds for the minimum distance we always mean *lower bounds*.

2.2 Evaluation codes

We introduce in this section the construction of *evaluation codes* also known as generalised Goppa codes. Indeed, evaluation codes were introduced by the Russian mathematician V. D. Goppa in the eighties ([16]) over smooth absolutely irreducible curves. Nevertheless his construction holds for smooth varieties of any dimension and thus we present here the general construction. To this end we consider an absolutely irreducible smooth projective algebraic variety X defined over $\mathbb{F}_q$ and a set $S = \{P_1, \ldots, P_n\}$ of rational points on X. Given a rational divisor G on X avoiding S, i.e. $S \cap \mathrm{Supp}(G) = \emptyset$, we consider the Riemann-Roch space associated to G (introduced in Subsection 1.2.2) defined by

$$L(G) = \{f \in \mathbb{F}_q(X) \setminus \{0\} \mid (f) + G \geq 0\} \cup \{0\}.$$

We recall that $L(G)$ is a $\mathbb{F}_q$-vector space. The algebraic geometry code $\mathcal{C}(X, G, S)$ can be presented from a functional point of view as the image of the following linear evaluation map ev

$$\begin{aligned} \mathrm{ev} : \quad L(G) &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f(P_1), \ldots, f(P_n)) \end{aligned} \tag{2.2}$$

which is clearly well defined when considering $S \subset X(\mathbb{F}_q)$ a subset of rational points on X such that $S \cap \mathrm{Supp}(G) = \emptyset$.

We remark that from the very definition, the length of the code $\mathcal{C}(X, G, S)$ is $n = \#S$, thus we will not discuss it further.

Remark 2.2.1. The previous construction naturally extends to the case where $S = X(\mathbb{F}_q)$ is an enumeration of the whole set of the rational points on X, as noticed by Manin and Vlăduţ in ([54, §3.1]). Indeed, one can rather consider the image of the following map:

$$\begin{aligned} \mathrm{ev} : H^0(X, \mathcal{L}) &\longrightarrow \bigoplus_{i=1}^{n} \mathcal{L}_{P_i} = \mathbb{F}_q^n \\ s &\longmapsto (s_{P_1}, \ldots, s_{P_n}), \end{aligned}$$

where we denote by $\mathcal{L}$ the line bundle associated to $L(G)$, by $\mathcal{L}_{P_i}$ the stalks at the P_i's, and by s_{P_i} the images of a global section $s \in H^0(X, \mathcal{L})$ in the stalks. Different choices of isomorphisms between the fibres $\mathcal{L}_{P_i}$ and $\mathbb{F}_q$ give rise to different maps but lead to equivalent codes. See also [26] or [1] for another constructive point of view.

2.2.1 Goppa codes

Evaluation codes from absolutely irreducible smooth curves are historically called Goppa codes. Let C be an absolutely irreducible projective smooth curve of genus g. Since varieties of codimension one on curves are points, divisors on C are formal sums of points with integer multiplicities. We recall that Riemann's inequality for curves states that if D is a divisor on C, then $\ell(D) \geq \deg(D) - g + 1$, where for a divisor $D = \sum_i n_i P_i$ the degree $\deg(D)$ is defined to be $\sum_i n_i \deg(P_i)$. We prove here the well-known bounds for the parameters of Goppa codes.

Theorem 2.2.2. *Let C be an absolutely irreducible projective smooth curve of genus g, let S be a set of n rational points on C and let G be a divisor on C with $\mathrm{Supp}(G) \cap S = \emptyset$. Suppose $\deg(G) < n$. Then the parameters of the $[n, k, d]$-code $\mathcal{C}(C, S, G)$ satisfy:*

1. $d \geqslant n - \deg(G)$;
2. $k \geqslant \deg(G) - g + 1$.

Proof. Let $f \in L(G) \setminus \{0\}$ with $\omega(\mathrm{ev}(f)) = d$, where ev is the evaluation map defined in (2.2). Thus there are $n - d$ points of S on which f has a zero. Let $P_1, \ldots, P_{n-d}$ be these points, and consider $G' = G - (P_1, \ldots, P_{n-d})$. Obviously $G' + (f)$ is still effective since $P_1, \ldots, P_{n-d}$ appear with positive multiplicities in $(f)_0$. Thus $f \in L(G')$ and we have $0 \leqslant \deg(G') \leqslant \deg(G) - n + d$ from which the first statement follows. Let us prove (2). Since $\deg(G) < n$, by the first item the minimum distance of the code is positive. Therefore the map ev is injective and gives an isomorphism between $L(G)$ and $\mathcal{C}(C, S, G)$. We conclude using Riemann's inequality to bound $\ell(G)$. □

Remark 2.2.3. In order to give a lower bound on the dimension of Goppa codes over curves we only need Riemann's inequality. Historically this inequality was proven over $\mathbb{C}$ by Riemann in 1857 and then completed eight years after by his student Roch in what is well-known as the Riemann-Roch theorem for curves: $\ell(D) - \ell(K - D) = \deg(D) - g + 1$, where K is the canonical divisor of the curve. It took nearly seventy years more and a completely different approach to extend this result to fields of arbitrary characteristics (see [44]).

Note that under the hypothesis that $\deg(D) \geqslant 2g - 1$ we have $\ell(K - D) = 0$. Thus one can get the exact dimension of Goppa codes using Riemann-Roch theorem, under the condition on the degree of the divisor chosen to construct the code.

2.3 Codes from algebraic surfaces

We have seen that the construction of codes introduced by Goppa over curves works for algebraic varieties of any dimension. Nevertheless, the more the dimension of the variety is high, the more the study of the parameters of the associated code becomes difficult. For instance, whereas the key tool for the study of the minimum distance in the one-dimensional case is the mere fact that a function has as many zeroes as poles, in the two-dimensional case most of the proofs rest on intersection theory.

We begin in this section the study of the generalisation of Goppa algebraic geometry codes from curves to surfaces. From now on, we consider an absolutely irreducible smooth projective algebraic surface X defined over $\mathbb{F}_q$ and a set $S = \{P_1, \ldots, P_n\}$ of rational points on X. Given a rational effective divisor G on X avoiding S, we consider the code $\mathcal{C}(X, G, S)$.

2.3.1 Dimension

As soon as the morphism ev is injective - see inequality (2.7) for a sufficient condition - the dimension of the code equals $\ell(G) = \dim_{\mathbb{F}_q} L(G)$, which can be easily bounded from below using standard algebraic geometry tools as follows. By Riemann-Roch theorem (Theorem 1.3.4), we have

$$\ell(G) - s(G) + \ell(K_X - G) = \frac{1}{2}G.(G - K_X) + 1 + p_a(X).$$

Since the superabundance $s(G)$ of G in X is itself the dimension of some vector space, it is non-negative. Furthermore, under the assumption that for some ample divisor H we have

$$K_X.H < G.H, \tag{2.3}$$

we get from [22, V, Lemma 1.7] that $\ell(K_X - G) = 0$. Thus, if the evaluation map ev is injective and under assumption (2.3), we get the lower bound

$$\dim \mathcal{C}(X, G, S) = \ell(G) \geq \frac{1}{2}G.(G - K_X) + 1 + p_a(X) \tag{2.4}$$

for the dimension of the code $\mathcal{C}(X, G, S)$.

2.3.2 Toward the minimum distance

The main difficulty in the study of the code $\mathcal{C}(X, G, S)$ lies in the estimation of its minimum distance $d(X, G, S)$. For any non-zero $f \in L(G)$, we introduce the number $N(f)$ of rational points on the divisor of zeroes of f. The Hamming weight $w(\mathrm{ev}(f))$ of the codeword $\mathrm{ev}(f)$ satisfies

$$w(\mathrm{ev}(f)) \geq \#S - N(f), \tag{2.5}$$

from which it follows that

$$d(X, G, S) \geq \#S - \max_{f \in L(G) \setminus \{0\}} N(f). \tag{2.6}$$

We also deduce from inequality (2.5) that

$$\text{ev is injective if } \max_{f \in L(G)\setminus\{0\}} N(f) < \#S. \tag{2.7}$$

We associate to any non-zero function $f \in L(G)$ the rational effective divisor

$$D_f := G + (f) = \sum_{i=1}^{k} n_i D_i \geq 0, \tag{2.8}$$

where (f) is the principal divisor associated to f, the n_i are positive integers and each D_i is a reduced $\mathbb{F}_q$-irreducible curve.

Note that in this setting, the integer k and the curves D_i's depend on $f \in L(G)$. Several lower bounds for the minimum distance $d(X, G, S)$ in this thesis will follow from the key lemma below.

Lemma 2.3.1 (Aubry, B., Herbaut, Perret, 2019, [6])**.** *Let X be a smooth absolutely irreducible projective surface defined over $\mathbb{F}_q$, S be a set of rational points on X and G be a rational effective divisor on X avoiding S. Set $m = \lfloor 2\sqrt{q} \rfloor$ and keep the notations introduced in (2.8). If there exist non-negative real numbers a, b_1, b_2, c, such that for any non-zero $f \in L(G)$ the three following assumptions are satisfied*

1. *$k \leqslant a$*
2. *$\sum_{i=1}^{k} \pi_{D_i} \leqslant b_1 + kb_2$ and*
3. *for any $1 \leqslant i \leqslant k$ we have $\#D_i(\mathbb{F}_q) \leqslant c + m\pi_{D_i}$,*

then the minimum distance $d(X, G, S)$ of $\mathcal{C}(X, G, S)$ satisfies

$$d(X, G, S) \geq \#S - a(c + mb_2) - mb_1.$$

Proof. Let us write the principal divisor $(f) = (f)_0 - (f)_\infty$ as the difference of its effective divisor of zeroes minus its effective divisor of poles. Since G is effective and f belongs to $L(G)$, we have $(f)_\infty \leqslant G$. Hence, formula (2.8) reads $G + (f)_0 - (f)_\infty = \sum_{i=1}^{k} n_i D_i$, that is

$$(f)_0 = \sum_{i=1}^{k} n_i D_i + (f)_\infty - G \leqslant \sum_{i=1}^{k} n_i D_i.$$

This means that any $\mathbb{F}_q$-rational point of $(f)_0$ lies in some D_i, so

$$N(f) \leqslant \sum_{i=1}^{k} \#D_i(\mathbb{F}_q). \tag{2.9}$$

Then it follows successively from the assumptions of the lemma that

$$N(f) \leqslant \sum_{i=1}^{k} (c + m\pi_{D_i}) \leqslant kc + m(b_1 + kb_2) \leqslant mb_1 + a(c + mb_2).$$

Finally Lemma 2.3.1 follows from inequality (2.6). □

2.3.3 Why ample divisors

In the following chapters we are going to study the minimum distance of the code $\mathcal{C}(X, G, S)$ from a surface X and a divisor G on X whose support has empty intersection with a set S of rational points on X. Even though the construction of evaluation codes works for any divisor, we will consider only ample divisors, more precisely we will take $G = rH$ for H an ample divisor on X and r a positive integer. One can ask if sometimes another choice of G could not be more suitable for obtaining good codes, but as a matter of fact codes constructed using non-ample divisors are not interesting. Indeed, if G is non-ample, then the code that we get is obtained by repeating the coordinates of another code constructed from an ample divisor. To be more explicit, let G be a non-ample divisor on a surface X and consider the code $\mathcal{C}(X, G, S)$. For $\ell = \dim L(G)$, let $\varphi_G : X \to \mathbb{P}^{\ell-1}$ be the rational map defined in Subsection 1.2.2. Let $X' = \varphi_*(X)$, $G' = \varphi_*(G)$ and $S' = \varphi_*(S)$, where φ_* denotes the push-forward of φ. Note that G' is a (very) ample divisor on X'. We claim that the code $\mathcal{C}(X, G, S)$ is obtained by repeating the coordinates of every codeword of the code $\mathcal{C}(X', G', S')$. This implies that the two codes have same dimension, while the length and the minimum distance of $\mathcal{C}(X, G, S)$ are increased proportionally. Therefore the code $\mathcal{C}(X', G', S')$ has better parameters than $\mathcal{C}(X, G, S)$, with respect to the Singleton Bound (2.1). One can prove the general case when the image of the surface X is also a surface. Indeed, if $\varphi_*(X)$ is a surface then one can deduce from [22, III, Exercise 4.1] that $L(G)$ and $L(G')$ are isomorphic via the map sending $f \in L(G)$ to $f \circ \varphi$. Thus the two codes are of same dimension and only of different length. Let us consider the following example when X' is not a surface.

Example 2.3.2. Let X be the quadric $xy = zt$ in $\mathbb{P}^3$ defined over $\mathbb{F}_5$. We have $\mathrm{Pic}(X) = \mathbb{Z} \oplus \mathbb{Z}$. Let G be the class of the line $x = z = 0$. Note that G is effective and non-ample. We have $L(G) =< 1, y/z >$ and thus $\ell_G = 2$. Therefore φ_G defines a map from X to $\mathbb{P}^1$ and we have $\varphi_*(X) = \mathbb{P}^1$. We consider S to be the set of rational points on X avoiding G. We have $\#S(\mathbb{F}_5) = 30$. Doing some calculation with Magma (one can also easily do it by hand) we get that $\mathcal{C}(X, G, S)$ is a $[30, 2, 25]$-code which is indeed obtained by repetition of the MDS $[6, 2, 5]$-code associated to the image of G on $X' = \mathbb{P}^1$.

2.4 Curves over surfaces

In order to fulfil assumption (2) in Lemma 2.3.1 we need to bound from above the number of rational points on algebraic curves. The most known upper bound in this context is the Serre-Weil bound ([46]) which states that the number of rational points on a smooth absolutely irreducible curve C of geometric genus g is bounded by

$$\#C(\mathbb{F}_q) \leqslant q + 1 + mg, \tag{2.10}$$

where $m = \lfloor 2\sqrt{q} \rfloor$. However, in our context we deal with curves that are $\mathbb{F}_q$-irreducible but possible not absolutely irreducible, and furthermore we allow the curves that appear in the decomposition of a divisor to be singular. Thus, we need to use other bounds than the Serre-Weil's one. A crucial point in the proofs of the bounds we are going to give in this section, is that the curves we deal with

are embedded in a smooth surface. Indeed, this assumption is necessary to prove Theorem 2.4.1 and for the results on abelian surfaces (Theorem 2.4.3 and Corollary 2.4.4). We do not need this assumption in Proposition 2.4.2 which concerns the relation between the number of rational points on curves with a surjective morphism between them.

2.4.1 Rational points on curves over smooth surfaces

The following theorem is used in Chapter 3 to fulfil assumption (2) in Lemma 2.3.1 when proving bounds on the minimum distance of codes from some families of surfaces. Point (2) of Theorem 2.4.1 appears in the proof of Theorem 3.3 of Little and Schenck in [30] within a more restrictive context, whereas point (1) follows from [2]. We state a general theorem and give here the full proof for the sake of completeness, following [30].

