HAL open science

The equivariant complexity of multiplication in finite field extensions

Jean-Marc Couveignes, Tony Ezome

▶ To cite this version:

Jean-Marc Couveignes, Tony Ezome. The equivariant complexity of multiplication in finite field extensions. Journal of Algebra, 2023, 622, pp.694-720. 10.1016/j.jalgebra.2023.01.022 . hal-03410146v2

HAL Id: hal-03410146
https://hal.science/hal-03410146v2

Submitted on 11 Jan 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

THE EQUIVARIANT COMPLEXITY OF MULTIPLICATION IN FINITE FIELD EXTENSIONS

JEAN-MARC COUVEIGNES AND TONY EZOME

ABSTRACT. We study the complexity of multiplication of two elements in a finite field extension given by their coordinates in a normal basis. We show how to control this complexity using the arithmetic and geometry of algebraic curves.

CONTENTS

1. Introduction 2
2. Various complexities 3
3. Algebraic complexity of a bilinear map 4
4. Equivariant algebraic complexity 5
5. General upper bounds 6
6. The complexity of multiplication in finite fields 7
7. The algebra $\mathbf{K}[x]/x^n$ 8
8. The equivariant complexity of multiplication in finite fields 8
9. Semi-simple algebras over finite fields 9
10. Extension of scalars I 9
11. Extension of scalars II 10
12. A geometric construction 10
13. A general bound 12
14. Non-special divisors 13
15. Elliptic curves 14
16. An asymptotic bound 15
17. Bounding $\nu_q^{sym}(n)$ 16
18. The case $q = 7$ and $n = 5$ 17
19. The case $q = 11$ and $n = 239$ 18
20. The case $q = 13$ and $n = 4639$ 20
21. Remarks and questions 21
References 22

Date: December 30, 2022.

1. Introduction

Let $\mathbf{K}$ be a finite field of cardinality q. Let $\mathbf{L}/\mathbf{K}$ be a finite field extension of degree n. Given a normal $\mathbf{K}$-basis $\mathcal{B}$ of $\mathbf{L}$ we can represent elements in $\mathbf{L}$ by their coordinates in $\mathcal{B}$. Exponentiation by q then corresponds to a cyclic shift of coordinates and can be computed at almost no cost. It is a natural concern in this context to bound the computational complexity of computing the product of two elements of $\mathbf{L}$ given by their coordinates in $\mathcal{B}$. There is a rich litterature about constructing normal bases where the cost of multiplication is as small as possible. See [10] for a survey. In this work we define and study the symmetric equivariant complexity $\nu_q^{sym}(n)$ of multiplication in the finite field extension $\mathbf{L}/\mathbf{K}$. This is the Galois equivariant counterpart to the symmetric bilinear complexity $\mu_q^{sym}(n)$. It is the size of the smallest decomposition of the multiplication tensor as a sum of pure equivariant tensors. This is an invariant of the field extension $\mathbf{L}/\mathbf{K}$ in the sense that it only depends on q and n. While the symmetric bilinear complexity $\mu_q^{sym}(n)$ partially controls the cost of multiplication in $\mathbf{L}$ (it only accounts for bilinear operations), in contrast, the symmetric equivariant complexity $\nu_q^{sym}(n)$ provides an asymptotic estimate for the total cost of multiplication in any normal basis: the linear part of the calculation consists of $3\nu_q^{sym}(n)$ convolution products, each of them beeing computed at the expense of $O(n\log(n)|\log(\log(n))|)$ operations in $\mathbf{K}$. We are interested in proving upper bounds for $\nu_q^{sym}(n)$. For example we prove that $\nu_q^{sym}(n)$ is bounded by a constant times $\lceil \log_q n \rceil$ in full generality. This implies that multiplication in any normal basis requires no more than $n(\log n)^{2+o(1)}$ operations in $\mathbf{K}$. We also provide methods to bound $\nu_q^{sym}(n)$ for given q and n.

Section 2 is a quick tour of various definitions of complexity in the context of multiplication in finite field extensions. In Section 3 we recall the elementary properties of the algebraic complexity of a bilinear map. We introduce in Section 4 the equivariant complexity of a C-equivariant bilinear map, where C is a given finite group. We prove in Section 5 an inequality between the equivariant complexity of a C-equivariant bilinear map and the bilinear complexity of its coordinates. Sections 6 and 7 recall classical results about the bilinear complexity of multiplication in finite field extensions and truncated power series algebras. The Galois equivariant complexity of multiplication in finite field extensions is introduced in Section 8. A useful generalization to semi-simple algebras is introduced in Section 9. The effect of extension and restriction of scalars on (equivariant) complexities is studied in Sections 10 and 11. We present in Section 12, 13, and 14 a general geometric recipe to bound from above the Galois equivariant complexity of multiplication in a finite extension $\mathbf{L}/\mathbf{K}$ of finite fields. We first construct a cyclic cover $\rho : Y \to X$ between two $\mathbf{K}$-curves, then realise $\mathbf{L}/\mathbf{K}$ as the residual algebra of the fiber of ρ above some rational point on X. Evaluation and interpolation on Y naturally produce $\mathbf{K}[C]$-linear maps. In the special case when X and Y are elliptic curves our construction generalizes the one presented in [8]. The Chudnovsky's method [7, 17, 2, 6, 13] to bound $\mu_q^{sym}(n)$ relies on the existence of families of curves having an increasing number of rational points while the genus is bounded by a constant times the number of points. Our construction requires Jacobians of smallest possible dimension having a point of given order. In Sections 15 and 16 we enhance the specific case when Y and X both have genus one. Although this special case is not optimal (because we lack rational points on elliptic curves when q is small compared to n) we have enough control on the group of points on an elliptic curve to prove a satisfactory asympotic statement, using the general

