université de BORDEAUX

université de BORDEAUX

THÈSE PRÉSENTÉE

POUR OBTENIR LE GRADE DE

DOCTEUR
DE L'UNIVERSITÉ DE BORDEAUX

ECOLE DOCTORALE MATHÉMATIQUES ET

INFORMATIQUE

MATHÉMATIQUES PURES

Par **Jean GASNIER**

Arithmétique et algorithmique des courbes algébriques et applications aux codes correcteurs et à la cryptographie

Sous la direction de : **Jean-Marc COUVEIGNES**

Soutenue le 10 juillet 2025, devant le jury présidé par : **Alain COUVREUR**

et composé de :

M. Alain COUVREUR	Directeur de Recherche INRIA	INRIA Saclay	Rapporteur
M. Pierrick GAUDRY	Directeur de Recherche CNRS	LORIA	Rapporteur
M. David KOHEL	Professeur des universités	Aix-Marseille Université	Examinateur
Mme Elisa LORENZO-GARCÍA	Maîtresse assistante	Université de Neuchâtel	Examinatrice
M. Jean-Marc COUVEIGNES	Professeur des universités	Université de Bordeaux	Directeur

Arithmétique et algorithmique des courbes algébriques et applications aux codes correcteurs et à la cryptographie

Résumé : L'arithmétique et l'algorithmique élémentaires des courbes algébriques est au cœur de contributions majeures à la théorie des codes correcteurs d'erreurs et à la cryptologie. Ce travail de thèse mobilise des notions plus avancées, provenant de la théorie du corps de classes, de la théorie de Riemann–Roch équivariante, et de la géométrie arithmétique des jacobiennes, pour établir un cadre général adapté à ces constructions et en améliorer l'efficacité.

On étudie notamment les propriétés de codes linéaires munis d'une structure de module sur l'algèbre d'un groupe fini G. On étudie plus spécifiquement les codes munis d'une structure de sous-module libre d'un module libre, et leur dualité. En particulier, on montre que ces codes peuvent être représentés par des matrices de contrôle à coefficients dans l'algèbre du groupe G. Dans le cas où G est commutatif, la transformée de Fourier rapide confère de bonnes propriétés algorithmiques à ces codes correcteurs. On montre aussi comment construire ces codes à l'aide de revêtements abéliens non ramifiés de courbes projectives lisses, et l'on donne les premiers exemples de codes correcteurs excellents encodables en temps quasi-linéaire et décodables en temps quasi-quadratique.

Une autre application concerne la construction de familles de courbes elliptiques à couplages, exploitées dans certains protocoles cryptographiques. La théorie de la multiplication complexe permet de réduire le problème géométrique sous-jacent à un problème d'arithmétique cyclotomique. On déduit de l'étude de ce problème une méthode unifiée de construction de familles de courbes elliptiques à couplages.
Mots-clés : Codes correcteurs, Cryptographie, Courbes algébriques, Géométrie Arithmétique, Théorie du corps de classes, Corps finis

---

Arithmetics and algorithmics of algebraic curves and applications to coding theory and cryptography

Abstract: The elementary arithmetics and algorithmics of algebraic curves is at the heart of major contributions to coding theory and cryptology. This PhD thesis draws on more advanced concepts, from class field theory, equivariant Riemann-Roch theory and the arithmetic geometry of jacobian varieties, to establish a general framework adapted to these constructions and improve their efficiency.

In particular, we study the properties of linear codes endowed with a module structure over the algebra of a finite group G. We study more specifically the codes endowed with a structure of free submodule of a free module, and their duality. Specifically, we show that these codes can be described by parity check matrices whose coefficients belong to the algebra of the group G. When G is commutative, the fast Fourier transform provides nice algorithmic properties to these error-correcting codes. We also show how to build these codes, using unramified abelian coverings of smooth projective curves, and we give the first examples of excellent codes encodable in quasi-linear time and decodable in quasi-quadratic time.

Another application involves the generation of families of pairing-friendly elliptic curves, used in some cryptographic protocols. The complex multiplication theory allows to reduce the underlying geometric problem to a problem of cyclotomic arithmetics. We deduce from the study of this problem an unified method of generation of families of pairing-friendly elliptic curves.
Keywords: Coding theory, Cryptography, Algebraic curves, Arithmetic Geometry, Class field theory, Finite fields

---

Unité de recherche
UMR 5251, Université de Bordeaux, Bordeaux INP, CNRS, INRIA, 33400 Talence, France.

Contents

Notation

General notation

We denote by :

$[a..b]$	for two integers $a \leqslant b$, the set of integers between a and b.
ν_p	for a prime p, the p-adic valuation over the integers.
$\mathbb{N}$	the set of non-negative integers.
$\mathbb{F}_p$	for a prime p, the finite field with p elements.
$\mathbb{P}^1$	the projective line.
$\mathbb{H}$	the upper half-plane.
$\mathrm{Re}(z)$	for a complex number z, the real part of z.
$O(f(n))$	the set of function g s.t. there exists $B \in \mathbb{R}$ such that $g(n) \underset{n\to\infty}{\leqslant} Bf(n)$.
$\lfloor . \rfloor$	the floor function.
$\lceil . \rfloor$	an application rounding to the closest integer.
I_n	for an integer $n > 0$, the identity matrix of size n.
M^t	for a matrix M, the transpose of M.

Algebraic curves

In the following:

- K denotes a finite field.
- L denotes an algebraic extension of K.
- X denotes a smooth projective curve geometrically integral over K.
- Y denotes a smooth projective curve geometrically integral over K, together with a covering $\tau : Y \longrightarrow X$.

We denote by:

X_L	the curve over L canonically associated to X.
$L(X)$	the function field of X_L.
$X(L)$	the places of $L(X)$ of degree 1, i.e. the L-rational points of X_L.
$\mathrm{Irr}(X)$	the set of places of $K(X)$.

$\mathrm{Irr}^d(X)$	for an integer $d > 0$, the set of places of $K(X)$ of degree d.
ν_P	for a place P of $K(X)$, the valuation of $K(X)$ associated to P.
$\mathcal{O}_P$	for a place P of $K(X)$, the valuation ring of ν_P.
K_P	for a place P of $K(X)$, the residue field at P.
$\mathrm{Div}(X)$	the divisor group of X.
$\mathrm{supp}\, D$	for $D \in \mathrm{Div}(X)$, the set of places P s.t. $\nu_P(D) \neq 0$.
$\deg D$	for $D \in \mathrm{Div}(X)$, the degree of D.
(f)	for a rational function $f \in K(X)$, the divisor of f.
$f(P)$	for $P \in X(K)$ and a function $f \in K(X)$ regular at P, the evaluation of f at P.
$\mathrm{Princ}(X)$	the subgroup of principal divisors of X.
$\mathrm{Eff}(X)$	the set of effective divisors of X.
$\mathcal{O}_X$	the sheaf of regular functions of X.
$\mathcal{O}_X(D)$	for $D \in \mathrm{Div}(X)$, the sheaf of functions of X associated to D.
Γ_X	the functor of of global sections on X.
$\Omega(X/K)$	the set of differentials of X (relatively to K).
df	for $f \in K(X)$, the differential associated to f.
$\mathrm{div}\, \omega$	for $\omega \in \Omega(X/K)$, the divisor of ω.
$\mathrm{Res}_P(\omega)$	for $p \in X(K)$ and $\omega \in \Omega(X/K)$ s.t. $\nu_P(\omega) \geqslant -1$, the residue of ω at P.
$\Omega_{X/K}(D)$	for $D \in \mathrm{Div}(X)$, the sheaf of differentials associated to D.
$D \sim D'$	for $D, D' \in \mathrm{Div}(X)$, this denotes that D and D' are equivalent.
$\mathrm{Pic}(X)$	the Picard group of X.
$\mathrm{Pic}^d(X)$	for $d \in \mathbb{Z}$, the subset of classes of $\mathrm{Pic}(X)$ of degree d.
$\mathcal{J}_X$	the Jacobian of X.
$\mathcal{J}_X(K)$	the K-rational points of $\mathcal{J}_X$.
$\mathcal{J}_X[n]$	for $n \in \mathbb{Z}$, the n-torsion $\mathcal{J}_X$.
$\mathcal{J}_X[n](K)$	for $n \in \mathbb{Z}$, the K-rational n-torsion points of $\mathcal{J}_X$.
$D(Q/P)$	for $P \in \mathrm{Irr}(X)$ and $Q \in \mathrm{Irr}(Y)$ above P, the decomposition group of Q.
$I(Q/P)$	for $P \in \mathrm{Irr}(X)$ and $Q \in \mathrm{Irr}(Y)$ above P, the inertia group of Q.

Number fields

In the following:

- $\mathcal{K}$ denotes a number field.
- $\mathcal{L}$ denotes a finite extension of $\mathcal{K}$.

We denote by:

$\mathbb{Z}_\mathcal{K}$	the integer ring of $\mathcal{K}$.
$\nu_\mathfrak{p}$	for a prime ideal $\mathfrak{p}$ of $\mathbb{Z}_\mathcal{K}$, the $\mathfrak{p}$-adic valuation.
$\mathcal{K}_\mathfrak{p}$	for a prime ideal $\mathfrak{p}$ of $\mathbb{Z}_\mathcal{K}$, the residue field at $\mathfrak{p}$.
$D(\mathfrak{P}/\mathfrak{p})$	for prime ideals $\mathfrak{p}$ and $\mathfrak{P}$ of $\mathcal{K}$ and $\mathcal{L}$, the decomposition group of $\mathfrak{P}$.
$I(\mathfrak{P}/\mathfrak{p})$	for prime ideals $\mathfrak{p}$ and $\mathfrak{P}$ of $\mathcal{K}$ and $\mathcal{L}$, the inertia group of $\mathfrak{P}$.

$I(\mathcal{K})$	the group of non-zero fractional ideals of $\mathbb{Z}_{\mathcal{K}}$.
$P(\mathcal{K})$	the group of principal non-zero fractional ideals of $\mathbb{Z}_{\mathcal{K}}$.
$\mathrm{Cl}(\mathcal{K})$	the class group of $\mathcal{K}$.
$\mathrm{cl}(\mathcal{K})$	the class number of $\mathcal{K}$.
$\mathrm{Hil}(\mathcal{K})$	the Hilbert class field of $\mathcal{K}$.

Chapter 1

Introduction

Since the early 1980s, contributions from algebraic geometry to cryptography and error-correcting codes have grown significantly. On the one hand, Goppa defined error-correcting codes by studying the evaluation morphism of functions of a linear space associated with a divisor of an algebraic curve. These codes generalize the famous Reed-Solomon codes and have excellent properties. On the other hand, following the attack on the Discrete Logarithm Problem (abbreviated to DLP) on finite fields by algorithms based on *index calculus*, the cryptography community began to design and study protocols whose security relies on the DLP on elliptic curves. Later, in the 2000s, a branch of this theory studied protocols using pairings. These protocols require special elliptic curves, known as *pairing-friendly curves*, and a section of the literature on this subject develops methods for constructing these curves. In this thesis, we study a new construction of Goppa codes benefiting from an additional structure, as well as a general method for generating families of pairing-friendly curves. These contributions fall within the scope of algorithmic arithmetic and geometry, and notably involves the class field theory of number fields and function fields.

Goppa codes

Let K be a finite field with q elements, and let n be an integer. A linear code of length n is a vector subspace of a K-vector space of dimension n endowed with a distance, for instance K^n endowed with the Hamming distance

$$d : K^n \times K^n \longrightarrow \mathbb{N}$$

which associates with every pair of vectors in K^n the number of non-zero coordinates of their difference. The elements of this vector subspace are called codewords.

A classic problem consists in determining the closest codeword to a given element of the ambient vector space (or one of the closest words, if there are several). It is common to restrict oneself to solving this problem only for elements at distance at most t from a codeword, where t is a positive integer. Let d be the minimum distance between two codewords. If $t < d/2$, every element of K^n has at most one codeword at distance less than

t. In this case, solving the problem amounts to giving, if it exists, the unique codeword in the ball of radius t centered on the element in question. This problem is called the *decoding problem*.

For a fixed dimension, the minimum distance determines the correction capacity t of the code. Singleton's bound is an upper bound for the minimum distance d at given length n and dimension k:

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

Codes that reach this bound are called MDS codes. Few MDS codes are known, and the most famous ones are Reed-Solomon codes. These codes are defined as vectors of K^n (equipped with the Hamming distance) whose components are the evaluations of a polynomial of degree at most $k - 1$ at n distinct fixed elements of K. One drawback of Reed-Solomon codes is their length, which is limited to q by definition.

Goppa geometric codes, also known as AG codes, are a generalization of Reed–Solomon codes. Let X be a smooth projective curve over K of genus g. Let $P_1, \ldots, P_n$ be pairwise distinct points of X, and let D be a divisor on X disjoint from $P = P_1 + \cdots + P_n$. The geometric Goppa code associated with D and P is the vector subspace of K^n (equipped with the Hamming distance) consisting of vectors whose components are the values of a function of the linear space associated with D at $(P_i)_{i\in[1..n]}$.

Goppa codes are not MDS codes in general, but their length n, dimension k and minimum distance d satisfy the relation

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

because a rational function cannot vanish at more points than its degree. The work of Ihara, Tsfasman, Vladut, and Zink has shown that under some conditions on K (e.g., the order of K is a square), there exist curves with a sufficiently large number of points n such that the defect associated with their genus g is not detrimental.

Contributions to Goppa codes

In the 1990s, decoding algorithms for Goppa codes generalizing the decoding algorithms for Reed-Solomon codes were developed. It has been shown that it is possible to decode these codes for $t < d/2$ in $O(n^3)$ operations in K. It should be noted that the general problem of decoding any linear code is an NP-hard problem, and that the best known probabilistic algorithms for decoding random linear codes have exponential complexity in the weight of the error. Thus, the structure derived from the algebraic geometry of Goppa codes also makes them efficient from an algorithmic point of view. Furthermore, as with all linear codes, it is possible to encode these codes, i.e. to compute an element of the code given its coordinates in a basis, in $O(n^2)$ operations in K.

However, from an application standpoint, Goppa codes are still considered too inefficient, compared to Reed-Solomon codes for example. One of the research goals on these codes is therefore to find more efficient encoding and decoding algorithms.

In this thesis, we define a subfamily of Goppa codes, for which we show that the algorithmic performance is improved. These codes are defined on an unramified abelian cover Y over another curve X, with covering map:

$$\tau : Y \longrightarrow X.$$

Let G be the Galois group of τ. Let D be a divisor on X and E its pullback on Y. Let $P_1, \ldots, P_n$ be K-rational points on X that are totally split in Y, and let Q be the set of points in the fibers above $P_1, \ldots, P_n$. The divisor E is stable under the action of G, so G acts on the functions in $L(E)$. Furthermore, G acts on the fibers of τ and therefore acts on Q. Finally, the evaluation of the functions of $L(E)$ at Q is compatible with the action of G. We can then view the Goppa code associated with Q and E as a $K[G]$-module. Moreover, under the usual assumptions, we can show that it is a free $K[G]$-module, which means that the action of G is very relevant in the description of the code.

Using this structure of free $K[G]$-module, we can define generator and parity-check matrices for these Goppa codes whose coefficients are elements of $K[G]$. It is possible to use the fast Fourier transform (FFT) to quickly compute multiplications in $K[G]$. When the order of G is very large compared to n, the complexity of the encoding and decoding algorithms is reduced. More precisely, it can be shown that in this favorable case, these codes can be encoded in quasi-linear time with respect to their length, and decoded in quasi-quadratic time.

It can also be shown that, under some conditions on K that are more restrictive than for classical Goppa codes, these codes are asymptotically excellent. More precisely, it is possible to find a family of unramified abelian covers with Galois groups of sufficiently fast growing order so that the encoding and decoding algorithms have quasi-linear and quasi-quadratic complexities, and which have enough K-rational points to exceed the Gilbert-Varshamov bound.

This construction is the first construction of Goppa codes that has both good asymptotic properties and a quasi-linear encoding algorithm. For comparison, in [NW19], the authors construct a family of asymptotically good Goppa codes, whose encoding has subquadratic complexity in the length of the code. In [BRS21], the authors show that Goppa codes derived from C_{ab} curves can be encoded in quasi-linear time. However, as with Reed-Solomon codes, these codes have a bounded length $n \leqslant q^2$ and cannot be considered asymptotically good.

This work resulted in the article "Explicit Riemann-Roch spaces in the Hilbert class field", which was accepted for publication in the conference proceedings of AGC2T 2023.

Pairing-based cryptography

Let K be a finite field, and let E/K be an elliptic curve. The curve E is naturally isomorphic to its Jacobian, and therefore has an algebraic group structure. The K-rational points of E, denoted by $E(K)$, form a finite abelian group with at most 2 invariant factors. Let G be a cyclic subgroup of $E(K)$. We can use G to instantiate cryptographic protocols whose security relies on the DLP, such as the Diffie-Hellman key exchange. The main advantage of

using elliptic curves to instantiate DLP-based protocols is that, apart from certain special cases, no known algorithm is more efficient than generic methods (those based exclusively on group operations) for solving the discrete logarithm in the group G.

Let n_E be the number of K-rational points of E, and r the largest prime factor of the order of G. We know that using the Pohlig-Hellman algorithm and the Baby-Step Giant-Step algorithm, it is possible to compute a discrete logarithm in $O(\sqrt{r})$ operations in G. Thus, to maximize the security of cryptographic protocols over G, it is preferable to choose as E an elliptic curve such that n_E has a large prime factor r, and to take G as the subgroup of order r of $E(K)$ (unique because $r > \sqrt{n_E}$). We also require that r be coprime to the characteristic of K.

It is possible to define pairings on elliptic curves, i.e., bilinear group morphisms that take two points on the curve as input and associate them with a nonzero element in a finite extension of K. For example, the Weil pairing

$$e_r : E[r] \times E[r] \longrightarrow \mu_r$$

takes as input two r-torsion points of the curve and returns an r-th root of unity. Since the early 2000s, several articles have used pairings to define new security protocols, such as Joux's tripartite key exchange [Jou00]. For these protocols to be effective, the degree k of the extension K_r of K defined by the r-th roots of unity must be as small as possible. However, it is extremely rare for k to be significantly smaller than r (in general, $\log\ k \approx \log\ r$). Curves whose *embedding degree* k is small enough for the pairing to be computable in practice are called *pairing-friendly curves*. It is commonly considered that $k \leqslant 54$ is required for a curve to be a pairing-friendly curve.

On the other hand, Menezes, Okamoto, and Vanstone showed that, using pairings, one was able to reduce the DLP in G (i.e., on the elliptic curve) to the DLP in K_r^*. However, the DLP in K_r^* is solved in sub-exponential time by algorithms based on index calculus. Therefore, in order to guarantee a sufficient level of security, k must be large enough so that computing a discrete logarithm in K_r^* requires at least as many operations as calculating a discrete logarithm in G.

These conflicting requirements between security and efficiency have led to the development of methods for producing pairing-friendly curves with predefined parameters (e.g., k), so that these parameters can then be optimized in order to determine which curves are both secure and most efficient for each pairing-based protocol.

Contribution to pairing-based cryptography

Let $k > 1$ be a fixed integer. The problem of generating pairing-friendly curves consists in finding K a finite field of order q and E/K an elliptic curve with a subgroup of K-rational points of order r coprime to the characteristic of K, such that the degree of the extension K_r/K is k. In order to guarantee the difficulty of the DLP, we require that $r > 2^{2s}$, where s is an integer denoting the desired level of security. For algorithmic reasons, we also ask

that $\log\ q < 2 \log\ r$. In this thesis, we will only consider ordinary pairing-friendly curves. Let t be the trace of the curve E, then $\mathrm{pgcd}(t, q) = 1$.

The usual way to solve this problem is to find integers q, t and r that satisfy the conditions necessary for the existence of such a curve. For example, if q is a prime power, if $\mathrm{pgcd}(t, q) = 1$ and if $|t| \leqslant 2\sqrt{q}$, we know that there exists an ordinary elliptic curve of trace t over a field with q elements. By adding further conditions regarding r and k, we obtain a set of necessary and sufficient conditions for the existence of a solution to the problem under consideration. Furthermore, if q is prime, Atkin and Morain's complex multiplication method [AM93] allows us to obtain the j-invariant of the solution curve when the discriminant of the curve is not too large.

In many cases, we are actually looking for families of pairing-friendly curves whose embedding degree is k. Usually, we look for a family $(E_i)_{i\in\mathbb{N}}$ parameterized by polynomials with rational coefficients Q, R and T, i.e., such that there exist integers $(x_i)_{i\in\mathbb{N}}$ such that for all $i \in \mathbb{N}$, the curve E_i is defined over a finite field with $Q(x_i)$ elements, with trace $T(x_i)$, and has a subgroup of rational points of order $R(x_i)$, relative to which its embedding degree is k. Naturally, for this to be possible, the polynomials Q, R and T must satisfy arithmetic conditions similar to those previously imposed on the integers q, r and t. To find families of pairing-friendly curves, we seek to find triples of polynomials satisfying these conditions.

To check the quality of such a family, we generally use the ρ-value

$$\rho = \frac{\deg Q}{\deg R}.$$

The closer ρ is to 1, the more efficient the arithmetic of the curves in the family will be.

This thesis presents a new method for generating such polynomials. This method follows the approach of Kachisa, Schaeffer, and Scott [KSS08], who noticed that the polynomial R can be viewed as the minimal polynomial of an element of a well-chosen number field. They use an exhaustive search over these algebraic numbers to generate parameterized families of curves. The new method generalizes and refines this approach by identifying algebraic numbers producing families whose ρ-value is nicely upper bounded.

The selection and use of these polynomials requires solving an algorithmic problem: given a polynomial with integer coefficients P, a prime number p, and a positive integer $n > 1$, solve for a variable $x \in \mathbb{Z}$

$$P(x) \equiv 0 \bmod p^n.$$

Hensel's lemma allows us to solve this type of equation when P has simple roots modulo p, by lifting the solutions modulo p to solutions modulo p^n. Surprisingly, it is difficult to find a solution to this problem in the literature when P has a multiple root modulo p. We therefore detail an algorithm that solves this problem in the general case.

We show that the new method produces families with a smaller ρ-value for the case $k = 22$ (and $k = 46$), and produces alternatives to already known families for several values of k. Furthermore, our approach uniformizes several of the most successful previous results. This explains why so many families produced by different methods have ρ-values following

a unified formula. This work resulted in the article «An Algebraic Point of View on the Generation of Pairing-Friendly Curves », co-authored with Aurore Guillevic, published in the SIAGA journal [GG25].

Thesis organisation

In **chapter** 2, we define the concepts and notation relating to algebraic curves and function fields that we will use in the rest of the thesis. We also discuss the algorithmic representation of these objects. More precisely, we draw up a list of conditions that must be satisfied for an algorithmic representation to be considered satisfactory. Finally, we show that by making these algorithmic assumptions, it is possible to draw uniformly at random from the rational subgroup of the Jacobian, to compute its structure as an abelian group, and to compute the Weil pairing.

In **chapter** 3, we recall some results from the class field theory of number fields and function fields. We also present some effective aspects of this theory for imaginary quadratic fields, and the application of the theory to the construction of curves with many rational points. In particular, we present new curves with a record number of points.

In **chapter** 4, after a brief recall on linear codes and Goppa codes, we present a new construction of geometric codes with a $K[G]$-module structure. We study the arithmetic of $K[G]$, for G an abelian group, and in particular an algorithm using the FFT to quickly compute products in $K[G]$, whose complexity is explicitely given. We then study linear codes with a free $K[G]$-module structure, where G is a finite group that is not necessarily abelian. These codes are special cases of quasi-G codes. In particular, we present some duality results in this context. We show that these codes can be described by linear algebra over $K[G]$, similarly to linear codes. Finally, we show that some Goppa codes, based over a Galois cover with Galois group G and with covering map

$$\tau : Y \longrightarrow X,$$

possess a $K[G]$-module structure. In the case where G is abelian and the covering τ is unramified, we give sufficient conditions on the divisors defining the code for the associated linear spaces (of functions and differentials) to be free $K[G]$-modules. We study the encoding, decoding, and asymptotic properties of these codes.

In **chapter** 5, we review some principles of curve-based cryptography, and briefly introduce pairing-based cryptography. We detail classical methods for generating pairing-friendly curves and families of pairing-friendly curves. In particular, we detail the method of Kachisa, Schaefer and Scott. Then, we present the new method for generating families of curves, implemented in Sagemath [The22] in [Gas23]. We explain its principle, then present the achieved results. In particular, we present a new family of curves obtained for the embedding degree $k = 22$. Finally, we present a general algorithm that solves equations of the form

$$P(x) \equiv 0 \bmod p^n$$

where P is a polynomial with integer coefficients, p is a prime number, $n > 1$ is an integer, and x is a variable with integer values. We explain its usefulness for the search for polynomials parameterizing families of pairing-friendly curves.

Chapter 6 contains the appendix to this thesis. It presents tables of results and proofs of some propositions used in this document, which are not central to the topic of the thesis.

Chapter 2

Function Fields and Jacobians

Smooth projective curves and their Jacobians are the fundamental objects of interest in this document. In particular, we are interested in their algorithmic aspects. In this chapter, in Section 2.1, we present specifications for the algorithmic representation of the function fields of curves and other associated objects, consisting of a list of operations that we must be able to perform in a reasonable amount of time to meet our needs in the following chapters. In Section 2.2, we examine the algorithmic representation of the Jacobian and present algorithms using elementary operations that we will define, which will be useful for the applications discussed in the following chapters.

We start by making a few definitions. Let K be a perfect field. We call any affine scheme associated to a finite-type reduced K-algebra an affine variety over K. We an call any scheme over K that can be covered by a finite number of affine subvarieties over K an algebraic variety over K. Note that this definition implies that every algebraic variety over K is (geometrically) reduced. We call any variety over K that is geometrically irreducible and of dimension 1 an algebraic curve over K. In particular, in this thesis, every algebraic curve over K is assumed to be geometrically integral.

Although several concepts discussed in this chapter are well defined for any perfect field K, we will be primarily interested in the case of finite fields. For this reason, it is necessary to clarify our assumptions regarding the algorithmic representation of finite fields. We essentially ask for two things: first, guarantees on the size of the representation of elements of the field, and on the complexity of arithmetic operations in the field, and second, the possibility of efficiently evaluating morphisms between finite fields. The second constraint is of interest in our geometric context because it often happens that solving certain algorithmic problems requires extending the base field or applying the Frobenius morphism.

Let us assume for a moment that K is a finite field with $q = p^m$ elements. If $m = 1$, then there exists a canonical model of K in the form of $\mathbb{Z}/p\mathbb{Z}$, i.e., the integers modulo p. In this case, we can refer to the unique field with p elements $\mathbb{F}_p$. If $m > 1$, there is no canonical model of the field with q elements, nor is there a canonical morphism between the different models. In [LdS13] and [Lü23], we find proposals for consistent standard models for finite fields and their morphisms. We will not go that far in normalization. We will represent the elements of K by their $\mathbb{F}_p$-coordinates in a fixed basis. In this model, we

make minimal assumptions about complexity: the addition of two elements is performed in $O(\log\ q)$ elementary operations; multiplication is performed at the cost of $O(m^2)$ additions and multiplications in $\mathbb{F}_p$; a morphism between two finite fields is described by its matrix in the chosen bases. It is also possible to draw uniformly at random an element of the field.

2.1 Algorithmic representation of function fields

We assume that the reader is familiar with several concepts of algebraic geometry. For an introduction to function fields, the reader may refer to the first chapter of [Sti08]. The reader may refer to the first chapter of [Har77] for a more general introduction to algebraic geometry. I also recommend the first chapters of [Liu02] for a deeper introduction to algebraic geometry.

Let K be a perfect field. There is a equivalence of category between the category of smooth projective curves over K (with dominant morphisms) and the category of function fields of transcendence degree 1 over K in which K is algebraically closed (with morphisms of K-algebras) [Liu02, Section 7, Proposition 3.13]. This means that many geometric problems regarding smooth projective curves over K can be addressed by studying these function fields.

2.1.1 Valuation rings and places

For the sake of brevity, we will adopt the following definition:

Definition 1. Let K be a perfect field. Let $K(x)$ be the field of rational fractions in one indeterminate over K. A **field of functions** over K is a finite extension of $K(x)$ in which K is algebraically closed.

Let X be a smooth projective curve over K, then $K(X)$, the field of rational functions of X, is a function field over K. In particular, the function field of $\mathbb{P}^1$ is isomorphic to the field of rational fractions in one indeterminate $K(x)$. Conversely, any function field over K is isomorphic to the field of rational functions of a smooth projective curve X over K. This curve X is unique up to isomorphism. We will therefore allow ourselves to write $K(X)$ to denote a function field over K.

Definition 2. Let $K(X)$ be a function field over K. Let

$$\nu : K(X) \longrightarrow \mathbb{Z} \cup \{\infty\}.$$

We say that ν is a **discrete valuation** of $K(X)$ if:

- $\nu(f) = \infty$ if and only if $f = 0$.
- $\nu(fg) = \nu(f) + \nu(g)$ for all $f, g \in K(X)$.
- $\nu(f + g) \geqslant \min(\nu(f), \nu(g))$ for all $f, g \in K(X)$.

- There exists $t \in K(X)$ such that $\nu(t) = 1$.
- $\nu(f) = 0$ for all constants $f \in K$.

Definition 3. Let $K(X)$ be a function field over K, and ν be a discrete valuation of $K(X)$.

- The set $P = \{f \in K(X) \mid \nu(f) > 0\}$ is called the **place** associated with ν.
- We call the ring $\mathcal{O}_P = \{f \in K(X) \mid \nu(f) \geqslant 0\}$ the **valuation ring** of ν. The place P is the unique maximal ideal of $\mathcal{O}_P$.
- An element $t \in P$ such that $\nu(t) = 1$ is called a **uniformizer** at P.

We call any place associated with a discrete valuation of $K(X)$ a place of $K(X)$. If P is a place of $K(X)$, we denote by ν_P the discrete valuation associated with P. We denote by $\mathrm{Irr}(X)$ the set of places of $K(X)$.

The notion of place corresponds to the notion of closed point of X. Let $\mathcal{O}_X$ be the sheaf of regular functions on X, then $\mathcal{O}_P$ is the set of germs at P of the sheaf $\mathcal{O}_X$. Let Γ_X be the functor of global sections on X. The quotient

$$K_P := \mathcal{O}_P/P = \Gamma_X(\mathcal{O}_X/\mathcal{O}_X(-P))$$

is the **residue field** at P. The **degree** of P, denoted by $\deg P$, is the degree of K_P over K. We denote by $\mathrm{Irr}^d(X)$ the set of places of degree d of $K(X)$. We denote by

$$X(K) := \mathrm{Irr}^1(X)$$

the set of places of degree 1 of X (or equivalently the set of K-rational points of X).

Let L be an algebraic extension of K. We naturally associate with X a smooth projective curve over L, denoted by X_L. We denote by $L(X)$ the field of functions (over L) of X_L. We have the following equality:

$$L(X) = L \otimes_K K(X).$$

We denote by

$$X(L) := \mathrm{Irr}^1(X_L)$$

as the set of places of degree 1 of $L(X)$ (or, equivalently, the set of L-rational points of X_L).

Suppose that K is a finite field with $q = p^m$ elements. From an algorithmic point of view, we will need to represent the functions in $K(X)$ and the places of $K(X)$ in a way that allows us to perform the following tasks:

1. Given $\alpha \in K$ and $f \in K(X)$, compute αf.
2. Given f_1 and f_2 two functions of $K(X)$, compute $f_1 + f_2$, $f_1 f_2$ and f_1/f_2 if $f_2 \neq 0$.
3. Given an integer $d > 0$, compute $\mathrm{Irr}^d(X)$.

4. Given P a place of $K(X)$, compute its degree.
5. Given a point P of $K(X)$, choose a uniformizer at P.
6. Given a place P of $K(X)$ and a function $f \in K(X)$, compute the multiplicity $\nu_P(f)$ of the zero of f at P.
7. Given a place P of $K(X)$ and a function $f \in \mathcal{O}_P$, evaluate f at P.
8. Given L a finite extension of K and $f \in K(X)$, compute the image of f in $L(X)$.
9. Given L a finite extension of K and P a place of $K(X)$, give the set of places of $L(X)$ above P.
10. Given L a finite extension of K and Q a place of $L(X)$, give the place P of $K(X)$ below Q.
11. Given L a finite extension of K, Q a place of $L(X)$, and $f \in L(X)$ a function, compute the place $F_K(Q)$ and the function $F_K(f)$ where $F_K : L(X) \longrightarrow L(X)$ is the Frobenius endomorphism relative to K.

In particular, requirement 5, requirement 6, and requirement 7 allow the calculation of the Laurent series expansion of f at P.

2.1.2 Divisors

Let K be a perfect field. Let X be a smooth projective curve over K and $K(X)$ its function field.

Definition 4. We define the **divisor group** of X, denoted by $\mathrm{Div}(X)$, as the free abelian group generated by the places of $K(X)$.

Definition 5. Let ν_P be a discrete valuation of $K(X)$, and let $D = \sum_Q n_Q Q$ be a divisor of X. We define

$$\nu_P(D) = n_P.$$

We call

$$\operatorname{supp} D = \{Q \in \mathrm{Irr}(X) \mid \nu_Q(D) \neq 0\}$$

the support of D.

Definition 6. Let $D = \sum_P n_P P$ be a divisor of X. We call

$$\deg D = \sum_P n_P \deg P$$

the **degree** of D.

Definition 7. Let $f \in K(X)^*$, we define the divisor of f as

$$(f) \;=\; \sum_P \nu_P(f)P.$$

Recall that there are only a finite number of places P such that $\nu_P(f) \neq 0$. A divisor is said to be **principal** if it is the divisor of a rational function. We denote by $\mathrm{Princ}(X)$ the subgroup of principal divisors of X.

Definition 8. Let $D = \sum_P n_P P$ be a divisor of X. We say that D is **effective** if n_P is positive for every place P, and we write $D \geqslant 0$. We denote by $\mathrm{Eff}(X)$ the set of effective divisors of X.

Remark 1. Let $f \in K(X)^*$. There exist two effective divisors $D_f^+, D_f^- \in \mathrm{Eff}(X)$ with disjoint supports such that

$$(f) = D_f^+ - D_f^-.$$

We say that the **degree** of f is $\deg(D_f^+)$.

Definition 9. Let D be a divisor of X. We call the Riemann-Roch space associated with D, or simply the linear space (of functions) associated with D, the vector space $\Gamma_X(\mathcal{O}_X(D))$ consisting of the zero function and rational functions on X satisfying

$$(f) + D \geqslant 0.$$

Assume for a moment that K is a finite field. We will use the natural algorithmic representation for divisors, i.e., the representation as a finite collection of pairs (n_P, P) where P is a place of $K(X)$ and n_P is the associated multiplicity. In particular, given a divisor, we can give its support and its valuation at each point of $K(X)$. We can also determine whether two divisors are equal.

We also expect to be able to perform the following operations:

1. Compute the divisor of a nonzero rational function.
2. Given D a divisor of X, compute the dimension k of $\Gamma_X(\mathcal{O}_X(D))$ and a basis $f_1, \ldots, f_k \in K(X)$ of $\Gamma_X(\mathcal{O}_X(D))$.

According to the Riemann-Roch theorem, it is possible to calculate the genus g of X by computing the dimension of a Riemann-Roch space of sufficiently large degree.

2.1.3 Differentials

Let K be a perfect field. Let X be a smooth projective curve over K. In this section, we define the differential space of X relative to K. We will use the Kähler definition, which is equivalent to the Weil definition in our setting [Sti08, Section 4.3].

Definition 10. Let E be a $K(X)$-vector space. A **K-derivation** of X in E is a K-linear map

$$\delta : K(X) \longrightarrow E$$

such that:

$$\forall f, g \in K(X),\ \delta(fg) = f\delta(g) + g\delta(f).$$

We denote by $\mathrm{Der}_K(K(X), E)$ the space of K-derivations from $K(X)$ to E.

Definition 11. There exists a K-derivation $d : K(X) \longrightarrow \Omega(X/K)$ satisfying the following universal property: for any $K(X)$-vector space E,

$$\begin{array}{ccc} \mathrm{Hom}_{K(X)}(\Omega(X/K), E) & \longrightarrow & \mathrm{Der}_K(K(X), E) \\ u & \longmapsto & u \circ d \end{array}$$

is an isomorphism of $K(X)$-vector spaces.

The space $\Omega(X/K)$ is called the **differential space** of X (relative to K), and is unique up to isomorphism. It is a $K(X)$-vector space of dimension 1.

Definition 12. Let $\omega \in \Omega(X/K) \setminus \{0\}$, let P be a point of $K(X)$, and let t be a uniformizer at P. Let $f \in K(X)$ be the unique function such that $\omega = f dt$. We define

$$\nu_P(\omega) = \nu_P(f).$$

We define the divisor of the differential ω as

$$\operatorname{div} \omega = \sum_P \nu_P(\omega) P.$$

Let D be a divisor of X. We call the differential space of X (relative to K) associated with D the space $\Gamma_X(\Omega_{X/K}(D))$ consisting of the zero differential and the differentials ω satisfying

$$\operatorname{div} \omega \geqslant D.$$

We denote by $\Gamma_X(\Omega_{X/K})$ the space of holomorphic differentials of X (whose divisor is effective).

Assume that K is a finite field. We require an algorithmic representation of the differentials of $\Omega(X/K)$ that allows us to perform the following operations:

1. Given $\omega \in \Omega(X/K)$ non-zero, compute the divisor of ω.
2. Given a function $f \in K(X)$, compute the differential df.
3. Given a divisor D of X, compute a basis for $\Gamma_X(\Omega_{X/K}(D))$.
4. Given a function $f \in K(X)$ and a differential $\omega \in \Omega(X/K)$, compute the differential $f\omega$.
5. Given two differentials $\omega_1, \omega_2 \in \Omega(X/K)$, compute the function $f = \omega_1/\omega_2$ and the differential $\omega_1 + \omega_2$.

Conditions 2 and 5 allow us to calculate the Laurent series expansion of a differential ω at a point P and, in particular, its residue at P.

2.1.4 Picard group

Let K be a perfect field. Let X be a smooth projective curve over K.

Definition 13. Two divisors D and D' of X are said to be **equivalent**, and we write

$$D \sim D'$$

if $D - D'$ is principal.

Definition 14. We define the **Picard group** of X as

$$\mathrm{Pic}(X) = \mathrm{Div}(X)/\,\mathrm{Princ}(X).$$

For all $d \in \mathbb{Z}$, we denote by $\mathrm{Pic}^d(X)$ the subset of $\mathrm{Pic}(X)$ consisting of classes of degree d. The set $\mathrm{Pic}^0(X)$ is a subgroup of $\mathrm{Pic}(X)$.

Assume that K is a finite field. The algorithmic representation of the classes of $\mathrm{Pic}(X)$ must allow the group operations to be computed:

1. Given D a divisor of X, compute the class c of D in $\mathrm{Pic}(X)$.
2. Given c a class in $\mathrm{Pic}(X)$, give a divisor D in the class c.
3. Given c and c' two classes in $\mathrm{Pic}(X)$, determine whether $c = c'$.
4. Given c and c' two classes in $\mathrm{Pic}(X)$, compute $c + c'$.
5. Given c a class in $\mathrm{Pic}(X)$, compute $-c$.

Remark 2. It is sometimes useful to have canonical representatives of the elements of the Picard group (see, for example, subsection 2.2.3). Indeed, an element of the Picard group can have several different representatives (algorithmically speaking). A canonical representative of $c \in \mathrm{Pic}(X)$ is a particular representative in the set of representatives of c that can be computed from any given representative of c. With our assumptions on the algorithmic representation of the Picard group, it is always possible to construct such representatives. If the curve X has a K-rational point P, it is possible to produce one as follows.

Let $c \in \mathrm{Pic}(X)$. By subtracting (or adding) P sufficiently many times, we can assume that $c \in \mathrm{Pic}^0(X)$. Let g be the genus of X, and let D be a divisor of class c. According to the Riemann-Roch theorem, the space $\Gamma_X(\mathcal{O}_X(D + gP))$ is nonzero. We can show that there exists a unique nonzero function f (up to a constant in K) from $\Gamma_X(\mathcal{O}_X(D + gP))$ whose valuation at P is maximal. Then $D + (f)$ is a canonical representative of c.

2.1.5 Zeta function

In this paragraph, we restrict ourselves to the case where K is a finite field with $q = p^m$ elements. Let X be a smooth projective curve over K, let $r \geqslant 1$ and let L be an extension of K of degree r. Let

$$N_r = \#X(L).$$

Definition 15. Let α_n be the number of effective divisors of X (over K) of degree n. We call

$$Z_X = \exp\left(\sum_{r\geqslant 1} \frac{N_r}{r} x^r\right) = \sum_{n\geqslant 0} \alpha_n x^n \in \mathbb{Z}[[x]]$$

the **zeta function** of X. We call

$$L_X = (1-x)(1-qx)Z_X \in \mathbb{Z}[x]$$

the **L-polynomial** of X.

Recall that the L-polynomial of X is a polynomial with integer coefficients of degree $2g$, where g is the genus of X. Its coefficients $\ell_0, \ldots, \ell_{2g}$ satisfy, for all $i \leqslant g$,

$$\ell_{2g-i} = q^{g-i}\ell_i.$$

Finally, it is known that $\ell_0 = 1$. We can therefore represent L_X algorithmically by the g coefficients $\ell_1, \ldots, \ell_g$. It is possible to determine the coefficients of the L-polynomial of X from the values N_r for $1 \leqslant r \leqslant g$ [Sti08, Section 5.1].

Computing the L-polynomial of the function field X is a complicated problem, and current algorithms for calculating it are not effective in all situations. The first category, generalizing the algorithms of Schoof [Sch85] and Pila [Pil90], are polynomial in $\log q = m \log p$ when the genus g is small, but their complexities depend exponentially on the genus. The second category, algorithms generalizing the algorithms of Satoh [Sat00] and Kedlaya [Ked01], have polynomial complexities in m, p, and g and are efficient for small characteristics.

2.2 Algorithmics of Jacobians

In this section, we present some algorithms using the elementary operations described in Section 2.1 that will be useful in the following chapters.

Let K be a finite field with $q = p^m$ elements. Let $\bar{K}$ be an algebraic closure of K. Let X be a smooth projective curve over K of genus g.

The Jacobian $\mathcal{J}_X$ of X is an abelian variety of dimension g. It can be shown that for any finite extension L of K,

$$\mathcal{J}_X(L) \simeq \mathrm{Pic}^0(X_L), \tag{2.2.1}$$

where X_L denotes the smooth projective curve over L naturally associated with the curve X. Furthermore, the isomorphism in equation (2.2.1) is functorial with respect to L. Thus, we will use the algorithmic representation of $\mathrm{Pic}^0(X_L)$ to represent $\mathcal{J}_X(L)$.

Assume that there exists $P \in X(K)$. We can then define

$$j_P : X \longrightarrow \mathcal{J}_X$$

the Jacobi map associated with P. This is a closed immersion of X into its Jacobian, induced by the map

$$\begin{array}{ccc} \mathrm{Div}(X) & \longrightarrow & \mathrm{Pic}^0(X) \\ \sum_Q n_Q Q & \longmapsto & \sum_Q n_Q (Q - \deg(Q) P) \end{array}.$$

2.2.1 Weil pairing

Definition 16. We use the notation from the beginning of Section 2.2. Let n be an integer not divisible by p. Assume that the n-torsion of the Jacobian $\mathcal{J}_X$ is K-rational, and that K contains the n-th roots of unity (in fact, Weil's pairing allows us to show that this second assumption is redundant). Let a and b be two K-rational classes of n-torsion of the Jacobian $(a, b) \in \mathcal{J}_X[n](K) \times \mathcal{J}_X[n](K)$. Let D_a be a divisor representing a and D_b a divisor representing b disjoint from D_a. Let f_a be a function of $K(X)$ with divisor nD_a and f_b a function with divisor nD_b. Let:

$$e_n(a, b) = \frac{f_b(D_a)}{f_a(D_b)}.$$

It is understood here that

$$f(D) = \prod_{P \in \mathrm{Irr}(X)} \left(\mathrm{Norm}_K^{K_P} f(P)\right)^{\nu_P(D)} = \prod_{P \in \mathrm{Irr}(X)} \prod_{\substack{Q \in \mathrm{Irr}(X/\bar{K}) \\ Q|P}} f(Q)^{\nu_P(D)} \tag{2.2.2}$$

for $f \in K(X)$ and $D \in \mathrm{Div}(X)$, a divisor disjoint from the support of f. Note that f_a and f_b depend on the choice of D_a and D_b, but not $e_n(a, b)$. Similarly, f_a and f_b are defined up to a constant, but according to equation (2.2.2), since D_a and D_b are of degree 0, the values $f(D_a)$ and $f(D_b)$ do not depend on this constant. Finally, according to Weil's reciprocity law, we have

$$\left(\frac{f_b(D_a)}{f_a(D_b)}\right)^n = \frac{f_b(nD_a)}{f_a(nD_b)} = 1.$$

This defines the Weil pairing

$$e_n : \mathcal{J}_X[n](K) \times \mathcal{J}_X[n](K) \longrightarrow \mu_n(K)$$

where $\mu_n(K)$ is the group of n-th roots of unity in K.

This definition of Weil pairing requires that the representatives D_a and D_b be disjoint. In the case where D_a and D_b are not disjoint, it is possible to find a divisor equivalent to D_b disjoint from D_a. Let D_0 be a divisor of degree $2g$ disjoint from D_a (over finite fields, such a divisor always exists). So, according to the Riemann-Roch theorem, $\Gamma_X(\mathcal{O}_X(D_0 + D_b))$ is a K-vector space of dimension $g + 1$ because

$$\deg(D_0 + D_b) = 2g \geqslant 2g - 1.$$

Let $f \in \Gamma_X(\mathcal{O}_X(D_0 + D_b))$, then the divisor $(f) + D_0 + D_b$ is effective. Thus, if $(f) + D_0 + D_b$ and D_a are not disjoint, there exists $P \in \operatorname{supp} D_a$ such that $f \in \Gamma_X(\mathcal{O}_X(D_0 + D_b - P))$. For any point $P \in \operatorname{supp} D_a$, the subspace $\Gamma_X(\mathcal{O}_X(D_0 + D_b - P))$ has dimension at most g and is therefore contained in a hyperplane of $\Gamma_X(\mathcal{O}_X(D_0 + D_b))$. Thus, the functions $f \in \Gamma_X(\mathcal{O}_X(D_0 + D_b))$ such that $(f) + D_0 + D_b$ is not disjoint from D_a belong to a union of at most $\#\operatorname{supp} D_a$ hyperplanes. If $\#\operatorname{supp} D_a < q$, we can use the algorithm in [ECdJ+11, Lemma 13.1.8] to compute a function $f \in \Gamma_X(\mathcal{O}_X(D_0 + D_b))$ such that

$$(f) + D_0 + D_b \text{ is disjoint from } D_a.$$

Then $(f) + D_b$ is a divisor equivalent to D_b disjoint from D_a.

If $\#\operatorname{supp} D_a \geqslant q$, the idea is to extend the base field and apply a similar technique. The reader may refer to [ECdJ+11, Lemma 13.1.9].

Let D_a^+ and D_a^- be two disjoint effective divisors such that $D_a = D_a^+ - D_a^-$, then the degree of the function f_a is $n \deg D_a^+$. It is therefore expected that the complexity of computing the Weil pairing depends polynomially on n and $\deg D_a^+$. However, Miller's algorithm (see [MOV93, Appendix] or [ECdJ+11, Section 13.3]) allows the Weil pairing to be evaluated with polynomial complexity in $\log n$ and $\deg D_a^+$.

2.2.2 Drawing uniformly at random in the Picard group

We use the notation from the beginning of Section 2.2. We seek to draw uniformly at random an element of degree 0 of the Picard group of X. This can be accomplished using the method described in [Bru13, Sections 3.2-6]. It is important to note that this method requires knowledge of the L-polynomial of X.

Draw of a place

Let $d > 0$ be an integer. We start by attempting to draw a place of degree d uniformly at random in $\operatorname{Irr}^d(X)$. A procedure is detailed in algorithm 2.2.1.

The algorithm 2.2.1 relies on two key points. First, it is easy to randomly draw an element from a Riemann-Roch space uniformly, since these are finite-dimensional vector spaces. Second, returning the result with probability $\#\operatorname{Irr}^d(D)/\lfloor \deg D_0/d \rfloor$ ensures that the probability of returning P does not depend on D.

Remark 3. In the following, it will be necessary to draw formal sums of places of common degree d, or equivalently sets with repetition (unordered). Drawing such a sum uniformly

Algorithme 2.2.1 : Random draw of a place of degree d

Entrées : $K(X)$ a function field over K, $d > 0$ an integer such that $\mathrm{Irr}^d(X)$ is nonempty

Output : $P \in \mathrm{Irr}^d(X)$ taken uniformly

1 Let D_0 be an effective divisor satisfying $\deg D_0 - d \geqslant 2g$.

2 Choose uniformly $f \in \Gamma_X(\mathcal{O}_X(D_0))$. Let $D = (f)$ be its divisor.

3 Compute $\#\mathrm{Irr}^d(D)$ the number of places of degree d present in D (counted with multiplicity).

4 With probability $\#\mathrm{Irr}^d(D)/\lfloor \deg D_0/d \rfloor$, return a uniformly chosen place $P \in \mathrm{Irr}^d(D)$. Come back to step 1.

at random is a little more complicated than drawing places one after the other with the algorithm 2.2.1, because sums with repetitions would not occur with the same probability as sums without repetitions. We will use a result from [Bru13, Algorithm 3.4]: there exists a generic algorithm which, given a set E of known finite cardinality, an integer ℓ, and an algorithm for uniform random draw in E (of a single element), returns a set with repetition of cardinality ℓ of elements of E, drawn uniformly at random.

