EVALUATION AND INTERPOLATION ON ALGEBRAIC CURVES

JEAN-MARC COUVEIGNES AND REYNALD LERCIER

CONTENTS

1. ACKNOWLEDGEMENTS

This text is concerned with some computational aspects of evaluating and interpolating in dimension one. We do not claim to be exhaustive. We have tried to illustrate the contribution to this topic of complexity theory, computer arithmetic, coding theory, commutative algebra, analytic and algebraic number theory, algebraic geometry. We have taken the liberty of reusing excerpts from articles written in collaboration with Tony Ezome, and Jean Gasnier. We also thank Joris Danneman and Lars Wagoner for inspiring discussions and relevant bibliographic suggestions. This is not a research article and most of the topics covered are very classical. This is not a survey paper either. We have selected and organized a few contributions so as to illustrate the role played by a few simple and natural ideas.

Warning : this text is in a very preliminary form. It has to be completed and some proofreading is evidently necessary. Please do not distribute this version.

Date: CAIPI seminar, June 2026.

2. INTRODUCTION

In this talk we are interested in the computational complexity of some basic problems in finite field arithmetics. These simple algebraic problems will range in two main classes: evaluation of a linear map, evaluation of a bilinear map.

Problem 1. *Let $\mathbf{K}$ be a finite field and let U and V be two vector spaces over $\mathbf{K}$. Let $a : U \to V$ be a linear map. On input $u \in U$, compute $a(u) \in V$.*

We assume that the input u is given by its coordinates in a fixed basis $\mathcal{U}$ of U. And the output $a(u)$ consists of the coordinates of $a(u)$ in a fixed basis $\mathcal{V}$ of V. The difficulty of this problem depends very much on the given map a and on the chosen bases.

Problem 2. *Let $\mathbf{K}$ be a finite field and let U, V, and W be three linear spaces over $\mathbf{K}$. Let $a : U \times V \to W$ be a bilinear map. On input $(u, v) \in U \times V$, compute $a(u, v) \in W$.*

Again we assume that three bases are given for U, V, and W respectively and we stress that here again the difficulty of the problem depends very much on the given map a and on the chosen bases. The three problems we shall mainly be interested in are evaluation, interpolation and multiplication. The first two problems are linear. We assume that we have a $\mathbf{K}$-linear space of functions U and a finite set of points $Q = \{Q_0, Q_1, \ldots, Q_{n-1}\}$ where functions can be evaluated. We assume that a basis $\mathcal{U}$ of U is fixed.

Problem 3 (Evaluation)**.** *Given a function f by its coordinates in $\mathcal{U}$, compute the $f(Q_i)$ for $0 \leqslant i \leqslant n-1$.*

Problem 4 (Interpolation)**.** *Given n scalars v_0, v_1, …, v_{n-1} in $\mathbf{K}$, compute the coordinates in $\mathcal{U}$ of a function f that takes value v_i at Q_i for every $0 \leqslant i \leqslant n-1$.*

For the interpolation problem, we will assume that the function f exists and is unique for every vector $(v_i)_{0 \leqslant i \leqslant n-1}$. In other words, the evaluation map is assumed to be a bijection. A typical example is when $U = \mathbf{K}[x]_{<n}$ the space of polynomials of degree $< n$ and the n evaluation points have their x coordinates that are n pairwise distinct scalars in $\mathbf{K}$.

To describe the third problem (multiplication) we assume that we are given a $\mathbf{K}$-algebra $\mathbf{L}$ and a $\mathbf{K}$-basis $\mathcal{B}$ of it.

Problem 5 (Multiplication)**.** *Given the coordinates in $\mathcal{B}$ of two elements f and g in the $\mathbf{K}$-algebra $\mathbf{L}$, compute the coordinates in $\mathcal{B}$ of the product $f.g$.*

This is a $\mathbf{K}$-bilinear problem. A typical example is when $\mathbf{L} = \mathbf{K}[x]$ and $\mathcal{B}$ is the monomial basis $1, x, x^2, x^3, \ldots$

We shall study the algorithmic complexity of evaluation, interpolation and multiplication. Our main concern will be to illustrate the role played by automorphisms and more precisely the algorithmic benefit of $\mathbf{K}[G]$-module structures.

3. STRAIGHT-LINE PROGRAMS

We need some complexity theory to evaluate the difficulty of the computational problems we are interested in. We shall use an elementary model of computation: straight line programs (SLP). We provide an example rather than a definition. See [3, Chapter 4] for a more formal study.

Let $(\mathbf{Z}, +, \times)$ be the ring of integers. Here is a straight line program that on input $(x, y) \in \mathbf{Z}^2$ computes $(2x - y, 2x + 3y)$. On each line, the expression in green gives the value assigned to the corresponding register.

$$\begin{array}{llll} X_{-1} & \leftarrow & x & x \\ X_0 & \leftarrow & y & y \\ X_1 & \leftarrow & 2 \bullet X_{-1} & 2x \\ X_2 & \leftarrow & (-1) \bullet X_0 & -y \\ X_3 & \leftarrow & X_1 + X_2 & 2x - y \\ X_4 & \leftarrow & 3 \bullet X_0 & 3y \\ X_5 & \leftarrow & X_1 + X_4 & 2x + 3y \end{array}$$

This straight line program consists of two input lines and five instructions: two additions and three scalar multiplications. No matter where the output appears: here in X_3 and X_5. To any linear map we can associate a straight line program that computes it using only additions and scalar multiplications.

There is **no branching** in a straight line program. Just a sequence of instructions. The **complexity** of a straight line program is the number of operations.

The complexity of a linear map is the minimum complexity of a straight line program computing it. The operations in such a SLP are additions $+$ and scalar multiplications $\bullet$. The latter are multiplications of a register by a constant in the base field $\mathbf{K}$.

Straight line programs can compute bilinear maps also. One then allows three operations: $+$, $\bullet$, and bilinear multiplications $\times$. The latter are multiplications of two registers.

Given a SLP computing a bilinear map, we define its complexity to be the total number of operations $+$, $\bullet$, and $\times$. We also can define its **bilinear complexity** to be the number of bilinear multiplications $\times$ only. The (bilinear) complexity of a bilinear map is the minimum (bilinear) complexity of a straight line program computing it. The bilinear complexity ignores the cost of linear maps (e.g. base change).

We thus have a sufficient complexity measure for evaluation and interpolation problems: counting $+$, $\bullet$. We also have two interesting complexity measures for multiplication problems: counting $+$, $\bullet$, and $\times$ or counting $\times$ only.

Any linear map $a : U \to V$ can be computed by a SLP using $\dim U \times \dim V$ scalar multiplications and $(\dim U - 1) \times \dim V$ additions. Any bilinear map $a : U \times V \to W$ can be computed by a SLP using $\dim U \times \dim V \times \dim W$ bilinear multiplications, $\dim U \times \dim V \times \dim W$ scalar multiplications, and $(\dim U \times \dim V - 1) \times \dim W$ additions. Indeed the corresponding SLP merely implement the standard methods for matrix multiplication.

4. Polynomials in one variable over a finite field

In this section we consider the simplest and most standard evaluation and interpolation problems: the case of polynomials in one variable. Let $n \geqslant 1$ be an integer and $\mathbf{K}$ a finite field and $U = \mathbf{K}[x]_{<n}$ and $\mathcal{U} = (1, x, x^2, \ldots, x^{n-1})$ the power basis of U and $V = \mathbf{K}^n$ and $\mathcal{V}$ its canonical basis. Let a_0, a_1, …, a_{n-1} be n pairwise distinct scalars in $\mathbf{K}$ and let $a : U \to V$ be the map $f \mapsto (f(a_i))_{0 \leqslant i \leqslant n-1}$. The matrix

$$A = (a_i^j)_{0 \leqslant i \leqslant n-1, 0 \leqslant j \leqslant n-1}$$

of a in the bases $\mathcal{U}$ and $\mathcal{V}$ is known to be a Vandermonde invertible matrix. The evaluation problem here is the problem of multiplying by A an input column vector

$$f_{\mathcal{B}} = \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_{n-1} \end{pmatrix}$$

of height n. The interpolation problem is the problem of multiplying by A^{-1} an input column vector

$$v = \begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_{n-1} \end{pmatrix}$$

of height n. An important naive remark: the vector $(f(a_i))_{0\leqslant i\leqslant n-1}$ is a linear expression in the coefficients of f but it is not at all linear in the evaluation points $(a_i)_{0\leqslant i\leqslant n-1}$. The evaluation problem we consider is for fixed $(a_i)_{0\leqslant i\leqslant n-1}$ to compute the map $f \mapsto (f(a_i))_{0\leqslant i\leqslant n-1}$.