properties of equivariant complexity established in Sections 5, 8, 11. In Section 17 we explain how to better bound $\nu_q^{sym}(n)$ for given q and n using the construction of Section 12. We experiment with three examples in Sections 18, 19, 20. These examples illustrate how the knowledge of special linear series on low genus curves helps bounding $\nu_q^{sym}(n)$ at a minimal computational cost. We conclude in Section 21 with remarks and questions.

This study has been carried out with financial support from the French State, managed by CNRS in the frame of the *Dispositif de Soutien aux Collaborations avec l'Afrique subsaharienne* and by the French National Research Agency (ANR) in the frame of the Programmes CIAO (ANR-19-CE48-0008), FLAIR (ANR-17-CE40-0012 ANR-10-IDEX-03-02) and CLap-CLap (ANR-18-CE40-0026), and by the Simons foundation.

Experiments presented in this paper were carried out using the PlaFRIM experimental testbed, supported by Inria, CNRS (LABRI and IMB), Université de Bordeaux, Bordeaux INP and Conseil Régional d'Aquitaine (see `https://www.plafrim.fr/`).

We thank the referee for his useful comments.

2. Various complexities

There are several notions of complexity in the context of multiplication in a degree n extension $\mathbf{L}/\mathbf{K}$ of finite fields. We assume that we are given a basis $\mathcal{B}$ and the coordinates of the two operands in $\mathcal{B}$. The output consists of the coordinates of the product in the basis $\mathcal{B}$.

In the computational model of straight line programs, one may count all arithmetic operations in $\mathbf{K}$: additions, subtractions, multiplications. Another option is to omit additions, subtractions, and multiplications by a constant in $\mathbf{K}$. One then only counts multiplications of two registers. This can be justified if the number of additions, subtractions and multiplications by a constant, is of the same order of magnitude as the number of multiplications.

In a more algebraic setting one may count the non-zero coordinates of the multiplication tensor in the basis $\hat{\mathcal{B}} \otimes \hat{\mathcal{B}} \otimes \mathcal{B}$. When $\mathcal{B}$ is a normal basis, this number can be written $n \times C_{\mathcal{B}}$ where $C_{\mathcal{B}}$ is an integer often called the complexity of the normal basis $\mathcal{B}$. It was shown by Mullin, Onyszchuk, Vanstone and Wilson [12] that $C_{\mathcal{B}}$ is at least $2n-1$. This means that if we only allow products between the coordinates of the inputs (no intermediate result) the number of arithmetic operations is at least quadratic in n, and most of the time even cubic. This is a rather pessimistic model that is well adapted to low capacity computing devices.

A more intrinsic algebraic approach is to define the bilinear complexity of multiplication in $\mathbf{L}/\mathbf{K}$ as the rank r of the multiplication tensor. The rank is independent of the basis. Given a decomposition of the multiplication tensor as a sum of r pure tensors, we can compute products at the expense of r multiplications between two registers, $3rn$ multiplications by a constant, and $3r(n-1)$ additions. According to Chudnovsky and Chudnovsky, r is bounded by a constant times n. But this says little about the cost of the linear part of the algorithm, since the bound $3rn$ is quadratic in n.

We define in Sections 4 and 8 the equivariant algebraic complexity of multiplication in $\mathbf{L}/\mathbf{K}$. The underlying idea is to stick to the intrinsic algebraic approach but restrict the linear part of the algorithm to Galois equivariant linear forms : convolution products in the algebra of the

Galois group. Respecting the symmetries of the problem is a natural restriction in view of the importance of convolution products in fast arithmetic. See [11, 19, 9].

3. Algebraic complexity of a bilinear map

We recall standard definitions about complexity of bilinear maps. A complete introduction can be found in [4][Chapter 14]. Let $\mathbf{K}$ be a commutative field. Let V and W be two finite dimensional $\mathbf{K}$-vector spaces. Let

$$t : V \times V \to W$$

be a $\mathbf{K}$-bilinear map. We let $\hat{V}$ be the dual of V. For ϕ_1, ϕ_2 in $\hat{V}$ and w in W we define the bilinear map

$$\begin{array}{rcl} \pi_{w,\phi_1,\phi_2} & : & V \times V \longrightarrow W \\ & & (v_1, v_2) \longmapsto \phi_1(v_1)\phi_2(v_2)w \end{array}$$

and we say that π_{w,ϕ_1,ϕ_2} is a **pure** bilinear map.

