Explicit Riemann-Roch spaces in the Hilbert class field

Jean-Marc Couveignes, Jean Gasnier

EXPLICIT RIEMANN-ROCH SPACES IN THE HILBERT CLASS FIELD

JEAN-MARC COUVEIGNES AND JEAN GASNIER

ABSTRACT. Let $\mathbf{K}$ be a finite field, X and Y two curves over $\mathbf{K}$, and $Y \to X$ an unramified abelian cover with Galois group G. Let D be a divisor on X and E its pullback on Y. Under mild conditions the linear space associated with E is a free $\mathbf{K}[G]$-module. We study the algorithmic aspects and applications of these modules.

1. INTRODUCTION

Given a curve Y over a field $\mathbf{K}$, and two divisors E and Q on Y, with Q effective and disjoint from E, the evaluation map $e : H^0(Y, \mathcal{O}_Y(E)) \to H^0(Q, \mathcal{O}_Q)$ is a natural $\mathbf{K}$-linear datum of some importance for various algorithmic problems such as efficient computing in the Picard group of Y (see [27, 28]), constructing good error correcting codes [15, 17, 47], or bounding the bilinear complexity of multiplication in finite fields [45, 44, 3, 4, 9, 37]. Assume G is a finite group of automorphisms of $Y/\mathbf{K}$, and the divisors E and Q are G-equivariant (they are equal to their pullback by any element of G). The evaluation map e is then a $\mathbf{K}[G]$-linear map between two $\mathbf{K}[G]$-modules. In some cases these modules can be shown to be both free, and their rank as $\mathbf{K}[G]$-modules is then smaller than their dimension as $\mathbf{K}$-vector spaces, by a factor $\mathfrak{o}$, the order of G. This is of quite some help when G is abelian, because multiplication in $\mathbf{K}[G]$ is achieved in quasi-linear time using discrete Fourier transform, and the advantage of lowering dimension is much stronger than the disadvantage of dealing with a larger ring of scalars.

In this work we review basic algebraic and algorithmic properties of $\mathbf{K}[G]$-modules when G is a finite group. We then focus on free $\mathbf{K}[G]$-modules arising from abelian groups acting freely on a curve. We will see that this special case has a rich mathematical background and produces interesting constructions.

In Section 2 we review elementary properties of $\mathbf{K}[G]$-modules when $\mathbf{K}$ is a commutative field and G a finite group. We recall in Section 3 how unramified fibers of Galois covers of curves produce free $\mathbf{K}[G]$-modules and we introduce natural bases for these modules and their duals. We study the abelian unramified case in Section 4 and see that Riemann-Roch spaces associated to G-equivariant divisors tend to be free $\mathbf{K}[G]$-modules then. Evaluating at another G-equivariant divisor then produces a $\mathbf{K}[G]$-linear map between two free $\mathbf{K}[G]$-modules. This makes it possible to treat evaluation and interpolation as $\mathbf{K}[G]$-linear problems. We introduce the matrices associated to these problems. Section 5 is devoted to the definition and computation of Padé approximants in this context. The complexity of arithmetic operations in $\mathbf{K}[G]$ is bounded in Section 6 using various classical discrete Fourier transforms. In Section 7 we use effective class field theory and the algorithmics of curves and jacobian varieties to compute the

Date: December 5, 2023.

evaluation and interpolation matrices introduced in Section 4. Section 8 provides two applications of interpolation with $\mathbf{K}[G]$-modules: multiplication in finite fields and geometric codes. The asymptotic properties of the codes constructed this way are studied in Section 9.

CONTENTS

2. DUALITY FOR $\mathbf{K}[G]$-MODULES

In this section $\mathbf{K}$ is a commutative field and G is a finite group. We state elementary properties of $\mathbf{K}[G]$-modules and their duals. In Section 2.1 we describe the natural correspondence between G-invariant $\mathbf{K}$-bilinear forms and $\mathbf{K}[G]$-bilinear forms. We see in Section 2.2 that the orthogonal of a $\mathbf{K}[G]$-submodule for either form is the same. Sections 2.3 concerns the canonical bilinear form relating a $\mathbf{K}[G]$-module and its dual The ring $\mathbf{K}[G]$ has the Frobenius property [12, Chapter IX]. We recall in Section 2.4 a convenient consequence of it.

2.1. **Invariant bilinear forms.** Let M be a right $\mathbf{K}[G]$-module. Let N be a left $\mathbf{K}[G]$-module. Let

$$< ., . >: M \times N \to \mathbf{K}$$

be a $\mathbf{K}$-bilinear form. We assume that this form is invariant by the action of G in the sense that

$$< m.\sigma, n > = < m, \sigma.n >$$

for every m in M, n in N, and σ in G. We define a map

$$(1) \qquad (.,.) \quad : \quad \begin{array}{ccc} N \times M & \longrightarrow & \mathbf{K}[G] \\ n, m & \longmapsto & (n, m) = \sum_{\sigma \in G} < m.\sigma^{-1}, n > \sigma \end{array}$$

Proposition 1. *The map $(.,.)$ in Equation (1) is $\mathbf{K}[G]$-bilinear.*

Proof Indeed for any τ in G, m in M, and n in N

$$\begin{aligned} (\tau.n, m) &= \sum_{\sigma \in G} < m.\sigma^{-1}, \tau.n > \sigma \\ &= \sum_{\sigma \in G} < m.\sigma^{-1}\tau^{-1}, \tau.n > \tau\sigma \\ &= \sum_{\sigma \in G} < m.\sigma^{-1}, n > \tau\sigma \\ &= \tau \sum_{\sigma \in G} < m.\sigma^{-1}, n > \sigma \\ &= \tau(n, m). \end{aligned}$$

And

$$\begin{aligned} (n, m.\tau) &= \sum_{\sigma \in G} < m.\tau\sigma^{-1}, n > \sigma \\ &= \sum_{\sigma \in G} < m.\tau\tau^{-1}\sigma^{-1}, n > \sigma\tau \\ &= \sum_{\sigma \in G} < m.\sigma^{-1}, n > \sigma\tau \\ &= (n, m)\tau. \end{aligned}$$

□

2.2. **Orthogonality.** In the situation of Section 2.1 we consider a right $\mathbf{K}[G]$-submodule U of M. Call

$$U^\perp = \{n \in N \mid < U, n >= 0\}$$

the orthogonal to U in N for the $< ., . >$ form. This is a $\mathbf{K}$-vector space. Since U is stable by the action of G, its orthogonal $U^\perp$ is a left $\mathbf{K}[G]$-module. And $U^\perp$ is the orthogonal to U for the $(.,.)$ form :

$$U^\perp = \{n \in N \mid (n, U) = 0\}.$$

We consider similarly a left $\mathbf{K}[G]$-submodule V of N and call

$$V^\circ = \{m \in M \mid < m, V >= 0\}$$

the orthogonal to V in M for the $< ., . >$ form. This is a right $\mathbf{K}[G]$ module. And V° is the orthogonal to V for the $(.,.)$ form :

$$V^\circ = \{m \in M \mid (V, m) = 0\}.$$

We have $U \subset (U^\perp)^\circ$ and $V \subset (V^\circ)^\perp$. These inclusions are equalities when M and N are finite dimensional and $< ., . >$ is perfect.

2.3. **The dual of a $\mathbf{K}[G]$-module.** Let N be a left $\mathbf{K}[G]$-module. We can see N as a $\mathbf{K}$-vector space and call $\hat{N}$ its dual. This is naturally a right $\mathbf{K}[G]$-module. For every φ in $\hat{N}$ and σ in G we set $\varphi.\sigma = \varphi \circ \sigma$. We consider the canonical $\mathbf{K}$-bilinear form defined by

$$< \varphi, n >= \varphi(n)$$

for every n in N and φ in $\hat{N}$. For every σ in G we have

$$< \varphi.\sigma, n >= \varphi(\sigma.n) =< \varphi, \sigma.n >$$

so $< ., . >$ is invariant by G. Following Section 2.1 we define a $\mathbf{K}[G]$-bilinear form

$$(.,.) : N \times \hat{N} \to \mathbf{K}[G]$$

by

$$(n, \varphi) = \sum_{\sigma \in G} \varphi(\sigma^{-1}.n)\sigma. \tag{2}$$

We define a map from $\hat{N}$ to the dual $\check{N}$ of N as a $\mathbf{K}[G]$-module, by sending φ to the map

$$\varphi^G : n \mapsto (n, \varphi). \tag{3}$$

We prove that this map is a bijection. First $\varphi \mapsto \varphi^G$ is trivially seen to be an injection. As for surjectivity we let $\psi : N \to \mathbf{K}[G]$ be a $\mathbf{K}[G]$-linear map. Writing

$$\psi(n) = \sum_{\sigma \in G} \psi_\sigma(n)\sigma$$

we define a $\mathbf{K}$-linear coordinate form ψ_σ on N for every σ in G. From the $\mathbf{K}[G]$-linearity of ψ we deduce that $\psi_\sigma(n) = \psi_1(\sigma^{-1}.n)$ where 1 is the identity element in G. So $\psi(n) = (n, \psi_1)$ for every n in N. So $\psi = (\psi_1)^G$.

2.4. **Free submodules of a $\mathbf{K}[G]$-module.** The ring $\mathbf{K}[G]$ may not be semisimple. Still free $\mathbf{K}[G]$-submodules of finite rank have a supplementary module.

Proposition 2. *Let G be finite group, $\mathbf{K}$ a commutative field, N a left $\mathbf{K}[G]$-module, V a submodule of N. If V is free of finite rank then it is a direct summand.*

Proof Let r be the rank of V. Let $v_1, v_2, \ldots, v_r$ be a basis of V. Let $\varphi_1, \varphi_2, \ldots, \varphi_r$ be the dual basis. For every i such that $1 \leqslant i \leqslant n$, the coordinate form $\varphi_{i,e}$ associated to the identity element in G belongs to $\hat{V}$. Let ψ_i be a $\mathbf{K}$-linear form on N whose restriction to V is $\varphi_{i,e}$. Let $\psi_i^G \in \check{N}$ be the associated $\mathbf{K}[G]$-linear form according to Equations (3) and (2). The restriction of ψ_i^G to V is φ_i. The map

$$\begin{array}{rcl} \psi & : & N \longrightarrow V \\ & & n \longmapsto \sum_{1\leqslant i\leqslant r} \psi_i^G(n).v_i \end{array}$$

is a $\mathbf{K}[G]$-linear projection onto V. Its kernel is a supplementary $\mathbf{K}[G]$-submodule to V. □

Proposition 2 is a consequence of the Frobenius property which is known [12, Chapter IX] to be satisfied by $\mathbf{K}[G]$. The proof above provides an algorithm to compute the supplementary module.

3. Curves with a group action

Let $\mathbf{K}$ be a commutative field. Let p be the characteristic of $\mathbf{K}$. Let X and Y be two smooth, projective, absolutely integral curves over $\mathbf{K}$. Let g_X be the genus of X. And similarly g_Y. Let $\tau : Y \to X$ be a Galois cover with Galois group G. Let $\mathfrak{o}$ be the order of G. There is a natural left action of G on $\mathbf{K}(Y)$ defined by

$$\sigma.f = f \circ \sigma^{-1} \quad \text{for } f \in \mathbf{K}(Y) \text{ and } \sigma \in G.$$

There is a natural right action of G on meromorphic differentials defined by

$$\omega.\sigma = \sigma^\star \omega \quad \text{for } \omega \in \Omega^1_{\mathbf{K}(Y)/\mathbf{K}} \text{ and } \sigma \in G.$$

These are $\mathbf{K}(X)$-linear actions. And the two actions are compatible in the sense that

$$(\omega.\sigma)(\sigma^{-1}.f) = (\omega f).\sigma \tag{4}$$

We study some free $\mathbf{K}[G]$-modules that arise naturally in this context.

3.1. **The residue ring of a non-ramified fiber.** Let P be a prime divisor (a place) on X. Let t_P be a uniformizing parameter at P. Let

$$a = \deg(P).$$

This is the degree over $\mathbf{K}$ of the residue field

$$\mathbf{K}_P = H^0(P, \mathcal{O}_P) = H^0(X, \mathcal{O}_X/\mathcal{O}_X(-P)).$$

We assume that τ is not ramified above P and let Q_1 be a place above P. We call G_1 the decomposition group of Q_1. This is the stabilizer of Q_1 in G. Places above P are parameterized by left cosets in G/G_1. We write the fiber above P

$$Q = \sum_{\sigma \in G/G_1} Q_\sigma \quad \text{with} \quad Q_\sigma = \sigma(Q_1).$$

We call

$$b = [G : G_1]$$

the number of places above P and let

$$c = \mathfrak{o}/b = |G_1|$$

be the residual degree, that is the degree of

$$\mathbf{K}_\sigma = H^0(Q_\sigma, \mathcal{O}_{Q_\sigma})$$

over $\mathbf{K}_P$ for all $\sigma \in G/G_1$. We call

$$\mathbf{R}_Q = H^0(Q, \mathcal{O}_Q) = H^0(Y, \mathcal{O}_Y/\mathcal{O}_Y(-Q))$$

the residue ring at Q. The action of G on $\mathbf{R}_Q$ makes it a free left $\mathbf{K}[G]$-module of rank a. Indeed it is a free $\mathbf{K}_P[G]$-module of rank 1. A basis for it consists of any normal element θ in $\mathbf{K}_1/\mathbf{K}_P$.