One needs to ensure that the integer d given as input to the algorithm satisfies the condition $\mathrm{Irr}^d(X) \neq \emptyset$, otherwise the algorithm will not terminate. It is possible to compute the value of $\#\mathrm{Irr}^d(X)$ using L_X, the L-polynomial of X [Bru13, Section 3].

Draw of an effective divisor

The uniform random draw of an effective divisor of degree d is done in two steps: first, the number of places of each degree (less than d) that appear in the sum is randomly drawn, then the places are randomly drawn using the algorithm 2.2.1.

Let r and d be two positive integers. An r-smooth decomposition type of degree d is a sequence of integers $(\ell_1, \ell_2, \ldots)$ such that $\sum_{i=1}^{r} \ell_i i = d$ and such that for all $i > r$, the integer ℓ_i is zero. In particular, to every effective divisor D of degree d, we can associate a d-smooth decomposition type of degree d, where ℓ_i is the number of places of degree i appearing in D (counted with multiplicity). We say that D is *r-smooth* if its decomposition type is, i.e. if D is supported by places of degree at most r. We denote by

$$\mathrm{Eff}^d_{\leqslant r}(X) = \{D \in \mathrm{Eff}(X) \mid \deg D = d \text{ and } D \text{ is } r\text{-smooth}\}$$

the set of effective r-smooth divisors of degree d of X, and for any integer ℓ we denote

$$\mathrm{Eff}^{\ell r}_{=r}(X) = \{D \in \mathrm{Eff}(X) \mid D \text{ is composed of } \ell \text{ places of degree } r\}$$

the set of effective divisors of degree ℓr composed solely of places of degree r. It is possible to recursively compute the values $\#\,\mathrm{Eff}^d_{\leqslant r}(X)$ for all d and r from the number of places of each degree less than r [Bru13, Section 3.3].

The uniform distribution on r-smooth divisors of degree d induces a probability distribution on the types of decomposition. If $r \geqslant 2$, we can express the marginal distribution associated with the r-th coordinate by:

$$\mathbb{P}(\ell_r = \ell) = \frac{\#\operatorname{Eff}^{\ell r}_{=r}(X) \cdot \#\operatorname{Eff}^{d-\ell r}_{\leqslant r-1}(X)}{\#\operatorname{Eff}^{d}_{\leqslant r}(X)},\ 0 \leqslant \ell \leqslant \lfloor d/r \rfloor \tag{2.2.3}$$

This gives us the recursive algorithm 2.2.2, which uses the fact that any r-smooth divisor of degree d is the sum of an $(r-1)$-smooth divisor of degree $d - \ell r$ and ℓ places of degree r, for a certain integer ℓ.

Algorithme 2.2.2 : Random draw of an r-smooth decomposition type of degree d
Entrées : (d, r) two positive integers
Output : $(\ell_1, \ldots, \ell_r, 0, \ldots)$ a uniformly chosen r-smooth decomposition type of degree d

1 If $r = 1$, return $(d, 0, \ldots)$. Otherwise, randomly select ℓ_r according to the probability distribution 2.2.3. Call the algorithm recursively with parameters $(d - \ell_r r, r - 1)$ to obtain a decomposition type $(\ell_1, \ldots, \ell_{r-1}, 0, \ldots)$. Return $(\ell_1, \ldots, \ell_r, 0, \ldots)$.

We combine the previous algorithms to obtain algorithm 2.2.3, which randomly selects a uniformly chosen effective divisor of fixed degree.

Algorithme 2.2.3 : Random draw an effective divisor of degree d
Entrées : $d > 0$ an integer, $K(X)$ a function field
Output : D a uniformly chosen effective divisor of degree d

1 Randomly draw a decomposition type $(\ell_1, \ldots, \ell_d, 0, \ldots)$, d-smooth of degree d using algorithm 2.2.2.
2 For $i = 1, \ldots, d$, randomly draw ℓ_i places of degree i as specified in Remark 3.
3 Return the sum of the places.

Draw of a divisor class

To draw a class uniformly at random in $\operatorname{Pic}^0(X)$, we can use the algorithm 2.2.3 to randomly draw an effective divisor of a given degree. All we need to know is a surjective map from $\operatorname{Eff}^d(X)$ to $\operatorname{Pic}^0(X)$ whose fibers have the same cardinality, for a certain degree d.

Let D_0 be an effective divisor of degree $d_0 \geqslant 2g - 1$. Then the map

$$D \in \operatorname{Eff}^{d_0}(X) \longmapsto [D - D_0] \in \operatorname{Pic}^0(X)$$

is surjective, and its fibers have the same cardinality. Indeed, let $c \in \operatorname{Pic}^0(X)$ be a class of degree 0. Let $\tilde{D}$ be a divisor in the class c. Then $\tilde{D} + D_0$ is of degree $d_0 \geqslant 2g - 1$, so $\Gamma_X(\mathcal{O}_X(\tilde{D}+D_0))$ is of dimension $d_0 - g + 1$ and for any nonzero function $f \in \Gamma_X(\mathcal{O}_X(\tilde{D}+D_0))$,

$$D := (f) + \tilde{D} + D_0 \geqslant 0 \text{ and } D - D_0 \sim \tilde{D}.$$

Furthermore, the fiber above c is in bijection with the set of vector lines of $\Gamma_X(\mathcal{O}_X(\tilde{D}+D_0))$, whose cardinality does not depend on c. We summarize these remarks in Algorithm 2.2.4.

Algorithme 2.2.4 : Random draw in the Picard group
Entrées : $K(X)$ a function field
Output : c a uniformly drawn class of $\mathrm{Pic}^0(X)$
1 Choose an effective divisor D_0 of degree $d_0 \geqslant 2g-1$
2 Randomly draw an effective divisor D of degree d_0 using algorithm 2.2.3.
3 Return the class of $D - D_0$

2.2.3 Strcuture of the Jacobian

We use the notation from the beginning of Section 2.2. Recall that K is a finite field. Let $P_\infty \in X(K)$. We will see below that class field theory gives a correspondence between the isomorphism classes of unramified abelian covers of X totally split above P_∞, and, the subgroups of $\mathcal{J}_X(K)$. We therefore wish to be able to determine the subgroups of $\mathcal{J}_X(K) \simeq \mathrm{Pic}^0(X)$, and to do so we present techniques for computing the abelian group structure of $\mathrm{Pic}^0(X)$.

Computing the group structure requires being able to compute a set of generators of $\mathrm{Pic}^0(X)$. Let ℓ be a prime integer, and $k > 0$ a positive integer. It is known that $\mathcal{J}_X[\ell^k](\bar{K})$ is a finite abelian group with at most $2g$ invariant factors. We deduce that $\mathcal{J}_X[\ell^k](K)$ is also a finite abelian group with at most $2g$ invariant factors. This implies that $\mathcal{J}_X(K)$ also has at most $2g$ invariant factors. Assume that L_X is known. We can uniformly sample $2g+2+n$ classes from $\mathrm{Pic}^0(X)$ using the algorithm 2.2.4 to obtain a generating family with probability greater than $1-1/2^n$ (see Section 6.2 of the Appendix).

Let us generalize the problem to the computation of the structure of any abelian group G. We briefly present the Buchmann–Schmidt algorithm [BS05]. Given n elements generating an abelian group G, this algorithm computes elements $\gamma_1, \ldots, \gamma_r \in G$ of respective orders $d_1 | \cdots | d_r$ generating G, by computing a basis B of the lattice of relations of the n generators of G, in Smith normal form. The diagonal of B is $(d_1, \ldots, d_r, 1, \ldots, 1)$, and

$$G = \langle \gamma_1 \rangle \times \cdots \times \langle \gamma_r \rangle \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}.$$

The Buchman–Schmidt algorithm is an extension of Shanks' discrete logarithm algorithm (see [Coh93, Section 5.4.1]), also known as the Baby-Step Giant-Step algorithm, and requires performing $O(n\sqrt{|G|})$ group operations in G and $O(n\sqrt{G}\log(G))$ comparisons of elements of G, and storing $O(\sqrt{|G|})$ elements of G.

Remark 4. It should be noted that in order to limit the number of comparisons in this way, it is necessary to be able to order the elements of G. If we have canonical representatives of elements of G, we can easily order them (for example, in lexicographical order).

Chapter 3

Effective class field theory

The object of (global) class field theory is the characterization of abelian extensions of number fields and function fields (over finite fields). These two types of fields share many characteristics, and consequently the results of class field theory can be expressed in a similar way in both situations. Several versions of this theory have been written, using different objects to express and prove its results. We will use the version employing the language of ideals for the study of number fields, as this is the simplest to adapt from an algorithmic point of view. For function fields, we will use the presentations by Rosen [Ros87] and Serre [Ser84].

In this chapter, we begin by briefly introducing the class field theory of number fields in Section 3.1. We present some applications and algorithmic methods derived from this theory in Section 3.2. In Section 3.3, we present the class field theory of function fields from two points of view, and briefly discuss the connection between these two presentations. Finally, we present an application of class field theory to the construction of algebraic curves with many rational points in Section 3.4. In particular, we present new curves with record numbers of rational points. The concepts and methods presented in this chapter will be used in chapters 4 and 5.

3.1 Class field theory in number fields

The aim of this section is to present the main objects of the class field theory of number fields and to summarize some of its results. For a more detailed exposition of the theory, the reader may refer to the following works [AT09, Jan96, Neu86, Lan94]. This section is inspired by [Coh00, Chapter 3].

The goal of class field theory is to describe the abelian extensions of a number field $\mathcal{K}$ (or, more generally, of a global field) using the arithmetic of $\mathcal{K}$. The starting point of the theory is the work of Hilbert and Furtwängler on unramified abelian extensions. Let $\mathcal{K}$ be a number field. The set of isomorphism classes of unramified abelian extensions of $\mathcal{K}$ has a maximum, in the sense that there exists an unramified abelian extension of $\mathcal{K}$ denoted $\mathrm{Hil}(\mathcal{K})$ such that every unramified abelian extension $\mathcal{L}$ of $\mathcal{K}$ is isomorphic to a sub-extension of $\mathrm{Hil}(\mathcal{K})$.

We call $\mathrm{Hil}(\mathcal{K})$ the Hilbert class field of $\mathcal{K}$. The degree of the extension $[\mathrm{Hil}(\mathcal{K}) : \mathcal{K}] = \mathrm{cl}(\mathcal{K})$ is the class number of $\mathcal{K}$, and the Galois group $\mathbf{Gal}(\mathrm{Hil}(\mathcal{K})/\mathcal{K})$ is canonically isomorphic to the class group $\mathrm{Cl}(\mathcal{K})$ of $\mathcal{K}$. Thus, Galois theory allows us to identify the subgroups of $\mathrm{Cl}(\mathcal{K})$ and the isomorphism classes of unramified abelian extensions of $\mathcal{K}$. Finally, the Hilbert class field has a second important property: let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}_{\mathcal{K}}$, and let f be the order of $\mathfrak{p}$ in the class group of $\mathcal{K}$. Then f is also the degree of inertia of $\mathfrak{p}$ in the extension $\mathrm{Hil}(\mathcal{K})/\mathcal{K}$.

We will see below that it is possible to generalize the notions of class group and class field to parameterize abelian extensions (ramified or not). Let $\mathcal{L}$ be an abelian extension of $\mathcal{K}$. The first step is to define objects that describe the ramification of $\mathcal{L}$.

Definition 17.

1. A modulus $\mathfrak{m}$ is a pair $(\mathfrak{m}_0, \mathfrak{m}_\infty)$ where $\mathfrak{m}_0$ is an ideal of $\mathbb{Z}_{\mathcal{K}}$ and $\mathfrak{m}_\infty$ is a set of real embeddings of $\mathcal{K}$ into $\mathbb{C}$.

2. If $\mathfrak{m} = (\mathfrak{m}_0, \mathfrak{m}_\infty)$ and $\mathfrak{n} = (\mathfrak{n}_0, \mathfrak{n}_\infty)$ are two moduli, we say that $\mathfrak{n}$ divides $\mathfrak{m}$ if $\mathfrak{n}_0 \mid \mathfrak{m}_0$ and $\mathfrak{n}_\infty \subset \mathfrak{m}_\infty$. We then write $\mathfrak{n} \mid \mathfrak{m}$.

3. If $\mathfrak{a}$ is a nonzero fractional ideal of $\mathbb{Z}_{\mathcal{K}}$, we say that $\mathfrak{a}$ is coprime to $\mathfrak{m}$ if $\mathfrak{a}$ is coprime to $\mathfrak{m}_0$, that is, there exist two ideals $\mathfrak{b}$ and $\mathfrak{c}$ coprime to $\mathfrak{m}_0$ such that $\mathfrak{a} = \mathfrak{b}/\mathfrak{c}$.

4. We say that $\alpha \in \mathcal{K}^*$ is coprime to $\mathfrak{m}$ if $\alpha\mathbb{Z}_{\mathcal{K}}$ is.

5. Let $\alpha \in \mathcal{K}^*$, we say that
$$\alpha = 1 \bmod {}^*\mathfrak{m}$$
if for every prime ideal $\mathfrak{p}$ dividing $\mathfrak{m}_0$, $\nu_{\mathfrak{p}}(\alpha - 1) \geqslant \nu_{\mathfrak{p}}(\mathfrak{m}_0)$ and for every $\sigma \in \mathfrak{m}_\infty$, $\sigma(\alpha) > 0$.

6. Let $\alpha, \beta \in \mathcal{K}^*$, we say that $\alpha = \beta \bmod {}^*\mathfrak{m}$ if α and β are coprime to $\mathfrak{m}$ and $\alpha/\beta = 1 \bmod {}^*\mathfrak{m}$.

The object that allows us to quantify the ramification of $\mathcal{L}$, and that will be useful later on, is a modulus called the conductor of $\mathcal{L}$ over $\mathcal{K}$. In order to define it, we recall the notion of local norm. Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}_{\mathcal{K}}$, and let $\mathcal{K}_{\mathfrak{p}}$ be the completion of $\mathcal{K}$ at $\mathfrak{p}$. Let $\mathfrak{P}$ be a prime ideal of $\mathbb{Z}_{\mathcal{L}}$ above $\mathfrak{p}$. We say that $\alpha \in \mathcal{K}_{\mathfrak{p}}^*$ is a local norm modulo $\mathfrak{p}$ if $\nu_{\mathfrak{p}}(\alpha) \geqslant 0$ and if there exists $\beta \in (\mathcal{L}_{\mathfrak{P}})^*$ such that $\alpha = \mathrm{Norm}_{\mathcal{K}_{\mathfrak{p}}}^{\mathcal{L}_{\mathfrak{P}}}(\beta)$.

Let $k_{\mathfrak{p}}$ be the smallest non-negative integer such that all elements $\alpha \in \mathcal{K}^*$ coprime to $\mathfrak{p}$ satisfying $\alpha = 1 \bmod {}^*\mathfrak{p}^{k_{\mathfrak{p}}}$ are local norms modulo $\mathfrak{p}$. It can be shown that $k_{\mathfrak{p}}$ exists, and that $k_{\mathfrak{p}} = 0$ if and only if $\mathfrak{p}$ is unramified in $\mathcal{L}/\mathcal{K}$ [Coh00, Sect 3.4.1].

Definition 18. We use the notation defined in the previous paragraph. Let
$$\mathfrak{c}_0 = \prod_{\mathfrak{p}} \mathfrak{p}^{k_{\mathfrak{p}}}$$

be an ideal of $\mathbb{Z}_\mathcal{K}$ (the product has a finite number of non-trivial factors). Let $\mathfrak{c}_\infty$ be the (finite) set of real embeddings of $\mathcal{K}$ in $\mathbb{C}$ associated with the real places of $\mathcal{K}$ that are ramified in $\mathcal{L}/\mathcal{K}$. Then we define the **conductor** of $\mathcal{L}/\mathcal{K}$ as the modulus

$$\mathfrak{c}_{\mathcal{L}/\mathcal{K}} = (\mathfrak{c}_0, \mathfrak{c}_\infty).$$

Remark 5. The conductor $\mathfrak{c}_{\mathcal{L}/\mathcal{K}}$ is supported by all the ramified places in $\mathcal{L}/\mathcal{K}$, and only those places.

If $\mathcal{L}_1$ and $\mathcal{L}_2$ are two abelian extensions of $\mathcal{K}$, such that $\mathcal{L}_1$ is isomorphic to a sub-extension of $\mathcal{L}_2$, then $\mathfrak{c}_{\mathcal{L}_1/\mathcal{K}} \mid \mathfrak{c}_{\mathcal{L}_2/\mathcal{K}}$. This motivates the following definition:

Definition 19. Let $\mathcal{K}$ be a number field, and let $\mathcal{L}$ be an abelian extension of $\mathcal{K}$. A modulus $\mathfrak{m}$ is said to be appropriate for the extension $\mathcal{L}/\mathcal{K}$ if $\mathfrak{c}_{\mathcal{L}/\mathcal{K}}$ divides $\mathfrak{m}$.

Next, we define the concept that will generalize the group of classes.

Definition 20. Using the previous notation,

1. We define
$$(\mathbb{Z}_\mathcal{K}/\mathfrak{m})^\times = (\mathbb{Z}_\mathcal{K}/\mathfrak{m}_0)^\times \times \mathbb{F}_2^{\mathfrak{m}_\infty}.$$
2. We denote by $I_\mathfrak{m}(\mathcal{K})$ the group of non-zero fractional ideals of $\mathbb{Z}_\mathcal{K}$ coprime to $\mathfrak{m}$.
3. We denote by $P_\mathfrak{m}(\mathcal{K})$ the group of principal non-zero fractional ideals of $\mathbb{Z}_\mathcal{K}$ generated by an element $\alpha \in \mathcal{K}^*$ such that $\alpha = 1 \bmod {}^*\mathfrak{m}$.
4. The group $P_\mathfrak{m}(\mathcal{K})$ is a subgroup of $I_\mathfrak{m}(\mathcal{K})$. We define the group of ray classes (modulo $\mathfrak{m}$) of $\mathcal{K}$ as the quotient
$$\mathrm{Cl}_\mathfrak{m}(\mathcal{K}) = I_\mathfrak{m}(\mathcal{K})/P_\mathfrak{m}(\mathcal{K}).$$

Remark 6. The group $(\mathbb{Z}_\mathcal{K}/\mathfrak{m})^\times$ will not be used in the rest of the presentation, but it must be defined because it is used in the algorithm for calculating the ray class groups $\mathrm{Cl}_\mathfrak{m}(\mathcal{K})$ (see [Coh00]) .

Example 1. Let $\mathbf{1} = (\mathfrak{m}_0, \mathfrak{m}_\infty)$ be the modulus such that:

- $\mathfrak{m}_0 = \mathbb{Z}_\mathcal{K}$.
- $\mathfrak{m}_\infty = \emptyset$.

Then we see that $I_\mathfrak{m}(\mathcal{K})$ is the group of non-zero fractional ideals of $\mathbb{Z}_\mathcal{K}$, that $P_\mathfrak{m}(\mathcal{K})$ is the group of principal non-zero ideals in $I_\mathfrak{m}(\mathcal{K})$, and that $\mathrm{Cl}_\mathfrak{m}(\mathcal{K}) = \mathrm{Cl}(\mathcal{K})$.

We also see that for any abelian unramified extension $\mathcal{L}'$ of $\mathcal{K}$, the conductor of $\mathcal{L}'/\mathcal{K}$ is $\mathbf{1}$. The class field is therefore the maximal extension of $\mathcal{K}$ whose conductor is $\mathbf{1}$.

This example shows that the definitions generalize the concepts known for the Hilbert class field. It also indicates how the Hilbert class field is generalized (see Theorem 3).

Let $\mathfrak{p}$ be a prime of $\mathbb{Z}_\mathcal{K}$ and $\mathfrak{P}$ a prime of $\mathbb{Z}_\mathcal{L}$ above $\mathfrak{p}$. We denote

$$D(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in \mathbf{Gal}(\mathcal{L}/\mathcal{K}) \mid \mathfrak{P}^\sigma = \mathfrak{P}\}$$

the decomposition group of $\mathfrak{P}$. We then have a canonical, surjective group morphism from $D(\mathfrak{P}/\mathfrak{p})$ to the Galois group $\mathbf{Gal}((\mathbb{Z}_\mathcal{L}/\mathfrak{P})/(\mathbb{Z}_\mathcal{K}/\mathfrak{p}))$, whose kernel is the inertia group $I(\mathfrak{P}/\mathfrak{p})$ of $\mathfrak{P}$.

The Galois group $\mathbf{Gal}((\mathbb{Z}_\mathcal{L}/\mathfrak{P})/(\mathbb{Z}_\mathcal{K}/\mathfrak{p}))$ is cyclic, generated by the Frobenius map:

$$\alpha \longmapsto \alpha^{\mathrm{Norm}_\mathbb{Q}^\mathcal{K}(\mathfrak{p})}.$$

If $\mathfrak{p}$ is unramified, then $I(\mathfrak{P}/\mathfrak{p})$ is trivial, and the map

$$D(\mathfrak{P}/\mathfrak{p}) \longrightarrow \mathbf{Gal}((\mathbb{Z}_\mathcal{L}/\mathfrak{P})/(\mathbb{Z}_\mathcal{K}/\mathfrak{p}))$$

is an isomorphism. There then exists a unique element $\mathfrak{s}_\mathfrak{P} \in D(\mathfrak{P}/\mathfrak{p})$ that is sent to the Frobenius morphism. Furthermore, since $\mathbf{Gal}(\mathcal{L}/\mathcal{K})$ is abelian, $D(\mathfrak{P}/\mathfrak{p})$ does not depend on the choice of $\mathfrak{P}$, so we can define $\mathfrak{s}_\mathfrak{p} = \mathfrak{s}_\mathfrak{P}$.

Let $\mathfrak{m}$ be an appropriate modulus for the extension $\mathcal{L}/\mathcal{K}$. In particular, all primes of $\mathcal{K}$ that ramify in $\mathcal{L}$ divide $\mathfrak{m}$. We can therefore define a map from $I_\mathfrak{m}(\mathcal{K})$ to $\mathbf{Gal}(\mathcal{L}/\mathcal{K})$ using the map from the previous paragraph.

Definition 21. Let $\mathfrak{a} = \prod \mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{a})} \in I_\mathfrak{m}(\mathcal{K})$. We define:

$$(\mathfrak{a}, \mathcal{L}/\mathcal{K}) = \prod_{\mathfrak{p}|\mathfrak{a}} \mathfrak{s}_\mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{a})}.$$

We call $(\cdot, \mathcal{L}/\mathcal{K})$ the Artin map, or the Artin symbol.

It is now possible to state the main theorems of class field theory.

Theorem 1 (Artin reciprocity law [Coh00, Theorems 3.4.3 and 3.4.5])**.** *Let $\mathcal{K}$ be a number field, $\mathcal{L}$ an abelian extension of $\mathcal{K}$, and $\mathfrak{m} = (\mathfrak{m}_0, \mathfrak{m}_\infty)$ an appropriate modulus to the extension $\mathcal{L}/\mathcal{K}$. Then:*

1. *The Artin map is a surjective group morphism from $I_\mathfrak{m}(\mathcal{K})$ to $\mathbf{Gal}(\mathcal{L}/\mathcal{K})$.*
2. *The kernel of the Artin map $A_\mathfrak{m}(\mathcal{L}/\mathcal{K})$ contains $P_\mathfrak{m}(\mathcal{K})$. More precisely,*

$$A_\mathfrak{m}(\mathcal{L}/\mathcal{K}) = P_\mathfrak{m}(\mathcal{K})\,\mathrm{Norm}_\mathcal{K}^\mathcal{L}(I_{\mathfrak{m}_0\mathbb{Z}_\mathcal{L}}(\mathcal{L}))$$

where $\mathfrak{m}_0\mathbb{Z}_\mathcal{L}$ denotes the ideal of $\mathbb{Z}_\mathcal{L}$ generated by the elements of $\mathfrak{m}_0$. This group is called the norm group (or Takagi group).

The Artin map induces an isomorphism between $\mathbf{Gal}(\mathcal{L}/\mathcal{K})$ and a quotient of the class group of rays $\mathrm{Cl}_{\mathfrak{m}}(\mathcal{K})$. To completely describe the extension $\mathcal{L}/\mathcal{K}$ in terms of the arithmetic of $\mathcal{K}$, one must be able to describe $A_{\mathfrak{m}}(\mathcal{L}/\mathcal{K})$ without involving $\mathcal{L}$.

Theorem 2 ([Coh00, Theorem 3.4.4])**.** *Let $\mathcal{K}$ be a number field, $\mathcal{L}$ an abelian extension of $\mathcal{K}$, and $\mathfrak{m} = (\mathfrak{m}_0, \mathfrak{m}_\infty)$ an appropriate modulus to the extension $\mathcal{L}/\mathcal{K}$.*

1. *Let $\mathfrak{p}$ be a prime of $\mathbb{Z}_{\mathcal{K}}$ in $I_{\mathfrak{m}}(\mathcal{K})$, and $\mathfrak{P}$ a prime of $\mathbb{Z}_{\mathcal{L}}$ above $\mathfrak{p}$. Let f be the order of $\mathfrak{p}$ modulo $A_{\mathfrak{m}}(\mathcal{L}/\mathcal{K})$, then f is the degree of inertia of $\mathfrak{P}$. Since it does not depend on the choice of $\mathfrak{P}$, we may call it the degree of inertia of $\mathfrak{p}$.*

2. *Conversely, $A_{\mathfrak{m}}(\mathcal{L}/\mathcal{K})$ is generated by the ideals $\mathfrak{p}^f$ (where $\mathfrak{p}$ is a prime in $I_{\mathfrak{m}}(\mathcal{K})$ and f is its degree of inertia) and $P_{\mathfrak{m}}(\mathcal{K})$. It is even possible to restrict oneself to the primes of $I_{\mathfrak{m}}(\mathcal{K})$ with inertia degree $f = 1$ (still with the ideals of $P_{\mathfrak{m}}(\mathcal{K})$).*

Finally, this last theorem states the existence of a maximal abelian extension associated with each modulus.

Theorem 3 (Takagi's existence theorem [Coh00, Theorem 3.5.1])**.** *Let $\mathcal{K}$ be a number field and let $\mathfrak{m}$ be a modulus over $\mathcal{K}$. There exists a maximal isomorphism class of abelian extensions of conductor dividing $\mathfrak{m}$. It is called the ray class field (modulo $\mathfrak{m}$) of $\mathcal{K}$, and is denoted by $\mathrm{Ray}_{\mathfrak{m}}(\mathcal{K})$.*

The Galois group of the extension $\mathbf{Gal}(\mathrm{Ray}_{\mathfrak{m}}(\mathcal{K})/\mathcal{K})$ is isomorphic to the ray class group $\mathrm{Cl}_{\mathfrak{m}}(\mathcal{K})$ (the isomorphism is induced by the Artin map).

Remark 7. Equivalently, we can characterize the ray class field $\mathrm{Ray}_{\mathfrak{m}}(\mathcal{K})$ as the unique abelian extension of $\mathcal{K}$ up to isomorphism such that the primes of $\mathcal{K}$ that are totally split in $\mathrm{Ray}_{\mathfrak{m}}(\mathcal{K})$ are exactly the primes of $P_{\mathfrak{m}}(\mathcal{K})$.

3.2 Complex multiplication of elliptic curves

In this section, we detail effective aspects of the class field theory of imaginary quadratic number fields, in the unramified case. The computation of the class group and Hilbert class field, in this specific context, can be handled using the complex multiplication theory of elliptic curves. In Subsection 3.2.1, we briefly present the few results from complex multiplication theory that we need. In Subsection 3.2.2, we present an algorithm for computing the Hilbert class polynomial associated with an imaginary quadratic field. Finally, in Subsection 3.2.3, we present the algorithm of Atkin and Morain, also known as the *complex multiplication* method, which allows us, given two integers q and t satisfying the ad hoc conditions, to compute an ordinary elliptic curve defined over a finite field with q elements and trace t.

3.2.1 Action du groupe de classes sur les courbes elliptiques à multiplication complexe

Before presenting the algorithms, we recall some theorems from complex multiplication theory. For more information on this subject, the reader may consult the books [Sil94, Chapter II] and [Coh93, Section 7.2].

Definition 22. Let $E/\mathbb{C}$ be an elliptic curve, let $\mathbb{K}$ be an imaginary quadratic field, and let $\mathbb{O}$ be an order of $\mathbb{K}$.

- We say that E has complex multiplication by $\mathcal{O}$ if $\mathrm{End}(E) \simeq \mathcal{O}$.
- We say that E has complex multiplication if $\mathrm{End}(E) \not\simeq \mathbb{Z}$, in which case E necessarily has complex multiplication by an order of an imaginary quadratic field.
- We denote by $\mathrm{Ell}(\mathcal{O})$ the set of isomorphism classes of elliptic curves over $\mathbb{C}$ with complex multiplication by $\mathcal{O}$. We denote by $[E]$ the class of E in $\mathrm{Ell}(\mathcal{O})$.

Definition 23. Let $\tau \in \mathbb{H}$ (where $\mathbb{H}$ denotes the complex upper half-plane), we define the following modular forms and functions:

1. (Eisenstein series) for all integers $k \geqslant 2$,
$$G_{2k}(\tau) = \sum_{\substack{m,n\in\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{(m\tau+n)^{2k}}.$$
2. $g_2(\tau) = 60G_4(\tau)$ and $g_3(\tau) = 140G_6(\tau)$.
3. (Modular discriminant) $\Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^2$.
4. (Modular j-invariant)
$$j(\tau) = 1728\frac{g_2(\tau)}{\Delta(\tau)}.$$

Definition 24. Let $E/\mathbb{C}$ be an elliptic curve and $\tau \in \mathbb{H}$ such that $E \simeq \mathbb{C}/\mathbb{Z}+\tau\mathbb{Z}$. We define the j-invariant of E as follows:
$$j(E) = j(\tau).$$
Note that $j(E)$ does not depend on the choice of τ as a property of the modular j-invariant.

Theorem 4 ([Coh93, Theorem 7.2.13])**.** *Let $\mathcal{K}$ be an imaginary quadratic field. Let $E/\mathbb{C}$ be an elliptic curve, and let $\tau \in \mathbb{H}$ such that $E \simeq \mathbb{C}/\mathbb{Z}+\tau\mathbb{Z}$. Then E has complex multiplication by an order of $\mathcal{K}$ if and only if $\tau \in \mathcal{K}$. Furthermore, if $\tau \in \mathcal{K}$, then $j(\tau)$ is an algebraic integer.*

Theorem 5 ([Sil94, Chapter II, Theorem 4.3])**.** *Let $\mathcal{K}$ be an imaginary quadratic field, and let $E/\mathbb{C}$ be an elliptic curve with complex multiplication by $\mathbb{Z}_\mathcal{K}$. Then:*

1. $\mathrm{Hil}(\mathcal{K}) \simeq \mathcal{K}(j(E))$.
2. $[\mathrm{Hil}(\mathcal{K}) : \mathcal{K}] = [\mathbb{Q}(j(E)) : \mathbb{Q}]$.
3. $\mathbf{Gal}(\mathrm{Hil}(\mathcal{K})/\mathcal{K}) \simeq \mathrm{Cl}(\mathcal{K})$ *acts freely on the set* $\mathrm{Ell}(\mathbb{Z}_\mathcal{K})$ *and:*

$$\forall \sigma \in \mathbf{Gal}(\mathrm{Hil}(\mathcal{K})/\mathcal{K}), j(\sigma * [E]) = \sigma(j(E)).$$

Definition 25. Let $\mathcal{K}$ be an imaginary quadratic field and D the discriminant of its integer ring. We define the Hilbert class polynomial (for the discriminant D):

$$H_D = \prod_{[E] \in \mathrm{Ell}(\mathbb{Z}_\mathcal{K})} (x - j([E])) \in \mathbb{Z}[x].$$

3.2.2 Calcul du polynôme de classes de Hilbert

Let $\mathcal{K}$ be an imaginary quadratic field and D the discriminant of $\mathbb{Z}_\mathcal{K}$. In order to be able to compute the Hilbert class polynomial of $\mathcal{K}$, we want to be able to perform two operations:

- determine $\tau_1, \ldots, \tau_{|\mathrm{Cl}(\mathcal{K})|} \in \mathbb{H}$ such that $(\mathbb{C}/\mathbb{Z} + \tau_k\mathbb{Z})$ form a family of representatives of $\mathrm{Ell}(\mathbb{Z}_\mathcal{K})$.
- given $\tau \in \mathbb{H}$ and a precision n, compute $j(\tau)$ with precision n.

If we are able to perform these two tasks, it is possible to compute the coefficients of H_D to a chosen precision. We can then use the fact that H_D has integer coefficients to find the exact values of its coefficients.

Since $\mathcal{K}$ is a quadratic imaginary field, it has been known since the work of Gauss [Gau01] that there is a group isomorphism between $\mathrm{Cl}(\mathcal{K})$ and the group of reduced positive definite binary quadratic forms. This isomorphism makes it possible to quickly enumerate the elements of the class group. We will present some properties of binary quadratic forms. For a more general presentation, the reader may refer, for example, to [BV07].

Definition 26.

- A binary quadratic form is a function of the form $f(x, y) = ax^2 + bxy + cy^2$ with coefficients a, b, c not all zero. For brevity, we write $f = (a, b, c)$ and call f a form.
- The form (a, b, c) is said to be primitive if $\mathrm{pgcd}(a, b, c) = 1$.
- Two forms f and g are said to be equivalent if there exists a matrix

$$U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

of $\mathrm{SL}_2(\mathbb{Z})$ such that

$$g(x, y) = f(\alpha x + \beta y, \gamma x + \delta y).$$

We then write $g = fU$.

- Let $f = (a, b, c)$ be a form, we define the discriminant $\mathrm{disc}(f) = b^2 - 4ac$ of f. Let D be an integer, we denote

$$\mathrm{Quad}(D) = \{(a, b, c) \mid b^2 - 4ac = D\}.$$

Proposition 6. According to [Coh93, Section 5.2]:

- Let f and g be two equivalent forms, then $\mathrm{disc}(f) = \mathrm{disc}(g)$.
- Any integer $D \neq 1$ congruent to 0 or 1 modulo 4 is the discriminant of a form.
- Let $U = -I_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. For any form f, we have $fU = f$.
- Let D be a discriminant, $\mathrm{PSL}_2(\mathbb{Z})$ acts on $\mathrm{Quad}(D)$.

Definition 27. Let $f = (a, b, c)$ be a form.

- We say that f is defined positive if $\mathrm{disc}(f) < 0$ and $a > 0$.
- We say that f is reduced if it is positive definite, $|b| \leqslant a \leqslant c$ and if $b \leqslant 0$ when a and $|b|$ or a and c are equal.
- Let $D < 0$ be a discriminant. We denote by $\mathrm{Quad}_{\mathrm{red}}(D)$ the set of reduced forms with discriminant D.

Proposition 7. According to [Coh93, Theorem 5.2.8, Proposition 5.3.3, Lemma 5.3.4]:

1. Let f be a positive definite form and g a form equivalent to f. Then g is positive definite.
2. Let f be a positive definite form, then there exists a reduced form g that is equivalent to f.
3. Let $f = (a, b, c)$ be a reduced form with discriminant D, then $a \leqslant \sqrt{|D|/3}$.
4. Let f and g be two reduced and equivalent forms, then $f = g$.

These properties are key to the algorithmic interest of quadratic forms. In fact, the reduced form of property 2 can be computed explicitly using Gauss's algorithm [Coh93, Algorithm 5.4.2]. Furthermore, property 3 allows us to design an algorithm for enumerating $\mathrm{Quad}_{\mathrm{red}}(D)$. Thus, the set $\mathrm{Quad}_{\mathrm{red}}(D)$ is a set of unique representatives of the equivalence classes of $\mathrm{Quad}(D)$ modulo the action of $\mathrm{PSL}_2(\mathbb{Z})$, which can be computed explicitly. In

the context of the application to the class field theory of imaginary quadratic fields, D is the discriminant of the ring of integers of the imaginary quadratic field $\mathcal{K}$. We can define a group law on $\mathrm{Quad}_{\mathrm{red}}(D)$ and explicitly state a group isomorphism between $\mathrm{Quad}_{\mathrm{red}}(D)$ and $\mathrm{Cl}(\mathcal{K})$ [Coh93, Section 5.2]. Here, we only need a weakened version of this theorem (see Theorem 8).

Definition 28. Let $f = (a, b, c)$ be a reduced form, and $D = \mathrm{disc}(f)$. Let $i \in \mathbb{H}$ such that $i^2 = -1$. We define

$$\tau_f = \frac{-b + i\sqrt{-D}}{2a} \in \mathbb{H}.$$

Theorem 8 ([Coh93, Theorem 5.2.8 and Proposition 5.3.3])**.** *Let $\mathcal{K}$ be an imaginary quadratic field and D the discriminant of $\mathbb{Z}_{\mathcal{K}}$. The map*

$$\begin{array}{ccc} \mathrm{Quad}_{red}(D) & \longrightarrow & \mathrm{Ell}(\mathbb{Z}_{\mathcal{K}}) \\ f & \longmapsto & [\mathbb{C}/\mathbb{Z} + \tau_f \mathbb{Z}] \end{array}$$

is a bijection.

This theorem solves the first problem, namely computing a family of representatives of $\mathrm{Ell}(\mathbb{Z}_{\mathcal{K}})$. The second step is to compute $j(\tau)$ for $\tau \in \mathbb{H}$. The main idea is to use the 1-periodicity of the function j to compute its Fourier series expansion [Sil94, Section I.7].

Theorem 9 ([Sil94, Chapter I, Proposition 7.4])**.** *There exists a sequence of integers $(c_n)_{n \geqslant 0}$ such that for all $\tau \in \mathbb{H}$,*

$$j(\tau) = \frac{1}{q} + \sum_{n \geqslant 0} c_n q^n$$

where $q = e^{2i\pi\tau}$.

This formula is not used in practice because the coefficients (c_n) grow rapidly. Instead, we will use the formula from Theorem 11 as in [Coh93, Section 7.6.1] and [AM93]:

Theorem 10 ([Sil94, Chapter I, Theorem 8.1] and [Coh93, Section 7.6.1])**.** *Let $\tau \in \mathbb{H}$ and $q = e^{2i\pi\tau}$. We have*

$$\Delta(\tau) = (2\pi)^{12} q \prod_{n \geqslant 1} (1 - q^n)^{24} = (2\pi)^{12} q \left(1 + \sum_{n \geqslant 1} (-1)^n \left(q^{n(3n-1)/2} + q^{n(3n+1)/2}\right)\right)^{24}.$$

The series involved in the decomposition is much more convenient because the terms are small, and the exponents grow quadratically in n. To use this decomposition, we need to relate the j-modular invariant and the modular discriminant:

Theorem 11 ([Coh93, Section 7.6.1])**.** *Let $\tau \in \mathbb{H}$ and $q = e^{2i\pi\tau}$. We have*

$$j(\tau) = \frac{(256 f(\tau) + 1)^3}{f(\tau)} \text{ where } f(\tau) = \frac{\Delta(2\tau)}{\Delta(\tau)}.$$

Remark 8. It should be noted that

$$\Delta(2\tau) = (2\pi)^{12} q^2 \left(1 + \sum_{n \geqslant 1} (-1)^n \left(q^{n(3n-1)} + q^{n(3n+1)}\right)\right)^{24}.$$

The article [AM93, Section 7] relates the desired accuracy and the number of terms needed to be computed in the series of Theorem 10:

Theorem 12 ([AM93, Section 7])**.** *Let N be an integer, and let $q \in \mathbb{C}$, $|q| < 1$. Then*

$$\left| \sum_{n \leqslant N+1} (-1)^n (q^{n(3n-1)/2} + q^{n(3n+1)/2}) \right| \leqslant 6|q|^{3N^2/2}.$$

Theorems 11 and 12 address the second issue. We can provide the complete algorithm for computing the Hilbert class polynomial (algorithm 3.2.1). Algorithm 3.2.1 relies on algorithm 3.2.2 to compute the precision required for computing the j-invariant. Algorithm 3.2.2 is detailed in [Coh93, Section 7.6.2].

Algorithme 3.2.1 : Computation of the Hilbert class polynomial [Coh93, Algorithme 7.6.1]

Entrées : D the discriminant of the integer ring of an imaginary quadratic field.

Output : H_D the corresponding Hilbert class polynomial

```
Let k = ComputePrecision(D).
Let P = 1, b = D mod 2, B = ⌊√(−D/3)⌋.
tant que b ⩽ B faire
    Let t = (b² − D)/4 and a = b.
    tant que a² ⩽ t faire
        si a | t alors
            Let j = j((−b + i√(−D))/(2a)) (computed with k bits of precision)
            si a = b or a² = t or b = 0 alors
                P ← (x − j)P
            sinon
                P ← (x² − 2 Re(j)x + |j|²)P
        a ← a + 1
    b ← b + 2
Round the coefficients of P and return it
```

Example 2. Let $\mathcal{K} = \mathbb{Q}(\sqrt{-5})$ be an imaginary quadratic field, whose ring of integers has discriminant $D = -20$. We set $B = \lfloor \sqrt{20/3} \rfloor = 2$. We begin enumerating the reduced quadratic forms with discriminant D.

- For $b = 0$, we define $t = (b^2 - D)/4 = 5$.

Algorithme 3.2.2 : ComputePrecision(D)

Entrées : D the discriminant of the integer ring of an imaginary quadratic field.

Let $S = 0$, $b = D \bmod 2$, $B = \lfloor \sqrt{-D/3} \rfloor$.
tant que $b \leqslant B$ **faire**
  Let $t = (b^2 - D)/4$ and $a = b$.
  tant que $a^2 \leqslant t$ **faire**
    si $a \mid t$ **alors**
      si $a = b$ *or* $a^2 = t$ *or* $b = 0$ **alors**
        $S \leftarrow S + \frac{1}{a}$
      sinon
        $S \leftarrow S + \frac{2}{a}$
    $a \leftarrow a + 1$
  $b \leftarrow b + 2$
Return $\lceil \frac{\pi\sqrt{-D}S}{\ln(10)} \rceil + 10$.

  - For $a = 0$, we have $a \nmid t$.
  - For $a = 1$, we have $a \mid t$, so we obtain the form $(1, 0, 5)$.
  - For $a = 2$, we have $a \nmid t$.

- For $b = 2$, we define $t = (b^2 - D)/4 = 6$.
  - For $a = 2$, we have $a \mid t$, so we obtain the form $(2, 2, 3)$.

We deduce the precision $k = 20$ from the enumeration. We compute the values of the j-invariants.

```
sage: tau = I*sqrt(D)/2; elliptic_j(tau,prec=66) #10^20 is around equal to 2^66
1.2645389094751405 09e6
sage: tau = (-2+I*sqrt(D))/4; elliptic_j(tau,prec=66)
-538.9094751405093202
```

We compute an approximate value of the Hilbert polynomial: $P = x^2 - 1264000.00000000x - 681472000.000000$. We conclude that

$$H_{-20} = x^2 - 1264000x - 681472000.$$

3.2.3 Generating elliptic curves with prescribed trace over finite fields

In this section, we present an application of class field theory to the generation of elliptic curves of prescribed order over finite fields. The problem considered is as follows: let N be a positive integer, and $p \geqslant 5$ a prime integer such that $|N - p - 1| \leqslant 2\sqrt{p}$ and $N \neq p + 1$.

We seek to construct an elliptic curve E over the field K with p elements, with trace $t = N - p - 1$. It is possible to find such a curve by computing the roots modulo p of the Hilbert class polynomial associated with a well-chosen discriminant.

For any N satisfying the above conditions, there exists:

- D a negative integer congruent to t^2 modulo 4 such that $8 \nmid D$ and for any prime $l > 2$ dividing D, we have $l^2 \nmid D$.
- an integer y such that $t^2 - 4p = Dy^2$.

In particular, D is the discriminant of the integer ring of the imaginary quadratic field $\mathcal{K} = \mathbb{Q}(\sqrt{D})$. We know that t and p are coprime, so $p \nmid Dy^2$ and $D \equiv (t/y)^2 \bmod p$ is a square modulo p. Therefore, the principal ideal $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ is split in $\mathcal{K}$. We know that, up to conjugation, $\mathfrak{p} = (\pi)$ where $\pi = \frac{t+\sqrt{D}y}{2} \in \mathbb{Z}_{\mathcal{K}}$ (π is an integer because t^2 and D have the same congruence modulo 4). The ideal $\mathfrak{p}$ is principal, so it is completely split in $\mathrm{Hil}(\mathcal{K})$. Let $\mathfrak{P}$ be a prime of $\mathrm{Hil}(\mathcal{K})$ above $\mathfrak{p}$, then $\mathrm{Hil}(\mathcal{K})_{\mathfrak{P}} = \mathbb{F}_p$.

The algorithm 3.2.3 computes a curve with trace t defined over $\mathbb{F}_p$. The idea behind the algorithm is that there exists a curve E_0 defined over $\mathrm{Hil}(\mathcal{K})$ that has complex multiplication by $\mathbb{Z}_{\mathcal{K}}$, and whose reduction modulo $\mathfrak{P}$ is an elliptic curve E defined over $\mathbb{F}_p$ such that

$$\mathbb{Z}_{\mathcal{K}} \simeq \mathrm{End}(E_0) \simeq \mathrm{End}(E),$$

and such that $\pi \in \mathbb{Z}_{\mathcal{K}}$ is sent to the Frobenius morphism in $\mathrm{End}(E)$ (for details on the reduction of elliptic curves in characteristic p, the reader may consult [Lan87]). We therefore conclude that the minimal Frobenius polynomial on E is $x^2 - tx + p$ and that t is the trace of E. We know that $j(E_0)$ is a root of H_D. We can therefore find the j-invariant of E directly by searching among the roots of H_D modulo p.

Algorithme 3.2.3 : Generation of elliptic curves with prescribed trace
Entrées : $p \geqslant 5$ a prime integer, $t \in [-2\sqrt{p}, 2\sqrt{p}] \setminus \{0\}$ an integer.
Output : E an elliptic curve with trace t over the finite field with p elements.

```
Find K a quadratic imaginary field and D the discriminant of its integer ring such
  that t^2 - 4p = 0 mod D and (t^2 - 4p)/D is a square.
Let y be an integer such that t^2 - 4p = Dy^2.
Compute H_D, the Hilbert class polynomial associated with the discriminant D.
Let K be a finite field with p elements. Compute R the set of roots of H_D in K.
pour j ∈ R faire
    Let E be an elliptic curve over K with j-invariant j.
    pour E' in the twists of E faire
        si E' has trace t alors
            Return E'.
```

Example 3. Let $p = 34873130969$ and $t = 372876$. We can verify that p is prime, and therefore p and t are coprime. We compute

$$t^2 - 4p = -456012500 = -20 \times 4775^2 \tag{3.2.1}$$

Let $\mathcal{K} = \mathbb{Q}(\sqrt{-5})$ and $\mathbb{Z}_\mathcal{K}$ be the ring of integers of $\mathcal{K}$. The discriminant of the order $\mathbb{Z}_\mathcal{K}$ is -20. Let $\mathbb{F}_p$ be a finite field with p elements. Equation (3.2.1) guarantees that there exists an elliptic curve E over $\mathbb{F}_p$, with complex multiplication by $\mathbb{Z}_\mathcal{K}$. In this case, its j-invariant is a root of the Hilbert class polynomial

$$H_{-20} = x^2 - 1264000x - 681472000 \equiv (x - 23162900482)(x - 11711494487) \bmod p$$

in $\mathbb{F}_p$. Let $j = 23162900482$, then the curve

$$\tilde{E} : y^2 = x^3 + 3j(1728 - j)x - 2j(1728 - j)^2 = x^3 + 22026048806x + 14488057806$$

has j-invariant j and trace $-372876 = -t$. Let

$$E : y^2 = x^3 + 302722578x + 19597229242$$

be a quadratic twist of $\tilde{E}$, then the trace of E is $t = 372876$. We have found a curve with the desired trace, so we do not consider the j-invariant $j = 11711494487$.

3.3 Class field theory of function fields

Function fields (of curves over finite fields) are similar to number fields from an arithmetic point of view. Their maximal orders are Dedekind rings, and in both cases we can define the concepts of places (the primes of the maximal orders), their associated valuations, and a class group. The uniqueness of the decomposition of an ideal into a product of prime ideals in the maximal orders allows us to study the behavior of places in extensions and to distinguish three cases: decomposition, inertia, and ramification. Given these similarities, it is not surprising that function fields have a class field theory, whose results are very close to those of class field theory for number fields. It is even possible to define a unified class field theory for global fields (i.e., a theory common to number fields and function fields defined over finite fields), as for example in [AT09].

However, although similar, the arithmetic of function fields differs from that of number fields in several ways. For example, function fields have an infinite number of maximal orders, unlike number fields, which have only one. Another example: let $\mathcal{K}$ be a number field, then its maximal unramified abelian extension $\mathrm{Hil}(\mathcal{K})$ is a finite extension, whereas for $K(X)$ a function field defined over a finite field K, and for $\bar{K}$ an algebraic closure of K, we see that $\bar{K} \otimes_K K(X)$ is an infinite-degree unramified abelian extension of $K(X)$. Finally, function fields have a positive characteristic, which makes the study of ramification more complex than for number fields. Thus, several expositions of class field theory have been written for the specific case of function fields.