If $\phi_1 = \phi_2 = \phi$ we write $\pi_{w,\phi}$ for $\pi_{w,\phi,\phi}$ and call $\pi_{w,\phi}$ a **pure symmetric** bilinear map. For t a $\mathbf{K}$-bilinear map we define the **bilinear complexity** $R_{\mathbf{K}}(t)$ of t to be the smallest integer such that t is the sum of $R_{\mathbf{K}}(t)$ pure bilinear maps. In case t is symmetric we define the **symmetric complexity** $S_{\mathbf{K}}(t)$ of t to be the smallest integer such that t is the sum of $S_{\mathbf{K}}(t)$ pure symmetric bilinear maps. Equivalently $S_{\mathbf{K}}(t)$ is the smallest integer k such that there exist two $\mathbf{K}$-linear maps

$$\top : V \to \mathbf{K}^k \quad \text{and} \quad \bot : \mathbf{K}^k \to W$$

such that

$$t(l_1, l_2) = \bot(\top(l_1) \bullet_k \top(l_2))$$

where the $\bullet_k$ between $\top(l_1)$ and $\top(l_2)$ stands for the componentwise product in $\mathbf{K}^k$.

The vector space of bilinear maps has a basis consisting of pure bilinear maps. So any bilinear map $t : V \times V \to W$ has complexity

$$R_{\mathbf{K}}(t) \leqslant \dim W \times (\dim V)^2.$$

The vector space of symmetric bilinear maps has a basis consisting of $\dim V \times \dim W$ pure symmetric bilinear maps and $\dim V \times (\dim V - 1)/2 \times \dim W$ maps of the form

$$\pi_{w,\phi_1,\phi_2} + \pi_{w,\phi_2,\phi_1} = \pi_{w,\phi_1+\phi_2} - \pi_{w,\phi_1} - \pi_{w,\phi_2}.$$

So any symmetric bilinear map $t : V \times V \to W$ has symmetric complexity

$$S_{\mathbf{K}}(t) \leqslant \dim W \times (\dim V) \times (3 \dim V - 1)/2.$$

If $t_1 : V_1 \times V_1 \to W_1$ and $t_2 : V_2 \times V_2 \to W_2$ are two symmetric $\mathbf{K}$-bilinear map, we say that t_2 is a **restriction** of t_1 if there exist two $\mathbf{K}$-linear maps $\top : V_2 \to V_1$ and $\bot : W_1 \to W_2$ such that $t_2 = \bot \circ t_1 \circ (\top \times \top)$. It follows that $S_{\mathbf{K}}(t_2) \leqslant S_{\mathbf{K}}(t_1)$. In case the maps $\top$ and $\bot$ are bijective we say that t_1 and t_2 are **isomorphic**.

4. Equivariant algebraic complexity

Let C be a finite group of order n. Let $\mathbf{K}$ be a commutative field. Let $\mathbf{K}[C]$ be the group algebra. We denote

$$\begin{array}{rcl} \star & : & \mathbf{K}[C]\times\mathbf{K}[C] \longrightarrow \mathbf{K}[C] \\ & & (\sum_{c\in C} a_c.c, \sum_{c\in C} b_c.c) \longmapsto \sum_{c\in C}\sum_{\substack{c_1,c_2\in C\\ c_1c_2=c}} (a_{c_1}b_{c_2}).c \end{array}$$

the (convolution) product in $\mathbf{K}[C]$. Considering the coefficients $(a_c)_{c\in C}$ in $\sum_{c\in C} a_c.c$ as a map $a : C \to \mathbf{K}$ we obtain a natural isomorphism of $\mathbf{K}$-vector spaces

$$\begin{array}{rcl} \mathbf{K}[C] & \longrightarrow & \mathrm{Hom}(C,\mathbf{K}) \\ \sum_{c\in C} a_c.c & \longmapsto & (c\mapsto a_c). \end{array}$$

between the group algebra $\mathbf{K}[C]$ and the algebra $\mathrm{Hom}(C,\mathbf{K})$ of maps from C to $\mathbf{K}$. Through this identification the group algebra inherits a componentwise product

$$\begin{array}{rcl} \diamond & : & \mathbf{K}[C]\times\mathbf{K}[C] \longrightarrow \mathbf{K}[C] \\ & & (\sum_{c\in C} a_c.c, \sum_{c\in C} b_c.c) \longmapsto \sum_{c\in C}(a_cb_c).c \end{array}$$

For any positive integer k we denote $\diamond_k$ the map

$$\begin{array}{rcl} \diamond_k & : & (\mathbf{K}[C])^k\times(\mathbf{K}[C])^k \longrightarrow (\mathbf{K}[C])^k \\ & & ((a_i)_{1\leqslant i\leqslant k},(b_i)_{1\leqslant i\leqslant k}) \longmapsto (a_i\diamond b_i)_{1\leqslant i\leqslant k} \end{array}$$

If L and M are two finitely generated left $\mathbf{K}[C]$-modules, we say that a $\mathbf{K}$-bilinear map

$$t : L\times L\to M$$

is a C-**equivariant bilinear map** if

$$t(c\cdot l_1, c\cdot l_2) = c\cdot t(l_1,l_2)$$

for any l_1, l_2 in L and c in C. If α_1 and α_2 are two $\mathbf{K}[C]$-linear maps from L to $\mathbf{K}[C]$, and if m is a vector in M, we define the C-equivariant $\mathbf{K}$-bilinear map

$$\begin{array}{rcl} \gamma_{m,\alpha_1,\alpha_2} & : & L\times L \longrightarrow M \\ & & (l_1,l_2) \longmapsto (\alpha_1(l_1)\diamond\alpha_2(l_2)).m \end{array}$$