Theorem 2.4.1 (Aubry and Perret, 1993, [2], Little and Schenck, 2018, [30])**.** *Let D be an $\mathbb{F}_q$-irreducible curve of arithmetic genus π_D lying on a smooth projective algebraic surface X. Set $m = \lfloor 2\sqrt{q} \rfloor$. Then,*

1. *we have $\#D(\mathbb{F}_q) \leqslant q + 1 + m\pi_D$.*
2. *If moreover D is* not *absolutely irreducible, we have*

$$\#D(\mathbb{F}_q) \leqslant \pi_D + 1.$$

Proof. We first prove the second item, following the proof of [30, Th. 3.3]. Since D is $\mathbb{F}_q$-irreducible, the Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ acts transitively on the set of its $\bar{r} \geq 1$ absolutely irreducible components $D_1, \ldots, D_{\bar{r}}$. Since a $\mathbb{F}_q$-rational point on D is stable under the action of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, it lies in the intersection $\cap_{1 \leqslant i \leqslant \bar{r}} D_i$. Under the assumption that D is not absolutely irreducible, that is $\bar{r} \geq 2$, it follows that $\#D(\mathbb{F}_q) \leqslant \#(D_i \cap D_j)(\overline{\mathbb{F}}_q) \leqslant D_i.D_j$ for every couple (i, j) with $i \neq j$.

As a divisor, D can be written over $\overline{\mathbb{F}}_q$ as $D = \sum_{i=1}^{\bar{r}} a_i D_i$. By transitivity of the Galois action, we have $a_1 = \cdots = a_{\bar{r}} = a$. Since D can be assumed to be reduced, we have $a = 1$, so that finally $D = \sum_{i=1}^{\bar{r}} D_i$. Using the adjonction formula (1.2) for D and each D_i, and taking into account that $\pi_{D_i} \geq 0$ for any i, we get

$$\begin{aligned} 2\pi_D - 2 &= (K_X + D).D \\ &= \sum_{i=1}^{\bar{r}} (K_X + D_i).D_i + \sum_{i \neq j} D_i.D_j \\ &= \sum_{i=1}^{\bar{r}} (2\pi_{D_i} - 2) + \sum_{i \neq j} D_i.D_j \\ &\geq -2\bar{r} + \sum_{i \neq j} D_i.D_j. \end{aligned}$$

Since there are $\bar{r}(\bar{r} - 1)$ pairs (i, j) with $i \neq j$, we deduce that for at least one such pair (i_0, j_0), we have

$$D_{i_0}.D_{j_0} \leqslant \frac{2(\pi_D - 1 + \bar{r})}{\bar{r}(\bar{r} - 1)}.$$

It is then easily checked that the right hand of the previous inequality is a decreasing function of $\bar{r} \geq 2$, so that we obtain

$$\#D(\mathbb{F}_q) \leqslant D_{i_0}.D_{j_0} \leqslant \frac{2(\pi_D - 1 + 2)}{2(2-1)} = \pi_D + 1$$

and the second item is proved.

The first item follows from Aubry-Perret's bound in [2] in case D is absolutely irreducible, that is in case $\bar{r} = 1$, and from the second item in case D is not absolutely irreducible since $\pi_D + 1 \leqslant q + 1 + m\pi_D$. □

2.4.2 Regular maps between curves and relation with rational points

The following bound will be useful in Subsection 3.2.3 for the study of codes from fibered surfaces. It can be deduced using two results proved by Aubry and Perret in [4].

Proposition 2.4.2 (Aubry and Perret, 2004, [4]). *Let C be a smooth projective absolutely irreducible curve of genus g_C over $\mathbb{F}_q$ and D be an $\mathbb{F}_q$-irreducible curve having $\bar{r}$ absolutely irreducible components $\overline{D}_1, \ldots, \overline{D}_{\bar{r}}$. Suppose there exists a regular map $D \to C$ in which no $\overline{\mathbb{F}}_q$-irreducible component does map to a point. Set $m = \lfloor 2\sqrt{q} \rfloor$. Then*

$$|\#D(\mathbb{F}_q) - \#C(\mathbb{F}_q)| \leqslant (\bar{r} - 1)q + m(\pi_D - g_C).$$

Proof. Since C is smooth and no geometric component of D does map to a point, the map $D \to C$ is flat. Hence by [4, Th.14] we have

$$|\#D(\mathbb{F}_q) - \#C(\mathbb{F}_q)| \leqslant (\bar{r} - 1)(q-1) + m\left(\sum_{i=1}^{\bar{r}} g_{\overline{D}_i} - g_C\right) + \Delta_D$$

where $\Delta_D = \#\tilde{D}(\overline{\mathbb{F}}_q) - \#D(\overline{\mathbb{F}}_q)$ with $\tilde{D}$ the normalization of D. The result follows from [4, Lemma 2] where it is proved that $m\sum_{i=1}^{\bar{r}} g_{\overline{D}_i} + \Delta_D - \bar{r} + 1 \leqslant m\pi_D$. □

2.4.3 Rational points on curves over abelian surfaces

We set A to be an abelian surface defined over the finite field $\mathbb{F}_q$ whose trace is denoted by $\mathrm{Tr}(A)$. The following theorem is proved in [18, Th. 4].

Theorem 2.4.3 (Haloui , 2017, [18]). *Set $m = \lfloor 2\sqrt{q} \rfloor$. The number of rational points on a projective $\mathbb{F}_q$-irreducible curve D defined over $\mathbb{F}_q$ of arithmetic genus π lying on an abelian surface A of trace $\mathrm{Tr}(A) \geq -q$ is bounded by*

$$\#D(\mathbb{F}_q) \leqslant q + 1 - \mathrm{Tr}(A) + |\pi - 2|m.$$

From the previous theorem we can easily deduce the following corollary. The two lower bounds of Corollary 2.4.4 are used in Chapter 4 to prove bounds on the minimum distance of codes from abelian surfaces.

Corollary 2.4.4. *Let D be a $\mathbb{F}_q$-irreducible curve on A of arithmetic genus π. Set $m = \lfloor 2\sqrt{q} \rfloor$. Then we have:*

1. $\#D(\mathbb{F}_q) \leqslant q + 1 - \mathrm{Tr}(A) + m\pi$.
2. *If moreover A is simple, then we have*

$$\#D(\mathbb{F}_q) \leqslant q + 1 - \mathrm{Tr}(A) + m(\pi - 2).$$

Proof. With no hypotheses on the abelian surface nor on the arithmetic genus π of D, we can only say that $\pi = 0$ cannot occur, and since $\pi \geqslant |\pi - 2|$ for $\pi \geqslant 1$, by the previous theorem we get bound (1). By Proposition 5 of [18], a simple abelian surface contains no irreducible curves of arithmetic genus 0 nor 1 defined over $\mathbb{F}_q$. Thus if A is simple, then also $\pi = 1$ cannot occur, so from Theorem 2.4.3 we obtain bound (2). □

We end this section with a well-known bound (which for instance appears in the proof of Theorem 4 of [18]) on the number of rational points on irreducible curves, not absolutely irreducible, embedded in an abelian surface. We shall use this bound in Chapter 4.

We have seen in Theorem 2.4.1 that the number of rational points on a $\mathbb{F}_q$-irreducible curve D that is not absolutely irreducible and which is embedded in a smooth surface, is bounded by $\#D(\mathbb{F}_q) \leqslant \pi_D + 1$, where π_D is the arithmetic genus of the curve. When the smooth surface is an abelian surface, the previous bound can be sharpened as follows.

Proposition 2.4.5. *Let D be a $\mathbb{F}_q$-irreducible curve of arithmetic genus π_D lying on an abelian surface. If D is* not *absolutely irreducible, then we have*

$$\#D(\mathbb{F}_q) \leqslant \pi_D - 1.$$

Proof. We have already seen in the proof of Theorem 2.4.1 that if $\{D_1, \ldots, D_n\}$ are the absolutely irreducible components of D, then $\#D(\mathbb{F}_q) \leqslant \#(D_i \cap D_j)(\overline{\mathbb{F}}_q) \leqslant D_i.D_j$ for every couple (i, j) with $i \neq j$. In the case of abelian surfaces, since $K_A = 0$ adjunction formula gives $2\pi_D - 2 = D^2$. Hence we get

$$\begin{aligned}\#D(\mathbb{F}_q) &\leqslant D_1.D_2 = \frac{1}{2}(D_1.D_2 + D_2.D_1) \\ &\leqslant \frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n} D_i.D_j = \frac{1}{2}D^2 \\ &= \pi_D - 1.\end{aligned}$$

□

Chapter 3

Bounds on the minimum distance of algebraic geometry codes defined over some families of surfaces

The aim of this chapter is to provide a study of the minimum distance $d(X, rH, S)$ of the algebraic geometry code $\mathcal{C}(X, rH, S)$ constructed from an algebraic surface X, a set S of rational points on X, a rational effective ample divisor H on X avoiding S and an integer $r > 0$. The results we present in this chapter are original and appear in a paper ([6]) accepted for publication in Contemporary Mathematics of the AMS.

The chapter is organised as follows. We prove in Section 3.1 lower bounds for the minimum distance of codes from surfaces whose canonical divisor is either nef or anti-strictly nef (Theorem 3.1.2) and from surfaces which do not contain irreducible curves of low genus (Theorem 3.1.4). In Section 3.2, we prove four improvements for these lower bounds adding some extra geometric assumptions on the surfaces. We consider surfaces whose arithmetic Picard number is one (Theorem 3.2.3), surfaces without irreducible curves defined over $\mathbb{F}_q$ with small self-intersection (Theorem 3.2.6) and fibered surfaces (Theorem 3.2.8 and Theorem 3.2.9). Finally, in Section 3.3, we specify our bounds to the case of surfaces of degree $d \geqslant 3$ embedded in $\mathbb{P}^3$.

3.1 The minimum distance of codes from some families of algebraic surfaces

We prove most of the bounds in this section using Lemma 2.3.1. We are unfortunately unable to fulfil simultaneously assumptions (1) and (2) of Lemma 2.3.1 for general surfaces. So we focus on two families of algebraic surfaces where we do succeed. To begin with, let us fix some common notations.

We consider a rational effective ample divisor H on the surface X avoiding a set S of rational points on X and for a positive integer r we consider $G = rH$. We study, in accordance to Section 2.3, the evaluation code $\mathcal{C}(X, rH, S)$ and we denote by $d(X, rH, S)$ its minimum distance.

3.1.1 Surfaces whose canonical divisor is either nef or anti-strictly nef

We study in this subsection codes defined over surfaces such that either the canonical divisor K_X is nef, or its opposite $-K_X$ is strictly nef. This family is quite large. It contains, for instance:

- surfaces whose anti-canonical divisor is ample (del Pezzo surfaces);
- minimal surfaces of Kodaira dimension 0, for which the canonical divisor is numerically zero, hence nef. These are abelian surfaces, $K3$ surfaces, Enriques surfaces and hyperelliptic or quasi-hyperelliptic surfaces (see [11]);
- minimal surfaces of Kodaira dimension 2. These are the so called minimal surfaces of general type. For instance, surfaces in $\mathbb{P}^3$ of degree $d \geqslant 4$, without curves C with $C^2 = -1$, are minimal of general type;
- surfaces whose arithmetic Picard number is one;
- surfaces of degree 3 embedded in $\mathbb{P}^3$.

The main theorem of this subsection (Theorem 3.1.2) rests mainly on the next lemma, designed to fulfil assumptions (1) and (2) of Lemma 2.3.1.

Lemma 3.1.1. *Let $D = \sum_{i=1}^{k} n_i D_i$ be the decomposition as a sum of $\mathbb{F}_q$-irreducible and reduced curves of an effective divisor D linearly equivalent to rH. Then we have:*

1. $k \leqslant rH^2$;
2. *(i) if K_X is nef, then $\sum_{i=1}^{k} \pi_{D_i} \leqslant \pi_{rH} - 1 + k$;*
   (ii) if $-K_X$ is strictly nef, then $\sum_{i=1}^{k} \pi_{D_i} \leqslant \pi_{rH} - 1 - \frac{1}{2} rH.K_X + \frac{1}{2}k$.

Proof. Using that D is numerically equivalent to rH, that $n_i > 0$ and $D_i.H > 0$ for every $i = 1, \ldots, k$ since H is ample, we prove item (1):

$$rH.H = D.H = \sum_{i=1}^{k} n_i D_i.H \geqslant \sum_{i=1}^{k} D_i.H \geqslant k.$$

Applying inequality (1.3) to H and D_i for every i, we get $D_i^2 H^2 \leqslant (D_i.H)^2$. We thus have, together with adjunction formula (1.2) and inequality $H^2 > 0$,

$$\pi_{D_i} - 1 \leqslant \frac{(D_i.H)^2}{2H^2} + \frac{D_i.K_X}{2}. \tag{3.1}$$

To prove item (2i) we sum from $i = 1$ to k and obtain

$$\begin{aligned}
\sum_{i=1}^{k} \pi_{D_i} - k &\leqslant \frac{1}{2H^2} \sum_{i=1}^{k} (D_i.H)^2 + \frac{1}{2} \sum_{i=1}^{k} D_i.K_X \\
&\leqslant \frac{1}{2H^2} \left(\sum_{i=1}^{k} n_i D_i.H \right)^2 + \frac{1}{2} \sum_{i=1}^{k} n_i D_i.K_X \\
&\leqslant \frac{(rH.H)^2}{2H^2} + \frac{rH.K_X}{2} \\
&= \pi_{rH} - 1,
\end{aligned} \tag{3.2}$$

where we use the positivity of the coefficients n_i, the numeric equivalence between D and $\sum_{i=1}^{k} n_i D_i$, the fact that H is ample and the hypothesis taken on K_X.

Under the hypothesis of point (2ii) we have $D_i.K_X \leqslant -1$. Replacing in the first line of (3.2) gives $\sum_{i=1}^{k} \pi_{D_i} - k \leqslant \frac{1}{2H^2} \sum_{i=1}^{k} (D_i.H)^2 - \frac{k}{2}$. We conclude in the same way. □

Theorem 3.1.2. *Let H be a rational effective ample divisor on a surface X avoiding a set S of rational points on X and let r be a positive integer. We set*

$$d^*(X, rH, S) := \#S - rH^2(q + 1 + m) - m(\pi_{rH} - 1). \tag{3.3}$$

1. *If K_X is nef, then*
$$d(X, rH, S) \geqslant d^*(X, rH, S).$$

2. *If $-K_X$ is strictly nef, then*
$$d(X, rH, S) \geqslant d^*(X, rH, S) + mr(\pi_H - 1).$$

Proof. The theorem follows from Lemma 2.3.1 for which assumptions (1) and (2) hold from Lemma 3.1.1 and assumption (2) holds from Theorem 2.4.1. □

3.1.2 Surfaces without irreducible curves of small genus

We consider in this subsection surfaces X with the property that there exists an integer $\ell \geqslant 1$ such that any $\mathbb{F}_q$-irreducible curve D lying on X and defined over $\mathbb{F}_q$ has arithmetic genus $\pi_D \geqslant \ell + 1$. It turns out that under this hypothesis, we can fulfil assumptions (1) and (2) of Lemma 2.3.1 without any hypothesis on K_X, contrary to the setting of Section 3.1.1.