In this thesis, we will only present the unramified case of class field theory over function fields. The ramified case is studied by Serre in [Ser84] using generalized Jacobians [Ros54]. We begin by presenting a geometric exposition à la Serre [Ser84] in Section 3.3.1. This is the point of view that interests us the most, since it will be used in Chapter 4 to define structured Goppa codes. We also present Rosen's exposition [Ros87], which very explicitly shows the analogy with number fields in Section 3.3.2. Finally, we briefly discuss the links between the two points of view in Section **??**.

3.3.1 Geometric approach

Let K be a finite field with $q = p^m$ elements, $\bar{K}$ an algebraic closure of K, and X a smooth projective curve over K. Class field theory (for unramified extensions) of function fields can be formulated geometrically using abelian (unramified) covers of X over K and the Jacobian $\mathcal{J}_X$.

Indeed, let

$$\tau : Y \longrightarrow X$$

be an abelian cover over K with Galois group G. It defines an abelian extension $K(Y)/K(X)$ of $K(X)$. This section summarizes some of the results of [Lan56a, Lan56b] and [Ser84] on the link between isogenies of the Jacobian and unramified abelian covers of the curve.

In what follows, we denote by F_V the Frobenius endomorphism (relative to K) of a K-variety V. Any K-variety V naturally defines a variety over $\bar{K}$ that we will identify with V.

Definition 29.

- Let $\theta : \mathbb{G} \longrightarrow \mathbb{G}'$ be a morphism of connected commutative algebraic groups over $\bar{K}$. We say that θ is an isogeny if θ is surjective and its kernel is finite.
- We say that θ is separable if its degree is equal to the order of its kernel.
- If $\mathbb{G}$ and $\mathbb{G}'$ are K-varieties, we say that θ is defined over K if

$$F_{\mathbb{G}'} \circ \theta = \theta \circ F_{\mathbb{G}}.$$

Definition 30. Let V be a $\bar{K}$-variety, $\mathbb{G}$ and $\mathbb{G}'$ two connected commutative algebraic groups over $\bar{K}$. Let $f : V \longrightarrow \mathbb{G}'$ be a regular map and $\theta : \mathbb{G} \longrightarrow \mathbb{G}'$ a separable isogeny. We define $V \times_{\mathbb{G}'} \mathbb{G}$ as the fiber product of V and $\mathbb{G}$ over $\mathbb{G}'$ as the submanifold of $V \times \mathbb{G}$ whose $\bar{K}$-rational points are

$$V \times_{\mathbb{G}'} \mathbb{G}(\bar{K}) = \{(x, g) \in V \times \mathbb{G} \mid f(x) = \theta(g)\}.$$

The fiber product $V \times_{\mathbb{G}'} \mathbb{G}$ is equipped with projections π_V and π_G that make the following diagram commute:

$$\begin{array}{ccc} V \times_{\mathbb{G}'} \mathbb{G} & \xrightarrow{\pi_{\mathbb{G}}} & \mathbb{G} \\ \downarrow{\scriptstyle \pi_V} & & \downarrow{\scriptstyle \theta} \\ V & \xrightarrow[f]{} & \mathbb{G}' \end{array}$$

We say that π_V is the pullback of θ by f, and we write $\pi_V = f^{-1}(\theta)$.

We note that the isogeny θ is a unramified abelian covering map of $\mathbb{G}'$ with Galois group G consisting of translations by elements of $\ker\theta$. Then π_V is an abelian cover with Galois group G, unramified of V.

Lemma 13. Using the notation from definition 30, if V, $\mathbb{G}$, and $\mathbb{G}'$ are K-varieties, and if f and θ are defined over K, then $V \times_{\mathbb{G}'} \mathbb{G}$ is a K-variety and π_V is defined over K.

Proof. Let $W = V \times_{\mathbb{G}'} \mathbb{G}$. Let $(x, g) \in W$. We want to check that W is stable by

$$F_{V\times\mathbb{G}} : (y, h) \longmapsto (F_V(y), F_{\mathbb{G}}(h)).$$

To do this, we compute

$$f(F_V(x)) = F_{\mathbb{G}'}(f(x)) = F_{\mathbb{G}'}(\theta(g)) = \theta(F_{\mathbb{G}}(g)),$$

so W is stable under $F_{V\times\mathbb{G}}$ and is indeed a K-variety.

Furthermore, $\pi_V(F_W((x, g))) = F_V(x) = F_V(\pi_V((x, g)))$, so π_V is defined on K. □

Let us return to the study of the curve X. The Jacobian $\mathcal{J}_X$ of X is a connected commutative algebraic group defined over K. Furthermore, let P be a K-rational point of X. The Jacobi map j_P associated with P is a regular map from X to $\mathcal{J}_X$ defined over K. Let

$$\theta : \mathbb{G} \longrightarrow \mathcal{J}_X$$

be a separable isogeny. Let

$$Y = X \times_{\mathcal{J}_X} \mathbb{G}.$$

Then Y is a smooth integral projective curve (over $\bar{K}$), and $\pi_X : Y \longrightarrow X$ is an unramified abelian covering of X. Furthermore, one can prove that

- Y is a K-variety and π_X is defined over K if and only if θ is defined over K.
- The covering π_X is Galois over K (meaning that $K(Y)/K(X)$ is a Galois extension) if and only if, in addition, the action of $F_{\mathbb{G}}$ on $\ker\theta$ is trivial. In this case, the covering is abelian with Galois group isomorphic to $\ker\theta$.
- The covering π_X is totally split above P if and only if, similarly, the action of $F_{\mathbb{G}}$ on $\ker\theta$ is trivial.

Theorem 14 ([Ser84, Chapter I, Corollary of Theorem 4 and Theorem 5])**.** *Let K be a finite field and X a smooth projective curve over K. Let P be a K-rational point of X.*

There exists a smooth projective curve Y_{max} over K and an abelian covering

$$\tau_{max} : Y_{max} \longrightarrow X$$

over K that is unramified, totally split above P, and maximal in the following sense: for any cover

$$\tau_Y : Y \longrightarrow X$$

satisfying these properties, there exists an unramified abelian covering

$$\tau_{Y_{max}/Y} : Y_{max} \longrightarrow Y$$

such that

$$\tau = \tau_Y \circ \tau_{Y_{max}/Y}.$$

The covering τ_{max} is obtained by pulling back the isogeny

$$\varphi = F_{\mathcal{J}_X} - \mathrm{Id},$$

by the Jacobi map j_P.

Theorem 14 induces a correspondence between the isomorphism classes of abelian, unramified covers of X totally split above P and the subgroups of $\mathcal{J}_X(K)$. Indeed, let H be a subgroup of $\mathcal{J}_X(K)$. There exists a separable isogeny whose kernel is H. We denote this isogeny by

$$\pi_H : \mathcal{J}_X \longrightarrow \mathcal{J}_X/H.$$

Then there exists

$$\theta : \mathcal{J}_X/H \longrightarrow \mathcal{J}_X$$

an isogeny such that

$$\theta \circ \pi_H = F_{\mathcal{J}_X} - \mathrm{Id}\,.$$

The covering

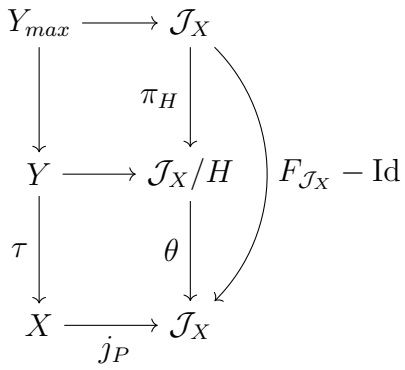
$$\tau = j_P^{-1}(\theta) \tag{3.3.1}$$

is an unramified abelian covering of X, totally split above P, with Galois group $\mathcal{J}_X(K)/H$.

Proposition 15. Using the notation from Theorem 14, let Q be a K-rational point of X, and let H be a subgroup of $\mathcal{J}_X(K)$. Let $\tau : Y \longrightarrow X$ be the unramified abelian cover, totally split above P, associated with H as defined in equation(3.3.1).

Then τ is totally split above Q if and only if the class of $Q - P$ in $\mathcal{J}_X(K)$ belongs to H.

Proof. We must check that the fiber of τ above Q is composed of K-rational points. We are in the following situation:



Let c be the class of $Q - P$ in $\mathcal{J}_X(K)$. We must check that the points of Y above Q are fixed by the Frobenius morphism on Y if and only if $c \in H$. Let $(Q, a + H)$ be a point of Y above Q. We have

$$F_Y((Q, a + H)) = (F_X(Q), F_{J_X/H}(a + H)) = (Q, F_{\mathcal{J}_X}(a) + H)$$

where $\theta(a + H) = j_P(Q) = c$. Therefore, $(Q, a + H)$ is fixed by F_Y if and only if $F_{J_X}(a) - a \in H$. But

$$F_{J_X}(a) - (a) = \theta(a + H) = c,$$

so $F_{J_X}(a) - a \in H$ if and only if $c \in H$. □

3.3.2 Algebraic approach

In this section, we summarize the presentation in [Ros87] of class field theory (unramified case), and its definition of a Hilbert class field for function fields. Let K be a finite field with $q = p^m$ elements, and let X be a smooth projective curve over K. Let $K(X)_{sep}$ be a separable closure of $K(X)$. Let $\bar{K}$ be the algebraic closure of K in $K(X)_{sep}$.

There exists a maximum abelian unramified extension of $K(X)$ in $K(X)_{sep}$, but this extension is of infinite degree (even relative to $\bar{K}(X)$). To define a Hilbert class field whose extension degree is finite, we must add a condition that, among other things, limits the extension of the field of constants. Let S_∞ be a finite non-empty set of places of $K(X)$ of arbitrary degrees. Let $\mathcal{O}_{X \setminus S_\infty}$ be the ring of functions with all poles in S_∞. This is a Dedekind ring (see [Ros87, Section 1]) whose class group $\mathrm{Cl}(\mathcal{O}_{X \setminus S_\infty})$ is finite. We can draw an analogy between the triplet $K(X), \mathcal{O}_{X \setminus S_\infty}, S_\infty$ and a number field, its ring of integers, and its places at infinity.

Proposition 16. There exists a maximum unramified abelian extension of $K(X)$ in $K(X)_{sep}$ in which the places of S_∞ are totally split. It is called the Hilbert class field of $K(X)$ with respect to S_∞, and is denoted by $\mathrm{Hil}_{S_\infty}(X)$.

Proof. The properties of being abelian, unramified, and totally split above S_∞ are preserved by compositum. □

Proposition 17. Let

$$\delta = \mathrm{pgcd}_{P \in S_\infty} \deg P.$$

Let $L = \bar{K} \cap \mathrm{Hil}_{S_\infty}(X)$ be the field of constants of $\mathrm{Hil}_{S_\infty}(X)$. Then L is the extension of K of degree δ in $\bar{K}$.

Proof. Let $P \in S_\infty$ and let Q be a place above P. Let K_Q be the residue field at Q. Since P is totally split in $\mathrm{Hil}_{S_\infty}(X)$, we know that K_Q is equal to K_P, the residue field at P. Now L is a subfield of K_Q, and therefore of K_P. So the degree of the extension L/K divides $\deg P$. This is true for any $P \in S_\infty$, so

$$[L : K] \mid \delta.$$

Let L' be the extension of K of degree δ in $\bar{K}$. Then the compositum $L' \mathrm{Hil}_{S_\infty}(X)$ is a Galois extension of $K(X)$ whose Galois group is a subgroup of

$$\mathbf{Gal}(L'(X)/K(X)) \times \mathbf{Gal}(\mathrm{Hil}_{S_\infty}(X)/K(X)) = \mathbf{Gal}(L'/K) \times \mathbf{Gal}(\mathrm{Hil}_{S_\infty}(X)/K(X)).$$

It is therefore an abelian extension of $K(X)$. Furthermore, according to [Sti08, Theorem 3.6.3], $L' \mathrm{Hil}_{S_\infty}(X)$ is unramified, and all places of S_∞ are totally split in $L' \mathrm{Hil}_{S_\infty}(X)$, since δ divides the degree of all places of S_∞. By the maximality of $\mathrm{Hil}_{S_\infty}(X)$, we deduce

$$L' \mathrm{Hil}_{S_\infty}(X) = \mathrm{Hil}_{S_\infty}(X) \text{ and } L' = L.$$

□

Proposition 18. Let N be the subgroup of $\mathrm{Div}(X)$ generated by the points of S_∞. Then there exists a group isomorphism

$$I(\mathcal{O}_{X \setminus S_\infty}) \simeq \mathrm{Div}(X)/N$$

where $I(\mathcal{O}_{X \setminus S_\infty})$ is the group of fractional ideals of $\mathcal{O}_{X \setminus S_\infty}$.

Proof. According to [Sti08, Proposition 3.2.9], the prime ideals of $\mathcal{O}_{X \setminus S_\infty}$ are in bijection with the places of $K(X)$ that are not in S_∞. Since $\mathrm{Div}(X)$ is the free abelian group generated by the places of $K(X)$, and $I(\mathcal{O}_{X \setminus S_\infty})$ is isomorphic to the free abelian group generated by the prime ideals of $\mathcal{O}_{X \setminus S_\infty}$, we deduce the proposition. □

We can define the Artin map of the extension $\mathrm{Hil}_{S_\infty}(X)/K(X)$ as in definition 21. Let P be a place of $K(X)$ and Q a place of $\mathrm{Hil}_{S_\infty}(X)$ above P. Let $D(Q/P)$ be the decomposition group of Q and $I(Q/P)$ its inertia group. Since $\mathrm{Hil}_{S_\infty}(X)/K(X)$ is an unramified extension, $I(Q/P)$ is trivial. Let K_P and K_Q be the residue fields at P and Q respectively, then we have a canonical isomorphism

$$D(Q/P) \longrightarrow \mathbf{Gal}(K_Q/K_P).$$

Let $\mathfrak{s}_Q \in D(Q/P)$ be the element associated with the Frobenius morphism via this isomorphism. Since it does not depend on the choice of Q (the extension is abelian), we denote it by $\mathfrak{s}_P$. We define

$$(.,\mathrm{Hil}_{S_\infty}(X)/K(X)): \begin{array}{ccc} \mathrm{Div}(X) & \longrightarrow & \mathbf{Gal}(\mathrm{Hil}_{S_\infty}(X)/K(X)) \\ \sum_P n_P P & \longmapsto & \prod \mathfrak{s}_P^{n_P} \end{array}$$

as the Artin map.

It can be noted that Artin's map is trivial on S_∞ by definition of $\mathrm{Hil}_{S_\infty}(X)$. Then $(.,\mathrm{Hil}_{S_\infty}(X)/K(X))$ induces a morphism

$$I(\mathcal{O}_{X\setminus S_\infty}) \longrightarrow \mathbf{Gal}(\mathrm{Hil}_{S_\infty}(X)/K(X)).$$

Theorem 19 ([Ros87, Theorem 1.3])**.** *Artin's map* $(.,\mathrm{Hil}_{S_\infty}(X)/K(X))$ *is surjective and induces an isomorphism*

$$\mathrm{Cl}(\mathcal{O}_{X\setminus S_\infty}) \xrightarrow{\sim} \mathbf{Gal}\left(\mathrm{Hil}_{S_\infty}(X)/K(X)\right).$$

This theorem shows that this definition of the Hilbert class field of $K(X)$ leads to a situation very similar to that of number fields. To complete this exposition, we need to express $\mathrm{Cl}(\mathcal{O}_{X\setminus S_\infty})$ in terms of $\mathrm{Pic}(X)$ and S_∞ and give its class number.

Theorem 20 ([Ros87, Theorem 1.3 and Lemmas 1.1-2])**.**

- *Let* N *be the subgroup of* $\mathrm{Pic}(X)$ *generated by the classes of the places of* S_∞*. Then*

$$\mathrm{Cl}(\mathcal{O}_{X\setminus S_\infty}) \simeq \mathrm{Pic}(X)/N.$$

- *Let* H *be the subgroup of* $\mathrm{Pic}^0(X)$ *generated by the places of* S_∞ *(i.e., the classes of linear combinations of* S_∞ *of degree* 0*). Then*

$$|\mathrm{Cl}(\mathcal{O}_{X\setminus S_\infty})| = \delta |\mathrm{Pic}^0(X)|/|H|$$

  where $\delta = \mathrm{pgcd}_{P\in S_\infty} \deg P$*.*

Corollary 20.1. $[\mathrm{Hil}_{S_\infty}(X) : K(X)]$ *is finite.*

Corollary 20.2. *The kernel of the Artin map is the subgroup of* $\mathrm{Div}(X)$ *generated by the principal divisors and the places of* S_∞*.*

Corollary 20.3. *Assume that* $S_\infty = \{P\}$ *where* P *is a point of* $K(X)$ *of degree* 1*. Then*

$$\mathbf{Gal}(\mathrm{Hil}_{S_\infty}(X)/K(X)) \simeq \mathrm{Pic}^0(X) = \mathcal{J}_X(K).$$

In particular, to every subgroup H *of* $\mathrm{Pic}^0(X)$*, we associate a unique unramified abelian extension of* $K(X)$ *in* $K(X)_{sep}$ *with a Galois group naturally isomorphic to* $\mathrm{Pic}^0(X)/H$ *(and vice versa).*

Corollary 20.4. *Assume that $S_\infty = \{P\}$ where P is a point of $K(X)$ of degree 1. Let $K(X) \subset K(Y) \subset \mathrm{Hil}_{S_\infty}(X)$ be the extension associated with the subgroup H of $\mathrm{Pic}^0(X)$. Let Q be a place of $K(X)$, then Q is totally split in $K(Y)$ if and only if*

$$Q - \deg(Q)P \in H.$$

Proof of Theorem 20. The first statement is a direct consequence of Proposition 18. We now prove the second statement.

We know that there exists an exact sequence of additive groups

$$0 \longrightarrow \mathrm{Pic}^0(X) \longrightarrow \mathrm{Pic}(X) \longrightarrow \mathbb{Z} \longrightarrow 0$$

according to a theorem by Schmidt [Sch31]. Similarly, we have

$$0 \to \mathrm{Pic}^0(X)/(\mathrm{Pic}^0(X) \cap N) \to \mathrm{Cl}(\mathcal{O}_{X\setminus S_\infty}) \to \mathrm{Pic}(X)/(N + \mathrm{Pic}^0(X)) \to 0$$

Now,

$$(\mathrm{Pic}^0(X) \cap N) = H,$$

and

$$\mathrm{Pic}(X)/\mathrm{Pic}^0(X) \simeq \mathbb{Z},$$

and

$$(N + \mathrm{Pic}^0(X))/\mathrm{Pic}^0(X) \simeq \delta\mathbb{Z}.$$

We deduce that

$$0 \longrightarrow \mathrm{Pic}^0(X)/H \longrightarrow \mathrm{Cl}(\mathcal{O}_{X\setminus S_\infty}) \longrightarrow \mathbb{Z}/\delta\mathbb{Z} \longrightarrow 0.$$

□

3.3.3 Link between the two approaches

We see that some of the results of Theorem 14 and Proposition 15 are found in Corollaries 20.3 and 20.4. In this section, we study the relationships between the algebraic and geometric perspectives.

Let K be a finite field with $q = p^m$ elements, and let X be a smooth projective curve over K. Let $K(X)_{sep}$ be a separable closure of $K(X)$. Let $\bar{K}$ be the algebraic closure of K in $K(X)_{sep}$. Let S_∞ be a non-empty finite set of places of $K(X)$ such that

$$\delta := \mathrm{pgcd}_{P \in S_\infty} \deg P = 1.$$

Let $\mathcal{O}_{X\setminus S_\infty}$ be the ring of functions with poles in S_∞.

Since the degree of the extension $\mathrm{Hil}_{S_\infty}(X)/K(X)$ is finite, the field $\mathrm{Hil}_{S_\infty}(X)$ is also a function field (over K because $\delta = 1$). Thus, there exists a smooth projective curve Y over K such that $K(Y) = \mathrm{Hil}_{S_\infty}(X)$. It is natural to ask what the geometric relations between X and Y are.

First case: S_∞ contains a place of degree 1

This is the simplest and most straightforward case. Let P be a K-rational point of X corresponding to a place of degree 1 of S_∞. The extension $K(Y)/K(X)$ is abelian and unramified, which means that there exists

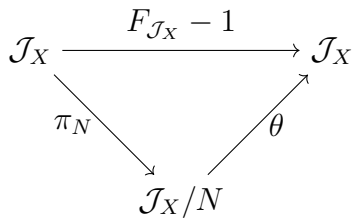
$$\tau : Y \longrightarrow X$$

an abelian unramified covering over K. Furthermore, since $P \in S_\infty$, we know that τ is totally split above P.

Let N be the subgroup of $\mathcal{J}_X(K)$ generated by the classes of $Q - \deg(Q)P$ for $Q \in S_\infty$. We know that

$$\mathbf{Gal}(K(Y)/K(X)) \simeq \mathcal{J}_X(K)/N$$

according to theorems 19 and 20. Let θ be the separable isogeny that makes the following diagram commutative:



where π_N is the quotient isogeny. Then τ is isomorphic to the pullback of θ by j_P, the Jacobi map associated with P according to Theorem 14.

General case

The general case requires a little more caution, as there may not be any places of degree 1 in S_∞. However, since $\delta = 1$, we know that there exists $D \in \mathrm{div}(X)$ a divisor generated by the places of S_∞ of degree 1. Let N be the subgroup of $\mathcal{J}_X(K)$ generated by the classes of $Q - \deg(Q)D$ for $Q \in S_\infty$. Then, according to theorems 19 and 20,

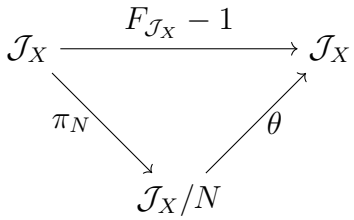
$$\mathbf{Gal}(K(Y)/K(X)) \simeq \mathcal{J}_X(K)/N.$$

There exists

$$\tau : Y \longrightarrow X$$

an abelian cover of X that is unramified and totally decomposed over the points associated with the places of S_∞.

Let j_D be the Jacobi map associated with the divisor D (which associates the class of $P - \deg(P)D$ in $\mathcal{J}_X$ with every closed point P of X). It is a regular map defined on K (since D has degree 1). Let θ be the separable isogeny that makes the following diagram commute:



Then τ is isomorphic to the pullback of θ by j_D.

3.4 Construction of algebraic curves with many rational points

Curves (smooth projective curves) defined over finite fields with many rational points are very interesting for many applications. Indeed, given a finite field K, it can be shown that, as the genus increases, Weil's bound gets less tight and is no longer sufficient to correctly estimate the maximum number of rational points that a curve can have. However, in the context of Goppa code design (see Section 4.2), it is important to know the curves X over K with the largest possible number of K-rational points relative to their genus. The manYPoints [vdGHLR09] database lists, according to the order of the field q and the genus g, the known curves with the largest number of points. It also lists the best known upper bounds on the maximum number of points a curve can have.

Let $q = p^m$ be the order of K, we define the Ihara constant

$$A(q) = \limsup_{X/K} \frac{N(X)}{g_X}$$

where $N(X)$ and g_X are, respectively, the number of K-rational points and the genus of X. The Ihara constant is a quantity that precisely describes the maximum number of points that a curve over K can have asymptotically. It is very useful for describing the quality of Goppa codes over K (as a family of codes).

Class field theory allows us to construct examples of curves with many points. In Subsection 3.4.1, we explain how to construct curves with many points as abelian extensions of other curves, and we give an example from [Ser20, Section 7.3]. We also present new curves with record numbers of points over the fields with 4, 9, 16, and 25 elements. In Subsection 3.4.2, we explain that it is possible to bound Ihara's constant from below by constructing towers of unramified abelian extensions of curves (according to [Ser20, Section 5.9]).

3.4.1 Examples of constructions

In this subsection, we explain how to construct an algebraic with many points as unramified abelian covers of another curve. In particular, we present new curves with a record number

of points relative to their genus over the finite fields with 4, 9, 16, and 25 elements. This method can be generalized to the ramified abelian case (see [Ser20, Section 7.3]).

Let X be a smooth projective curve over a finite field K. Suppose that X has a K-rational point P. Let H be a subgroup of $\mathcal{J}_X(K)$. According to Theorem 14, there exists a smooth projective curve Y_H and an unramified abelian covering

$$\tau_H : Y_H \longrightarrow X$$

with Galois group isomorphic to $\mathcal{J}_X(K)/H$, and totally split above P. Furthermore, according to Proposition 15, the K-rational points of Y_H are in the (totally split) fibers above the points Q of X of degree 1, such that

$$j_P(Q) \in H.$$

Let n be the number of K-rational points of X whose image by j_P belongs to H. Let

$$d = \frac{|\mathcal{J}_X(K)|}{|H|},$$

and let g_X be the genus of X and g_{Y_H} the genus of Y_H. Then

- the curve Y_H has nd K-rational points.
- according to the Riemann-Hurwitz formula, since τ_H is unramified,

$$g_{Y_H} = d(g_X - 1) + 1.$$

The following example is taken from [Ser20, Section 7.3].

Example 4. Let X be the smooth projective curve of genus $g_X = 2$ defined over $\mathbb{F}_2$ by

$$X : y^2 + y = \frac{x^2 + x}{x^3 + x + 1}.$$

The curve X has six $\mathbb{F}_2$-rational points, and we can show that there exists an isomorphism of abelian groups

$$\mathcal{J}_X(\mathbb{F}_2) \simeq \mathbb{Z}/19\mathbb{Z}.$$

Let P be an $\mathbb{F}_2$-rational point of X, and let

$$\tau : Y \longrightarrow X$$

be an unramified abelian cover of X totally split above P with Galois group isomorphic to $\mathcal{J}_X(\mathbb{F}_2)$ (associated with the subgroup $H = \{0\}$). Then P is the only $\mathbb{F}_2$-rational point of X that is totally split in Y, and Y is a curve of genus $g_Y = 20$ with 19 $\mathbb{F}_2$-rational points.

It can be shown that a curve of genus 20 over $\mathbb{F}_2$ has at most 21 points [Ser20, Section 7.1]. The question of whether there exists a curve of genus 20 over $\mathbb{F}_2$ with at least 20 points is still open [vdGHLR09].

The number of subgroups of $\mathcal{J}_X(K)$ can grow exponentially in the genus and polynomially in q, the number of elements of K. Thus, it quickly becomes difficult to enumerate these subgroups to produce record curves. We present a trick used in [GX22, NX98, Que89, vdG09] consisting in studying a specific subgroup. Assume that there exists κ a subfield of K of index 2, and that the curve X is defined over κ, i.e., there exists a smooth projective curve X_κ over κ such that

$$X = (X_\kappa)_K .$$

In this context, the trick is to choose for P a κ-rational point of X, i.e., stable under the action of $\mathbf{Gal}(K/\kappa)$ on X, and to set

$$H = \mathcal{J}_{X_\kappa}(\kappa)$$

as the subgroup of κ-rational points of $\mathcal{J}_X(K)$. Then, $\tau_H : Y_H \longrightarrow X$ is an unramified abelian cover with Galois group

$$G = \mathcal{J}_X(K)/\mathcal{J}_X(\kappa),$$

and the points of X that are totally split in Y_H are precisely the κ-rational points of X.

In particular, if the L-polynomial of X_κ is known, we can compute:

- the L-polynomial of X.
- the order of $\mathcal{J}_X(\kappa)$ and the order of $\mathcal{J}_X(K)$.
- the trace of X_κ, or equivalently the number of κ-rational points of X.

We can then determine the order of G, the genus g_{Y_H} of Y_H and the number of K-rational points of Y_H.

We will now use this trick to produce new record curves. The LMFDB [LMF25] database lists, among other things, L-polynomials of algebraic curves over finite fields with 2, 3, 4, and 5 elements (among others). By enumerating this data, we can produce new curves with a record number of points over finite fields with 4, 9, 16, and 25 elements. These records are presented in Tables 3.1, 3.2, 3.3, and 3.4.

LMFDB label of X	$\lvert G\rvert$	g_{Y_H}	$\#Y_H(\mathbb{F}_4)$	Old record ([vdGHLR09])
4.2.d_i_o_x	11	34	66	65
5.2.e_m_ba_bv_cu	12	49	84	81

Table 3.1: New curves with a record number of rational points over a field with 4 elements

ŁMFDB label of X	$\lvert G\rvert$	g_{Y_H}	$\#Y_H(\mathbb{F}_9)$	Old record ([vdGHLR09])
4.3.i_bi_ds_hn	9	28	108	105
4.3.h_ba_co_ez	11	34	121	114
4.3.h_bb_ct_fk	12	37	132	126

Table 3.2: New curves with a record number of rational points over a field with 9 elements

ŁMFDB label of X	$\lvert G\rvert$	g_{Y_H}	$\#Y_H(\mathbb{F}_{16})$	Old record ([vdGHLR09])
3.4.g_v_bx	19	39	209	194
3.4.f_p_bg	23	47	230	$\emptyset$

Table 3.3: New curves with a record number of rational points over a field with 16 elements

3.4.2 Towers of curves

Let K be a finite field with $q = p^m$ elements. We want to lower bound the Ihara constant

$$A(q) = \limsup_{X/K} \frac{N(X)}{g_X}$$

where $N(X)$ denotes the number of K-rational points on X and g_X denotes the genus of X. To do this, we must define a sequence of smooth projective curves $(X_i)_{i\in\mathbb{N}}$ over K such that $N(X_i)/g_{X_i}$ converges to a nonzero constant.

It is possible to use class field theory to define such sequences of curves [Ser20, Section 5.9]. Let X be a smooth projective curve over K, let S be a finite non-empty set of K-rational points of X, and let ℓ be a prime (potentially equal to the characteristic p). We define

- $(X_0, S_0) = (X, S)$;
- for all $i \in \mathbb{N}$, the cover $\tau_i : X_{i+1} \longrightarrow X_i$ is the maximal abelian, unramified cover of degree a power of ℓ, totally split above the points of S_i;
- for all $i \in \mathbb{N}$, the set S_{i+1} is the set of points in the fibers above the points of S_i.

ŁMFDB label of X	$\lvert G\rvert$	g_{Y_H}	$\#Y_H(\mathbb{F}_{25})$	Old record ([vdGHLR09])
3.5.k_bv_fc	16	33	256	226
3.5.j_bn_ec	20	41	300	260
3.5.j_bo_eh	21	43	315	276
3.5.i_bf_dc	24	49	336	315

Table 3.4: New curves with a record number of rational points over a field with 25 elements

By composing the τ_i, we obtain a sequence of unramified Galois covers of X totally split above S. Note that we can assert that these covers are Galois thanks to the maximality of the τ_i. We call the sequence $(X_i)_{i\in\mathbb{N}}$ the (S,ℓ)-*class field tower* of X.

Let G_i be the Galois group of the cover $X_i \longrightarrow X$ for all $i \in \mathbb{N}$, then G_i is a finite group of order a power of ℓ. Furthermore, for all $i \in \mathbb{N}$, the group G_i is a quotient of G_{i+1}. We define

$$G = \lim_{\leftarrow} G_i.$$

The group G is a pro-ℓ-group. Let r be the minimum number of generators of G (as a pro-ℓ-group). Note that $r \geqslant 1$ if and only if $\mathcal{J}_X(K)$ has a subgroup of order ℓ.

Theorem 21 ([Ser20, Theorem 5.9.4])**.** *We use the notation from the beginning of Subsection 3.4.2. Assume that $r \geqslant 1$ and that*

$$\#S \leqslant \frac{r^2}{4} - r + \begin{cases} 1 \text{ if } \ell \text{ divides } q-1, \\ 0 \text{ otherwise.} \end{cases}$$

Then the (S,ℓ)-class field tower of X is infinite, i.e. the sequence $(X_i)_{i\in\mathbb{N}}$ is not asymptotically constant.

The following theorem uses an infinite class field tower of X to lower bound Ihara's constant.

Theorem 22 ([Ser20, Theorem 5.9.5])**.** *We use the notation from the beginning of Subsection 3.4.2. Assume that the (S,ℓ)-class field tower of X is infinite. Then*

$$A(q) \geqslant \frac{\#S}{g_X - 1}.$$

Proof. Let d_i be the order of G_i for all $i \in \mathbb{N}$. According to the Riemann–Hurwitz formula, we have

$$g_{X_i} = d_i(g_X - 1) + 1.$$

Furthermore, since the points of S are totally split in X_i, then $N(X_i)$, the number of K-rational points of X_i, satisfies

$$N(X_i) \geqslant \#S \cdot d_i.$$

In particular, $(N(X_i)_{i\in\mathbb{N}})$ tends to infinity because $(d_i)_{i\in\mathbb{N}}$ does as well. We have

$$\frac{N(X_i)}{g_{X_i}} \geqslant \frac{\#S \cdot d_i}{d_i(g_X - 1) + 1}$$

and taking the limit as $i \to +\infty$

$$A(q) \geqslant \limsup_{i\in\mathbb{N}} \frac{N(X_i)}{g_{X_i}} \geqslant \frac{\#S}{g_X - 1}.$$

□

Corollary 22.1 ([Ser20, Corollary 5.9.7])**.** *Let $q = p^m$ be a prime power with $m > 0$. Then*

$$A(q) > 0.$$

Chapter 4

Error correcting codes

The objective of this chapter is to present a family of Goppa codes with an additional structure. This structure has an algorithmic interest, allowing to reduce the space required to store the generator and parity-check matrices of the codes, and in some cases allowing to reduce the complexity of encoding and decoding these codes.

In Section 4.1, we briefly review the basic concepts of linear error-correcting code theory. Then, in Section 4.2, we present the definition of geometric Goppa codes, also known as AG codes, and some of their properties. In Section 4.3, we recall the definition of a group algebra and present the Fourier transform of a finite abelian group algebra. We detail the complexity of computing the Fourier transform over finite fields and show that finite abelian group algebras over finite fields have fast multiplication.

Next, in Section 4.4, given G a finite group and K a finite field, we study linear codes defined by the free left (and right) submodules of $K[G]^E$, where E is a finite set. In particular, we define the notion of dual code in this particular context, and we show that these codes have generator matrices (and parity-check matrices) with coefficients in $K[G]$. Finally, in Section 4.5, we define a new family of geometric codes, coming from unramified abelian covers with Galois group G. Under certain usual assumptions, these codes are free sub-$K[G]$-modules of $K[G]^E$, for E a finite set. We study the specific features of this new family of codes.

4.1 Linear codes

We start by introducing the basic concepts of error-correcting code theory. The reader can refer to [Sti08] or any book on the subject of error-correcting codes for more details on what follows. In this section, K denotes a finite field with $q = p^m$ elements.

4.1.1 General definitions

A *error-correcting code* C of *length* n and *dimension* k over K is a vector subspace of K^E of dimension k, where E is a set of cardinality n. We also say that C is an $[n, k]$-code over

K. Let $c \in C$, we say that c is a codeword of the code C. We will sometimes use the notation $\operatorname{len} C$ to denote the length of C and $\dim C$ to denote its dimension. In the case where $E = [1..n]$ is the set of integers from 1 to n, we will write $K^E = K^n$.

Definition 31. Let $a = (a_i)_{i \in E} \in K^E$, we define the weight of a:

$$\operatorname{wt}(a) = \#\{i \in E | a_i \neq 0\}.$$

We define the *Hamming distance* d on K^E

$$\forall a, b \in K^E, d(a, b) = \operatorname{wt}(b - a).$$

The Hamming distance is a metric over K^E.

Definition 32. Let C be an $[n, k]$-code over K with $k > 0$. We define

$$d(C) = \min_{a,b \in C \text{ and } a \neq b} d(a, b) = \min_{c \in C \text{ and } c \neq 0} \operatorname{wt}(c)$$

as the *minimum distance* of C. We also define the *rate* and the *relative distance* of C

$$\rho(C) = \frac{k}{n} \text{ and } \delta(C) = \frac{d(C)}{n}.$$

In the case where $d \in \mathbb{N}$ is the minimum distance of C, we say that C is an $[n, k, d]$-code over K. We call the *correction capacity* of C the integer $t(C) = \lfloor \frac{d-1}{2} \rfloor$.

The minimum distance, dimension, and length of a linear code are related as follows:

Theorem 23 (Singleton bound)**.** *Let C be an $[n, k, d]$-code over K, then*

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

If the above inequality is an equality, then C is said to be MDS *(Maximum Distance Separable).*

Let F be a set of cardinality k. We denote by $\mathcal{M}_{F,E}(K)$ the K-vector space of matrices indexed by $F \times E$. In the case where $F = [1..k]$, we will write $\mathcal{M}_{k,E}(K)$ instead of $\mathcal{M}_{F,E}(K)$. In the case where $E = [1..n]$, we will write $\mathcal{M}_{F,n}(K)$ instead of $\mathcal{M}_{F,E}(K)$.

To represent a matrix of $\mathcal{M}_{F,E}(K)$ as a table of coefficients, we must fix an order on the elements of F and E. By convention, if E or F are sets of integers, we will systematically choose the natural order on the integers.

Let G be a finite set. Recall the definition of the matrix product

$$\begin{array}{ccc} \mathcal{M}_{F,E}(K) \times \mathcal{M}_{E,G}(K) & \longrightarrow & \mathcal{M}_{F,G}(K) \\ ((m_{i,j})_{(i,j) \in F \times E}, (m'_{i,j})_{(i,j) \in E \times G}) & \longmapsto & (\sum_{e \in E} m_{i,e} m'_{e,j})_{(i,j) \in F \times G} \end{array}$$

Let $C \subset K^E$ be an $[n, k]$-code over K. There exists a matrix $\mathcal{E} \in \mathcal{M}_{F,E}(K)$ such that

$$C = \{a\mathcal{E}; a \in K^F\}.$$

We say that $\mathcal{E}$ is a *generator matrix* of C. Let G be a set of cardinality $n-k$. There exists a matrix $\mathcal{C} \in \mathcal{M}_{E,G}(K)$ such that

$$C = \{a \in K^E \mid a\mathcal{C} = 0\}.$$

We say that $\mathcal{C}$ is a *parity-check matrix* of C. We have

$$\mathcal{E}\mathcal{C} = 0.$$

The vector space K^E is naturally equipped with a non-degenerate symmetric bilinear form:

$$\langle ., . \rangle : a, b \in K^E \mapsto \sum_{i \in E} a_i b_i. \tag{4.1.1}$$

We then define the dual code $C^\perp$ of C by

$$C^\perp = \{a \in K^E \mid \forall c \in C, \langle a, c \rangle = 0\}.$$

If C is an $[n,k]$-code, then $C^\perp$ is an $[n, n-k]$-code. The generator matrices of $C^\perp$ are the transpose of the parity-check matrices of C, and vice versa.

4.1.2 Families of linear codes

Let $(C_i)_{i \in \mathbb{N}}$ be a family of codes with lengths tending to infinity. We write

$$\delta_{lim} = \liminf \delta(C_i) \text{ and } \rho_{lim} = \liminf \rho(C_i).$$

Then Singleton's bound implies that

$$\delta_{lim} + \rho_{lim} \leqslant 1.$$

One of the objectives of coding theory is to produce codes that come as close as possible to this bound. A classic result is the following:

Theorem 24 (Gilbert–Varshamov bound)**.** *Let $\delta_{lim} \in]0, 1 - q^{-1}[$, there exists $(C_i)_{i \in \mathbb{N}}$ a family of linear codes over K whose lengths tend to infinity such that $\liminf \delta(C_i) = \delta_{lim}$ and*

$$\rho_{lim} = \liminf \rho(C_i) = 1 - H_q(\delta_{lim}),$$

where

$$H_q : x \longmapsto x \log_q(q-1) - x \log_q(x) - (1-x) \log_q(1-x).$$

Remark 9. This bound is reached by families of random codes (whose lengths tend to infinity).

One naturally might ask whether there exist families of codes whose parameters are better than those of the Gilbert-Varshamov theorem. More precisely, let $\delta_{lim} \in]0, 1 - q^{-1}[$, is there a family of linear codes $(C_i)_{i \in \mathbb{N}}$ over K whose lengths tend to infinity and such that

$$\liminf \delta(C_i) = \delta_{lim} \text{ and } \liminf \rho(C_i) > 1 - H_q(\delta_{lim}) \ ?$$

This question motivates the following definitions (see [Lac86]).

Definition 33. Let $(C_i)_{i\in\mathbb{N}}$ be a family of linear codes over K whose lengths tend to infinity. We say that $(C_i)_{i\in\mathbb{N}}$ is a family of *good codes* if

$$\liminf \delta(C_i) > 0 \text{ and } \liminf \rho(C_i) > 0.$$

Definition 34. Let $(C_i)_{i\in\mathbb{N}}$ be a family of good linear codes over K. Let $\delta_{lim} = \liminf \delta(C_i)$. Assume that $\delta_{lim} \in]0, 1 - q^{-1}[$. We say that $(C_i)_{i\in\mathbb{N}}$ is a family of *excellent codes* if

$$\liminf \rho(C_i) > 1 - H_q(\delta_{lim}).$$

4.1.3 The decoding problem

To conclude this section, we present the decoding problem for linear codes. Let $C \subset K^E$ be an $[n, k, d]$-code over K. Let c be a codeword of C and $e \in K^E$. Let $t > 0$ be an integer, we assume that

$$\mathrm{wt}(e) \leqslant t \leqslant t(C) = \lfloor (d-1)/2 \rfloor.$$

Finally, let

$$r = c + e.$$

The decoding problem is as follows: given C, r and t, determine c, the unique codeword C at distance at most t from r.

The decoding problem is an NP-hard problem [BMvT78]. However, when the decoding problem is restricted to certain families of codes, it can be solved in polynomial time with respect to the length of the code. In particular, we will see in section 4.2.3 that this is the case for Goppa codes.

4.2 Geometric Goppa codes

Geometric Goppa codes, also known as AG codes, are a specific family of linear codes introduced by Goppa in the early 1980s [Gop83] to generalize Reed–Solomon codes [RS60]. Geometric Goppa codes have good asymptotic properties and beat the Gilbert-Varshamov bound when q, the cardinality of the base field, is large enough. The reader can refer to [Sti08] for a detailed study of AG codes.

We start by introducing Reed-Solomon codes. Let K be a finite field with $q = p^m$ elements. Let k and n be two integers such that $0 < k \leqslant n \leqslant q$. Let $P_1, \ldots, P_n \in K$ be distinct elements. We define

$$P = \{P_i; 1 \leqslant i \leqslant n\}.$$

Let $K[x]_{\leqslant k-1}$ be the set of polynomials in one indeterminate over K of degree less than $k-1$. This is obviously a K-vector space of dimension k. Let us consider the K-linear evaluation map at P

$$\mathrm{ev}_P : f \in K[x]_{\leqslant k-1} \longmapsto (f(P_i))_{P_i \in P} \in K^P.$$

This map is injective since a nonzero polynomial $f \in K[x]_{\leqslant k-1}$ has at most $k-1 < n$ roots. Using the canonical isomorphism of K-vector spaces

$$\begin{array}{rccc} \varphi : & K^k & \longrightarrow & K[x]_{\leqslant k-1} \\ & (f_i)_{0 \leqslant i \leqslant k-1} & \longmapsto & \sum_{i=0}^{k-1} f_i x^i \end{array}$$

we can define a $[n,k]$-Reed-Solomon code (or RS code) with generator matrix $\mathcal{E}$ corresponding to the linear map $\mathrm{ev}_P \circ \varphi$ in the canonical bases of K^k and K^P:

$$\mathcal{E} = \begin{pmatrix} 1 & 1 & & 1 \\ P_1 & P_2 & & P_n \\ P_1^2 & P_2^2 & \cdots & P_n^2 \\ \vdots & \vdots & & \vdots \\ P_1^{k-1} & P_2^{k-1} & & P_n^{k-1} \end{pmatrix} \in \mathcal{M}_{k,P}(K).$$

We thus define

$$\mathrm{RS}(k,P) = \mathrm{Im}\ \mathcal{E} = \{(f(P_i))_{P_i \in P}; f \in K[x]_{\leqslant k-1}\}.$$

Proposition 25. $\mathrm{RS}(k,P)$ is an MDS code. In other words,

$$d(\mathrm{RS}(k,P)) = n - k + 1.$$

RS codes are interesting because they reach the Singleton bound. In addition, they have good algorithmic properties. Their main drawback is their length: Reed-Solomon codes cannot be longer than q, which makes them relatively short codes. Goppa's idea in introducing geometric codes was to generalize Reed-Solomon codes in a situation where more evaluation points are available.

4.2.1 Definition

Let K be a finite field with $q = p^m$ elements. Let X be a smooth projective curve over K, and let $K(X)$ be its function field. Let g be the genus of X. Let $P_1, \ldots, P_n \in X(K)$ be K-rational points of X that are pairwise distinct, and

$$P = \sum_{i=1}^{n} P_i \in \mathrm{Div}(X).$$

Let $D \in \mathrm{Div}(X)$ be a divisor with non-negative degree such that $\mathrm{supp}\, D \cap \mathrm{supp}\, P = \emptyset$. We write

$$\mathcal{L}(D) := \Gamma_X(\mathcal{O}_X(D))$$

for the Riemann-Roch space associated with D, and $\ell(D)$ for its dimension as a K-vector space. We also write

$$\mathbf{R}_P := \Gamma_X(\mathcal{O}_X/\mathcal{O}_X(-P))$$

for the residue algebra at P. We will write K^P instead of $K^{\operatorname{supp} P}$. We write

$$\operatorname{ev}_{D,P} : \mathcal{L}(D) \longrightarrow \mathbf{R}_P$$

for the evaluation map of functions from the Riemann-Roch space $\mathcal{L}(D)$ to P. In this particular case, there is a canonical isomorphism of K-vector spaces

$$\mathbf{R}_P \simeq \bigoplus_{i=1}^{n} K_{P_i}$$

between the residue algebra at P and the direct sum of the residue fields at the places P_i. Since the places P_i are K-rational, these residue fields are naturally isomorphic to K. We can then define the geometric Goppa code associated with D and P:

$$\operatorname{Gop}(P, D) = \{(f(P_i))_{P_i \in P} \in K^P ; f \in \mathcal{L}(D)\} \simeq \operatorname{Im} \operatorname{ev}_{D,P}.$$

The map $\operatorname{ev}_{D,P}$ is generally not injective. Its kernel is $\mathcal{L}(D - P)$. We can deduce the following property:

Proposition 26. Using the previous notation,

$$\dim(\operatorname{Gop}(P, D)) = \ell(D) - \ell(D - P).$$

In particular, if $2g - 1 \leqslant \deg D \leqslant n - 1$, Riemann–Roch's theorem implies that

$$\dim(\operatorname{Gop}(P, D)) = \deg D - g + 1.$$

Let $k = \dim(\operatorname{Gop}(P, D))$. If $k > 0$, we can give an estimate of the minimum distance of $\operatorname{Gop}(P, D)$:

Proposition 27. Using the previous notation, if $k > 0$

$$d(\operatorname{Gop}(P, D)) \geqslant n - \deg D.$$

In particular, if $2g - 1 \leqslant \deg D \leqslant n - 1$,

$$d(\operatorname{Gop}(P, D)) \geqslant n - k - g + 1.$$

Indeed, let $f \in \mathcal{L}(D)$, such that f vanishes at $\deg D + 1$ places of P. Let P' be the divisor of degree $\deg D + 1$ composed of the places P_i where f vanishes, then $f \in \mathcal{L}(D - P')$ because $\operatorname{supp} D \cap \operatorname{supp} P' = \emptyset$. Now $\deg(D - P') = -1$, so f must be zero.

We write

$$d^*(P, D) = n - \deg D \tag{4.2.1}$$

the *designed distance* of the code $\operatorname{Gop}(P, D)$. Proposition 27 shows that AG codes are close to being MDS. In the special case $g = 0$, they always are (for instance, Reed-Solomon codes). We define

$$t^*(P, D) = \left\lfloor \frac{d^*(P, D) - 1}{2} \right\rfloor \tag{4.2.2}$$

the *designed correction capacity* of $\mathrm{Gop}(P, D)$.

In the case where $\deg D \leqslant n-1$, the map $\mathrm{ev}_{D,P}$ is injective, and we can define a generator matrix $\mathcal{E}_{D,P}$ of the code $\mathrm{Gop}(P, D)$. It is not canonical since there is generally no canonical basis for $\mathcal{L}(D)$. Let $f_1, \ldots, f_k$ be a basis for $\mathcal{L}(D)$, we set

$$\mathcal{E}_{D,P} = \begin{pmatrix} f_1(P_1) & f_1(P_2) & & f_1(P_n) \\ f_2(P_1) & f_2(P_2) & & f_2(P_n) \\ f_3(P_1) & f_3(P_2) & \cdots & f_3(P_n) \\ \vdots & \vdots & & \vdots \\ f_k(P_1) & f_k(P_2) & & f_k(P_n) \end{pmatrix} \in \mathcal{M}_{k,P}(K).$$

The dual codes of AG codes also are geometric in nature. Indeed, the K-vector space $\mathbf{R}_P$ is dual to the K-vector space

$$\Omega_P := \Gamma_X(\Omega_{X/K}(-P)/\Omega_{X/K})$$

via the K-bilinear form

$$\begin{array}{rccc} \langle ., . \rangle_X : & \mathbf{R}_P \times \Omega_P & \longrightarrow & K \\ & (f, \omega) & \longmapsto & \sum_{i=1}^{n} \mathrm{Res}_{P_i}(f\omega) \end{array} \tag{4.2.3}$$

where $\mathrm{Res}_{P_i}(f\omega)$ denotes the residue at P_i of $f\omega$.