We say that $\gamma_{m,\alpha_1,\alpha_2}$ is a **pure** C-**equivariant** $\mathbf{K}$-bilinear map. If $\alpha_1 = \alpha_2 = \alpha$ we write $\gamma_{m,\alpha}$ for $\gamma_{m,\alpha,\alpha}$ and call $\gamma_{m,\alpha}$ a **pure symmetric** C-**equivariant** $\mathbf{K}$-bilinear map. For t a C-equivariant $\mathbf{K}$-bilinear map we define the **equivariant complexity** of t to be the smallest integer $R_{\mathbf{K},C}(t)$ such that t is the sum of $R_{\mathbf{K},C}(t)$ pure C-equivariant maps. In case t is symmetric we define the **symmetric equivariant complexity** of t to be the smallest integer $S_{\mathbf{K},C}(t)$ such that t is the sum

of $S_{\mathbf{K},C}(t)$ pure symmetric C-equivariant $\mathbf{K}$-bilinear maps. Equivalently $S_{\mathbf{K},C}(t)$ is the smallest integer k such that there exist two $\mathbf{K}[C]$-linear maps

$$\top : L \to (\mathbf{K}[C])^k \quad \text{and} \quad \bot : (\mathbf{K}[C])^k \to M$$

such that

$$t(l_1, l_2) = \bot(\top(l_1) \diamond_k \top(l_2)).$$

If $t_1 : L_1 \times L_1 \to M_1$ and $t_2 : L_2 \times L_2 \to M_2$ are two symmetric $\mathbf{K}$-bilinear C-equivariant maps, we say that t_2 is a **restriction** of t_1 if there exist two $\mathbf{K}[C]$-linear maps $\top : L_2 \to L_1$ and $\bot : M_1 \to M_2$ such that $t_2 = \bot \circ t_1 \circ (\top \times \top)$. It follows that $S_{\mathbf{K},C}(t_2) \leqslant S_{\mathbf{K},C}(t_1)$. In case the maps $\top$ and $\bot$ are bijective we say that t_1 and t_2 are **isomorphic**.

5. General upper bounds

Let C be a finite group of order n. Let e be the identity element in C. Let M be a left $\mathbf{K}[C]$-module. We let

$$\hat{M} = \mathrm{Hom}_{\mathbf{K}}(M, \mathbf{K})$$

be the dual of M as a $\mathbf{K}$-vector space. Let

$$\check{M} = \mathrm{Hom}_{\mathbf{K}[C]}(M, \mathbf{K}[C])$$

be the dual of M as a $\mathbf{K}[C]$-module. For any ϕ in $\check{M}$ and m in M we write

$$\phi(m) = \sum_{c \in C} \phi_c(m).c$$

and thus define n coordinate forms $(\phi_c)_{c \in C}$ in $\hat{M}$. We check that

$$\phi_c(m) = \phi_e(c^{-1}.m)$$

so the $\mathbf{K}$-linear map

$$\begin{aligned} \check{M} &\longrightarrow \hat{M} \\ \phi &\longmapsto \phi_e \end{aligned}$$

is an isomorphism of $\mathbf{K}$-vector spaces. For every ψ in $\hat{M}$ we write ψ^C for the corresponding element in $\check{M}$. So

$$\psi^C(m) = \sum_{c \in C} \psi(c^{-1}.m)c.$$

We now let L and M be two finitely generated $\mathbf{K}[C]$-module. We assume that M is free. So there exists a $\mathbf{K}$-vector space W such that

$$M = \bigoplus_{c \in C} c.W$$

as a $\mathbf{K}$-vector space. Let $t : L \times L \to M$ be a C-equivariant $\mathbf{K}$-bilinear map. There are n maps $(t_c)_{c \in C}$ such that $t_c : L \times L \to W$ is $\mathbf{K}$-bilinear for every c in C and for x and y in L we have

$$t(x, y) = \sum_{c \in C} c.t_c(x, y).$$

We check that

$$t_c(x,y) = t_e(c^{-1}.x, c^{-1}.y)$$

for every $c \in C$ and x, y in L. The map

$$\begin{array}{ccc} \mathrm{Bil}_C(L,M) & \longrightarrow & \mathrm{Bil}_{\mathbf{K}}(L,W) \\ t & \longmapsto & t_e \end{array}$$

is thus an isomorphism between the $\mathbf{K}$-vector space $\mathrm{Bil}_C(L,M)$ of C-equivariant $\mathbf{K}$-bilinear maps from $L \times L$ to M, and the space $\mathrm{Bil}_{\mathbf{K}}(L,W)$ of $\mathbf{K}$-bilinear maps from $L \times L$ to W. For every u in $\mathrm{Bil}_{\mathbf{K}}(L,W)$ we write u^C the corresponding map in $\mathrm{Bil}_C(L,M)$. So

$$u^C(x,y) = \sum_{c \in C} c.u(c^{-1}.x, c^{-1}.y).$$

Let α_1 and α_2 in $\check{L}$. Let $(\alpha_{1,c})_{c \in C}$ be the n forms in $\hat{L}$ such that

$$\alpha_1(l) = \sum_{c \in C} \alpha_{1,c}(l).c$$

for every l in L. We similarly define n forms $(\alpha_{2,c})_{c \in C}$ in $\hat{L}$. Let $w \in W$ and let $t = \gamma_{w,\alpha_1,\alpha_2}$. Then for l_1 and l_2 in L we have

$$t(l_1,l_2) = (\alpha_1(l_1) \diamond \alpha_2(l_2)).w = \sum_{c \in C} \alpha_{1,c}(l_1)\alpha_{2,c}(l_2)c.w.$$