If m is a positive integer, Taylor expansion provides an isomorphism of $\mathbf{K}_P[G]$-modules

$$H^0(Y, \mathcal{O}_Y/\mathcal{O}_Y(-mQ)) \simeq \mathbf{R}_Q[t_P]/t_P^m$$

between the residue ring at mQ and the ring of truncated series in t_P. So the former is a free left $\mathbf{K}_P[G]$-module of rank m. A basis for it is made of the θt_P^k for $0 \leqslant k < m$.

3.2. **The residue ring of a non-ramified G-equivariant divisor.** We take P an effective divisor on X. We assume that τ does not ramify above P and call Q the pullback of P by τ. We write

$$P = \sum_{1 \leqslant i \leqslant I} m_i P_i.$$

We let t_i be a uniformizing parameter at P_i. We call a_i the degree of the place P_i. We call b_i the number of places of Y above P_i. We let $c_i = \mathfrak{o}/b_i$. For every $1 \leqslant i \leqslant I$ we choose a place $Q_{i,1}$ above P_i and call $G_{i,1}$ the decomposition group at $Q_{i,1}$. We call Q_i the pullback of P_i by τ and write

$$Q_i = \sum_{\sigma \in G/G_{i,1}} Q_{i,\sigma} \quad \text{with} \quad Q_{i,\sigma} = \sigma(Q_{i,1}).$$

its decomposition as a sum of b_i places. We call $\mathbf{K}_{i,\sigma}$ the residue field at $Q_{i,\sigma}$. We denote by $\mathbf{A}$ the residue algebra $H^0(Q, \mathcal{O}_Q)$. Taylor expansion induces an isomorphism of $\mathbf{K}$-algebras

$$\mathbf{A} = H^0(Q, \mathcal{O}_Q) = H^0(Y, \mathcal{O}_Y/\mathcal{O}_Y(-Q)) \simeq \bigoplus_{i=1}^{I} \bigoplus_{\sigma \in G/G_{i,1}} \mathbf{K}_{i,\sigma}[t_i]/t_i^{m_i}$$

which is compatible with the action of G. In the special case when all the places P_i have degree one, a basis for the $\mathbf{K}[G]$-module $H^0(Q, \mathcal{O}_Q)$ is made of the $\theta_i t_i^{k_i}$ for $1 \leqslant i \leqslant I$ and $0 \leqslant k_i < m_i$ where θ_i is a normal element in the extension $\mathbf{K}_{i,1}/\mathbf{K}$. The proposition below follows from the discussion in this section and the previous one.

Proposition 3. *Assume the hypotheses at the beginning of Section 3. Let P be an effective divisor on X. Assume that τ is not ramified above P and let Q be the pullbak of P by τ. The residue ring $H^0(Q, \mathcal{O}_Q)$ is a free $\mathbf{K}[G]$-module of rank the degree of P.*

3.3. **Duality.** We need a dual of $\mathbf{A}$ as a $\mathbf{K}$-vector space. We set

$$\hat{\mathbf{A}} = H^0(Y, \Omega^1_{Y/\mathbf{K}}(-Q)/\Omega^1_{Y/\mathbf{K}}) \simeq \bigoplus_{i=1}^{I} \bigoplus_{\sigma \in G/G_{i,1}} (\mathbf{K}_{i,\sigma}[t_i]/t_i^{m_i})\, \frac{dt_i}{t_i^{m_i}}.$$

For $f \in \mathbf{A}$ and $\omega \in \hat{\mathbf{A}}$ we write $< \omega, f >$ for the sum of the residues of ωf at all the geometric points of Q. This is a $\mathbf{K}$-bilinear form. We deduce from Equation (4) that this form is invariant by the action of G

$$< \omega.\sigma, f > = < \omega, \sigma.f >$$

We define a $\mathbf{K}[G]$-bilinear form using the construction in Section 2.1

$$(f, \omega) = \sum_{\sigma \in G} < \omega.\sigma^{-1}, f > \sigma \in \mathbf{K}[G]. \tag{5}$$

These two bilinear forms turn $\hat{\mathbf{A}}$ into the dual of $\mathbf{A}$ as a $\mathbf{K}$-vector space (resp. as a $\mathbf{K}[G]$-module). In the special case when all the places P_i have degree one, the dual basis to the basis introduced before Proposition 3 is made of the $\mu_i t_i^{m_i - k_i} dt_i/t_i$ for $1 \leqslant i \leqslant I$ and $0 \leqslant k_i < m_i$ where μ_i is the dual to the normal element θ_i in the extension $\mathbf{K}_{i,1}/\mathbf{K}$.

4. Free commutative actions

We study the situation at the beginning of Section 3 in the special case when the Galois cover $\tau : Y \to X$ is abelian and unramified. We prove that large enough equivariant Riemann-Roch spaces are free $\mathbf{K}[G]$-modules. To this end we prove in Section 4.2 that evaluation at some fibers induces an isomorphism with one of the $\mathbf{K}[G]$-modules studied in Section 3.2. We need a criterion for an equivariant divisors on Y to be non-special. We recall such a criterion in Section 4.1. We introduce in Section 4.3 the evaluation, interpolation and checking matrices whose existence follows from the freeness of the considered modules.

4.1. **Special invariant divisors.** The pullback by τ of a degree $g_X - 1$ divisor on X is a degree $g_Y - 1$ divisor on Y. We need a criterion for the latter divisor to be special.

Proposition 4. *Assume the hypotheses at the beginning of Section 3 with τ abelian and unramified and $\mathbf{K}$ algebraically closed. Write $\mathfrak{o} = \mathfrak{o}_p \times \mathfrak{o}_{p'}$ where $\mathfrak{o}_p$ is the largest power of p dividing $\mathfrak{o}$. Let c be a divisor class of degree $g_X - 1$ on X and let $\tau^\star(c)$ be its pullback on Y. If the class $\tau^\star(c)$ is effective then c is the sum of an effective class of degree $g_X - 1$ and a class of degree 0 annihilated by $\tau^\star$ and by $\mathfrak{o}_{p'}$.*

Proof From [11, §14]. Let D be a divisor in c and let E be the pullback of D by τ. We assume that $\tau^\star(c)$ is effective. The space $H^0(Y, \mathcal{O}_Y(E))$ is non-zero and is acted on by G. Let f be an eigenvector for this action. The divisor of f is $J - E$ where J is effective and stable under the action of G. So there exists an effective divisor I on X such that J is the pullback of I by τ. And the class of $I - D$ is annihilated by $\tau^\star$. It is also annihilated by $\mathfrak{o}_{p'}$ because $f^{\mathfrak{o}_{p'}}$ is invariant by G. □

4.2. **Riemann-Roch spaces.** Let E be a divisor on Y defined over $\mathbf{K}$ and invariant by G. The Riemann-Roch space $H^0(Y,\mathcal{O}_Y(E))$ is a $\mathbf{K}[G]$-module. This module is free provided the degree of E is large enough.

Proposition 5. *Assume the hypotheses at the beginning of Section 3 with τ abelian and unramified. Let D be a divisor on X with degree $\geqslant 2g_X-1$. Let E be the pullback of D by τ. The $\mathbf{K}$-vector space $H^0(Y,\mathcal{O}_Y(E))$ is a free $\mathbf{K}[G]$-module of rank $\deg(D)-g_X+1$.*

Proof We may assume that $\mathbf{K}$ is algebraically closed because of the Noether-Deuring theorem [8, §2, Section 5]. Let $k=\deg(D)-g_X+1$. We note that $k\geqslant g_X$. So there exist k points

$$P_1,P_2,\dots,P_k \quad \text{on} \quad X$$

such that the class of $D-P_1-P_2-\cdots-P_k$ is not the sum of an effective class of degree g_X-1 and a class annihilated by

$$\tau^\star:\mathrm{Pic}(X)\to\mathrm{Pic}(Y).$$

Let P be the divisor sum of all P_i and let Q be its pullback by τ. According to Proposition 4 the class of $E-Q$ is ineffective. Thus the evaluation map

$$H^0(Y,\mathcal{O}_Y(E))\to H^0(Q,\mathcal{O}_Q)$$

is an isomorphism of $\mathbf{K}[G]$-modules. Proposition 3 then implies that $H^0(Q,\mathcal{O}_Q)$ is a free $\mathbf{K}[G]$-module of rank k. □

When the degree of D is smaller than $2g_X-1$ it is not granted that $H^0(Y,\mathcal{O}_Y(E))$ is free. We mention two useful partial results.

Proposition 6. *Assume the hypotheses at the beginning of Section 3 with τ abelian and unramified. Assume p does not divide $\mathfrak{o}$. Let D be a divisor on X with degree $\geqslant g_X$. Let E be the pullback of D by τ. Then $H^0(Y,\mathcal{O}_Y(E))$ contains a free $\mathbf{K}[G]$-module of rank $\deg(D)-g_X+1$.*

Proof The ring $\mathbf{K}[G]$ is semi-simple. Let $\mathcal{L}(E)=H^0(Y,\mathcal{O}_Y(E))$. Let m be the smallest among the multiplicities in $\mathcal{L}(E)$ of irreducible representations of G. This is the smallest among the multiplicities of multiplicative characters of G in $\mathcal{L}(E)\otimes\bar{\mathbf{K}}$ where $\bar{\mathbf{K}}$ is an algebraic closure of $\mathbf{K}$. It is clear that $\mathcal{L}(E)$ contains m copies of the regular representation of G. On the other hand let $\chi:G\to\bar{\mathbf{K}}$ be a multiplicative character. Let r be an eigenfunction in $\bar{\mathbf{K}}(Y)$ associated with χ. The divisor of r is the pullback by τ of a divisor R on X. Let $\mathcal{L}(E)_\chi$ be the eigenspace in $\mathcal{L}(E)$ associated with χ. The map $f\mapsto f/r$ is a bijection between $\mathcal{L}(E)_\chi$ and $H^0(X,\mathcal{O}_X(D+R))$. The dimension of the latter is at least $\deg(D)-g_X+1$. □

Whe can say something also when G is a p-group and $\mathbf{K}$ a finite field.

Proposition 7. *Assume the hypotheses at the beginning of Section 3 with τ abelian and unramified. Assume $\mathbf{K}$ is a finite field with at least 4 elements. Assume $\mathfrak{o}$ is a power of p. Assume $g_X\geqslant 2$. Let $d\geqslant g_X$ be an integer. Let $r=d-g_X+1$. Assume there exists an effective divisor on X with degree r and defined over $\mathbf{K}$. Then there exists a divisor D on X such that D is defined over $\mathbf{K}$, D has degree d, and $H^0(Y,\mathcal{O}_Y(E))$ is a free $\mathbf{K}[G]$-module of rank $r=d-g_X+1$ where E is the pullback of D by τ.*

Proof Set $r = d - g_X + 1$. Let P be an effective divisor on X with degree r and defined over $\mathbf{K}$. According to a theorem of Ballet and Le Brigand [2, Theorem 11] there exists a degree $g_X - 1$ non-special divisor I defined over $\mathbf{K}$. Set $D = I + P$. Let E, J, and Q be the pullbacks of D, I, and P by τ. The divisor J is ineffective according to Proposition 4. So the evaluation map $H^0(Y, \mathcal{O}_Y(E)) \to H^0(Q, \mathcal{O}_Q)$ is a bijection. And the latter is a free $\mathbf{K}[G]$-module according to Proposition 3. □

4.3. **The orthogonal submodule.** In the situation of the beginning of Section 3 and assuming that τ is abelian and unramified we let D and P be divisors on X with P effective. We assume that D and P are disjoint. We assume that

$$2g_X - 1 \leqslant \deg(D) \leqslant \deg(P) - 1. \tag{6}$$

We call E the pullback of D by τ and Q the pullback of P. We write

$$\mathcal{L}(E) = H^0(Y, \mathcal{O}_Y(E)) \quad \text{and} \quad \Omega(-Q + E) = H^0(Y, \Omega_{Y/\mathbf{K}}(-Q + E)).$$

Proposition 5 and Equation (6) imply that these two $\mathbf{K}[G]$-modules are free. And the evaluation maps

$$\mathcal{L}(E) \longrightarrow \mathbf{A} \quad \text{and} \quad \Omega(-Q + E) \longrightarrow \hat{\mathbf{A}} \quad \text{are injective.}$$

So $\mathcal{L}(E)$ can be seen as a free submodule of $\mathbf{A}$ and $\Omega(-Q + E)$ as a free submodule of $\hat{\mathbf{A}}$. These two $\mathbf{K}[G]$-modules are orthogonal to each other for the form introduced in Equation (5). Proposition 2 implies that $\mathcal{L}(E)$ has a supplementary submodule in $\mathbf{A}$ that is isomorphic to the dual of $\Omega(-Q + E)$ and is thus a free submodule. Similarly $\Omega(-Q + E)$ has a free supplementary submodule in $\hat{\mathbf{A}}$ that is isomorphic to the dual of $\mathcal{L}(E)$.