Remark 10. The notation in equation (4.2.3) is slightly misleading, so let us clarify our point. The sheaf $\mathcal{O}_X/\mathcal{O}_X(-P)$ has a finite number of non-zero stalks, the stalks at the points $(P_i)_{i\in[1..n]}$ of P. Furthermore, for $i \in [1..n]$, the stalk of $\mathcal{O}_X/\mathcal{O}_X(-P)$ at P_i is

$$\mathcal{O}_{P_i}/P_i = K_{P_i}.$$

We then know that an element f of $\mathbf{R}_P = \Gamma_X(\mathcal{O}_X/\mathcal{O}_X(-P))$ is exactly the data of its germs

$$f_i \in \mathcal{O}_{P_i}/P_i$$

for all $i \in [1..n]$. Let $\tilde{f}_i \in \mathcal{O}_{P_i}$ be such that

$$\tilde{f}_i \bmod P_i = f_i.$$

Similarly, given $\omega \in \Omega_P$, we can determine $(\tilde{\omega_i})_{i\in[1..n]}$ a family of differentials of $\Omega(X/K)$ such that

$$\nu_{P_i}(\tilde{\omega_i}) \geqslant -1$$

describing the germ of ω at $(P_i)_{i\in[1..n]}$. Then we can check that for all $i \in [1..n]$, the residue $\mathrm{Res}_{P_i}(\tilde{f}_i\tilde{\omega_i})$ depends only on f and ω. We therefore denote it by $\mathrm{Res}_{P_i}(f\omega)$.

Since the $(P_i)_{i\in[1..n]}$ are K-rational, we know that the residue fields $(K_{P_i})_{i\in[1..n]}$ are naturally isomorphic to K. Thus, the bilinear map in equation (4.2.3) corresponds to the canonical bilinear form $\langle ., . \rangle$ on K^P via the natural isomorphisms

$$\begin{array}{ccc} \mathbf{R}_P & \longrightarrow & K^P \\ f & \longmapsto & (f(P_i))_{P_i \in P} \end{array}$$

and

$$\begin{array}{ccc} \Omega_P & \longrightarrow & K^P \\ \omega & \longmapsto & (\mathrm{Res}_{P_i}(\omega))_{P_i \in P} \end{array}.$$

Equation (4.2.3) motivates the definition of codes based on differential spaces. For any divisor D' of X, we define

$$\Omega(D') := \Gamma_X(\Omega_{X/K}(D'))$$

and $\iota(D')$ its dimension as a K-vector space (or equivalently the index of specialty of D'). Since D and P are disjoint, we have a map

$$\mathrm{res}_{D,P} : \Omega(D-P) \longrightarrow \Omega_P. \tag{4.2.4}$$

The image of $\mathrm{res}_{D,P}$ in Ω_P is the orthogonal of the image of $\mathrm{ev}_{D,P}$, for the bilinear form $\langle ., . \rangle_X$.

We can define

$$\begin{aligned} \mathrm{Gop}_\Omega(P, D) &= \{(\mathrm{Res}_{P_i}(\omega))_{P_i \in P} \in K^P ; \omega \in \Omega(D-P)\} \\ &\simeq \mathrm{Im}\ \mathrm{res}_{D,P} \end{aligned}$$

Proposition 28. Using previous notation,

$$\mathrm{Gop}_\Omega(P, D) = \mathrm{Gop}(P, D)^\perp.$$

In particular, if $2g - 1 \leqslant \deg D \leqslant n - 1$, then the map $\mathrm{res}_{D,P}$ is injective and

$$\begin{aligned} \dim \mathrm{Gop}_\Omega(P, D) = \dim \Omega(D-P) &= \iota(D-P) \\ &= n - \deg D + g - 1 \\ &= n - k. \end{aligned}$$

Given a basis $(\omega_1, \ldots, \omega_{n-k})$ of $\Omega(D-P)$, we have a generator matrix of $\mathrm{Gop}_\Omega(P, D)$:

$$\mathcal{C}_{D,P} = \begin{pmatrix} \mathrm{Res}_{P_1}(\omega_1) & \mathrm{Res}_{P_2}(\omega_1) & & \mathrm{Res}_{P_n}(\omega_1) \\ \mathrm{Res}_{P_1}(\omega_2) & \mathrm{Res}_{P_2}(\omega_2) & & \mathrm{Res}_{P_n}(\omega_2) \\ \mathrm{Res}_{P_1}(\omega_3) & \mathrm{Res}_{P_2}(\omega_3) & \cdots & \mathrm{Res}_{P_n}(\omega_3) \\ \vdots & \vdots & & \vdots \\ \mathrm{Res}_{P_1}(\omega_{n-k}) & \mathrm{Res}_{P_2}(\omega_{n-k}) & & \mathrm{Res}_{P_n}(\omega_{n-k}) \end{pmatrix} \in \mathcal{M}_{n-k,P}(K).$$

In particular, ${\mathcal{C}_{D,P}}^t$ is a parity-check matrix of $\mathrm{Gop}(P, D)$ (where $.^t$ denotes the transpose of matrices).

Remark 11. It is possible to generalize the definitions of this section to the case where

$$\mathrm{supp}\, D \cap \mathrm{supp}\, P \neq \emptyset.$$

Indeed, the quotient maps

$$\mathcal{L}(D) \longrightarrow \Gamma_X(\mathcal{O}_X(D)/\mathcal{O}_X(D-P))$$

and

$$\Omega(D-P) \longrightarrow \Gamma_X(\Omega_{X/K}(D-P)/\Omega_{X/K}(D))$$

offer alternatives to $\mathrm{ev}_{D,P}$ and $\mathrm{res}_{D,P}$ in this context. On the other hand, there are no longer any natural isomorphisms between $\Gamma_X(\mathcal{O}_X(D)/\mathcal{O}_X(D-P))$ or $\Gamma_X(\Omega_{X/K}(D-P)/\Omega_{X/K}(D))$ and K^P.

This problem is solved with ease. It is sufficient to find two isomorphisms,

$$\varphi\colon \Gamma_X(\mathcal{O}_X(D)/\mathcal{O}_X(D-P)) \longrightarrow K^P$$

and

$$\psi\colon \Gamma_X(\Omega_{X/K}(D-P)/\ Omega_{X/K}(D)) \longrightarrow K^P,$$

such that, for all

$$f \in \Gamma_X(\mathcal{O}_X(D)/\mathcal{O}_X(D-P)) \text{ and } \omega \in \Gamma_X(\Omega_{X/K}(D-P)/\ Omega_{X/K}(D)),$$

we have

$$\langle \varphi(f), \psi(\omega) \rangle = \sum_{i=1}^{n} \mathrm{Res}_{P_i}(f\omega),$$

where $\langle ., . \rangle$ denotes the natural K-bilinear form on K^P defined in equation (4.1.1). It is easy to construct such isomorphisms, using uniformizers at the points $P_i \in \operatorname{supp} P \cap \operatorname{supp} D$.

4.2.2 Asymptotic properties

Let K be a finite field with $q = p^m$ elements. To find an interesting family of AG codes, we look for smooth projective curves $(X_i)_{i\in\mathbb{N}}$ over K with a large number of K-rational points relatively to their genera. The quantity we are interested in is therefore the Ihara constant

$$A(q) = \limsup \frac{\#X(K)}{g_X}$$

where g_X denotes the genus of X. In Section 3.4, we discussed the defect of the Weil bound when the genus tends to infinity. Theorem 29 illustrates this.

Theorem 29 (Drinfeld–Vladut bound [VD83])**.** *Using the previous notation,*

$$A(q) \leqslant \sqrt{q} - 1.$$

This inequality holds for any prime power $q = p^m$. In the case where m is even, i.e., q is a square, the constructions of [Iha81] and [TVZ82] show that $A(q) = \sqrt{q} - 1$.

We use this result to define a family of AG codes. Let $(X_i)_{i\in\mathbb{N}}$ be a family of smooth projective curves of increasing genus g_{X_i}, such that

$$\lim \#X_i(K)/g_{X_i} = \sqrt{q} - 1.$$

For all $i \in \mathbb{N}$, let $n_i = \#X_i(K)$ and let $P_{i,1}, \ldots, P_{i,n_i}$ be K-rational points of X_i and

$$P_i = P_{i,1} + \cdots + P_{i,n_i}.$$

Let D_i be a divisor of X_i such that $2g_{X_i} - 1 \leqslant \deg D_i \leqslant n_i - 1$. Let

$$C_i = \mathrm{Gop}(P_i, D_i).$$

Then

$$\rho(C_i) = \frac{\deg D_i - g_{X_i} + 1}{n_i} \text{ and } \delta(C_i) \geqslant \frac{n_i - \deg D_i}{n_i},$$

and therefore

$$\rho(C_i) \geqslant \frac{n_i - g_{X_i} + 1}{n_i} - \delta(C_i).$$

In the case where $\deg D_i / g_{X_i}$ converges, setting $\delta_{lim} = \lim \delta(C_i)$ and $\rho_{lim} = \lim \rho(C_i)$, we obtain

$$\rho_{lim} \geqslant 1 - \frac{1}{\sqrt{q} - 1} - \delta_{lim}. \tag{4.2.5}$$

We see that this family of codes closely approximates the Singleton bound when q is large. In fact, when $q \geqslant 49$, the lower bound (4.2.5) is sometimes better than the Gilbert-Varshamov bound.

Theorem 30 (Tsfasman–Vladut–Zink bound[TVZ82])**.** *Using the previous notation, if q is a square and $q \geqslant 49$, there exist $0 < \delta_1 \leqslant \delta_2 < 1 - \frac{1}{q}$ such that for all $x \in [\delta_1, \delta_2]$,*

$$1 - \frac{1}{\sqrt{q} - 1} - x \geqslant 1 - H_q(x).$$

These results show that there exists excellent families of AG codes. More precisely, there exists excellent families of AG codes over K if q is a square and $q \geqslant 49$.

4.2.3 Decoding geometric codes

In the early 1990s, a significant number of contributions aiming at generalizing Reed-Solomon decoding algorithms to AG codes were proposed. The first algorithm was the so-called basic algorithm, generalizing the algorithms of Arimoto [Ari61] and Peterson [Pet60], first developed by Justesen, Larsen, Elbrønd Jensen, Havemose, and Høholdt [Hav89, JLJ+89] in the case of plane curves, then by Skorobogatov and Vladut in the general case [SV90]. Sugiyama, Kasahara, Hirasawa, and Namekawa [SKHN75] developed an algorithm based on Euclid's algorithm, which was then generalized by Porter [Por88]. These algorithms have the disadvantage of not decoding AG codes up to their designed correction capacity. Ehrhard's algorithm [Ehr93] improves on the basic algorithm and allows decoding up to the designed correction capacity. Another approach, developed by Feng and Rao [FR93] and Duursma [Duu93], uses syndrome decoding and also allows AG codes to be decoded up to

their designed correction capacity. For more details on these algorithms, the reader can refer to the excellent state-of-the-art reviews by Høholdt and Pellikaan [HP95] and Beelen and Høholdt [BH08].

Here we present the basic algorithm for solving the decoding problem (see Subsection 4.1.3). Let K be a finite field with $q = p^m$ elements. Let X be a smooth projective curve over K. Let $P_1, \ldots, P_n$ be distinct K-rational points of X and $P = \sum_{i=1}^{n} P_i$. Let g be the genus of X and $D \in \operatorname{Div} X$ a divisor such that

$$\operatorname{supp} D \cap \operatorname{supp} P = \emptyset \text{ and } 2g - 1 \leqslant \deg D \leqslant n - 1.$$

We give a decoding algorithm for $\operatorname{Gop}(P, D)$.

Let $c \in \operatorname{Gop}(P, D)$ and $e \in K^P$ such that $\operatorname{wt}(e) \leqslant t^*(P, D)$ (the designed correction capacity defined in equation (4.2.2)). Let $r = c+e$, our goal is to recover the codeword c from the data r. Using the natural isomorphism between K^P and $\mathbf{R}_P$, we obtain $f_r, f_c, f_e \in \mathbf{R}_P$, such that

$$f_r = f_c + f_e \in \mathbf{R}_P, \ \ f_c \in \operatorname{Im} \operatorname{ev}_{D,P} \text{ and } \# \operatorname{supp} f_e \leqslant t^*(P, D).$$

We write $P_{\text{err}} = \operatorname{supp} f_e$ for the sum divisor of the P_i at which f_e does not vanish, and $t = \deg P_{\text{err}}$. The objective is to find a function h that vanishes on P_{err}. This function will help us locate the positions of the errors.

Let F be a divisor such that

$$\deg F \geqslant g + t \text{ and } \operatorname{supp} F \cap \operatorname{supp} P = \emptyset. \tag{4.2.6}$$

Then $\mathcal{L}(F - P_{\text{err}}) \neq \{0\}$ according to the Riemann-Roch theorem, because $\deg(F - P_{\text{err}}) \geqslant g$. There is therefore at least one function in $\mathcal{L}(F)$ that vanishes on P_{err}. It remains to give a way of determining such a function.

Let $h \in \mathcal{L}(F)$ be any function. It is clear that h induces K-linear maps

$$\begin{array}{rccc} m_{D,h} : & \mathcal{L}(D) & \longrightarrow & \mathcal{L}(D+F) \\ & s & \longmapsto & hs \end{array}$$

and

$$\begin{array}{rccc} m_{P,h} : & \mathbf{R}_P & \longrightarrow & \mathbf{R}_P \\ & s & \longmapsto & \operatorname{ev}_{F,P}(h)s \end{array}$$

making the following diagram commutative:

$$\begin{array}{ccc} \mathcal{L}(D) & \xrightarrow{\operatorname{ev}_{D,P}} & \mathbf{R}_P \\ \Big\downarrow{\scriptstyle m_{D,h}} & & \Big\downarrow{\scriptstyle m_{P,h}} \\ \mathcal{L}(D+F) & \xrightarrow[\operatorname{ev}_{D+F,P}]{} & \mathbf{R}_P \end{array}$$

If $h \in \mathcal{L}(F - P_{\text{err}})$, then $hf_e = 0$ and $hf_r = hf_c \in \text{Im ev}_{D+F,P}$. We want to ensure that the converse is true, i.e., that if $hf_r \in \text{Im ev}_{D+F,P}$ then $h \in \mathcal{L}(F - P_{\text{err}})$. To do this, we will need to make a second assumption about F (and about t).

Assume that $h \in \mathcal{L}(F)$ is such that $hf_r \in \text{Im ev}_{D+F,P}$. Equivalently, $hf_e \in \text{Im ev}_{D+F,P}$, so there exists a function $a \in \mathcal{L}(D + F)$ such that

$$\text{ev}_{D+F,P}(a) = \text{ev}_{F,P}(h)f_e.$$

In particular, a vanishes on $P - P_{\text{err}}$ (because f_e does), so $a \in \mathcal{L}(D + F - P + P_{\text{err}})$. Since we want to prove $a = 0$, it is sufficient to show that

$$\mathcal{L}(D + F - P + P_{\text{err}}) = \{0\}.$$

A sufficient condition on F is then

$$\deg F \leqslant n - 1 - \deg D - t. \tag{4.2.7}$$

Thus, if

$$g + t \leqslant \deg F \leqslant n - 1 - \deg D - t,$$

then we can determine $\mathcal{L}(F - P_{\text{err}})$ by computing

$$\{h \in \mathcal{L}(F) \mid hf_r \in \text{Im ev}_{D+F,P}\}.$$

We define the diagonal matrix $\mathcal{D}_r$ of the multiplication by f_r in $\mathbf{R}_P$. The computation of $\mathcal{L}(F - P_{\text{err}})$ then reduces to the computation of the left kernel of

$$\mathcal{E}_{F,P} \times \mathcal{D}_r \times {\mathcal{C}_{D+F,P}}^t \in \mathcal{M}_{\ell(F),(n-\ell(D+F))}(K)$$

where $\mathcal{E}_{F,P}$ is a generator matrix of $\text{Gop}(F, P)$ and $\mathcal{C}_{D+F,P}$ is a generator matrix of $\text{Gop}_\Omega(D+F, P)$.

Let us now consider $h \in \mathcal{L}(F - P_{\text{err}})$. Let P_h be the sum divisor of the P_i where h vanishes, then $P_{\text{err}} \leqslant P_h$. In particular, the restriction of f_r to $\mathbf{R}_{P-P_h}$ is in the image of the map $\text{ev}_{D,P-P_h}$, and is equal to the restriction of f_c. In order to recover f_c, $\text{ev}_{D,P-P_h}$ must be injective. It is sufficient to assume that

$$\deg D \leqslant \deg(P - P_h) - 1.$$

Now $\deg(P - P_h) \geqslant n - \deg F$, so it is sufficient that

$$\deg F \leqslant n - \deg D - 1. \tag{4.2.8}$$

This condition is weaker than condition (4.2.7).

The conditions of equations (4.2.6) and (4.2.7) on the degree of F imply that

$$0 \leqslant n - 1 - \deg D - g - 2t,$$

or equivalently

$$t \leqslant \frac{d^*(P,D) - 1 - g}{2}.$$

In particular, it is generally not possible to decode up to the designed correction capacity $t^*(P,D)$. On the other hand, this algorithm is essentially a matrix kernel computation (once certain precomputations have been performed) whose time and space complexities are polynomial. In particular, the time complexity of the decoding algorithm is at most that of the matrix multiplication in $\mathcal{M}_n(K)$ [BCG+17, Theorem 8.5].

4.3 Discrete Fourier transform

The objective of this section is to estimate the cost of a multiplication in $K[G]$ for K a field and G a finite abelian group. To do this, we must study more generally the Fourier transform in $A[G]$ for any commutative K-algebra A.

4.3.1 Definitions and properties

Let K be a field. Let A be a commutative K-algebra and G a finite group. We denote by $A[G]$ the ring which, equipped with its addition, forms the free A-module generated by G

$$\left\{ \sum_{\sigma \in G} \alpha_\sigma \sigma ; \alpha := (\alpha_\sigma)_{\sigma \in G} \in A^G \right\},$$

and equipped with the convolution product

$$\left(\sum_{g \in G} \alpha_g g \right) \left(\sum_{h \in G} \beta_h h \right) = \sum_{g,h \in G} \alpha_g \beta_h gh = \sum_{\sigma \in G} \left(\sum_{\tau \in G} \alpha_\tau \beta_{\tau^{-1}\sigma} \right) \sigma.$$

We call $A[G]$ the group algebra of G over A. Note that $A[G]$ is generally not a commutative K-algebra, but it is if G is abelian.

We note that G injects canonically into $A[G]^\times$. In particular,

$$1_G = 1_{A[G]}.$$

Furthermore, A injects canonically into $A[G]$ via the map $a \mapsto a1_G$.

Let G' be a finite group and $\chi : G \longrightarrow G'$ a group morphism, then χ extends by A-linearity to an A-algebra morphism

$$\begin{array}{rccc} \tilde{\chi} : & A[G] & \longrightarrow & A[G'] \\ & \sum_{\sigma \in G} \alpha_\sigma \sigma & \longmapsto & \sum_{\sigma \in G} \alpha_\sigma \chi(\sigma) \end{array}$$

and we will denote $\tilde{\chi}$ by χ, in a slightly abusive manner. In particular, if $G' = A^\times$, then χ induces an evaluation morphism

$$\mathrm{ev}_\chi : A[G] \longrightarrow A$$

by viewing the formal sum in $A[A^\times]$ as a sum in A.

Similarly, let B be a commutative K-algebra and $\varphi : A \longrightarrow B$ a morphism of K-algebras, then there exists a unique morphism of K-algebras

$$\begin{array}{rccc} \tilde{\varphi}: & A[G] & \longrightarrow & B[G] \\ & \sum_{\sigma\in G} \alpha_\sigma \sigma & \longmapsto & \sum_{\sigma\in G} \varphi(\alpha_\sigma)\sigma \end{array}$$

extending φ. We will refer to $\tilde{\varphi}$ as φ, in a slightly abusive manner.

As an A-module, $A[G]$ is canonically isomorphic to A^G via the isomorphism of A-modules

$$\begin{array}{rccc} \mathsf{T}: & A^G & \longrightarrow & A[G] \\ & \alpha & \longmapsto & \sum_{\sigma\in G} \alpha(\sigma)\sigma \end{array}$$

Let K be a finite field with $q = p^m$ elements, A a finite-dimensional commutative K-algebra, and G a finite group. We represent the elements of $A[G]$ algorithmically in a natural manner, that is, as a set of pairs $(\alpha_\sigma, \sigma)_{\sigma\in G}$.

4.3.2 Fourier transform

Let K be a field, A a commutative K-algebra, and G a finite abelian group. Let

$$\mathfrak{o} = |G|$$

be the order of the group G and $\mathfrak{e}$ its exponent. We assume that K contains a primitive $\mathfrak{e}$-th root of unity, which implies that $\mathfrak{e}$ and $\mathfrak{o}$ are nonzero in K. Let

$$\hat{G} = \mathrm{Hom}(G, K^\times)$$

be the dual group of G. In particular, $\hat{G}$ is a group, so we can define, as before, the algebra $A[\hat{G}]$ and the isomorphism of free A-modules $\hat{\mathsf{T}} : A^{\hat{G}} \longrightarrow A[\hat{G}]$.

We define the morphisms of A-algebras

$$\begin{array}{rccc} \mathrm{FT}_G: & A[G] & \longrightarrow & A^{\hat{G}} \\ & \sum_{\sigma\in G} \alpha_\sigma \sigma & \longmapsto & \left(\chi \mapsto \sum_{\sigma\in G} \alpha_\sigma \chi(\sigma)\right) \end{array}$$

and

$$\begin{array}{rccc} \mathrm{FT}_{\hat{G}}: & A[\hat{G}] & \longrightarrow & A^G \\ & \sum_{\chi\in\hat{G}} \alpha_\chi \chi & \longmapsto & \left(\sigma \mapsto \sum_{\chi\in\hat{G}} \alpha_\chi \chi(\sigma)\right) \end{array}$$

where A^G and $A^{\hat{G}}$ are endowed with component-wise multiplication. We call these maps the Fourier transforms of G and $\hat{G}$. We will see that these maps are close to being inverse to one another.

Proposition 31. Using the notation above, let

$$\iota : A[G] \longrightarrow A[G]$$

be the extension of inversion in G by A-linearity, then

$$\mathsf{T} \circ \mathrm{FT}_{\hat{G}} \circ \hat{\mathsf{T}} \circ \mathrm{FT}_G = \mathfrak{o}\iota.$$

In particular, FT_G and $\mathrm{FT}_{\hat{G}}$ are isomorphisms of algebras.

Proof. By A-linearity, it is enough to show that the image of σ is $\mathfrak{o}\sigma^{-1}$ for all $\sigma \in G$. Let $\sigma \in G$. Then

$$\hat{\mathsf{T}} \circ \mathrm{FT}_G(\sigma) = \sum_{\chi \in \hat{G}} \chi(\sigma)\chi,$$

and therefore

$$\mathrm{FT}_{\hat{G}} \circ \hat{\mathsf{T}} \circ \mathrm{FT}_G(\sigma) = \left(\sigma' \mapsto \sum_{\chi \in \hat{G}} \chi(\sigma)\chi(\sigma') \right).$$

Let $\sigma' \in G$, then

$$\sum_{\chi \in \hat{G}} \chi(\sigma)\chi(\sigma') = \sum_{\chi \in \hat{G}} \chi(\sigma\sigma').$$

Let $\mathfrak{o}_{\sigma\sigma'}$ be the order of $\sigma\sigma'$, and let $\zeta_{\mathfrak{o}_{\sigma\sigma'}}$ be a primitive $\mathfrak{o}_{\sigma\sigma'}$-th root of unity in K (which exists because K contains the $\mathfrak{e}$-th roots of unity). We have

$$\sum_{\chi \in \hat{G}} \chi(\sigma\sigma') = \frac{\mathfrak{o}}{\mathfrak{o}_{\sigma\sigma'}} \sum_{i=1}^{\mathfrak{o}_{\sigma\sigma'}} \zeta_{\mathfrak{o}_{\sigma\sigma'}}^{i} \in K.$$

This sum is 0 if $\zeta_{\mathfrak{o}_{\sigma\sigma'}} \neq 1$, i.e. if $\sigma' \neq \sigma^{-1}$. We deduce that

$$\mathsf{T} \circ \mathrm{FT}_{\hat{G}} \circ \hat{\mathsf{T}} \circ \mathrm{FT}_G(\sigma) = \mathfrak{o}\sigma^{-1}.$$

□

Remark 12. There is an alternative (but equivalent) definition of the Fourier transform. Let $\alpha \in K^G$, we define the Fourier transform of α

$$\begin{array}{rccc} \hat{\alpha}: & \hat{G} & \longrightarrow & K \\ & \chi & \longmapsto & \frac{1}{\mathfrak{o}} \sum_{\sigma \in G} \alpha(\sigma)\chi(\sigma)^{-1} \end{array}$$

so that α can be decomposed into the basis formed by the characters of G:

$$\alpha = \sum_{\chi \in \hat{G}} \hat{\alpha}(\chi)\chi.$$

This definition is equivalent to composing FT_G with $\frac{1}{\mathfrak{o}}\iota \circ \mathsf{T}$.

From an algorithmic point of view, the map FT_G is very useful because the time complexity of multiplication in $A^{\hat{G}}$ is linear. It can be used to upper bound the time complexity of the multiplication in $A[G]$. Using this method, the time complexity of the multiplication in $A[G]$ is essentially the complexity of evaluating FT_G. Note that we are mostly aiming for the case where K is a finite field, but Theorems 32 and 33 are true for any field with the appropriate roots of unity.

Special case: cyclic groups

In this paragraph only, we assume that G is cyclic. Let ζ be an $\mathfrak{o}$-th root of unity in K and σ a generator of G. Let $\chi \in \hat{G}$ such that $\chi(\sigma) = \zeta$. We can then establish the following isomorphisms of K-algebras:

$$\begin{array}{ccc} A[G] & \longrightarrow & A[x]/(x^{\mathfrak{o}} - 1) \\ \sum_{i=0}^{\mathfrak{o}-1} \alpha_i \sigma^i & \longmapsto & \sum_{i=0}^{\mathfrak{o}-1} \alpha_i x^i \end{array}$$

and

$$\begin{array}{ccc} A^{\hat{G}} & \longmapsto & A^{\mathfrak{o}} \\ (\chi^i \mapsto \alpha_i) & \longmapsto & (\alpha_i)_{0 \leqslant i \leqslant \mathfrak{o}-1} \end{array}$$

The Fourier transform becomes via the isomorphisms of algebras:

$$\begin{array}{rccc} \mathrm{FT}_{\sigma,\zeta} : & A[x]/(x^{\mathfrak{o}} - 1) & \longmapsto & A^{\mathfrak{o}} \\ & f & \longmapsto & (f(\zeta^i))_{0 \leqslant i \leqslant \mathfrak{o}-1} \end{array}$$

Computing the Fourier transform of an element $f \in A[x]/(x^{\mathfrak{o}} - 1)$ therefore consists in performing a multipoint evaluation of f at $(1, \zeta, \ldots, \zeta^{\mathfrak{o}-1})$. This evaluation can be computed quickly if K contains a primitive t-th root of unity for t a power of 2 strictly greater than $3(\mathfrak{o} - 1)$, thanks to an idea from [RSR69, Blu70].

Theorem 32. *Let K be a field, A a commutative K-algebra, and G a finite cyclic group of order $\mathfrak{o} \geqslant 2$. We assume that K contains a primitive $\mathfrak{o}$-th root of unity ζ and a primitive t-th root of unity for t a power of 2 strictly greater than $3(\mathfrak{o} - 1)$. Let $\sigma \in G$ be a generator of G. Let*

$$f = \sum_{i=0}^{\mathfrak{o}-1} f_i x^i \in A[x]/(x^{\mathfrak{o}} - 1).$$

Then $\mathrm{FT}_{\sigma,\zeta}(f)$ can be computed with $O(\mathfrak{o} \log \mathfrak{o})$ additions in A, scalar multiplications in A (by an element of K) and multiplications in K. More precisely, there exists an absolute constant $\mathcal{Q}$ such that $\mathrm{FT}_{\sigma,\zeta}(f)$ can be computed with $\mathcal{Q}\mathfrak{o} \log \mathfrak{o}$ of these operations.

Proof. We show that the computation of $\mathrm{FT}_{\sigma,\zeta}(f)$ reduces in linear time to the multiplication of a polynomial in $K[x]$ with a polynomial in $A[x]$, following the proof in [BCG+17, Proposition 5.10]. We can then conclude by adapting the arguments from [BCG+17, Theorem 2.8, Algorithm 2.3].

For all $0 \leqslant i \leqslant 2\mathfrak{o} - 2$, we set

$$c_i = i(i-1)/2 \text{ and } \beta_i = \zeta^{c_i}.$$

Since $\zeta^{\mathfrak{o}} = 1$, it is enough to compute the $\mathfrak{o}$ powers of ζ ($\mathfrak{o}$ multiplications in K) and use $\beta_i = \zeta^{c_i \bmod \mathfrak{o}}$. We observe that for all $0 \leqslant i, j \leqslant \mathfrak{o} - 1$

$$c_{i+j} = c_i + c_j + ij \text{ and } \beta_{i+j} = \beta_i \beta_j \zeta^{ij}.$$

We set for all $0 \leqslant i \leqslant \mathfrak{o} - 1$

$$h_i = \beta_i^{-1} f_i = \zeta^{-c_i \bmod \mathfrak{o}} f_i.$$

These coefficients can be computed with $\mathfrak{o}$ scalar multiplications in A, since $\zeta \in K$. We then have for all $0 \leqslant i \leqslant \mathfrak{o} - 1$

$$f(\zeta^i) = \sum_{j=0}^{\mathfrak{o}-1} \zeta^{ij} f_j = \beta_i^{-1} \sum_{j=0}^{\mathfrak{o}-1} \beta_{i+j} h_j.$$

The trick is to note that $\sum_{j=0}^{\mathfrak{o}-1} \beta_{i+j} h_j$ is the $(\mathfrak{o} - 1 + i)$-th coefficient of a polynomial. We set

$$h(x) = \sum_{i=0}^{\mathfrak{o}-1} h_{\mathfrak{o}-1-i} x^i \in A[x] \text{ and } b(x) = \sum_{i=0}^{2\mathfrak{o}-2} \beta_i x^i \in K[x] \tag{4.3.1}$$

and

$$r(x) = b(x)h(x) := \sum_{i=0}^{3\mathfrak{o}-3} r_i x^i \in A[x].$$

Then for all $0 \leqslant i \leqslant \mathfrak{o} - 1$

$$r_{fo-1+i} = \sum_{j=0}^{fo-1} \beta_{i+j} h_j \text{ and } f(\zeta^i) = \beta_i^{-1} r_{fo-1+i}.$$

Thus, we have reduced the computation of $\mathrm{FT}_{\sigma,\zeta}(f)$ to the computation of $r(x) = b(x)h(x)$. □

General abelian group

We show that Theorem 32 extends to any finite abelian group.

Theorem 33. *Let K be a field, A a commutative K-algebra, and G a finite abelian group. Let $\mathfrak{o} \geqslant 2$ be the order of G and $\mathfrak{e}$ its exponent. Let t be a power of 2 strictly greater than $3(\mathfrak{e} - 1)$. We assume that K contains primitive $\mathfrak{e}$-th and t-th roots of unity. We assume that we have an explicit decomposition of G into products of cyclic groups*

$$G = C_1 \times \cdots \times C_I$$

of orders $2 \leqslant \mathfrak{o}_1 \mid \cdots \mid \mathfrak{o}_I = \mathfrak{e}$. Then there exists a recursive algorithm evaluating

$$\mathrm{FT}_G : A[G] \longrightarrow A^{\hat{G}}$$

with $O(\mathfrak{o} \sum_{i=0}^{I} \log \mathfrak{o}_i) = O(\mathfrak{o} \log \mathfrak{o})$ additions in A, scalar multiplications in A and multiplications in K. More precisely, there exists an absolute constant $\mathcal{Q}$ such that FT_G can be evaluated with $\mathcal{Q}\mathfrak{o} \log \mathfrak{o}$ of these operations. The depth of the recursion tree is $O(I)$.

Remark 13. In particular, if $A = K$, then the Fourier transform on $K[G]$ requires $\mathcal{Q}\mathfrak{o}\log\mathfrak{o}$ additions and multiplications in K.

Proof. It is sufficient to show that the theorem holds for an absolute constant $\mathcal{Q}$ greater than that in Theorem 32. We will use an inductive argument on I. The case $I = 1$ simply follows from Theorem 32. Assume that $I \geqslant 2$, and that the theorem is true for any group having $I - 1$ invariant factors. We note that $\mathrm{FT}_{C_1\times\cdots\times C_{I-1}}$ extends to an isomorphism of A-algebras

$$A[G] = A[C_1]\dots[C_{I-1}][C_I] \overset{\mathrm{FT}_{C_1\times\cdots\times C_{I-1}}}{\longrightarrow} A^{\hat{C}_1\times\cdots\times\hat{C_{I-1}}}[C_I] =: A'[C_I].$$

Computing this isomorphism requires computing $\mathfrak{o}_I$ Fourier transforms $\mathrm{FT}_{C_1\times\cdots\times C_{I-1}}$. By the recurrence hypothesis, there exists a constant $\mathcal{Q}$ such that computing the extension of $\mathrm{FT}_{C_1\times\cdots\times C_{I-1}}$ to $A[G]$ requires $\mathfrak{o}_I\mathcal{Q}\frac{\mathfrak{o}}{\mathfrak{o}_I}\log(\frac{\mathfrak{o}}{\mathfrak{o}_I}) = \mathcal{Q}\mathfrak{o}\log(\frac{\mathfrak{o}}{\mathfrak{o}_I})$ operations. It remains to compute

$$\mathrm{FT}_{C_I} : A'[C_I] \longrightarrow A'^{\hat{C}_I} = A^{\hat{C}_1\times\cdots\times\hat{C}_I} = A^{\hat{G}}$$

The sum and scalar multiplication in A' can be computed with $\frac{\mathfrak{o}}{\mathfrak{o}_I}$ sums and scalar multiplications in A. According to Theorem 32, the evaluation of FT_{C_I} requires $\mathcal{Q}\mathfrak{o}_I\log\mathfrak{o}_I$ additions and scalar multiplications in A', or $\mathcal{Q}\mathfrak{o}\log\mathfrak{o}_I$ additions and scalar multiplications in A. Thus, it is possible to compute FT_G in $\mathcal{Q}\mathfrak{o}\log(\frac{\mathfrak{o}}{\mathfrak{o}_I}) + \mathcal{Q}\mathfrak{o}\log\mathfrak{o}_I = \mathcal{Q}\mathfrak{o}\log\mathfrak{o}$ operations. By induction, we deduce Theorem 33. □

Remark 14. We can give an iterative formulation of the algorithm of Theorem 33. To do so, let us define

$$A_0 = A \text{ and } \forall 1 \leqslant i \leqslant I, A_i = A^{\hat{C}_1\times\cdots\times\hat{C}_i}$$

as well as $\forall 0 \leqslant i \leqslant I-1$,

$$\mathrm{FT}_i : (A_i[C_{i+2}]\dots[C_I])\,[C_{i+1}] \longrightarrow (A_i[C_{i+2}]\dots[C_I])^{\hat{C}_{i+1}}.$$

Noting that $\forall 0 \leqslant i \leqslant I-1$,

$$A_i[C_{i+1}]\dots[C_I] = (A_i[C_{i+2}]\dots[C_I])\,[C_{i+1}]$$

and

$$(A_i[C_{i+2}]\dots[C_I])^{\hat{C}_{i+1}} = A_{i+1}[C_{i+2}]\dots[C_I],$$

we deduce that

$$\mathrm{FT}_G = \mathrm{FT}_{I-1}\circ\cdots\circ\mathrm{FT}_0.$$

Computing FT_i requires at most $\mathcal{Q}\mathfrak{o}\log\mathfrak{o}_{i+1}$ additions and scalar multiplications in A and multiplications in K.

4.3.3 Multiplication in the algebra of a finite abelian group

Let K be a finite field with $q = p^m$ elements and G a finite (non-trivial) abelian group. Let $\mathfrak{o}$ be the order of G and $\mathfrak{e}$ its exponent. Let t be a power of 2 strictly greater than $3(\mathfrak{e}-1)$. It is clear from Theorem 33 that if K contains primitive $\mathfrak{e}$-th and t-th roots of unity, it is possible to use the Fourier transform FT_G to multiply in $K[G]$. Note that Theorem 33 requires to know an explicit decomposition of G into cyclic factors. This is not a problem in Proposition 34 and Theorem 36 because such a decomposition always exists and can be precomputed.

Proposition 34. Let K be a finite field and G a finite abelian group of order $\mathfrak{o} \geqslant 2$ and exponent $\mathfrak{e}$. Let t be a power of 2 strictly greater than $3(\mathfrak{e}-1)$. Assume that K contains primitive $\mathfrak{e}$-th and t-th roots of unity, then multiplication in $K[G]$ requires $O(\mathfrak{o}\log\mathfrak{o})$ operations in K. More precisely, there exists an absolute constant $\mathcal{Q}$ such that multiplication in $K[G]$ can be computed with $\mathcal{Q}\mathfrak{o}\log\mathfrak{o}$ additions and multiplications in K.

Proof. Let $a, b \in K[G]$. Let $\mathcal{Q}$ be the absolute constant of Theorem 33. We compute

$$\mathrm{FT}_G(ab) = \mathrm{FT}_G(a)\,\mathrm{FT}_G(b)$$

by performing at most $2\mathcal{Q}\mathfrak{o}\log\mathfrak{o} + \mathfrak{o}$ operations in K (since the multiplication in K^G is component-wise). According to Proposition 31, we can compute

$$\mathfrak{o}\iota(ab) = \intercal \circ \mathrm{FT}_{\hat{G}} \circ \hat{\intercal}(\mathrm{FT}_G(ab))$$

with at most $\mathcal{Q}\mathfrak{o}\log\mathfrak{o}$ additional operations in K. Since K contains the $\mathfrak{e}$-th primitive roots of unity, then $\mathfrak{o}$ has an inverse $\mathfrak{o}^{-1}$ in K. We can therefore compute $\iota(ab) = \mathfrak{o}^{-1}\mathfrak{o}\iota(ab)$ with one additional multiplication in K. Finally, ι is an involution that permutes the coordinates of the elements of $K[G]$, so we can recover ab with $O(\mathfrak{o})$ additional operations in K. □

We now consider the case where K does not contain the necessary roots of unity. Let us begin with the special case where $m = 1$, i.e., $K = \mathbb{Z}/p\mathbb{Z}$. In the worst case, $\mathrm{pgcd}(p, \mathfrak{o}) \neq 1$ and it is impossible to find a K-algebra containing $\mathfrak{e}$-th roots of unity.

The trick we will use is to reduce the computation of the product in $K[G]$ to the computation of the product in $K'[G]$ via non-algebraic maps, where $K' = \mathbb{Z}/p'\mathbb{Z}$ is a finite field of characteristic $p' > p$. We begin by giving constraints on the choice of p'.

We define

$$\mathrm{lift}_p : K \longrightarrow \mathbb{Z}$$

the (set) section of the reduction modulo p with image in $[0, p[$. The map lift_p extends to a non-algebraic map

$$\begin{array}{rccc} \mathrm{lift}_p : & K[G] & \longrightarrow & \mathbb{Z}[G] \\ & \sum_{\sigma\in G} \alpha_\sigma \sigma & \longmapsto & \sum_{\sigma\in G} \mathrm{lift}_p(\alpha_\sigma)\sigma \end{array}.$$

We similarly define for any $p' > p$

$$\mathrm{lift}_{p'} : K'[G] \longrightarrow \mathbb{Z}[G].$$

We can also define maps

$$\uparrow\colon \begin{array}{ccc} K & \longrightarrow & K' \\ \alpha & \longmapsto & \mathrm{lift}_p(\alpha) \bmod p' \end{array} \quad \text{and} \quad \downarrow\colon \begin{array}{ccc} K' & \longrightarrow & K \\ \alpha' & \longmapsto & \mathrm{lift}_{p'}(\alpha') \bmod p \end{array}.$$

In particular, for all $\alpha \in K$,

$$\downarrow (\uparrow (\alpha)) = \alpha.$$

The maps $\uparrow$ and $\downarrow$ extend to maps

$$\uparrow\colon K[G] \longrightarrow K'[G] \text{ and } \downarrow\colon K'[G] \longrightarrow K[G].$$

We wish for the maps $\uparrow$ and $\downarrow$ to satisfy

$$\forall a, b \in K[G], \downarrow (\uparrow (a) \cdot \uparrow (b)) = ab.$$

Let

$$a = \sum_{\sigma \in G} \alpha_\sigma \sigma \in K[G] \text{ and } b = \sum_{\sigma \in G} \beta_\sigma \sigma \in K[G]$$

and let

$$A = \mathrm{lift}_p(a) \in \mathbb{Z}[G] \text{ and } B = \mathrm{lift}_p(b) \in \mathbb{Z}[G].$$

The coefficients of $AB \in \mathbb{Z}[G]$ are integers in $[0, \mathfrak{o}(p-1)^2]$, and $ab = AB \bmod p$. Then

$$AB = \mathrm{lift}_{p'}(\uparrow (a) \uparrow (b)) \Longrightarrow \downarrow (\uparrow (a) \cdot \uparrow (b)) = ab. \tag{4.3.2}$$

The left term of the equation (4.3.2) is satisfied for any $a, b \in K[G]$ if and only if

$$p' > \mathfrak{o}(p-1)^2. \tag{4.3.3}$$

We also ask that $K' = \mathbb{Z}/p'\mathbb{Z}$ contains primitive $\mathfrak{e}$-th and t-th roots of unity. It is equivalent to ask

$$p' \equiv 1 \bmod \mathrm{ppcm}(\mathfrak{e}, t). \tag{4.3.4}$$

We choose p' as the smallest prime satisfying conditions (4.3.3) and (4.3.4). The question that now needs to be asked concerns the size of p'. Let p'' be the smallest prime satisfying

$$p'' \equiv 1 \bmod (\mathfrak{o}(p-1)^2 t),$$

then it is clear that p'' satisfies conditions (4.3.3) and (4.3.4), so $p' \leqslant p''$. According to Heath-Brown's results [HB92] on the constant in Linnik's theorem on primes in arithmetic progressions, there exists a constant $\mathcal{Q}$ such that

$$p' \leqslant p'' \leqslant \mathcal{Q}(\mathfrak{o}(p-1))^{11}. \tag{4.3.5}$$

In other words,

$$\log p' = O(\log(\mathfrak{o}) + \log(p)).$$

Remark 15. This upper bound is clearly not optimal. First, a result by Xylouris [Xyl11] slightly refines the exponent in inequality (4.3.5). Furthermore, a result by Bach–Sorenson [BS96] shows that, assuming GRH, there exists $\mathcal{Q}$ such that

$$p'' \leqslant \mathcal{Q}\left(\varphi(\mathfrak{o}^2(p-1)^2)\log(\mathfrak{o}(p-1))\right)^2$$

where φ denotes the Euler totient function. Next, we use the inequality $t \leqslant 6\mathfrak{o}$, which is rather poor when the group G decomposes into a large number of cycles. Finally, it seems that, in many examples, the inequality $p' \leqslant p''$ is also rather broad. However, this bound is sufficient to arrive at the desired result.

Proposition 34 and equation (4.3.5) allow us to make the following statement:

Proposition 35. There exists an absolute constant $\mathcal{Q}$ such that the following statement is true. Let K be the finite field with p elements. Let G be a finite abelian group of order $\mathfrak{o} \geqslant 2$ and exponent $\mathfrak{e}$. Let t be a power of 2 strictly greater than $3(\mathfrak{e}-1)$. There exists a prime $p' \leqslant \mathcal{Q}(\mathfrak{o}p)^{11}$ that satisfies conditions (4.3.3) and (4.3.4). Then, multiplication in $K[G]$ can be computed with $\mathcal{Q}\mathfrak{o}\log\mathfrak{o}$ operations. An operation is understood to be an addition or a multiplication in $K' = \mathbb{Z}/p'\mathbb{Z}$, or an evaluation of $\uparrow$ or $\downarrow$.

We still need to address the case where $m > 1$, i.e., K is not a prime field. Our assumptions about the algorithmic representation of finite fields in Chapter 2 allow us to view K as a $\mathbb{Z}/p\mathbb{Z}$ vector space of dimension m, and to identify the elements of K with their coordinates in a $\mathbb{Z}/p\mathbb{Z}$-basis of K. We can therefore use the Chudnovsky–Chudnovsky algorithm for multiplying in finite fields [CC88], which allows us to generalize the previous approach. The work of Chudnovsky–Chudnovsky [CC88], Shparlinski–Tsfasman–Vladut [STV92], Shokrollahi [Sho92], Ballet–Rolland [BR04], Chaumine [Cha08], Randriambololona [Ran12] and others, demonstrate that there exists an absolute constant $\mathcal{Q}$, an integer $r \leqslant \mathcal{Q}m$, $\mathbb{Z}/p\mathbb{Z}$-linear forms $\phi_1, \ldots, \phi_r$ and $\psi_1, \ldots, \psi_r$ over K, and $w_1, \ldots, w_r \in K$ such that

$$\forall x, y \in K,\ xy = \sum_{i=1}^{r} \phi_i(x)\psi_i(y)w_i.$$

For $1 \leqslant i \leqslant r$, the linear forms can be extended to group algebras.

$$\begin{array}{rccc} \tilde{\phi}_i : & K[G] & \longrightarrow & \mathbb{Z}/p\mathbb{Z}[G] \\ & \sum_{\sigma\in G}\alpha_\sigma\sigma & \longmapsto & \sum_{\sigma\in G}\phi_i(\alpha_\sigma)\sigma \end{array}$$

$$\begin{array}{rccc} \tilde{\psi}_i : & K[G] & \longrightarrow & \mathbb{Z}/p\mathbb{Z}[G] \\ & \sum_{\sigma\in G}\alpha_\sigma\sigma & \longmapsto & \sum_{\sigma\in G}\psi_i(\alpha_\sigma)\sigma \end{array}$$

Note that

$$\forall a, b \in K[G],\ ab = \sum_{i=1}^{r} w_i\tilde{\phi}_i(a)\tilde{\psi}_i(b)$$

so that the bilinear part of the multiplication in $K[G]$ reduces to r multiplications in $\mathbb{Z}/p\mathbb{Z}[G]$. From this formula and Proposition 35, we deduce Theorem 36:

Theorem 36. *There exists an absolute constant $\mathcal{Q}$ such that the following statement is true. Let K be a finite field with p^m elements. Let G be a finite abelian group of order $\mathfrak{o} \geqslant 2$. There exists a prime $p' \leqslant \mathcal{Q}(\mathfrak{o}p)^{11}$ that satisfies conditions (4.3.3) and (4.3.4). Then a multiplication in $K[G]$ can be computed in $\mathcal{Q}(m\mathfrak{o}\log\mathfrak{o} + m^2\mathfrak{o})$ operations. An operation is understood to be an addition or a multiplication in $\mathbb{Z}/p\mathbb{Z}$ or in $\mathbb{Z}/p'\mathbb{Z}$, or an evaluation of $\uparrow$ or $\downarrow$.*

4.4 Codes over finite group algebras

In Section 4.3, we focused mainly on finite abelian group algebras. In Section 4.5, we will also focus mainly on the abelian case. However, the content of this section applies equally to abelian and non-abelian groups. We will therefore make no assumptions about the commutativity of the considered finite groups.

For this entire section, we set G as a finite group of order $\mathfrak{o}$ and K as a finite field with $q = p^m$ elements.

4.4.1 A few bilinear forms

We begin by defining a notation for the K-bilinear and $K[G]$-bilinear forms that we will use later. Let R be a ring (unitary, associative) and E a finite set. We denote

$$\begin{array}{rccc} \langle .,. \rangle : & R^E \times R^E & \longrightarrow & R \\ & (a_i)_{i\in E}, (b_i)_{i\in E} & \longmapsto & \sum_{i\in E} a_i b_i \end{array} \tag{4.4.1}$$

the canonical R-bilinear form on R^E. This notation is slightly ambiguous, as it does not specify the base ring R. We will take care to remove the ambiguity later, when necessary.

In particular, this defines the canonical $K[G]$-bilinear form on $K[G]^E$

$$\langle .,. \rangle : K[G]^E \times K[G]^E \longrightarrow K[G].$$

We also define the K-bilinear form

$$\begin{array}{rccc} \langle .,. \rangle_K : & K[G]^E \times K[G]^E & \longrightarrow & K \\ & a, b & \longmapsto & 1_G^*(\langle a, b \rangle) \end{array} \tag{4.4.2}$$

which is the component of $\langle .,. \rangle$ associated with the neutral element of G. In general, for any $\sigma \in G$, we denote by $\sigma^* : K[G] \longrightarrow K$ the map returning the component associated with σ of the elements of $K[G]$.