We deduce

$$t_e(l_1,l_2) = \alpha_{1,e}(l_1)\alpha_{2,e}(l_2)w \quad \text{so} \quad t_e = \pi_{w,\alpha_{1,e},\alpha_{2,e}}.$$

Equivalently, if β_1 and β_2 are in $\hat{L}$ and w is in W we have

$$\pi^C_{w,\beta_1,\beta_2} = \gamma_{w,\beta_1^C,\beta_2^C}.$$

We deduce that if L and M are $\mathbf{K}[C]$-modules with M free, and if $t : L \times L \to M$ is a C-equivariant bilinear map, then every decomposition of t_e as a sum of k pure $\mathbf{K}$-bilinear maps results in a decomposition of t as a sum of k pure C-equivariant $\mathbf{K}$-bilinear maps. So

$$R_{\mathbf{K},C}(t) \leqslant R_{\mathbf{K}}(t_e) \leqslant \mathrm{rank}(M) \times (\dim_{\mathbf{K}}(L))^2.$$

And in case t is symmetric

$$S_{\mathbf{K},C}(t) \leqslant S_{\mathbf{K}}(t_e) \leqslant \mathrm{rank}(M) \times \dim_{\mathbf{K}}(L) \times (3\dim_{\mathbf{K}}(L) - 1)/2. \tag{1}$$

6. The complexity of multiplication in finite fields

Let $\mathbf{K}$ be a finite field with q elements and let $\mathbf{L}$ be a degree $n \geqslant 1$ field extension of $\mathbf{K}$. The multiplication map $\times_{\mathbf{L}} : \mathbf{L} \times \mathbf{L} \to \mathbf{L}$ is $\mathbf{K}$-bilinear and symmetric. Its bilinear complexity $R_{\mathbf{K}}(\times_{\mathbf{L}})$ is usually denoted $\mu_q(n)$ and its symmetric bilinear complexity $S_{\mathbf{K}}(\times_{\mathbf{L}})$ is denoted $\mu_q^{sym}(n)$. It is known that $\mu_q^{sym}(n) \geqslant 2n-1$. See [13, Lemma 1.9.] for example. Lagrange interpolation shows that $\mu_q^{sym}(n) = 2n-1$ when $q \geqslant 2n-2$. Chudnovsky and Chudnovsky have proved [7] linear upper bounds for these bilinear complexities using interpolation on algebraic curves. Their method has been extensively studied and improved, notably by Shparlinski, Tsfasmann, Vladut [17], Shokrollahi [16], Ballet and Rolland [2, 3], Chaumine [6], Randriambololona [13] and

others, achieving sharper and sharper upper bounds for the bilinear complexity of multiplication in finite extensions of finite fields. See [1] for a recent survey. We will use the following theorem.

Theorem 1 (Chudnovsky (1987), Shparlinski, Tsfasmann and Vladut (1992), Ballet (1999))**.** *There exists an effective absolute constant $\mathcal{Q}$ such that $\mu_q^{sym}(n) \leqslant \mathcal{Q}n$ for all $n \geqslant 1$ and all prime power q.*

7. The algebra $\mathbf{K}[x]/x^n$

Let $\mathbf{K}$ be a field with q elements. Let $n \geqslant 1$ be an integer. Let $\mathbf{L}$ be a degree $2n-1$ field extension of $\mathbf{K}$. Let $\mathbf{K}[x]_{n-1}$ be the $\mathbf{K}$-vector space of polynomials with degree $\leqslant n-1$. The multiplication map $\mathbf{K}[x]_{n-1} \times \mathbf{K}[x]_{n-1} \to \mathbf{K}[x]_{2n-2}$ is a restriction of the multiplication map $\mathbf{L} \times \mathbf{L} \to \mathbf{L}$. And the multiplication map $\mathbf{K}[x]/x^n \times \mathbf{K}[x]/x^n \to \mathbf{K}[x]/x^n$ is a restriction of $\mathbf{K}[x]_{n-1} \times \mathbf{K}[x]_{n-1} \to \mathbf{K}[x]_{2n-2}$. So the symmetric bilinear complexity of multiplication in the quotient $\mathbf{K}[x]/x^n$ is bounded from above by $\mu_q^{sym}(2n-1)$. So

$$S_{\mathbf{K}}(\times : \mathbf{K}[x]/x^n \times \mathbf{K}[x]/x^n \to \mathbf{K}[x]/x^n) \leqslant \mathcal{Q}n \tag{2}$$

for some effective absolute constant $\mathcal{Q}$.