4.1. **Butterflies.** It was first noticed by Gauss [18] and rediscovered by Cooley and Tukey [6] that the map $a : f \mapsto (f(a_i))_{0\leqslant i\leqslant n-1}$ can be evaluated quickly when

(1) the characteristic of $\mathbf{K}$ is not 2,
(2) $n = 2^\nu$ is a power of 2,
(3) the evaluation points are the set of n-th root of unity: $Q_i = \omega^i$ where ω is a primitive n-th root of unity in $\mathbf{K}$.

While Gauss and Cooley-Tukey were interested in calculation with complex numbers, we notice that for our purpose, the existence of a primitive n-th root of unity ω in the finite field $\mathbf{K}$ is equivalent to the cardinality of $\mathbf{K}$ being congruent to 1 modulo $n = 2^\nu$. This is a rather restrictive condition.

The key idea of Gauss-Cooley-Tukey is to use the involution $x \mapsto -x$ to decompose the polynomial to be evaluated $f(x) = \sum_{0\leqslant j\leqslant n-1} f_j\, x^j$ as a sum

$$f(x) = f^+(x) + f^-(x)$$

where

$$f^+(x) = \sum_{0\leqslant 2j\leqslant n-1} f_{2j}\, x^{2j} \quad \text{and} \quad f^-(x) = \sum_{0\leqslant 2j+1\leqslant n-1} f_{2j+1}\, x^{2j+1} = x \sum_{0\leqslant 2j+1\leqslant n-1} f_{2j+1}\, x^{2j}$$

are the even and odd parts of $f(x)$. Setting $y = x^2$ and

$$f^0(y) = \sum_{0\leqslant 2j\leqslant n-1} f_{2j}\, y^j \quad \text{and} \quad f^1(y) = x^{-1} f^-(x) = \sum_{0\leqslant 2j+1\leqslant n-1} f_{2j+1}\, y^j$$

we decompose

$$f(x) = f^0(y) + x f^1(y) \tag{1}$$

where f^0 and f^1 are polynomials of degree $\leqslant n/2 - 1$. This decomposition reduces the evaluation of $f(x)$ at the $(\omega^i)_{0\leqslant i\leqslant n-1}$ to two similar problems of halved size. Indeed we may define $\eta = \omega^2$ a primitive $2^{\nu-1}$ root of unity an notice that

$$f(\omega^j) = f^0(\eta^j) + \omega^j . f^1(\eta^j) \tag{2}$$

allowing a recursive approach that is classically illustrated using diagrams called butterflies (see Figure 1).

We denote by $T(\nu)$ the number of operations in $\mathbf{K}$ that are needed to evaluate a polynomial of degree $\leqslant 2^\nu - 1$ at all the 2^ν-th roots of unity. We just proved

$$T(\nu) \leqslant 2T(\nu - 1) + 2^{\nu+1}.$$

We deduce by induction that $T(\nu) \leqslant 2.\nu.2^\nu$ for every $\nu \geqslant 1$. Since $n = 2^\nu$ this gives a complexity of $2.n.\log_2 n$ operations in $\mathbf{K}$. This is much better than the general quadratic bound.

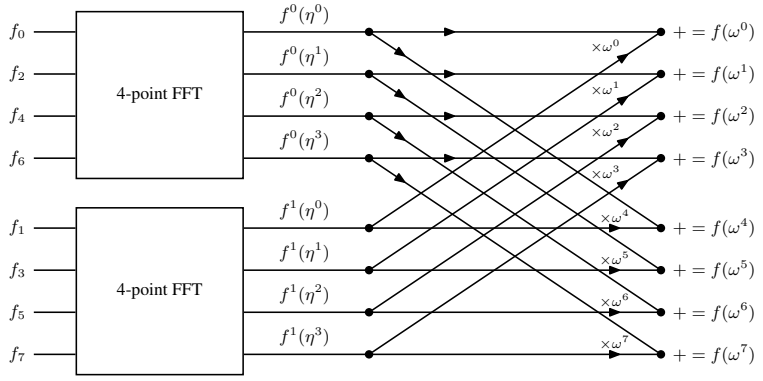

FIGURE 1. An 8-point FFT butterfly

Theorem 1 (Gauss-Cooley-Tukey)**.** *Let* $\mathbf{K}$ *be a field of characteristic different from* 2*. Let* $\nu \geqslant 1$ *be an integer and let* $n = 2^\nu$ *be a power of* 2*. Assume that* $\mathbf{K}$ *contains a primitive* n*-th root of unity* ω*. Then there exists a straight line program that takes as input the coefficients of a polynomial* $f(x)$ *of degree* $\leqslant n-1$ *and computes the* n *values* $f(\omega^i)$ *for* $0 \leqslant i \leqslant n-1$*, at the expense of* $2.n.\log_2 n$ *operations in* $\mathbf{K}$*.*

We denote A_ω the matrix of the map $a : \mathbf{K}[x]_{<n} \to \mathbf{K}^n$ in the bases $\mathcal{U}$, the polynomial basis of $\mathbf{K}[x]_{<n}$, and $\mathcal{V}$, the canonical basis of $\mathbf{K}^n$. It is well known that the inverse of A_ω is

$$A_\omega^{-1} = \frac{1}{n} A_{\omega^{-1}}.$$

We deduce the following theorem.

Theorem 2 (Gauss-Cooley-Tukey)**.** *Let* $\mathbf{K}$ *be a field of characteristic different from* 2*. Let* $\nu \geqslant 1$ *be an integer and let* $n = 2^\nu$ *be a power of* 2*. Assume that* $\mathbf{K}$ *contains a primitive* n*-th root of unity* ω*. Then there exists a straight line program that takes as input* n *scalars* $(v_i)_{0\leqslant i\leqslant n-1}$ *in* $\mathbf{K}$*, and computes a polynomial* $f(x) = \sum_{0\leqslant j\leqslant n-1} f_j x^j$ *such that* $f(\omega^i) = v_i$ *for every* $0 \leqslant i \leqslant n-1$*, at the expense of* $2.n.\log_2 n$ *operations in* $\mathbf{K}$*.*

Note that if $\mathbf{K}$ has characteristic 2, there cannot be primitive roots of unity of even order in $\mathbf{K}$. So the butterfly method does not apply. However, assuming that the characteristic of $\mathbf{K}$ is not three, we may consider polynomials of degree $\leqslant n-1$ for some $n = 3^\nu$. Assuming that $\mathbf{K}$ contains a primitive n-th root of unity, the butterfly method can be adapted using a tripartition. We decompose the polynomial $f(x)$ as a sum of three eigenvectors associated to the three eigenvalues of the automorphism of order 3 mapping x to ζx, where $\zeta \in \mathbf{K}$ is a primitive third root of unity. Namely

$$f(x) = \sum_{0\leqslant 3j\leqslant n-1} f_{3j}\, x^{3j} + x \sum_{0\leqslant 3j+1\leqslant n-1} f_{3j+1}\, x^{3j} + x^2 \sum_{0\leqslant 3j+2\leqslant n-1} f_{3j+2}\, x^{3j} = f^0(y) + x f^1(y) + x^2 f^2(y)$$

where $y = x^3$ and f^0, f^1, and f^2 have degree $\leqslant n/3 - 1$.

It is time for a first geometric interpretation. A polynomial is a function on the curve $\mathbf{P}^1$ having poles only at infinity. More precisely the vector space $\mathbf{K}[x]_{\leqslant n-1}$ is the linear space associated with the divisor $E = (n-1)[\infty]$. The n evaluation points form a divisor also

$$Q = [1] + [\omega] + [\omega^2] + \cdots + [\omega^{n-2}] + [\omega^{n-1}].$$

The map $\tau : x \mapsto \omega x$ defines an automorphism of $\mathbf{P}^1$, of order n, that leaves invariant both divisors E and Q. Calling G the group generated by τ, we see that the map $a : \mathbf{K}[x]_{\leqslant n-1} \to \mathbf{K}^n$ is a

morphism between two free $\mathbf{K}[G]$-modules of rank 1. The recursive algorithm relies on the existence of a composition series

$$G =< \omega > \supset < \omega^2 > \supset < \omega^4 > \supset < \omega^8 > \supset \ \ldots \ \supset \ \langle -1 \rangle \ \supset \ \langle 1 \rangle.$$

The map $x \mapsto y = x^2$ is a degree two Galois cover $\varphi : \mathbf{P}^1 \to \mathbf{P}^1$ with Galois group $\langle -1 \rangle \subset G$. Equations (1) and (2) reduce the initial evaluation problem to two similar problems on the quotient curve.