The free $K[G]$-module $K[G]^E$ is naturally acted on by G in two ways (on the left and on the right):

$$\forall \sigma \in G, \forall a = (a_i)_{i\in E} \in K[G]^E,\ \sigma \cdot a = (\sigma a_i)_{i\in E} \text{ and } a \cdot \sigma = (a_i \sigma)_{i\in E}. \tag{4.4.3}$$

The form $\langle .,. \rangle_K$ is compatible with the action of G on $K[G]^E$ in the following sense:

Proposition 37. We use the notation from the beginning of Section 4.4 and Subsection 4.4.1. Let $\sigma \in G$, let $a, b \in K[G]^E$, then

$$\langle a \cdot \sigma, b \rangle_K = \langle a, \sigma \cdot b \rangle_K.$$

Proof. Let $a = (a_i)_{i \in E} \in K[G]^E$ and $b = (b_i)_{i \in E} \in K[G]^E$. Then

$$\begin{aligned} \langle a \cdot \sigma, b \rangle_K &= 1_G^* \left(\sum_{i \in E} (a_i \sigma) b_i \right) \\ &= 1_G^* \left(\sum_{i \in E} a_i (\sigma b_i) \right) \\ &= \langle a, \sigma \cdot b \rangle_K. \end{aligned}$$

□

Proposition 38. We use the notation of the beginning of Section 4.4 and of Subsection 4.4.1. Let $a, b \in K[G]^E$. Then

$$\langle a, b \rangle = \sum_{\sigma \in G} \langle a, b \cdot \sigma^{-1} \rangle_K \sigma.$$

Proof. Let $\sigma \in G$. One has

$$\begin{aligned} \sigma^*(\langle a, b \rangle) &= 1_G^*(\langle a, b \rangle \sigma^{-1}) \\ &= 1_G^*(\langle a, b\sigma^{-1} \rangle) \\ &= \langle a, b\sigma^{-1} \rangle_K. \end{aligned}$$

□

Remark 16. More generally, given M a left $K[G]$-module, N a right $K[G]$-module, and a $K[G]$-bilinear map

$$< .,. >: M \times N \longrightarrow K[G],$$

we can associate to it a K-bilinear map

$$< .,. >_K : b, a \in N \times M \longmapsto 1_G^*(< a, b >)$$

compatible with the action of G on M and N, and vice versa. In Definition (4.4.2), we can afford not to reverse the order of the parameters because $\langle ., . \rangle_K$ is symmetric (see Proposition 40).

Let us define the isomorphisms of K-vector spaces

$$\begin{array}{rccc} \varphi : & K[G]^E & \longrightarrow & K^{E \times G} \\ & (\sum_{\sigma \in G} a_{i,\sigma} \sigma)_{i \in E} & \longmapsto & (a_{i,\sigma})_{(i,\sigma) \in E \times G} \end{array} \tag{4.4.4}$$

and

$$\begin{array}{rccc} \iota: & K[G]^E & \longrightarrow & K[G]^E \\ & (\sum_{\sigma\in G}\alpha_{i,\sigma}\sigma)_{i\in E} & \longmapsto & (\sum_{\sigma\in G}\alpha_{i,\sigma^{-1}}\sigma)_{i\in E} \end{array}. \tag{4.4.5}$$

Notice that applying ι is equivalent to applying the involution $\sigma \longmapsto \sigma^{-1}$ coordinate by coordinate. We will also denote this involution by ι.

We can explicitly describe a connection between the K-bilinear forms

$$\langle .,. \rangle_K : K[G]^E \times K[G]^E \longrightarrow K$$

and

$$\langle .,. \rangle : K^{E\times G} \times K^{E\times G} \longrightarrow K$$

using the isomorphisms φ and ι.

Proposition 39. We use the notation from the beginning of Section 4.4 and Section 4.4.1. Let $a, b \in K[G]^E$, then

$$\langle a, b\rangle_K = \langle \varphi \circ \iota(a), \varphi(b)\rangle.$$

Proof. Let $a = (a_i)_{i\in E} \in K[G]^E$ and $b = (b_i)_{i\in E} \in K[G]^E$. For all $i \in E$, we write

$$a_i = \sum_{\sigma\in G} a_{i,\sigma}\sigma \text{ and } b_i = \sum_{\sigma\in G} b_{i,\sigma}\sigma$$

Then

$$\begin{aligned} \langle a, b\rangle_K &= 1_G^*\left(\sum_{i\in E} a_i b_i\right) \\ &= \sum_{i\in E} 1_G^*(a_i b_i) \\ &= \sum_{i\in E} 1_G^*\left(\sum_{\sigma\in G}\left(\sum_{\tau\in G} a_{i,\tau} b_{i,\tau^{-1}\sigma}\right)\sigma\right) \\ &= \sum_{i\in E}\sum_{\tau\in G} a_{i,\tau} b_{i,\tau^{-1}} \\ &= \sum_{i\in E}\sum_{\tau\in G} a_{i,\tau^{-1}} b_{i,\tau} \\ &= \langle \varphi \circ \iota(a), \varphi(b)\rangle. \end{aligned}$$

□

This proof also demonstrates the following proposition:

Proposition 40. We use the notation from the beginning of the Section 4.4 and from Subsection 4.4.1. Let $a, b \in K[G]^E$. Then

$$\langle a, b\rangle_K = \langle b, a\rangle_K$$

4.4.2 Submodules and codes

We use the notation from the beginning of Section 4.4, the linear forms (4.4.1) and (4.4.2), and the isomorphisms (4.4.4) and (4.4.5). In this subsection, we show how to define linear codes from free sub-$K[G]$-modules of free $K[G]$-modules of finite rank.

Definition 35. Let $n \geqslant 0$ be an integer and E a set of cardinality n. Let M be a free left (resp. right) submodule of $K[G]^E$. We define a linear code structure on M by setting, for all $a \in M$,

$$\mathrm{wt}(a) = \mathrm{wt}(\varphi(a)) \text{ (resp. } \mathrm{wt}(\varphi \circ \iota(a))).$$

Then the length of M is

$$\mathrm{len}\, M = \#(E \times G) = n\mathfrak{o}.$$

We call n the G-length of M over K. Let k be the rank of M as a free $K[G]$-module, then the dimension of M as a K-vector space is

$$\dim M = k\mathfrak{o}.$$

Remark 17. If G is abelian, the codes defined in Definition 35 are a special case of quasi-abelian codes [Was77]. If G is not abelian, they are examples of quasi-group codes, or quasi-G-codes [DGTT18, BW23].

4.4.3 The orthogonal and dual codes

We use the notation from the beginning of Section 4.4, the linear forms (4.4.1) and (4.4.2), and the isomorphisms (4.4.4) and (4.4.5).

Let E be a finite set of cardinality n. Let M be a left submodule of $K[G]^E$. We define

$$M^\perp = \{a \in K[G]^E \mid \langle M, a\rangle = 0\} \tag{4.4.6}$$

the orthogonal of M. The $K[G]$-bilinearity of $\langle ., .\rangle$ allows us to prove that $M^\perp$ is a right submodule of $K[G]^E$. Similarly, if M is a right submodule of $K[G]^E$, we define

$$M^\perp = \{a \in K[G]^E \mid \langle a, M\rangle = 0\} \tag{4.4.7}$$

the orthogonal of M. It is a left submodule of $K[G]^E$.

Note that the placement of M in equations (4.4.6) and (4.4.7) is significant. Indeed, if G is not abelian, $\langle ., .\rangle$ is not symmetric. For instance, if E is a singleton, $\langle ., .\rangle$ denotes the product in $K[G]$. Let $\sigma, \tau \in G$ be two elements that do not commute, then

$$\langle \sigma, \tau\rangle \neq \langle \tau, \sigma\rangle.$$

Proposition 41. We use the notation from the beginning of Subsection 4.4.3. Let M be a left submodule of $K[G]^E$. Then

$$M^\perp = \{a \in K[G]^E \mid \langle a, M\rangle_K = 0\}$$

Similarly, let M be a right submodule of $K[G]^E$. Then

$$M^\perp = \{a \in K[G]^E \mid \langle M, a\rangle_K = 0\}$$

Proof. We make the demonstration when M is a left submodule of $K[G]^E$. Let $a \in M^\perp$, and $b \in M$ then

$$\begin{aligned}\langle a, b\rangle_K &= \langle b, a\rangle_K \\ &= 1_G^*(\langle b, a\rangle) \\ &= 1_G^*(0) = 0.\end{aligned}$$

Therefore

$$M^\perp \subset \{a \in K[G]^E \mid \langle a, M\rangle_K = 0\}.$$

Conversely, let $a \in K[G]^E$ such that $\langle a, M\rangle_K = 0$, and let $b \in M$. Let $\sigma \in G$. Then, after Propositions 37 and 38, one has

$$\begin{aligned}\sigma^*(\langle b, a\rangle) &= \langle b, a\sigma^{-1}\rangle_K \\ &= \langle a\sigma^{-1}, b\rangle_K \\ &= \langle a, \sigma^{-1}b\rangle_K \\ &= 0\end{aligned}$$

because $\sigma^{-1}b \in M$, as M is a left $K[G]$-module. Therefore, we showed that $\langle b, a\rangle = 0$, so

$$\{a \in K[G]^E \mid \langle a, M\rangle_K = 0\} \subset M^\perp.$$

□

Remark 18. Following from Remark 16, Proposition 41 can be generalized to any $K[G]$-bilinear map.

Let M be a free (left or right) submodule of $K[G]^E$ of rank k. According to Theorem 79 proven in the appendix, $M^\perp$ is also a free (right or left) submodule of $K[G]^E$ of rank $n-k$. Furthermore, the code associated with $M^\perp$ is the dual code of the code associated with M, according to Proposition 39.

4.4.4 Generator and parity-check matrices

We use the notation from the beginning of Section 4.4, the linear forms (4.4.1) and (4.4.2), the isomorphisms (4.4.4) and (4.4.5), and the orthogonals (4.4.6) and (4.4.7).

Let E be a set of cardinality n. We will define generator matrices and parity-check matrices with coefficients in $K[G]$ for codes associated with free submodules of $K[G]^E$.

Definition 36. Using the notation from the beginning of Subsection 4.4.4. Let M be a free left submodule of $K[G]^E$ of rank k. Let F be a set of cardinality k. We say that $\mathcal{E} \in \mathcal{M}_{F,E}(K[G])$ is a G-generator matrix of M if

$$M = \{a\mathcal{E}; a \in K[G]^F\}.$$

Let H be a set of cardinality $n-k$. We say that $\mathcal{C} \in \mathcal{M}_{E,H}(K[G])$ is a G-parity-check matrix of M if

$$M = \{a \in K[G]^E \mid a\mathcal{C} = 0\}.$$

Let M be a free right submodule of $K[G]^E$ of rank k. Similarly, we say that $\mathcal{E} \in \mathcal{M}_{E,F}(K[G])$ is a G-generator matrix of M if

$$M = \{\mathcal{E}a; a \in K[G]^F\}.$$

We say that $\mathcal{C} \in \mathcal{M}_{H,E}(K[G])$ is a G-parity-check matrix of M if

$$M = \{b \in K[G]^E \mid \mathcal{C}b = 0\}.$$

Remark 19. It is correct to define the G-generator matrices and G-parity-check matrices in this way because the modules are assumed to be free. In this case, their orthogonal is also free (see Theorem 79).

Remark 20. The writing conventions in Definition 36 are not arbitrary. Let M be a free left submodule of $K[G]^E$ of rank k. There exists $a_1, \dots, a_k \in K[G]^E$ a $K[G]$-basis of M and in particular

$$M = K[G] \cdot a_1 \oplus K[G] \cdot a_2 \oplus \cdots \oplus K[G] \cdot a_k.$$

If G is not abelian, M is generally not stable under right multiplication. Thus, the matrix whose columns are the coordinates of $(a_i)_{i\in[1..k]}$ cannot be considered a G-generator matrix of M. The generators of M must be viewed as rows.

Let $a \in K[G]$, then the right multiplication by a induces a linear endomorphism of K^G via the isomorphism φ, defined in equation 4.4.4. We can then identify a with a matrix in $\mathcal{M}_G(K)$.

Let M be a free left submodule of $K[G]^E$ of rank k. Let F be a set of cardinality k. Let $\mathcal{E} \in \mathcal{M}_{F,E}(K[G])$ be a G-generator matrix of M. We seek to define a matrix with coefficients in K associated with $\mathcal{E}$ that generates $\varphi(M)$. Such a matrix can be obtained by replacing the coefficients in $K[G]$ of $\mathcal{E}$ with the matrices of $\mathcal{M}_G(K)$ corresponding to right multiplication by these elements. This gives a matrix in $\mathcal{M}_{F,E}(\mathcal{M}_G(K))$, which is naturally associated with a matrix $\mathcal{E}_K \in \mathcal{M}_{F\times G,E\times G}(K)$, the unique matrix satisfying

$$\forall a \in K[G]^F, \varphi^{-1}(\varphi(a)\mathcal{E}_K) = a\mathcal{E}.$$

Let M be a free right submodule of $K[G]^E$ of rank k. Let $\mathcal{E} \in \mathcal{M}_{E,F}(K[G])$ be a G-generator matrix of M. In this case, we seek to define a matrix $\mathcal{E}_K \in \mathcal{M}_{F\times G,E\times G}(K)$ generating $\varphi \circ \iota(M)$. We can define it using a similar equation.

Definition 37. Let M be a free left submodule of $K[G]^E$ of rank k. Let $\mathcal{E} \in \mathcal{M}_{F,E}(K[G])$ be a G-generator matrix of M. We define $\mathcal{E}_K \in \mathcal{M}_{F\times G,E\times G}(K)$ as the matrix such that

$$\forall a \in K[G]^F, \varphi(a)\mathcal{E}_K = \varphi(a\mathcal{E}).$$

Let M be a free right submodule of $K[G]^E$ of rank k. Let $\mathcal{E} \in \mathcal{M}_{E,F}(K[G])$ be a G-generator matrix of M. We define $\mathcal{E}_K \in \mathcal{M}_{F\times G,E\times G}(K)$ as the matrix such that

$$\forall a \in K[G]^F, (\varphi \circ \iota)(a)\mathcal{E}_K = (\varphi \circ \iota)(\mathcal{E}a).$$

Remark 21. It may seem surprising to associate a matrix $\mathcal{E}_K \in \mathcal{M}_{F\times G,E\times G}(K)$ with a matrix $\mathcal{E} \in \mathcal{M}_{E,F}(K[G])$. In reality, in this case, it is simply a convention of notation because multiplication in K is commutative. Our choice is justified by the usual conventions on the notation of generator matrices of linear codes and by Proposition **??**, which shows that the matrix associated with the G-generator matrix of the dual of M is a generator of the dual code of $\varphi(M)$, where M is a free left submodule of $K[G]^E$. In order to change the convention, one would need to use the equation

$$\forall a \in K[G]^F, \mathcal{E}_K(\varphi \circ \iota)(a) = (\varphi \circ \iota)(\mathcal{E}a).$$

Example 5. Let $K = \mathbb{F}_2$ and $G = \{1, \tau, \tau^2\}$ be a group isomorphic to $\mathbb{Z}/3\mathbb{Z}$ where $\tau^3 = 1$. Let M be the free left submodule of $\mathbb{F}_2[G]^2$ of rank 1 generated by $(1, \tau)$;

$$M = \mathbb{F}_2[G] \cdot (1, \tau).$$

The orthogonal of M is a free right submodule of rank 1 of $\mathbb{F}_2[G]^2$; we deduce that

$$M^\perp = (-\tau, 1) \cdot \mathbb{F}_2[G] = (\tau, 1) \cdot \mathbb{F}_2[G].$$

A G-generator matrix of M (as a free left submodule) is

$$\mathcal{E} = \begin{pmatrix} 1 & \tau \end{pmatrix}$$

and a G-generator matrix of $M^\perp$ (as a free right submodule) is

$$\mathcal{C} = \begin{pmatrix} \tau \\ 1 \end{pmatrix}.$$

The latter is also a G-parity-check matrix of M.

We now are going to compute $\mathcal{E}_{\mathbb{F}_2}$ and $\mathcal{C}_{\mathbb{F}_2}$, the matrices associated with $\mathcal{E}$ and $\mathcal{C}$, and we will check that they indeed generate $\varphi(M)$ and $\varphi \circ \iota(M^\perp)$. Let

$$\alpha = a + b\tau + c\tau^2 \in \mathbb{F}_2[G],$$

we identify α with the vector $\begin{pmatrix} a & b & c \end{pmatrix}$ via the map φ (and the identification $K^G \simeq K^3$). One has

$$\alpha\tau = c + a\tau + b\tau^2.$$

We conclude that the matrix associated with the right multiplication by τ in the canonical basis of K^G is

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

where we identify K^G and K^3. Thus, the generator matrix of $\varphi(M)$ associated with $\mathcal{E}$ is

$$\mathcal{E}_{\mathbb{F}_2} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix},$$

which is indeed a generator matrix of $\varphi(M)$.

Since $M^\perp$ is a right-$K[G]$-module, the linear code wich is associated with it is $\varphi \circ \iota(M^\perp)$. One has

$$\iota(M^\perp) = \mathbb{F}_2[G] \cdot \iota((\tau, 1)) = \mathbb{F}_2[G] \cdot (\tau^2, 1) = M. \tag{4.4.8}$$

Therefore, $\varphi \circ \iota(M^\perp) = \varphi(M)$.

Let us compute the generator matric of $\varphi \circ \iota(M^\perp)$ associated with $\mathcal{C}$. Let

$$\alpha = a + b\tau + c\tau^2 \in \mathbb{F}_2[G],$$

we identify α to the vector $\begin{pmatrix} a & c & b \end{pmatrix}$ via the map $\varphi \circ \iota$. One has

$$\mathcal{C}\alpha = \begin{pmatrix} \tau\alpha \\ \alpha \end{pmatrix} = \begin{pmatrix} c + a\tau + b\tau^2 \\ a + b\tau + c\tau^2 \end{pmatrix}$$

that we identify to the vector $\begin{pmatrix} c & b & a & a & c & b \end{pmatrix}$ via the map $\varphi \circ \iota$. We conclude that

$$\mathcal{C}_{\mathbb{F}_2} = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix},$$

which indeed generates $\varphi \circ \iota(M^\perp) = \varphi(M)$. We can also notice that this matrix corresponds to the result of equation (4.4.8), as

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

is the matrix associated with the right multiplication by τ^2.

Finally, notice that

$$\mathcal{E}_{\mathbb{F}_2} \mathcal{C}_{F_2}^t = 0.$$

Remark 22. The example motivates to call M autodual when $M = \iota(M^\perp)$.

Proposition 42. Let E be a finite set of cardinality n. Let M be a free left (resp. right) submodule of $K[G]^E$ of rank k. Let $\mathcal{E}$ be a G-generator matrix of M, then $\mathcal{E}_K$ is a generator matrix of $\varphi(M)$ (resp. $\varphi \circ \iota(M)$).

Proof. We make the proof when M is a right $K[G]$-module. Let F be a set of cardinality k. We assume that $\mathcal{E} \in \mathcal{M}_{F,E}(K[G])$. Let $c \in K^{E \times G}$, one has

$$\begin{aligned} c \in \varphi \circ \iota(M) &\Leftrightarrow \exists a \in K[G]^F, c = \varphi \circ \iota(\mathcal{E}a) \\ &\Leftrightarrow \exists a \in K[G]^F, c = \varphi \circ \iota(a)\mathcal{E}_K \\ &\Leftrightarrow \exists a \in K^{F \times G}, c = a\mathcal{E}_K. \end{aligned}$$

Therefore $\mathcal{E}_K$ is a generator matrix of $\varphi \circ \iota(M)$. □

We will take the liberty of saying, somewhat abusively, that $\mathcal{E}_K$ is a generator matrix of M.

Proposition 43. Let E be a finite set of cardinality n. Let $M \subset K[G]^E$ be a free left (resp. right) submodule of $K[G]^E$ of rank k. Let F be a set of cardinality k and let $\mathcal{E} \in \mathcal{M}_{F,E}(K[G])$ (resp. $\mathcal{E} \in \mathcal{M}_{E,F}(K[G])$) be a G-generator matrix of M. The module $\iota(M)$ is a right (resp. left) submodule of $K[G]^E$.

Let

$$\mathcal{E}' := \iota(\mathcal{E})^t,$$

where ι is applied coefficient-wise. Then $\mathcal{E}'$ is a G-generator matrix of $\iota(M)$, and

$$\mathcal{E}_K = \mathcal{E}'_K.$$

Proof. We prove the proposition for left modules. Recall that ι is an involution. Let $a \in K[G]^F$, we have

$$\iota(\iota(a)\mathcal{E}) = \iota(\mathcal{E})^t a,$$

Indeed, let $(b_i)_{i\in F}$ be a column of $\mathcal{E}$, let $a = (a_i)_{i\in F}$, then

$$\iota(\sum_{i\in F} \iota(a_i)b_i) = \sum_{i\in F} \iota(b_i)\iota(\iota(a_i)) = \sum_{i\in F} \iota(b_i)a_i,$$

because $\iota : K[G] \longrightarrow K[G]$ is an anti-isomorphism of K-algebras on $K[G]$. We conclude that

$$(\varphi \circ \iota)(a)\mathcal{E}_K = \varphi(\iota(a)\mathcal{E}) = \varphi \circ \iota(\iota(\mathcal{E})^t a) = (\varphi \circ \iota)(\mathcal{E}'a).$$

□

It can be shown that the generator matrix associated with a G-generator matrix of $M^\perp$ generates the dual of $\varphi(M)$ (resp. $\varphi \circ \iota(M)$).

Proposition 44. Let E be a finite set of cardinality n. Let $M \subset K[G]^E$ be a free left (resp. right) submodule of $K[G]^E$. Let $\mathcal{C}$ be a G-generator matrix of $M^\perp$. Then $\mathcal{C}$ is a G-parity-check matrix of M and ${\mathcal{C}_K}^t$ is a parity-check matrix of $\varphi(M)$ (resp. $\varphi \circ \iota(M)$).

Proof. We write the proof for left submodules of $K[G]$. Let k and n be the rank and G-length of M. Let H be a set of cardinality $n-k$, let $\mathcal{C} \in \mathcal{M}_{E,H}(K[G])$ be a G-generator matrix of $M^\perp$, and let $(c_j)_{j\in H}$ be the $K[G]$-basis of $M^\perp$ consisting of the columns of $\mathcal{C}$. For all $j \in H$, we set

$$c_j = (c_{i,j})_{i\in E}.$$

Let $a = (a_i)_{i\in E} \in K[G]^E$. Then

$$\begin{aligned} a\mathcal{C} = 0 &\Leftrightarrow \forall j \in H, \sum_{i\in E} a_i c_{i,j} = 0 \\ &\Leftrightarrow \forall j \in H, \langle a, c_j \rangle = 0 \\ &\Leftrightarrow a \in (M^\perp)^\perp = M. \end{aligned}$$

Therefore, $\mathcal{C}$ is a G-parity-check matrix of M.

Furthermore, $\mathcal{C}_K$ is a generator matrix of $\varphi \circ \iota(M^\perp)$. Therefore, according to Proposition 39, the matrix ${\mathcal{C}_K}^t$ is a parity-check matrix of $\varphi(M)$. □

We show a final result of compatibility between matrix operations over $K[G]$ and over K.

Proposition 45. Let E be a set of cardinality n. Let M be a free right submodule of $K[G]^E$ of rank k. Let $\mathcal{E} \in \mathcal{M}_{E,F}(K[G])$ be a G-generator matrix of M. Let $a \in K[G]^E$, then we have

$$\varphi(a\mathcal{E}) = \mathcal{E}_K \varphi(a).$$

Let M be a free left submodule of $K[G]^E$ of rank k. Let F be a set of cardinality k and let $\mathcal{E} \in \mathcal{M}_{F,E}(K[G])$ be a G-generator matrix of M. Let $a \in K[G]^E$, we have

$$(\varphi \circ \iota)(\mathcal{E}a) = \mathcal{E}_K (\varphi \circ \iota)(a).$$

Proof. We make the proof for left submodules. For all $b \in K^{E \times G}$ one has

$$\begin{aligned}
\langle b, \varphi \circ \iota(\mathcal{E}a) \rangle &= \langle \varphi^{-1}(b), \mathcal{E}a \rangle_K, \text{ from Proposition 39,} \\
&= 1_G^*(\langle \varphi^{-1}(b), \mathcal{E}a \rangle), \text{ by definition of } \langle ., . \rangle_K, \\
&= 1_G^*(\langle \varphi^{-1}(b)\mathcal{E}, a \rangle), \text{ by associativity of the matrix multiplication,} \\
&= \langle \varphi^{-1}(b)\mathcal{E}, a \rangle_K, \text{ by definition of } \langle ., . \rangle_K, \\
&= \langle b\mathcal{E}_K, \varphi \circ \iota(a) \rangle, \text{ from Proposition 39,} \\
&= \langle b, \mathcal{E}_K \varphi \circ \iota(a) \rangle, \text{ by associativity of the matrix multiplication.}
\end{aligned}$$

□

We conclude this section by defining G-interpolation matrices, pseudo-inverses of the generator G-matrices.

Proposition 46. Let M be a free left submodule of $K[G]^E$, and let $\mathcal{E} \in \mathcal{M}_{F,E}(K[G])$ be a G-generator matrix of M. There exists a matrix $\mathcal{I} \in \mathcal{M}_{E,F}(K[G])$ such that

$$\mathcal{E}\mathcal{I} = \mathrm{Id}_F \,.$$

We say that $\mathcal{I}$ is an interpolation matrix of M associated with $\mathcal{E}$.

Let M be a free right-$K[G]$-module over $K[G]^E$, and let $\mathcal{E} \in \mathcal{M}_{E,F}(K[G])$ be a G-generator matrix of M. There exists a matrix $\mathcal{I} \in \mathcal{M}_{F,E}(K[G])$ such that

$$\mathcal{I}\mathcal{E} = \mathrm{Id}_F \,.$$

We say that $\mathcal{I}$ is an interpolation matrix of M associated with $\mathcal{E}$.

Proof. We write the proof for left modules. Let $(m_i)_{i \in F}$ be the $K[G]$-basis of M associated with the matrix $\mathcal{E}$. Let $(e_i)_{i \in E}$ be the canonical basis of $K[G]^E$. According to Proposition 77, there exists a left submodule N of $K[G]^E$ such that $K[G]^E = M \oplus N$. Then π the projection onto M parallel to N is a left $K[G]$-module morphism, and $\mathcal{I}$ is the matrix of π in the bases $(e_i)_{i \in E}$ and $(m_i)_{i \in F}$. □

4.5 Geometric codes over finite group algebras

Let K be a finite field with $q = p^m$ elements. In this section, we study the structure of $K[G]$-modules of certain linear spaces of non-ramified abelian covers with Galois group G of a smooth projective curve X over K. When G is abelian, under certain assumptions, these spaces are free $K[G]$-modules. We can then define structured Goppa codes. We show that there exist algorithms for encoding and decoding these codes that exploit the $K[G]$-module structure. In certain cases, these algorithms are significantly faster than the classical encoding and decoding algorithms for Goppa codes. Finally, we define families of structured Goppa codes that are asymptotically good, and sometimes excellent, and whose codes can be encoded in quasi-linear time in their length and decoded in quasi-quadratic time. In Subsection 4.5.4, we give an example of a structured geometric code and detail the computation of a generator matrix.

4.5.1 Construction

This subsection is divided into several steps. First, we show how the Galois group of a Galois cover

$$\tau : Y \longrightarrow X$$

acts on $K(Y)$ and on $\Omega(Y/K)$. This induces an action on the residue algebras at effective divisors that are invariant under the action of G, and their dual spaces (for the bilinear map $\langle ., . \rangle_Y$ defined in equation (4.2.3)). We study their structure as $K[G]$-modules when τ is unramified. We also show that the map $\langle ., . \rangle_Y$ is compatible with the action of G, in the sense of Proposition 37. Thus, we show that when τ is unramified, the Goppa codes defined by divisors of Y invariant under the action of G are $K[G]$-modules. Finally, we give sufficient conditions for these codes to be free $K[G]$-modules when τ is an unramified abelian cover.

Galois actions

In this paragraph, we do not need to assume that K is a finite field. Let K be a perfect field. Let X and Y be two smooth projective curves over K. Let

$$\tau : Y \longrightarrow X$$

be a Galois cover over K with Galois group G. We can define a right action of G on $K(Y)$ by

$$\forall f \in K(Y), \forall \sigma \in G, \ f \cdot \sigma = f \circ \sigma. \tag{4.5.1}$$

Definition 38. Let $\sigma \in \mathrm{Aut}(Y)$. Recall that $\Omega(Y/K)$ is a $K(Y)$-vector space of dimension 1. Let dt be a generator of $\Omega(Y/K)$. Let $\omega \in \Omega(Y/K)$ be a differential, there exists $f \in K(Y)$ such that $\omega = f dt$. We define the pullback of ω by σ as

$$\sigma^* \omega = (f \circ \sigma) d(t \circ \sigma).$$

Remark 23. The definition of pullback does not depend on the choice of dt. Let dt_2 be a generator of $\Omega(Y/K)$ as a $K(Y)$-vector space, there exists $g \in K(Y)$ such that $\omega = g dt_2$. We have

$$\frac{dt_2}{dt} = \frac{f}{g}.$$

Since $x \mapsto x \circ \sigma$ is a morphism of K-algebras, we have

$$\frac{d(t_2 \circ \sigma)}{d(t \circ \sigma)} = \frac{dt_2}{dt} \circ \sigma.$$

Then

$$\begin{aligned}
\sigma^* \omega &= (f \circ \sigma) d(t \circ \sigma) \\
&= (f \circ \sigma) \frac{d(t \circ \sigma)}{d(t_2 \circ \sigma)} d(t_2 \circ \sigma) \\
&= (f \circ \sigma)(\frac{dt}{dt_2} \circ \sigma) d(t_2 \circ \sigma) \\
&= (g \circ \sigma) d(t_2 \circ \sigma)
\end{aligned}$$

We can thus define a right action of G on $\Omega(Y/K)$ by

$$\forall \omega \in \Omega(Y/K), \forall \sigma \in G,\ \omega \cdot \sigma = \sigma^* \omega$$

which is canonically associated with a left action

$$\forall \omega \in \Omega(Y/K), \forall \sigma \in G,\ \sigma \cdot \omega = (\sigma^{-1})^* \omega. \tag{4.5.2}$$

We have the following compatibility equation:

$$\forall \omega \in \Omega(Y/K), \forall f \in K(Y), \forall \sigma \in G,\ \sigma \cdot (f\omega) = (f \cdot \sigma^{-1})(\sigma \cdot \omega). \tag{4.5.3}$$

Extensions of residue algebras

Let K be a perfect field. Let X and Y be two smooth projective curves over K. Let

$$\tau : Y \longrightarrow X$$

be a Galois cover over K with Galois group G. We now assume that τ is unramified.

We want to show that the residual algebras at effective divisors of Y that are invariant under the action of G are free $K[G]$-modules. We begin with the case of the fiber of a single K-rational point.

Let P be a place of $K(X)$ of degree 1 totally split in $K(Y)$. Let Q_1 be a place of $K(Y)$ above P. In particular, $\deg Q_1 = 1$. We write

$$\forall \sigma \in G,\ Q_\sigma := \sigma(Q_1) \text{ and } Q = \sum_{\sigma \in G} Q_\sigma.$$

The divisor Q is the fiber of τ above P. Let

$$\tau^* : \mathrm{Div}(X) \longrightarrow \mathrm{Div}(Y)$$

be the abelian group morphism induced by τ, which, with a place associates the fiber of τ above this place. By definition, $Q = \tau^*(P)$.

One has canonical isomorphisms of K-algebras

$$\forall \sigma \in G, K_{Q_\sigma} \simeq K$$

and

$$\mathbf{R}_Q = \Gamma_Y(\mathcal{O}_Y/\mathcal{O}_Y(-Q)) \simeq \bigoplus_{\sigma \in G} K_{Q_\sigma} \simeq K^G.$$

The group G acts on $\mathbf{R}_Q$ on the right by composition. Let $\sigma, \sigma' \in G$, and let $f \in K_{Q_\sigma}$, then

$$f \circ \sigma' \in K_{Q_{\sigma'^{-1}\sigma}}.$$

For all $f \in \mathbf{R}_Q$, we will write $f = (f_\sigma)_{\sigma \in G}$ where $f_\sigma \in K_{Q_\sigma}$.

$$\forall (f_\sigma)_{\sigma \in G} \in \mathbf{R}_Q, \forall \sigma' \in G,\ (f_\sigma)_{\sigma \in G} \cdot \sigma' = (f_{\sigma'\sigma} \cdot \sigma')_{\sigma \in G}. \tag{4.5.4}$$

This action gives $\mathbf{R}_Q$ the structure of a free right $K[G]$-module of rank 1.

Now consider the case of a single place of arbitrary degree. Let $P \in \mathrm{Irr}(X)$ be a place of X and let $Q = \tau^*(P)$. Let Q_1 be a place of Y above P. Let $D(Q_1/P)$ be the decomposition group of Q_1. The places above P are parameterized by the left classes of $G/D(Q_1/P)$. For all $\sigma \in G/D(Q_1/P)$, we define

$$Q_\sigma = \sigma(Q_1)$$

and we have

$$D(Q_\sigma/P) = \sigma D(Q_1/P)\sigma^{-1}$$

In particular

$$Q = \sum_{\sigma \in G/D(Q_1/P)} Q_\sigma.$$

One has a natural isomorphism

$$\mathbf{R}_Q \simeq \bigoplus_{\sigma \in G/D(Q_1/P)} K_{Q_\sigma}.$$

Let $\sigma \in D(Q_1/P)$ and let $f \in K_{Q_\sigma}$, then, since τ is unramified, $D(Q_\sigma/P)$ is isomorphic to the Galois group of the extension K_{Q_σ}/K_P. Furthermore, for any right class σ' of $D(Q_\sigma/P)\backslash G$, we have

$$f \circ \sigma' \in K_{Q_{\sigma'^{-1}\sigma}}.$$

We can therefore define an action on the right on $\mathbf{R}_Q$ in a similar way to equation (4.5.4). Let θ be a normal element of the extension K_{Q_1}/K_P, then the orbit of θ for the action of G forms a basis of $\mathbf{R}_Q$ as a K_P-vector space. Indeed, since θ is normal in K_{Q_1}/K_P,

$$\theta \cdot D(Q_1/P) \text{ is a basis of } K_{Q_1}.$$

Let $\sigma \in G$ represent the right class $D(Q_1/P)\sigma$, then $\theta \cdot \sigma$ is normal in the extension $K_{Q_{\sigma^{-1}}}/K_P$ and

$$\theta \cdot D(Q_1/P) \cdot \sigma = \theta \cdot \sigma \cdot D(Q_{\sigma^{-1}}/P) \text{ is a basis of } K_{Q_{\sigma^{-1}}}.$$

Therefore, $\theta \cdot G$ is a basis of $\mathbf{R}_Q$ as a K_P-vector space. Therefore, $\mathbf{R}_Q$ is a free right $K[G]$-module of rank $\deg P$.

Let us now consider the case of a place with positive multiplicity. Let $n > 0$ be an integer, and let $P \in \mathrm{Irr}(X)$. Let $Q = \tau^*(P)$. Let t be a uniformizer at P, then $t \circ \tau$ is a uniformizer at all places above P, which we will denote by t thereafter. Let us write

$$\mathbf{R}_{nQ} := \Gamma_Y(\mathcal{O}_Y/\mathcal{O}_Y(-nQ)),$$

then t induces an isomorphism of K-vector spaces

$$\mathbf{R}_{nQ} \simeq \mathbf{R}_Q[x]/(x^n) \tag{4.5.5}$$

via $t \longmapsto x$. The group G acts on the right on $\mathbf{R}_Q[x]/(x^n)$ via the action on the coefficients. Thus, since $t \circ \sigma = t$ for all $\sigma \in G$, the isomorphism (4.5.5) is an isomorphism of right $K[G]$-modules. Finally, we have

$$\mathbf{R}_Q[x]/(x^n) \simeq \mathbf{R}_Q^n.$$

Therefore, $\mathbf{R}_{nQ}$ is a free right $K[G]$-module of rank $n \deg P$.

We deduce the following proposition:

Proposition 47. Let X and Y be two smooth projective curves over K, a perfect field. Let

$$\tau : Y \longrightarrow X$$

be an unramified Galois cover with Galois group G. Let $P \in \mathrm{Div}(X)$ be an effective divisor and let $Q = \tau^*(P)$. Then $\mathbf{R}_Q$ is a free right $K[G]$-module of rank $\deg P$.

Duality

Let K be a perfect field. Let X and Y be two smooth projective curves over K. Let

$$\tau : Y \longrightarrow X$$

be an unramified Galois cover over K with Galois group G. Let $P_1, \ldots, P_n \in X(K)$ be distinct K-rational points of X that are totally split in Y. Let

$$P = P_1 + \cdots + P_n \text{ and } Q = \tau^*(P).$$

Let $i \in [1..n]$, and let $Q_{i,1}$ be a K-rational point of Y above P_i. Let $\sigma \in G$, we set

$$Q_{i,\sigma} = \sigma(Q_{i,1}).$$

One has

$$Q = \sum_{i=1}^{n} \sum_{\sigma \in G} Q_{i,\sigma}.$$

The dual space of $\mathbf{R}_Q$ as a K-vector space is

$$\Omega_Q = \Gamma_Y(\Omega_{Y/K}(-Q)/\ Omega_{Y/K}) \simeq \bigoplus_{i=1}^{n} \bigoplus_{\sigma \in G} \Gamma_Y(\Omega_{Y/K}(-Q_{i,\sigma})/\Omega_{Y/K})$$

via the K-bilinear form

$$\begin{array}{rccc} \langle ., . \rangle_Y : & \mathbf{R}_Q \times \Omega_Q & \longrightarrow & K \\ & (f, \omega) & \longmapsto & \sum_{i=1}^{n} \sum_{\sigma \in G} \mathrm{Res}_{Q_{i,\sigma}}(f\omega) \end{array}$$

First, we note that the action of G on the left on $\Omega(Y/K)$ induces an action on the left on Ω_Q by permutation of the germs. Let $\omega = (\omega_{i,\sigma})_{i,\sigma \in [1..n] \times G} \in \Omega_Q$. Let $\sigma' \in G$, for all $1 \leqslant i \leqslant n$ and for all $\sigma \in G$ we have

$$(\sigma' \cdot \omega)_{i,\sigma} = ({\sigma'}^{-1})^* \omega_{i,\sigma'^{-1}\sigma}. \tag{4.5.6}$$

This action defines a free left $K[G]$-module structure of rank n on Ω_Q. Furthermore, equations (4.5.3), (4.5.4), and (4.5.6) show that the K-bilinear form $\langle ., . \rangle_Y$ satisfies the compatibility relation in Proposition 37:

$$\forall f \in \mathbf{R}_Q, \forall \omega \in \Omega_Q, \forall \sigma \in G,\ \langle f \cdot \sigma, \omega \rangle_Y = \langle f, \sigma \cdot \omega \rangle.$$

We can therefore define a $K[G]$-bilinear map by following Proposition 38:

$$\begin{array}{rccc} \langle ., . \rangle_G : & \Omega_Q \times \mathbf{R}_Q & \longrightarrow & K[G] \\ & (\omega, f) & \longmapsto & \sum_{\sigma \in G} \langle f \cdot \sigma^{-1}, \omega \rangle_Y \sigma \end{array}.$$

The map $\langle ., . \rangle_G$ allows to identify Ω_Q to the dual module of $\mathbf{R}_Q$, as a $K[G]$-module.

Morphisms and codes

We use the notation from the beginning of paragraph 4.5.1. We assume that K is a finite field with $q = p^m$ elements. Let $E \in \mathrm{Div}(Y)$ be a G-invariant divisor disjoint from Q. There exists $D \in \mathrm{Div}(X)$ such that

$$\tau^*(D) = E$$

because the cover τ is unramified. Let

$$\mathcal{L}(E) := \Gamma_Y(\mathcal{O}_Y(E))$$

be the Riemann-Roch space associated with E. The right action of G on $K(Y)$ defined in equation (4.5.1) induces a structure of right $K[G]$-module on $\mathcal{L}(E)$. Indeed, let $f \in K(Y)$, then for all $\sigma \in G$ we have

$$(f \cdot \sigma) = \sigma^{-1} \cdot (f). \tag{4.5.7}$$

Equations (4.5.1) and (4.5.4) indicate that the canonical evaluation morphism introduced in Section 4.2

$$\mathrm{ev}_{E,Q} : \mathcal{L}(E) \longrightarrow \mathbf{R}_Q$$

is a right $K[G]$-module morphism.

Similarly, let

$$\Omega(E-Q) = \Gamma_Y(\Omega_{Y/K}(E-Q)).$$

The left action of G on $\Omega(Y/K)$ defined in equation (4.5.2) induces a left $K[G]$-module structure on $\Omega(E-Q)$. Indeed, let $\omega \in \Omega(Y/K)$, then for all $\sigma \in G$,

$$\mathrm{div}(\sigma \cdot \omega) = \sigma \cdot \mathrm{div}\,\omega. \tag{4.5.8}$$

Equations (4.5.2) and (4.5.6) indicate that the canonical morphism

$$\mathrm{res}_{E,Q} : \Omega(E-Q) \longrightarrow \Omega_Q$$

is a left $K[G]$-module morphism.

Let g_Y be the genus of Y. Assume that

$$2g_Y - 2 < \deg E < \deg Q,$$

so that $\mathrm{ev}_{E,Q}$ and $\mathrm{res}_{E,Q}$ are injective. We then see $\mathcal{L}(E)$ as a right submodule of $\mathbf{R}_Q$ and $\Omega(E-Q)$ as a left submodule of Ω_Q. We have seen that Ω_Q is isomorphic to the dual of $\mathbf{R}_Q$ via the map $\langle ., . \rangle_G$. The orthogonal of $\mathcal{L}(E)$ for the map $\langle ., . \rangle_G$ is the orthogonal of $\mathcal{L}(E)$ for the form $\langle ., . \rangle_Y$, i.e. the space of differentials $\Omega(E-Q)$.

We will denote $K[G]^{\mathrm{supp}\,P}$ by $K[G]^P$. Let us define the respectively right and left morphisms of $K[G]$-modules

$$\begin{array}{rccc} \psi : & \mathbf{R}_Q & \longrightarrow & K[G]^P \\ & f & \longmapsto & (\sum_{\sigma\in G} f(Q_{i,\sigma^{-1}})\sigma)_{P_i\in P} \end{array},$$

and

$$\begin{array}{rccc} \chi : & \Omega_Q & \longrightarrow & K[G]^P \\ & \omega & \longmapsto & (\sum_{\sigma\in G} \mathrm{Res}_{Q_{i,\sigma}}(\omega)\sigma)_{P_i\in P} \end{array}.$$

We have

$$\forall f \in \mathbf{R}_Q, \forall \omega \in \Omega_Q, \langle \omega, f \rangle_G = \langle \chi(\omega), \psi(f) \rangle$$

where $\langle ., . \rangle$ is the $K[G]$-bilinear form defined in (4.4.1), and therefore

$$\forall f \in \mathbf{R}_Q, \forall \omega \in \Omega_Q, \langle f, \omega \rangle_Y = \langle \psi(f), \chi(\omega) \rangle_K.$$

We define

$$\mathrm{Gop}^G(Q,E) = \psi(\mathcal{L}(E))$$

and

$$\mathrm{Gop}^G_\Omega(Q,E) = \chi(\Omega(E-Q)).$$

If $\mathcal{L}(E)$ (or equivalently $\Omega(E-Q)$) is a free $K[G]$-module, then $\mathrm{Gop}^G(Q,E)$ and $\mathrm{Gop}^G_\Omega(Q,E)$ are also free, and we can apply the results of Section 4.4. In paragraph 4.5.1, we give sufficient conditions on E for $\mathcal{L}(E)$ to be free when G is abelian.

Remark 24. The isomorphisms ψ and χ are not canonical because they depend on the choice of $(Q_{i,1})_{i\in n}$. This has little impact on the codes $\mathrm{Gop}^G(Q,E)$ and $\mathrm{Gop}^G_\Omega(Q,E)$ because changing the choice of $Q_{i,1}$ amounts to multiplying the i-th component of the elements of $\mathrm{Gop}^G(Q,E)$ and $\mathrm{Gop}^G_\Omega(Q,E)$ by an element of G, which does not change the weight of the code words.

Remark 25. In the case where E and Q are not disjoint, we can still define $K[G]$-codes $\mathrm{Gop}^G(Q,E)$ and $\mathrm{Gop}^G_\Omega(Q,E)$ by proceeding as in Remark 11 with one precaution: the chosen uniformizers must be permuted by the action of G on the right. A simple solution is to take uniformizers at the $(P_i)_{1\leqslant i\leqslant n}$ and use the uniformizers induced on the fibers.

Freeness of modules of functions

We restrict ourselves to the abelian case. Let K be a finite field with $q=p^m$ elements. Let X and Y be two smooth projective curves over K. Let

$$\tau : Y \longrightarrow X$$

be an unramified abelian cover over K with Galois group G. Let g_X be the genus of X, g_Y the genus of Y, and $\mathfrak{o}$ the order of G. The Riemann-Hurwitz formula shows that

$$g_Y - 1 = \mathfrak{o}(g_X - 1).$$

In this context, it can be shown that under certain mild conditions, $\mathcal{L}(E)$ is a free $K[G]$-module. The main strategy will be to show that $\mathcal{L}(E)$ is isomorphic to a residue algebra at an effective G-invariant divisor of Y. We begin by proving a proposition based on the semisimplicity of $K[G]$ when p does not divide $\mathfrak{o}$.

Proposition 48. We use the notation from the beginning of paragraph 4.5.1. Suppose that p does not divide $\mathfrak{o}$. Let $D\in\mathrm{Div}(X)$ be a divisor of degree $\deg D \geqslant g_X$. Let $E=\tau^*(D)$, then $\mathcal{L}(E)$ contains a free right $K[G]$-module of rank $\deg D - g_X + 1$.

Proof. The K-algebra $K[G]$ is semisimple according to Maschke's theorem [Lan02, Chapter XVIII, Theorem 1.2]. Thus, every $K[G]$-module is semisimple [Lan02, Chapter XVII, Proposition 4.1], i.e., it decomposes as a direct sum of simple submodules. Let $\mathcal{S}$ be the set of simple $K[G]$-modules (considered up to isomorphism). $\mathcal{S}$ is finite since $K[G]$ is Noetherian (and semisimple). Then

$$\mathcal{L}(E) \simeq \bigoplus_{S\in\mathcal{S}} (\mathcal{L}(E) : S) S$$

where $(\mathcal{L}(E) : S)$ denotes the Jordan-Hölder multiplicity of S in $\mathcal{L}(E)$ (see definition 52). Let $\bar{K}$ be an algebraic closure of K. Let $\hat{G} = \mathrm{Hom}(G, \bar{K}^*)$ be the dual group of G. Then every simple $\bar{K}[G]$-module is a $\bar{K}$-vector space of dimension 1 associated with a unique character $\chi\in\hat{G}$ [Lan02, Chapter XVIII, Theorem 3.1]. We denote by S_χ the simple

$\bar{K}[G]$-module associated with $\chi \in \hat{G}$. Noticing that, since the regular representation is the sum of all irreducible representations,

$$\bar{K}[G] = \bigoplus_{\chi \in \hat{G}} S_\chi = \bigoplus_{S \in \mathcal{S}} S \otimes_K \bar{K}$$

we deduce that for every $\chi \in \hat{G}$, there exists a unique $S \in \mathcal{S}$ such that

$$(S \otimes_K \bar{K} : S_\chi) \neq 0$$

(in which case $(S \otimes_K \bar{K} : S_\chi) = 1$). We have

$$\mathcal{L}(E) \otimes_K \bar{K} \simeq \bigoplus_{S \in \mathcal{S}} (\mathcal{L}(E) : S) S \otimes_K \bar{K}.$$

Let

$$\mu = \min_{\chi \in \hat{G}} \{(\mathcal{L}(E) \otimes_K \bar{K} : S_\chi)\}.$$

For all $\chi \in \hat{G}$, there exists $S \in \mathcal{S}$ such that

$$(\mathcal{L}(E) \otimes_K \bar{K} : S_\chi) = (\mathcal{L}(E) : S).$$

Therefore,

$$\mu = \min_{S \in \mathcal{S}} \{(\mathcal{L}(E) : S)\}.$$

It is then clear that $\mathcal{L}(E)$ contains a free $K[G]$-module of rank μ. We show that $\mu \geqslant \deg D - g_X + 1$.

Let $\chi \in \hat{G}$. Since $\bar{K}(Y)$ is a $\bar{K}[G]$-module, it contains an eigenspace associated with χ. This eigenspace is nonzero (see Theorem **??** below). Let $r \in \bar{K}(Y)$ be an eigenvector associated with χ. This implies that the divisor (r) of r is G-invariant, so there exists $R \in \mathrm{Div}(X_{\bar{K}})$ such that $\tau^*(R) = (r)$. Let $(\mathcal{L}(E) \otimes_K \bar{K})_\chi$ be the eigenspace of $\mathcal{L}(E) \otimes_K \bar{K}$ associated with χ. Let $f \in (\mathcal{L}(E) \otimes_K \bar{K})_\chi$, then f/r is invariant under the action of G. We can therefore view f/r as a function on $X_{\bar{K}}$. We then have an isomorphism of $\bar{K}$-vector spaces between $(\mathcal{L}(E) \otimes_K \bar{K})_\chi$ and $\Gamma_{X_{\bar{K}}}(\mathcal{O}_{\bar{K}}(D + R))$:

$$\begin{array}{ccc} (\mathcal{L}(E) \otimes_K \bar{K})_\chi & \longrightarrow & \Gamma_{X_{\bar{K}}}(\mathcal{O}_{\bar{K}}(D + R)) \\ f & \longmapsto & f/r \end{array}.$$

Therefore, according to the Riemann-Roch theorem,

$$\dim_{\bar{K}}((\mathcal{L}(E) \otimes_K \bar{K})_\chi) = \dim_{\bar{K}}(\Gamma_{X_{\bar{K}}}(\mathcal{O}_{\bar{K}}(D + R))) \geqslant \deg D - g_X + 1.$$

In particular, since $(\mathcal{L}(E) \otimes_K \bar{K} : S_\chi) = \dim_{\bar{K}}((\mathcal{L}(E) \otimes_K \bar{K})_\chi)$, we obtain

$$\mu \geqslant \deg D - g_X + 1.$$

□

We then demonstrate a proposition that extends the results of this section on linear spaces of functions to linear spaces of differentials.