In case $q \geqslant 2n-2$, Lagrange interpolation shows that the symmetric bilinear complexity of $\mathbf{K}[x]_{n-1} \times \mathbf{K}[x]_{n-1} \to \mathbf{K}[x]_{2n-2}$ is $\leqslant 2n-1$. So the symmetric bilinear complexity of multiplication in $\mathbf{K}[x]/x^n$ is $\leqslant 2n-1$ in that case. In the other direction, Winograd has proved in [20] that this complexity is always $\geqslant 2n-1$. More precise, more general and stronger statements can be found in [4, 2, 13] and [1, Section 2].

8. The equivariant complexity of multiplication in finite fields

Let $\mathbf{K}$ be a finite field with q elements and let $\mathbf{L}$ be a degree $n \geqslant 1$ field extension of $\mathbf{K}$. Let C be the Galois group of $\mathbf{L}/\mathbf{K}$. Then $\mathbf{L}$ is a free $\mathbf{K}[C]$-module of rank one. We denote

$$\times_{\mathbf{K},n} : \mathbf{L} \times \mathbf{L} \to \mathbf{L}$$

the multiplication map in $\mathbf{L}$. This is a C-equivariant $\mathbf{K}$-bilinear map. We define $\nu_q(n)$ to be the C-equivariant complexity of $\times_{\mathbf{K},n}$ over $\mathbf{K}$. We similarly define $\nu_q^{sym}(n)$ to be the C-equivariant symmetric complexity of $\times_{\mathbf{K},n}$ over $\mathbf{K}$.

The equivariant complexity $\nu_q^{sym}(n)$ controls the computational difficulty of multiplying two elements in $\mathbf{L}$ given by their coordinates in a normal basis. Indeed assume that $\nu_q^{sym}(n) = \sigma$. There exist two $\mathbf{K}[C]$-linear maps

$$\top : \mathbf{L} \to (\mathbf{K}[C])^\sigma \quad \text{and} \quad \perp : (\mathbf{K}[C])^\sigma \to \mathbf{L}$$

such that

$$l_1 \times l_2 = \perp(\top(l_1) \diamond_\sigma \top(l_2)) \tag{3}$$

for any l_1, l_2 in $\mathbf{L}$. We note that $\top$ is a linear map between two free $\mathbf{K}[C]$-modules of respective ranks 1 and σ. Once chosen a basis of $\mathbf{L}$ we can describe $\top$ by a $\sigma \times 1$ matrix with coefficients in $\mathbf{K}[C]$. Giving a basis of $\mathbf{L}$ as a $\mathbf{K}[C]$-module boils down to choosing a normal basis of $\mathbf{L}/\mathbf{K}$. Similarly $\perp$ can be described by a $1 \times \sigma$ matrix with coefficients in $\mathbf{K}[C]$. So using Equation (3)

we compute the product of two elements in $\mathbf{L}$ given by their coordinates in a given normal basis in three steps:

1. Apply $\top$ to each element.
2. Multiply the two elements thus obtained in $\mathbf{K}[C]^\sigma$ using the $\diamond_\sigma$ law.
3. Apply $\perp$ to the result.

The first step requires twice σ multiplications in $\mathbf{K}[C]$. We note that multiplication in $\mathbf{K}[C]$ is the standard convolution product. The second step is a $\diamond_\sigma$ product between two vectors in $\mathbf{K}[C]^\sigma$. The third step requires σ multiplications in $\mathbf{K}[C]$. The only bilinear step is the second one. All the multiplications in the first and third steps involve a variable and a constant. The total cost (omitting additions) is 3σ convolution products between vectors of length n and σn multiplications in $\mathbf{K}$. According to work by Schönhage and Strassen [14] and Cantor and Kaltofen [5], convolution products of length $n \geqslant 2$ over an arbitrary commutative ring can be computed at the expense of $O(n\log(n)|\log(\log(n))|)$ operations in this ring. See also [19, Theorem 8.23]. Note in particular that it is not necessary to have n-th roots of unity in the base ring in order to compute convolution products efficiently.

9. Semi-simple algebras over finite fields

Let $\mathbf{K}$ be a finite field with q elements. Let $n_1 \geqslant 1$ be an integer. Let $\mathbf{L}$ be a degree n_1 extension of $\mathbf{K}$. Let $F_q : \mathbf{L} \to \mathbf{L}$ be the Frobenius automorphism of $\mathbf{L}/\mathbf{K}$. Let $n_2 \geqslant 1$ be an integer. Set $\mathbf{M} = \mathbf{L}^{n_2}$. This is a semisimple $\mathbf{K}$-algebra of degree $n = n_1 n_2$. We define an automorphism of $\mathbf{M}$ over $\mathbf{K}$ by sending $(x_0, x_1, \ldots, x_{n_2-1})$ onto $(x_1, x_2, \ldots, x_{n_2-1}, F_q(x_0))$. We call C the group generated by this automorphism. This is a cyclic group of order n. And $\mathbf{M}$ is a free $\mathbf{K}[C]$-module of rank 1. We let

$$\times_{\mathbf{K},n_1,n_2} : \mathbf{M} \times \mathbf{M} \to \mathbf{M}$$

be the multiplication map in $\mathbf{M}$. This is a symmetric C-equivariant $\mathbf{K}$-bilinear map. We denote $\nu_q^{sym}(n_1, n_2)$ its symmetric equivariant complexity.