Examples of surfaces with this property do exist. For instance:

- simple abelian surfaces satisfy this property for $\ell = 1$ (the case of abelian surfaces is discussed further in Chapter 4);
- fibered surfaces on a smooth base curve B of genus $g_B \geqslant 1$ and generic fiber of arithmetic genus $\pi_0 \geqslant 1$, and whose singular fibers are $\mathbb{F}_q$-irreducible, do satisfy this property for $\ell = \min(g_B, \pi_0) - 1$;
- smooth surfaces in $\mathbb{P}^3$ of degree d whose arithmetic Picard group is generated by the class of an hyperplane section do satisfy this property for $\ell = \frac{(d-1)(d-2)}{2} - 1$ (see Lemma 3.3.2).

The main theorem of this subsection (Theorem 3.1.4) rests mainly on the next lemma, conceived to fulfil assumptions (1) and (2) of Lemma 2.3.1.

Lemma 3.1.3. *Let X be a surface without $\mathbb{F}_q$-irreducible curves of arithmetic genus less than or equal to a positive integer ℓ. Consider a rational effective ample divisor H on X and a positive integer r. Let $D = \sum_{i=1}^{k} n_i D_i$ be the decomposition as a sum of $\mathbb{F}_q$-irreducible and reduced curves of an effective divisor D linearly equivalent to rH. Then we have*

1. $k \leqslant \frac{\pi_{rH} - 1}{\ell}$;
2. $\sum_{i=1}^{k} \pi_{D_i} \leqslant \pi_{rH} - 1 + k$.

In case X falls in both families of Subsection 3.1.1 and of this Subsection 3.1.2, the present new bound of the first item for k is better than the one of Lemma 3.1.1 if and only if $\pi_{rH}-1<\ell r H^2$, that is if and only if $\ell>\frac{H.K_X}{2H^2}+\frac{r}{2}$. In the general setting, this inequality sometimes holds true, sometimes not. As a matter of example, suppose K_X is ample and let us consider $H=K_X$. In this setting, the inequality holds if and only if $r<2\ell-1$.

Proof. By assumption, we have $0\leqslant\ell\leqslant\pi_{D_i}-1$ and $n_i\geqslant 1$ for any $1\leqslant i\leqslant k$, hence using adjunction formula (1.2), we have

$$2\ell k\leqslant 2\sum_{i=1}^{k}(\pi_{D_i}-1)\leqslant 2\sum_{i=1}^{k}n_i(\pi_{D_i}-1)=\sum_{i=1}^{k}n_iD_i^2+\sum_{i=1}^{k}n_iD_i.K_X.$$

Moreover using (1.3) and (2.8), we get

$$2\ell k\leqslant 2\sum_{i=1}^{k}(\pi_{D_i}-1)\leqslant\sum_{i=1}^{k}n_i\frac{(D_i.H)^2}{H^2}+\left(\sum_{i=1}^{k}n_iD_i\right).K_X\leqslant\sum_{i=1}^{k}n_i^2\frac{(D_i.H)^2}{H^2}+rH.K_X.$$

Since H is ample, we obtain

$$2\ell k\leqslant 2\sum_{i=1}^{k}(\pi_{D_i}-1)\leqslant\sum_{i,j=1}^{k}n_in_j\frac{(D_i.H)(D_j.H)}{H^2}+rH.K_X=\frac{(\sum_{i,=1}^{k}n_iD_i.H)^2}{H^2}+rH.K_X.$$

By (2.8), we conclude that

$$2\ell k\leqslant 2\sum_{i=1}^{k}(\pi_{D_i}-1)\leqslant\frac{(rH.H)^2}{H^2}+rH.K_X=2(\pi_{rH}-1),$$

and both items of Lemma 3.1.3 follow. □

Theorem 3.1.4. *Let X be a surface without $\mathbb{F}_q$-irreducible curves of arithmetic genus less than or equal to a positive integer ℓ. Consider a rational effective ample divisor H on X avoiding a finite set S of rational points on X and let r be a positive integer. Then we have*

$$d(X,rH,S)\geqslant d^*(X,rH,S)+\left(rH^2-\frac{\pi_{rH}-1}{\ell}\right)(q+1+m).$$

Proof. The theorem follows from Lemma 2.3.1, for which items (1) and (2) hold from Lemma 3.1.3 and item (2) holds from Theorem 2.4.1. □

3.2 Four improvements

In this section we manage to obtain better parameters for conditions (1), (2) or (2) of Lemma 2.3.1 in four cases: for surfaces of arithmetic Picard number one, for surfaces which do not contain $\mathbb{F}_q$-irreducible curves of small self-intersection and whose canonical divisor is either nef or anti-nef, for fibered surfaces with nef canonical divisor, and for fibered surfaces whose singular fibers are $\mathbb{F}_q$-irreducible curves.

3.2.1 Surfaces with Picard number one

The case of surfaces X whose arithmetic Picard number equals one has already attracted some interest (see [61], [55], [30] and [10]). We prove in this subsection Lemma 3.2.1 and Theorem 3.2.3 which improve, under this rank one assumption, the bounds of Lemma 3.1.1 and Theorem 3.1.2. These new bounds depend on the sign of $3H^2 + H.K_X$, where H is the ample generator of $\mathrm{NS}(X)$.

Lemma 3.2.1. *Let X be a smooth projective surface of arithmetic Picard number one. Let H be the ample generator of $\mathrm{NS}(X)$ and let r be a positive integer. For any non-zero function $f \in L(rH)$ consider the decomposition $D_f = \sum_{i=1}^{k} n_i D_i$ into $\mathbb{F}_q$-irreducible and reduced curves D_i with positive integer coefficients n_i as in (2.8). Then the sum of the arithmetic genera of the curves D_i satisfies:*

1. $\sum_{i=1}^{k} \pi_{D_i} \leqslant (k-1)\pi_H + \pi_{(r-k+1)H}$ *if* $3H^2 + H.K_X \geqslant 0$;
2. $\sum_{i=1}^{k} \pi_{D_i} \leqslant H^2(r-k)^2/2 + H^2(r-2k) + k$ *if* $3H^2 + H.K_X < 0$.

Remark 3.2.2. Note that the condition $3H^2 + H.K_X \geqslant 0$ is satisfied as soon as $H.K_X \geqslant 0$. It is also satisfied in the special case where $K_X = -H$ which corresponds to del Pezzo surfaces.

Proof. In order to prove the first item, we consider a non-zero function $f \in L(rH)$ and we keep the notation already introduced in (2.8), namely $D_f = \sum_{i=1}^{k} n_i D_i$. As $\mathrm{NS}(X) = \mathbb{Z}H$, for all i we have $D_i = a_i H$ and we know by Lemma 2.2 in [61] that $k \leqslant r$. Intersecting with the ample divisor H enables to prove that for all i we have $a_i \geqslant 1$ and that $\sum_{i=1}^{k} n_i a_i = r$. Thus to get an upper bound for $\sum_{i=1}^{k} \pi_{D_i} = \sum_{i=1}^{k} \pi_{a_i H}$, we are reduced to bounding $\left(\sum_{i=1}^{k} a_i^2\right) H^2/2 + \left(\sum_{i=1}^{k} a_i\right) H.K_X/2 + k$ under the constraint $\sum_{i=1}^{k} a_i n_i = r$. Our strategy is based on the two following arguments.

First, the condition $3H^2 + H.K_X \geqslant 0$ guarantees that $a \mapsto \pi_{aH}$ is an increasing sequence. Indeed, for integers $a' > a \geqslant 1$ we have $\pi_{a'H} \geqslant \pi_{aH}$ if and only if $(a+a')H^2 \geqslant -H.K_X$, which is true under the condition above because $a + a' \geqslant 3$. As a consequence, if we fix an index i between 1 and k and if we consider that the product $n_i a_i$ is constant, then the value of $\pi_{a_i H}$ is maximum when a_i is, that is when $a_i = n_i a_i$ and $n_i = 1$.

Secondly, assume that all the n_i equal 1 and that $\sum_{i=1}^{k} a_i = r$. We are now reduced to bounding $\sum_{i=1}^{k} a_i^2$. We can prove that the maximum is reached when all the a_i equal 1 except one which equals $r - k + 1$. Otherwise, suppose for example that $2 \leqslant a_1 \leqslant a_2$. Then $a_1^2 + a_2^2 < (a_1 - 1)^2 + (a_2 + 1)^2$ and $\sum_{i=1}^{k} a_i^2$ is not maximum, and the first item is thus proved.

For the second item, using the adjonction formula we get

$$\sum_{i=1}^{k} \pi_{D_i} - k \leqslant \frac{1}{2H^2} \sum_{i=1}^{k} (D_i.H)^2 + \frac{1}{2} \sum_{i=1}^{k} D_i.K_X.$$

Again as $\mathrm{NS}(X) = \mathbb{Z}H$, for all i we have $D_i = a_i H$. Thus we get

$$\sum_{i=1}^{k} \pi_{D_i} - k \leqslant \frac{1}{2H^2} \sum_{i=1}^{k} a_i^2 (H^2)^2 + \frac{1}{2} \sum_{i=1}^{k} a_i H.K_X.$$

Now using that $H.K_X \leqslant -3H^2$ by hypothesis, that $\sum_{i=1}^k a_i \geqslant k$ since every a_i is positive and that since $\sum_{i=1}^k a_i \leqslant r$ we can prove again that $\sum_{i=1}^k a_i^2 \leqslant (r-k+1)^2 + (k-1)$, we get

$$\sum_{i=1}^{k} \pi_{D_i} - k \leqslant \frac{H^2}{2}((r-k+1)^2 + (k-1)) - \frac{3H^2}{2}k.$$

Some easy calculation shows that this is equivalent to our second statement. □

Theorem 3.2.3. *Let X be a smooth projective surface of arithmetic Picard number one. Let H be the ample generator of $\mathrm{NS}(X)$ and S a finite set of rational points on X avoiding H. For any positive integer r, the minimum distance $d(X, rH, S)$ of the code $\mathcal{C}(X, rH, S)$ satisfies:*

1. *if $3H^2 + H.K_X \geqslant 0$, then*

$$d(X, rH, S) \geqslant \begin{cases} \#S - (q + 1 + m\pi_{rH}) & \text{if } r > \frac{2(q+1+m)}{mH^2}, \\ \#S - r(q + 1 + m\pi_H) & \text{otherwise.} \end{cases}$$

2. *If $3H^2 + H.K_X < 0$, then*

$$d(X, rH, S) \geqslant \begin{cases} \#S - (q + 1 + m) - m(r^2 - 3)\frac{H^2}{2} & \text{if } r > \frac{2(q+1+m)}{mH^2 - 3}, \\ \#S - r(q + 1 + m - mH^2) & \text{otherwise.} \end{cases}$$

Proof. For any non-zero $f \in L(rH)$, we get from inequality (2.9) and from point (1) of Theorem 2.4.1 the following inequality

$$N(f) \leqslant k(q+1) + m\sum_{i=1}^{k} \pi_{D_i}.$$

We apply item (1) of Lemma 3.2.1 to bound $\sum_{i=1}^k \pi_{D_i}$. We get in the first case $N(f) \leqslant \phi(k)$, where $\phi(k) := m\pi_{(r-k+1)H} + k(q+1+m\pi_H) - m\pi_H$. Note that $\pi_{(r-k+1)H}$ is quadratic in k and so $\phi(k)$ is a quadratic function with positive leading coefficient. In [55, Lemma 2.2], Voloch and Zarzar proved that if X has arithmetic Picard number one then $k \leqslant r$. Thus $\phi(k)$ attains its maximum for $k = 1$ or for $k = r$ and $N(f) \leqslant \max\{\phi(1), \phi(r)\}$. A simple calculus shows that $\phi(1) - \phi(r) > 0$ if and only if $r > 2(q + 1 + m)/mH^2$. Since we have $d(X, rH, S) \geqslant \#S - \max_{f \in L(rH)\setminus\{0\}} N(f)$, part (1) of the theorem is proved.

The treatment of part (2) is the same, except that we use item (2) of Lemma 3.2.1 to bound $\sum_{i=1}^k \pi_{D_i}$.

□

Remark 3.2.4. Little and Schenck have given bounds in [30, §3] for the minimum distance of codes defined over algebraic surfaces of Picard number one. In particular, they obtain (if we keep the notations of Theorem 3.2.3): $d(X, rH, S) \geqslant \#S - (q + 1 + m\pi_H)$ for $r = 1$ ([30, Th. 3.3]) and $d(X, rH, S) \geqslant \#S - r(q + 1 + m\pi_H)$ for $r > 1$ and q large ([30, Th. 3.5]). Comparing their bounds with Theorem 3.2.3, one can see that when $3H^2 + H.K_X \geqslant 0$ we get the same bound for $r = 1$ and also for $r > 1$ without any hypothesis on q. Moreover, when $3H^2 + H.K_X < 0$, our bounds improve the ones given by Little and Schenck, again without assuming q to be large enough when $r > 1$.

3.2.2 Surfaces without irreducible curves defined over $\mathbb{F}_q$ with small self-intersection and whose canonical divisor is either nef or anti-nef

We consider in this section surfaces X such that there exists some integer $\beta \geqslant 0$ for which any $\mathbb{F}_q$-irreducible curve D lying on X and defined over $\mathbb{F}_q$ has self-intersection $D^2 \geqslant \beta$. We prove in this case Lemma 3.2.5 below, from which we can tackle assumption (1) in Lemma 2.3.1 in case $\beta > 0$. Unfortunately, Lemma 3.2.5 enables to fulfil assumption (2) of Lemma 2.3.1 only in case the intersection of the canonical divisor with $\mathbb{F}_q$-irreducible curves has constant sign, that is for surfaces of Section 3.1.1. The lower bound for the minimum distance we get is better than the one given in Theorem 3.1.2.

Let us propose some examples of surfaces with this property:

- simple abelian surfaces satisfy this property for $\beta = 2$;
- surfaces whose arithmetic Picard number is one. Indeed, consider a curve D defined over $\mathbb{F}_q$ on X, and assume that $\mathrm{NS}(X) = \mathbb{Z}H$ with H ample. Then we have that $D = aH$ for some integer a. Since H is ample we get $1 \leqslant D.H = aH^2$, hence $a \geqslant 1$ and $D^2 = a^2H^2 \geqslant H^2$;
- surfaces whose canonical divisor is anti-nef and without irreducible curves of arithmetic genus less than or equal to $\ell > 0$. Indeed, the adjunction formula gives $D^2 = 2\pi_D - 2 - D.K_X \geqslant 2\pi_D - 2 \geqslant 2\ell$.