4.2. **Application: fast multiplication of polynomials.** We assume again that $n = 2^\nu$ and $\mathbf{K}$ is a finite field containing a primitive n-th root of unity ω. We denote by a the evaluation map studied in the previous section. Identifying $\mathbf{K}[x]_{<n}$ with $\mathbf{K}[x]/(x^n - 1)$, the linear map a is an isomorphism between the $\mathbf{K}$-algebras $\mathbf{K}[x]/(x^n - 1)$ and $\mathbf{K}^n$, often called the discrete Fourier transform (DFT). Multiplication of two elements in $\mathbf{K}^n$ is the componentwise product and is achieved at the expense of n multiplications in $\mathbf{K}$. In order to multiply two elements u_1 and u_2 in $\mathbf{K}[x]/(x^n - 1)$ given in the power basis, one computes $a^{-1}(a(u_1).a(u_2))$ at a total cost of

$$4.n.\log_2 n + n + 2.n.\log_2 n = n(1 + 6\log_2 n).$$

Assume now we want to multiply two polynomials f_1 and f_2 of degree $\leqslant n/2 - 1$. The quotient map

$$\rho : \mathbf{K}[x] \to \mathbf{K}[x]/(x^n - 1)$$

is an epimorphism of $\mathbf{K}$ algebras. We define a section

$$\sigma : \mathbf{K}[x]/(x^n - 1) \to \mathbf{K}[x]$$

by setting $\sigma(x^j \bmod x^n - 1) = x^j$. This is a $\mathbf{K}$-linear map and $\rho \circ \sigma$ is the identity of $\mathbf{K}[x]/(x^n - 1)$. On the other hand $\sigma \circ \rho$ is the projection on $\mathbf{K}[x]_{\leqslant n-1}$ with kernel $(x^n - 1)\mathbf{K}[x]$. While σ is not a morphism of algebras we still have that

$$f_1.f_2 = \sigma(\rho(f_1).\rho(f_2))$$

because $\deg(f_1) + \deg(f_2) \leqslant n - 1$. We deduce that multiplication of two polynomials reduces to a multiplication in $\mathbf{K}[x]/(x^n - 1)$ for n a power of two bigger than twice the degrees of both f_1 and f_2.

Theorem 3. *Let $\mathbf{K}$ be a field of characteristic different from 2. Let $\nu \geqslant 1$ be an integer and let $n = 2^\nu$ be a power of 2. Assume that $\mathbf{K}$ contains a primitive n-th root of unity ω. Then there exists a straight line program that takes as input two polynomials $f_1(x)$ and $f_2(x)$ of degree $< n/2$ and computes their product, at the expense of $n(1 + 6\log_2 n)$ operations in $\mathbf{K}$. Both the input and the output are given in the monomial basis.*

The calculation above provides a first example of using non-algebraic maps. These maps often are set-theoretic sections of ring homomorphisms, that are not ring homomorphisms themselves but behave like ring homomorphisms when one imposes metric conditions on their input.

Theorem 3 only applies when the base field contains a primitive root of unity of order a large enough power of two. This is because we use fast Fourier transform to evaluate and interpolate. We shall see later how to get around this difficulty. For the moment we notice that if we consider the bilinear complexity (meaning that we ignore the cost of the linear part of the calculation) then we obtain a linear upper bound provided $\mathbf{K}$ is large enough.

Theorem 4. *Let n_1 and n_2 be two positive integers. Let $\mathbf{K}$ be a field with cardinality bigger than $n_1 + n_2$. Then there exists a straight line program that takes as input two polynomials $f_1(x)$ and $f_2(x)$ of respective degrees $\leqslant n_1$ and $\leqslant n_2$ and computes their product using no more than $n_1 + n_2 + 1$ multiplications in $\mathbf{K}$. Both the input and the output are given in the monomial basis.*

Indeed let $a_0, a_1, \ldots, a_{n_1+n_2}$ be n_1+n_2+1 pairwise distinct scalars in $\mathbf{K}$. Let

$$a : \mathbf{K}[x]_{\leqslant n_1+n_2} \to \mathbf{K}^{n_1+n_2+1}$$

be the evaluation map at these n_1+n_2+1 scalars. This map is the restriction to $\mathbf{K}[x]_{\leqslant n_1+n_2}$ of an epimorphism of algebras. This restriction is a bijective $\mathbf{K}$-linear map and, assuming that $\deg(f_1) \leqslant n_1$ and $\deg(f_2) \leqslant n_2$, we check that $f_1.f_2 = a^{-1}(a(f_1).a(f_2))$.

So the computation of the polynomial product $f_1.f_2$ reduces to a componentwise product in $K^{n_1+n_2+1}$ plus some linear part that we ignore. This finishes the proof of Theorem 4.

Comparing Theorem 4 and Theorem 3 we notice that, in order to bound the bilinear complexity, we only need the base field to be large enough. In contrast, bounding the full complexity uses a primitive root of unity with order a large enough power of two, which is a much more restrictive condition.

4.3. **Application: fast multiplication in some finite field extensions I.** Let $n \geqslant 2$ be an integer. Let $\mathbf{K}$ be a finite field. Let $\mathbf{L}/\mathbf{K}$ be a degree n field extension. Let $\mathcal{B}$ be a $\mathbf{K}$-basis of $\mathbf{L}$. We are interested in the complexity of multiplication in $\mathbf{L}$. This is a $\mathbf{K}$-bilinear map. Given the coordinates in $\mathcal{B}$ of two elements ℓ_1 and ℓ_2 in $\mathbf{L}$, we want to compute the coordinates of their product.

We first consider the bilinear complexity. It is independent of the basis $\mathcal{B}$ because base change is a linear operation. In fact the bilinear complexity only depends on the extension $\mathbf{L}/\mathbf{K}$ up to isomorphism, that is to say on the degree n of $\mathbf{L}$ over $\mathbf{K}$ and on the cardinality q of $\mathbf{K}$.

We let $B(x) \in \mathbf{K}[x]$ be an irreducible polynomial of degree n. We set $\mathbf{L} = \mathbf{K}[x]/B(x)$ and take $\mathcal{B}$ to be the monomial basis $(1, x, x^2, \ldots, x^{n-1})$. We denote e_B the residue map

$$\begin{array}{rccc} e_B & : & \mathbf{K}[x]_{\leqslant n-1} & \longrightarrow & \mathbf{L} \\ & & f(x) & \longmapsto & f(x) \bmod B(x) \end{array}$$

This is a bijective $\mathbf{K}$-linear map. We denote e_B^{-1} its inverse. We shall also need a similar map accepting as input a polynomial of degree $\leqslant 2n-2$. We call it e_B^2.

$$\begin{array}{rccc} e_B^2 & : & \mathbf{K}[x]_{\leqslant 2n-2} & \longrightarrow & \mathbf{L} \\ & & f(x) & \longmapsto & f(x) \bmod B(x) \end{array}$$

We assume that the cardinality of $\mathbf{K}$ is $\geqslant 2n-1$ and we let $q_0, q_1, \ldots, q_{2n-2}$ be $2n-1$ pairwise distinct scalars in $\mathbf{K}$. We denote e_Q the evaluation map

$$\begin{array}{rccc} e_Q & : & \mathbf{K}[x]_{\leqslant 2n-2} & \longrightarrow & \mathbf{K}^{2n-1} \\ & & f(x) & \longmapsto & (f(q_i))_{0 \leqslant i \leqslant 2n-2} \end{array}$$

This is a bijective $\mathbf{K}$-linear map. It thus admits an inverse map that we denote

$$e_Q^{-1} : \mathbf{K}^{2n-1} \to \mathbf{K}[x]_{\leqslant 2n-2}.$$

In order to multiply two elements $\ell_1 = f_1(x) \bmod B(x)$ and $\ell_2 = f_2(x) \bmod B(x)$ we first multiply the two polynomials $f_1(x) = e_B^{-1}(\ell_1)$ and $f_2(x) = e_B^{-1}(\ell_2)$. In order to compute

$$f_3(x) = f_1(x).f_2(x)$$

we proceed as in Section 4.2. We evaluate $f_1(x)$ and $f_2(x)$ at the $(q_i)_{0 \leqslant i \leqslant 2n-2}$. We then multiply the values taken by $f_1(x)$ and $f_2(x)$. And we interpolate to obtain

$$f_3(x) = e_Q^{-1}(e_Q(f_1).e_Q(f_2)).$$

Finally the product $\ell_1.\ell_2$ is

$$\ell_3 = e_B^2(f_3) = e_B^2(e_Q^{-1}(e_Q(e_B^{-1}(\ell_1)).e_Q(e_B^{-1}(\ell_2)))).$$

The bilinear part in this computation consists of one product in the algebra $\mathbf{K}^{2n-1}$. We deduce the theorem below.

Theorem 5. *Let $\mathbf{K}$ be a finite field. Let n be an integer such that $n \leqslant (\#\mathbf{K}+1)/2$. Let $\mathbf{L}$ be a field extension of $\mathbf{K}$ with degree n. The bilinear complexity of multiplication in $\mathbf{L}$ is $\leqslant 2n-1$.*

Again we can give a geometric interpretation of the above. We consider the projective line $\mathbf{P}^1$ over $\mathbf{K}$ and denote E the divisor $(n-1).[\infty]$ and Q the divisor $[q_0]+[q_1]+\cdots+[q_{2n-2}]$. The polynomial $B(x)$ defines an irreducible divisor on $\mathbf{P}^1$ that we call B also. The space $\mathbf{K}[x]_{\leqslant n-1}$ is the linear space $\mathcal{L}(E)$ associated with E. The maps e_B and e_Q are residue maps. The residue field at B is $\mathbf{L}$, a degree n field extension of $\mathbf{K}$. The residue ring at Q is $\mathbf{K}^{2n-1}$. The method reduces a multiplication in the residue field at B to a multiplication in the residue ring at Q.