Proposition 49. Let $D \in \mathrm{Div}(X)$ be a divisor, and let C_X be a canonical divisor of X. Let $E = \tau^*(D)$ and $C_Y = \tau^*(C_X)$, then $\Omega(E)$ is a free left $K[G]$-module if and only if $\mathcal{L}(C_Y - E)$ is a free right $K[G]$-module.

Furthermore, $\Omega(E)$ contains a free submodule of rank $k \geqslant 0$ if and only if $\mathcal{L}(C_Y - E)$ contains a free submodule of rank k.

Proof. Let $\omega_0 \in \Omega(X/K)$ be a regular differential with divisor C_X, then $\tau^*(\omega_0)$, the pullback of ω_0 by τ, is a homogeneous differential on Y with divisor C_Y. The map

$$\begin{array}{ccc} \Omega(E) & \longrightarrow & \mathcal{L}(C_Y - E) \\ \omega & \longmapsto & \omega/\tau^*(\omega_0) \end{array}$$

is an isomorphism of K-vector spaces compatible with the action of G in the following sense:

$$\forall \sigma \in G, \forall \omega \in \Omega(E), \frac{\sigma \cdot \omega}{\tau^*(\omega_0)} = \frac{\sigma \cdot \omega}{\sigma \cdot \tau^*(\omega_0)} = \frac{\omega}{\tau^*(\omega_0)} \cdot \sigma^{-1}.$$

Since $\sigma \longrightarrow \sigma^{-1}$ defines an anti-isomorphism of $K[G]$, we deduce the result. □

Let $f \in K(X)$ be a nonzero function, then we have a divisor equality

$$\tau^*((f)) = (f \circ \tau).$$

Thus, τ^* induces a group morphism from $\mathrm{Pic}(X)$ to $\mathrm{Pic}(Y)$.

The following lemma allows us to produce non-special divisors of Y of degree $g_Y - 1$ that are invariant under the action of G.

Lemma 50. [CE23, Section 14] We use the notation from the beginning of paragraph 4.5.1. Let $\bar{K}$ be an algebraic closure of K. Let

$$\mathfrak{o} = \mathfrak{o}_p \times \mathfrak{o}_{p'}$$

where $\mathfrak{o}_p$ is the largest power of p dividing $\mathfrak{o}$. Let $c \in \mathrm{Pic}^{g_X - 1}(X_{\bar{K}})$, and let $\tau^*(c) \in \mathrm{Pic}^{g_Y - 1}(Y_{\bar{K}})$ be its pullback by τ. Then $\tau^*(c)$ is special if and only if c is the sum of a special class and a class in the intersection of the kernels of τ^* and of the multiplication by $\mathfrak{o}_{p'}$.

Proof. Let D be a divisor representing the class c. Let $E = \tau^*(D)$, which is a divisor of the class $\tau^*(c)$. Let

$$\mathcal{L}(E)_{\bar{K}} := \Gamma_{Y_{\bar{K}}}(\mathcal{O}_{Y_{\bar{K}}}(E)).$$

Assume that $\tau^*(c)$ is special, then $\mathcal{L}(E)_{\bar{K}}$ is a nonzero $\bar{K}[G]$-module (since its dimension is nonzero by hypothesis). Recall that G is a subgroup of the automorphisms of the $\bar{K}$-vector space of $\mathcal{L}(E)_{\bar{K}}$. Since G is finite and commutative, and $\bar{K}$ is algebraically closed, there

exists $f \in \mathcal{L}(E)_{\bar{K}}$ an eigenvector of all the elements of G. Therefore, there exists an effective divisor $J \in \mathrm{Div}(Y_{\bar{K}})$ such that

$$(f) = J - E.$$

Since f is an eigenvector of the action of G, its divisor (f) is stable under the action of G, and so is J. Therefore, there exists $I \in \mathrm{Div}(X_{\bar{K}})$ an effective divisor such that

$$\tau^*(I - D) = J - E = (f).$$

Let c' be the class of $D - I$, we deduce that $\tau^*(c') = 0$. Let c'' be the class of I, then c'' is special because I is effective, so

$$\dim_{\bar{K}} \mathcal{L}(I)_{\bar{K}} > 0.$$

We have $c = c' + c''$. It remains to be shown that $\mathfrak{o}_{p'} c' = 0$. First, note that $f^{\mathfrak{o}_{p'}}$ is stable under the action of G. Let $\sigma \in G$. Since $\bar{K}$ has characteristic p, every $\mathfrak{o}$-th root of unity is an $\mathfrak{o}_{p'}$-th root of unity. There therefore exists an $\mathfrak{o}_{p'}$-th root of unity ζ such that

$$f^{\mathfrak{o}_{p'}} \cdot \sigma = (f \cdot \sigma)^{\mathfrak{o}_{p'}} = (\zeta f)^{\mathfrak{o}_{p'}} = f^{\mathfrak{o}_{p'}}.$$

The function $f^{\mathfrak{o}_{p'}}$ is G-invariant, so there exists $g \in \bar{K}(X)$ such that $f^{\mathfrak{o}_{p'}} = g \circ \tau$. We have $\mathfrak{o}_{p'}(D - I) = -(g)$, so $\mathfrak{o}_{p'} c' = 0$.

The converse is straightforward. □

Theorem 51. *We use the notation from the beginning of paragraph 4.5.1. Let $E \in \mathrm{Div}(Y)$ be a divisor invariant under the action of G. Assume that*

$$\deg E > 2g_Y - 2.$$

Then $\mathcal{L}(E)$ is a free $K[G]$-module.

Proof. The proof is trivial if $g_X = 0$ because in this case G is trivial. We assume $g_X \geqslant 1$. Let $D \in \mathrm{Div}(X)$ be a divisor such that $\tau^*(D) = E$ (which exists because τ is unramified). Then $\deg D > 2g_X - 2$. Let $\bar{K}$ be an algebraic closure of K. According to the Noether-Deuring theorem [CR62, Theorem 29.7], it is enough to show that

$$\mathcal{L}(E)_{\bar{K}} := \mathcal{L}(E) \otimes_K \bar{K} \simeq \Gamma_{Y_{\bar{K}}}(\mathcal{O}_{Y_{\bar{K}}}(E))$$

is a free $\bar{K}[G]$-module.

Let

$$k = \deg D - g_X + 1$$

be the dimension of $\mathcal{L}(D)$ (according to the Riemann-Roch theorem). $\mathrm{Pic}^{g_X - 1}(X_{\bar{K}})$ is a variety over $\bar{K}$ of the same dimension as the Jacobian $\mathcal{J}_{X_{\bar{K}}}$, therefore of dimension g_X. For any class $c \in \mathrm{Pic}^{g_X - 1}(X_{\bar{K}})$, there exist

$$P_1, \ldots, P_k \in X(\bar{K})$$

such that the divisor $D - P_1 - \cdots - P_k$ is in the class c (since $k \geqslant g_X$). On the other hand, the set of special classes of degree $g_X - 1$ is a subvariety of $\mathrm{Pic}^{g_X-1}(X_{\bar{K}})$ of dimension $g_X - 1$. Furthermore, the kernel $\ker(\tau^*)$ of the group morphism τ^* is finite (since it is included in the kernel of the multiplication by $\mathfrak{o}$). Thus, by dimension, and since $\bar{K}$ is algebraically closed, there exist places $P_1, \ldots, P_k \in X(\bar{K})$ such that the class of $D - P_1 - \cdots - P_k$ is not the sum of a special class and a class of $\ker(\tau^*)$.

Let $P = P_1 + \cdots + P_k$ and $Q = \tau^*(P)$. According to Lemma 50, the divisor $E - Q$ is a non-special divisor of degree $g_Y - 1$. Then the evaluation morphism

$$\mathrm{ev}_{E,Q} : \mathcal{L}(E)_{\bar{K}} \longrightarrow \Gamma_{Y_{\bar{K}}}(\mathcal{O}_{Y_{\bar{K}}}(E)/\mathcal{O}_{Y_{\bar{K}}}(E - Q))$$

is an isomorphism of $\bar{K}[G]$-modules. Since $\Gamma_{Y_{\bar{K}}}(\mathcal{O}_{Y_{\bar{K}}}(E)/\mathcal{O}_{Y_{\bar{K}}}(E - Q))$ is isomorphic to $\mathbf{R}_Q \otimes_K \bar{K}$ as a $\bar{K}[G]$-module, then, according to Proposition 47, the $\bar{K}[G]$-module $\mathcal{L}(E)_{\bar{K}}$ is free. □

Proposition 52. We use the notation from the beginning of paragraph 4.5.1. Assume that K is a finite field with at least four elements, that $g_X \geqslant 2$ and that $\mathfrak{o}$ is a power of p. Let $d \geqslant g_X$ be an integer such that there exists an effective divisor of X of degree $d - g_X + 1$. Then there exists $E \in \mathrm{Div}(Y)$ a divisor invariant under the action of G of degree $d\mathfrak{o}$ such that $\mathcal{L}(E)$ is a free $K[G]$-module of rank $d - g_X + 1$.

Proof. Let $P \in \mathrm{Div}(X)$ be an effective divisor of degree $d - g_X + 1$. According to a theorem by Ballet and Le Brigand [BLB06, Theorem 11], there exists a non-special divisor I of X of degree $g_X - 1$. Let $D = I + P$. Let $E = \tau^*(D)$, $J = \tau^*(I)$ and $Q = \tau^*(P)$. Lemma 50 allows us to assert that J is a non-special divisor (note that $\mathfrak{o}_{p'} = 1$). Thus, the evaluation morphism

$$\mathrm{ev}_{E,Q} : \mathcal{L}(E) \longrightarrow \Gamma_Y(\mathcal{O}_Y(E)/\mathcal{O}_Y(E - Q)) \simeq \mathbf{R}_Q$$

is an isomorphism of $K[G]$-modules. Then Proposition 47 shows that $\mathcal{L}(E)$ is free. □

4.5.2 Encoding and decoding in the abelian case

In this subsection, we study the costs of encoding and decoding codes constructed with unramified abelian covers.

Let K be a finite field with $q = p^m$ elements. Let X and Y be two smooth projective curves over K and

$$\tau : Y \longrightarrow X$$

an unramified abelian cover with Galois group G. Let $\mathfrak{o}$ be the order of G, g_X the genus of X and g_Y the genus of Y. According to the Riemann-Hurwitz formula, we have

$$g_Y - 1 = \mathfrak{o}(g_X - 1).$$

Let $P_1, \ldots, P_n$ be K-rational points of X that totally split in Y, let

$$P = \sum_{i=1}^{n} P_i$$

and let

$$Q = \tau^*(P).$$

Let D be a divisor of X disjoint from P such that

$$2g_X - 1 \leqslant \deg D \leqslant n - 1.$$

Let

$$E = \tau^*(D).$$

Let

$$k = \deg D - g_X + 1.$$

According to Theorem 51, the $K[G]$-modules $\mathrm{Gop}^G(Q, E)$ and $\mathrm{Gop}^G_\Omega(Q, E)$ are free submodules of $K[G]^P$ with ranks k and $n - k$ respectively. Let

$$N = \mathfrak{o}n.$$

Then, according to definition 35, $\mathrm{Gop}^G(Q, E)$ defines a linear code over K of length N and dimension $\mathfrak{o}k$. Its designed distance is

$$d^*(Q, E) = N - \deg E = N - \mathfrak{o}k - g_Y + 1.$$

Let φ and ι be the K-linear isomorphisms defined in equations (4.4.4) and (4.4.5). We can check that

$$\varphi \circ \iota(\mathrm{Gop}^G(Q, E)) = \mathrm{Gop}(Q, E) \text{ and } \varphi(\mathrm{Gop}^G_\Omega(Q, E)) = \mathrm{Gop}_\Omega(Q, E).$$

According to the results in Section 4.4.4, there exists

$$\mathcal{E} \in \mathcal{M}_{P,k}(K[G])$$

a G-generator matrix of $\mathrm{Gop}^G(Q, E)$, to which we associate a generator matrix of $\mathrm{Gop}(Q, E)$

$$\mathcal{E}_K \in \mathcal{M}_{k\times G, P\times G}(K),$$

and there exists

$$\mathcal{C} \in \mathcal{M}_{(n-k),P}(K[G])$$

a G-parity-check matrix of $\mathrm{Gop}^G(Q, E)$ (or equivalently, a G-generator matrix of $\mathrm{Gop}^G_\Omega(Q, E)$), to which we associate a generator matrix of $\mathrm{Gop}_\Omega(Q, E)$

$$\mathcal{C}_K \in \mathcal{M}_{(n-k)\times G, P\times G}(K).$$

Encoding

We use the notation defined at the beginning of Subsection 4.5.2. We seek to encode an element $a \in K^{k\times G}$ into an element of $\mathrm{Gop}(Q,E)$. This amounts to computing

$$a\mathcal{E}_K = \varphi\circ\iota\left(\mathcal{E}(\varphi\circ\iota)^{-1}(a)\right). \tag{4.5.9}$$

In the worst case, the applications $\varphi\circ\iota$ and $(\varphi\circ\iota)^{-1}$ can be evaluated in $n\mathfrak{o}$ and $k\mathfrak{o}$ operations, respectively. Thus, the cost of encoding a is reduced to the cost of computing

$$\mathcal{E}(\varphi\circ\iota)^{-1}(a).$$

This operation requires computing kn multiplications in $K[G]$. According to Theorem 36, there exists an absolute constant $\mathcal{Q}$ such that a multiplication in $K[G]$ requires at most

$$\mathcal{Q}(m\mathfrak{o}\log\mathfrak{o} + m^2\mathfrak{o})$$

operations in $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/p'\mathbb{Z}$, where p' is a prime and $p' \leqslant \mathcal{Q}(\mathfrak{o}p)^{11}$. Then there exists an absolute constant $\mathcal{Q}'$ such that the computation (4.5.9) can be performed with

$$\mathcal{Q}'\cdot kn\cdot\mathfrak{o}\log\mathfrak{o}\cdot m^2\cdot(\log\mathfrak{o}+\log p)^2$$

elementary operations.

In the construction of Subsection **??**, there exists an absolute constant $\alpha > 0$ such that $\alpha\sqrt[4]{q}\log\mathfrak{o} \geqslant k\log p$ and $\alpha\log\mathfrak{o} \geqslant \log p$. Then

$$\begin{aligned}
\mathcal{Q}'\cdot nk\cdot\mathfrak{o}\log\mathfrak{o}\cdot m^2\cdot(\log\mathfrak{o}+\log p)^2 &\leqslant \mathcal{Q}'\cdot m^2\cdot N\cdot\log\mathfrak{o}\cdot(k\log\mathfrak{o}+\alpha\sqrt[4]{q}\log\mathfrak{o})\cdot(\log\mathfrak{o}+\log p)\\
&\leqslant \mathcal{Q}'\cdot m^2\cdot N\cdot\log\mathfrak{o}\cdot(\alpha\sqrt[4]{q}(\log\mathfrak{o})^2+\alpha\sqrt[4]{q}\log\mathfrak{o})\cdot(\log\mathfrak{o}+\alpha\log\mathfrak{o})\\
&\leqslant \mathcal{Q}'\cdot m^2\cdot N\cdot(\log\mathfrak{o})\cdot\alpha\sqrt[4]{q}\cdot((\log\mathfrak{o})^2+\log\mathfrak{o})\cdot(1+\alpha)\cdot\log\mathfrak{o}\\
&\leqslant \mathcal{Q}''\cdot m^2\cdot\sqrt[4]{q}\cdot N\cdot(\log\mathfrak{o})^4\\
&\leqslant \mathcal{Q}''\cdot m^2\cdot\sqrt[4]{q}\cdot N(\log N)^4
\end{aligned}$$

where $\mathcal{Q}''$ is an absolute constant. If we consider that $q = p^m$ is fixed, then the encoding is quasi-linear in the length N of the code.

Decoding

We use the notation defined at the beginning of Subsection 4.5.2. Let $f_r, f_c, f_e \in \mathbf{R}_Q$ such that

$$f_r = f_c + f_e,\ \ f_c \in \mathrm{Im}\ \mathrm{ev}_{E,Q} \text{ and } \#\operatorname{supp} f_e \leqslant t^*(Q,E).$$

We write

$$Q_{\mathrm{err}} = \operatorname{supp} f_e \text{ and } t = \deg Q_{\mathrm{err}}.$$

We know from Subsection 4.2.3 that given f_r, it is possible to compute f_c in $O(N^3)$ operations in K if

$$t \leqslant \frac{d^*(Q,E) - g_Y - 1}{2}.$$

Assume that

$$t \leqslant \mathfrak{o}\lfloor \frac{d^*(P,D) + g_X - 1}{2} \rfloor - g_Y. \tag{4.5.10}$$

Let $F \in \mathrm{Div}(Y)$ be a divisor of degree

$$\deg F = \mathfrak{o}\lfloor \frac{d^*(P,D) + g_X - 1}{2} \rfloor = \mathfrak{o}\lfloor \frac{n-k}{2} \rfloor$$

disjoint from Q and invariant under the action of G (note that $\mathfrak{o}$ divides $\deg F$). We then have

$$g_Y + t \leqslant \deg F \leqslant N - 1 - \deg E - t.$$

We assume that the right $K[G]$-module $\mathcal{L}(F)$ contains a free sub-$K[G]$-module of rank $(\deg F/\mathfrak{o}) - g_X + 1$. Note that if

$$\lfloor \frac{n-k}{2} \rfloor > 2(g_X - 1) \tag{4.5.11}$$

or

$$\mathfrak{o} \text{ is corprime to } p \tag{4.5.12}$$

or

$$\mathfrak{o} \text{ is a power of } p \text{ and } q \geqslant 4 \text{ and } g_X \geqslant 2, \tag{4.5.13}$$

then, by Theorem 51 or Proposition 48 or Proposition 52, $\mathcal{L}(F)$ does indeed contain a free sub-$K[G]$-module of rank $(\deg F/\mathfrak{o}) - g_X + 1$. To simplify the notation, even if it means restricting $\mathcal{L}(F)$, we will assume that $\mathcal{L}(F)$ is a free $K[G]$-module of rank $(\deg F/\mathfrak{o}) - g_X + 1$.

Since $g_Y + t \leqslant \deg F \leqslant N - 1 - \deg E - t$, we know that, as in Subsection 4.2.3, the maps $\mathrm{ev}_{F,Q}$ and $\mathrm{ev}_{E+F,Q}$ are injective, and that $h \in \mathcal{L}(F)$ vanishes at Q_{err} if and only if $\mathrm{ev}_{F,Q}(h)f_r \in \mathrm{Im}\ \mathrm{ev}_{E+F,Q}$. Under our assumptions, $\mathrm{ev}_{F,Q}$ and $\mathrm{ev}_{E+F,Q}$ are injective morphisms of $K[G]$-modules. Let

$$\mathcal{E}_F \in \mathcal{M}_{P,(\ell(F)/\mathfrak{o})}(K[G])$$

be a G-generator matrix of $\mathcal{L}(F)$ and

$$\mathcal{E}_{F,K} \in \mathcal{M}_{(\ell(F)/\mathfrak{o})\times G, P\times G}(K)$$

the associated matrix with coefficients in K, and

$$\mathcal{C}_{E+F} \in \mathcal{M}_{(n-\ell(E+F)/\mathfrak{o}),P}(K[G])$$

a G-parity-check matrix of $\mathcal{L}(E+F)$, and

$$\mathcal{C}_{E+F,K} \in \mathcal{M}_{(n-\ell(E+F)/\mathfrak{o})\times G, P\times G}(K)$$

the associated matrix with coefficients in K. Finally, let

$$\mathcal{D}_r \in \mathcal{M}_n(K)$$

be the diagonal matrix corresponding to multiplication by f_r (coordinate by coordinate).

Here, the matrix $\mathcal{D}_r$ is not generally associated with a matrix with coefficients in $K[G]$, so $\ker(\mathcal{E}_{F,K} \times \mathcal{D}_r \times {\mathcal{C}_{E+F,K}}^t)$ is not generally a $K[G]$-module. Finding an element of the kernel (on the left) of this matrix product cannot be reduced to a linear algebra problem over $K[G]$. We will try to use Theorem 53. We must show that it is possible to quickly evaluate (on the left) the matrices $\mathcal{E}_{F,K}$, $\mathcal{D}_r$ and ${\mathcal{C}_{E+F,K}}^t$.

According to the previous paragraph, using fast arithmetic in $K[G]$, it is possible to evaluate the matrix $\mathcal{E}_{F,K}$ with an absolute constant times

$$n \cdot (\lfloor (n-k)/2 \rfloor) \cdot m^2 \cdot \mathfrak{o} \log \mathfrak{o} \cdot (\log \mathfrak{o} + \log p)^2$$

elementary operations. Next, the matrix $\mathcal{D}_r$ is diagonal, so it can be evaluated by performing $N = \mathfrak{o}n$ multiplications in K. Finally, according to Proposition 45, the cost of multiplication by $\mathcal{C}^t_{E+F,K}$ is the cost of multiplication by $\mathcal{C}_{E+F}$. Thus, it is possible to evaluate ${\mathcal{C}_K}^t$ with an absolute constant times

$$n^2 \cdot m^2 \cdot \mathfrak{o} \log \mathfrak{o} \cdot (\log \mathfrak{o} + \log p)^2$$

elementary operations. Thus, there exists an absolute constant $\mathcal{Q}$ such that it is possible to evaluate $\mathcal{E}_{F,K} \times \mathcal{D}_r \times {\mathcal{C}_{E+F,K}}^t$ with

$$n^2 \cdot m^2 \cdot \mathfrak{o} \log \mathfrak{o} \cdot (\log \mathfrak{o} + \log p)^2$$

elementary operations.

We will now use a random algorithm from [Wie86, KS91].

Theorem 53 (Wiedemann, Kaltofen, Saunders)**.** *The notations in this theorem are independent. There exists a probabilistic (Las Vegas) algorithm that takes as input a matrix A of dimensions $\ell \times n$ with coefficients in a field K and a vector b of K^ℓ, and returns a uniformly distributed solution x of $Ax = b$ with a probability greater than $1/2$, at the cost of $\mathcal{Q}m \log m$ evaluations of A (as a black box) and $\mathcal{Q}(m \log m)^2$ operations in K (addition, multiplication, random draw, inversion), where $\mathcal{Q}$ is an absolute constant and $m = \max(\ell, n)$.*

Corollary 53.1. *We use the notation from the beginning of Subsection 4.5.2. We assume that equations (4.5.10) and (4.5.11) are verified. There is a probabilistic algorithm (Las Vegas) that takes as input $f_r \in \mathbf{R}_Q$ and the matrices $\mathcal{E}_{F,K}$, $\mathcal{E}_F$, $\mathcal{C}_{E+F,K}$ and $\mathcal{C}_{E+F}$ and returns f_c with a probability greater than $1/2$, at the cost of*

$$\mathcal{Q} \cdot n^2 \cdot N^2 (\log N)^2 \cdot m^2 \cdot (\log p + \log \mathfrak{o})^2$$

elementary operations, where $\mathcal{Q}$ is an absolute constant.

Remark 26. We have explained how to find the localizations of the errors by finding a solution to

$$x\mathcal{E}_{F,K} \times \mathcal{D}_r \times \mathcal{C}^t_{E+F,K} = 0.$$

If the error location Q_{err} is not a G-invariant divisor, $\mathbf{R}_{Q-Q_{\mathrm{err}}}$ is not a $K[G]$-module. The equation

$$\mathrm{ev}_{E,Q-Q_{\mathrm{err}}}(x) = f_c$$

is therefore not $K[G]$-linear. This is not a problem because we can use the same trick: the map $\mathrm{ev}_{E,Q-Q_{\mathrm{err}}}$ can be evaluated quickly by restricting the map $\mathrm{ev}_{E,Q}$. By applying Theorem 53, we show that this equation can be solved in

$$\mathcal{Q}' \cdot n \cdot N^2 (\log N)^2 \cdot m^2 \cdot (\log p + \log \mathfrak{o})^2$$

elementary operations, where $\mathcal{Q}'$ is an absolute constant.

In the construction of Section 4.5.3, there exists an absolute constant $\alpha > 0$ such that

$$\alpha \sqrt[4]{q} \log \mathfrak{o} \geqslant k \log p$$

and

$$\alpha \log \mathfrak{o} \geqslant \log p$$

and

$$\alpha \sqrt[4]{q} \log \mathfrak{o} \geqslant n.$$

Then there exists an absolute constant $\mathcal{Q}''$ such that the decoding algorithm can be performed with

$$\mathcal{Q}'' \cdot m^2 \cdot \sqrt[4]{q} \cdot N^2 (\log N)^5$$

elementary operations. In particular, if we consider that $q = p^m$ is fixed, then decoding is quasi-quadratic in the length N of the code.

4.5.3 Families of structured geometric codes

In this section, we construct an asymptotically good family of Goppa codes associated with divisors that are invariant under the action of some Galois groups (i.e., the liminf of the rates and relative distances are nonzero), and whose encoding and decoding algorithms have quasi-linear and quasi-quadratic time complexities, respectively.

The construction of this family relies on the existence of a family of unramified abelian covers

$$\tau_i : Y_i \longrightarrow X_i$$

of smooth projective curves over a finite field K with q elements, whose degree $\deg \tau_i$ grows exponentially with the genus g_{X_i} of X_i, and whose number of K-rational points of X_i completely split in Y_i grows linearly with the genus of X_i. According to Section 3.3,

in particular Theorem 14, any unramified abelian cover of X_i totally split above a point $P_\infty \in X_i(K)$ is the pullback of a factor of the isogeny

$$\Phi = F_{\mathcal{J}_{X_i}} - 1.$$

More precisely, to every subgroup H of $\mathcal{J}_{X_i}(K)$, we can associate

$$\tau_{i,H} : Y_{i,H} \longrightarrow X_i$$

an unramified abelian cover of X_i totally split above P_∞ with Galois group $\mathcal{J}_{X_i}(K)/H$. Let P be a K-rational point of X_i. Then, according to Proposition 15, the point P is totally split in $Y_{i,H}$ if and only if $P - P_\infty \in H$.

The success of the construction depends essentially on the ability to find subgroups of $\mathcal{J}_{X_i}(K)$ suited to our needs, for curves X_i having a large number of rational points. A significant number of previous works deal with similar problems. For example, if q is a square, we can find in [Iha81], [TVZ82], and [GS95] families of curves over K for which the ratio

$$\#X_i(K)/g_{X_i}$$

converges to $\sqrt{q} - 1$. Geometric techniques for constructing curves with many points, which are interesting for our problem, can also be found in [Ser20]. We will use another technique, used in [GX22, NX98, Que89, vdG09], which requires that K contain a strict subfield κ, that the curves X_i be defined over κ and have a κ-rational point.

We now explain our construction. Let $m > 0$ be an integer. Let κ be a finite field with p^{2m} elements and K an extension of κ of degree 2, i.e., a finite field with $q = p^{4m}$ elements. Since p^{2m} is a square, there exists a family $(X_i)_{i\in\mathbb{N}}$ of smooth projective curves over κ of genera $(g_{X_i})_{i\in\mathbb{N}}$, such that

$$\lim_{i\to\infty} \#X_i(\kappa)/g_{X_i} = p^m - 1.$$

To simplify notations, we will drop the index $i \in \mathbb{N}$ in what follows. Let

$$n = \#X(\kappa) > 0.$$

Let $P_1, \ldots, P_n$ be the κ-rational points of X. We naturally identify X with a smooth projective curve X_K over K, and $(P_j)_{j\in[1..n]}$ with the n points of X_K that are stable under the action of $\mathbf{Gal}(K/\kappa)$ on X_K. Let us write

$$P = \sum_{j=1}^{n} P_j.$$

Let

$$H = \mathcal{J}_X(\kappa)$$

be the group of κ-rational points of $\mathcal{J}_X(K)$, i.e., the points of $\mathcal{J}_X(K)$ that are stable under the action of $\mathbf{Gal}(K/\kappa)$. Let $\tilde{Y}$ be a smooth projective curve over K such that there exists

$$\tilde{\tau} : \tilde{Y} \longrightarrow X$$

a, unramified abelian cover totally split above P_1 with Galois group

$$\tilde{G} = \mathcal{J}_X(K)/H.$$

According to Riemann's hypothesis (proved for function fields by Weil [Wei48]), we have

$$\tilde{\mathfrak{o}} := |\tilde{G}| \geqslant (p^{2m}-1)^{2g_X}/(p^m+1)^{2g_X} = (p^m-1)^{2g_X}.$$

We want a Galois group whose order is either a power of p or coprime to p, in order to apply propositions 48 and 52. Write

$$\tilde{G} = \tilde{G}_p \times \tilde{G}_{p'}$$

where $\tilde{G}_p$ is a maximal subgroup of $\tilde{G}$ of order $\tilde{\mathfrak{o}}_p$ a power of p and $\tilde{G}_{p'}$ is a supplement of $\tilde{G}_p$, of order $\tilde{\mathfrak{o}}_{p'} = \tilde{\mathfrak{o}}/\tilde{\mathfrak{o}}_p$ coprime to p. Let $\tilde{H}$ be the smallest of these two subgroups. Then there exists Y a smooth projective curve over K and

$$\tau : Y \longrightarrow X$$

an unramified abelian cover totally split above P_1 with Galois group

$$G = \tilde{G}/\tilde{H}.$$

The order of G, denoted $\mathfrak{o}$, is either a power of p or coprime to p, and

$$\mathfrak{o} \geqslant \sqrt{\tilde{\mathfrak{o}}} \geqslant (p^m-1)^{g_X}.$$

All κ-rational points of X are totally split in Y (since they are totally split in $\tilde{Y}$). Let

$$Q = \tau^*(P),$$

be a divisor on Y of degree

$$\deg Q = n\mathfrak{o} = N.$$

We assume that

$$p^m > 3,$$

so, on the one hand, $\mathfrak{o} \geqslant (p^m-1)^{g_X}$ grows exponentially with respect to g_X and, on the other hand, we have

$$(p^m-1)g_X > 2g_X - 1.$$

Thus, we have asymptotically

$$n > 2g_X - 1.$$

Let

$$\delta_{lim} \in]0, 1 - \frac{2}{p^m-1}[$$

and let

$$\rho_{lim} = 1 - \delta_{lim} - \frac{1}{p^m-1} \in]\frac{1}{p^m-1}, 1 - \frac{1}{p^m-1}[.$$

Let $D \in \mathrm{Div}(X)$ be a divisor disjoint from P, such that

$$\deg D = \lceil \rho_{lim} n + g_X - 1 \rfloor.$$

Then asymptotically we have

$$2g_X - 2 < \deg D < (p^m - 1)g_X \approx n.$$

Let

$$E = \tau^*(D)$$

and

$$k = \deg D - g_X + 1.$$

Then $\mathcal{L}(E)$ is a free $K[G]$-module of rank k. We have

$$|\rho(\mathrm{Gop}(Q, E)) - \rho_{lim}| \leqslant \frac{1}{2n} \text{ and } |\delta^*(Q, E) - \delta_{lim}| \leqslant \frac{1}{2n}$$

where $\delta^*(Q, E) := d^*(Q, E)/N$ denotes the designed relative distance of $\mathrm{Gop}(Q, E)$.

Let $\varepsilon > 0$. We ask to be able to decode $\lfloor \varepsilon n \mathfrak{o} \rfloor$ errors for the code $\mathrm{Gop}(E, Q)$. According to equation (4.5.10), it is possible to decode at most

$$\mathfrak{o} \lfloor \frac{d^*(P, D) + g_X - 1}{2} \rfloor - g_Y \approx \frac{d^*(Q, E) - g_Y - 1}{2}$$

errors. We must therefore have

$$0 < \varepsilon \leqslant \frac{1}{2} \left(\frac{d^*(Q, E)}{nfo} - \frac{g_Y + 1}{nfo} \right) \approx \frac{1}{2} \left(\delta^*(D, P) - \frac{1}{p^m - 1} \right).$$

We must impose

$$\delta_{lim} > \frac{1}{p^m - 1}$$

which implies

$$\frac{1}{p^m - 1} < 1 - \frac{2}{p^m - 1}$$

or, equivalently,

$$p^m > 4.$$

Recall that

$$\log \mathfrak{o} \geqslant g_X \log(p^m - 1),$$

so since $n \approx (\sqrt[4]{q} - 1)g_X$, there exists an absolute constant

$$\alpha > 0$$

(in particular, independent of the index $i \in \mathbb{N}$) such that

$$\alpha \sqrt[4]{q} \log \mathfrak{o} \geqslant k \log p \text{ and } \alpha \sqrt[4]{q} \log \mathfrak{o} \geqslant n \text{ and } \alpha \log \mathfrak{o} \geqslant \log p. \tag{4.5.14}$$

Note also that one of the conditions (4.5.12) or (4.5.13) is satisfied by construction. Therefore, based on the results in Subsection 4.5.2, we deduce Theorem 54.

Theorem 54. *Let p be a prime integer and $m > 0$ an integer such that*

$$p^m \geqslant 4.$$

Let K be a finite field with p^{4m} elements. Let

$$\delta_{lim} \in]0, 1 - \frac{2}{p^m - 1}[.$$

Then there exists a family of geometric codes equipped with a module structure of a K-group algebra

- *whose lengths tend to infinity.*
- *whose designed relative distances converge to $\delta_{lim} > 0$.*
- *whose rates converge to $1 - \delta_{lim} - \frac{1}{p^m - 1} > 0$.*
- *that can be encoded in quasi-linear time in their length.*

If, in addition,

$$p^m \geqslant 5 \text{ and } \delta_{lim} > \frac{1}{p^m - 1},$$

then there exists a family of geometric codes equipped with a module structure of a K-group algebra satisfying the previous points, and that can decode an error-rate of

$$\frac{1}{2}\left(\delta_{lim} - \frac{1}{p^m - 1}\right)$$

in quasi-quadratic time in their length.

Remark 27. These codes can be excellent if q is large enough. To verify this, we perform a calculation similar to that of Lachaud [Lac86, Section 4.7]. Recall that a family of codes over the field K is excellent if δ_{lim} and ρ_{lim}, the liminf of the relative distances and rates of the family, satisfy

$$\rho_{lim} > 1 - H_q(\delta_{lim}).$$

Using our formulas, we obtain:

$$\begin{aligned}\exists x \in [0,1], 1 - \frac{1}{p^m - 1} - x > 1 - H_q(x) &\Leftrightarrow \frac{1}{p^m - 1} < \log_q\left(\frac{2q-1}{q}\right) \\ &\Leftrightarrow q \geqslant 19^4.\end{aligned}$$

If we select for the calculation not δ_{lim}, but the relative distance that can actually be decoded with the basic algorithm $\delta_{lim} - \frac{1}{p^m - 1}$, we get excellent codes if

$$\begin{aligned}\exists x \in [0,1], 1 - \frac{2}{p^m - 1} - x > 1 - H_q(x) &\Leftrightarrow \frac{2}{p^m - 1} < \log_q\left(\frac{2q-1}{q}\right) \\ &\Leftrightarrow q \geqslant 47^4.\end{aligned}$$

4.5.4 An example of structured geometric code

In this subsection, we compute an example of a structured geometric code. Let κ be a field with 4 elements and K an extension of κ of degree 2, thus having 16 elements. Let $a \in K$ be an element such that

$$a^4 + a + 1 = 0.$$

Let

$$X : y^2 + y = x^5 + x^4 + x^3$$

be a hyperelliptic curve (and therefore a smooth projective curve) over K of genus $g_X = 2$. Note that X is defined over κ. Let L_κ and L_K be the L-polynomials of X_κ and X respectively. We have

$$L_\kappa = 16z^4 + 16z^3 + 12z^2 + 4z + 1 \text{ and } L_K = 256z^4 + 128z^3 + 48z^2 + 8z + 1.$$

We deduce that

- X has 9 κ-rational points and 25 K-rational points.
- $|\mathcal{J}_X(K)| = 441 = 49 \cdot 9$ and $|\mathcal{J}_X(\kappa)| = 49$.

Our first objective is to determine an abelian, unramified cover of X over K, with a Galois group isomorphic to $\mathcal{J}_X(K)/\mathcal{J}_X(\kappa)$, completely split over the κ-rational points of X.

Let P_∞ be the unique point at infinity of X. It is a κ-rational point of X. Let $P_1, \ldots, P_8$ be the other κ-rational points of X whose affine coordinates are:

$$\begin{array}{rcc|rcc} P_1 & = & (0,0) & P_2 & = & (0,1) \\ P_3 & = & (a^2+a,0) & P_4 & = & (a^2+a,1) \\ P_5 & = & (a^2+a+1,0) & P_6 & = & (a^2+a+1,1) \\ P_7 & = & (1,a^2+a) & P_8 & = & (1,a^2+a+1). \end{array}$$

Finally, let P_9 and P_{10} be K-rational points of X whose affine coordinates are:

$$P_9 = (a^3, a^3) \text{ and } P_{10} = (a^3+1, a+1).$$

Let c_1 and c_2 be the classes of divisors $3P_\infty + P_{10} - 4P_9$ and $P_\infty - P_9$ in $\mathcal{J}_X(K)$. We can show that c_1 and c_2 generate $\mathcal{J}_X(K)$, or more precisely

$$\mathcal{J}_X(K) = (\mathbb{Z}/21\mathbb{Z})c_1 \times (\mathbb{Z}/21\mathbb{Z})c_2.$$

Thus

$$\mathcal{J}_X(K)/\mathcal{J}_X(\kappa) \simeq (\mathbb{Z}/3\mathbb{Z})^2.$$

In particular, this group has exponent 3. Note that K has a primitive cubic root of unity

$$\zeta_3 = a^2 + a.$$

According to Kummer's theory, any abelian extension of $K(X)$ of degree 9 and exponent 3 is isomorphic to an extension of the form $K(X)[z_1, z_2]/\langle z_1^3 - R_1, z_2^3 - R_2\rangle$, where $R_1, R_2 \in K(X)^*$ are not cubes. According to [Sti08, Proposition 3.7.3], the extension associated with R_1 and R_2 is unramified if and only if there exist two divisors Γ_1 and Γ_2 such that

$$(R_1) = 3\Gamma_1 \text{ and } (R_2) = 3\Gamma_2. \tag{4.5.15}$$

Finally, the extension is purely geometric (i.e., the field of constants of the extension is K) if and only if the classes of Γ_1 and Γ_2 in $\mathcal{J}_X(K)$ are of order 3.

Conversely, let

$$\Gamma_1 = P_{11} + P_{12} - 2P_\infty \text{ and } \Gamma_2 = P_9 + P_{13} - 2P_\infty$$

where the affine coordinates of P_{11}, P_{12} and P_{13} are

$$P_{11} = (a^3 + a, a^3 + a + 1)\ ;\ P_{12} = (a^3 + a^2, a^3 + a^2)\ ;\ P_{13} = (a^3 + a^2 + a + 1, a^3 + a^2 + a).$$

One has

$$\Gamma_1 \sim 7 * c_1 \text{ and } \Gamma_2 \sim 7 * c_2$$

so the classes of Γ_1 and Γ_2 are of order 3 and generate the 3-torsion of $\mathcal{J}_X(K)$. Let $R_1, R_2 \in K(X)^*$ be functions satisfying condition (4.5.15), and such that

$$R_1(P_1) = R_2(P_1) = 1.$$

Then $K(X)[z_1, z_2]/\langle z_1^3 - R_1, z_2^3 - R_2\rangle$ is an abelian, unramified, purely geometric extension of $K(X)$, with Galois group of order 9 and exponent 3. We denote

$$K(Y) := K(X)[z_1, z_2]/\langle z_1^3 - R_1, z_2^3 - R_2\rangle$$

and we denote Y a smooth projective curve over K whose function field is $K(Y)$. Then there exists a non-ramified abelian covering

$$\tau : Y \longrightarrow X$$

with Galois group G isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$.

It remains to show that τ is totally split over the κ-rational points of X. To do this, according to Theorem 14 and Proposition 15, it is enough to show that τ is totally split over P_1. Let $r_1, r_2 \in K(Y)$ such that

$$r_1^3 = R_1 \text{ and } r_2^3 = R_2.$$

Let Q be a K-rational point of Y in the fiber of τ above P_1. We know that, as a K-algebra, the residual field K_Q is generated by $r_1(Q)$ and $r_2(Q)$. Now, by construction,

$$r_1(Q)^3 = R_1(Q) = R_1(P_1) = 1 \text{ and similarly } r_2(Q)^3 = 1.$$

Since K contains the cubic roots of unity, we deduce that $K_Q \simeq K$, and therefore P_1 is totally split in Y.

Our second objective is to compute a G-encoding matrix of a geometric code over Y. Let

$$D = 3P_9 \text{ and } P = P_\infty + \sum_{i=1}^{8} P_i$$

and let

$$E = \tau^*(D) \text{ and } Q = \tau^*(P).$$

Note that the points of P are κ-rational, so they are totally split in Y. Let

$$k = \deg D - g_X + 1 = 2.$$

Recall that r_1 and r_2 are functions of $K(Y)^*$ such that

$$r_1^3 = R_1 \text{ and } r_2^3 = R_2.$$

In particular, one has

$$(r_1) = \tau^*(\Gamma_1) \text{ and } (r_2) = \tau^*(\Gamma_2).$$

We fix a generating family of G. Let σ_1 and σ_2 be elements of G such that

$$\begin{array}{ll} r_1 \cdot \sigma_1 = \zeta_3 r_1 & r_1 \cdot \sigma_2 = r_1 \\ r_2 \cdot \sigma_1 = r_2 & r_2 \cdot \sigma_2 = \zeta_3 r_2 \end{array}$$

then σ_1 and σ_2 generate G. We also fix a generating family of

$$\hat{G} = \mathrm{Hom}(G, K^*).$$

Let χ_1 and χ_2 be two characters of $\hat{G}$ such that

$$\begin{array}{ll} \chi_1(\sigma_1) = \zeta_3 & \chi_1(\sigma_2) = 1 \\ \chi_2(\sigma_1) = 1 & \chi_2(\sigma_2) = \zeta_3. \end{array}$$

According to the Riemann-Hurwitz formula, the genus of Y is

$$g_Y = 9(g_X - 1) + 1 = 10.$$

We have

$$\deg E = 9 \deg D = 27 > 18 = 2g_Y - 2,$$

so according to Theorem 51, the vector space $\mathcal{L}(E)$ is a free $K[G]$-module of rank $k = 2$. Recall that the order of G is coprime to 16, the number of elements of K. Furthermore, since K contains the cubic roots of unity, $\mathcal{L}(E)$ decomposes as follows:

$$\mathcal{L}(E) = \bigoplus_{0 \leqslant i,j \leqslant 2} \mathcal{L}(E)_{\chi_1^i \chi_2^j}$$

where for all $0 \leqslant i, j \leqslant 2$, the K-vector space $\mathcal{L}(E)_{\chi_1^i \chi_2^j}$ is the simple sub-$K[G]$-module of $\mathcal{L}(E)$ associated with the character $\chi_1^i \chi_2^j$, i.e. the set of functions $f \in \mathcal{L}(E)$ such that

$$\forall \alpha, \beta \in [0..2], f \cdot (\sigma_1^\alpha \sigma_2^\beta) = \zeta_3^{(\alpha i + \beta j)} f.$$

In this case, these are K-vector spaces of dimension $k = 2$.

Let $i, j \in [0..2]$, and let $f \in \mathcal{L}(E)_{\chi_1^i \chi_2^j}$. For all $\alpha, \beta \in [0..2]$, we have

$$\frac{f}{r_1^i r_2^j} \cdot (\sigma_1^\alpha \sigma_2^\beta) = \frac{\zeta_3^{(\alpha i + \beta j)} f}{\zeta_3^{(\alpha i + \beta j)} r_1^i r_2^j} = \frac{f}{r_1^i r_2^j}.$$

In other words, $f/(r_1^i r_2^j) \in K(X)$ and more precisely

$$f/(r_1^i r_2^j) \in \mathcal{L}(D + i\Gamma_1 + j\Gamma_2).$$

For all $i, j \in [0..2]$, we fix $(f_{(1,i,j)}, f_{(2,i,j)})$, a K-basis of $\mathcal{L}(D + i\Gamma_1 + j\Gamma_2)$. Let

$$f_1 = \sum_{1 \leqslant i,j \leqslant 3} f_{(1,i,j)} r_1^i r_2^j \text{ and } f_2 = \sum_{0 \leqslant i,j \leqslant 2} f_{(2,i,j)} r_1^i r_2^j,$$

then (f_1, f_2) is a $K[G]$-basis of $\mathcal{L}(E)$.

In order to compute a G-generator matrix of $\mathrm{Gop}^G(Q, E)$, we must be able to evaluate f_1 and f_2 on the fiber above P. We explain how to evaluate f_1 on the fiber above P_1. Recall that

$$R_1(P_1) = R_2(P_1) = 1,$$

so the values of r_1 and r_2 on the fiber above P_1 are cubic roots of unity. Let $Q_{1,1}$ be the point of Y above P_1 such that

$$r_1(Q_{1,1}) = r_2(Q_{1,1}) = \zeta_3.$$

For all $\sigma \in G$, we define

$$Q_{1,\sigma} = \sigma(Q_{1,1}).$$

So for all $\alpha, \beta \in [0..2]$,

$$\begin{aligned} f_1(Q_{i,\sigma_1^\alpha \sigma_2^\beta}) &= \sum_{0 \leqslant i,j \leqslant 2} \zeta_3^{(\alpha i + \beta j)} f_{(1,i,j)}(P_1) r_1(Q_{1,1})^i r_2(Q1,1)^j \\ &= \sum_{0 \leqslant i,j \leqslant 2} \zeta_3^{((\alpha+1) i + (\beta+1) j)} f_{(1,i,j)}(P_1) \end{aligned}$$

Note that these calculations only require computing a primitive cubic root of unity ζ_3, the functions $(f_{(1,i,j)})_{i,j \in [0..2]}$, and cubic roots of $R_1(P_1)$ and $R_2(P_1)$.

Finally, we compute the matrix $\mathcal{E} \in \mathcal{M}_{P,2}(K[G])$, whose (P_i, j)-component is

$$\mathcal{E}_{P_i,j} = \sum_{0 \leqslant \alpha,\beta \leqslant 2} f_j(Q_{j,\sigma_1^{-\alpha}\sigma_2^{-\beta}})\sigma_1^\alpha \sigma_2^\beta.$$

For the coordinate component $(P_1, 1)$, we find

$$\begin{array}{rccccc} \mathcal{E}_{P_1,1} = & (a^3+a^2+a+1) & + & a^2\sigma_1 & + & (a^3+1)\sigma_1^2 \\ + & (a+1)\sigma_2 & + & (a^3+a+1)\sigma_1\sigma_2 & & \\ + & (a^3+a)\sigma_2^2 & + & (a^2+1)\sigma_1\sigma_2^2 & + & (a^3+1)\sigma_1^2\sigma_2^2. \end{array}$$

Chapter 5

Pairing-friendly elliptic curves

Elliptic curves are now an essential tool in public-key cryptography. In particular, cryptosystems whose security relies on the difficulty of computing discrete logarithms are used in many situations. Since the early 2000s, new protocols using elliptic curve pairings have been developed. These protocols require specific curves, known as *pairing-friendly* curves, to function satisfactorily. The generation of coupled curves is therefore an important matter when discussing the efficiency and security of these protocols.

In this chapter, after a brief introduction to pairing-based cryptography, we present the classic methods for generating pairing-friendly curves. Next, we present a new method for producing families of curves, as well as the families produced by this method. Finally, we study one of the algorithmic problems involved in using the method.

5.1 Pairing-based cryptography

This section provides a brief overview of pairing-based cryptography.

5.1.1 Recalls on curve-based cryptography

Let's start with some recalls about elliptic curves. Let K be a finite field with $q = p^m$ elements, where $p \geqslant 5$. Let $\bar{K}$ be an algebraic closure of K. An elliptic curve E can be defined on K by a polynomial in short Weierstrass form:

$$E/K : y^2z = x^3 + Axz^2 + Bz^3,$$

where $A, B \in K$ satisfy $4A^3 + 27B^2 \neq 0$. Let P_∞ be the point at infinity of the curve E, whose projective coordinates are $[0 : 1 : 0]$. In the case of elliptic curves, the Jacobi map $P \mapsto P - P_\infty$ is an isomorphism between E and $\mathcal{J}_E$, which induces an algebraic group structure on E. We denote by $E(K)$ the group of K-rational points of the curve.

For any integer r, we denote by $E[r]$ the r-torsion of the curve E. We then denote by $E[r](K)$ the group of rational r-torsion points of E and by $E[r](\bar{K})$ the group of r-torsion points of E defined over $\bar{K}$.

The L-polynomial of the elliptic curve E is of the form

$$L_{E/K} = qX^2 - tX + 1$$

where t is an integer called the trace of E. Since the curve E is isomorphic to its Jacobian, we know that

$$|E(K)| = L_{E/K}(1) = q + 1 - t.$$

The Hasse–Weil bound guarantees that $|t| \leqslant 2\sqrt{q}$. The curve E is ordinary if $\text{pgcd}(t, p) = 1$, otherwise it is supersingular.

If E is an ordinary elliptic curve, then $\text{End}(E)$ is a ring isomorphic to an order $\mathcal{O}$ in an imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$ (where D is a positive integer not divisible by a square). The Frobenius endomorphism generates a ring isomorphic to a suborder of $\mathcal{O}$, whose discriminant is the same, up to a square factor, as that of $\mathcal{O}$ or that of the field $\mathbb{Q}(\sqrt{-D})$. The discriminant of the suborder generated by Frobenius is equal to the discriminant of its characteristic polynomial $X^2 - tX + q$:

$$\text{disc}(X^2 - tX + q) = t^2 - 4q.$$

Therefore, D is the greatest divisor without square factors of $4q - t^2$, and there exists an integer y such that:

$$-Dy^2 = t^2 - 4q.$$

Remark 28. The term discriminant can refer to several different values: the discriminant of the curve $-16(4A^3 + 27B^2)$, the discriminant of its ring of endomorphisms, the discriminant of the Frobenius map, or the discriminant of the maximal order of $\mathbb{Q}(\sqrt{-D})$. Furthermore, in the literature on the generation of pairing-friendly curves, D is often also referred to as the discriminant. In this chapter, unless otherwise stated, we will refer to the discriminant of the endomorphism ring as the discriminant, and the positive integer without square factors D as the cryptographic discriminant.