Lemma 3.2.5. *Let X be a surface on which any $\mathbb{F}_q$-irreducible curve has self-intersection at least $\beta \geqslant 0$. Assume that H is a rational effective ample divisor on X and let r be a positive integer. Let $D = \sum_{i=1}^{k} n_i D_i$ be the decomposition as a sum of $\mathbb{F}_q$-irreducible and reduced curves of an effective divisor D linearly equivalent to rH. Then we have:*

1. *if $\beta > 0$, then $k \leqslant r\sqrt{\frac{H^2}{\beta}}$;*
2. *$\sum_{i=1}^{k}(2\pi_{D_i} - 2 - D_i.K_X) \leqslant \varphi(k)$, with*

$$\varphi(k) := (k-1)\beta + \left(r\sqrt{H^2} - (k-1)\sqrt{\beta}\right)^2. \tag{3.4}$$

Proof. Since by hypothesis we have $\sqrt{\beta} \leqslant \sqrt{D_i^2}$, we deduce that $k\sqrt{\beta} \leqslant \sum_{i=1}^{k} n_i\sqrt{D_i^2}$. Applying inequality (1.3), we get $k\sqrt{\beta} \leqslant \sum_{i=1}^{k} n_i \frac{D_i.H}{\sqrt{H^2}} = \frac{rH.H}{\sqrt{H^2}} = r\sqrt{H^2}$, from which the first item follows.

Setting $x_i := \sqrt{2\pi_{D_i} - 2 - D_i.K_X}$, we have by adjunction formula $x_i = \sqrt{D_i^2} \geqslant \sqrt{\beta}$. Moreover, the previous inequalities ensure that $\sum_{i=1}^{k} x_i \leqslant \sum_{i=1}^{k} n_i\sqrt{D_i^2} \leqslant r\sqrt{H^2}$. Then, the maximum of $\sum_{i=1}^{k}(2\pi_{D_i} - 2 - D_i.K_X) = \sum_{i=1}^{k} x_i^2$ under the conditions $x_i \geqslant \sqrt{\beta}$ and $\sum_{i=1}^{k} x_i \leqslant r\sqrt{H^2}$, is reached when each but one x_i equals the minimum $\sqrt{\beta}$, and only one is equal to $r\sqrt{H^2} - (k-1)\sqrt{\beta}$. This concludes the proof. □

Theorem 3.2.6. *Let X be a surface on which any $\mathbb{F}_q$-irreducible curve has self-intersection at least $\beta > 0$. Consider a rational effective ample divisor H on X avoiding a set S of rational points on X and let r be a positive integer. Then*

$$d(X, rH, S) \geqslant \begin{cases} \#S - \max\left\{\psi(1), \psi\left(r\sqrt{\frac{H^2}{\beta}}\right)\right\} - \frac{m}{2}r\sqrt{\frac{H^2}{2\beta}} & \text{if } K_X \text{ is nef,} \\ \#S - \max\left\{\psi(1), \psi\left(r\sqrt{\frac{H^2}{\beta}}\right)\right\} & \text{if } -K_X \text{ is nef} \end{cases}$$

with

$$\psi(k) \coloneqq \frac{m}{2}\varphi(k) + k(q+1+m),$$

where $\varphi(k)$ is given by equation (3.4).

Proof. For any non-zero $f \in L(rH)$, we have by (2.9) and by point (1) of Theorem 2.4.1 that $N(f) \leqslant k(q+1) + m\sum_{i=1}^{k} \pi_{D_i}$. Lemma 3.2.5 implies that $N(f) \leqslant k(q+1) + \frac{m}{2}\big(2k + \varphi(k) + \sum_{i=1}^{k} D_i.K_X\big)$. In case K_X is nef, we have $\sum_{i=1}^{k} D_i.K_X \leqslant \sum_{i=1}^{k} n_i D_i.K_X = rH.K_X$, and in case $-K_X$ is nef, we get $\sum_{i=1}^{k} D_i.K_X \leqslant 0$, and the theorem follows. □

3.2.3 Fibered surfaces with nef canonical divisor

We consider in this subsection algebraic geometry codes from fibered surfaces whose canonical divisor is nef. We adopt the vocabulary of [48, III, §8] and we refer the reader to this text for more details on the basic notions we recall here.

A fibered surface is a surjective morphism $\pi : X \to B$ from a smooth projective surface X to a smooth absolutely irreducible curve B. We denote by π_0 the common arithmetic genus of the fibers and by g_B the genus of the base curve B. Elliptic surfaces are among the first non-trivial examples of fibered surfaces. For such surfaces we have $\pi_0 = 1$ and the canonical divisor is always nef (see [11]).

We recall that on a fibered surface every divisor can be uniquely written as a sum of *horizontal* curves (that is mapped onto B by π) and *fibral* curves (that is mapped onto a point by π).

Lemma 3.2.7. *Let $\pi : X \to B$ be a fibered surface. Let H be a rational effective ample divisor on X and let r be a positive integer. For any effective divisor D linearly equivalent to rH, consider its decomposition $D = \sum_{i=1}^{k} n_i D_i$ as a sum of reduced $\mathbb{F}_q$-irreducible curves as in (2.8). Denote by $\overline{r}_i$ the number of absolutely irreducible components of D_i. Then we have*

$$\sum_{i=1}^{k} \overline{r}_i \leqslant rH^2.$$

Proof. Write $D = \sum_{i=1}^{k} n_i D_i = \sum_{i=1}^{k} n_i \sum_{j=1}^{\overline{r}_i} D_{i,j}$ where the $D_{i,j}$ are the absolutely irreducible components of D_i.

We use that $n_i > 0$, that D is numerically equivalent to rH and that $D_{i,j}.H > 0$ to get

$$\sum_{i=1}^{k} \overline{r}_i \leqslant \sum_{i=1}^{k}\sum_{j=1}^{\overline{r}_i} D_{i,j}.H \leqslant \sum_{i=1}^{k} n_i \sum_{j=1}^{\overline{r}_i} D_{i,j}.H = \sum_{i=1}^{k} n_i D_i.H = rH.H,$$

which proves the lemma. □

The next theorem involves the *defect* $\delta(B)$ of a smooth absolutely irreducible curve B defined over $\mathbb{F}_q$ of genus g_B, which is defined by

$$\delta(B) \coloneqq q + 1 + mg_B - \#B(\mathbb{F}_q).$$

By the Serre-Weil bound (2.10) this defect is a non-negative number. The so-called maximal curves have defect 0, and the smaller the number of rational points on B is, the greater the defect is.

Theorem 3.2.8. *Let $\pi : X \to B$ be a fibered surface whose canonical divisor K_X is nef. Assume that H is a rational effective ample divisor on X having at least one horizontal component and avoiding a set S of rational points on X. For any positive integer r the minimum distance of the code $\mathcal{C}(X, rH, S)$ satisfies*

$$d(X, rH, S) \geqslant d^*(X, rH, S) + \delta(B)$$

where $d^*(X, rH, S)$ is given by formula (3.3).

Recall that the general bound we obtain in Theorem 3.1.2 in Section 3.1 for surfaces with nef canonical divisor is $d(X, rH, S) \geqslant d^*(X, rH, S)$, thus the bound from Theorem 3.2.8 is always equal or better. Actually Theorem 3.2.8 is surprising, since it says that the lower bound for the minimum distance is all the more large because the defect $\delta(B)$ is. Consequently it looks like considering fibered surfaces on curves with few rational points and large genus could lead to potentially good codes.

Proof. Recall that for any non-zero $f \in L(rH)$, we have $d(X, rH, S) \geqslant \#S - N(f)$, and that $N(f) \leqslant \sum_{i=1}^{k} \#D_i(\mathbb{F}_q)$ if we use the notation $D_f := rH + (f) = \sum_{i=1}^{k} n_i D_i$ introduced in (2.8). We again denote by $\overline{r}_i$ the number of absolutely irreducible components of D_i. In order to introduce the $\mathbb{F}_q$-irreducible components of D_f, write $k = h + v$, where h (respectively v) is the number of horizontal curves denoted by $H_1, \ldots, H_h$, (respectively fibral curves denoted by $F_1, \ldots, F_v$). Thus we get $N(f) \leqslant \sum_{i=1}^{h} \#H_i(\mathbb{F}_q) + \sum_{i=1}^{v} \#F_i(\mathbb{F}_q)$. Since B is a smooth curve, the morphisms $H_i \to B$ are flat. Applying Proposition 2.4.2 to horizontal curves and Theorem 2.4.1 to fibral curves gives

$$\begin{aligned} N(f) &\leqslant h(\#B(\mathbb{F}_q) - mg_B) + m\sum_{i=1}^{h} \pi_{H_i} + q\sum_{i=1}^{h}(\overline{r}_i - 1) + qv + v + m\sum_{i=1}^{v} \pi_{F_i} \\ &= h(\#B(\mathbb{F}_q) - mg_B - q) + m\sum_{i=1}^{k} \pi_{D_i} + q\sum_{i=1}^{k} \overline{r}_i + v, \end{aligned} \tag{3.5}$$

where we used the fact that $v \leqslant \sum_{i=h+1}^{k} \overline{r}_i$.

Since the canonical divisor of the fibered surface is assumed to be nef, Lemma 3.1.1 gives a bound for $\sum_{i=1}^{k} \pi_{D_i}$. We set $v = k - h$ and we use Lemma 3.2.7 with (3.5) to obtain

$$\begin{aligned} N(f) &\leqslant h(\#B(\mathbb{F}_q) - mg_B - q) + m(\pi_{rH} - 1) + mk + qrH^2 + v \\ &= h(\#B(\mathbb{F}_q) - mg_B - q - 1) + m(\pi_{rH} - 1) + mk + qrH^2 + k \\ &= -h\delta(B) + m(\pi_{rH} - 1) + mk + qrH^2 + k. \end{aligned}$$

Now, $D_f.F \equiv rH.F > 0$ since F is a generic fiber and rH is assumed to have at least one horizontal component. Thus, D_f has also at least one horizontal component, that is $h \geqslant 1$. Moreover, again from Lemma 3.1.1, we have $k \leqslant rH^2$. As the defect $\delta(B)$ is non-negative it follows that

$$N(f) \leqslant -\delta(B) + rH^2(q + 1 + m) + m(\pi_{rH} - 1)$$

and the theorem is proved. □

3.2.4 Fibered surfaces whose singular fibers are irreducible

In this subsection we drop off the condition on the canonical divisor of the fibered surface $\pi : X \to B$. Instead, we assume that every singular fiber on X is $\mathbb{F}_q$-irreducible. To construct examples of such surfaces, fix any $d \geqslant 1$ and recall that the dimension of the space of degree d homogeneous polynomials in three variables is $\binom{d+2}{2}$. Hence the space $\mathcal{P}_d$ of plane curves of degree d is $\mathcal{P}_d = \mathbb{P}^{\binom{d+2}{2}-1}$. Any curve B drawn in $\mathcal{P}_d$ gives rise to a fibered surface, whose fibers are plane curves of degree d, that is with $\pi_0 = \frac{(d-1)(d-2)}{2}$. The locus of singular curves being a subvariety of $\mathcal{P}_d$, choosing B not contained in this singular locus yields to a fibered surface with smooth generic fiber. As the locus of reducible curves has high codimension in $\mathcal{P}_d$, choosing B avoiding this locus yields to fibered surfaces without reducible fibers.

We consider the case where π_0 and g_B are both at least 2 and we set $\ell = \min(\pi_0, g_B) - 1 \geqslant 1$. We recall again that every divisor on X can be uniquely written as a sum of horizontal and fibral curves. If we denote by H an horizontal curve and by V a fibral curve defined over $\mathbb{F}_q$, we have that $\pi_H \geqslant g_B$ and $\pi_V = \pi_0$. Therefore, in this setting, X contains no $\mathbb{F}_q$-irreducible curves defined over $\mathbb{F}_q$ of arithmetic genus smaller than or equal to ℓ. Thus Lemma 3.1.3 applies and gives the same bound for $\sum_{i=1}^{k} \pi_i$ as when K_X is nef and the bound $k \leqslant (\pi_{rH} - 1)/\ell$ for the number k of $\mathbb{F}_q$-irreducible components of D_f. We consider this new bound for k in the proof of Theorem 3.2.8 and we get instead the following result.

Theorem 3.2.9. *Let $\pi : X \to B$ be a fibered surface. We consider a rational effective ample divisor H on X having at least one horizontal component and avoiding a set S of rational points on X. Let r be a positive integer. We denote by g_B the genus of B and by π_0 the arithmetic genus of the fibers and we set $\ell = \min(\pi_0, g_B) - 1$. Suppose that every singular fiber is $\mathbb{F}_q$-irreducible and that $\ell \geqslant 1$. Then the minimum distance of the code $\mathcal{C}(X, rH, S)$ satisfies*

$$d(X, rH, S) \geqslant d^*(X, rH, S) + \left(rH^2 - \frac{\pi_{rH} - 1}{\ell} \right) (q + 1 + m) + \delta(B),$$

where $d^*(X, rH, S)$ is given by formula (3.3).

Naturally this bound is better than the one in Theorem 3.2.8 if and only if $\pi_{rH} - 1 < \ell r H^2$. Furthermore it improves the bound of Theorem 3.1.4 by the addition of the non-negative term $\delta(B)$.

3.3 An example: surfaces in $\mathbb{P}^3$

We conclude the chapter with this section devoted to the study of the minimum distance of algebraic geometry codes from a surface X of degree $d \geqslant 3$ embedded in $\mathbb{P}^3$. We consider the class L of an hyperplane section of X. The divisor L is ample, we have $L^2 = d$ and the canonical divisor on X is $K_X = (d-4)L$ (see [47, p. III.6.4]). In this setting, we fix a rational effective ample divisor H and r a positive integer. We apply our previous theorems in this context to give bounds on the minimum distance of the code $\mathcal{C}(X, rH, S)$.

We recall that cubic surfaces are considered by Voloch and Zarzar in [55] and [61] to provide computationally good codes. In Section 4 of [30], Little and Schenck

propose theoretical and experimental results for surfaces in $\mathbb{P}^3$, always in the prospect of finding good codes. We also contribute to this study with a view to bounding the minimum distance according to the geometry of the surface.

Proposition 3.3.1. *Let X be a surface of degree $d \geqslant 3$ embedded in $\mathbb{P}^3$. Consider a rational effective ample divisor H avoiding a set S of rational points on X and let r be a positive integer. Then the minimum distance of the code $\mathcal{C}(X, rH, S)$ satisfies:*

1. *if X is a cubic surface, then*

$$d(X, rH, S) \geqslant d^*(X, rH, S) + mr(\pi_H - 1).$$

2. *If X has degree $d \geqslant 4$, then*

$$d(X, rH, S) \geqslant d^*(X, rH, S),$$

where

$$d^*(X, rH, S) = \#S - rH^2(q + 1 + m) - m(\pi_{rH} - 1)$$

is the function defined in (3.3).

Proof. Since $K_X = (d-4)L$ we have for cubic surfaces that $K_X = -L$ and thus the canonical divisor is anti-ample, while for surfaces of degree $d \geqslant 4$ the canonical divisor is ample or the zero divisor, thus it is nef. Hence we can apply Theorem 3.1.2 from which the proposition follows. □

3.3.1 Surfaces in $\mathbb{P}^3$ without irreducible curves of low genus

In the complex setting, the Noether-Lefschetz theorem asserts that a general surface X of degree $d \geqslant 4$ in $\mathbb{P}^3$ is such that $\mathrm{Pic}(X) = \mathbb{Z}L$, where L is the class of an hyperplane section (see [17]). Here, general means outside a countable union of proper subvarieties of the projective space parametrizing the surfaces of degree d in $\mathbb{P}^3$. Even if we do not know an analog of this statement in our context, it suggests us the strong assumption we take in this subsection, namely in Lemma 3.3.2 and Proposition 3.3.3.