4.4. **Application: fast multiplication in some finite field extensions II.** We now consider the (full) complexity of multiplication in $\mathbf{L}$. This time we no longer ignore the cost of linear steps: evaluating, interpolating, reducing modulo $B(x)$. Our plan is to use butterflies. So we shall restrict to the very specific case when

(1) the characteristic p of $\mathbf{K}$ is not 2,
(2) $n = 2^\nu$ is a power of 2,
(3) the cardinality q of $\mathbf{K}$ is congruent to 1 modulo $2n$.

We look for a simple irreducible polynomial $B(x)$ of degree n. Such a polynomial is provided by the Kummer theory of the multiplicative group. Let $\mathbf{K}_s$ be a separable closure of $\mathbf{K}$. Let Γ be the Galois group of $\mathbf{K}_s$ over $\mathbf{K}$. The Frobenius automorphism

$$\begin{array}{ccccc} F_{\mathbf{K}} & : & \mathbf{K}_s & \longrightarrow & \mathbf{K}_s \\ & & x & \longmapsto & x^q \end{array}$$

is a topological generator of Γ. We denote by δ the 2-valuation of $q-1$. Condition (3) above implies that $\delta \geqslant \nu+1$. Let b be an element of order $2^{\delta+\nu}$ in $\mathbf{K}_s^*$. Let

$$t = F_{\mathbf{K}}(b)/b = b^q/b = b^{q-1}.$$

This is an element of multiplicative order $n = 2^\nu$. So it belongs to $\mathbf{K}^*$. We deduce that the Galois conjugates of b are the $b.t^i$ for $0 \leqslant i \leqslant n-1$. And $\mathbf{K}(b)$ is a degree n extension of $\mathbf{K}$. We call it $\mathbf{L}$. We set

$$a = b^n.$$

This is an element of order 2^δ in $\mathbf{K}^*$. And $\mathbf{L}$ is the splitting field of $B(x) = x^n - a$. We identify $\mathbf{L}$ with $\mathbf{K}[x]/(x^n-a)$ and b with $x \bmod x^n - a$.

In order to multiply two elements $\ell_1 = f_1(x) \bmod B(x)$ and $\ell_2 = f_2(x) \bmod B(x)$ we first multiply the two polynomials $f_1(x)$ and $f_2(x)$. To this end we evaluate $f_1(x)$ and $f_2(x)$ at the $(\omega^i)_{0\leqslant i\leqslant 2n-1}$ where ω is an element of order $2n$ in $\mathbf{K}^*$. We then multiply the values taken by $f_1(x)$ and $f_2(x)$ at the $(\omega^i)_{0\leqslant i\leqslant 2n-1}$. And we interpolate to obtain $f_3(x)$, a polynomial of degree $\leqslant 2n-2$. These evaluation and interpolation steps are achieved at the expense of $12.n.\log_2(2n)$ operations in $\mathbf{K}$, using the method in Section 4.1. We finally reduce $f_3(x)$ modulo $B(x) = x^n - a$. This requires $n-1$ multiplications and $n-1$ additions in $\mathbf{K}$.

Theorem 6. *Let $n = 2^\nu$ with $\nu \geqslant 1$ an integer. Let $\mathbf{K}$ be a finite field with cardinality congruent to 1 modulo $2n$. Let $\mathbf{L}$ be a field extension of $\mathbf{K}$ with degree n. There exists a $\mathbf{K}$-basis $\mathcal{B}$ of $\mathbf{L}$ and a straight line program that takes as input the coordinates in $\mathcal{B}$ of two elements in $\mathbf{L}$ and computes the coordinates in $\mathcal{B}$ of their product, at the expense of $n.(16 + 12\log_2 n)$ operations in $\mathbf{K}$.*

The basis $\mathcal{B}$ in the theorem above is the power basis $(x^j \bmod x^n - a)_{0\leqslant j\leqslant n-1}$. We set

$$\theta = 1 + x + x^2 + \cdots + x^{n-1} \bmod x^n - a$$

and notice that θ is a normal element in $\mathbf{L}/\mathbf{K}$ in the sense that the set of its conjugates is a $\mathbf{K}$-basis of $\mathbf{L}$. We denote Θ this normal basis. We notice that passing from basis Θ to basis $\mathcal{B}$ amounts to computing a discrete Fourier transform of order $n = 2^\nu$. We deduce the following refinement of Theorem 6.

Theorem 7. *Let $n = 2^\nu$ with $\nu \geqslant 1$ an integer. Let $\mathbf{K}$ be a finite field with cardinality congruent to 1 modulo $2n$. Let $\mathbf{L}$ be a field extension of $\mathbf{K}$ with degree n. There exists a normal $\mathbf{K}$-basis $\mathcal{B}$ of $\mathbf{L}$ and a straight line program that takes as input the coordinates in $\mathcal{B}$ of two elements in $\mathbf{L}$ and computes the coordinates in $\mathcal{B}$ of their product, at the expense of $n.(16 + 18\log_2 n)$ operations in $\mathbf{K}$.*

The geometric picture here is the following. The map $\tau : x \mapsto \omega^2 x$ defines an automorphism of $\mathbf{P}^1$ of order n. The quotient map is a Galois cover $I : \mathbf{P}^1 \to \mathbf{P}^1$ with Galois group G generated by τ. Indeed I is the polynomial $I(x) = x^n$. The fiber $I^{-1}(a)$ is irreducible over $\mathbf{K}$ with residue field $\mathbf{L}$. The group generated by ω is the union of the fibers $I^{-1}(1)$ and $I^{-1}(-1)$. These two fibers split over $\mathbf{K}$. As in the previous section the method reduces a multiplication in the residue field at $B = I^{-1}(a)$ to a multiplication in the residue ring at $Q = I^{-1}(1) \cup I^{-1}(-1)$. The new feature is that both divisors B and Q are acted on by the group $G = \langle\omega^2\rangle$. In particular the space $\mathcal{L}((n-1).[\infty])$ and the residue rings at B and Q are $\mathbf{K}[G]$-modules. Also the residue maps are $\mathbf{K}[G]$-linear. Further the group $G = \langle\omega^2\rangle$ has a composition series with quotients of order 2. Kummer theory controls which fibers of I are irreducible and which decompose over $\mathbf{K}$. In fact we have a fully explicit description of Galois action on $\mathbf{K}_s^*$. The Frobenius multiplies by $q = \#\mathbf{K}$.

4.5. **Application: fast Reed-Solomon codes.** Let $\mathbf{K}$ be a finite field. Let $n \geqslant 2$ be an integer. Let $q_0, q_1, \ldots, q_{n-1}$ be n pairwise distinct scalars in $\mathbf{K}$. Let k be an integer such that $1 \leqslant k \leqslant n$. Let E be the space $\mathbf{K}[x]_{\leqslant k-1}$ of polynomials with degree $\leqslant k-1$. Let e_Q be the evaluation map

$$\begin{array}{cccc} e_Q & : & \mathbf{K}[x]_{\leqslant k-1} & \longrightarrow & \mathbf{K}^n \\ & & f(x) & \longmapsto & (f(q_i))_{0\leqslant i\leqslant n-1} \end{array}$$

The image of e_Q is a k-dimensional subspace $C \subset \mathbf{K}^n$ known as a Reed-Solomon code. Its minimum distance is $d = n - k + 1$ which is best possible for a code of length n and dimension k.

Assume now that

(1) the characteristic p of $\mathbf{K}$ is odd,
(2) $n = 2^\nu$ is a power of 2,
(3) the cardinality q of $\mathbf{K}$ is congruent to 1 modulo n,

We let ω be a primitive n-th root of 1 in $\mathbf{K}$ and we set $q_i = \omega^i$ for $0 \leqslant i \leqslant n-1$. Evaluating e_Q is achieved at the expense of $2.n.\log_2 n$ operations in $\mathbf{K}$ using butterflies. We thus obtain a particularly fast encoding. See [35].

Theorem 8. *Let $n = 2^\nu$ with $\nu \geqslant 1$ an integer. Let $\mathbf{K}$ be a finite field with cardinality congruent to 1 modulo n. Let k be an integer such that $1 \leqslant k \leqslant n$. There exists a linear $[n, k, n-k+1]$-code over $\mathbf{K}$ that can be encoded and checked at the expense of $2.n.\log_2 n$ operations in $\mathbf{K}$.*

5. When $\mathbf{K}$ is too small or lacks roots of unity

The various methods presented in Section 4 assume that the base field $\mathbf{K}$ is large enough (to evaluate and interpolate at a large set of scalars) or even contains a primitive root of unity of order a large power of two (to allow a recursive approach). There are several methods to bypass these restrictions. The method of Schönhage and Strassen presented in Section 5.1 relies on algebraic and non-algebraic maps. An important ingredient in the work of Harvey and van der Hoeven is a number theoretic conjecture about the smallest prime in an arithmetic progression. We give references in Section 5.2. The method introduced by Chudnovsky and Chudnovsky in [5] to upper bound the bilinear complexity of multiplication in finite field extensions relies on the geometry of algebraic curves over finite fields. We sketch this method in Section 5.4. And Section 5.3 surveys the complexity of computing in the algebra of a commutative group.