10. Extension of scalars I

Let $\mathbf{K}$ be a commutative field. Let V and W be two finite dimensional $\mathbf{K}$-vector spaces. Let $t : V \times V \to W$ be a symmetric $\mathbf{K}$-bilinear map. Let $S_{\mathbf{K}}(t)$ be the symmetric bilinear complexity of t. Let $\mathbf{L}$ be a finite field extension of $\mathbf{K}$. We set $V_{\mathbf{L}} = V \otimes_{\mathbf{K}} \mathbf{L}$, $W_{\mathbf{L}} = W \otimes_{\mathbf{K}} \mathbf{L}$, $t_{\mathbf{L}} = t \otimes_{\mathbf{K}} \mathbf{L}$. Let $S_{\mathbf{L}}(t_{\mathbf{L}})$ be the symmetric bilinear complexity of $t_{\mathbf{L}}$ as an $\mathbf{L}$-bilinear map. We have

$$S_{\mathbf{L}}(t_{\mathbf{L}}) \leqslant S_{\mathbf{K}}(t). \tag{4}$$

We denote by $S_{\mathbf{K}}(\times_{\mathbf{L}})$ the symmetric $\mathbf{K}$-bilinear complexity of $\times_{\mathbf{L}} : \mathbf{L} \times \mathbf{L} \to \mathbf{L}$, the multiplication map in $\mathbf{L}$ seen as a $\mathbf{K}$-bilinear map. According to [13, Lemma 1.10]

$$S_{\mathbf{K}}(t) \leqslant S_{\mathbf{L}}(t_{\mathbf{L}}) \times S_{\mathbf{K}}(\times_{\mathbf{L}}). \tag{5}$$

11. Extension of scalars II

We now study the effect of extension of scalars on equivariant bilinear maps. The main motivation for extending scalars is to increase the number of rational points in the context of the geometric methods presented in Section 12. Let C be a finite group of order n. Let $\mathbf{K}$ be a commutative field. Let L and M be two finitely generated $\mathbf{K}[C]$-modules. Let $t : L \times L \to M$ be a symmetric C-equivariant $\mathbf{K}$-bilinear form. We denote $S_{\mathbf{K},C}(t)$ the symmetric equivariant complexity of t.

Let $\mathbf{L}$ be a finite field extension of $\mathbf{K}$. We set $L_{\mathbf{L}} = L \otimes_{\mathbf{K}} \mathbf{L}$, $M_{\mathbf{L}} = M \otimes_{\mathbf{K}} \mathbf{L}$, $t_{\mathbf{L}} = t \otimes_{\mathbf{K}} \mathbf{L}$. We call $S_{\mathbf{L},C}(t_{\mathbf{L}})$ the symmetric equivariant complexity of $t_{\mathbf{L}}$. We have

$$S_{\mathbf{L},C}(t_{\mathbf{L}}) \leqslant S_{\mathbf{K},C}(t). \tag{6}$$

Let $S_{\mathbf{K}}(\times_{\mathbf{L}})$ be the symmetric bilinear complexity of $\times_{\mathbf{L}} : \mathbf{L} \times \mathbf{L} \to \mathbf{L}$, as a $\mathbf{K}$-bilinear map. Then

$$S_{\mathbf{K},C}(t) \leqslant S_{\mathbf{L},C}(t_{\mathbf{L}}) \times S_{\mathbf{K}}(\times_{\mathbf{L}}). \tag{7}$$

Assume $\mathbf{K}$ is a finite field with q elements. Let $\mathbf{L}$ be a degree n field extension of $\mathbf{K}$. Let C be the Galois group of $\mathbf{L}/\mathbf{K}$. The multiplication $\times_{\mathbf{K},n} : \mathbf{L} \times \mathbf{L} \to \mathbf{L}$ is $\mathbf{K}$-bilinear symmetric and C-equivariant. Let $\mathbf{K}'$ be a degree m field extension of $\mathbf{K}$. We tensor product the multiplication $\times_{\mathbf{K},n}$ by $\mathbf{K}'$ over $\mathbf{K}$. The resulting C-equivariant $\mathbf{K}'$-bilinear map is isomorphic to $\times_{\mathbf{K}',n_1,n_2}$ as defined in Section 9, with

$$n_2 = \gcd(n, m) \quad \text{and} \quad n_1 = n/n_2.$$

Equations 6 and 7 thus imply

$$\nu_{q^m}^{sym}(n_1, n_2) \leqslant \nu_q^{sym}(n)$$

and

$$\nu_q^{sym}(n) \leqslant \nu_{q^m}^{sym}(n_1, n_2) \times \mu_q^{sym}(m). \tag{8}$$