For cryptographic applications, we consider the case where $|E(K)| = rh$, where r is a prime integer, different from p the characteristic of K, and $h \ll r$, such that

$$\log(q) \approx \log(|E(K)|) \approx \log(r).$$

In this case, it is clear that the rational r-torsion of the curve E is cyclic. It is considered that computing a discrete logarithm in $E[r](K)$ requires $O(\sqrt{r})$ operations in $E(K)$. Therefore, to guarantee s bits of security (which defines the security level s) for cryptographic schemes based on the difficulty of computing the discrete logarithm, it is necessary that $\log(r) \geqslant 2s$. Thus, computing the discrete logarithm requires performing at least $\sqrt{r} \geqslant 2^s$ operations on the curve.

5.1.2 Pairings

In general, a pairing is a group morphism between a product of groups (noted additively) $\mathbb{G}_1 \times \mathbb{G}_2$ and a group (noted multiplicatively) $\mathbb{G}_T$

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$$

satisfying two conditions:

- *(Non-degeneracy)*

$$\forall P \in \mathbb{G}_1 \setminus \{0\}, \exists Q \in \mathbb{G}_2, e(P,Q) \neq 1,$$

  and

$$\forall Q \in \mathbb{G}_2 \setminus \{0\}, \exists P \in \mathbb{G}_1, e(P,Q) \neq 1.$$

- *(Bilinearity)* $\forall P_1, P_2 \in \mathbb{G}_1, \forall Q_1, Q_2 \in \mathbb{G}_2, \forall n_1, n_2 \in \mathbb{Z}$,

$$e(n_1P_1 + n_2P_2, Q_1) = e(P_1, Q_1)^{n_1} e(P_2, Q_1)^{n_2},$$

  and

$$e(P_1, n_1Q_1 + n_2Q_2) = e(P_1, Q_1)^{n_1} e(P_1, Q_2)^{n_2}.$$

The Weil pairing introduced in Section 2.2.1 is an example of a pairing. Let us return to the notation used in Subsection 5.1.1: E is an elliptic curve over K, and r is a prime number distinct from the characteristic p dividing $|E(K)|$. In this case, since E is isomorphic to its Jacobian, we define the Weil pairing as follows

$$e_r : E[r](\bar{K}) \times E[r](\bar{K}) \longrightarrow \mu_r(\bar{K})$$

by identifying every point P with the divisor $P - P_\infty$.

Let k be the order of q modulo r, we call k the **embedding degree**. Suppose that $k > 1$. Let K_r be an extension of degree k of K. Since r is coprime to the characteristic, part of the r-torsion is rational, and $k > 1$, we know that the r-torsion of E is K_r-rational, and that K_r contains all the r-th roots of unity. In this case, the Weil pairing is defined on K_r.

If $r^2 \nmid q^k - 1$, we can also define the (reduced) **Tate pairing**[Ver10]

$$\mathfrak{e}_r : E[r](K_r) \times E(K_r)/rE(K_r) \longrightarrow \mu_r(K_r)$$

in a similar manner to the Weil pairing. Let $P \in E[r](K_r)$, let f_P be the function with divisor $rP - (rP) - (r-1)P_\infty$ normalized at P_∞, i.e. given a uniformizer u_∞ at P_∞, we have $u_\infty^{r-1} f_P(P_\infty) = 1$. Let $Q \in E(K_r)/rE(K_r)$, then

$$\mathfrak{e}_r(P,Q) = f_P(Q)^{(q-1)/r}.$$

There exists a pairing derived from Tate's pairing, called **optimal Ate pairing**, whose evaluation requires fewer operations than that of the Tate pairing [Ver10].

It is clear from the above that, in order for these pairings to be computed efficiently, the embedding degree k must be of reasonable size (in practice, it is common to require $k \leqslant 54$).

In this case, we say that E is a pairing-friendly curve. However, curves with pairings are extremely rare [BK98], and cannot be found at random. Nevertheless, there are methods for constructing them, and we will detail some of these in Section 5.2.

As an example, we know that supersingular curves have small embedding degrees ($k \leqslant 6$). In other words, there is no obstacle to computing pairings on a supersingular curve. On the other hand, having such a small embedding degree compromises the security of protocols based on the discrete logarithm, as explained in Subsection 5.1.4. Thus, we will focus instead on the construction of pairing-friendly ordinary curves.

5.1.3 An example of pairing-based protocol

Pairings can be used for several cryptographic applications. Here we present a tripartite key exchange protocol proposed by Joux in [Jou00].

Let P be a generator of the rational r-torsion of E. The famous Diffie-Hellman key exchange works as follows: two parties $\mathcal{A}$ and $\mathcal{B}$ agree to use the public parameters E, r, and P. Party $\mathcal{A}$ randomly selects a secret parameter $s_{\mathcal{A}} \in \mathbb{Z}/r\mathbb{Z}$ and computes the point $s_{\mathcal{A}}P$, which is its public key. Party $\mathcal{B}$ randomly selects $s_{\mathcal{B}} \in \mathbb{Z}/r\mathbb{Z}$ and computes $s_{\mathcal{B}}P$. The parties send each other their public keys and can compute the shared key $s_{\mathcal{A}}s_{\mathcal{B}}P = s_{\mathcal{B}}s_{\mathcal{A}}P$.

But how should three protagonists $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ proceed to exchange a common key? One solution would be to use the above protocol several times to compute $s_{\mathcal{A}}s_{\mathcal{B}}s_{\mathcal{C}}P$. For example, $\mathcal{A}$ and $\mathcal{B}$ exchange their key $s_{\mathcal{A}}s_{\mathcal{B}}P$ and send it to $\mathcal{C}$, which can then compute $s_{\mathcal{A}}s_{\mathcal{B}}s_{\mathcal{C}}P$. This solution has several drawbacks, notably requiring $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ to be connected simultaneously.

Joux's solution consists in using the reduced Tate pairing $\mathfrak{e}_r$ to compute a common key:

- $\mathcal{A}$ computes $\mathfrak{e}_r(s_{\mathcal{B}}P, s_{\mathcal{C}}P)^{s_{\mathcal{A}}} = \mathfrak{e}_r(P,P)^{s_{\mathcal{A}}s_{\mathcal{B}}s_{\mathcal{C}}}$.
- $\mathcal{B}$ computes $\mathfrak{e}_r(s_{\mathcal{A}}P, s_{\mathcal{C}}P)^{s_{\mathcal{B}}} = \mathfrak{e}_r(P,P)^{s_{\mathcal{A}}s_{\mathcal{B}}s_{\mathcal{C}}}$.
- $\mathcal{C}$ computes $\mathfrak{e}_r(s_{\mathcal{A}}P, s_{\mathcal{B}}P)^{s_{\mathcal{C}}} = \mathfrak{e}_r(P,P)^{s_{\mathcal{A}}s_{\mathcal{B}}s_{\mathcal{C}}}$.

This solution has the advantage of reducing the number of rounds required to exchange keys. For example, if $\mathcal{C}$ wants to send a message common to $\mathcal{A}$ and $\mathcal{B}$, using Joux's key exchange, it only needs to retrieve their public keys, instead of having to wait for $\mathcal{A}$ and $\mathcal{B}$ to send their shared secret.

Pairings can also be used for other applications. For example, in [BLS01], Boneh, Lynn, and Shacham propose using pairings to construct short signatures. Another interesting application of pairings is identity-based encryption introduced by Boneh and Franklin in [BF03].

5.1.4 Security of pairing-friendly curves

We reuse the notation from Subsection 5.1.2.

Pairing-friendly curves are vulnerable to an attack presented in [MOV93], known as the MOV attack. The principle is to use a pairing to reduce the discrete logarithm problem in the r-torsion of the curve E over K to the discrete logarithm problem in K_r^*. The complexity of solving the discrete logarithm problem in K_r^* is subexponential in $k \log\ q$ [BGK15]. For pairing-friendly curves with a small embedding degree k relative to q (in practice, we always have $k \leqslant \log\ q$, for example), it is possible that discrete logarithms are easier to compute in K_r^* than in $E(K)$.

For practical reasons, this means that it is costly to use curves with very small embedding degrees (supersingular curves, for example) because, in order to preserve the difficulty of the discrete logarithm, the size of the parameters r and q must be increased.

5.2 Generation of pairing-friendly curves

As mentioned in paragraph 5.1.2, pairing-friendly curves require specific construction methods. In this section, we review classical methods for generating pairing-friendly curves and families of pairing-friendly curves. We will focus solely on techniques that produce ordinary curves.

5.2.1 Ordinary curves and complex multiplication

The standard approach to producing pairing-firendly curves consists in fixing the desired embedding degree k as the starting parameter, then deducing conditions on the other parameters. Let us fix $k > 1$ as an integer. We seek to produce ordinary friendly curves with embedding degree k.

Let E be an ordinary elliptic curve defined over a finite field K with q elements. Let t be the trace of E, then $\text{pgcd}(t, q) = 1$. Furthermore, the Hasse-Weil bound states that

$$|t| \leqslant 2\sqrt{q}$$

or equivalently $4q - t^2 > 0$. According to [Wat69], the converse is true: for any pair of integers (q, t) where q is a prime power and t is coprime to q such that $4q - t^2 > 0$, there exists an ordinary elliptic curve E, defined over a finite field K with q elements, with trace t.

To produce pairing-friendly curves, we add an integer r and conditions on r, q, t, and k describing that E must have a subgroup of K-rational points of order r and embedding degree k.

Proposition 55 ([FST10])**.** Let $k \geqslant 1$ be an integer. Let q, r, t be integers such that:

1. q is a prime power.
2. r is prime, and $r \nmid kq$.
3. t and q are coprime.

4. there exists an integer h such that $q + 1 - t = rh$.

5. r divides $\Phi_k(t-1)$ where Φ_k denotes the k-th cyclotomic polynomial.

6. $4q - t^2 > 0$.

Then there exists an ordinary elliptic curve E defined over a finite field K with q elements, of trace t, having a K-rational subgroup of order r, with embedding degree k.

Now, we need to be able to compute E explicitly. Assuming that q is prime, we can use Atkin and Morain's complex multiplication method (see Subsection 3.2.3) to compute the j-invariant of E. Let D be the cryptographic discriminant of the curve E (i.e., the smallest integer D such that there exists $y \in \mathbb{Z}$ such that $4q - t^2 = Dy^2$). The complex multiplication algorithm requires computing (or knowing) the Hilbert class polynomial of the field $\mathbb{Q}(\sqrt{-D})$. This is only achievable if D is relatively small. For this reason, it is common to set D as a starting parameter with k.

Corollary 55.1. Let $k \geqslant 1$ be an integer, and D a positive integer not divisible by a square. Let q, r, t be integers such that:

1. q is prime.

2. r is prime, and $r \nmid kq$.

3. t and q are coprime.

4. there exists an integer h such that $q + 1 - t = rh$.

5. r divides $\Phi_k(t-1)$ where Φ_k denotes the k-th cyclotomic polynomial.

6. there exists an integer y such that $4q - t^2 = Dy^2$.

Then there exists an ordinary elliptic curve E defined over a finite field K with q elements, of trace t, having a K-rational subgroup of order r, of embedding degree k. The cryptographic discriminant of E is D.

Condition 6 is called the **CM equation**. It is equivalent to

$$Dy^2 = 4hr - (t-2)^2 \tag{6'}$$

in the sense that it is possible to replace condition 6 with condition 6' without changing the proposition.

Finally, it has already been mentioned that for cryptographic applications, we want

$$\log\ r \approx \log\ q.$$

Generally, the closer the ratio $\log\ q / \log\ r$ is to 1, the more interesting the curve is. We define the value-ρ

$$\rho = \frac{\log\ q}{\log\ r}$$

which will be the main quality criterion for the produced pairing-friendly curves.

5.2.2 Cocks–Pinch method

We use the notation from Corollary 55.1. The Cocks-Pinch method [FST10] is a method for constructing pairing-friendly curves. The idea behind this method is to use the arithmetic relations between q, t and y modulo r, so that they can be computed once r is fixed.

Condition 5 implies that $t-1$ is a primitive k-th root of unity modulo r, and condition 6' implies that $-D$ has a square root modulo r. Thus, we obtain additional constraints on r, namely:

- $k \mid r-1$,
- $\left(\frac{-D}{r}\right) = 1$.

We can then generate a pairing-friendly curve with Algorithm 5.2.1.

Algorithme 5.2.1 : Cocks–Pinch algorithm
Entrées : $k \geqslant 1$ an integer, D a positive integer not divisible by a square
Output : q, r and t integers parameterizing a pairing-friendly curve

1 Let r be a prime integer such that $k \mid r-1$ and $\left(\frac{-D}{r}\right) = 1$
2 Let ζ_k be a k-th root of unity modulo r
3 Compute an integer $t \equiv \zeta_k + 1 \bmod r$
4 Compute an integer $y \equiv (\zeta_k - 1)/\sqrt{-D} \bmod r$
5 Compute $q = (t^2 + Dy^2)/4$
6 If q is a prime integer, return q, r and t, otherwise go back to 1. and change r, ζ_k, t or y.

We can always choose t and y in $[-r, r]$, so $q \leqslant \frac{D+1}{4} r^2$. Thus, in general, the Cocks-Pinch method generates pairing-friendly curves whose value ρ is close to 2, which makes them rather poor curves compared to the curves used in practice, produced by other methods. However, this method is very flexible and allows a great deal of control over r, for example over the Hamming weight of its binary decomposition. In addition, most of the generation methods used for families of curves are inspired by the Cocks-Pinch method, for example the Brezing-Weng method (see Section 5.2.4).

5.2.3 Families of curves

In this subsection, we address the problem of constructing families of pairing-friendly curves. Most pairing-friendly curves used in practice have been produced as elements of families of curves. It is interesting to study methods that produce families of curves because, in many cases, they produce curves with a better ρ-value than those produced by methods that construct one curve at a time, such as the Cocks-Pinch method.

In order to construct families of pairing-friendly curves, we seek polynomials Q, R, and T with rational coefficients such that there exist integers $(x_i)_{i \in \mathbb{N}}$ such that $Q(x_i)$, $R(x_i)$, and $T(x_i)$ satisfy the conditions of Corollary 55.1 for all $i \in \mathbb{N}$.

In particular, Q must take an infinite number of prime integer values. Based on current knowledge, we do not know of any necessary and sufficient condition on Q (non-trivial) for this to be the case. We will assume that the Bunyakovsky–Schinzel conjecture is true:

Conjecture 1 (Bunyakovsky–Schinzel)**.** *Let Q be a polynomial of $\mathbb{Q}[Z]$. Then Q takes prime values at an infinite number of integers if and only if:*

- *Q is non constant, irreductible and has a positive leading coefficient.*
- *Q takes an integer value at some $z \in \mathbb{Z}$.*
- $\text{pgcd}(\{Q(z) \mid z, Q(z) \in \mathbb{Z}\}) = 1$.

We say that a polynomial with rational coefficients represents primes if it satisfies the conditions of the conjecture.

Definition 39. Let $k \geqslant 1$ be an integer and D a positive integer not divisible by a square. Let Q, R and T be polynomials of $\mathbb{Q}[X]$. We say that Q, R, and T parameterize a **potential family** of pairing-friendly curves (with embedding degree k and cryptographic discriminant D) if:

1. R is a non-constant, irreducible polynomial with a positive leading coefficient.
2. There exists a polynomial $H \in \mathbb{Q}[X]$ such that $HR = Q + 1 - T$.
3. R divides $\Phi_k(T-1)$.
4. There exists a polynomial $Y \in \mathbb{Q}[X]$ such that $DY^2 = 4Q - T^2$.

We say that Q, R, and T parameterize a **family** of pairing-friendly curves if, in addition:

5. Q represents primes.
6. Q, R, T, Y, H take integer values at a common integer $x \in \mathbb{Z}$.

We define the **value-ρ** of a family of curves:

$$\rho = \frac{\deg\ Q}{\deg\ R}$$

In this way, the ρ-values of the curves in the family $\frac{\log Q(x)}{\log R(x)}$ converge to the ρ-value of the family.

Remark 29. In what follows, we will only consider families parameterized by polynomials. For the sake of brevity, we will sometimes identify the family and the polynomials parameterizing it.

5.2.4 Brezing–Weng method

The polynomials parameterizing a family must satisfy arithmetic relations similar to those described in Corollary 55.1. Thus, the Cocks–Pinch method generalizes well to the production of families of curves. Brezing and Weng formalized this generalization [BW05]. We reformulate their algorithm from a perspective closer to the Kachisa-Schaefer-Scott approach.

Let $\bar{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$. Let $\mathcal{C}_k$ be the k-th cyclotomic field in $\bar{\mathbb{Q}}$ and $\sqrt{-D}$ a square root of $-D$ in $\bar{\mathbb{Q}}$.

Lemma 56. Let $\mathcal{K}$ be a number field and θ a primitive element of $\mathcal{K}$ (i.e., $\mathcal{K} = \mathbb{Q}(\theta)$). Let ζ be an element of $\mathcal{K}$. There exists a unique polynomial $T \in \mathbb{Q}[X]$ of minimal degree, such that:

$$T(\theta) = \zeta \ .$$

We say that T is the canonical polynomial mapping θ to ζ.

Proof. Let R be the minimal polynomial of θ. We have a canonical isomorphism

$$\begin{array}{ccc} \mathbb{Q}[X]/\langle R\rangle & \longrightarrow & \mathcal{K} \\ P \bmod R & \longmapsto & P(\theta) \end{array}$$

Let $P \in \mathbb{Q}[X]$ such that $P(\theta) = \zeta$. Then T is the remainder of the Euclidean division of P by R. □

Similar to the Cocks–Pinch method, the Brezing-Weng method (Algorithm 5.2.2) consists of generating potential families with a chosen polynomial R until a family is obtained.

Algorithme 5.2.2 : Brezing–Weng method

Entrées : $k > 1$ an integer and D a positive integer not divisible by a square

Output : Q, R, T, Y, H parameterizing a family of curves with cryptographic discriminant D and embedding degree k

1 Set $\mathcal{K} \subset \bar{\mathbb{Q}}$ a number field containing $\mathcal{C}_k$ and $\mathbb{Q}(\sqrt{-D})$.
2 Set $\theta \in \mathcal{K}$ a primitive element (i.e. $\mathcal{K} = \mathbb{Q}(\theta)$).
3 Compute $R \in \mathbb{Q}[X]$ the minimal polynomial of θ.
4 Set ζ_k a primitive k-th root of unity in $\mathcal{K}$.
5 Determine $T \in \mathbb{Q}[X]$ the canonical polynomial mapping θ to $\zeta_k + 1$.
6 Determine $Y \in \mathbb{Q}[X]$, the canonical polynomial mapping θ to $\frac{\zeta_k - 1}{\sqrt{-D}}$. Compute $Q = (T^2 + DY^2)/4 \in \mathbb{Q}[X]$ and $H = (Q + 1 - T)/R \in \mathbb{Q}[X]$. If Q represents primes and if there exists an integer z_0 and a rational number $\lambda > 0$ such that $Q(z_0)$, $\lambda R(z_0)$, $T(z_0)$, $Y(z_0)$ and $H(z_0)/\lambda$ are integers, return $(Q, \lambda R, T, Y, H/\lambda)$, otherwise go back to 1 and change $\mathcal{K}$, θ or ζ_k.

Since T and Y have degree strictly smaller than R, we can show that the families produced by this method satisfy

$$\rho \leqslant 2 - \frac{2}{\deg\ R}.$$

Generally, equality is achieved. We now need to find polynomials R (or, equivalently, algebraic numbers θ) that produce families whose ρ-value is significantly smaller than 2.

A first technique consists in noting that, when $D = 1$ or $D = 3$, the field $\mathcal{C}_k(\sqrt{-D})$ is a cyclotomic extension of $\mathbb{Q}$. If $D = 1$, resp. $D = 3$, let $\ell = \text{ppcm}(k, 4)$, resp. $\ell = \text{ppcm}(k, 3)$, and let $\theta = \zeta_\ell$ be an ℓ-th primitive root of unity in $\bar{\mathbb{Q}}$. Then θ can be used in the Brezing-Weng method. The first to use cyclotomic polynomials to generate families of curves were Barreto, Lynn, and Scott [BLS03], and in parallel Brezing and Weng [BW05]. Their work was taken up and extended by Freeman, Scott, and Teske [FST10]. For most embedding degrees k, the best known families come from these contributions [FST10, Table 8.2]. Notable exceptions are the cases $18 \mid k$ and sometimes $k \equiv 4 \bmod 6$.

Kachisa, Schaefer, and Scott also worked in the cyclotomic field $\mathcal{C}_\ell$, but proceeded by exhaustive search on the parameters θ and ζ_k [KSS08], with the aim of producing families for problematic cases, in particular $18 \mid k$. Let ζ_ℓ be an ℓ-th root of unity in $\mathcal{C}_\ell$. Let B_1 and B_2 be two positive integers. We define $\mathbf{KSS}(B_1, B_2)$ as the set of primitive elements of $\mathcal{C}_\ell$ of the form

$$P(\zeta_\ell) = \sum_{i=0}^{\varphi(\ell)-1} P_i \zeta_\ell^i,$$

where $P = \sum_{i=0}^{\varphi(\ell)-1} P_i X^i$ is a polynomial with rational coefficients such that

- P has at most B_1 nonzero coefficients.
- $\forall i \in [0, \varphi(\ell) - 1], \max(\text{num}(|P_i|), \text{denom}(|P_i|)) \leqslant B_2$, where φ denotes the Euler indicator.

The families constructed by Kachisa, Schaefer, and Scott come from primitive elements of $\mathcal{C}_\ell$ in $\mathbf{KSS}(2, 3)$.

With a few exceptions, the families obtained by the two previous methods are the families with the smallest known ρ-values [FST10, Table 8.2].

5.3 The new method

In this section, we present an improvement and generalization of the method of Kachisa, Schaefer, and Scott. The idea behind this construction is to identify a family of algebraic numbers that produce potential families whose ρ-value is upper bounded. We also present new families of curves produced with this new method. A Sagemath [The22] implementation of the method is available [Gas23]. This section contains my personal contributions to the article [GG25], co-authored with Aurore Guillevic.

5.3.1 Presentation of the method

Let $k \geq 1$ be an integer, let D be a squarefree positive integer, and let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$. Let $F = \mathbb{Q}(\sqrt{-D}) \subset \overline{\mathbb{Q}}$ and let $K = F\mathcal{C}_k \subset \overline{\mathbb{Q}}$. One can see K as an F-vector

space. Let $F\zeta_k$ be the F-vector line in K spanned by ζ_k.

$$F\zeta_k = \{\alpha\zeta_k; \alpha \in F\} = \{(a + b\sqrt{-D})\zeta_k; a, b \in \mathbb{Q}\}.$$

Let $\theta \in F\zeta_k$, and assume θ is a primitive element in K (over $\mathbb{Q}$). Let R be the minimal polynomial of θ (over $\mathbb{Q}$). Set

$$\alpha = \theta/\zeta_k \in F.$$

Let e be the minimal divisor of k such that $\zeta_k^e \in F$. Assume that $\theta^e \in F$ is a primitive element in F. Note that this assumption is not very restrictive.

Since $\alpha, \sqrt{-D} \in F$, there exist P_1, P_2 and P_3, three rational polynomials of degree at most 1 such that:

$$\begin{aligned} P_1(\theta^e) &= 1/\alpha, \\ P_2(\theta^e) &= 1/(\alpha\sqrt{-D}), \\ P_3(\theta^e) &= 1/\sqrt{-D}. \end{aligned}$$

Then one has

$$P_1(\theta^e)\theta + 1 = \theta/\alpha + 1 = \zeta_k + 1$$

and

$$P_2(\theta^e)\theta - P_3(\theta^e) = \zeta_k/\sqrt{-D} - 1/\sqrt{-D} = (\zeta_k - 1)/\sqrt{-D}\ .$$

Let T be the canonical rational polynomial mapping θ to $\zeta_k + 1$, and let Y be the canonical rational polynomial mapping θ to $(\zeta_k - 1)/\sqrt{-D}$. Then T is the remainder of the Euclidean division of $P_1(X^e)X + 1$ by R. As such, one has

$$\deg T \leqslant \deg(P_1(X^e)X + 1) \leqslant e + 1\ .$$

Similarly, one has $\deg(Y) \leqslant \deg(P_2(X^e)X - P_3(X^e)) \leqslant e + 1$. Consequently

$$\max(\deg(T), \deg(Y)) \leqslant e + 1\ .$$

Let $Q = (T^2 + DY^2)/4$, then

$$\deg(Q) \leqslant 2e + 2\ .$$

Thus, since $\deg R = [K : \mathbb{Q}]$, one has

$$\rho(\theta, \zeta_k) \leqslant \frac{2e + 2}{[K : \mathbb{Q}]}\ .$$

Moreover, if $\frac{2e+2}{[K:\mathbb{Q}]} < 2$, i.e. if $e + 1 < \deg R$, one has

$$T = P_1(X^e)X + 1 \text{ and } Y = P_2(X^e)X - P_3(X^e)$$

by definition of remainder of a Euclidean division of polynomials. Now, since α and $\alpha\sqrt{-D}$ can not be rationals simultaneously, then at least one of P_1 or P_2 must have degree 1. Then at least one of T or Y must have degree $e + 1$. Thus, in this case we have an equality

$$\rho(\theta, \zeta_k) = \frac{2e + 2}{[K : \mathbb{Q}]}\ .$$

Theorem 57. *With the notation of the beginning of 5.3.1, let*

$$\mathcal{S} = \{\theta \in F\zeta_k \text{ primitive in } K \mid \theta^e \text{ is primitive in } F\}.$$

Then, if $\frac{2e+2}{[K:\mathbb{Q}]} < 2$*, one has*

$$\rho(\mathcal{S}, \zeta_k) = \frac{2e+2}{[K:\mathbb{Q}]}.$$

Remark 30. Note that the construction can be generalized very simply to the case where F is an extension of $\mathbb{Q}(\sqrt{-D})$. Then P_1,P_2,P_3 have degree at most $[F:\mathbb{Q}]-1$ and the bound on the ρ-value becomes:

$$\rho(\mathcal{S}, \zeta_k) \leqslant \frac{2e([F:\mathbb{Q}]-1)+2}{[K:\mathbb{Q}]}.$$

We studied the cases where F is not quadratic as well, and found that the method produced potential families with a larger ρ-value (but smaller than 2 in some cases).

We now give more explicit bounds on $\rho(\mathcal{S}, \zeta_k)$.

Theorem 58. *With the notation of 57, assume* $\frac{2e+2}{[K:\mathbb{Q}]} < 2$.

1. *Assume that k is a multiple of 6 and $D = 3$. Then $e = k/6$ and*

$$\rho(\mathcal{S}, \zeta_k) = \frac{k/3+2}{\varphi(k)}.$$

2. *Assume that k is a multiple of 4 and $D = 1$. Then $e = k/4$ and*

$$\rho(\mathcal{S}, \zeta_k) = \frac{k/2+2}{\varphi(k)}.$$

3. *Assume that k is an odd multiple of 3 and $D = 3$. Then $e = k/3$ and*

$$\rho(\mathcal{S}, \zeta_k) = \frac{2k/3+2}{\varphi(k)}.$$

4. *Assume that k is even and $\sqrt{-D} \notin \mathcal{C}_k$. Then $e = k/2$ and*

$$\rho(\mathcal{S}, \zeta_k) = \frac{k/2+1}{\varphi(k)}.$$

5. *Assume that k is odd and $\sqrt{-D} \notin \mathcal{C}_k$. Then $e = k$ and*

$$\rho(\mathcal{S}, \zeta_k) = \frac{k+1}{\varphi(k)}.$$

Proof. We only prove case 4 as an example. Assume that k is even and $\sqrt{-D} \notin \mathcal{C}_k$. Then $[K : \mathbb{Q}] = 2\varphi(k)$ as K is a quadratic extension of $\mathcal{C}_k$. Now we prove $e = k/2$. Since $\sqrt{-D} \notin \mathcal{C}_k$, then ζ_k^e is not primitive in F (otherwise $F \subset \mathcal{C}_k$), and F is quadratic so ζ_k^e is rational. Then $\zeta_k^e \in \{1, -1\}$, because ζ_k^e is a root of unity. Since k is even, $e = k/2$ and $\zeta_k^e = -1$. Thus, by 57,

$$\rho(\mathcal{S}, \zeta_k) = \frac{2e+2}{[K:\mathbb{Q}]} = \frac{k+2}{2\varphi(k)} = \frac{k/2+1}{\varphi(k)}.$$

□

We refer to the method of generation of families via exhaustive search over the algebraic integers of $\mathcal{S}$ as the subfield method. Note that considering only algebraic integers is not very restrictive, as one can obtain remaining potential families by applying an affine substitution (over $\mathbb{Q}$).

Remark 31. Note that when $D = 1$ or $D = 3$ and for some values of k, every element in $\mathcal{S}$ is an element in $\mathbf{KSS}(2, B)$ for B sufficiently large. More precisely, take $\ell = \text{ppcm}(k, 4))$ if $D = 1$ or $\ell = \text{ppcm}(k, 3)$ if $D = 3$. Let ζ_ℓ be a ℓ-th root of unity in $\mathcal{C}_\ell$. Then $\zeta_k := \zeta_\ell^{\ell/k}$ is a primitive k-th root of unity. Moreover, there exists $d \in \{3, 4, 6\}$ maximal such that $\zeta_d := \zeta_\ell^{\ell/d} \in F$ is a non-rational root of unity in $F = \mathbb{Q}(\sqrt{-D})$. Then for any $\theta \in \mathcal{S}$, there exists two rationals a and b such that

$$\theta = (a\zeta_d + b)\zeta_k = (a\zeta_\ell^{\ell/d} + b)\zeta_\ell^{\ell/k}.$$

If $\ell/d + \ell/k < \varphi(\ell)$ then $\theta \in \cup_{B>0} \mathbf{KSS}(2, B)$. In particular, one can check that the inequality holds when $k \in \{16, 18, 32, 36, 40\}$. Moreover, it so happens that the families introduced by Kachisa et al. come from elements in such an $\mathcal{S}$. Therefore, we can see the subfield method as a refinement of the enumeration method of Kachisa et al. in these cases. This also means that when $D \in \{1, 3\}$ one can produce any family generated with the subfield method using the KSS method, at the expense of a longer exhaustive search. However, when $D \notin \{1, 3\}$, the subfield method is a strict generalization of the work of Kachisa et al.

5.3.2 Results

The interest of the subfield method depends on its ability to satisfy the following conditions:

1. The method produces potential families with ρ-values less than or equal to the reference values in the first column of [FST10, Table 8.2].

2. the method produces actual families among the potential families.

3. the families produced by the method can be used to generate pairing-friendly curves for the desired security level.

For condition 3, it may happen that the family only allows the generation of pairing-friendly curves whose parameters q and r are too large compared to the sizes required to guarantee the desired security level. This can occur when the denominators of the polynomials Q, R, and T parameterizing the family are large.

Next, we will present new families of curves, produced using the subfield method, which generate curves adapted to the 192-bit security level. Thus, the three previous conditions are met.

Assume that $k \notin \{2, 3, 4, 6, 12\}$, then the potential families produced by the subfield method have ρ-values at least as small as the reference values in [FST10, Table 8.2]. The embedding degrees for which the ρ-values are improved are compiled in Table 5.1. A bold value indicates an improvement, while a green box indicates that it is possible to find families among the potential families produced by my Sagemath implementation of the method [Gas23].

k	$\rho, D = 1$	$\rho, D = 3$	$\rho, \sqrt{-D} \notin \mathcal{C}_k$	ρ, Previous method
16	1.250	1.125	**1.125**	1.250, [FST10, 6.11]
22	**1.200**	**1.200**	**1.200**	1.300, [FST10, 6.3]
28	1.333	1.250	**1.250**	1.333, [FST10, 6.4]
40	1.375	1.3125	**1.3125**	1.375, [FST10, 6.15]
46	1.091	1.091	**1.091**	1.136, [FST10, 6.3]

Table 5.1: Comparison of the ρ-values of the potential families produced by the subfield method with the reference values [FST10].

We give two families with embedding degrees $k = 22$ and $k = 28$ whose denominators are not too large and whose ρ-values are strictly less than the reference values:

Example 6 (GG22 family [GG25]). Let $k = 22$ and $D = 7$. Let us fix an algebraic closure of $\mathbb{Q}$ and $\sqrt{-7}$ a square root of -7. Let $\mathcal{F} = \mathbb{Q}(\sqrt{-7})$. Let $\mathcal{K} = \mathcal{F}\mathcal{C}_{22}$. Let ζ_{22} be a primitive 22th root of unity, and let $\omega = \frac{1+\sqrt{-7}}{2}$. We have $\mathcal{K} = \mathbb{Q}(\omega, \zeta_{22})$.

Let $\alpha = 1 + \omega$ and $\theta = \alpha\zeta_{22}$. We have $\zeta_{22}^{11} \in \mathcal{F}$, and $\theta^{11} \notin \mathbb{Q}$. Therefore, $\mathbb{Q}(\theta^{11}) = \mathcal{F}$, and $\theta \in \mathcal{S}$. My Sagemath implementation of the subfield method [Gas23] gives:

- $T = (X^{12} + 45X + 46)/46$
- $Y = (X^{12} - 4X^{11} - 47X - 134)/322$
- $R = (X^{20} - X^{19} - X^{18} + 3X^{17} - X^{16} - 5X^{15} + 7X^{14} + 3X^{13} - 17X^{12} + 11X^{11} + 23X^{10} + 22X^9 - 68X^8 + 24X^7 + 112X^6 - 160X^5 - 64X^4 + 384X^3 - 256X^2 - 512X + 1024)/23$
- $Q = (X^{24} - X^{23} + 2X^{22} + 67X^{13} + 94X^{12} + 134X^{11} + 2048X^2 + 5197X + 4096)/7406$

The family generated by θ has a value-ρ of $6/5$. This value-ρ is less than the reference value of $13/10$ for $k = 22$.

Example 7. Let $k = 28$, $D = 11$, $\omega = (-1 + \sqrt{-11})/2$, $\alpha = \omega$, $\theta = \alpha\zeta_{28}$. One has:

- $T = (X^{15} + 718X + 3237)/3237$
- $Y = (X^{15} + 6X^{14} + 7192X + 7545)/35607$
- $R = (X^{24} + 5X^{22} + 16X^{20} + 35X^{18} + 31X^{16} - 160X^{14} - 1079X^{12} - 1440X^{10} + 2511X^8 + 25515X^6 + 104976X^4 + 295245X^2 + 531441)/(3^{12} \cdot 13^2 \cdot 83^2)$
- $Q = (X^{30} + X^{29} + 3X^{28} + 2515X^{16} + 14384X^{15} + 7545X^{14} + 4782969X^2 + 13304911X + 14348907)/38419953$

The ρ-value of this family is $5/4$, improving on the reference value of $4/3$.

The GG22 family from example 6 is of cryptographic interest for specific situations and has been studied in [AFG24, LZZ24] following the publication of an article on this new method.

A final advantage of the new method lies in its ability to generate numerous alternative families to known families of equivalent quality. This makes it possible to avoid attacks specific to a particular family. Thus, in [AFG24], the authors consider a curve of embedding degree $k = 20$ produced by the subfield method instead of the old curve from [FST10, Construction 6.4].

The list of alternative families produced by the subfield method is given in the appendix (Subsection 6.1.1). A list of integers $x \in \mathbb{Z}$ that can be used to generate curves for the 192-bit security level for some of the new families is also given (Subsection 6.1.2).

5.4 Algorithm computing the roots of a integral polynomial modulo a prime power

Let Q, R, and T be polynomials with rational coefficients parameterizing a potential family of pairing-friendly curves. The question is to prove that Q, R and T parameterize a family of curves. To do this, we must show that Q represents the primes and that the polynomials take integer values at the same $x \in \mathbb{Z}$ (note that this implies that there are infinitely many such integers x).

To verify these two conditions, it is enough to be able to:

- compute at which integers a polynomial with rational coefficients takes integer values.
- compute the GCD of the integer values of a polynomial with rational coefficients.

Let's take the polynomial Q as an example. Let Δ be the denominator of Q, i.e., the smallest positive integer such that $\Delta Q \in \mathbb{Z}[X]$. Let $x \in \mathbb{Z}$, then

$$Q(x) \in \mathbb{Z} \Leftrightarrow \Delta Q(x) \equiv 0 \bmod \Delta.$$

We can therefore find the integers for which Q takes integer values by computing the roots of ΔQ modulo p^n, for all p^n appearing in the prime factorization of Δ, if it is known.

Assume that the integers at which Q takes integer values are known. Let α be the GCD of some integer values of Q. If $\alpha = 1$, then the GCD of the integer values of Q is 1. Otherwise, for every prime p dividing α, we ask whether p divides the integer values of Q. We have

$$\forall x \in \mathbb{Z} \text{ such that } Q(x) \in \mathbb{Z}, Q(x) \equiv 0 \bmod p \Leftrightarrow \Delta Q(x) \equiv 0 \bmod p\Delta.$$

It is therefore sufficient to compare the set of roots of ΔQ modulo Δ and modulo $p\Delta$.

It remains to be explained how, given $P \in \mathbb{Z}[X]$, p a prime integer, and $n > 0$ an integer, to compute the set of integers x such that

$$P(x) \equiv 0 \bmod p^n. \tag{5.4.1}$$

The standard approach to this problem is to start by solving

$$P(x) \equiv 0 \bmod p$$

and then lifting the solutions modulo p^n. Hensel's lemma [Ser78] is used to lift any *simple* root modulo p to a unique root modulo p^n. However, the literature is quite sparse for the degenerate case. In this section, we give a general algorithm for solving such polynomial equations. We start by giving an appropriate way to represent the set of solutions of 5.4.1 in 5.4.1. In 5.4.2, we introduce the μ function, which is central in the final algorithm, and explain how to compute it. Finally, in 5.4.3, we present 5.4.1 which solves 5.4.1.

For the entire section, we fix a polynomial $P \in \mathbb{Z}[X]$, a prime number p and an integer $n > 0$.

5.4.1 Representing the set of solutions

We will use the following elementary sets to describe the set of solutions of $P(x) = 0 \bmod p^n$ in $\mathbb{Z}$.

Definition 40. Let a be an integer and let $j \geq 0$ be an integer. We define

$$D(a, j) = \{x \in \mathbb{Z} \mid x \equiv a \bmod p^j\}$$

the p-congruence class of a modulo p^j. It is indeed a congruence class.

The following proposition will prove useful later.

Proposition 59. Let a_1, a_2 be integers and let j_1, j_2 be two integers larger than 0 such that $j_1 \leqslant j_2$. Define $D(a_1, j_1)$ and $D(a_2, j_2)$ as in 40. Assume that

$$D(a_1, j_1) \cap D(a_2, j_2) \neq \emptyset.$$

Then

$$D(a_2, j_2) \subset D(a_1, j_1).$$

Proof. Let $x \in D(a_1, j_1) \cap D(a_2, j_2)$ be an integer. Then

$$x \equiv a_1 \bmod p^{j_1} \text{ and } x \equiv a_2 \bmod p^{j_2}.$$

Since $j_1 \leqslant j_2$, one has

$$x \equiv a_2 \bmod p^{j_1}.$$

Thus,

$$a_2 \equiv a_1 \bmod p^{j_1} \text{ and } D(a_2, j_2) \subset D(a_1, j_1).$$

□

Now, let $S \subset \mathbb{Z}$ be a p^n-periodic set of integers.

Definition 41. A representation by p-congruence classes of S is a collection of p-congruence classes $(D(a_i, j_i))_{i \in I}$ such that

$$S = \cup_{i \in I} D(a_i, j_i).$$

It is called finite if I is finite.

Remark 32. S always admits a finite representation by p-congruence classes. Indeed, S is p^n-periodic, which means that S is a (finite) union of classes of integers modulo p^n. More clearly,

$$S = \cup_{a \in S \cap [0, p^n - 1]} D(a, n).$$

We want to define a canonical finite representation by p-congruence classes of S. A first step is to ask that the congruence classes $(D(a_i, j_i))_{i \in I}$ be disjoint, but it is not sufficient. Let a be an integer and let $j \geq 0$ be an integer. Then $D(a, j) = \cup_{i=0}^{p-1} D(a + i \cdot p^j, j + 1)$, and the union on the right is disjoint. It turns out that this is the only other obstacle.

Definition 42. Let C be a p-congruence class in S. We say that C is maximal in S if it is maximal as a p-congruence class for the inclusion.

According to 59, S is the disjoint union of its maximal p-congruence classes. The representation of S composed of its maximal p-congruence classes is called the **reduced representation** of S.

5.4.2 The key quantity

Recall that we ultimately want to compute the set

$$S = \{x \in \mathbb{Z} \mid P(x) \equiv 0 \bmod p^n\}. \tag{5.4.2}$$

Since S is p^n-periodic, we ask to compute a reduced representation of S by p-congruence classes. The content of this section will help us to achieve this goal in the following subsection.

Definition 43. Let us define

$$\mu(P) = \sup\{j \in \mathbb{Z}_{\geq 0} \mid \forall x \in \mathbb{Z}, P(x) \equiv 0 \bmod p^j\} \ . \tag{5.4.3}$$

Remark 33. The objects defined in 40 and 43 depend on p. We do not indicate p in the notation because it will not lead to any confusion in this work.

Example 8. We give two toy examples for the prime $p = 2$:

- let $P = X^2 + 3$. Observe that $P(0) = 3 \not\equiv 0 \bmod 2$. Then $\mu(P) = 0$.
- let $P = X^2 - X$. Since for any integer x, either x or $x - 1$ is even, $P(x)$ is even. Thus, one can check that $\mu(P) = 1$.

It is easily seen that $S = \mathbb{Z}$ if and only if $\mu(P) \geq n$. More generally, one can use the μ function to check if a p-congruence class is in S.

Proposition 60. Let n be a positive integer, let $P \in \mathbb{Z}[X]$, and let S and μ be as in **??**. Let a be an integer and let $j \geq 0$ be an integer. Define $D(a, j)$ as in 40. Then

$$\mu(P(a + p^j X)) \geq n \text{ if and only if } D(a, j) \subset S.$$

Proof.

$$\begin{aligned} \mu(P(a + p^j X)) \geq n &\Leftrightarrow \forall b \in \mathbb{Z}, P(a + p^j b) \equiv 0 \bmod p^n \\ &\Leftrightarrow \forall x \in D(a, j), P(x) \equiv 0 \bmod p^n \\ &\Leftrightarrow D(a, j) \subset S. \end{aligned}$$

□

Therefore, being able to evaluate μ allows us to check if a p-congruence class is in the set of solutions S. The following theorem explains how to evaluate μ.

Theorem 61. *Let $P \in \mathbb{Z}[X]$ and let p be a prime integer. Let μ be the function defined in 5.4.3. Let $a_0, a_1, \ldots, a_{\deg P}$ be integers such that*

$$P = \sum_{i=0}^{\deg P} a_i \binom{X}{i}$$

where

$$\binom{X}{i} = \frac{X(X-1)\ldots(X-i+1)}{i!}.$$

Then

$$\mu(P) = \min_{0 \leqslant i \leqslant \deg P} (\mathrm{val}_p(a_i)).$$

Proof. It is well-known that $(\binom{X}{i})_{i\in\mathbb{Z}}$ is a $\mathbb{Z}$-basis of the group of integer-valued polynomials. Since P is integer valued, such $a_0, a_1, \ldots, a_{\deg P}$ exists.

Let $m = \min_{0\leqslant i\leqslant \deg P}(\mathrm{val}_p(a_i))$. It is clear that

$$\mu(P) \geq m.$$

Let $0 \leqslant i_0 \leqslant \deg P$ be the smallest integer such that

$$\mathrm{val}_p(a_{i_0}) = m.$$

Then

$$\begin{aligned} P(i_0) &= \sum_{i=0}^{\deg P} a_i \binom{i_0}{i} \\ &= \sum_{i=0}^{i_0} a_i \binom{i_0}{i} \\ &\equiv a_{i_0}\binom{i_0}{i_0} \bmod p^{m+1} \text{ by minimality of } i_0 \\ &\equiv a_{i_0} \bmod p^{m+1} \\ &\not\equiv 0 \bmod p^{m+1}. \end{aligned}$$

Thus,

$$\mu(P) \leqslant m.$$

□

5.4.3 Computing the roots of a polynomial modulo a prime power

We design a recursive algorithm to compute a reduced representation of the set S of integer solutions of

$$P(x) \equiv 0 \bmod p^n.$$

The idea of the algorithm is actually very straightforward. One computes μ to check if $\mu(P) \geq n$. If the answer is yes, one knows that $S = \mathbb{Z}$. Otherwise, we recursively search for solutions in every congruence class modulo p using substitutions.

Before presenting Algorithm 5.4.1, let us recall the following lemma.

Lemma 62. Let $P \in \mathbb{Z}[X]$, let p be a prime integer and let a be any integer. Then

$$P(a) \equiv 0 \bmod p$$

if and only if

$$p \mid P(a + pX), \text{ i.e. } \frac{P(a+pX)}{p} \in \mathbb{Z}[X].$$

Proof. One can check that there exists a polynomial $Q \in \mathbb{Z}[X]$ such that

$$P(a+X) = P(a) + X \cdot Q(X).$$

Thus,

$$P(a+pX) = P(a) + pX \cdot Q(pX),$$

and one can easily deduce the lemma. □

Algorithm 5.4.1 is given below. One can easily see that the algorithm finishes because n is strictly decreasing in the tree of recursion, and is lower bounded by 0. Correctness comes from 60 and the observation that if

$$P(a) \not\equiv 0 \bmod p$$

then

$$\forall x \equiv a \bmod p, P(x) \not\equiv 0 \bmod p.$$

Algorithme 5.4.1 : RootsModPrimePowers(P, p, n)
Entrées : $P \in \mathbb{Z}[X]$, p a prime integer, $n > 0$ an integer

```
si μ(P) ⩾ n alors
    Return D(0, 0).
sinon
    S ← ∅
    pour 0 ⩽ a ⩽ p − 1 faire
        si P(a) ≡ 0 mod p alors
            Q ← P(a + pX)/p
            ∪_{i∈I} D(a_i, j_i) ← RootsModPrimePowers(Q, p, n − 1)
            S ← ∪_{i∈I} D(a + p · a_i, j_i + 1) ∪ S
    Return S.
```

Remark 34. We presented the algorithm with the goal of making it as clear as possible. It can be improved in many ways. Firstly, rather than testing if $P(a) \equiv 0 \bmod p$ for every $a \bmod p$, one should use the Berlekamp algorithm to compute every root of P modulo p. Secondly, one should divide $P(a+pX)$ by the largest power of p possible, in order to reduce the size of the tree of recursion. Finally, one should always seek to use Hensel's lemma, whenever possible during the recursion. The algorithm is implemented with all these improvements in [Gas23].

Chapter 6

Appendix

6.1 New pairing-friendly curves

In this section, we list some additional outputs of the new method for generating families of pairing-friendly curves from Section 5.3.1. In Subsection 6.1.1, we give the families produced by this new method, whose ρ value does not improve on previous records, but which are of cryptographic interest for the reasons given in Section 5.3.2. Subsection 6.1.2 gives integers that can be used to generate new pairing-friendly curves for the 192-bit security level with our new families.

6.1.1 Alternative families

Here are some examples of new families of pairing-friendly curves.

Example 9 (GG20a). Let $k = 20$, and $D = 1$. Let $\theta = (1 - 2\sqrt{-1})\zeta_{20}$. Then

- $T = (2X^6 + 117X + 205)/205$
- $Y = (X^6 - 5X^5 - 44X - 190)/205$
- $R = (X^8 + 4X^7 + 11X^6 + 24X^5 + 41X^4 + 120X^3 + 275X^2 + 500X + 625)/25625$
- $Q = (X^{12} - 2X^{11} + 5X^{10} + 76X^7 + 176X^6 + 380X^5 + 3125X^2 + 12938X + 15625)/33620$

is a family of pairing-friendly curves with embedding degree $k = 20$ cryptographic discriminant $D = 1$.

Example 10 (GG20b). Let $k = 20$, let $D = 1$, and let $\theta = (1 + 2\sqrt{-1})\zeta_{20}$. Then

- $T = (-2X^6 + 117X + 205)/205$
- $Y = (X^6 - 5X^5 + 44X + 190)/205$
- $R = (X^8 - 4X^7 + 11X^6 - 24X^5 + 41X^4 - 120X^3 + 275X^2 - 500X + 625)/25625$

- $Q = (X^{12} - 2X^{11} + 5X^{10} - 76X^7 - 176X^6 - 380X^5 + 3125X^2 + 12938X + 15625)/33620$

is a family of pairing-friendly curves with embedding degree $k = 20$ cryptographic discriminant $D = 1$.

Example 11 (GG28). Let $k = 28$, let $D = 1$, and let $\theta = (1 + 2\sqrt{-1})\zeta_{28}$. Then

- $T = (-2X^8 - 527X + 145)/145$
- $Y = (X^8 - 5X^7 + 336X - 1390)/145$
- $R = (X^{12} + 4X^{11} + 11X^{10} + 24X^9 + 41X^8 + 44X^7 - 29X^6 + 220X^5 + 1025X^4 + 3000X^3 + 6875X^2 + 12500X + 15625)/29$
- $Q = (X^{16} - 2X^{15} + 5X^{14} + 556X^9 - 1344X^8 + 2780X^7 + 78125X^2 - 217382X + 390625)/16820$

is a family of pairing-friendly curves with embedding degree $k = 28$ cryptographic discriminant $D = 1$.