5.1. **Schönhage-Strassen.** Let R be a commutative ring with unit. Assume that 2 is invertible in R. Let d be a positive integer. According to a result of Schönhage and Strassen, there exists a SLP that computes the product of two polynomials in $R[x]$ having degree $\leqslant d$, at the expense of a constant times $d.\log(d).\log(\log(d))$ operations in R. See [38, Section 8.3] and [3, Theorem 2.13]. We give an overview of the ideas behind this result. As in Section 4.2 we will use non-algebraic maps.

Assume ν is the smallest even number such that $n = 2^\nu$ is bigger than $2d$. Let $m = 2^{\nu/2}$ be the square-root of n. Let $\rho : R[x,y] \to R[x]$ be the R-algebra homomorphism that substitute y by x^m. Equivalently this is the quotient by the ideal $y - x^m$.

$$\begin{array}{rcl} \rho & : & R[x,y] \longrightarrow R[x] \\ & & P(x,y) \longmapsto P(x,x^m) \end{array}$$

The map ρ is an example of Kronecker substitution. See [22, 38]. As a R-linear map, ρ admits a section σ which we define by setting

$$\sigma(x^a) = y^b x^r \quad \text{where} \quad a = mb + r \quad \text{is the euclidean division of} \quad a \quad \text{by} \quad m.$$

We deduce that for $f_1(x)$ and $f_2(x)$ in $R[x]$

$$\rho(\sigma(f_1).\sigma(f_2)) = f_1.f_2.$$

When the degree of f_1 and f_2 is $< n/2$ we reduce the multiplication of f_1 and f_2 to the multiplication of $\sigma(f_1)$ and $\sigma(f_2)$ that are polynomials of degree in x strictly smaller than m and degree in y smaller than $n/(2m) = m/2$. To compute the latter multiplication we define an auxiliary ring

$$S = R[x]/(x^{2m} - 1)$$

and consider another homomorphism of R-algebras

$$\begin{array}{rcl} \rho' & : & R[x,y] \longrightarrow R[x,y]/(x^{2m}-1) = S[y] \\ & & P(x,y) = \sum_{i\geqslant 0} p_i(x).y^i \longmapsto \sum_{i\geqslant 0}(p_i(x) \bmod x^{2m}-1).y^i. \end{array}$$

As an R-linear map, ρ' admits a section σ' which we define by setting

$$\sigma'\left((x^j \bmod x^{2m}-1).y^i\right) = x^j.y^i \quad \text{for} \quad 0 \leqslant i \text{ and } 0 \leqslant j \leqslant 2m-1.$$

The map $\sigma' \circ \rho'$ is the projection of $R[x,y]$ onto the R-submodule of $R[x,y]$ containing polynomials with degree in x strictly smaller than $2m$, with kernel the ideal of $R[x,y]$ generated by $x^{2m} - 1$. We deduce that for $F_1(x)$ and $F_2(x)$ in $R[x,y]$ having degree in x strictly smaller than m,

$$\sigma'(\rho'(F_1).\rho'(F_2)) = F_1.F_2.$$

In particular if $F_1 = \sigma(f_1)$ and $F_2 = \sigma(f_2)$ where $f_1(x)$ and $f_2(x)$ have degree $< n/2$ then we reduce the multiplication of F_1 and F_2 to the multiplication of $\rho'(F_1)$ and $\rho'(F_2)$ that are polynomials in $S[y]$ of degree strictly smaller than $m/2$ in y. Since S contains a primitive m-th root of unity

$$\omega = x^2 \bmod x^{2m} - 1$$

we can use the method presented in Section 4.2. It is important to notice that multiplication by ω in S amounts to a cyclic shift of coordinates. In the SLP model, such a cyclic shift is for free. Even in a more pessimistic model (such as a multitape Turing machine) a cyclic shift is achieved in linear time. Putting all this together, and using a more intelligent recursion, Schönhage and Strassen prove that multiplication of two polynomials of degree $\leqslant d$ with coefficients in a commutative ring with unit where 2 is invertible, can be compute by a SLP at the expense of a constant times $d.\log(d).\log(\log(d))$ operations in R. In case 2 is not invertible in R we assume that 3 is invertible and use a variant of the method above using tripartitions.

5.2. **Harvey-van der Hoeven.** There are recent advances in the complexity of polynomial multiplication over a finite field. See [16] and [15] for example. In [15] Harvey and van der Hoeven prove that the product of two polynomials of degree $\leqslant n$ over a field with q elements can be computed by a Turing machine in time $O(n \log q \log(n \log q))$ uniformly in q, that is $O(n \log n)$ for fixed q. These upper bounds are conditional in the sense that they rely on some conjecture in number theory which is of independent interest.

A theorem of Linnik states that there exists two real numbers c and L such that for every coprime integers a and $n \geqslant 2$ there exists a prime integer congruent to a modulo n and smaller than or equal to $c.n^L$. A Linnik constant is by definition a real L that makes the above statement correct. By a result of Heath-Brown, one can take $L = 11/2$. See [17] and the recent improvement [40]. The proof of the upper bound by Harvey and van der Hoeven assumes that the exponent L in Linnik's theorem can be taken $< 1 + 2^{-1162}$.

5.3. **Convolution.** Let R be a commutative ring with unit. The product in $A = R[x]/(x^n - 1)$ is often called a convolution product. We are given two elements $f_1(x) \bmod x^n - 1$ and $f_2(x) \bmod x^n - 1$ in A, where the degrees of $f_1(x)$ and $f_2(x)$ are $\leqslant n - 1$. We want to compute $f_1(x).f_2(x) \bmod x^n - 1$. Equivalently we look for the remainder of the euclidean division of $f_1(x).f_2(x)$ by $x^n - 1$ We first compute the product $f_3(x) = f_1(x).f_2(x)$. We then reduce $f_3(x)$ modulo $x^n - 1$. The second step amounts to $n - 1$ additions. So we focus on the first step.

We assume that either 2 or 3 is invertible in R. Using the method presented in Section 5.1 we compute $f_3(x) = f_1(x).f_2(x)$ at the expense of a constant times $n.\log(n).\log(\log(n))$ operations in R. We deduce $f_1(x).f_2(x) \bmod x^n - 1$ at the expense of $n - 1$ more operations.

This problem admits a natural generalization. We let G be a finite commutative group and call $R[G]$ the group algebra of G over R. Theorem 9 below [8, Theorem 2] concerns the case when R is a finite field of characteristic p. The statement involves an auxiliary prime p' such that $p' - 1$ is divisible by a large smooth integer, so as to allow fast Fourier transform. The statement also involves two natural non-algebraic maps $\ell : \mathbf{Z}/p\mathbf{Z} \to \mathbf{Z}/p'\mathbf{Z}$ and $\ell' : \mathbf{Z}/p'\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$. For c a congruence class in $\mathbf{K} = \mathbf{Z}/p\mathbf{Z}$ we denote by $\ell(c)$ the lift of c, that is the unique integer in the intersection of c with the interval $[0, p[$. We write

$$\uparrow(c) = \ell(c) \bmod p'. \tag{3}$$

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

$$\downarrow(c) = \ell'(c) \bmod p \quad \text{for} \quad c \in \mathbf{K}'. \tag{4}$$

Theorem 9 (Couveignes-Gasnier)**.** *There exists an absolute constant $\mathcal{Q}$ such that the following is true. Let G be a finite commutative group of order $\mathfrak{o}$. 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 straight-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 (3) and (4).*

The proof combines several classical ideas and results. The meaning of this theorem is that products in a commutative convolution algebra are computed in quasi-linear time in the dimension of the algebra. This is coherent with what we already observed: linear and bilinear maps can be computed quickly when they are compatible with a large group action.

5.4. **The bilinear complexity of multiplication in finite field extensions.** We have seen in Section 4.3 that the bilinear complexity of multiplication in a finite field extension $\mathbf{L}/\mathbf{K}$ of degree n is $\leqslant 2n-1$ provided the cardinality of $\mathbf{K}$ is at least $2n-1$. The reason for this limitation is that we need enough scalars in $\mathbf{K}$ where to evaluate polynomials. Chudnovsky and Chudnovsky proposed in [5] a generalization of the interpolation method presented in Section 4.3 involving functions on general curves rather than mere polynomials. So we let Y be a curve over a finite field $\mathbf{K}$. We assume that Y is projective, smooth and absolutely irreducible. Let $m \geqslant 1$ be an integer. Let $Q_0, Q_1, \ldots, Q_{m-1}$ be $\mathbf{K}$-rational points on Y. We call $Q = Q_0 + Q_1 + \cdots + Q_{m-1}$ the divisor consisting of the sum of all these m points. Let E be a divisor on Y. Let B be an irreducible divisor of degree n on Y. We assume that E, Q and B are pairwise disjoint. We adapt the construction of Section 4.3 to this context.