In the special case when all the places P_i have degree one, we have introduced a natural basis for $\mathbf{A}$ before Proposition 3 and its dual basis $\hat{\mathbf{A}}$ in Section 3.3, using Taylor expansions at the places above the P_i. We choose $\mathbf{K}[G]$-bases for $\mathcal{L}(E)$ and $\Omega(-Q + E)$.

We denote $\mathcal{E}_E$ the $\deg(P) \times (\deg(D) - g_X + 1)$ matrix with coefficients in $\mathbf{K}[G]$ of the evaluation map $\mathcal{L}(E) \to \mathbf{A}$ in the chosen bases. We denote $\mathcal{C}_E$ the $\deg(P) \times (\deg(P) - \deg(D) + g_X - 1)$ matrix of the map $\Omega(-Q + E) \to \hat{\mathbf{A}}$ in the chosen bases. The matrix $\mathcal{C}_E$ checks that a vector in $\mathbf{A}$ belongs to $\mathcal{L}(E)$. Its left kernel is the image of $\mathcal{E}_E$. So

$$\mathcal{C}_E^t \times \mathcal{E}_E = 0$$

the zero $(\deg(P) - \deg(D) + g_X - 1) \times (\deg(D) - g_X + 1)$ matrix with coefficients in $\mathbf{K}[G]$.

We choose a $\mathbf{K}[G]$-linear projection $\mathbf{A} \to \mathcal{L}(E)$ and denote $\mathcal{I}_E$ the $(\deg(D) - g_X + 1) \times \deg(P)$ matrix of this projection. This is an interpolation matrix since it recovers a function in $\mathcal{L}(E)$ from its evaluation at Q. Equivalently

$$\mathcal{I}_E \times \mathcal{E}_E = 1$$

the $(\deg(D) - g_X + 1) \times (\deg(D) - g_X + 1)$ identity matrix with coefficients in $\mathbf{K}[G]$. We note that applying either of the matrices $\mathcal{E}_E, \mathcal{C}_E, \mathcal{I}_E$ requires at most a constant times $\deg(P)^2$ operations in $\mathbf{K}[G]$.

5. Padé approximants

In the situation of the beginning of Section 3 and assuming that τ is abelian and unramified we let D_0, D_1 and P be divisors on X with P effective. We assume that D_0 and D_1 are disjoint from P. We call E_0, E_1, and Q the pullbacks of D_0, D_1, and P by τ. We assume

$$2g_X - 1 \leqslant \deg(D_1) \leqslant \deg(P) - 1, \tag{7}$$

$$g_X \leqslant \deg(D_0) \leqslant \deg(P) - 1. \tag{8}$$

Equation (7) implies that the $\mathbf{K}[G]$-modules $\mathcal{L}(E_1)$ and $\Omega(-Q + E_1)$ are free and the evaluation maps into $\mathbf{A}$ and $\hat{\mathbf{A}}$ are injective. We assume that $\mathcal{L}(E_0)$ contains a free $\mathbf{K}[G]$-module of rank $\deg(D_0) - g_X + 1$ and denote $\mathcal{L}(E_0)_{\mathbf{fr}}$ such a submodule.

Given r in $\mathbf{A}$, $a_0 \neq 0$ in $\mathcal{L}(E_0)$ and a_1 in $\mathcal{L}(E_1)$ such that

$$a_0 r - a_1 = 0 \in \mathbf{A},$$

we say that (a_0, a_1) is a Padé approximant of r and call a_0 a **denominator** for r. Denominators for r are non-zero a_0 in $\mathcal{L}(E_0) \subset \mathbf{A}$ such that

$$a_0 r \in \mathcal{L}(E_1).$$

Equivalently

$$(a_0 r, \omega) = 0 \quad \text{for every} \quad \omega \in \Omega(-Q + E_1). \tag{9}$$

Denominators are thus non-zero solutions of a $\mathbf{K}$-linear system of equations. We note that this is not a $\mathbf{K}[G]$-linear system in general. In Section 5.1 we show that one can be a bit more explicit in some cases. We consider the problem of computing Padé approximants in Section 5.2.

5.1. The split case.

Assume that $P = P_1 + \cdots + P_n$ is a sum of n pairwise distinct rational points over $\mathbf{K}$. Assume that the fiber of τ above each P_i decomposes as a sum of $\mathfrak{o}$ rational points over $\mathbf{K}$. We choose a point $Q_{i,1}$ above each P_i and set

$$Q_{i,\sigma} = \sigma(Q_{i,1}) \quad \text{for every} \quad \sigma \in G.$$

For every $1 \leqslant i \leqslant n$ we call α_i the function in $\mathbf{A}$ that takes value 1 at $Q_{i,1}$ and zero everywhere else. We thus form a basis

$$\mathcal{A}_G = (\alpha_i)_{1 \leqslant i \leqslant n}$$

of $\mathbf{A}$ over $\mathbf{K}[G]$. We note $\hat{\mathcal{A}}_G$ its dual basis. For every $1 \leqslant i \leqslant n$ and $\sigma \in G$ we call

$$\alpha_{i,\sigma} = \sigma.\alpha_i = \alpha_i \circ \sigma^{-1}$$

the function in $\mathbf{A}$ that takes value 1 at $Q_{i,\sigma}$ and zero everywhere else. We thus form a basis

$$\mathcal{A}_{\mathbf{K}} = (\alpha_{i,\sigma})_{1 \leqslant i \leqslant n,\, \sigma \in G}$$

of $\mathbf{A}$ over $\mathbf{K}$. The coordinates of r in the $\mathbf{K}[G]$-basis $\mathcal{A}_G$ are

$$r_G = \Big(\sum_{\sigma \in G} r(Q_{i,\sigma})\sigma\Big)_{1 \leqslant i \leqslant n}$$

and the coordinates of $r \in \mathbf{A}$ in the $\mathbf{K}$-basis $\mathcal{A}_{\mathbf{K}}$ are

$$r_{\mathbf{K}} = (r(Q_{i,\sigma}))_{1 \leqslant i \leqslant n,\, \sigma \in G}.$$

Multiplication by r is a $\mathbf{K}$-linear map from $\mathbf{A}$ to $\mathbf{A}$. We call

$$\mathcal{R}_{\mathbf{K}} \in \mathcal{M}_{\mathfrak{o}.n,\mathfrak{o}.n}(\mathbf{K})$$

the $\mathfrak{o}.n \times \mathfrak{o}.n$ diagonal matrix of this map in the basis $\mathcal{A}_{\mathbf{K}}$.

We choose a $\mathbf{K}[G]$-basis $\mathcal{Z}_G$ for $\mathcal{L}(E_0)_{\mathbf{fr}}$ and denote $\mathcal{E}_G^0$ the $\deg(P) \times (\deg(D_0) - g_X + 1)$ matrix of the $\mathbf{K}[G]$-linear map

$$\mathcal{L}(E_0)_{\mathbf{fr}} \to \mathbf{A} \tag{10}$$

in the bases $\mathcal{Z}_G$ and $\mathcal{A}_G$. We denote $\mathcal{Z}_{\mathbf{K}}$ the $\mathbf{K}$-basis of $\mathcal{L}(E_0)_{\mathbf{fr}}$ obtained by letting G act on $\mathcal{Z}_G$. Call $\mathcal{E}_{\mathbf{K}}^0$ the matrix of the map (10) in the bases $\mathcal{Z}_{\mathbf{K}}$ and $\mathcal{A}_{\mathbf{K}}$. The matrix $\mathcal{E}_{\mathbf{K}}^0$ is obtained from $\mathcal{E}_G^0$ by replacing each $\mathbf{K}[G]$ entry by the corresponding $\mathfrak{o} \times \mathfrak{o}$ circulant-like matrix with entries in $\mathbf{K}$.

We choose a $\mathbf{K}[G]$-basis $\mathcal{U}_G$ for $\Omega(-Q + E_1)$ and denote $\mathcal{C}_G^1$ the matrix of the injective map

$$\Omega(-Q + E_1) \to \hat{\mathbf{A}} \tag{11}$$

in the bases $\mathcal{U}_G$ and $\hat{\mathcal{A}}_G$. This is a $\deg(P) \times (\deg(P) - \deg(D_1) + g_X - 1)$ matrix with entries in $\mathbf{K}[G]$. We denote $\mathcal{U}_{\mathbf{K}}$ the $\mathbf{K}$-basis of $\Omega(-Q + E_1)$ obtained by letting G act on $\mathcal{U}_G$. The matrix of the map (11) in the bases $\mathcal{U}_{\mathbf{K}}$ and $\hat{\mathcal{A}}_{\mathbf{K}}$ is called $\mathcal{C}_{\mathbf{K}}^1$.

Let a_0 in $\mathcal{L}(E_0)_{\mathbf{fr}}$ and let x_G be the coordinates of a_0 in the $\mathbf{K}[G]$-basis $\mathcal{Z}_G$. This is a column of height $\deg(D_0) - g_X + 1$. We call $x_{\mathbf{K}}$ the coordinates of a_0 in the $\mathbf{K}$-basis $\mathcal{Z}_{\mathbf{K}}$. This is a column of height $\mathfrak{o}.(\deg(D_0) - g_X + 1)$ obtained from x_G by replacing each entry by its $\mathfrak{o}$ coefficients in the canonical basis of $\mathbf{K}[G]$. We deduce from Equation (9) that a_0 is a denominator for r if and only if $x_{\mathbf{K}}$ is in the kernel of the matrix

$$\mathcal{D}_r = (\mathcal{C}_{\mathbf{K}}^1)^t \times \mathcal{R}_{\mathbf{K}} \times \mathcal{E}_{\mathbf{K}}^0 \in \mathcal{M}_{\mathfrak{o}.(\deg P - deg D_1 + g_X - 1) \times \mathfrak{o}.(\deg D_0 - g_X + 1)}(\mathbf{K}).$$

Proposition 8. *Assume we are in the context of the beginning of Section 5. In particular assume Equations (7) and (8), assume that P is a sum of n pairwise distinct $\mathbf{K}$-rational points, and that the n corresponding fibers of τ split over $\mathbf{K}$. Assume we are given the matrices $\mathcal{E}_{\mathbf{K}}^0$ and $\mathcal{C}_{\mathbf{K}}^1$. On input an $r = (r(Q_{i,\sigma}))_{1 \leqslant i \leqslant n,\, \sigma \in G}$ in $\mathbf{A}$ and some a_0 in $\mathcal{L}(E_0)_{\mathbf{fr}}$, given by its coordinates $x_{\mathbf{K}}$ in the basis $\mathcal{Z}_{\mathbf{K}}$, one can check if $a_0 r \in \mathcal{L}(E_1)$ at the expense of $\mathcal{Q}.n^2$ operations in $\mathbf{K}[G]$ (addition, multiplication) and $\mathcal{Q}.\mathfrak{o}.n$ operations in $\mathbf{K}$ (addition, multiplication) where $\mathcal{Q}$ is some absolute constant.*

Proof We first multiply $x_{\mathbf{K}}$ by $\mathcal{E}_{\mathbf{K}}^0$. This requires less than $2\deg(P) \times (\deg(D_0) - g_X + 1)$ operations in $\mathbf{K}[G]$. We then multiply the result by $\mathcal{R}_{\mathbf{K}}$. This requires less than $\mathfrak{o}.\deg(P)$ operations in $\mathbf{K}$. We finally multiply the result by $(\mathcal{C}_{\mathbf{K}}^1)^t$. This requires less than $2\deg(P) \times (\deg(P) - \deg(D_1) + g_X - 1)$ operations in $\mathbf{K}[G]$. □

5.2. **Computing Padé approximants.** Beeing able to check a denominator we can find a random one, if there is some in $\mathcal{L}(E_0)_{\mathbf{fr}}$, using an iterative method as in [51, 24]. Recall that an $\ell \times n$ **black box** matrix A with coefficients in a field $\mathbf{K}$ is an oracle that on input an $n \times 1$ vector x returns Ax.