Lemma 3.3.2. *Let X be a surface of degree $d \geqslant 4$ in $\mathbb{P}^3$ of arithmetic Picard number one. Suppose that $\mathrm{NS}(X)$ is generated by the class of an hyperplane section L. Consider a $\mathbb{F}_q$-irreducible curve D on X of arithmetic genus π_D. Then*

$$\pi_D \geqslant \frac{(d-1)(d-2)}{2}.$$

Proof. Let a be the integer such that $D = aL$ in $\mathrm{NS}(X)$. Since D is a $\mathbb{F}_q$-irreducible curve and L is ample, we must have $a > 0$. Then, using the adjonction formula, we get

$$\begin{aligned} 2\pi_D - 2 = D^2 + D.K &= a^2L^2 + aL.(d-4)L \\ &= a^2 d + ad(d-4) \geqslant d + d(d-4), \end{aligned}$$

from which the statement follows. □

By the previous lemma, it is straightforward that in our context X does not contain any $\mathbb{F}_q$-irreducible curve of arithmetic genus smaller than or equal to ℓ for $\ell = (d-1)(d-2)/2 - 1 = d(d-3)/2$. This allows us to apply Theorem 3.1.4, and get the following proposition.

Proposition 3.3.3. *Let X be a degree $d \geqslant 4$ surface in $\mathbb{P}^3$ of arithmetic Picard number one whose Néron-Severi group $\mathrm{NS}(X)$ is generated by the class of an hyperplane section L. Assume that S is a set of rational points on X avoiding L. For any positive integer r the minimum distance of the code $\mathcal{C}(X, rL, S)$ satisfies*

$$d(X, rL, S) \geqslant d^*(X, rL, S, L) + rd\left(1 - \frac{r+d-4}{d(d-3)}\right)(q+1+m)$$

where

$$d^*(X, rL, S) = \#S - rd(q+1+m) - mrd\frac{r+d-4}{2}.$$

3.3.2 Surfaces in $\mathbb{P}^3$ of arithmetic Picard number one

In this subsection we suppose that the arithmetic Picard number of X is one, but we do not take the assumption that the Néron-Severi group is generated by an hyperplane section. Also in this case we can apply Theorem 3.2.3 which brings us to the following proposition.

Proposition 3.3.4. *Let X be a surface of degree $d \geqslant 4$ in $\mathbb{P}^3$. Assume that $\mathrm{NS}(X) = \mathbb{Z}H$ for an ample divisor H. Consider $L = hH$, the class of an hyperplane section of X, for h a positive integer. Let S be a set of rational points on X avoiding H and let r be a positive integer. Then the minimum distance of the code $\mathcal{C}(X, rH, S)$ satisfies*

$$d(X, rH, S) \geqslant \begin{cases} \#S - (q+1+m) - \frac{rH^2}{2}(r + h(d-4)) \text{ if } r > \frac{2(q+1+m)}{mH^2}, \\ \#S - r(q+1+m) - \frac{rH^2}{2}(1 + h(d-4)) \text{ otherwise.} \end{cases}$$

Proof. Since we have $3H^2 + H.K_X = 3H^2 + H.(d-4)L = 3H^2 + h(d-4)H^2 = H^2(3 + h(d-4)) \geqslant 0$, we can apply point (1) of Theorem 3.2.3, from which the proposition follows. □

Chapter 4

Algebraic geometry codes over abelian surfaces containing no absolutely irreducible curves of low genus

In this chapter we focus on the study of codes constructed from abelian surfaces. In particular, we give bounds on the minimum distance $d(A, rH, S)$ of the algebraic geometry code $\mathcal{C}(A, rH, S)$ constructed from an abelian surface A, a set S of rational points on A, a rational effective ample divisor H on A avoiding S and an integer $r > 0$. The results we present in this chapter are original and appear in a paper ([5]) submitted to an international review.

The chapter is structured as follows. In Section 4.1, we consider evaluation codes on general abelian surfaces. We compute their dimension and give a lower bound on their minimum distance (Theorem 4.1.2) using results from the previous chapter. In Section 4.2, we sharpen this lower bound in the case of abelian surfaces which do not contain absolutely irreducible curves defined over $\mathbb{F}_q$ of arithmetic genus less or equal than a fixed integer ℓ (Theorem 4.2.3). We remark that the bound obtained for $\ell = 2$ improves the one obtained for $\ell = 1$ for q sufficiently large and $1 < r < \sqrt{q}$ (Remark 4.2.5). Thus we investigate in Section 4.3 the case of abelian surfaces with no curves of genus 1 nor 2. We prove Proposition 4.3.2 and Proposition 4.3.3, that give all the possibility for abelian surfaces containing no absolutely irreducible curves of genus up to 2. Finally, in Section 4.4, we make explicit the terms that appear in the lower bounds for the minimum distance obtained in Theorem 4.1.2 and Theorem 4.2.3.

4.1 The parameters of codes from abelian surfaces

In this section we begin the estimation of the parameters of the code $\mathcal{C}(A, rH, S)$. To this end, let A be an abelian surface defined over $\mathbb{F}_q$, let H be an effective ample divisor on A rational over $\mathbb{F}_q$ avoiding a set S of rational points on A and let r be an integer large enough so that rH is very ample ($r \geqslant 3$ is sufficient by [38, III, §17]).

Since A is an abelian surface we have ([38, III, §16]) $K_A = 0$ and $p_a(A) = -1$. Moreover if rH is very ample, then we can deduce from [22, V, Lemma 1.7] that $\ell(K - rH) = \ell(-rH) = 0$ and that $s(rH) = 0$ ([38, III, §16]). So, finally, if the evaluation map ev is injective, we get from Subsection 2.3.1 that the dimension of the code $\mathcal{C}(A, rH, S)$ is

$$\dim_{\mathbb{F}_q} L(rH) = r^2 \frac{H^2}{2}.$$

We are now going to give a lower bound on the minimum distance of $\mathcal{C}(A, rH, S)$ using Lemma 2.3.1. As to do so, we need Lemma 4.1.1 below, giving upper bounds on the number k of irreducible components of the effective divisor D linearly equivalent to rH and on the sum of the arithmetic genera of its components D_i. We recall for this purpose that in the case of abelian surfaces the generalisation of the adjunction formula introduced in Section 1.3 says that for any curve D of arithmetic genus π lying on A we have $D^2 = 2\pi - 2$, since $K_A = 0$.

Lemma 4.1.1. *Let D be an effective divisor linearly equivalent to rH. Let $D = \sum_{i=1}^{k} n_i D_i$ be its decomposition as a sum of $\mathbb{F}_q$-irreducible curves and let π_i be the arithmetic genus of D_i for $i = 1, \ldots, k$. Then we have:*

1. $\sum_{i=1}^{k} \pi_i \leqslant r^2 \frac{H^2}{2} + k$;
2. $k \leqslant rH^2$.

Proof. The first bound can be retrieved by Lemma 3.1.1 (2i). Indeed in the case of abelian surfaces K_A is nef and since $K_A = 0$ we have $\pi_{rH} = r^2 H^2/2$. The second bound is exactly the first statement of Lemma 3.1.1. □

As a consequence of Lemma 4.1.1 we can state the following theorem.

Theorem 4.1.2. *Let A be an abelian surface defined over $\mathbb{F}_q$ of trace $\mathrm{Tr}(A)$. Consider a set S of rational points on A, a rational effective ample divisor H on A avoiding S, and a positive integer r. Then the minimum distance $d(A, rH, S)$ of the code $\mathcal{C}(A, rH, S)$ satisfies*

$$d(A, rH, S) \geqslant \#S(\mathbb{F}_q) - rH^2(q + 1 - \mathrm{Tr}(A) + m) - mr^2 \frac{H^2}{2}.$$

Proof. The theorem follows from Lemma 2.3.1, for which items (1) and (2) hold from Lemma 4.1.1 and item (2) holds from Corollary 2.4.4 (1). □

Remark 4.1.3. Let H be an ample divisor. Suppose that H is irreducible over $\mathbb{F}_q$, but reducible on a Galois extension of prime degree e. Then H is a sum of e conjugate irreducible components such that the intersection points are also conjugates under the Galois group. Then, by Lemma 2.3 of [55], we have

$$k \leqslant r \frac{H^2}{e}.$$

Hence, under this hypothesis, we get a sharper bound on the number of irreducible components of a divisor linearly equivalent to rH, thus a sharper bound for $d(A, rH, S)$ in Theorem 4.1.2.

4.2 Codes from abelian surfaces without curves of small genus

We consider now evaluation codes $\mathcal{C}(A, rH, S)$ on abelian surfaces which contain no absolutely irreducible curves defined over $\mathbb{F}_q$ of arithmetic genus smaller than or equal to an integer ℓ.

Throughout this section A denotes a *simple* abelian surface defined over $\mathbb{F}_q$. Note that by Proposition 5 of [18] a simple abelian surface contains no $\mathbb{F}_q$-irreducible curves of arithmetic genus 0 nor 1 defined over $\mathbb{F}_q$. In particular every irreducible curve on A has arithmetic genus greater than or equal to 2 and thus it is relevant to take $\ell \geqslant 1$.

Let us recall that in Subsection 2.3.2 for any non-zero function $f \in L(G)$ we have defined $N(f)$ to be the number of rational points on the divisor of zeroes of f. In the context of this section, we can bound this quantity as follows.

Lemma 4.2.1. *Let A be a simple abelian surface defined over $\mathbb{F}_q$ of trace $\mathrm{Tr}(A)$. Let ℓ be a positive integer such that for every absolutely irreducible curves of arithmetic genus π lying on A we have $\pi > \ell$. Let f be a function in $L(rH)$ with associated effective rational divisor $D = \sum_{i=1}^{k} n_i D_i$ as given in equation (2.8). Write $k = k_1 + k_2$ where k_1 is the number of D_i which have arithmetic genus $\pi_i > \ell$ and k_2 is the number of D_i which have arithmetic genus $\pi_i \leqslant \ell$. Then*

$$N(f) \leqslant k_1(q + 1 - \mathrm{Tr}(A) - 2m) + m \sum_{i=1}^{k_1} \pi_i + k_2(\ell - 1), \tag{4.1}$$

where $\pi_i > \ell$.

Proof. Without loss of generality, we consider $\{D_1, \ldots, D_{k_1}\}$ to be the set of the D_i which have arithmetic genus $\pi_i > \ell$ and $\{D_{k_1+1}, \ldots, D_k\}$ to be the set of the k_2 curves which have arithmetic genus $\pi_i \leqslant \ell$. Thus, using Corollary 2.4.4 (2) we get

$$\sum_{i=1}^{k_1} \#D_i(\mathbb{F}_q) \leqslant k_1(q + 1 - \mathrm{Tr}(A) - 2m) + m \sum_{i=1}^{k_1} \pi_i$$

where $\pi_i > \ell$. Under the hypothesis that any absolutely irreducible curve on A has arithmetic genus $\pi > \ell$, we have that the k_2 curves that have arithmetic genus $\pi_i \leqslant \ell$ are necessarily non absolutely irreducible. Applying Proposition 2.4.5 to these curves and summing on k_2, we get

$$\sum_{i=k_1+1}^{k} \#D_i(\mathbb{F}_q) \leqslant \sum_{i=k_1+1}^{k} (\pi_i - 1) \leqslant k_2(\ell - 1).$$

The proof is now complete using that $N(f) \leqslant \sum_{i=1}^{k} \#D_i(\mathbb{F}_q)$ (see inequality (2.9) in the proof of Lemma 2.3.1). □

In order to use inequality (4.1) to deduce a lower bound on the minimum distance of the code $\mathcal{C}(A, rH, S)$, it is sufficient to bound the numbers k_1 and k_2 and the sum $\sum_{i=1}^{k_1} \pi_i$.

Lemma 4.2.2. *With the same notations and under the same hypotheses as Lemma 4.2.1 we have:*

1. $k_1\sqrt{\ell} + k_2 \leqslant r\sqrt{\frac{H^2}{2}}$,
2. $\sum_{i=1}^{k_1} \pi_i \leqslant \alpha^2 + 2\sqrt{\ell}\alpha + (\ell+1)k_1$, *where* $\alpha := r\sqrt{\frac{H^2}{2}} - k_1\sqrt{\ell} - k_2$.

Proof. Let us prove the first assertion. Since H is ample, we have that $D_i.H > 0$ for every $i = 1, \ldots, k$ and $H^2 > 0$. From inequality (3.1) in the proof of Lemma 3.1.1 we deduce that $\pi_{D_i} - 1 \leqslant (D_i.H)^2/2H^2$ since $K_A = 0$. Taking the square root, we get

$$\sqrt{\pi_i - 1} \leqslant \frac{D_i.H}{\sqrt{2H^2}}.$$

Now taking into account that $1 \leqslant \pi_i - 1$ since A is assumed to be simple, summing for $i \in \{1, \ldots, k\}$, using that $n_i > 0$ and that $\sum_{i=1}^{k} n_i D_i.H = rH^2$, we obtain

$$\begin{aligned}
\sum_{i=1}^{k_1} \sqrt{\pi_i - 1} &= \sum_{i=1}^{k} \sqrt{\pi_i - 1} - \sum_{i=k_1+1}^{k} \sqrt{\pi_i - 1} \\
&\leqslant \sum_{i=1}^{k} \sqrt{\pi_i - 1} - k_2 \\
&\leqslant \frac{1}{\sqrt{2H^2}} \sum_{i=1}^{k} n_i D_i.H - k_2 \\
&= r\sqrt{\frac{H^2}{2}} - k_2.
\end{aligned}$$

Considering the k_1 curves that have arithmetic genus $\pi_i > \ell$, we have $\sqrt{\ell} \leqslant \sqrt{\pi_i - 1}$ and so $k_1\sqrt{\ell} \leqslant \sum_{i=1}^{k_1} \sqrt{\pi_i - 1}$. Thus we get

$$k_1\sqrt{\ell} + k_2 \leqslant r\sqrt{\frac{H^2}{2}}.$$

Let us now prove the last statement. For $i = 1, \ldots, k_1$, set $s_i = \sqrt{\pi_i - 1} - \sqrt{\ell}$. Under the hypothesis that $\pi_i \geqslant \ell + 1$, the s_i are non-negative real numbers. Thus

$$\sum_{i=1}^{k_1} s_i^2 \leqslant \left(\sum_{i=1}^{k_1} s_i\right)^2.$$

Moreover, we have seen above that

$$\sum_{i=1}^{k_1} s_i = \sum_{i=1}^{k_1} \sqrt{\pi_i - 1} - k_1\sqrt{\ell} \leqslant r\sqrt{\frac{H^2}{2}} - k_1\sqrt{\ell} - k_2 = \alpha.$$

Therefore, since $\pi_i = (s_i + \sqrt{\ell})^2 + 1 = s_i^2 + 2s_i\sqrt{\ell} + \ell + 1$ for $i \in \{1, \ldots, k_1\}$, we have

$$\begin{aligned}
\sum_{i=1}^{k_1} \pi_i &= \sum_{i=1}^{k_1} s_i^2 + 2\sqrt{\ell}\sum_{i=1}^{k_1} s_i + (\ell+1)k_1 \\
&\leqslant \left(\sum_{i=1}^{k_1} s_i\right)^2 + 2\sqrt{\ell}\sum_{i=1}^{k_1} s_i + (\ell+1)k_1 \\
&\leqslant \alpha^2 + 2\sqrt{\ell}\alpha + (\ell+1)k_1,
\end{aligned} \tag{4.2}$$

which completes the proof of the lemma. □

We can now prove the following theorem.