We call $\mathbf{L}$ the residue field at B. This a degree n extension of $\mathbf{K}$. We denote e_B the residue map

$$\begin{array}{rccc} e_B & : & \mathcal{L}(E) & \longrightarrow \mathbf{L} \\ & & f & \longmapsto f_{|B} \end{array}$$

which we assume to be surjective. We choose a right inverse e_B^{-1} of e_B. Since we plan to multiply two functions in $\mathcal{L}(E)$, we shall need a residue map modulo B for functions in $\mathcal{L}(2E)$. We call it e_B^2.

$$\begin{array}{rccc} e_B^2 & : & \mathcal{L}(2E) & \longrightarrow \mathbf{L} \\ & & f & \longmapsto f_{|B} \end{array}$$

We denote e_Q the evaluation map

$$\begin{array}{rccc} e_Q & : & \mathcal{L}(2E) & \longrightarrow \mathbf{K}^m \\ & & f & \longmapsto (f(Q_i))_{0\leqslant i\leqslant m-1} \end{array}$$

which we assume to be injective. We choose a left inverse e_Q^{-1} of e_Q.

In order to multiply two elements ℓ_1 and ℓ_2 we first multiply the two functions $f_1 = e_B^{-1}(\ell_1)$ and $f_2 = e_B^{-1}(\ell_2)$. In order to compute

$$f_3 = f_1.f_2$$

we evaluate f_1 and f_2 at the $(Q_i)_{0\leqslant i\leqslant m-1}$. We then multiply the values taken by f_1 and f_2. And we interpolate to obtain

$$f_3 = e_Q^{-1}(e_Q(f_1).e_Q(f_2)).$$

Finally the product $\ell_1.\ell_2$ is

$$\ell_3 = e_B^2(f_3) = e_B^2(e_Q^{-1}(e_Q(e_B^{-1}(\ell_1)).e_Q(e_B^{-1}(\ell_2)))).$$

The bilinear part in this computation consists of one product in the algebra $\mathbf{K}^m$.

According to the Riemann-Roch theorem, and denoting g_Y the genus of Y, we see that the surjectivity of e_B is granted if

$$\deg(E - B) \geqslant 2g_Y - 1,$$

and the injectivity of e_Q is granted if

$$\deg(2E - Q) = 2\deg(E) - m < 0.$$

Combining these two inequalities we see that this construction provides a bound for the bilinear complexity of multiplication in a degree n extension of $\mathbf{K}$ if there exists a curve Y over $\mathbf{K}$ such that

$$\#Y(\mathbf{K}) \geqslant 4g_Y + 2n - 1.$$

This is not optimal at all but still useful if we find a sequence of curves over $\mathbf{K}$ such that

$$\#Y(\mathbf{K}) \to +\infty \text{ and the quotient } \#Y(\mathbf{K})/g_Y \text{ has a limit } > 4.$$

One says that a family of curves over a fixed finite field of cardinality q has many points when the ratio $\#Y(\mathbf{K})/g_Y$ tends to $\sqrt{q} - 1$. This is know to be best possible, when possible. Modular curves $X_0(N)$ have many points over finite fields with p^2 elements, corresponding to supersingular moduli, as was noticed by Ihara [19] and by Tsfasman, Vladut, and Zink [36]. These authors also find families of Shimura curves having many points over any field with cardinality a square. Garcia and Stichtenoth [11] construct for every square prime power 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.

This and the construction above suffice to bound the bilinear complexity of multiplication when q is a square bigger than 25. The general case is treated thanks to a base change. Following these lines Chudnovsky [5], Shparlinski, Tsfasmann, Vladut [34], Shokrollahi [33], Ballet and Rolland [1, 2], Chaumine [4], Randriambololona [28] and others prove that the $\mathbf{K}$-bilinear complexity of multiplication in a degree n extension $\mathbf{L}/\mathbf{K}$ is bounded by an absolute constant times n.

5.5. **Goppa codes.** We quickly review the construction of Goppa codes. See [12, 14, 13, 23]. Let Y be a projective, smooth and absolutely irreducible curve. Let g be the genus of Y. Let $m \geqslant 1$ be an integer. Let $Q_0, Q_1, \ldots, Q_{m-1}$ be $\mathbf{K}$-rational points on Y. We call $Q = Q_0 + Q_1 + \cdots + Q_{m-1}$ the divisor consisting of the sum of all these m points. Let E be a divisor on Y of degree

$$\deg E \geqslant 2g - 1.$$

We assume that E and Q are disjoint. We denote e_Q the evaluation map

$$\begin{array}{rccc} e_Q & : & \mathcal{L}(E) & \longrightarrow & \mathbf{K}^m \\ & & f & \longmapsto & (f(Q_i))_{0 \leqslant i \leqslant m-1} \end{array}$$

We assume that

$$m > \deg(E).$$

So e_Q is injective. The image of e_Q is a code C over $\mathbf{K}$ having length m, dimension $k = \deg E - g + 1$ and minimum distance $d \geqslant m - \deg E$. It fails to be MDS because of the $-g$ term in the dimension. We have seen that for $\mathbf{K}$ a finite field with cardinality q a square, there exist curves with many points

over $\mathbf{K}$ meaning that the genus tends to infinity and the ratio $\#Y(\mathbf{K})/g$ tends to $\sqrt{q}-1$. For $q \geqslant 16$ a square, this results in the existence, for every real ρ such that

$$\frac{1}{\sqrt{q}-1} < \rho < 1 - \frac{1}{\sqrt{q}-1},$$

of a family of codes over $\mathbf{K}$ such that the rate k/m tends to ρ while the relative minimum distance d/m tends to

$$\delta = 1 - \rho - 1/(\sqrt{q}-1).$$

As a $\mathbf{K}$-linear map e_Q is described by a $\deg Q \times (\deg E - g_Y + 1) = m \times k$ matrix with coefficients in $\mathbf{K}$. So encoding in this context has cost $m \times k$ operations in $\mathbf{K}$.

6. Curves with automorphisms

The constructions presented in Sections 4.1, 4.2, 4.4,4.5, make use of the existence of automorphisms of the projective line (roots of unity) to design fast evaluation, interpolation, and multiplication algorithms. The automorphism group exploited by these constructions is a group of roots of unity. In order to generalize these constructions we need more curves over a finite field having a large commutative group of automorphism and we would like this group to be as general as possible. More precisely we are given a finite field $\mathbf{K}$ and we look for two projective, smooth and absolutely irreducible curves X and Y together with a Galois cover $I : Y \to X$ with abelian Galois group G. We call $\mathfrak{o}$ the cardinality of G. We need some control on fibers of I. In particular we need a collection of $\mathbf{K}$-rational points $P_0, P_1, \ldots, P_{m-1}$ on X such that the fibers of I above these points are totally split. We denote P the divisor sum of these points. We let Q be the inverse image of P by I. It consists of $\mathfrak{o}.m$ rational points. We also chose a divisor D on X that is disjoint to P and call E the inverse image of D by I. When I is unramified, the space of functions $\mathcal{L}(E)$ is a $\mathbf{K}[G]$-module that can be proved to be free of rank $\deg D - g_X + 1$ as soon as $\deg D \geqslant 2g_X - 1$. See [26][Theorem 2] and [8][Theorem 1]. The residue ring $\Gamma(\mathcal{O}_Q)$ at Q is a $\mathbf{K}[G]$-module also and it is free of rank $\deg P$ provided I is unramified above P. When these conditions are met, the evaluation map $e_Q : \mathcal{L}(E) \to \Gamma(\mathcal{O}_Q)$ is a $\mathbf{K}[G]$-linear map between two free $\mathbf{K}[G]$-modules. One deduces the existence of excellent linear codes that can be encoded in quasi-linear time and decoded in quasi-quadratic time. See Couveignes and Gasnier [8]. Indeed we are in the situation of Section 5.5 with the extra property that the Goppa code C has a structure of a free $\mathbf{K}[G]$-submodules of a free $\mathbf{K}[G]$-modules. Encoding amounts to evaluating the map e_Q. As a $\mathbf{K}$-linear map e_Q is described by a $\deg Q \times (\deg E - g_Y + 1)$ matrix with coefficients in $\mathbf{K}$. As a $\mathbf{K}[G]$-linear map e_Q is described by a $\deg P \times (\deg D - g_X + 1)$ matrix with coefficients in $\mathbf{K}[G]$. We replace $\deg Q \times (\deg E - g_Y + 1)$ operations in $\mathbf{K}$ by $\deg P \times (\deg D - g_X + 1)$ in $\mathbf{K}[G]$. The number of operations is divided by $\mathfrak{o}^2$. The cost of an operation in $\mathbf{K}[G]$ is $O(\mathfrak{o}.\log^2 \mathfrak{o})$ operations in $\mathbf{K}$ for fixed $\mathbf{K}$ according to Theorem 9. We save almost a factor $\mathfrak{o}$ in the complexity. This is significant when $\mathfrak{o}$ is exponentially large with respect to g_X.