Proposition 9 (Wiedemann, Kaltofen, Saunders)**.** *There exists a probabilistic (Las Vegas) algorithm that takes as input an $\ell \times n$ black box matrix A and an $\ell \times 1$ vector b with entries in a finite field $\mathbf{K}$ and returns a uniformly distributed random solution x to the system $Ax = b$*

with probability of success $\geqslant 1/2$ *at the expense of* $\mathcal{Q}.m.\log m$ *calls to the black box for* A *and* $\mathcal{Q}.m^2.(\log(m))^2$ *operations in* $\mathbf{K}$ *(addition, multiplication, inversion, picking a random element) where* $m = \max(\ell, n)$ *and* $\mathcal{Q}$ *is some absolute constant.*

From Propositions 8 and 9 we deduce

Proposition 10. *Under the hypotheses of Proposition 8 and on input a vector* $r = (r(Q_{i,j})_{i,j})$ *in* $\mathbf{A}$ *one can find a uniformly distributed random denominator, if there is some in* $\mathcal{L}(E_0)_{\mathbf{fr}}$*, for* r *with probability of success* $\geqslant 1/2$ *at the expense of* $\mathcal{Q}.\mathfrak{o}.n^3.\log(\mathfrak{o}.n)$ *operations in* $\mathbf{K}[G]$ *(addition, multiplication) and* $\mathcal{Q}.(\mathfrak{o}.n.\log(\mathfrak{o}.n))^2$ *operations in* $\mathbf{K}$ *(addition, multiplication, inversion, picking a random element) where* $\mathcal{Q}$ *is some absolute constant.*

Once we have found a denominator a_0 for r we set $a_1 = ra_0$ and recover the coordinates of a_1 applying the interpolation matrix associated to E_1.

6. Computing in the group algebra

Given a finite commutative group G and a finite field $\mathbf{K}$ we will need efficient algorithms to multiply in $\mathbf{K}[G]$. This is classically achieved using discrete Fourier transform when G is cyclic and $\mathbf{K}$ contains enough roots of unity. The complexity analysis requires some care in general. This is the purpose of this section. We recall in Section 6.1 the definition of Fourier transform in the setting of commutative finite groups. The most classical case of cyclic groups is studied in Section 6.2 from an algorithmic point of view. The general case follows by induction as explained in Section 6.3. The complexity of the resulting multiplication algorithm in $\mathbf{K}[G]$ is bounded in Section 6.4.

6.1. **Fourier transform.** Let G be a finite commutative group. Let $\mathfrak{o}$ be the order of G. Let e be its exponent. Let $\mathbf{K}$ be a commutative field containing a primitive e-th root of unity. In particular e and $\mathfrak{o}$ are non-zero in $\mathbf{K}$. Let $\hat{G}$ be the dual of G defined as the group of characters $\chi : G \to \mathbf{K}^*$. We define a map from the group algebra of G to the algebra of functions on G

$$\begin{array}{rccc} \top & : & \mathbf{K}[G] & \longrightarrow \mathrm{Hom}(G, \mathbf{K}) \\ & & \sum_{\sigma\in G} a_\sigma \sigma & \longmapsto \sigma \mapsto a_\sigma \end{array}$$

This is an isomorphism of $\mathbf{K}$-vector space. We call $\perp : \mathrm{Hom}(G, \mathbf{K}) \to \mathbf{K}[G]$ the reciprocal map. We dualy define

$$\begin{array}{rccc} \hat{\top} & : & \mathbf{K}[\hat{G}] & \longrightarrow \mathrm{Hom}(\hat{G}, \mathbf{K}) \\ & & \sum_{\chi\in\hat{G}} a_\chi \chi & \longmapsto \chi \mapsto a_\chi \end{array}$$

and its reciprocal map $\hat{\perp}$. We call

$$\iota_G : \mathbf{K}[G] \to \mathbf{K}[G]$$

the $\mathbf{K}$-linear involution that maps σ onto σ^{-1}. We define the Fourier transform

$$\begin{array}{rccc} \mathrm{FT}_G & : & \mathbf{K}[G] & \longrightarrow \mathrm{Hom}(\hat{G}, \mathbf{K}) \\ & & \sum_{\sigma\in G} a_\sigma \sigma & \longmapsto \chi \mapsto \sum_\sigma a_\sigma \chi(\sigma) \end{array}$$

The Fourier transform evaluates an element in the group algebra at every character. The Fourier transform of the dual group

$$\begin{aligned} \mathrm{FT}_{\hat{G}} \qquad : \qquad & \mathbf{K}[\hat{G}] \longrightarrow \mathrm{Hom}(G, \mathbf{K}) \\ & \textstyle\sum_{\chi \in \hat{G}} a_\chi \chi \longmapsto \sigma \mapsto \sum_\chi a_\chi \chi(\sigma) \end{aligned}$$

provides an inverse for FT_G in the sense that

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

is the $\mathbf{K}$-linear invertible map that sends σ to $\mathfrak{o}.\sigma^{-1}$.

Let M be a finite dimensional $\mathbf{K}$-vector space. We set

$$M[G] = M \otimes_{\mathbf{K}} \mathbf{K}[G]$$

and note that

$$\mathrm{Hom}(\hat{G}, M) = M \otimes_{\mathbf{K}} \mathrm{Hom}(\hat{G}, \mathbf{K}).$$

We define a Fourier transform on M

$$\begin{aligned} \mathrm{FT}_M \qquad : \qquad & M[G] \longrightarrow \mathrm{Hom}(\hat{G}, M) \\ & \textstyle\sum_{\sigma \in G} m_\sigma \otimes \sigma \longmapsto \chi \mapsto \sum_\sigma \chi(\sigma) m_\sigma \end{aligned}$$

It turns a free $\mathbf{K}[G]$-module into a free $\mathrm{Hom}(\hat{G}, \mathbf{K})$-module.

6.2. **Univariate Fourier transform.** We assume in this section that the group G is cyclic of order $\mathfrak{o}$. We choose a primitive $\mathfrak{o}$-th root of unity ω in $\mathbf{K}$. We choose a generator in $\hat{G}$ and deduce the following identifications

$$\mathrm{Hom}(\hat{G}, \mathbf{K}) = \mathbf{K}^{\mathfrak{o}} \quad \text{and} \quad \mathbf{K}[G] = \mathbf{K}[x]/(x^{\mathfrak{o}} - 1).$$

Let M be a finite dimensional $\mathbf{K}$-vector space. Setting

$$M[x] = M \otimes_{\mathbf{K}} \mathbf{K}[x] \quad \text{and} \quad M[G] = M \otimes_{\mathbf{K}} \mathbf{K}[x]/(x^{\mathfrak{o}} - 1).$$

the Fourier transform is

$$\begin{aligned} \mathrm{FT}_M \qquad : \qquad & M[G] \longrightarrow M^{\mathfrak{o}} \\ & m \longmapsto (m(1), m(\omega), m(\omega^2), \ldots, m(\omega^{\mathfrak{o}-1})) \end{aligned}$$

Given m in $M[G] = M \otimes_{\mathbf{K}} \mathbf{K}[x]/(x^{\mathfrak{o}} - 1)$ the computation of $\mathrm{FT}_M(m)$ reduces to the multiplication of a polynomial of degree $2\mathfrak{o} - 2$ in $\mathbf{K}[x]$ and a vector of degree $\mathfrak{o} - 1$ in $M[x]$ using formulae by Rabiner, Schafer, Rader, and Bluestein [36, 6].

Proposition 11. *Let $\mathbf{K}$ be a commutative field. Let M be a finite dimensional $\mathbf{K}$-vector space. Let $\mathfrak{o} \geqslant 2$ be an integer. Assume that $\mathbf{K}$ contains a primitive $\mathfrak{o}$-th root of unity ω and a primitive root of unity of order a power of two that is bigger than $3\mathfrak{o} - 3$. Let*

$$m = m_0 \otimes 1 + m_1 \otimes x + \cdots + m_{\mathfrak{o}-1} \otimes x^{\mathfrak{o}-1} \bmod x^{\mathfrak{o}} - 1 \in M \otimes_{\mathbf{K}} \mathbf{K}[x]/(x^{\mathfrak{o}} - 1).$$

One can compute $\mathrm{FT}_M(m)$ at the expense of $\mathcal{Q}.\mathfrak{o}.\log \mathfrak{o}$ additions, multiplications and inversions in $\mathbf{K}$, additions and scalar multiplications in M, where $\mathcal{Q}$ is an absolute constant.

Proof We adapt the notation from [7, I.5.4, Proposition 5.10]. For every $0 \leqslant i \leqslant 2\mathfrak{o} - 2$ let

$$t_i = i(i-1)/2 \quad \text{and} \quad \beta_i = \omega^{t_i}.$$

We note that

$$t_{i+1} = t_i + i \quad \text{and} \quad \beta_{i+1} = \beta_i \omega^i.$$

So one can compute the β_i for $0 \leqslant i \leqslant 2\mathfrak{o} - 2$ at the expense of $4\mathfrak{o}$ operations in $\mathbf{K}$. We then compute the inverse of every β_i. For every $0 \leqslant i \leqslant \mathfrak{o} - 1$ let

$$n_i = \beta_i^{-1} m_i.$$

These can be computed at the expense of $\mathfrak{o}$ scalar multiplications in M. Let

$$n(x) = n_{\mathfrak{o}-1} + n_{\mathfrak{o}-2} \otimes x + \cdots + n_0 \otimes x^{\mathfrak{o}-1} \in M[x]$$

and let

$$b(x) = \beta_0 + \beta_1 x + \cdots + \beta_{2\mathfrak{o}-2} x^{2\mathfrak{o}-2} \in \mathbf{K}[x].$$

Let

$$r(x) = b(x).n(x) = \sum_{0 \leqslant i \leqslant 3\mathfrak{o}-3} r_i \otimes x^i \in M[x].$$

From the identity

$$t_{i+j} = t_i + t_j + ij$$

we deduce

$$\omega^{ij} \beta_i \beta_j = \beta_{i+j} \quad \text{for} \quad 0 \leqslant i, j \leqslant \mathfrak{o} - 1$$

and

$$\sum_{j=0}^{\mathfrak{o}-1} \omega^{ij} m_j = \beta_i^{-1} \sum_{j=0}^{o-1} \beta_{i+j} n_j.$$

We deduce that $\mathrm{FT}_M(m) = (\beta_0^{-1} r_{\mathfrak{o}-1}, \beta_1^{-1} r_{\mathfrak{o}}, \beta_2^{-1} r_{\mathfrak{o}+1}, \ldots, \beta_{\mathfrak{o}-1}^{-1} r_{2\mathfrak{o}-2})$. Since $\mathbf{K}$ contains a primitive root of unity of order a power of two that is bigger than $3\mathfrak{o} - 3$, the coefficients in the product $r(x) = b(x).n(x)$ can be computed at the expense of $\mathcal{Q}.\mathfrak{o}.\log \mathfrak{o}$ operations in $\mathbf{K}$, additions in M and products of a vector in M by a scalar in $\mathbf{K}$. See [7, I.2.4, Algorithme 2.3]. □

6.3. **Multivariate Fourier transform.** Let $(\mathfrak{o}_i)_{1 \leqslant i \leqslant I}$ be integers such that $2 \leqslant \mathfrak{o}_1 | \mathfrak{o}_2 | \ldots | \mathfrak{o}_I$. Let $C_i = \mathbf{Z}/\mathfrak{o}_i\mathbf{Z}$ and $G = \Pi_{1 \leqslant i \leqslant I} C_i$. For $1 \leqslant i \leqslant I$ set

$$A_i = \mathbf{K}[C_i] \quad \text{and} \quad B_i = \mathrm{Hom}(C_i, \mathbf{K}).$$

For $0 \leqslant i \leqslant I$ set

$$M_i = \bigotimes_{j \leqslant i} B_j \otimes \bigotimes_{j > i} A_j.$$

So $M_0 = \mathbf{K}[G]$ and $M_I = \mathrm{Hom}(G, \mathbf{K})$. For $1 \leqslant i \leqslant I$ write

$$M_i = \bigotimes_{j < i} B_j \otimes \mathbf{K}[C_i] \otimes \bigotimes_{j > i} A_j$$

as a $\mathbf{K}[C_i]$-module and call

$$F_i : M_i \to M_{i+1}$$

the corresponding Fourier transform as defined in Section 6.2. We check that

$$\mathrm{FT}_G = F_I \circ F_{I-1} \circ \cdots \circ F_1.$$

Using Proposition 11 we deduce

Proposition 12. *Let $(\mathfrak{o}_i)_{1\leqslant i\leqslant I}$ be integers such that $2\leqslant \mathfrak{o}_1|\mathfrak{o}_2|\dots|\mathfrak{o}_I$. Let $G=\prod_{1\leqslant i\leqslant I}(\mathbf{Z}/\mathfrak{o}_i\mathbf{Z})$. Let $\mathfrak{o}$ be the order of G. Let $e=\mathfrak{o}_I$ be the exponent of G. Let $\mathbf{K}$ be a commutative field containing a primitive root of unity of order e and a primitive root of unity of order a power of two that is bigger than $3e-3$. Given an element $a=\sum_{\sigma\in G}a_\sigma\sigma$ in $\mathbf{K}[G]$ one can compute $\mathrm{FT}_G(a)$ in $\mathrm{Hom}(\hat{G},\mathbf{K})$ at the expense of $\mathcal{Q}.\mathfrak{o}.\log\mathfrak{o}$ additions, multiplications and inversions in $\mathbf{K}$. Here $\mathcal{Q}$ is some absolute constant.*

6.4. **Fast multiplication in $\mathbf{K}[G]$.** Let G, $\mathfrak{o}$, e be as in Section 6.3. Let $\mathbf{K}$ be a commutative field. In this section we study the algorithmic complexity of computing the product of two given elements

$$a=\sum_{\sigma\in G}a_\sigma\sigma \quad\text{and}\quad b=\sum_{\sigma\in G}b_\sigma\sigma \quad\text{in}\quad \mathbf{K}[G]. \tag{12}$$

It will depend on the field $\mathbf{K}$. We first treat the case when $\mathbf{K}$ has enough roots of unity.