6.1.2 New curves

We provide integers that can be used to generate pairing-friendly curves from some of our new families.

curve family	seed $x \in \mathbb{Z}$	$\log q$	$\log r$	ρ	$\log q^k$	security K_r^*
GG20a	$-(2^{49} + 2^{46} + 2^{41} + 2^{18} + 2^3 + 2^2 + 1)$	576	379	1.52	11520	196
GG20a	$2^{49} + 2^{46} + 2^{44} + 2^{40} + 2^{34} + 2^{27} + 2^{14} + 1$	576	380	1.52	11500	196
GG20b	$-2^{49} - 2^{45} - 2^{42} - 2^{36} + 2^{11} + 1$	575	379	1.52	11500	196
GG20b	$-2^{49} + 2^{46} - 2^{41} + 2^{35} + 2^{30} - 1$	575	379	1.52	11500	196
GG20b	$-2^{49} - 2^{47} + 2^{45} - 2^{27} - 2^{22} - 2^{18} - 1$	576	380	1.52	11520	196
GG22D7	$-2^{19} - 2^{17} - 2^{15} - 2^{13} - 2^7 + 1$	453	380	1.19	9966	220
GG22D7	$-2^{20} + 2^{18} + 2^{14} + 2^{12} + 2^{10} - 2^8 - 2^5 + 1$	457	382	1.20	10054	220
GG22D7	$-2^{20} + 2^{18} + 2^{13} - 2^{10} - 2^8 - 2^2 + 1$	457	383	1.19	10054	220

Table 6.1: Parameters of new curves for the 192 bits security level.

6.2 Random generators of an abelian group

The objective of this section is to prove Corollary 63.1 and Theorem 64. These theorems upper bound the probability of not generating a finite abelian group by uniformly sampling a given number of elements. These theorems are used, for example, to find a set of generators of the Jacobian of a smooth projective curve over a finite field (see Section 2.2.3).

Let G be a finite abelian group.

Definition 44. We call the integers $d_1|\dots|d_r$ such that:

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$$

the **invariant factors** of G.

We will study the number of elements that need to be randomly drawn from G in order to generate it entirely with a probability of failure less than $1/2^n$, where n is an integer. We can start by observing that the probability that k elements $g_1, \dots, g_k$ are contained in a maximal subgroup H of G is $1/[G:H]^k \leqslant 1/2^k$. Therefore, the probability that k elements do not generate G is bounded above by $\#\{H \text{ maximal subgroup of } G\}/2^k$. However, every maximal subgroup corresponds to a unique character of G of which it is the kernel. Since the number of characters of G is bounded by $|G|$, we have:

$$\mathbb{P}(\langle g_1, \dots, g_k\rangle \subsetneq G) \leqslant |G|/2^k$$

In particular, for $\mathbb{P}(\langle g_1, \dots, g_k\rangle \subsetneq G) \leqslant 1/2^n$, it suffices that $k \geqslant \lceil \log|G| \rceil + n$. This bound has good asymptotic properties, since we see that drawing an additional element divides the probability of failure by 2. However, the term $\lceil \log|G| \rceil$ makes it uninteresting when $n = o(\log|G|)$, because it does not take into account the structure of the group. For example, if G is an ℓ-cyclic group, where ℓ is a prime number, the expected number of elements of G to be drawn uniformly to generate G is $\ell/(\ell-1)$.

Random generators of ℓ-groups

We begin by considering the case of ℓ-groups. Let ℓ be a prime number. Let G be a finite abelian ℓ-group, and let r be the number of invariant factors of G. We know that at least r elements of G are needed to generate it entirely. Furthermore, elements $g_1, \dots, g_r$ of G generate G if and only if [Pom01]:

$$\forall 1 \leqslant i \leqslant r, g_i \neq 0 \bmod \ell G + \langle g_1, \dots, g_{i-1}\rangle.$$

Thus, for $1 \leqslant i \leqslant r$, let $g_1, \dots, g_{i-1}$ be elements of G satisfying the previous condition, and let g_i be uniformly sampled from G, then

$$\mathbb{P}\left(g_i \neq 0 \bmod \ell G + \langle g_1, \dots, g_{i-1}\rangle\right) = \frac{\ell^{r-i+1}-1}{\ell^{r-i+1}} = 1 - \frac{1}{\ell^{r-i+1}}$$

because $G/(\ell G + \langle g_1, \dots, g_{i-1}\rangle) \cong \mathbb{F}_\ell^{r-i+1}$.

We now consider a sequence $X_1, X_2, \dots$ of independent random variables identically distributed according to the uniform distribution on G. We define

$$T_1 = \min\{j \in \mathbb{N} \mid X_j \neq 0 \bmod \ell G\}$$

and for all $2 \leqslant i \leqslant r$,

$$T_i = \min\{j \in \mathbb{N} \mid X_j \neq 0 \bmod \ell G + \langle X_{T_1}, \dots, X_{T_{i-1}}\rangle\} - T_{i-1}$$

Therefore, for all $1 \leqslant i \leqslant r$, the random variable T_i is a stopping time, which refers to the first success in a sequence of independent Bernoulli trials with probability of success $p_i = 1 - \frac{1}{\ell^{r-i+1}}$. The variable T_i therefore follows a geometric distribution with parameter p_i:

$$T_i \sim \mathcal{G}\left(1 - \frac{1}{\ell^{r-i+1}}\right)$$

Let $S = \sum_{i=1}^{r} T_i$, then for any integer $n > 0$,

$$\mathbb{P}(\langle X_1, \ldots, X_n \rangle = G) = \mathbb{P}(S \leqslant n)$$

We thus wish to bound the probability $\mathbb{P}(S > n)$ for any integer n. In the article [Pom01], an explicit formula for the probability $\mathbb{P}(S \leqslant n)$ is given. However, the bound in Theorem 63 allows us to simplify the calculations:

Theorem 63. *Let ℓ be a prime integer. Let $(T_i)_{i \in \mathbb{N}}$ be a sequence of mutually independent random variables such that for all $i \in \mathbb{N}$,*

$$T_i \sim \mathcal{G}(1 - \frac{1}{\ell^i})$$

For all $r \geqslant 1$, we define the sum $S_r = \sum_{i=1}^{r} T_i$. Then for all integers n,

$$\mathbb{P}(S_r > n) \leqslant \left(\sum_{i=0}^{r-1} \frac{1}{\ell^i}\right) \frac{1}{\ell^{n-r+1}}$$

Proof. We proceed by recurrence on r. For $r = 1$, then $S_1 = T_1$ follows a geometric distribution with parameter $1 - 1/\ell$, so for all $n \geqslant 1$,

$$\mathbb{P}(S_1 > n) = \left(1 - (1 - \frac{1}{\ell})\right)^n = \frac{1}{\ell^n}$$

If $n \leq 0$, then $\mathbb{P}(S_1 > n) = 1 \leq \frac{1}{\ell^n}$. Therefore, the theorem is true for $r = 1$.

Let $r \geqslant 2$. We will assume that the theorem is true at rank $r-1$. Then, for all $n \in \mathbb{Z}$,

$$\begin{aligned}
\mathbb{P}(S_r > n) &= \sum_{i=1}^{\infty} \mathbb{P}(T_r = i)\mathbb{P}(S_{r-1} > n-i) \\
&\leqslant \sum_{i=1}^{\infty} \frac{1}{\ell^{r(i-1)}} \left(1 - \frac{1}{\ell^r}\right) \left(\sum_{j=0}^{r-2} \frac{1}{\ell^j}\right) \frac{1}{\ell^{n-i-r+2}} \\
&\leqslant \left(\sum_{j=0}^{r-2} \frac{1}{\ell^j}\right) \left(1 - \frac{1}{\ell^r}\right) \sum_{i=1}^{\infty} \frac{1}{\ell^{n+i(r-1)-2(r-1)}} \\
&\leqslant \left(\sum_{j=0}^{r-2} \frac{1}{\ell^j}\right) \left(1 - \frac{1}{\ell^r}\right) \frac{1}{\ell^{n-2(r-1)}} \frac{1}{\ell^{r-1}-1} \\
&\leqslant \frac{\sum_{j=0}^{r-2} \ell^j}{\ell^{r-2}} \frac{\ell^r - 1}{\ell^r} \frac{1}{\ell^{r-1}-1} \frac{1}{\ell^{n-2(r-1)}} \\
&\leqslant \frac{\left(\sum_{j=0}^{r-2} \ell^j\right)}{\ell^{r-2}} \frac{(\ell-1)\left(\sum_{j=0}^{r-1} \ell^j\right)}{\ell^r} \frac{1}{(\ell-1)\left(\sum_{j=0}^{r-2} \ell^j\right)} \frac{1}{\ell^{n-2(r-1)}} \\
&\leqslant \frac{\left(\sum_{j=0}^{r-2} \ell^j\right)(\ell-1)\left(\sum_{j=0}^{r-1} \ell^j\right)}{\ell^{2(r-1)}(\ell-1)\left(\sum_{j=0}^{r-2} \ell^j\right)} \frac{1}{\ell^{n-2(r-1)}} \\
&\leqslant \left(\sum_{j=0}^{r-1} \frac{1}{\ell^j}\right) \frac{1}{\ell^{n-(r-1)}}
\end{aligned}$$

By induction on r, the theorem is proved. □

Corollary 63.1. *Let G be a finite abelian ℓ-group. Let r be its number of invariant factors. Let $n \geqslant r$ be an integer, and let $g_1, \ldots, g_n$ be uniformly drawn elements of G. Then*

$$\mathbb{P}(\langle g_1, \ldots, g_n \rangle \subsetneq G) \leqslant \left(\sum_{i=0}^{r-1} \frac{1}{\ell^i}\right) \frac{1}{\ell^{n-r+1}} \leqslant \frac{1}{\ell^{n-r}(\ell-1)}$$

General case

Let G be a finite abelian group, let r be its number of invariant factors, let ℓ be a prime number, and let h_ℓ be the greatest divisor of $|G|$ that is coprime to ℓ, then $h_\ell G$ is an ℓ-group whose number of invariant factors is less than r. Furthermore, the uniform distribution on G and the multiplication by h_ℓ induce the uniform distribution on $h_\ell G$.

Let $n \geqslant r$, and let $g_1, \ldots, g_n$ be uniformly drawn elements of G. They generate G if and only if for all prime ℓ,

$$\langle h_\ell g_1, \ldots, h_\ell g_n \rangle = h_\ell G.$$

Furthermore, the events $(\{\langle h_\ell g_1, \dots, h_\ell g_n\rangle = h_\ell G\})_\ell$ are independent. Therefore

$$\begin{aligned}\mathbb{P}(\langle g_1, \dots, g_n\rangle \subsetneq G) &= 1 - \mathbb{P}(\langle g_1, \dots, g_n\rangle = G)\\ &= 1 - \prod_{\ell \text{ premier}} \mathbb{P}(\langle h_\ell g_1, \dots, h_\ell g_n\rangle = h_\ell G)\\ &= 1 - \prod_{\ell \text{ premier}} (1 - \mathbb{P}(\langle h_\ell g_1, \dots, h_\ell g_n\rangle \subsetneq h_\ell G))\end{aligned}$$

Using the bounds obtained previously, we obtain the following theorem:

Theorem 64. *Let G be a finite abelian group. Let r be its number of invariant factors. Let $n \geqslant r+2$ be an integer, and let $g_1, \dots, g_n$ be uniformly drawn elements of G. Then*

$$\mathbb{P}(\langle g_1, \dots, g_n\rangle \subsetneq G) \leqslant \frac{2}{3}\left(\frac{1}{2}\right)^{n-r-2}$$

Proof. We use the fact that the groups $h_\ell G$ are ℓ-groups with fewer than r invariant factors, and Corollary 63.1.

$$\begin{aligned}\mathbb{P}(\langle g_1, \dots, g_n\rangle \subsetneq G) &= 1 - \prod_{\ell \text{ prime}} (1 - \mathbb{P}(\langle h_\ell g_1, \dots, h_\ell g_n\rangle \subsetneq h_\ell G))\\ &\leqslant 1 - \prod_{\ell \text{ prime}} \left(1 - \frac{1}{\ell^{n-r}(\ell-1)}\right)\end{aligned}$$

Now, since $n - r \geqslant 2$, for all prime ℓ, one has $\frac{1}{\ell^{n-r}(\ell-1)} \in [0, 1/2]$ and

$$\ln(1 - \frac{1}{\ell^{n-r}(\ell-1)}) \geqslant -2\frac{1}{\ell^{n-r}(\ell-1)}$$

using the inequality

$$\forall x \in [-1/2, 0],\ 2x \leqslant \ln(1+x).$$

Thus

$$\begin{aligned}\mathbb{P}(\langle g_1, \dots, g_n\rangle \subsetneq G) &\leqslant 1 - e^{-2\sum_{\ell \text{ prime}} \frac{1}{\ell^{n-r}(\ell-1)}}\\ &\leqslant 2\sum_{\ell \text{ prime}} \frac{1}{\ell^{n-r}(\ell-1)}\end{aligned}$$

using the convexity inequality

$$\forall x \in \mathbb{R}, 1 - e^x \leqslant -x.$$

This sum converges because $n - r \geqslant 2$.

Finally,

$$\frac{1}{\ell^{n-r}(\ell-1)} = \frac{1}{\ell^{n-r-2}} \frac{1}{\ell^2(\ell-1)} \leqslant \frac{1}{2^{n-r-2}} \frac{1}{\ell^2(\ell-1)}.$$

Thus,

$$\mathbb{P}(\langle g_1, \ldots, g_n \rangle \subsetneq G) \leqslant \frac{1}{2^{n-r-2}} \left(2 \sum_{\ell \text{ premier}} \frac{1}{\ell^2(\ell-1)} \right).$$

We conclude by computing using a computer that

$$2 \sum_{\ell \text{ prime}} \frac{1}{\ell^2(\ell-1)} \leqslant \frac{2}{3}.$$

□

6.3 Simplicity and freeness of K[G]-modules

The purpose of this section is to prove Theorem 79. This result is used in Section 4.4 to justify the existence of a dual code.

Modules, simplicity and Jordan-Hölder theorem

We begin by reviewing some concepts from module theory before considering the specific case of $K[G]$-modules (i.e., linear representations of groups). This subsection is based on a lecture by Pierre Baumann [Bau08].

Let A be a (unitary) ring.

Definition 45. Let M be an abelian group (with additive notation). We say that M is a left A-module if there exists a left action (with multiplicative notation) of A on M such that:

- $\forall m \in M, 1_A m = m$.
- $\forall a, b \in A, \forall m, n \in M, (a+b)(m+n) = am + bm + an + bn$.
- $\forall a, b \in A, \forall m \in M, (ab)m = a(bm)$.

A submodule N of M is an abelian subgroup of M stable under the action of A. The quotient group M/N is also an A-module:

$$\forall a \in A, \forall m \in M, a(m+N) = am + N.$$

Example 12. The ring A naturally has a structure of left A-module, acting on itself by left multiplication. We call this module the regular left A-module, and we denote it by ${}_AA$.

Let I be a set and let $A^{(I)}$ be the set of families of elements of A indexed by I with finite support. Let $i \in I$, we denote by e_i the element $A^{(I)}$ whose component with index i is 1_A and whose other components are zero. Then $(e_i)_{i\in I}$ forms a basis for $A^{(I)}$. We call (left) modules that have a basis free (left) modules.

Finally, $\{0\}$ is an A-module called the zero module. It is sometimes denoted simply by 0.

Definition 46. Let M and N be two left A-modules. Let $\varphi : M \longrightarrow N$ be a group morphism. We say that φ is a left A-module morphism if

$$\forall a \in A, \forall m \in M, \varphi(am) = a\varphi(m).$$

We denote by $\mathrm{Hom}_A(M, N)$ the set of morphisms of A-modules from M to N. It is an abelian subgroup of $\mathrm{Hom}_{\mathbb{Z}}(M, N)$. The image of φ is a submodule of N, and the kernel of φ is a submodule of M.

The above definitions naturally generalize "to the right". Some properties of modules do not depend on which side A acts on. We will avoid specifying "left" or "right" in statements when it is not necessary.

Definition 47. Let M be a left A-module. Then $\mathrm{Hom}_A(M, {}_AA)$, the group of left A-module morphisms from M to ${}_AA$, is naturally equipped with a right A-module structure:

$$\forall f \in \mathrm{Hom}_A(M, {}_AA), \forall a \in A, \forall m \in M, (fa)(m) = f(m)a.$$

It is called the dual module of M, and is sometimes denoted by M^*.

Proposition 65. $({}_AA)^*$ is isomorphic to A_A, the regular right A-module.

Proof. We give the isomorphism explicitly:

$$\begin{array}{ccc} \mathrm{Hom}_A({}_AA, {}_AA) & \longrightarrow & A_A \\ f & \longmapsto & f(1) \end{array}.$$

□

Definition 48. Let M be an A-module. We say that

- M is Noetherian if every increasing sequence of submodules of M is stationary.
- M is Artinian if every decreasing sequence of submodules of M is stationary.
- M is simple if it has exactly two submodules M and 0.

We see that every simple A-module is Artinian and Noetherian.

Proposition 66. Let M be a simple left A-module. Then there exists a maximal left ideal $\mathfrak{m}$ of A such that $M \simeq A/\mathfrak{m}$.

Proof. Let $m \in M$ be nonzero. Then $\mathfrak{m}$ is the kernel of the map $a \in A \longmapsto am \in M$. This map is surjective because its image is a nonzero submodule of M. □

Proposition 67. Let M be a Noetherian (resp. Artinian) A-module. Then every non-empty set of submodules of M has a maximal (resp. minimal) element for inclusion.

Proof. Suppose there exists a non-empty set $\mathcal{E}$ of submodules of M that does not have a maximal element for inclusion. Then it is possible to find a sequence $N_0 \subsetneq N_1 \subsetneq \dots$ of submodules of M in $\mathcal{E}$. Therefore, M is not Noetherian. A similar argument proves the Artinian case. □

Definition 49. Let M be an A-module. An ascending filtration of M is an ascending sequence $(M_n)_{n\in\mathbb{Z}}$ of submodules of M such that:

- $\cup_{n\in\mathbb{Z}} M_n = M$.
- $\cap_{n\in\mathbb{Z}} M_n = 0$.

The A-modules M_{n+1}/M_n are called the quotients or factors of the filtration.

Let $(M_n)_{n\in\mathbb{Z}}$ and $(N_n)_{n\in Z}$ be two ascending filtrations of M. We say that $(N_n)_{n\in Z}$ is a refinement of $(M_n)_{n\in Z}$ if there exists an ascending injection $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}$ such that

$$\forall n \in \mathbb{Z}, M_n = N_{\varphi(n)}.$$

A composition series of M is a filtration in which all quotients are simple. Two composition series are said to be equivalent if they have the same sequence of quotients up to permutation and isomorphism.

Lemma 68 (Schur)**.** Let $\varphi : M \longrightarrow N$ be a morphism of simple A-modules. Then φ is either an isomorphism or the zero morphism.

A proof is available in [Lan02, Chapter 7, Proposition 1.1].

Theorem 69 (Jordan-Hölder)**.** *Let M be an A-module. If M has composition series, they are all equivalent.*

A proof is available in [CR62, Theorem 13.7].

Definition 50. The quotients of a composition series of M are called the Jordan-Hölder quotients of M.

Proposition 70. Let M be an Artinian and Noetherian A-module. Then M has a composition series.

Proof. Let $\mathcal{E}$ be the set of submodules of M that admit a composition series. The set $\mathcal{E}$ is nonempty because $0 \in \mathcal{E}$. Since M is Noetherian, $\mathcal{E}$ contains a maximal element N for inclusion.

Suppose that $N \neq M$. Then the set $\mathcal{F}$ of submodules of M strictly containing N is nonempty because $M \in \mathcal{F}$. Since M is Artinian, $\mathcal{F}$ contains a minimal element L for inclusion. Therefore, N is a maximal submodule of L, and thus L/N is simple. Therefore, L admits a composition series, which is absurd.

Therefore, $N = M$, and M admits a composition series. □

Definition 51. Let M be an A-module. We say that M is of finite-type if there exists a finite set I and a surjective morphism of A-modules $\pi : A^{(I)} \longrightarrow M$, or equivalently if it is generated by a finite number of elements.

Lemma 71. Every Noetherian A-module is of finite-type.

Proof. Let M be a Noetherian A-module. Let $\mathcal{E}$ be the set of submodules of finite-type of M. Then, since M is Noetherian, $\mathcal{E}$ has a maximal element N for inclusion. Furthermore, for all $x \in M$, $N + Ax$ is of finite-type (since N is). By the maximality of N, we have $N = N + Ax$, so $x \in L$. Therefore, $N = M$. □

Definition 52. Let M be an Artinian and Noetherian A-module. Let S be a simple A-module. We denote by $\ell(M)$ the number of quotients in a composition series of M, otherwise known as the length of M (finite, since M is finite). Let $(M : S)$ be the number of Jordan-Hölder quotients of M isomorphic to S. We say that $(M : S)$ is the Jordan-Hölder multiplicity of M with respect to S.

Proposition 72. Let L, M, N be three A-modules such that

$$0 \to L \to M \to N \to 0.$$

Then M is Artinian and Noetherian if and only if L and N are Artinian and Noetherian.

Proof. We can assume that $L \subset M$ and $N = M/L$. Suppose that L and M/L are Noetherian. Let $(T_n)_{n\in\mathbb{N}}$ be an increasing sequence of submodules of M. Then $(T_n \cap L)_{n\in\mathbb{N}}$ is an increasing sequence of submodules of L and $((T_n + L)/L)_{n\in\mathbb{N}}$ is an increasing sequence of submodules of M/L. Then there exist two submodules $T_L \subset L$ and $T_{M/L} \subset M/L$, and $n_0 \in \mathbb{N}$ such that for all $n \geqslant n_0$, $(T_n \cap L) = T_L$ and $((T_n + L)/L) = T_{M/L}$. This implies that for all $n \geqslant n_0$, the module T_n is constant. Therefore, M is Noetherian. The converse does not pose any difficulties. The proof is similar for Artinian modules. □

Proposition 73. Let M be a Noetherian (resp. Artinian) A-module. Then for any integer $n \geqslant 0$, M^n is Noetherian (resp. Artinian).

Proof. Noting the existence of an exact sequence

$$0 \to M \to M^n \to M^{n-1} \to 0$$

we reason by induction using Proposition 72. □

Proposition 74. Let L, M, N be three Artinian and Noetherian A-modules such that

$$0 \to L \to M \to N \to 0.$$

Then

$$\ell(M) = \ell(L) + \ell(N)$$

and for any simple A-module S,

$$(M : S) = (L : S) + (N : S).$$

Proof. We can assume that $L \subset M$ and $N = M/L$. Let $0 = L_0 \subset L_1 \subset \cdots \subset L_{\ell(L)} = L$ be a composition series of L and $0 = N_0 \subset N_1 \subset \cdots \subset N_{\ell(N)} = N$ a composition series of N. Let $\pi_L : M \longrightarrow N$ be the quotient morphism. Then we have a filtration

$$0 = L_0 \subset L_1 \subset \cdots \subset L_{\ell(L)} = L = \pi_L^{-1}(N_0) \subset \pi_L^{-1}(N_1) \subset \cdots \subset \pi_L^{-1}(N_{\ell(N)}) = M.$$

For all $0 \leq i \leq \ell(N) - 1$,

$$\pi_L^{-1}(N_{i+1})/\pi_L^{-1}(N_i) \simeq N_{i+1}/N_i$$

is a simple module, so $L_0 \subset \cdots \subset \pi_L^{-1}(N_{\ell(N)})$ is a composition series of M. We deduce the proposition. □

Proposition 75. There exists a set containing a representative of all isomorphism classes of Artinian and Noetherian A-modules.

Proof. Let $\mathcal{M}$ be an isomorphism class of Artinian and Noetherian A-modules. The modules in the class of M are therefore finite. Then there exists a submodule N of $A^{\mathbb{N}}$ and M a module of the isomorphism class $\mathcal{M}$ such that $M = A^{\mathbb{N}}/N$.

Let $\mathcal{E}$ be the set of submodules of $A^{\mathbb{N}}$ (contained in the set of parts). It is in bijection with the set $\{A^{\mathbb{N}}/N; N \in \mathcal{E}\}$ which contains (at least) one representative of all isomorphism classes of Artinian and Noetherian A-modules. □

Definition 53. Let $\mathcal{E}$ be a set of representatives of the isomorphism classes of Artinian and Noetherian A-modules. Let $\mathbb{Z}^{(\mathcal{E})}$ be the free abelian group on $\mathcal{E}$, and let $\mathrm{Gr}(A)$ be the quotient of $\mathbb{Z}^{(\mathcal{E})}$ by the subgroup generated by elements of the form $M - L - N$ for any exact sequence

$$0 \to L \to M \to N \to 0$$

of elements L, M, N of $\mathcal{E}$. We call $\mathrm{Gr}(A)$ the Grothendieck group of isomorphism classes of Artinian and Noetherian A-modules.

Remark 35. $\mathrm{Gr}(A)$ does not depend on the choice of $\mathcal{E}$ and is uniquely characterized by A.

Definition 54. Let L, M, N be A-modules.

- We say that N is projective if there exists a free A-module M and an A-module L such that $M \simeq L \oplus N$.

- We say that L is injective if every short exact sequence

$$0 \to L \to M \to N \to 0$$

splits, i.e., $M \simeq L \oplus N$.

Definition 55. We define $\mathrm{PGr}(A)$ as the Grothendieck group of isomorphism classes of projective Artinian and Noetherian A-modules (see definition **??**). Let P be an Artinian and Noetherian projective A-module. We denote by $[P]$ the image of P in $\mathrm{PGr}(A)$.

Freeness of the orthogonal

Let K be a (commutative) field and G a finite group.

Definition 56. Let ${}_GK[G]$ denote the regular left $K[G]$-module and $K[G]_G$ denote the regular right $K[G]$-module.

Proposition 76. Regular $K[G]$-modules (right and left) are Artinian and Noetherian.

Proof. Every $K[G]$-module is a K-vector space. Furthermore, $K[G]$ is a finite-dimensional K-vector space. Let $M_0 \subset M_1 \subset \dots$ be an increasing sequence of submodules of $K[G]$. Then $\dim(M_0) \leqslant \dim(M_1) \leqslant \dots$ is an increasing sequence of integers bounded above by $\dim(K[G])$. Therefore, the sequence of dimensions is stationary, and so is $(M_i)_{i\in\mathbb{N}}$. Therefore, the regular $K[G]$-modules are Noetherian. A similar argument shows that they are Artinian. □

Corollary 76.1. Every finite-type $K[G]$-module is Artinian and Noetherian.

Proof. This follows from Propositions 73 and 72. □

Proposition 77. Let M be a $K[G]$-module and N a free submodule of M. Then there exists L a submodule of M such that $M = N \oplus L$.

Proof. This property is due to the fact that the algebra $K[G]$ is a Frobenius algebra [CR62, Theorem 62.1], i.e.

$$\mathrm{Hom}_{K[G]}(K[G]_G, K[G]_G) \simeq \mathrm{Hom}_K(K[G]_G, K).$$

Then every projective $K[G]$-module is also injective [CR62, Theorem 62.3]. In particular, N is free and therefore projective, and thus injective. Thus, the exact sequence

$$0 \to N \to M \to M/N \to 0$$

splits, so there exists a submodule L of M such that $L \simeq M/N$ and $M = N \oplus L$. □

Proposition 78. Let P_1 and P_2 be two Artinian and Noetherian projective $K[G]$-modules. Then $P_1 \simeq P_2$ if and only if $[P_1] = [P_2]$ in $\mathrm{PGr}(K[G])$.

Proof. The proposition is proven in [Ser71, Chapter 14, Corollary 3]. □

Let $n \geqslant 1$ be an integer. Recall that $\langle ., . \rangle$ denotes the $K[G]$-bilinear form on $K[G]^n$ defined in equation (4.4.1).

Theorem 79. *Let M be a free submodule of ${}_GK[G]^n$ (resp. $K[G]^n_G$). Then $M^\perp$, the orthogonal of M for the $K[G]$-bilinear form $\langle ., . \rangle$, is a free submodule of $K[G]^n_G$ (resp. ${}_GK[G]^n$).*

Proof. We prove the case where M is a left $K[G]$-module. Let k be the rank of M as a free $K[G]$-module. Therefore, $M \simeq {}_GK[G]^k$. According to Proposition 77, there exists a submodule N of ${}_GK[G]^n$ such that

$$ {}_GK[G]^n = M \oplus N. \tag{6.3.1} $$

Furthermore, we trivially have

$$ {}_GK[G]^n \simeq {}_GK[G]^k \oplus {}_GK[G]^{n-k}. \tag{6.3.2} $$

The modules ${}_GK[G]^n$, ${}_GK[G]^k$, ${}_GK[G]^{n-k}$, M, and N are projective, Artinian, and Noetherian (since they are finite). We have

$$ \begin{aligned} [N] &= [{}_GK[G]^n] - [M] && \text{according to equation (6.3.1)} \\ &= [{}_GK[G]^n] - [{}_GK[G]^k] && \text{because } M \simeq {}_GK[G]^k \\ &= [{}_GK[G]^{n-k}] && \text{according to equation (6.3.2)} \end{aligned} $$

According to Proposition 78, the module $N \simeq {}_GK[G]^{n-k}$ is a free left $K[G]$-module. Thus, $\mathrm{Hom}_{K[G]}(N, {}_GK[G])$ is a free right $K[G]$-module. Indeed, we have

$$ \begin{aligned} \mathrm{Hom}_{K[G]}(N, {}_GK[G]) &\simeq \mathrm{Hom}_{K[G]}({}_GK[G]^{n-k}, {}_GK[G]) \\ &\simeq \mathrm{Hom}_{K[G]}({}_GK[G], {}_GK[G])^{n-k} \\ &\simeq (K[G]_G)^{n-k} \end{aligned} $$

according to proposition 66.

Finally, we show that $M^\perp \simeq \mathrm{Hom}_{K[G]}(N, {}_GK[G])$. Let

$$ L = \{ f \in \mathrm{Hom}_{K[G]}({}_GK[G]^n, {}_GK[G]) \mid f_{|M} = 0 \}, $$

then $L \simeq \mathrm{Hom}_{K[G]}(N, {}_GK[G])$. It remains to be shown that $M^\perp \simeq L$. Let

$$ \begin{array}{rccc} \phi : & M^\perp & \longrightarrow & L \\ & m & \longmapsto & \langle ., m \rangle \end{array}, $$

is an injective $K[G]$-module morphism. Furthermore, $M^\perp$ and L are K-vector spaces of the same dimension. Indeed, L is a free right $K[G]$-module of rank $(n-k)$, and therefore its dimension (over K) is $|G|(n-k)$. Then, according to Proposition 41, the right $K[G]$-module $M^\perp$ is the dual of M for the form $\langle ., . \rangle_K$, and therefore its dimension is also $|G|(n-k)$. We deduce that

$$M^\perp \simeq L \simeq \mathrm{Hom}_{K[G]}(N, {}_G K[G]).$$

□

Bibliography

[AFG24] Diego F. Aranha, Georgios Fotiadis, and Aurore Guillevic. A short-list of pairing-friendly curves resistant to the special TNFS algorithm at the 192-bit security level. *IACR Communications in Cryptology*, 1(3), 2024.

[AM93] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comput.*, 61(203):29–68, 1993.

[Ari61] S. Arimoto. Encoding and decoding of p-ary group codes and the correction system. *Information Processing in Japan*, 2:320–325, 1961. (in Japanese).

[AT09] Emil Artin and John Tate. *Class field theory*. Providence, RI: AMS Chelsea Publishing, reprint of the 1990 2nd ed. edition, 2009.

[Bau08] Pierre Baumann. Introduction à la théorie des représentations. cours de M2 donné à l'Université Louis Pasteur, 2008. https://irma.math.unistra.fr/~baumann/coursM2-2008.pdf.

[BCG+17] Alin Bostan, Frédéric Chyzak, Marc Giusti, Romain Lebreton, Grégoire Lecerf, Bruno Salvy, and Éric Schost. *Algorithmes Efficaces en Calcul Formel*. Frédéric Chyzak (auto-édit.), Palaiseau, September 2017. 686 pages. Imprimé par CreateSpace. Aussi disponible en version électronique.

[BF03] Dan Boneh and Matt Franklin. Identity-based encryption from the Weil pairing. *SIAM J. of Computing*, 32(3):586–615, 2003.

[BGK15] Razvan Barbulescu, Pierrick Gaudry, and Thorsten Kleinjung. The Tower Number Field Sieve. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015*, volume 9453 of *Advances in cryptology-Asiacrypt 2015*, pages 31–58, Auckland, New Zealand, 2015. International Association of Cryptologic Research, Springer.

[BH08] Peter Beelen and Tom Høholdt. The decoding of algebraic geometry codes. In *Advances in algebraic geometry codes.*, pages 49–98. Hackensack, NJ: World Scientific, 2008.

[BK98] R. Balasubramanian and Neal Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the menezes - okamoto - vanstone algorithm. *J. Cryptology*, 11:141–145, 1998.

[BLB06] S. Ballet and D. Le Brigand. On the existence of non-special divisors of degree g and $g-1$ in algebraic function fields over $\mathbb{F}_2$. *J. Number Theory*, 116(2):293–310, 2006.

[BLS01] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the weil pairing. In Colin Boyd, editor, *Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 9-13, 2001, Proceedings*, volume 2248 of *Lecture Notes in Computer Science*, pages 514–532. Springer, 2001.

[BLS03] Paulo S. L. M. Barreto, Ben Lynn, and Michael Scott. Constructing elliptic curves with prescribed embedding degrees. In *Security in communication networks. Third international conference, SCN 2002, Amalfi, Italy, September 11–13, 2002. Revised papers*, pages 257–267. Berlin: Springer, 2003.

[Blu70] L. Bluestein. A linear filtering approach to the computation of discrete fourier transform. *IEEE Transactions on Audio and Electroacoustics*, 18(4):451–455, 1970.

[BMvT78] Elwyn R. Berlekamp, Robert J. McEliece, and Henk C. A. van Tilborg. On the inherent intractability of certain coding problems. *IEEE Trans. Inf. Theory*, 24:384–386, 1978.

[BR04] S. Ballet and R. Rolland. Multiplication algorithm in a finite field and tensor rank of the multiplication. *J. Algebra*, 272(1):173–185, 2004.

[BRS21] Peter Beelen, Johan Rosenkilde, and Grigory Solomatov. Fast encoding of AG codes over C_{ab} curves. *IEEE Trans. Inf. Theory*, 67(3):1641–1655, 2021.

[Bru13] Peter Bruin. Computing in Picard groups of projective curves over finite fields. *Math. Comput.*, 82(283):1711–1756, 2013.

[BS96] Eric Bach and Jonathan Sorenson. Explicit bounds for primes in residue classes. *Math. Comput.*, 65(216):1717–1735, 1996.

[BS05] Johannes Buchmann and Arthur Schmidt. Computing the structure of a finite Abelian group. *Math. Comput.*, 74(252):2017–2026, 2005.

[BV07] Johannes Buchmann and Ulrich Vollmer. *Binary quadratic forms. An algorithmic approach*, volume 20 of *Algorithms Comput. Math.* Berlin: Springer, 2007.

[BW05] Friederike Brezing and Annegret Weng. Elliptic curves suitable for pairing based cryptography. *Des. Codes Cryptography*, 37(1):133–141, 2005.

[BW23] Martino Borello and Wolfgang Willems. On the algebraic structure of quasi-group codes. *J. Algebra Appl.*, 22(10):16, 2023. Id/No 2350222.

[CC88] D. V. Chudnovsky and G. V. Chudnovsky. Algebraic complexities and algebraic curves over finite fields. *J. Complexity*, 4(4):285–316, 1988.

[CE23] Jean-Marc Couveignes and Tony Ezome. The equivariant complexity of multiplication in finite field extensions. *J. Algebra*, 622:694–720, 2023.

[Cha08] Jean Chaumine. Multiplication in small finite fields using elliptic curves. In *Algebraic geometry and its applications*, volume 5 of *Ser. Number Theory Appl.*, pages 343–350. World Sci. Publ., Hackensack, NJ, 2008.

[Coh93] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Grad. Texts Math.* Berlin: Springer-Verlag, 1993.

[Coh00] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Grad. Texts Math.* New York, NY: Springer, 2000.

[CR62] Charles W. Curtis and Irving Reiner. Representation theory of finite groups and associative algebras. Pure and Applied Mathematics. 11. New York-London: Interscience Publishers, a division of John Wiley & Sons. xiv, 685 pp. (1962)., 1962.

[DGTT18] Steven T. Dougherty, Joseph Gildea, Rhian Taylor, and Alexander Tylyshchak. Group rings, G-codes and constructions of self-dual and formally self-dual codes. *Des. Codes Cryptography*, 86(9):2115–2138, 2018.

[Duu93] I.M. Duursma. *Decoding codes from curves and cyclic codes*. PhD thesis, Eindhoven Univ. Techn., Sept. 1993.

[ECdJ+11] Bas Edixhoven, Jean-Marc Couveignes, Robin de Jong, Franz Merkl, and Johan Bosman. *Computational Aspects of Modular Forms and Galois Representations*. Princeton University Press, 2011. Edited by Bas Edixhoven and Jean-Marc Couveignes.

[Ehr93] Dirk Ehrhard. Achieving the designed error capacity in decoding algebraic-geometric codes. *IEEE Trans. Inf. Theory*, 39(3):743–751, 1993.

[FR93] Gui-Liang Feng and T. R. N. Rao. Decoding algebraic-geometric codes up to the designed minimum distance. *IEEE Trans. Inf. Theory*, 39(1):37–45, 1993.

[FST10] David Freeman, Michael Scott, and Edlyn Teske. A taxonomy of pairing-friendly elliptic curves. *J. Cryptology*, 23(2):224–280, 2010.

[Gas23] Jean Gasnier. Sagemath code for the subfield method. https://gitlab.inria.fr/jgasnier/subfield-method, 2023.

[Gau01] Carl Friedrich Gauss. *Disquisitiones Arithmeticae*. 1801.

[GG25] Jean Gasnier and Aurore Guillevic. An algebraic point of view on the generation of pairing-friendly curves. *SIAM Journal on Applied Algebra and Geometry*, 9(2):456–480, 2025.

[Gop83] V. D. Goppa. Algebraico-geometric codes. *Math. USSR, Izv.*, 21:75–91, 1983.

[GS95] Arnaldo Garcia and Henning Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound. *Invent. Math.*, 121(1):211–222, 1995.

[GX22] Venkatesan Guruswami and Chaoping Xing. Optimal rate list decoding over bounded alphabets using algebraic-geometric codes. *J. ACM*, 69(2):48, 2022. Id/No 10.

[Har77] Robin Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer, 1977.

[Hav89] A. Havemose. *Decoding algebraic geometric codes*. PhD thesis, Danmarks Tekniske Højskole, Aug. 1989.

[HB92] D. R. Heath-Brown. Zero-free regions for Dirichlet L-functions and the least prime in an arithmetic progression. *Proc. Lond. Math. Soc. (3)*, 64(2):265–338, 1992.

[HP95] Tom Høholdt and Ruud Pellikaan. On the decoding of algebraic-geometric codes. *IEEE Trans. Inf. Theory*, 41(6):1589–1614, 1995.

[Iha81] Yasutaka Ihara. Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci., Univ. Tokyo, Sect. I A*, 28:721–724, 1981.

[Jan96] Gerald J. Janusz. *Algebraic number fields.*, volume 7 of *Grad. Stud. Math.* Providence, RI: AMS, American Mathematical Society, 2nd ed. edition, 1996.

[JLJ+89] Jørn Justesen, Knud J. Larsen, H. Elbrønd Jensen, Allan Havemose, and Tom Høholdt. Construction and decoding of a class of algebraic geometry codes. *IEEE Trans. Inf. Theory*, 35(4):811–821, 1989.

[Jou00] Antoine Joux. A one round protocol for tripartite diffie-hellman. In Wieb Bosma, editor, *Algorithmic Number Theory, 4th International Symposium, ANTS-IV, Leiden, The Netherlands, July 2-7, 2000, Proceedings*, volume 1838 of *Lecture Notes in Computer Science*, pages 385–394. Springer, 2000.

[Ked01] Kiran S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.*, 16(4):323–338, 2001.

[KS91] Erich Kaltofen and B. David Saunders. On Wiedemann's method of solving sparse linear systems. In *Applied algebra, algebraic algorithms and error-correcting codes. 9th international symposium, AAECC '9, New Orleans, LA, USA, October 7–11, 1991. Proceedings*, pages 29–38. Berlin etc.: Springer-Verlag, 1991.

[KSS08] Ezekiel J. Kachisa, Edward F. Schaefer, and Michael Scott. Constructing brezing-weng pairing-friendly elliptic curves using elements in the cyclotomic field. In Steven D. Galbraith and Kenneth G. Paterson, editors, *Pairing-Based Cryptography - Pairing 2008, Second International Conference, Egham, UK, September 1-3, 2008. Proceedings*, volume 5209 of *Lecture Notes in Computer Science*, pages 126–135. Springer, 2008.

[Lac86] Gilles Lachaud. The geometric Goppa codes. Sémin. Bourbaki, 37e année, Vol. 1984/85, Exp. No. 641, Astérisque 133/134, 189-207 (1986)., 1986.

[Lan56a] Serge Lang. Sur les séries L d'une variété algébrique. *Bull. Soc. Math. Fr.*, 84:385–407, 1956.

[Lan56b] Serge Lang. Unramified class field theory over function fields in several variables. *Ann. Math. (2)*, 64:285–325, 1956.

[Lan87] Serge Lang. *Elliptic functions. Second edition*, volume 112 of *Grad. Texts Math.* Springer, Cham, 1987.

[Lan94] Serge Lang. *Algebraic number theory.*, volume 110 of *Grad. Texts Math.* New York: Springer-Verlag, 2nd ed. edition, 1994.

[Lan02] Serge Lang. *Algebra*. Springer New York, NY, 2002.

[LdS13] Hendrik Lenstra and Bart de Smit. Standard models of finite fields. In Gary L. Mullen and Daniel Panario, editors, *Handbook of Finite Fields*, Discrete mathematics and its applications, pages 345–363. CRC Press, 2013.

[Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxf. Grad. Texts Math.* Oxford: Oxford University Press, 2002.

[LMF25] The LMFDB Collaboration. The L-functions and modular forms database. https://www.lmfdb.org, 2025. [Online; accessed 20 February 2025].

[LZZ24] Jianming Lin, Chang-An Zhao, and Yuhao Zheng. Efficient implementation of super-optimal pairings on curves with small prime fields at the 192-bit security level. ePrint 2024/1195, 2024.

[Lü23] Frank Lübeck. Standard generators of finite fields and their cyclic subgroups. *Journal of Symbolic Computation*, 117:51–67, 2023.

[MOV93] Alfred Menezes, Tatsuaki Okamoto, and Scott A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Trans. Inf. Theory*, 39(5):1639–1646, 1993.

[Neu86] Jürgen Neukirch. *Class field theory*, volume 280 of *Grundlehren Math. Wiss.* Springer, Cham, 1986.

[NW19] Anand Kumar Narayanan and Matthew Weidner. Subquadratic time encodable codes beating the Gilbert-Varshamov bound. *IEEE Trans. Inf. Theory*, 65(10):6010–6021, 2019.

[NX98] Harald Niederreiter and Chaoping Xing. A general method of constructing global function fields with many rational places. In *Algorithmic number theory. 3rd international symposium, ANTS-III, Portland, OR, USA, June 21–25, 1998. Proceedings*, pages 555–566. Berlin: Springer, 1998.

[Pet60] W. W. Peterson. Encoding and error-correction procedures for the Bose-Chaudhuri codes. IRE Trans. Inf. Theory IT-6, 459-470 (1960); translation in Kibern. Sb. 6, 25-54 (1963);, 1960.

[Pil90] J. Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Math. Comput.*, 55(192):745–763, 1990.

[Pom01] Carl Pomerance. The expected number of random elements to generate a finite Abelian group. *Period. Math. Hung.*, 43(1-2):191–198, 2001.

[Por88] S.C. Porter. *Decoding codes arising from Goppa's construction on algebraic curves*. PhD thesis, Yale univ., Dec. 1988.

[Que89] Heinz-Georg Quebbemann. Cyclotomic Goppa codes. *IEEE Trans. Inf. Theory*, 34(5):1317–1320, 1989.

[Ran12] Hugues Randriambololona. Bilinear complexity of algebras and the Chudnovsky-Chudnovsky interpolation method. *J. Complexity*, 28(4):489–517, 2012.

[Ros54] Maxwell Rosenlicht. Generalized jacobian varieties. *Ann. Math. (2)*, 59:505–530, 1954.

[Ros87] Michael Rosen. The Hilbert class field in function fields. *Expo. Math.*, 5:365–378, 1987.

[RS60] I. S. Reed and Gustave Solomon. Polynomial codes over certain finite fields. *J. Soc. Ind. Appl. Math.*, 8:300–304, 1960.

[RSR69] Lawrence R. Rabiner, Ronald W. Schafer, and Charles M. Rader. The chirp z-transform algorithm and its application. *Bell System Tech. J.*, 48:1249–1292, 1969.

[Sat00] Takakazu Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 15(4):247–270, 2000.

[Sch31] Friedrich Karl Schmidt. Analytische Zahlentheorie in Körpern der Charakteristik p. *Math. Z.*, 33:1–32, 1931.

[Sch85] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comput.*, 44:483–494, 1985.

[Ser71] Jean-Pierre Serre. Représentations linéaires des groupes finis. 2e éd., refondue. (Linear representations of finite groups. 2nd ed., revised). Collection methodes. Paris: Hermann. 182 p. 32 F (1971)., 1971.

[Ser78] Jean-Pierre Serre. *A course in arithmetic. Translation of "Cours d'arithmetique". 2nd corr. print*, volume 7 of *Grad. Texts Math.* Springer, Cham, 1978.

[Ser84] Jean-Pierre Serre. Groupes algébriques et corps de classes. 2ième éd., rev. et corr. (Nouv. tirage). Actualités Scientifiques et Industrielles. 1264. Publications de l'Institut de Mathématique de l'Université de Nancago, VII. Paris: Hermann. 208 p. (1984)., 1984.

[Ser20] Jean-Pierre Serre. *Rational points on curves over finite fields.*, volume 18 of *Doc. Math. (SMF)*. Paris: Société Mathématique de France (SMF), 2020. With contributions by Everett Howe, Joseph Oesterlé and Christophe Ritzenthaler. Edited by Alp Bassa, Elisa Lorenzo García, Christophe Ritzenthaler and René Schoof.

[Sho92] Mohammad Amin Shokrollahi. Optimal algorithms for multiplication in certain finite fields using elliptic curves. *SIAM J. Comput.*, 21(6):1193–1198, 1992.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Grad. Texts Math.* New York, NY: Springer-Verlag, 1994.

[SKHN75] Yasuo Sugiyama, Masao Kasahara, Shigeichi Hirasawa, and Toshihiko Namekawa. A method for solving key equation for decoding Goppa codes. *Inf. Control*, 27:87–99, 1975.

[Sti08] Henning Stichtenoth. *Algebraic Function Fields and Codes.* Springer Publishing Company, Incorporated, 2nd edition, 2008.

[STV92] Igor E. Shparlinski, Michael A. Tsfasman, and Serge G. Vladut. Curves with many points and multiplication in finite fields. In *Coding theory and algebraic geometry (Luminy, 1991)*, volume 1518 of *Lecture Notes in Math.*, pages 145–169. Springer, Berlin, 1992.

[SV90] Alexei N. Skorobogatov and Sergei G. Vlăduţ. On the decoding of algebraic-geometric codes. *IEEE Trans. Inf. Theory*, 36(5):1051–1060, 1990.

[The22] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.3)*, 2022. `https://www.sagemath.org`.

[TVZ82] M. A. Tsfasman, S. G. Vlădut, and Th. Zink. Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. *Math. Nachr.*, 109:21–28, 1982.

[VD83] S. G. Vladut and V. G. Drinfel'd. Number of points of an algebraic curve. *Funct. Anal. Appl.*, 17:53–54, 1983.

[vdG09] Gerard van der Geer. Hunting for curves with many points. In *Coding and cryptology. Second international workshop, IWCC 2009, Zhangjiajie, China, June 1–5, 2009. Proceedings*, pages 82–96. Berlin: Springer, 2009.

[vdGHLR09] Gerard van der Geer, Everett W. Howe, Kristin E. Lauter, and Christophe Ritzenthaler. Tables of curves with many points, 2009. Retrieved January 2025.

[Ver10] Frederik Vercauteren. Optimal pairings. *IEEE Trans. Inf. Theory*, 56(1):455–461, 2010.

[Was77] Siri Krishan Wasan. Quasi abelian codes. *Publ. Inst. Math., Nouv. Sér.*, 21:201–206, 1977.

[Wat69] W. C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. Éc. Norm. Supér. (4)*, 2:521–560, 1969.

[Wei48] André Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent*, volume 7 of *Publ. Inst. Math. Univ. Strasbourg.* Hermann, Paris, 1948.

[Wie86] Douglas H. Wiedemann. Solving sparse linear equations over finite fields. *IEEE Trans. Inf. Theory*, 32:54–62, 1986.

[Xyl11] Triantafyllos Xylouris. On the least prime in an arithmetic progression and estimates for the zeros of Dirichlet L-functions. *Acta Arith.*, 150(1):65–91, 2011.