Theorem 4.2.3. *Let A be a simple abelian surface defined over $\mathbb{F}_q$ of trace $\mathrm{Tr}(A)$. Let $m = \lfloor 2\sqrt{q} \rfloor$, H be an ample divisor on A rational over $\mathbb{F}_q$ and r be a positive integer large enough so that rH is very ample. Moreover, let ℓ be a positive integer such that for every absolutely irreducible curves of arithmetic genus π lying on A we have $\pi > \ell$. Then the minimum distance $d(A, rH, S)$ of the code $\mathcal{C}(A, rH, S)$ satisfies*

$$d(X, rH, S) \geqslant \#S(\mathbb{F}_q) - \max\left(\left\lfloor r\sqrt{\frac{H^2}{2}} \right\rfloor (\ell - 1), \varphi(1), \varphi\left(\left\lfloor r\sqrt{\frac{H^2}{2\ell}} \right\rfloor\right)\right),$$

where

$$\varphi(x) := m\left(r\sqrt{\frac{H^2}{2}} - x\sqrt{\ell}\right)^2 + 2m\sqrt{\ell}\left(r\sqrt{\frac{H^2}{2}} - x\sqrt{\ell}\right) + x\left(q+1-\mathrm{Tr}(A)+(\ell-1)\left(m-\sqrt{\ell}\right)\right) + r\sqrt{\frac{H^2}{2}}(\ell-1).$$

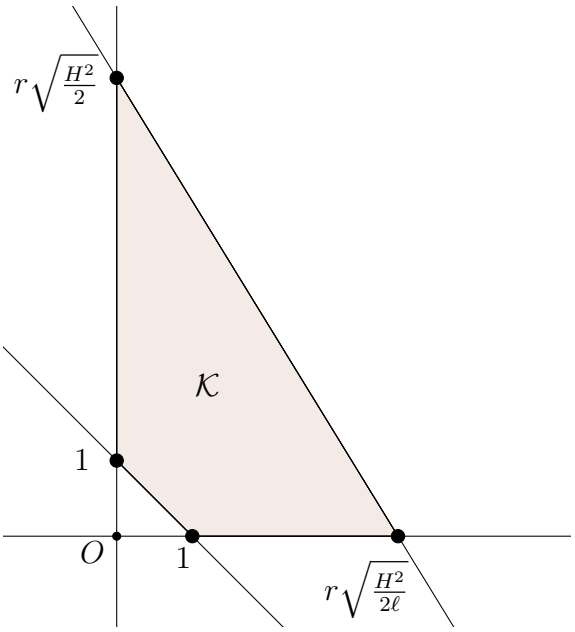
Proof. Combining Lemma 4.2.1 and Lemma 4.2.2, we get that $N(f) \leqslant \phi(k_1, k_2)$ where $\phi(k_1, k_2)$ is defined by

$$\phi(k_1, k_2) = \begin{cases} k_2(\ell - 1) & \text{if } k_1 = 0 \\ k_1\left(q + 1 - \mathrm{Tr}(A) + (\ell - 1)\left(m - \sqrt{\ell}\right)\right) & \\ +m\alpha^2 + 2m\sqrt{\ell}\alpha + r\sqrt{\frac{H^2}{2}}(\ell - 1) & \text{if } k_1 > 0 \end{cases}$$

where we have set $\alpha := r\sqrt{\frac{H^2}{2}} - k_1\sqrt{\ell} - k_2 \geqslant 0$. It thus remains to maximise the function $\phi(k_1, k_2)$ on the integer points inside the polygon $\mathcal{K}$ defined by

$$\mathcal{K} = \left\{(k_1, k_2) \mid 0 \leqslant k_1, 0 \leqslant k_2, 1 \leqslant k_1 + k_2, \sqrt{\ell}k_1 + k_2 \leqslant r\sqrt{\frac{H^2}{2}}\right\}$$

and represented below.



First, in the case where $k_1 = 0$, we notice that $k_2 \leqslant \left\lfloor r\sqrt{\frac{H^2}{2}} \right\rfloor$, which implies $\phi(0,k_2) \leqslant \left\lfloor r\sqrt{\frac{H^2}{2}} \right\rfloor (\ell-1)$. Secondly, for a fixed positive value of k_1 less than or equal to $r\sqrt{\frac{H^2}{2}}$, we can consider ϕ as a degree-2 polynomial in $\alpha \geqslant 0$, namely $\phi(k_1,k_2) = m\alpha(\alpha + 2\sqrt{\ell}) + \text{constant}$. This way, it is clear that the maximum of ϕ is reached for the maximal value of α, that is for the minimal value of k_2 such that $(k_1,k_2) \in \mathcal{K}$. Hence, for this second case we are reduced to maximise ϕ on the segment $\left[(1,0), \left(r\sqrt{\frac{H^2}{2\ell}}, 0\right)\right]$. As easily checked, ϕ is a convex function on this segment, so the maximum is reached at an extremal integer point, $(1,0)$ or $\left(\left\lfloor r\sqrt{\frac{H^2}{2\ell}} \right\rfloor, 0\right)$. Finally, note that we have $\phi(x,0) = \varphi(x)$. Since $d(X,rH,S) \geqslant \#S(\mathbb{F}_q) - \max\{N(f), f \in L(rH) \setminus \{0\}\}$, the theorem is proved. □

Remark 4.2.4. The bound in Theorem 4.2.3 applies with $\ell = 1$ on simple abelian surfaces since they do not contain irreducible curves of arithmetic genus 0 nor 1, as remarked at the beginning of this section. Note that for $\ell = 1$ we have $\left\lfloor r\sqrt{\frac{H^2}{2}} \right\rfloor (\ell - 1) = 0$ and thus in this context we are reduced to consider the maximum between $\varphi(1)$ and $\varphi\left(\left\lfloor r\sqrt{\frac{H^2}{2}} \right\rfloor\right)$ in Theorem 4.2.3. In order to easily compare these two values, let us consider a weaker version of our theorem by removing the integer part. Indeed, $\varphi\left(\left\lfloor r\sqrt{\frac{H^2}{2}} \right\rfloor\right) \leqslant \varphi\left(r\sqrt{\frac{H^2}{2}}\right)$. Consequently we have $d \geqslant \#A(\mathbb{F}_q) - \max\left(\varphi(1), \varphi\left(r\sqrt{\frac{H^2}{2}}\right)\right)$ and after some calculations we get

$$d(X,rH,S) \geqslant \begin{cases} \#S(\mathbb{F}_q) - r\sqrt{\frac{H^2}{2}}\,(q+1-\mathrm{Tr}(A)) & \text{if } r \leqslant \frac{\sqrt{2}(q+1-\mathrm{Tr}(A)-m)}{m\sqrt{H^2}}, \\ \#S(\mathbb{F}_q) - (q+1-\mathrm{Tr}(A)-m) - mr^2\frac{H^2}{2} & \text{otherwise.} \end{cases}$$

In particular if $A = \mathrm{Jac}(C)$ is the Jacobian of a curve C of genus 2 which is simple, then setting $H = C$ with $H^2 = C^2 = 2\pi_C - 2 = 2$ by the adjunction formula, and taking $S = \mathrm{Jac}(C)(\mathbb{F}_q)$, we obtain

$$d(\mathrm{Jac}(C), rC) \geqslant \begin{cases} \#\,\mathrm{Jac}(C)(\mathbb{F}_q) - r\#C(\mathbb{F}_q) & \text{if } r \leqslant \frac{q+1-\mathrm{Tr}(A)-2m}{m}, \\ \#\,\mathrm{Jac}(C)(\mathbb{F}_q) - \#C(\mathbb{F}_q) - m(r^2-1) & \text{otherwise.} \end{cases}$$

This bound coincides with the bound in the main theorem of [18].

Remark 4.2.5. We point out, using an elementary asymptotic analysis for large q, that our estimation of the minimum distance is better for larger ℓ. We assume that ℓ is small (for example ℓ is a fixed value) and that $r = q^\rho$ for some $\rho > 0$. For simplicity, we also assume that $H^2 = 2$ (see Section 4.4) and remove the integer part. Taking into account that $|\mathrm{Tr}(A)| \leqslant 4\sqrt{q}$ yields to

$$\begin{cases} r(\ell-1)\sqrt{\frac{H^2}{2}} & \underset{q\to\infty}{\sim} & (\ell-1)q^\rho, \\ \varphi(1) & \underset{q\to\infty}{\sim} & cq^{\max\{1,2\rho+\frac{1}{2}\}}, \\ \varphi\left(r\sqrt{\frac{H^2}{2\ell}}\right) & \underset{q\to\infty}{\sim} & \frac{1}{\sqrt{\ell}}q^{1+\rho}, \end{cases}$$

where $c = 1, 3$ or 2 depending on whether $\rho < 1/4, \rho = 1/4$ or $\rho > 1/4$. Consequently, in this setting, the lower bound d^* obtained in Theorem 4.2.3 satisfies

$$\begin{cases} \#S(\mathbb{F}_q) - d^* \underset{q\to\infty}{\sim} 2q^{2\rho+\frac{1}{2}} \text{ if } \rho \geqslant \frac{1}{2}, \\ \#S(\mathbb{F}_q) - d^* \underset{q\to\infty}{\sim} \frac{1}{\sqrt{\ell}} q^{1+\rho} \text{ if } 0 < \rho < \frac{1}{2}. \end{cases}$$

So for q sufficiently large and $r = q^\rho$ with $0 < \rho < \frac{1}{2}$, the bound in Theorem 4.2.3 obtained for instance for $\ell = 2$ is better than the one obtained for $\ell = 1$, that is for any simple abelian variety. We thus focus in the next section on the existence of simple abelian surfaces which do not contain absolutely irreducible curves of arithmetic genus 2.

4.3 Abelian surfaces without curves of genus 1 nor 2

In light of Remark 4.2.5, considering abelian surfaces without absolutely irreducible curves of small arithmetic genus will lead to a sharper lower bound on the minimum distance of the evaluation code $\mathcal{C}(A, rH, S)$. Hence, in this section, we look for abelian surfaces which satisfy the property of containing no absolutely irreducible curves defined over $\mathbb{F}_q$ of arithmetic genus 0, 1 nor 2.

By the theorem of classification of Weil (Theorem 1.4.10), a principally polarized abelian surface defined over $\mathbb{F}_q$ is isomorphic to either the polarized Jacobian of a curve of genus 2 over $\mathbb{F}_q$, either the product of two polarized elliptic curves over $\mathbb{F}_q$ or either the Weil restriction from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$ of a polarized elliptic curve defined over $\mathbb{F}_{q^2}$. It is straightforward to see that the Jacobian of a curve of genus 2 contains the curve itself and that the product of two elliptic curves contains copies of each of them. Therefore, it remains two cases to consider. First, there is the case of abelian surfaces which do not admit a principal polarization. We prove in Proposition 4.3.2 that they always satisfy the desired property. Secondly, there is the case of Weil restrictions of elliptic curves. We give in Proposition 4.3.3 necessary and sufficient conditions for Weil restrictions of elliptic curves to satisfy the property we want.

Throughout this section we will make use of the two following well-known results. An abelian surface contains a *smooth* absolutely irreducible curve of genus 1 if and only if it is isogenous to the product of two elliptic curves. Moreover, a simple abelian surface contains a *smooth* absolutely irreducible curve of genus 2 if and only if it is isogenous to the Jacobian of a curve of genus 2 (see [15, Proposition 2]). The following lemma gives necessarily and sufficient conditions to avoid the presence of *non necessarily smooth* absolutely irreducible curves of arithmetic genus 0, 1 and 2.

Lemma 4.3.1. *Let A be an abelian surface. Then the three following statements are equivalent:*

1. *A is simple and not isogenous to a Jacobian surface;*
2. *A does not contain absolutely irreducible curves of arithmetic genus 0, 1 nor 2;*
3. *A does not contain absolutely irreducible smooth curves of genus 0, 1 nor 2.*

Proof. Let us prove that (1) ⇒ (2). Let A be a simple abelian surface which is not isogenous to the Jacobian of a genus 2 curve. Let C be an absolutely irreducible curve lying on A and let $\nu : \tilde{C} \mapsto C$ be its normalisation map. The case of genus 0 and 1 is treated in [18, §2]. For the genus 2 case, assume by contradiction that $\pi(C) = 2$. We get $g(\tilde{C}) = \pi(C) = 2$ so $\tilde{C} = C$ is smooth and thus by Proposition 2 of [15] A is isogenous to the Jacobian of C, in contradiction with the hypotheses.

The implication (2) ⇒ (3) is trivial since for smooth curves the geometric and arithmetic genus coincide.

Finally let us prove that (3) ⇒ (1). Assume by contradiction that A is not simple, hence A is isogenous to the product of two elliptic curves and thus it contains at least a smooth absolutely irreducible curve of genus 1, in contradiction with (3). Now assume that A is simple and isogenous to a Jacobian surface. Then by Proposition 2 of [15], A contains a smooth absolutely irreducible curve of genus 2, again in contradiction with (3). This concludes the proof.

□

4.3.1 Non-principally polarized abelian surfaces

An isogeny class of abelian varieties over $\mathbb{F}_q$ is said to be not principally polarizable if it does not contain a principally polarizable abelian variety over $\mathbb{F}_q$. We recalled a characterization of non-principally polarized isogeny class of abelian surfaces in Subsection 1.4.3. The following proposition states that abelian surfaces which do not admit a principal polarization have naturally the property we are searching for.

Proposition 4.3.2. *Let A be an abelian surface in a not principally polarizable isogeny class. Then A does not contain absolutely irreducible curves of arithmetic genus* 0, 1 *nor* 2.

Proof. It is well-known that an abelian variety contains no curves of genus 0. Since A is not isogenous to a principally polarizable abelian surface, it follows that it is not isogenous to a product of two elliptic curves nor to a Jacobian surface. By Lemma 4.3.1 we conclude the proof. □

Thus for A an abelian surface which do not admit a principal polarization Theorem 4.2.3 applies with $\ell = 2$.

4.3.2 Weil restrictions of elliptic curves

Let $k = \mathbb{F}_q$ and let K denotes an extension of finite degree $[K : k]$ of k. Let E be an elliptic curve defined over K. The K/k-Weil restriction of scalars of E is an abelian variety $W_{K/k}(E)$ of dimension $[K : k]$ defined over k (see [37, §16] for a presentation in terms of universal property and see [15, §3] for a constructive approach). We consider here the $\mathbb{F}_{q^2}/\mathbb{F}_q$-Weil restriction of an elliptic curve E defined over $\mathbb{F}_{q^2}$ which is an abelian surface A defined over $\mathbb{F}_q$.