Proposition 13. *In the context of the beginning of Section 6.4 assume that $\mathbf{K}$ contains a primitive root of unity of order e and a primitive root of unity of order a power of two that is bigger than $3e-3$. One can compute the product $ab\in\mathbf{K}[G]$ at the expense of $\mathcal{Q}.\mathfrak{o}.\log\mathfrak{o}$ operations in $\mathbf{K}$ where $\mathcal{Q}$ is some absolute constant.*

Proof We compute $A=\mathrm{FT}_G(a)$ and $B=\mathrm{FT}_G(b)$ as in Section 6.3. We then compute $C=AB$ in $\mathrm{Hom}(\hat{G},\mathbf{K}^*)$ at the expense of $\mathfrak{o}$ multiplications in $\mathbf{K}$. We then deduce $c=ab$ applying FT_G^{-1} to C. The cost of this computation is bounded using Proposition 12. □

We now consider the case when $\mathbf{K}$ is $\mathbf{Z}/p\mathbf{Z}$ where p is a prime integer. We miss roots of unity in $\mathbf{K}$ in general. So we transport the problem into another ring using non-algebraic maps. We let t be the smallest power of 2 that is bigger than $3e-3$. Let p' be the smallest prime integer congruent to 1 modulo $\mathfrak{o}.(p-1)^2.t$. We set $\mathbf{K}'=\mathbf{Z}/p'\mathbf{Z}$ and note that $\mathbf{K}'$ contains a primitive root of unity of order e and a primitive root of order a power of two bigger than $3e-3$. Also

$$p'>\mathfrak{o}.(p-1)^2.$$

By a result of Heath-Brown, the exponent in Linnik's theorem for primes in arithmetic progressions can be taken to be $11/2$. See [19] and the recent improvement [52]. We deduce that there exists an absolute constant $\mathcal{Q}$ such that

$$p'\leqslant\mathcal{Q}(\mathfrak{o}.p)^{11}.$$

For c a congruence class in $\mathbf{K}=\mathbf{Z}/p\mathbf{Z}$ we denote $\ell(c)$ the lift of c, that is the unique integer in the intersection of c with the interval $[0,p[$. We write

$$\uparrow(c)=\ell(c)\bmod p'. \tag{13}$$

We thus define maps $\ell:\mathbf{K}\to\mathbf{Z}$ and $\uparrow:\mathbf{K}\to\mathbf{K}'$. We similarly define the lifting map $\ell':\mathbf{K}'\to\mathbf{Z}$ and $\downarrow:\mathbf{K}'\to\mathbf{K}$ by

$$\downarrow(c)=\ell'(c)\bmod p \quad\text{for}\quad c\in\mathbf{K}'. \tag{14}$$

These four maps can be extended to the corresponding group algebras by coefficientwise application. Given a and b as in Equation (12) we define

$$A = \ell(a) = \sum_{\sigma\in G} \ell(a_\sigma)\sigma \quad \text{and} \quad B = \ell(b) = \sum_{\sigma\in G} \ell(b_\sigma)\sigma \ \text{ in } \ \mathbf{Z}[G] \quad \text{and} \quad C = AB.$$

The coefficients in C belong to the interval $[0, \mathfrak{o}.(p-1)^2[$. So

$$C = \ell'((A \mod p') \times (B \mod p')) \quad \text{and} \quad ab = \downarrow(\uparrow(a)\uparrow(b)).$$

Using Proposition 13 we deduce

Proposition 14. *There exists an absolute constant $\mathcal{Q}$ such that the following is true. Let G, $\mathfrak{o}$, e be as in Section 6.3. Let $\mathbf{K} = \mathbf{Z}/p\mathbf{Z}$. There exists a prime integer $p' \leqslant \mathcal{Q}(\mathfrak{o}.p)^{11}$ and a straight-line program of length smaller than $\mathcal{Q}.\mathfrak{o}.\log\mathfrak{o}$ that computes the product $c = \sum_g c_g[g]$ of two elements $a = \sum_g a_g[g]$ and $b = \sum_g b_g[g]$ in $\mathbf{K}[G]$ given by their coefficients $(a_g)_g$ and $(b_g)_g$. The operations in this straigth line program are additions and multiplications in $(\mathbf{Z}/p'\mathbf{Z})$ and evaluations of the maps $\uparrow$ and $\downarrow$ defined in Equations (13) and (14).*

Now let $\mathbf{L}$ be a field extension of degree d of $\mathbf{K} = \mathbf{Z}/p\mathbf{Z}$. We assume that elements in $\mathbf{L}$ are represented by their coordinates in some $\mathbf{K}$-basis of $\mathbf{L}$. Work by Shparlinsky, Tsfasmann, Vladut [45], Shokrollahi [44], Ballet and Rolland [3, 4], Chaumine [9], Randriambololona [37] and others imply that the $\mathbf{K}$-bilinear complexity of $\mathbf{L}$ is bounded by an absolute constant times d. We deduce the following proposition.

Proposition 15. *There exists an absolute constant $\mathcal{Q}$ such that the following is true. Let G, $\mathfrak{o}$, e be as in Section 6.3. Let $\mathbf{K} = \mathbf{Z}/p\mathbf{Z}$ and $\mathbf{L}$ a field extension of degree d of $\mathbf{K}$. There exists a prime integer $p' \leqslant \mathcal{Q}(\mathfrak{o}.p)^{11}$ and a straight-line program of length $\leqslant \mathcal{Q}(d.\mathfrak{o}.\log\mathfrak{o} + d^2.\mathfrak{o})$ that computes the product $c = \sum_g c_g[g]$ of two elements $a = \sum_g a_g[g]$ and $b = \sum_g b_g[g]$ in $\mathbf{L}[G]$ given by their coefficients $(a_g)_g$ and $(b_g)_g$. The operations in this straigth line program are additions and multiplications in $(\mathbf{Z}/p\mathbf{Z})$ and in $(\mathbf{Z}/p'\mathbf{Z})$ and evaluations of the maps $\uparrow$ and $\downarrow$ defined in Equations (13) and (14).*

7. Constructing functions in the Hilbert class field

We have defined in Section 4 matrices $\mathcal{E}$, $\mathcal{C}$ and $\mathcal{I}$ for the evaluation and interpolation of global sections of a G-equivariant invertible sheaf on a curve Y. We have seen in Sections 4, 5, and 6 how to efficiently compute with these matrices. In this section we address the problem of computing these matrices.

We recall in Section 7.1 the necessary background from class field theory of function fields over a finite field. We illustrate the constructive aspects of class fields on a small example in section 7.2. An important feature of this method is that we only work with divisors and functions on X. This is of some importance since in the applications presented in Sections 8 and 9 the genus of Y is much larger (e.g. exponentially) than the genus of X.

7.1. **Class field theory and the jacobian variety.** We start from a projective curve X over a finite field $\mathbf{K}$ of characteristic p. We assume that X is smooth and absolutely integral. We let $\bar{\mathbf{K}}$ be an algebraic closure of $\mathbf{K}$. We need an abelian cover $\tau : Y \to X$ over $\mathbf{K}$, with Y absolutely integral. We will require that Y have a $\mathbf{K}$-rational point Q_1. This implies that τ is completely split above $P_1 = \tau(Q_1)$.

According to class field theory [42, 38] there is a maximal abelian unramified cover of X over $\mathbf{K}$ that splits totally above P_1. We briefly recall its geometric construction. Let J_X be the jacobian variety of X and let

$$j_X : X \to J_X$$

be the Jacobi map with origin P_1. Let

$$F_{\mathbf{K}} : J_X \to J_X$$

be the Frobenius endomorphism of degree $|\mathbf{K}|$, the cardinality of $\mathbf{K}$. The endomorphism

$$\wp = F_{\mathbf{K}} - 1 : J_X \to J_X$$

is an unramified Galois cover between $\mathbf{K}$-varieties with Galois group $J_X(\mathbf{K})$. We denote

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

the pullback of $\wp$ along j_X. This is the maximal abelian unramified cover of X that splits totally above P_1. Any such cover $\tau : Y \to X$ is thus a quotient of $\tau_{\max}$ by some subgroup H of $J_X(\mathbf{K})$. We set $G = J_X(\mathbf{K})/H$ and notice that G is at the same time the fiber of τ above P_1 and its Galois group, acting by translations in J_X/H.

$$\begin{array}{ccccc}
J_X(\mathbf{K}) & \hookrightarrow & Y_{\max} & \hookrightarrow & J_X \\
\downarrow & & \downarrow & & \downarrow H \\
G = J_X(\mathbf{K})/H & \hookrightarrow & Y & \hookrightarrow & J_X/H \\
\downarrow & & \downarrow \tau & & \downarrow G \\
0 = P_1 & \hookrightarrow & X & \hookrightarrow & J_X
\end{array} \qquad \wp$$

Let P be a $\mathbf{K}$-rational point on X and let $Q_{\max}$ be any point on $Y_{\max}(\bar{\mathbf{K}})$ such that

$$\tau_{\max}(Q_{\max}) = \wp(Q_{\max}) = P.$$

We have $F_{\mathbf{K}}(Q_{\max}) = Q_{\max} + P$. So the Artin map and the Jacobi map coincide, and the decomposition group of any place on Y above P is the subgroup in G/H generated by P itself. In particular the fiber of τ above P splits over $\mathbf{K}$ if and only if P is sent into H by the Jacobi map. Equivalently the class of $P - P_1$ belongs to H.

7.2. **An example.** In this section $\mathbf{K}$ is the field with three elements and X is the plane projective curve with homogeneous equation

$$Y^2Z^3 = X(X - Z)(X^3 + X^2Z + 2Z^3).$$

This is a smooth absolutely integral curve of genus 2. The characteristic polynomial of the Frobenius of $X/\mathbf{K}$ is

$$\chi_{\mathbf{K}}(t) = t^4 + t^3 + 2t^2 + 3t + 9. \tag{15}$$

The characteristic polynomial of the Frobenius of a curve over a finite field (given by a reasonable model) can be computed in time polynomial in $p.g.n$ where p is the characteristic of the field, n its degree over the prime field, and g the genus of the curve, using the so called p-adic methods introduced by Kato-Lubkin [25], Satoh [39], Mestre [31], Kedlaya [26], Lauder and Wan [29] and widely extended since then.

When the genus of the curve is fixed, the characteristic polynomial of the Frobenius can be computed in time polynomial in the logarithm of the cardinality of $\mathbf{K}$, using the ℓ-adic method introduced by Schoof [41] and generalized by Pila [33].

We deduce from Equation (15) that the jacobian variety J_X of X has

$$\chi_{\mathbf{K}}(1) = 16$$

rational points. There are 5 places of degree 1 on X. We call P_1 the unique place at $(0,1,0)$ and let

$$P_2 = (0,0,1),\ P_3 = (1,0,1),\ P_4 = (2,2,1),\ P_5 = (2,1,1).$$

The Picard group $J_X(\mathbf{K})$ is the direct sum of a subgroup of order 8 generated by the class of $P_4 - P_1$ and a subgroup of order 2 generated by $P_2 - P_1$. The class of $4(P_4 - P_1)$ is the class of $P_3 - P_1$. The classes of $P_2 - P_1$ and $P_3 - P_1$ generate a subgroup H of $\mathrm{Pic}^0(X)$ isomorphic to $(\mathbf{Z}/2\mathbf{Z})^2$. The quotient group

$$G = J_X(\mathbf{K})/H = \mathrm{Pic}^0(X)/H$$

is cyclic of order 4 generated by $P_4 - P_1$. So the subcover $\tau : Y \to X$ of $Y_{\max}$ associated with H is cyclic of order 4. And the fibers above P_1, P_2, and P_3 in this cover all split over $\mathbf{K}$. We will work with this cover.

According to Kummer theory, there is a duality (as group schemes) between the prime to p part of $\mathrm{Pic}^0(X)$ and the étale part of the kernel of $F_{\mathbf{K}} - p$. Associated to the quotient $G = \mathrm{Pic}^0(X)/H$ there must be a subgroup scheme isomorphic to μ_4 inside the latter kernel.