Assume now we want to multiply in an extension of $\mathbf{K}$ of degree n. We let G be cyclic of order $\mathfrak{o} = n$. We assume that there is a $\mathbf{K}$-rational point a on X such that the fiber $B = I^{-1}(a)$ of I above a is irreducible. The Frobenius above a generates G. The maps e_B and e_Q introduced in Section 5.4 are now $\mathbf{K}[G]$-linear maps. We assume that e_B has a right inverse e_B^{-1}. We also assume that e_Q has a left inverse e_Q^{-1}. The linear maps in Chudnovsky's method are now $\mathbf{K}[G]$-linear maps. They have complexity quasi-linear in n. In [9] and [7] one deduces

Theorem 10 (Ezome-Lercier-Couveignes)**.** *Let $\mathbf{K}$ be a finite field of cardinality q. Let $\mathbf{L}/\mathbf{K}$ be an extension of degree $n \geqslant 2$. Let $\mathcal{B}$ be a normal basis of $\mathbf{L}/\mathbf{K}$. There exists a SLP that computes the*

product of two elements in $\mathbf{L}$ *given by their coordinates in* $\mathcal{B}$ *at the expense of*

$$\leqslant \mathcal{Q} \times n \times \lceil \log_q(n) \rceil \times \log(n) \times |\log(\log(n))|$$

operations in $\mathbf{K}$ *where* $\mathcal{Q}$ *is an absolute constant.*

There remains to explain how to find curves with a large automorphism group over a finite field. There are two natural sources for such curves: elliptic curves and class field theory. Elliptic curves allow very explicit calculations and offer already some variety since their order varies in the Hasse interval. However the number of points on an elliptic curve over a field with cardinality q is upper bounded by $q + 1 + 2\sqrt{q}$. Class field theory provides curves with an arbitrary large commutative automorphism group over a fixed finite field.

6.1. **Elliptic curves with a point of order** n**.** Let $\mathbf{K}$ be a finite field of order q. Many of the methods presented in Section 4 assume that $\mathbf{K}$ contains a primitive root of unity ω of a given order n. Equivalently $\mathbf{P}^1$ has an automorphism $x \mapsto \omega x$ of order n. This is possible when n divides $q - 1$. Using an elliptic curve rather than the projective line offers new possibilities. It is thus natural to state a sufficient condition for the existence of an elliptic curve over $\mathbf{K}$ having a point of order n. We have the following simple theorem.

Theorem 11. *Let* $\mathbf{K}$ *be a field with* q *elements. Let* n *be a positive integer such that* $n^4 \leqslant 4q$*. Then there exists an elliptic curve over* $\mathbf{K}$ *having a* $\mathbf{K}$*-rational point of order* n*.*

Indeed the length of the Hasse interval is $4\sqrt{q}$. So there are two consecutive multiples of n^2 in it. At least one of them is not congruent to 1 modulo p. Call it m. Let $c = q+1-m$, then $|c| \leq 2\sqrt{q}$ and $m \not\equiv 1 \pmod{p}$ is equivalent to $c \not\equiv 0 \pmod{p}$. By a theorem of Waterhouse [39], for any integer c with $|c| \leq 2\sqrt{q}$ and $p \nmid c$, there exists an ordinary elliptic curve E over $\mathbb{F}_q$ with trace c, hence with exactly m rational points (for prime fields this was already proved by Deuring [10]). The group of an elliptic curve over a finite field is either cyclic or a product of two cyclic groups $C_{n_1} \times C_{n_2}$ with $n_1 \mid n_2$. If n^2 divides m, then n_2 must be a multiple of n. Hence there exists a point of order n.

6.2. **Class field theory.** According to class field theory [32, 29] there is a maximal abelian unramified cover of X over $\mathbf{K}$ that splits totally above P_0. We briefly recall its geometric construction. Let J_X be the jacobian variety of X. Recall $J_X(\mathbf{L})$ is the group of divisor classes of degree 0 on $X \otimes_{\mathbf{K}} \mathbf{L}$ for every extension $\mathbf{L}$ of $\mathbf{K}$. Let

$$j_X : X \to J_X$$

be the Jacobi map with origin P_0. The image by j_X of a point P on X is the class of the divisor $P - P_0$. Let

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

be the Frobenius endomorphism of partial degree $|\mathbf{K}|$, the cardinality q 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 by

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

the pullback of $\wp$ along j_X. This is the maximal abelian unramified cover of X that splits totally above P_0. 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_0 and its Galois group, acting by translations in J_X/H.

$$\begin{array}{ccccc} J_X(\mathbf{K}) & \hookrightarrow & Y_{\max} & \hookrightarrow & J_X \\ \downarrow & & \downarrow & & \downarrow H \\ G = J_X(\mathbf{K})/H & \hookrightarrow & Y & \hookrightarrow & J_X/H \\ \downarrow & & \downarrow \tau & & \downarrow G \\ 0 = P_0 & \hookrightarrow & X & \hookrightarrow & J_X \end{array} \qquad \wp$$

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

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

We have $F_{\mathbf{K}}(Q_{\max}) = Q_{\max} + P$. The Frobenius action on the fiber above P is translation by P. In other words the Artin map and the Jacobi map coincide, and the decomposition group of any place on Y above P is the subgroup in $G = J_X(\mathbf{K})/H$ 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 $P - P_0$ belongs to H. Similarly the fiber of τ above P is irreducible over $\mathbf{K}$ if and only if P generates the quotient $G = J_X(\mathbf{K})/H$.

6.3. **Small degree elliptic functions.** In this section, we study the simplest elliptic functions: those with degree 2 and 3. We prove simple linear and quadratic relations between these functions. We let $\mathbf{K}$ be a field and E an elliptic curve over $\mathbf{K}$. We assume E is given by some Weierstrass equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3\,.$$

We set $x = X/Z$, $y = Y/Z$ and $z = -x/y = -X/Y$, and find

$$\begin{aligned} x &= \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3 z + O(z^2)\,, \\ y &= -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 + O(z)\,. \end{aligned}$$

If A is a geometric point on E, we denote by τ_A the translation by A. We denote by $z_A = z \circ \tau_{-A}$ the composition of z with the translation by $-A$. We define x_A and y_A in a similar way.

If A and B are two distinct geometric points on E, we denote by $u_{A,B}$ the function on E defined as

$$u_{A,B} = \frac{y_A - y(A-B)}{x_A - x(A-B)}\,.$$

It has polar divisor $-[A] - [B]$. It is invariant by the involution exchanging A and B,

$$u_{A,B}(A + B - P) = u_{A,B}(P)\,.$$

If C is any third geometric point, we set $\Gamma(A,B,C) = u_{A,B}(C)$. This is the slope of the secant (resp. tangent) to E going through $C - A$ and $A - B$. It is well defined for any three points A, B, C such that $\#\{A,B,C\} \geqslant 2$. It is finite if and only if $\#\{A,B,C\} = 3$.

The Taylor expansions of $u_{A,B}$ at A and B are

$$\begin{aligned} u_{A,B} &= -\frac{1}{z_A} - x_A(B) z_A + (y_A(B) + a_3) z_A^2 + O(z_A^3) \\ &= \frac{1}{z_B} - a_1 + x_A(B) z_B + (y_A(B) + a_1 x_A(B)) z_B^2 + O(z_B^3). \end{aligned}$$

As a consequence $u_{B,A} = -u_{A,B} - a_1$ and

$$u_{A,B} + u_{B,C} + u_{C,A} = \Gamma(A,B,C) - a_1$$

and

$$\Gamma(A,B,C) = u_{B,C}(A) = u_{C,A}(B) = u_{A,B}(C) = -u_{B,A}(C) - a_1.$$

We deduce

$$u_{B,C} = u_{B,C}(A) - (x_A(C) - x_A(B))z_A + (y_A(C) - y_A(B))z_A^2 + O(z_A^3).$$

By comparison of Taylor expansions at A, B and C we prove

$$u_{A,B}u_{A,C} = x_A + \Gamma(A,B,C)u_{A,C} + \Gamma(A,C,B)u_{A,B} + a_2 + x_A(B) + x_A(C).$$

In the same vein,

$$u_{A,B}^2 = x_A + x_B - a_1 u_{A,B} + x_A(B) + a_2\,.$$

To some extent these simple minded functions play the role of polynomials in the context of elliptic curves. Let $n \geqslant 2$ be an integer. Let t be a point of order n in $E(\mathbf{K})$. Let G be the subgroup of $E(\mathbf{K})$ generated by t. Let

$$E = [O] + [t] + [2t] + \cdots + [(n-1)t]$$

be the corresponding divisor. The linear space $\mathcal{L}(E)$ has dimension n. The functions $u_{kt,(k+1)t}$ for $0 \leqslant k \leqslant n-1$ are nice candidates to form a basis of $\mathcal{L}(E)$. Indeed they have small degree and they are permuted by G. One first notices that their sum is a constant in $\mathbf{K}$. Then it is easy to check that the $(u_{kt,(k+1)t})_{0\leqslant k\leqslant n-1}$ form a basis of $\mathcal{L}(E)$ if and only if their sum is non-zero. It can be proved that there exists a constant c in $\mathbf{K}$ such that the functions $u_k = u_{kt,(k+1)t} + c$ for $0 \leqslant k \leqslant n-1$ form a basis of $\mathcal{L}(E)$. See [9][Lemma 5].