Let $f_{E/\mathbb{F}_{q^2}}(t)$ be the Weil polynomial of the elliptic curve E defined over $\mathbb{F}_{q^2}$. Then the Weil polynomial of A over $\mathbb{F}_q$ is given (see [14, Prop 3.1]) by

$$f_{A/\mathbb{F}_q}(t) = f_{E/\mathbb{F}_{q^2}}(t^2). \tag{4.3}$$

Since $f_{E/\mathbb{F}_{q^2}}(t) = t^2 - \mathrm{Tr}(E/\mathbb{F}_{q^2})t + q^2$ we have $f_A(t) = t^4 - \mathrm{Tr}(E/\mathbb{F}_{q^2})t^2 + q^2$, thus it follows from formula (1.4) that the trace of A over $\mathbb{F}_q$ is equal to 0. Moreover, since the number of $\mathbb{F}_q$-rational points on an abelian variety A defined over $\mathbb{F}_q$ equals $f_{A/\mathbb{F}_q}(1)$, we get that the number of rational points on $A = W_{\mathbb{F}_{q^2}/\mathbb{F}_q}(E)$ over $\mathbb{F}_q$ is the same as the number of rational points on E over $\mathbb{F}_{q^2}$, i.e. we have $\#A(\mathbb{F}_q) = f_{A/\mathbb{F}_q}(1) = f_{E/\mathbb{F}_{q^2}}(1) = \#E(\mathbb{F}_{q^2})$. Indeed this equality comes from a canonical isomorphism $A(\mathbb{F}_q) \cong E(\mathbb{F}_{q^2})$.

Proposition 4.3.3. *Let q be a power of a prime p. Let E be an elliptic curve defined over $\mathbb{F}_{q^2}$ of Weil polynomial $f_{E/\mathbb{F}_{q^2}}(t) = t^2 - \mathrm{Tr}(E/\mathbb{F}_{q^2})t + q^2$. Let A be the $\mathbb{F}_{q^2}/\mathbb{F}_q$-Weil restriction of the elliptic curve E. Then A does not contain absolutely irreducible curves defined over $\mathbb{F}_q$ of arithmetic genus 0, 1 nor 2 if and only if one of the following conditions holds*

1. $\mathrm{Tr}(E/\mathbb{F}_{q^2}) = 2q - 1$;
2. $p > 2$ *and* $\mathrm{Tr}(E/\mathbb{F}_{q^2}) = 2q - 2$;
3. $p \equiv 11 \mod 12$ *or* $p = 3$, q *is a square and* $\mathrm{Tr}(E/\mathbb{F}_{q^2}) = q$;
4. $p = 2$, q *is nonsquare and* $\mathrm{Tr}(E/\mathbb{F}_{q^2}) = q$;
5. $q = 2$ *or* $q = 3$ *and* $\mathrm{Tr}(E/\mathbb{F}_{q^2}) = 2q$.

Proof. Let E be an elliptic curve defined over $\mathbb{F}_{q^2}$ and let A be the $\mathbb{F}_{q^2}/\mathbb{F}_q$-Weil restriction of E. Let $f_A(t) = t^4 + at^3 + bt^2 + qat + q^2$ be the Weil polynomial of A. Recall that we have $f_A(t) = t^4 - \mathrm{Tr}(E/\mathbb{F}_{q^2})t^2 + q^2$ by equation (4.3) and thus $(a, b) = (0, -\mathrm{Tr}(E/\mathbb{F}_{q^2}))$. Theorem 1.2-(2) with Table 1.2 in [24] gives necessary and sufficient conditions on the couple (a, b) for a simple abelian surface with the corresponding Weil polynomial not to be isogenous to the Jacobian of a smooth curve of genus 2.

Let us suppose that the trace of the elliptic curve E over $\mathbb{F}_{q^2}$ does not fit one of the conditions (1) – (5). Let us remark that by Theorem 1.4 in [24] the first case of Table 1.2 in [24, Theorem 1.2-(2)] corresponds to all simple abelian surfaces which do not admit a principal polarization. Moreover, the cases (1) – (5) cover the remaining cases of Table 1.2. Then $f_A(t)$ does not represent an isogeny class of simple principally polarizable abelian surfaces not containing a Jacobian surface. Hence A is either not principally polarizable, or not simple or isogenous to the Jacobian of a curve of genus 2. In the first case A would not be a Weil restriction of an elliptic curve since these last one admit a principal polarization. In the second case, A would contain a curve of genus 1 and finally in the third case it would contain a curve of genus 2. Thus we proved that if A does not contain absolutely irreducible curves defined over $\mathbb{F}_q$ of arithmetic genus 0, 1 nor 2 then one of conditions (1) – (5) holds.

Conversely, using again Table 1.2 in [24, Theorem 1.2-(2)] we get that in each case from (1) to (5) of our proposition, the couple $(0, -\mathrm{Tr}(E/\mathbb{F}_{q^2}))$ corresponds to simple abelian surfaces not isogenous to the Jacobian of a curve of genus 2. Therefore in these cases A does not contain absolutely irreducible *smooth* curves of geometric genus 0, 1 nor 2, and thus by Lemma 4.3.1, A does not contain absolutely irreducible curves of arithmetic genus 0, 1 nor 2. □

Remark 4.3.4. Let us mention two cases in which Weil restrictions of elliptic curves do contain curves of genus 1 or 2. First, if the elliptic curve E is defined over $\mathbb{F}_q$,

it is clearly a subvariety of A. Note that in Proposition 4.3.3 we do not need to suppose that the elliptic curve E defined over $\mathbb{F}_{q^2}$ is not defined over $\mathbb{F}_q$, because none of the the elliptic curves with trace over $\mathbb{F}_{q^2}$ as in cases (1)-(5) is defined over $\mathbb{F}_q$. Secondly, it is well-known that there are Weil restrictions of elliptic curves that are isogenous to Jacobian surfaces (see for example [45]) which thus contain smooth curves of genus 2.

Remark 4.3.5. Let $q^2 = p^{2n}$ with p prime. By Deuring theorem (see for instance [56, Th. 4.1]) for every integer β satisfying $|\beta| \leqslant 2q$ such that $\gcd(\beta, p) = 1$, or $\beta = \pm 2q$, or $\beta = \pm q$ and $p \not\equiv 1 \mod 3$, there exists an elliptic curve of trace β over $\mathbb{F}_{q^2}$. Using Deuring theorem it is easy to check the existence of an elliptic curve with the given trace for each of the five cases in the previous theorem.

Remark 4.3.6. Note that the bound in Theorem 4.2.3 becomes relevant for $q \geqslant B$ with $B \approx 4(\sqrt{H^2} + 1)^2$ and it is non-relevant for small q. Therefore case (5) of Proposition 4.3.3 does not give rise to practical cases.

Let us briefly outline the results obtained in the last sections. The surfaces arising in Propositions 4.3.2 and 4.3.3 give rise to codes for which the lower bound on the minimum distance of Theorem 4.2.3 applies with $\ell = 2$.

We have exploited the fact that, for q sufficiently large and $r = q^\rho$ with $0 < \rho < \frac{1}{2}$, the bound obtained for $\ell = 2$ improves the one obtained for $\ell = 1$. Note also that under the same hypotheses the bound for $\ell = 3$ improves the one for $\ell = 2$. Hence it would be interesting in the future to investigate on the existence of abelian surfaces without absolutely irreducible curves of genus ≤ 3 lying on them.

4.4 To make explicit the lower bounds for the minimum distance

Let us take S to be whole set of rational points on A and consider the code $\mathcal{C}(A, rH)$. We now show how the terms $\#A(\mathbb{F}_q)$, $\mathrm{Tr}(A)$ and H^2 appearing in the lower bounds for the minimum distance $d(A, rH)$ given in Theorems 4.1.2 and 4.2.3 can be computed in many cases. As recalled in the introduction of Section 4.3, three cases have to be distinguished in the case of principally polarized abelian surfaces, according to Weil classification (Theorem 1.4.10).

Let A be a principally polarized abelian surface defined over $\mathbb{F}_q$ with Weil polynomial $f_A(t) = (t - \omega_1)(t - \overline{\omega}_1)(t - \omega_2)(t - \overline{\omega}_2)$ where the ω_i's are complex numbers of modulus $\sqrt{q}$. Then we get:

$$\#A(\mathbb{F}_q) = f_A(1) = (1 - \omega_1)(1 - \overline{\omega}_1)(1 - \omega_2)(1 - \overline{\omega}_2).$$

We recall that by Definition 1.4.8 we have $\mathrm{Tr}(A) = \omega_1 + \overline{\omega}_1 + \omega_2 + \overline{\omega}_2$.

Moreover, for any divisor H on A, the adjunction formula (1.2) gives

$$H^2 = 2\pi_H - 2.$$

As recalled in Section 4.1, if the divisor H is ample then rH is very ample as soon as $r \geqslant 3$.

1. In case A is the Jacobian $\mathrm{Jac}(C)$ of a genus 2 curve C defined over $\mathbb{F}_q$, the numerator $P_C(t)$ of the zeta function of C is equal to the reciprocal polynomial of the Weil polynomial $f_{\mathrm{Jac}(C)}(t)$:

$$P_C(t) = t^4 f_{\mathrm{Jac}(C)}\left(\frac{1}{t}\right) = (1-\omega_1 t)(1-\overline{\omega}_1 t)(1-\omega_2 t)(1-\overline{\omega}_2 t).$$

   Hence we obtain

$$\begin{cases} \#C(\mathbb{F}_q) &= q+1-(\omega_1+\overline{\omega}_1+\omega_2+\overline{\omega}_2) \\ \#C(\mathbb{F}_{q^2}) &= q^2+1-(\omega_1^2+\overline{\omega}_1^2+\omega_2^2+\overline{\omega}_2^2) \end{cases}$$

   and thus

$$\#\,\mathrm{Jac}(C)(\mathbb{F}_q) = \frac{1}{2}\left(\#C(\mathbb{F}_{q^2}) + \#C(\mathbb{F}_q)^2\right) - q.$$

   Choosing $H = C$ for instance, we get an ample divisor on A with $H^2 = C^2 = 2\pi_C - 2 = 2$.

2. In case A is the product $E_1 \times E_2$ of two elliptic curves E_1 and E_2, each partial trace $\mathrm{Tr}(E_i) = \omega_i + \overline{\omega}_i$ is determined by $\#E_i(\mathbb{F}_q) = q+1-\mathrm{Tr}(E_i)$. So we have $\#A(\mathbb{F}_q) = \#E_1(\mathbb{F}_q) \times \#E_2(\mathbb{F}_q)$ and $\mathrm{Tr}(A) = \mathrm{Tr}(E_1) + \mathrm{Tr}(E_2)$.

   Any choice of rational points $P_i \in E_i$ leads to an ample divisor $H = E_1 \times \{P_2\} + \{P_1\} \times E_2$ such that $H^2 = (E_1 \times \{P_2\})^2 + (\{P_1\} \times E_2)^2 + 2(E_1 \times \{P_2\}).(\{P_1\} \times E_2) = 0 + 0 + 2 \times 1 = 2$.

3. In the last case where $A = W_{\mathbb{F}_{q^2}/\mathbb{F}_q}(E)$ is the $\mathbb{F}_{q^2}/\mathbb{F}_q$-Weil restriction of an elliptic curve E defined over $\mathbb{F}_{q^2}$, then we have already seen in Subsection 4.3.2 that $\#A(\mathbb{F}_q) = \#E(\mathbb{F}_{q^2})$ and that $\mathrm{Tr}(A) = 0$.

   As an ample divisor on A, one can choose for instance $H = E + E^q$ where E^q is the image of E by the generator $\sigma : x \longmapsto x^q$ of the Galois group $\mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q)$. We thus have $H^2 = E^2 + (E^q)^2 + 2E.E^q = 0 + 0 + 2 \times 1 = 2$.

Bibliography

[1] Y. Aubry. « Algebraic geometric codes on surfaces ». Talk at Eurocode'92 - International symposium on coding theory and applications (1992, Udine, Italie), in Ph.D. thesis of the University of Aix-Marseille II, France (1993), hal-00979000. URL: https://hal.archives-ouvertes.fr/hal-00979000/file/EuroCode.1992.pdf (cit. on pp. xvi, 7, 15).

[2] Y. Aubry and M. Perret. « A Weil theorem for singular curves ». In: *Arithmetic, geometry and coding theory (Luminy, 1993)*. de Gruyter, Berlin, 1996, pp. 1–7 (cit. on pp. 19, 20).

[3] Y. Aubry and M. Perret. « Coverings of singular curves over finite fields ». In: *Manuscripta Math.* 88.4 (1995), pp. 467–478. ISSN: 0025-2611. DOI: 10.1007/BF02567835. URL: https://doi.org/10.1007/BF02567835.

[4] Y. Aubry and M. Perret. « On the characteristic polynomials of the Frobenius endomorphism for projective curves over finite fields ». In: *Finite Fields Appl.* 10.3 (2004), pp. 412–431. ISSN: 1071-5797. DOI: 10.1016/j.ffa.2003.09.005. URL: https://doi.org/10.1016/j.ffa.2003.09.005 (cit. on p. 20).

[5] Y. Aubry et al. « Algebraic geometry codes over abelian surfaces containing no absolutely irreducible curves of low genus ». In: *CoRR* abs/1904.08227 (2019). arXiv: 1904.08227. URL: http://arxiv.org/abs/1904.08227 (cit. on pp. xviii, 35).

[6] Y. Aubry et al. « Bounds on the minimum distance of algebraic geometry codes defined over some families of surfaces ». In: *CoRR* abs/1912.07450 (2019). to appear in Contemporary Mathematics, AMS. arXiv: 1912.07450. URL: https://arxiv.org/abs/1912.07450 (cit. on pp. xvii, 17, 23).

[7] E. Barelli et al. « Two-point codes for the generalized GK curve ». In: *IEEE Trans. Inform. Theory* 64.9 (2018), pp. 6268–6276. ISSN: 0018-9448. DOI: 10.1109/TIT.2017.2763165. URL: https://doi.org/10.1109/TIT.2017.2763165 (cit. on p. xvi).

[8] P. Beelen and K. Brander. « Efficient list decoding of a class of algebraic-geometry codes ». In: *Adv. Math. Commun.* 4.4 (2010), pp. 485–518. ISSN: 1930-5346. DOI: 10.3934/amc.2010.4.485. URL: https://doi.org/10.3934/amc.2010.4.485 (cit. on p. xvi).

[9] P. Beelen and T. Høholdt. « The decoding of algebraic geometry codes ». In: *Advances in algebraic geometry codes* 5 (2008), pp. 49–98 (cit. on p. xvi).

[10] R. Blache et al. « Anticanonical codes from del Pezzo surfaces with Picard rank one ». In: *CoRR* abs/1903.09397 (2019). arXiv: 1903.09397. URL: http://arxiv.org/abs/1903.09397 (cit. on pp. xvi, 27).