We let ζ be a primitive fourth root of unity in $\bar{\mathbf{K}}$ and denote $\mathbf{L}$ the degree two extension of $\mathbf{K}$ generated by ζ. In order to find the group of order 4 we are interested in, we use algorithms to compute the kernels of $F_{\mathbf{K}} - 1$ and $F_{\mathbf{K}} - p$ described in [13, Chapter 13]. The idea is to pick random elements in $J_X(\mathbf{L})$ and project them onto the relevant characteristic subspaces for the action of $F_{\mathbf{K}}$, using our knowledge of the characteristic polynomial $\chi_{\mathbf{K}}$. We set

$$P_6 = (2\zeta, 2) \quad \text{and} \quad \Gamma = 2(P_6 - P_4)$$

and find that the class γ of Γ is of order 4 and satisfies

$$F_{\mathbf{K}}(\gamma) = 3\gamma.$$

Thus γ generates the group we were looking for. There is a unique function R in $\mathbf{L}(X)$ with divisor 4Γ and taking value 1 at P_1. The cover $\tau : Y \to X$ we are interested in is obtained by

adding a 4-th root r of R to $\mathbf{L}(X)$. To be quite precise this construction produces the base change to $\mathbf{L}$ of the cover we are interested in. This will be fine for our purpose. So we let

$$r = R^{1/4}$$

be the 4-th root of R taking value 1 at Q_1. Equivalently we define Q_1 to be the point over P_1 where r takes the value 1. With the notation of Section 4.3 we take

$$D = 2P_5 \quad \text{and} \quad P = P_1 + P_2 + P_3.$$

We call E the pullback of D by τ and Q the pullback of P. We expect

$$\mathcal{L}(E) = H^0(Y, \mathcal{O}_Y(E))$$

to be a free $\mathbf{K}[G]$-module of rank

$$\deg(D) - g_X + 1 = 1.$$

This will be confirmed by our computations. Because the fibers above P_1, P_2 and P_3 all split over $\mathbf{K}$, the evaluation map $\mathcal{L}(E) \to \mathbf{A}$ is described by a 3×1 matrix with coefficients in $\mathbf{K}[G]$.

For every $2 \leqslant i \leqslant 3$ we choose a 4-th root of $R(P_i)$ in $\mathbf{L}$. This amounts to choosing a point $Q_{i,1}$ in the fiber of τ above P_i. We call σ the unique element in G that sends r to $\zeta.r$ so

$$G \ni \sigma : r \mapsto \zeta.r.$$

The $\mathbf{K}$-vector space $\mathcal{L}(E)$ decomposes over $\mathbf{L}$ as a sum of four eigenspaces associated to the four eigenvalues 1, ζ, $\zeta^2 = -1$, $\zeta^3 = -\zeta$ of σ. Let $0 \leqslant j \leqslant 3$ and let f be an eigenfunction in $\mathcal{L}(E)$ associated with the eigenvalue ζ^j. Then the quotient f/r^j is invariant by G and its divisor satisfies

$$(f/r^j) \geqslant -E - j.(r) = -E - j.\tau^*(\Gamma).$$

So f/r^j can be seen as a function on X with divisor bigger than or equal to $-D - j\Gamma$. The eigenspace $\mathcal{L}(E)_j$ associated to ζ^j is thus obtained as the image of the map

$$\begin{aligned} H^0(X, \mathcal{O}_X(D + j\Gamma)) &\longrightarrow \mathcal{L}(E)_j \\ F &\longmapsto f = Fr^j \end{aligned}$$

Evaluating f at $Q_{i,1}$ for $1 \leqslant i \leqslant 3$ then reduces to evaluating $F = f/r^j$ at P_i and multiplying the result by the chosen 4-th root of $R(P_i)$, raised to the power j.

This remark enables us to compute a $\mathbf{K}$-basis of $\mathcal{L}(E)$ consisting of eigenfunctions of σ and to evaluate the functions in this basis at the $(Q_{i,1})_{1 \leqslant i \leqslant 3}$ without ever writing equations for Y. We only need to compute the Riemann-Roch spaces associated to the divisors $D + j\Gamma$ on X for $0 \leqslant j \leqslant 3$. The Riemann-Roch space of a divisor $D = D_+ - D_-$ on a curve X is computed in time polynomial in the genus of X and the degrees of the positive and negative parts D_+ and D_- of D, using Brill-Noether algorithm and its many variants. See [21, 50, 20] and the most efficient general algorithm due to Makdisi [27, 28]. In case the exponent of G is large, we may have to compute linear spaces like $H^0(X, \mathcal{O}_X(D + j\Gamma))$ for large j. In that case, one should use the method introduced by Menezes, Okamoto, and Vanstone [30] in the context of pairing computation, in order to replace j by its logarithm in the complexity.

Passing from the values of the eigenfunctions to the evaluation matrix $\mathcal{E}$ reduces to applying an inverse Fourier transform. We find

$$\mathcal{E} = \begin{pmatrix} 1 \\ e_{1,2} \\ e_{1,3} \end{pmatrix} \quad \text{with} \quad e_{1,1} = 1,\ e_{1,2} = 1 + 2\sigma + 2\sigma^2 + 2\sigma^3,\ e_{1,3} = 2 + 2\sigma + 2\sigma^2 + \sigma^3.$$

Having a unit for $e_{1,1}$ is quite convenient. In general one says that $\mathcal{E}$ is systematic when the top square submatrix is the identity. This is possible when the first points $Q_{i,1}$ form a basis for the dual of $\mathcal{L}(E)$. This situation is generic in some sense but not granted. From a systematic matrix $\mathcal{E}$ it is trivial to deduce the associated checking and interpolation matrices

$$\mathcal{C} = \begin{pmatrix} e_{1,2} & e_{1,3} \\ -1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{and} \quad \mathcal{I} = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}.$$

8. Interpolation on algebraic curves

In this section we recall two classical applications of interpolation on algebraic curves over finite fields and illustrate the benefit of $\mathbf{K}[G]$-module structures in this context. Section 8.1 is concerned with the multiplication tensor in finite fields. In Sections 8.2 and 8.3 we see that geometric codes associated to G-equivariant divisors can be encoded in quasi-linear time and decoded in quasi-quadratic time if G is abelian, acts freely, and is big enough.

8.1. The complexity of multiplication in finite fields.

The idea of using Lagrange interpolation over an algebraic curve to multiply two elements in a finite field is due to Chudnovsky [10] and has been developped by Shparlinski, Tsfasmann and Vladut [45], Ballet and Rolland [3], Chaumine [9], Randriambololona [37] and others.

Let $\mathbf{K}$ be a finite field and let $\mathfrak{o} \geqslant 2$ be an integer. Let Y be a smooth, projective, absolutely integral curve over $\mathbf{K}$ and B an irreducible divisor of degree $\mathfrak{o}$ on Y. We call $\mathbf{L} = H^0(B, \mathcal{O}_B)$ the residue field at B. We choose a divisor E disjoint from B and assume that the evaluation map

$$e_B : H^0(Y, \mathcal{O}_Y(E)) \to \mathbf{L}$$

is surjective so that elements in $\mathbf{L}$ can be represented by functions in $H^0(Y, \mathcal{O}_Y(E))$. The latter functions will be characterized by their values at a collection $(Q_i)_{1 \leqslant i \leqslant N}$ of $\mathbf{K}$-rational points on Y. We denote

$$e_Q : H^0(Y, \mathcal{O}_Y(2E)) \to \mathbf{K}^N$$

the evaluation map at these points which we assume to be injective. The multiplication of two elements $e_B(f_1)$ and $e_B(f_2)$ in $\mathbf{K}$ can be achieved by evaluating f_1 and f_2 at the Q_i, then multiplying each $f_1(Q_i)$ by the corresponding $f_2(Q_i)$, then finding the unique function f_3 in $H^0(Y, \mathcal{O}_Y(2E))$ taking value $f_1(Q_i)f_2(Q_i)$ at Q_i, then computing $e_B(f_3)$. The number of bilinear multiplications in $\mathbf{K}$ in the whole process is equal to N.

This method uses curves over $\mathbf{K}$ with arbitrarily large genus having a number of $\mathbf{K}$-points bigger than some positive constant times their genus. It bounds the $\mathbf{K}$-bilinear complexity of multiplication in $\mathbf{L}$ by an absolute constant times the degree $\mathfrak{o}$ of $\mathbf{L}$ over $\mathbf{K}$, but it says little

abound the linear part of the algorithm : evaluation of the maps e_B and e_Q and their right (resp. left) inverses.

Now assume that the group of $\mathbf{K}$-automorphisms of Y contains a cyclic subgroup G of order $\mathfrak{o}$ acting freely on Y. We call $\tau : Y \to X$ the quotient by G map. Assume that B is the fiber of τ above some rational point a on X. Assume that E (resp. Q) is the pullback by τ of a divisor D (resp. P) on X. Under mild conditions, all the linear spaces above become free $\mathbf{K}[G]$-modules and the evaluation maps are G-equivariant. A computational consequence is that the linear part in the Chudnovsky algorithm becomes quasi-linear in the degree $\mathfrak{o}$ of the extension $\mathbf{L}/\mathbf{K}$. This remark has been exploited in [11] to bound the complexity of multiplication of two elements in a finite field given by their coordinates in a normal basis. The decompositions of the multiplication tensor that are proven to exist in [11] can be actually computed using the techniques presented in Section 7.

8.2. **Geometric codes.** The construction of error correcting codes by evaluating functions on algebraic curves of higher genus is due to Goppa [15, 16]. Let Y be a smooth, projective, absolutely integral curve over a finite field $\mathbf{K}$ of characteristic p. Let d be the degree of $\mathbf{K}$ over the prime field $\mathbf{Z}/p\mathbf{Z}$. Let g_Y be the genus of Y. Let $Q_1, \ldots, Q_N$ be pairwise distinct $\mathbf{K}$-rational points on Y. Let t_i be a uniformizing parameter at Q_i. Let E be a divisor that is disjoint from $Q = Q_1 + \cdots + Q_N$. Assume that

$$2g_Y - 1 \leqslant \deg(E) \leqslant \deg(Q) - 1. \tag{16}$$

Let

$$\mathbf{A} = H^0(Q, \mathcal{O}_Q) = H^0(Y, \mathcal{O}_Y/\mathcal{O}_Y(-Q)) \simeq \mathbf{K}^N$$

be the residue algebra at Q. Let

$$\hat{\mathbf{A}} = H^0(Y, \Omega^1_{Y/\mathbf{K}}(-Q)/\Omega^1_{Y/\mathbf{K}}) \simeq \bigoplus_{i=1}^{N} \mathbf{K}\frac{dt_i}{t_i} \simeq \mathbf{K}^N$$

be the dual of $\mathbf{A}$. Evaluation at the Q_i defines an injective linear map

$$\mathcal{L}(E) = H^0(Y, \mathcal{O}_Y(E)) \to \mathbf{A}.$$

We similarly define an injective linear map

$$\Omega(-Q + E) = H^0(Y, \Omega_{Y/\mathbf{K}}(-Q + E)) \to \hat{\mathbf{A}}.$$

The two vector subspaces $\mathcal{L}(E)$ and $\Omega(-Q + E)$ are orthogonal to each other. They can be considered as linear codes over $\mathbf{K}$ and denoted $C_{\mathcal{L}}$ and C_Ω respectively. The code $C_{\mathcal{L}}$ has length N, dimension

$$K = \deg(E) - g_Y + 1$$

and minimum distance greater than or equal to $N - \deg(E)$. Given a basis of $\mathcal{L}(E)$ one defines the generating matrix $\mathcal{E}_E$ of the code $C_{\mathcal{L}}$ to be the $N \times K$-matrix of the injection $\mathcal{L}(E) \to \mathbf{A} = \mathbf{K}^N$. One similarly defines the parity-check matrix $\mathcal{C}_E$ to be the $N \times (N - K)$-matrix of $\Omega(-Q + E) \to \hat{\mathbf{A}}$. We finally call $\mathcal{I}_E$ the $K \times N$-matrix of some projection of $\mathbf{A}$ onto $C_{\mathcal{L}}$. A message of length K is encoded by multiplying the corresponding column on the left by $\mathcal{E}_E$. The received word is checked by multiplying it on the left by the transpose of $\mathcal{C}_E$. And the initial message is recovered

from a correct codeword applying the interpolation matrix $\mathcal{I}_E$. In full generality, coding, testing and interpolating respectively require $2NK$, $2N(N-K)$ and $2KN$ operations in $\mathbf{K}$.