If one needs a basis of $\mathcal{L}(2E)$ it is natural to consider the translates of x by the multiples of t. For $\mathcal{L}(3E)$ we will use the translates of y. And so on. The functions obtained this way are the analogue of polynomials in the context of elliptic curves. See Vélu's thesis [37].

6.4. **The maximal unramified Kummer extension.** Given that class field theory proves the existence of interesting curves having many points and many automorphisms, we would like to get our hands on this treasure. We will treat here the simplest part of algorithmic class field theory: computing the prime to p part of the maximal abelian unramified extension of a function field of characteristic p.

We start with a finite field $\mathbf{K}$ of characteristic p and cardinality $q = p^n$ and a curve X over $\mathbf{K}$ which we assume to be projective, smooth and absolutely irreducible. We call g the genus of X. We let P_0 be a $\mathbf{K}$-rational point on X. We assume that we know how to efficiently

- represent a point P on X,
- represent a function f on X,
- compute the Taylor expansion of f at P, as a series in some local parameter π_P,
- compute the divisor of f,
- given a divisor D, compute a basis of $\mathcal{L}(D)$,
- pick a random effective divisor of given degree on X,
- base change to a finite extension $\mathbf{L}$ of $\mathbf{K}$.

Under very mild conditions, there are polynomial time algorithms for all these tasks. These basic operations allow us to compute in the Picard group of X. Thanks to base change we can even work in the group of $\mathbf{K}_s$-points of the jacobian J of X.

We note also that Taylor expansion at P_0 defines an embedding of the function field $\mathbf{K}_s(X)$ inside the field of series in the local parameter π_0 at P_0. This embedding is compatible with the action of the Galois group $\mathrm{Gal}(\mathbf{K}_s/\mathbf{K})$.

The next task is more delicate: we need the L-function of X, that is the characteristic polynomial of the Frobenius. This polynomial can be computed in time polynomial in $p.g.n$ where n is the degree of $\mathbf{K}$ over the prime field. All the known efficient methods in this situation use p-adic theories. See Kato-Lubkin [20], Satoh [30], Mestre [25], Kedlaya [21], Lauder and Wan [24] among others. When p is large one uses the ℓ-adic method introduced by Schoof [31] and generalized by Pila [27] to compute the L-function in time polynomial in the logarithm of q for fixed genus g. Unfortunately the complexity in g of the ℓ-adic method is exponential. To summarize: if either the genus or the characteristic is small we can efficiently compute the L-function.

We will be interested in points c in $J(\mathbf{K}_s)$ such that $F_{\mathbf{K}}(c) = q.c$. These points are sometimes called *anti-rational*. Let c be such a non-zero point and let $m \geqslant 2$ be its order. So $m.c = 0$. Let $\mathbf{L}$ be an extension of $\mathbf{K}$ such that c is defined over $\mathbf{L}$. We denote $X_{\mathbf{L}}$ the base change of X from $\mathbf{K}$ to $\mathbf{L}$. Let C be a divisor on $X_{\mathbf{L}}$ in the class c. We can assume that P_0 is not in the support of C. The divisor $m.C$ is principal. Let R_c be the unique function having divisor $m.C$ and taking value 1 at P_0. Let r_c be the m-th root of R_c in $\mathbf{K}_s(\pi_0)$ having constant coefficient one.

When c runs over a set of generators of the group of antirational points in $J(\mathbf{K}_s)$, the corresponding functions r_c generate a finite extension of $\mathbf{K}_s(X)$ inside $\mathbf{K}_s((\pi_0))$. We consider the subfield fixed by the Frobenius $F_{\mathbf{K}}$ inside this extension. This field is the maximal abelian unramified extension of $\mathbf{K}(X)$ of degree prime to p and totally split over P_0.

REFERENCES

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

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

[3] Peter Bürgisser, Michael Clausen, and M. Amin Shokrollahi. *Algebraic complexity theory*, volume 315 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1997. With the collaboration of Thomas Lickteig.

[4] 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.

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

[6] James W. Cooley and John W. Tukey. An algorithm for the machine calculation of complex Fourier series. *Math. Comp.*, 19:297–301, 1965.

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

[8] Jean-Marc Couveignes and Jean Gasnier. Explicit Riemann-Roch spaces in the Hilbert class field. In *Arithmetic, geometry, cryptography and coding theory. 19th international conference, AGC2T, Centre International de Rencontres Mathématiques, Marseille, France, June 5–9, 2023*, pages 37–65. Providence, RI: American Mathematical Society (AMS), 2026.

[9] Jean-Marc Couveignes and Reynald Lercier. Elliptic periods for finite fields. *Finite Fields Appl.*, 15(1):1–22, 2009.

[10] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941.

[11] 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.

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

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

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

[15] David Harvey and Joris van der Hoeven. Polynomial multiplication over finite fields in time \(O (n \log n) \). *J. ACM*, 69(2):12:1–12:40, 2022.
[16] David Harvey, Joris van der Hoeven, and Grégoire Lecerf. Faster polynomial multiplication over finite fields. *J. ACM*, 63(6):52:1–52:23, 2017.
[17] 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.
[18] Michael T. Heideman, Don H. Johnson, and C. Sidney Burrus. Gauss and the history of the fast Fourier transform. *Arch. Hist. Exact Sci.*, 34:265–277, 1985.
[19] 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.
[20] Goro C. Kato and Saul Lubkin. Zeta matrices of elliptic curves. *J. Number Theory*, 15(3):318–330, 1982.
[21] Kiran S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.*, 16(4):323–338, 2001.
[22] L. Kronecker. Grundzüge einer arithmetischen Theorie der algebraischen Grössen. (Festschrift zu Herrn Ernst Eduard Kummers fünfzigjährigem Doctor-Jubiläum, 10 September 1881). *J. Reine Angew. Math.*, 92:1–122, 1882.
[23] Gilles Lachaud. Les codes géométriques de Goppa. In *Astérisque*, volume 133-134, pages 189–207. 1986. Seminar Bourbaki, 1984/85, exp. 641.
[24] 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.
[25] J.-F. Mestre. Lettre adressée à Gaudry et Harley. https://webusers.imj-prg.fr/~jean-francois.mestre/, december 2010.
[26] S. Nakajima. On Galois module structure of the cohomology groups of an algebraic variety. *Invent. Math.*, 75:1–8, 1984.
[27] 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.
[28] Hugues Randriambololona. Bilinear complexity of algebras and the Chudnovsky-Chudnovsky interpolation method. *J. Complexity*, 28(4):489–517, 2012.
[29] Michael Rosen. The Hilbert class field in function fields. *Exposition. Math.*, 5(4):365–378, 1987.
[30] 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.
[31] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, 44(170):483–494, 1985.
[32] Jean-Pierre Serre. *Algebraic groups and class fields*, volume 117 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1988.
[33] Mohammad Amin Shokrollahi. Optimal algorithms for multiplication in certain finite fields using elliptic curves. *SIAM J. Comput.*, 21(6):1193–1198, 1992.
[34] 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.
[35] Alexandre Soro and Jérôme Lacan. FNT-based Reed-Solomon erasure codes. In *7th IEEE Consumer Communications and Networking Conference, CCNC 2010, Las Vegas, NV, USA, January 9-12, 2010*, pages 1–5. IEEE, 2010.
[36] 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.
[37] Jacques Vélu. Courbes elliptiques munies d'un sous-groupe $\mathbb{Z}/n\mathbb{Z} \times \mu_n$. *Bull. Soc. Math. Fr., Suppl., Mém.*, 57:152, 1978.
[38] Joachim von zur Gathen and Jürgen Gerhard. *Modern Computer Algebra (3. ed.)*. Cambridge University Press, 2013.
[39] William C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, 2:521–560, 1969.
[40] 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

REYNALD LERCIER, DGA & UNIV. RENNES, CNRS, IRMAR - UMR 6625, F-35000 RENNES, FRANCE.
Email address: reynald.lercier@univ-rennes.fr