[11] E. Bombieri and D. B. Mumford. « Enriques' classification of surfaces in char. p, III ». In: *Inventiones Mathematicae* 35.1 (1976), pp. 197–232 (cit. on pp. 24, 30).

[12] A. Couvreur. « Construction of rational surfaces yielding good codes ». In: *Finite Fields Appl.* 17.5 (2011), pp. 424–441. ISSN: 1071-5797. DOI: 10.1016/j.ffa.2011.02.007. URL: https://doi.org/10.1016/j.ffa.2011.02.007 (cit. on p. xvi).

[13] I. M. Duursma. « Algebraic geometry codes: general theory ». In: *Advances in algebraic geometry codes*. World Scientific, 2008, pp. 1–48 (cit. on p. 13).

[14] S. D. Galbraith. « Limitations of constructive Weil descent ». In: *Public-key cryptography and computational number theory (Warsaw, 2000)*. de Gruyter, Berlin, 2001, pp. 59–70 (cit. on p. 42).

[15] S. D. Galbraith and N. P. Smart. « A cryptographic application of Weil descent ». In: *Cryptography and coding (Cirencester, 1999)*. Vol. 1746. Lecture Notes in Comput. Sci. Springer, Berlin, 1999, pp. 191–200. DOI: 10.1007/3-540-46665-7_23. URL: https://doi.org/10.1007/3-540-46665-7_23 (cit. on pp. 41, 42).

[16] V. D. Goppa. « Codes on algebraic curves ». In: *Dokl. Akad. Nauk SSSR* 259.6 (1981), pp. 1289–1290. ISSN: 0002-3264 (cit. on pp. xv, 14).

[17] P. Griffiths and J. Harris. « On the Noether-Lefschetz theorem and some remarks on codimension-two cycles ». In: *Mathematische Annalen* 271.1 (1985), pp. 31–51 (cit. on p. 33).

[18] S. Haloui. « Codes from Jacobian surfaces ». In: *Arithmetic, geometry, cryptography and coding theory*. Vol. 686. Contemp. Math. Amer. Math. Soc., Providence, RI, 2017, pp. 123–135 (cit. on pp. xvi, xviii, 20, 21, 37, 40, 42).

[19] J. P. Hansen. « Toric surfaces and error-correcting codes ». In: *Coding theory, Cryptography and related areas*. Springer, 2000, pp. 132–142 (cit. on p. xvi).

[20] J. P. Hansen and H. Stichtenoth. « Group codes on certain algebraic curves with many rational points ». In: *Appl. Algebra Engrg. Comm. Comput.* 1.1 (1990), pp. 67–77. ISSN: 0938-1279. DOI: 10.1007/BF01810849. URL: https://doi.org/10.1007/BF01810849 (cit. on p. xvi).

[21] S. H. Hansen. « Error-correcting codes from higher-dimensional varieties ». In: *Finite Fields Appl.* 7.4 (2001), pp. 531–552. ISSN: 1071-5797 (cit. on pp. xvi, 7, 13).

[22] R. Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977 (cit. on pp. 1, 4, 7–9, 16, 18, 36).

[23] M. Hindry and J. H. Silverman. *Diophantine geometry*. Vol. 201. Graduate Texts in Mathematics. An introduction. Springer-Verlag, New York, 2000, pp. xiv+558. ISBN: 0-387-98975-7; 0-387-98981-1. DOI: 10.1007/978-1-4612-1210-2. URL: https://doi.org/10.1007/978-1-4612-1210-2 (cit. on pp. 1, 4).

[24] E. W. Howe, E. Nart, and C. Ritzenthaler. « Jacobians in isogeny classes of abelian surfaces over finite fields ». In: *Ann. Inst. Fourier (Grenoble)* 59.1 (2009), pp. 239–289. ISSN: 0373-0956. URL: http://aif.cedram.org/item?id=AIF_2009__59_1_239_0 (cit. on pp. 11, 43).

[25] E. W. Howe et al. « Principally polarizable isogeny classes of abelian surfaces over finite fields ». In: *Math. Res. Lett.* 15.1 (2008), pp. 121–127. ISSN: 1073-2780. DOI: 10.4310/MRL.2008.v15.n1.a11. URL: https://doi.org/10.4310/MRL.2008.v15.n1.a11 (cit. on p. 12).

[26] G. Lachaud. « Number of points of plane sections and linear codes defined on algebraic varieties ». In: *Arithmetic, geometry and coding theory (Luminy, 1993)* (1996), pp. 77–104 (cit. on p. 15).

[27] S. Lang. *Abelian varieties*. Reprint of the 1959 original. Springer-Verlag, New York-Berlin, 1983, pp. xii+256. ISBN: 0-387-90875-7 (cit. on p. 9).

[28] R. Lazarsfeld. *Positivity in algebraic geometry. I.* Vol. 48. A Series of Modern Surveys in Mathematics. Classical setting: line bundles and linear series. Springer-Verlag, Berlin, 2004, pp. xviii+387. ISBN: 3-540-22533-1. DOI: 10.1007/978-3-642-18808-4. URL: https://doi.org/10.1007/978-3-642-18808-4 (cit. on p. 7).

[29] J. H. Lint. *Introduction to coding theory; 2nd ed.* Graduate Texts in Mathematics. Berlin: Springer, 1992. DOI: 10.1007/978-3-662-00174-5. URL: https://cds.cern.ch/record/1618065 (cit. on p. 13).

[30] J. Little and H. Schenck. « Codes from surfaces with small Picard number ». In: *SIAM J. Appl. Algebra Geom.* 2.2 (2018), pp. 242–258. ISSN: 2470-6566. DOI: 10.1137/17M1128277. URL: https://doi.org/10.1137/17M1128277 (cit. on pp. xvi, 7, 19, 27, 28, 32).

[31] J. Little and H. Schenck. « Toric surface codes and Minkowski sums ». In: *SIAM J. Discrete Math.* 20.4 (2006), pp. 999–1014. ISSN: 0895-4801. DOI: 10.1137/050637054. URL: https://doi.org/10.1137/050637054.

[32] J. B. Little. « Algebraic geometry codes from higher dimensional varieties ». In: *Advances in algebraic geometry codes*. Vol. 5. Ser. Coding Theory Cryptol. World Sci. Publ., Hackensack, NJ, 2008, pp. 257–293 (cit. on pp. xvi, 13).

[33] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes. I.* North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977, i–xv and 1–369. ISBN: 0-444-85009-0 (cit. on p. 13).

[34] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes. II.* North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977, i–ix and 370–762. ISBN: 0-444-85010-4 (cit. on p. 13).

[35] R. J. McEliece. « A public-key cryptosystem based on algebraic ». In: *Coding Thv* 4244 (1978), pp. 114–116 (cit. on p. xvi).

[36] J. S. Milne. *Abelian Varieties (v2.00)*. Available at www.jmilne.org/math/. 2008 (cit. on pp. 1, 9, 11).

[37] J. S. Milne. *Algebraic Geometry (v6.02)*. Available at www.jmilne.org/math/. 2017 (cit. on pp. 4, 42).

[38] D. Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London, 1970, pp. viii+242 (cit. on pp. 9, 11, 35, 36).

[39] C. Munuera, A. Sepúlveda, and F. Torres. « Algebraic Geometry codes from Castle curves ». In: *Coding Theory and Applications*. Springer, 2008, pp. 117–127 (cit. on p. xvi).

[40] C. Munuera, A. Sepúlveda, and F. Torres. « Generalized Hermitian codes. » In: *Des. Codes Cryptography* 69.1 (2013), pp. 123–130 (cit. on p. xvi).

[41] C. Munuera, W. Tenório, and F. Torres. « Quantum error-correcting codes from algebraic geometry codes of Castle type ». In: *Quantum Inf. Process.* 15.10 (2016), pp. 4071–4088. ISSN: 1570-0755. DOI: 10.1007/s11128-016-1378-9. URL: https://doi.org/10.1007/s11128-016-1378-9 (cit. on p. xvi).

[42] J. Nardi. « Algebraic geometric codes on minimal Hirzebruch surfaces ». In: *J. Algebra* 535 (2019), pp. 556–597. ISSN: 0021-8693. DOI: 10.1016/j.jalgebra.2019.06.022. URL: https://doi.org/10.1016/j.jalgebra.2019.06.022 (cit. on p. xvi).

[43] J. S. R. Nielsen and P. Beelen. « Sub-quadratic decoding of one-point Hermitian codes ». In: *IEEE Trans. Inform. Theory* 61.6 (2015), pp. 3225–3240. ISSN: 0018-9448. DOI: 10.1109/TIT.2015.2424415. URL: https://doi.org/10.1109/TIT.2015.2424415 (cit. on p. xvi).

[44] F. K. Schmidt. « Analytische Zahlentheorie in Körpern der Charakteristikp ». In: *Mathematische Zeitschrift* 33.1 (1931), pp. 1–32 (cit. on p. 15).

[45] J. Scholten. « Weil restriction of an elliptic curve over a quadratic extension ». Preprint. 2003. URL: https://www.researchgate.net/publication/228946053_Weil_restriction_of_an_elliptic_curve_over_a_quadratic_extension (cit. on p. 44).

[46] J.-P. Serre. « Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini ». In: *C. R. Acad. Sci. Paris Sér. I Math.* 296.9 (1983), pp. 397–402. ISSN: 0249-6291 (cit. on p. 18).

[47] I. R. Shafarevich. *Basic algebraic geometry. 1*. Second. Varieties in projective space, Translated from the 1988 Russian edition and with notes by Miles Reid. Springer-Verlag, Berlin, 1994, pp. xx+303. ISBN: 3-540-54812-2 (cit. on pp. 1, 4, 6, 32).

[48] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics, No. 151. Springer-Verlag, New York-Heidelberg, 1995 (cit. on p. 30).

[49] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics, No. 106. Springer-Verlag, New York-Heidelberg, 1986 (cit. on pp. 1, 2).

[50] H. Stichtenoth. « A note on Hermitian codes over GF(q2) ». In: *IEEE Transactions on Information Theory* 34.5 (1988), pp. 1345–1348 (cit. on p. xvi).

[51] M. A. Tsfasman, S. G. Vlăduţ, and T. Zink. « Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound ». In: *Math. Nachr.* 109 (1982), pp. 21–28. ISSN: 0025-584X. DOI: 10.1002/mana.19821090103. URL: https://doi.org/10.1002/mana.19821090103 (cit. on p. xvi).

[52] M. Tsfasman, S. G. Vlăduţ, and D. Nogin. *Algebraic geometric codes: basic notions*. Vol. 139. Mathematical Surveys and Monographs. American Mathematical Society, Providence, RI, 2007, pp. xx+338. ISBN: 978-0-8218-4306-2. DOI: 10.1090/surv/139. URL: https://doi.org/10.1090/surv/139 (cit. on p. 13).

[53] M. Tsfasman, S. Vlăduţ, and D. Nogin. *Algebraic geometry codes: advanced chapters*. Vol. 238. American Mathematical Soc., 2019 (cit. on p. 13).

[54] S. G. Vlăduţ and Y. I. Manin. « Linear codes and modular curves ». In: *Journal of Soviet Mathematics* 30.6 (1985), pp. 2611–2643. ISSN: 1573-8795. DOI: 10.1007/BF02249124. URL: https://doi.org/10.1007/BF02249124 (cit. on p. 15).

[55] J. F. Voloch and M. Zarzar. « Algebraic geometric codes on surfaces ». In: *Arithmetics, geometry, and coding theory (AGCT 2005)*. Vol. 21. Sémin. Congr. Soc. Math. France, Paris, 2010, pp. 211–216 (cit. on pp. xvi, 7, 27, 28, 32, 36).

[56] W. C. Waterhouse. *Abelian varieties over finite fields*. Thesis (Ph.D.)–Harvard University. ProQuest LLC, Ann Arbor, MI, 1968 (cit. on p. 44).

[57] S. B. Wicker. *Reed-Solomon Codes and Their Applications*. IEEE Press, 1994. ISBN: 078031025X (cit. on p. xv).

[58] C. Xing. « Goppa geometric codes achieving the Gilbert-Varshamov bound ». In: *IEEE transactions on information theory* 51.1 (2005), pp. 259–264.

[59] C. Xing and H. Chen. « Improvements on parameters of one-point AG codes from Hermitian curves ». In: *IEEE Trans. Inform. Theory* 48.2 (2002), pp. 535–537. ISSN: 0018-9448. DOI: 10.1109/18.979330. URL: https://doi.org/10.1109/18.979330 (cit. on p. xvi).

[60] K. Yang and P. V. Kumar. « On the true minimum distance of Hermitian codes ». In: *Coding theory and algebraic geometry*. Springer, 1992, pp. 99–107 (cit. on p. xvi).

[61] M. Zarzar. « Error-correcting codes on low rank surfaces ». In: *Finite Fields Appl.* 13.4 (2007), pp. 727–737. ISSN: 1071-5797. DOI: 10.1016/j.ffa.2007.05.001. URL: https://doi.org/10.1016/j.ffa.2007.05.001 (cit. on pp. xvi, 7, 27, 32).

Glossary of Notations

$\mathbb{A}^n$	affine space of dimension n
$\mathcal{C}(X, G, S)$	evaluation code from a surface X and a divisor G avoiding a set of rational points S
$d(X, S, G)$	minimum distance of the code $\mathcal{C}(X, S, G)$
$\delta(B)$	defect of the curve B
$\deg(D)$	degree of the divisor D
$\mathrm{Div}(X)$	group of divisors of the variety X
$\dim(X)$	dimension of the variety X
$D \sim D'$	linear equivalence of divisors
$D \equiv D'$	numerical equivalence of divisors
$D.D'$	intersection number
D^2	self-intersection number
$\mathbb{F}_q$	finite field with q elements
$f_A(t)$	Weil polynomial of the abelian variety A
(f)	principal divisor associated to a function f
H	ample divisor
k	a field
$k[x_0, \ldots, x_n]$	polynomial ring
$\overline{k}$	algebraic closure of the field k
K	finite extension of k
$[K : k]$	degree of a finite extension
K_X	canonical divisor of the variety X
$k[X]$	coordinate ring of the variety X
$k(X)$	function field of the variety X
$L(D)$	Riemann-Roch space associated to D
$\ell(D)$	dimension of $L(D)$
m	integer part of $2\sqrt{q}$
$\mathrm{NS}(X)$	Néron-Severi group of the variety X
$\mathrm{Num}(X)$	numerical group of the variety X
$\mathbb{P}^n$	projective space of dimension n
P	point on a variety
$p_a(X)$	arithmetic genus of the surface X
π_D	arithmetic genus of D
$\pi : X \to B$	fibered surface
$\mathrm{Pic}(X)$	Picard group of the variety X
$\mathcal{O}_X$	ring of regular functions on the variety X
$\mathcal{O}_{P,X}$	local ring of a point P on the variety X
$s(D)$	superabundance of D
$\mathrm{Supp}(D)$	support of the divisor D
$\mathrm{Tr}(A)$	trace of the abelian variety A
$W_{K/k}(E)$	K/k-Weil restriction of scalars of E

Index