Assume now that the group of $\mathbf{K}$-automorphisms of Y contains a finite commutative subgroup G of order $\mathfrak{o}$ acting freely on Y. Let $\tau : Y \to X$ be the quotient by G map. Assume that $\mathfrak{o}$ divides N and let

$$n = N/\mathfrak{o}.$$

Assume that Q is the pullback by τ of a divisor

$$P = P_1 + \cdots + P_n$$

on X. Assume that E is the pullback of some divisor D on X. We are thus in the situation of Section 4. The code $C_{\mathcal{L}}$ is a free $\mathbf{K}[G]$-submodule of $\mathbf{A}$ of rank

$$k = K/\mathfrak{o}$$

and $\mathcal{C}_\Omega$ is its orthogonal module for the $\mathbf{K}[G]$-bilinear form defined in Section 3.3.

The matrices $\mathcal{E}_E$, $\mathcal{C}_E$, and $\mathcal{I}_E$ can be seen as matrices with coefficients in $\mathbf{K}[G]$ of respective sizes $n \times k$, $n \times (n-k)$, and $k \times n$. Coding now requires $2nk$ operations in $\mathbf{K}[G]$ rather than $2NK$ operations in $\mathbf{K}$. According to Proposition 15, each such operation requires less than $\mathcal{Q}.d^2.\mathfrak{o}.\log\mathfrak{o}$ operations in $\mathbf{Z}/p\mathbf{Z}$ and $\mathbf{Z}/p'\mathbf{Z}$ where $p' \leqslant \mathcal{Q}.(\mathfrak{o}.p)^{11}$ for some absolute constant $\mathcal{Q}$. The total cost of coding is thus bounded by a constant times

$$\frac{NK}{\mathfrak{o}^2}.d^2.\mathfrak{o}.\log\mathfrak{o}(\log p + \log\mathfrak{o})$$

elementary operations. Assuming that

(17) $\log\mathfrak{o}$ is bigger than a positive constant times $k\log p$

we bound the encoding complexity by a constant times

$$N(\log N)^3 d^2$$

elementary operations, where d is the degree of $\mathbf{K}$ over the prime field $\mathbf{Z}/p\mathbf{Z}$ and N is the length of the code. We obtain the same complexity estimate for parity-checking and interpolating.

8.3. **Basic decoding.** In the situation of the beginning of Section 8.2 we assume that we have received a message r in $\mathbf{A} = \mathbf{K}^N$. Let c be the closest codeword to r in $C_{\mathcal{L}}$ for the Hamming distance in $\mathbf{K}^N$. Write

$$r = c + \epsilon$$

and call ϵ the error vector. Let f be the unique function in $\mathcal{L}(E)$ such that $f = c \bmod Q$. The support of the error vector ϵ is the effective divisor $\mathrm{Supp}(\epsilon)$ consisting of all points Q_i where ϵ is not-zero. The degree of $\mathrm{Supp}(\epsilon)$ is the number of errors in r.

The principle of the basic decoding algorithm [23, 46] is : if a_0 is a small degree function vanishing at every point in the support $\mathrm{Supp}(\epsilon)$ then $a_0 r = a_0 c \mod Q$ is the residue modulo Q of an algebraic function $a_0 f$ of not too large degree. This function can be recovered from its values at Q if N is large enough. More concretely we let E_0 be some auxiliary divisor on Y with degree at least g_Y and set

$$E_1 = E + E_0.$$

We call $\mathcal{P}$ the subspace of $\mathcal{L}(E_0)$ consisting of all a_0 such that there exists a_1 in $\mathcal{L}(E_1)$ with $a_0 r = a_1 \bmod Q$. Non-zero elements in $\mathcal{P}$ are denominators for r in the sense of Section 5. We just saw that every function in $\mathcal{L}(E_0)$ vanishing at every point in the support of ϵ belongs to $\mathcal{P}$.

Conversely if a_0 is in $\mathcal{P}$ then $a_0 r$ belongs to $\mathcal{L}(E_1)$ modulo Q. But $a_0 c$ belongs to $\mathcal{L}(E_1)$ modulo Q also because a_0 is in $\mathcal{L}(E_0)$ modulo Q and c is in $\mathcal{L}(E)$ modulo Q. So $a_0(r-c) = a_0\epsilon$ belongs to $\mathcal{L}(E_1)$ modulo Q. There is a function in $\mathcal{L}(E_1)$ that is $a_0\epsilon$ modulo Q. This function has $N - \deg(\mathrm{Supp}(\epsilon))$ zeros and degree $\leqslant \deg(E_1) = \deg(E) + \deg(E_0)$. If we assume that

$$\deg(\mathrm{Supp}(\epsilon)) \leqslant N - 1 - \deg(E) - \deg(E_0) \tag{18}$$

then the latter function must be zero. So a_0 vanishes at $\mathrm{Supp}(\epsilon)$. Assuming Equation (18) we thus have $\mathcal{P} = \mathcal{L}(E_0 - \mathrm{Supp}(\epsilon))$. Assuming further that

$$\deg(\mathrm{Supp}(\epsilon)) \leqslant \deg(E_0) - g \tag{19}$$

this space is non-zero. Computing it is a matter of linear algebra and requires a constant times N^3 operations in $\mathbf{K}$. Given any non-zero element a_0 in $\mathcal{P}$ we denote A_0 the divisor consisting of all Q_i where a_0 vanishes. The degree of A_0 is bounded by $\deg E_0$. The error ϵ is an element in $\mathbf{A}$ with support contained in A_0 and such that $r - \epsilon$ belongs to $C_{\mathcal{L}}$. Finding ϵ is a linear problem in $\leqslant \deg E_0$ unknows and $N - \deg(E) + g_Y - 1$ equations. The solution is unique because the difference of two solutions is in $C_{\mathcal{L}}$ and has at least $N - \deg(E_0)$ zeros. And this is strictly greater than $\deg(E)$ by Equation (18).

Combining Equations (18) and (19) we see that the basic decoding algorithm corrects up to d_{basic} errors where

$$d_{\mathrm{basic}} = \frac{N - \deg(E) - 1 - g_Y}{2}. \tag{20}$$

Assume now that the group of $\mathbf{K}$-automorphisms of Y contains a finite commutative subgroup G of order $\mathfrak{o}$ acting freely on Y. Let $\tau : Y \to X$ be the quotient by G map. Assume that $\mathfrak{o}$ divides N and let $n = N/\mathfrak{o}$. Assume that Q is the pullback by τ of a divisor

$$P = P_1 + \cdots + P_n$$

on X. Assume that E is the pullback of some divisor D on X. Assume that E_0 is the pullback of some divisor D_0 on X. Assume that $\mathcal{L}(E_0)$ contains a free $\mathbf{K}[G]$-module of rank $\deg(D_0) - g_X + 1$. According to Proposition 6, such an E_0 exists if the order $\mathfrak{o}$ of G is prime to p. According to Proposition 7, such an E_0 exists if the order $\mathfrak{o}$ of G is a power of p, and the cardinality q of $\mathbf{K}$ is at least 4, and the genus of X is at least 2. Another sufficient condition if that $\deg(D_0) \geqslant 2g_X - 1$. According to Proposition 10 we can find a denominator a_0 at the expense of $\mathcal{Q}.(\mathfrak{o}.n.\log(\mathfrak{o}.n))^2$ operations in $\mathbf{K}$ and $\mathcal{Q}.\mathfrak{o}.n^3\log(\mathfrak{o}.n)$ operations in $\mathbf{K}[G]$. According to Proposition 15, each operation in $\mathbf{K}[G]$ requires less than

$$\mathcal{Q}.d^2.\mathfrak{o}.\log\mathfrak{o}(\log p + \log\mathfrak{o})$$

elementary operations. The total cost of finding a denominator is thus bounded by a constant times

$$N^2.n.d^2.\log^3(\mathfrak{o}.n.p)$$

elementary operation. Assuming Condition (17) and

$$\log \mathfrak{o} \quad \text{is bigger than a positive constant times} \quad n - \log n$$

we obtain a complexity of a constant times

$$N^2 (\log N)^4 d^2$$

elementary operations where d is the degree of $\mathbf{K}$ over the prime field $\mathbf{Z}/p\mathbf{Z}$ and N is the length of the code. Once obtained a denominator, the error can be found at the same cost.

9. Good geometric codes with quasi-linear encoding

In this section we specialize the constructions presented in Sections 8.2 and 8.3 using curves with many points and their Hilbert class fields. We quickly review in Section 9.1 some standard useful results and observations which we apply in Section 9.2 to the construction of families of good geometric codes having quasi-linear encoding and a quasi-quadratic decoder. Recall that a family of codes over a fixed alphabet is said to be good when the length tends to infinity while both the rate and the minimum distance have a strictly positive liminf.

9.1. Controling the class group and the Artin map.

We keep the notation in Section 7.1. In particular P_1 is a $\mathbf{K}$-rational point on X and

$$j_X : X \to J_X$$

is the Jacobi map with origin P_1. For the applications we have in mind we need some control on the $\mathbf{K}$-rational points on X, on the group $\mathrm{Pic}^0(X)$ and most importantly on the image of $X(\mathbf{K})$ in $\mathrm{Pic}^0(X)$ by the Jacobi map. A typical advantageous situation would be :

(1) X has enough $\mathbf{K}$-rational points, that is a fixed positive constant times its genus g_X,
(2) a fixed positive proportion of these points are mapped by j_X into a subgroup H,
(3) H is not too large i.e. the quotient $\log|H|/\log|\mathrm{Pic}^0(X)|$ is smaller than a fixed constant smaller than 1.

A range of geometric techniques relevant to that problem is presented in Serre's course [43] with the related motivation of constructing curves with many points. One says that (a family of) curves over a fixed finite field of cardinality q have many points when the ratio of the number of rational points by the genus tends to $\sqrt{q}-1$. Modular curves $X_0(N)$ have many points over finite fields with p^2 elements, corresponding to supersingular moduli, as was noticed by Ihara [22] and by Tzfasman, Vladut, and Zink [48]. These authors also find families of Shimura curves having many points over fields with cardinality a square. Garcia and Stichtenoth [14] construct for every square q an infinite tower of algebraic curves over $\mathbf{F}_q$ such that the quotient of the number of $\mathbf{F}_q$-points by the genus converges to $\sqrt{q}-1$, and the quotient of the genera of two consecutive curves converges to q.

As for conditions (2) and (3) above, it is noted in [43, 5.12.4] that the images by j_X of $P_2, \ldots, P_n$ generate a subgroup H with at most $n-1$ invariant factors. If the class group $J_X(\mathbf{K})$ has $I \geqslant n-1$ invariant factors then the size of the quotient G is bigger than or equal to the product of the $I-(n-1)$ smallest invariant factors of $J_X(\mathbf{K})$.

Another favourable situation exploited in [35, 32, 49, 18] is when $\mathbf{K}$ has a strict subfield $\mathbf{k}$ and X is defined over $\mathbf{k}$ and P_1 is $\mathbf{k}$-rational. Then the Jacobi map sends the points in $X(\mathbf{k})$ into the subgroup $J_X(\mathbf{k})$ of $J_X(\mathbf{K})$. We will use this remark in the next section.

9.2. **A construction.** Let $\mathbf{k}$ be a finite field with characteristic p. Let q be the cardinality of $\mathbf{k}$. We assume that q is a square. We consider a family of curves $(X_k)_{k\geqslant 1}$ over $\mathbf{k}$ having many points over $\mathbf{k}$. For example we may take X_k to be k-th curve in the Garcia-Stichtenoth tower associated with q. We denote g_X the genus of X_k. We omit the index k in the sequel because there is no risk of confusion. We denote n the number of $\mathbf{k}$-rational points on X. We denote these points $P_1, \ldots, P_n$ and let P be the effective divisor sum of all these points. We let $\mathbf{K}$ be a non-trivial extension of $\mathbf{k}$. We will assume that the degree of $\mathbf{K}$ over $\mathbf{k}$ is 2 because higher values seem to bring nothing but disadvantages. We denote T the quotient

$$T = J_X(\mathbf{K})/J_X(\mathbf{k}).$$

We denote T_p the p-Sylow subgroup of T. We denote $T_{p'}$ the complementary subgroup to T_p in T. We call G the bigger among T_p and $T_{p'}$. This is a quotient of T. We call H the kernel of the composite map $J_X(\mathbf{K}) \to T = J_X(\mathbf{K})/J_X(\mathbf{k}) \to G$. We let $\mathfrak{o}$ be the order of G. We note that

$$\#J_X(\mathbf{K})/J_X(\mathbf{k}) \geqslant (\sqrt{q}-1)^{2g_X} \quad \text{so} \quad \mathfrak{o} \geqslant \sqrt{\sharp T} \geqslant (\sqrt{q}-1)^{g_X}.$$

grows exponentially in g_X provided $q \geqslant 9$. And G is either a p-group or a p'-group. We find ourselves in the situation of Section 7.1. We call $Y_{\max}$ the maximal unramified cover of X over $\mathbf{K}$ which is totally decomposed over $\mathbf{K}$ above P_1. We call Y the quotient of $Y_{\max}$ by H. The fibers of

$$\tau : Y \to X$$

above the points $P_1, \ldots, P_n$ all split over $\mathbf{K}$. We call Q the pullback of P by τ. This is a divisor on Y of degree

$$N = \mathfrak{o}.n.$$

We choose a real number ϱ such that

$$0 < \varrho < \frac{\sqrt{q}}{2} - 2. \tag{21}$$

Our goal is to correct up to $\varrho.\mathfrak{o}.g_X$ errors. Let D be a divisor on X that is disjoint from P and such that

$$\deg(D) = \lceil (\sqrt{q} - 2 - 2\varrho) g_X \rfloor$$

the closest integer to $(\sqrt{q}-2-2\varrho)g_X$. Let E be the pullback of D by τ. We deduce from Equation (21) that condition (16) is met at least asymptotically. From X, Y, E, and Q the construction in Section 8.2 produces a code $C_{\mathcal{L}}$ over the field $\mathbf{K}$ with q^2 elements, having length

$$N = \mathfrak{o}.n \simeq (\sqrt{q}-1).\mathfrak{o}.g_X$$

and dimension

$$K = \mathfrak{o}.(\deg(D) - g_X + 1) \simeq (\sqrt{q} - 3 - 2\varrho).\mathfrak{o}.g_X.$$

The code $C_{\mathcal{L}}$ can be encoded and parity-checked in quasi-linear deterministic time in its length N. One can decode with the same complexity when there are no errors. Using the basic decoding algorithm as in Section 8.3 one can decode in the presence of errors in quasi-quadratic probabilistic (Las Vegas) time up to the distance

$$d_{\text{basic}} = \frac{N - \deg(E) - 1 - g_Y}{2} \simeq \varrho.\mathfrak{o}.g_X$$

defined by Equation (20). We denote δ_{basic} the relative distance d_{basic}/N. The existence of a divisor D_0 with all the properties required in Section 8.3 is granted because G is either a p-group or a p'-group. So we can apply Proposition 6 or Proposition 7 depending on the case.

Proposition 16. *Let p be a prime integer and let q be a power of p. Assume that q is a square and*

$$q \geqslant 25. \tag{22}$$

Let ϱ be a real such that

$$0 < \varrho < \frac{\sqrt{q}}{2} - 2. \tag{23}$$

The construction above produces a family of error correcting codes over the field with q^2 elements having length N tending to infinity and such that

1. *the codes can be encoded in quasi-linear time in their length,*
2. *the rate R satisfies*
$$\lim R = \frac{\sqrt{q} - 3 - 2\varrho}{\sqrt{q} - 1}$$
3. *the codes can be decoded in quasi-quadratic probabilistic (Las Vegas) time in N up to the relative distance δ_{basic} and*
$$\lim \delta_{\text{basic}} = \frac{\varrho}{\sqrt{q} - 1}.$$

We may want to use the general purpose algorithm of Beelen, Rosenkilde, Solomatov [5] to decode up to half the Goppa designed minimum distance. Inequalities (22) and (23) are then replaced by

$$q \geqslant 16 \quad \text{and} \quad 0 < \varrho < \frac{\sqrt{q} - 3}{2},$$

and the limit of the rate is now

$$\lim R = \frac{\sqrt{q} - 2 - 2\varrho}{\sqrt{q} - 1}.$$

However the complexity of decoding is then of order $\mu^{\omega-1}(N + g_Y)$ where N is the length of the code, μ is the gonality of Y, and ω is the exponent in the complexity of matrix multiplication. Curves with many points have large gonality. In particular $\mu \geqslant N/(q^2 + 1)$ in our situation, so that for fixed q, the complexity of this decoder is of order greater than N^ω. It is known [1] that $2 \leqslant \omega < 2.37286$ but it is not granted that $\omega = 2$.

Power decoding [40] seems attractive in the context of $\mathbf{K}[G]$-modules because of its purely linear nature. However the rigorous analysis of its performances is delicate in general [34] and

particularly here because we fix the base field, let the genus tend to infinity and use a rather rigid construction.

REFERENCES

[1] Josh Alman and Virginia Vassilevska Williams. A refined laser method and faster matrix multiplication. In Dániel Marx, editor, *Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms, SODA 2021, Virtual Conference, January 10 - 13, 2021*, pages 522–539. SIAM, 2021.

[2] S. Ballet and D. Le Brigand. On the existence of non-special divisors of degree g and $g-1$ in algebraic function fields over $\mathbb{F}_q$. *J. Number Theory*, 116(2):293–310, 2006.

[3] S. Ballet and R. Rolland. Multiplication algorithm in a finite field and tensor rank of the multiplication. *J. Algebra*, 272(1):173–185, 2004.

[4] Stéphane Ballet. Curves with many points and multiplication complexity in any extension of $\mathbf{F}_q$. *Finite Fields Appl.*, 5(4):364–377, 1999.

[5] Peter Beelen, Johan Rosenkilde, and Grigory Solomatov. Fast decoding of ag codes, 2022.

[6] Leo I. Bluestein. A linear filtering approach to the computation of discrete Fourier transform. *IEEE Transactions on Audio and Electroacoustics*, 18:451–455, 1970.

[7] Alin Bostan, Frédéric Chyzak, Marc Giusti, Romain Lebreton, Grégoire Lecerf, Bruno Salvy, and Éric Schost. Algorithmes efficaces en calcul formel, August 2017. 686 pages. Édition 1.0.

[8] N. Bourbaki. *Éléments de mathématique. Algèbre. Chapitre 8. Modules et anneaux semi-simples*. Springer, Berlin, 2012. Second revised edition of the 1958 edition.

[9] 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.

[10] D. V. Chudnovsky and G. V. Chudnovsky. Algebraic complexities and algebraic curves over finite fields. *J. Complexity*, 4(4):285–316, 1988.

[11] Jean-Marc Couveignes and Tony Ezome. The equivariant complexity of multiplication in finite field extensions. *J. Algebra*, 622:694–720, 2023.

[12] Charles W. Curtis and Irving Reiner. *Representation theory of finite groups and associative algebras*, volume Vol. XI of *Pure and Applied Mathematics*. Interscience Publishers, New York-London, 1962.

[13] Bas Edixhoven and Jean-Marc Couveignes, editors. *Computational aspects of modular forms and Galois representations*, volume 176 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2011.

[14] Arnaldo García and Henning Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound. *Invent. Math.*, 121(1):211–222, 1995.

[15] V. D. Goppa. Codes on algebraic curves. *Dokl. Akad. Nauk SSSR*, 259(6):1289–1290, 1981.

[16] V. D. Goppa. Algebraic-geometric codes. *Izv. Akad. Nauk SSSR Ser. Mat.*, 46(4):762–781, 896, 1982.

[17] V. D. Goppa. *Geometry and codes*, volume 24 of *Mathematics and its Applications (Soviet Series)*. Kluwer Academic Publishers Group, Dordrecht, 1988.

[18] Venkatesan Guruswami and Chaoping Xing. Optimal rate list decoding over bounded alphabets using algebraic-geometric codes. *J. ACM*, 69(2):Art. 10, 48, 2022.

[19] D. R. Heath-Brown. Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression. *Proc. London Math. Soc. (3)*, 64(2):265–338, 1992.

[20] F. Hess. Computing Riemann-Roch spaces in algebraic function fields and related topics. *J. Symbolic Comput.*, 33(4):425–445, 2002.

[21] Ming-Deh Huang and Doug Ierardi. Efficient algorithms for the Riemann-Roch problem and for addition in the Jacobian of a curve. *J. Symbolic Comput.*, 18(6):519–539, 1994.

[22] Yasutaka Ihara. Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 28(3):721–724 (1982), 1981.

[23] 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. Inform. Theory*, 35(4):811–821, 1989.

[24] Erich L. Kaltofen and B. David Saunders. On Wiedemann's method of solving sparse linear systems. In Harold F. Mattson, Teo Mora, and T. R. N. Rao, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 9th International Symposium, AAECC-9, New Orleans, LA, USA, October 7-11, 1991, Proceedings*, volume 539 of *Lecture Notes in Computer Science*, pages 29–38. Springer, 1991.
[25] Goro C. Kato and Saul Lubkin. Zeta matrices of elliptic curves. *J. Number Theory*, 15(3):318–330, 1982.
[26] Kiran S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.*, 16(4):323–338, 2001.
[27] Kamal Khuri-Makdisi. Linear algebra algorithms for divisors on an algebraic curve. *Math. Comp.*, 73(245):333–357, 2004.
[28] Kamal Khuri-Makdisi. Asymptotically fast group operations on Jacobians of general curves. *Math. Comp.*, 76(260):2213–2239, 2007.
[29] Alan G. B. Lauder and Daqing Wan. Counting points on varieties over finite fields of small characteristic. In *Algorithmic number theory: lattices, number fields, curves and cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, pages 579–612. Cambridge Univ. Press, Cambridge, 2008.
[30] Alfred J. Menezes, Tatsuaki Okamoto, and Scott A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Trans. Inform. Theory*, 39(5):1639–1646, 1993.
[31] J.-F. Mestre. Lettre adressée à Gaudry et Harley. `https://webusers.imj-prg.fr/~jean-francois.mestre/`, december 2010.
[32] Harald Niederreiter and Chaoping Xing. A general method of constructing global function fields with many rational places. In *Algorithmic number theory (Portland, OR, 1998)*, volume 1423 of *Lecture Notes in Comput. Sci.*, pages 555–566. Springer, Berlin, 1998.
[33] Jonathan S. Pila. *Frobenius maps of Abelian varieties and finding roots of unity in finite fields*. ProQuest LLC, Ann Arbor, MI, 1988. Thesis (Ph.D.)–Stanford University.
[34] Sven Puchinger, Johan Rosenkilde, and Irene Bouw. Improved power decoding of interleaved one-point Hermitian codes. *Des. Codes Cryptogr.*, 87(2-3):589–607, 2019.
[35] Heinz-Georg Quebbemann. Cyclotomic Goppa codes. *IEEE Trans. Inform. Theory*, 34(5):1317–1320, 1988. Coding techniques and coding theory.
[36] 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.
[37] Hugues Randriambololona. Bilinear complexity of algebras and the Chudnovsky-Chudnovsky interpolation method. *J. Complexity*, 28(4):489–517, 2012.
[38] Michael Rosen. The Hilbert class field in function fields. *Exposition. Math.*, 5(4):365–378, 1987.
[39] 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.
[40] Georg Schmidt, Vladimir R. Sidorenko, and Martin Bossert. Syndrome decoding of Reed-Solomon codes beyond half the minimum distance based on shift-register synthesis. *IEEE Trans. Inform. Theory*, 56(10):5245–5252, 2010.
[41] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, 44(170):483–494, 1985.
[42] Jean-Pierre Serre. *Algebraic groups and class fields*, volume 117 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1988.
[43] Jean-Pierre Serre. *Rational points on curves over finite fields*, volume 18 of *Documents Mathématiques (Paris)*. Société Mathématique de France, Paris, 2020. With contributions by Everett Howe, Joseph Oesterlé and Christophe Ritzenthaler.
[44] Mohammad Amin Shokrollahi. Optimal algorithms for multiplication in certain finite fields using elliptic curves. *SIAM J. Comput.*, 21(6):1193–1198, 1992.
[45] 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.

[46] Alexei N. Skorobogatov and Sergei G. Vlăduţ. On the decoding of algebraic-geometric codes. *IEEE Trans. Inform. Theory*, 36(5):1051–1060, 1990.
[47] M. A. Tsfasman and S. G. Vlăduţ. *Algebraic-geometric codes*, volume 58 of *Mathematics and its Applications (Soviet Series)*. Kluwer Academic Publishers Group, Dordrecht, 1991.
[48] M. A. Tsfasman, S. G. Vlăduţ, and Th. Zink. Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. *Math. Nachr.*, 109:21–28, 1982.
[49] Gerard van der Geer. Hunting for curves with many points. In *Coding and cryptology*, volume 5557 of *Lecture Notes in Comput. Sci.*, pages 82–96. Springer, Berlin, 2009.
[50] Emil J. Volcheck. Computing in the Jacobian of a plane algebraic curve. In *Algorithmic number theory (Ithaca, NY, 1994)*, volume 877 of *Lecture Notes in Comput. Sci.*, pages 221–233. Springer, Berlin, 1994.
[51] Douglas H. Wiedemann. Solving sparse linear equations over finite fields. *IEEE Trans. Inf. Theory*, 32(1):54–62, 1986.
[52] 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.

JEAN-MARC COUVEIGNES, UNIV. BORDEAUX, CNRS, INRIA, BORDEAUX-INP, IMB, UMR 5251, F-33400 TALENCE, FRANCE.
Email address: jean-marc.couveignes@u-bordeaux.fr

JEAN GASNIER, UNIV. BORDEAUX, CNRS, INRIA, BORDEAUX-INP, IMB, UMR 5251, F-33400 TALENCE, FRANCE.
Email address: jean.gasnier@u-bordeaux.fr