12. A geometric construction

Let $\mathbf{K}$ be a finite field with q elements. We call p the characteristic of $\mathbf{K}$. Let Y be a smooth absolutely integral projective curve over $\mathbf{K}$. Let C be a cyclic group of $\mathbf{K}$-automorphisms of Y. We call n the cardinality of C. We assume that $n \geqslant 2$ and p does not divide n. We call X the quotient Y/C. This is a smooth absolutely integral projective curve over $\mathbf{K}$. We call $\rho : Y \to X$ the quotient map. Let $\mathfrak{r}$ be an effective divisor on Y. We assume that $\mathfrak{r}$ and $c.\mathfrak{r}$ are disjoint for every c in C. We set

$$R = \sum_{c \in C} c.\mathfrak{r}$$

and call $\mathbf{K}[R]$ the residue ring at R. We identify the ring $K[\mathfrak{r}]$ with the subring of $\mathbf{K}[R]$ consisting of functions vanishing at $c.\mathfrak{r}$ for every c in C different from e. As a $\mathbf{K}$-vector space

$$\mathbf{K}[R] = \bigoplus_{c \in C} c.\mathbf{K}[\mathfrak{r}].$$

So $\mathbf{K}[R]$ is a free $\mathbf{K}[C]$-module. The multiplication map $\mathbf{K}[\mathfrak{r}] \times \mathbf{K}[\mathfrak{r}] \to \mathbf{K}[\mathfrak{r}]$ is $\mathbf{K}$-bilinear and symmetric. We denote σ its symmetric bilinear complexity. According to Equation (1) this is an

upper bound for the C-equivariant symmetric complexity of $\mathbf{K}[R] \times \mathbf{K}[R] \to \mathbf{K}[R]$. So there exist two $\mathbf{K}[C]$-linear maps

$$\top : \mathbf{K}[R] \to \mathbf{K}[C]^\sigma \quad \text{and} \quad \bot : \mathbf{K}[C]^\sigma \to \mathbf{K}[R]$$

such that

$$l_1 \times l_2 = \bot(\top(l_1) \diamond_\sigma \top(l_2))$$

for $l_1, l_2 \in \mathbf{K}[R]$.

We denote $X(\mathbf{K})$ the set of $\mathbf{K}$-points on X. Let $a \in X(\mathbf{K})$ such that ρ is not ramified above a. Let n_1 be the inertial degree of ρ at a. Let $n_2 = n/n_1$. The fiber $B = \rho^{-1}(a)$ is a reduced $\mathbf{K}$-scheme consisting of n_2 irreducible components, each of degree n_1 above a. We call $\mathbf{M}$ the residue ring $\mathbf{K}[B]$ of B. This is a free $\mathbf{K}[C]$-module of rank 1. As a $\mathbf{K}$-bilinear symmetric C-equivariant map, the multiplication map in $\mathbf{M}$ is isomorphic to the map $\times_{\mathbf{K},n_1,n_2}$ introduced in Section 9. Its symmetric equivariant complexity is thus $\nu_q^{sym}(n_1, n_2)$.

Let D be a divisor on $X/\mathbf{K}$. We call $E = \rho^{-1}(D)$ the pullback of D on Y. Let ϵ be a local equation of D in a neighborhood of a and $\rho(R)$. Seen as a function on Y this is a local equation of E in a neighborhood of B and R. Let

$$\begin{array}{rcl} e_B & : & H^0(Y, \mathcal{O}_Y(E)) \longrightarrow \mathbf{M} \\ & & f \longmapsto (f \times \epsilon) \bmod B \end{array}$$

be the evaluation map at B. We similarly define

$$\begin{array}{rcl} e_B^2 & : & H^0(Y, \mathcal{O}_Y(2E)) \longrightarrow \mathbf{M} \\ & & f \longmapsto (f \times \epsilon^2) \bmod B \end{array}$$

These maps are morphisms of $\mathbf{K}[C]$-modules. For f_1 and f_2 in $H^0(Y, \mathcal{O}_Y(E))$ we have

$$e_B^2(f_1 \times f_2) = e_B(f_1) \times e_B(f_2).$$

We assume that e_B is surjective. Since p does not divide n, the ring $\mathbf{K}[C]$ is semi-simple. So the kernel of e_B is a direct factor. We deduce that e_B has a right inverse

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

which is $\mathbf{K}[C]$-linear. Let

$$\begin{array}{rcl} e_R & : & H^0(Y, \mathcal{O}_Y(E)) \longrightarrow \mathbf{K}[R] \\ & & f \longmapsto (f \times \epsilon) \bmod R \end{array}$$

and

$$\begin{array}{rcl} e_R^2 & : & H^0(Y, \mathcal{O}_Y(2E)) \longrightarrow \mathbf{K}[R] \\ & & f \longmapsto (f \times \epsilon^2) \bmod R \end{array}$$

be the evaluation maps at R. These are $\mathbf{K}[C]$-linear maps. We assume that e_R^2 is injective. Since the ring $\mathbf{K}[C]$ is semi-simple, the image of e_R^2 is a direct factor of $\mathbf{K}[R]$. We deduce the existence of a left inverse

$$e_R^\star : \mathbf{K}[R] \to H^0(Y, \mathcal{O}_Y(2E))$$

to the evaluation map e_R^2. Let s_1 and s_2 be two funtions in $H^0(Y, \mathcal{O}_Y(E))$, representing the two elements

$$e_B(s_1) = (s_1 \times \epsilon) \bmod B \quad \text{and} \quad e_B(s_2) = (s_2 \times \epsilon) \bmod B$$

in $\mathbf{M}$. The product $s_3 = s_1 s_2$ belongs to $H^0(Y, \mathcal{O}_Y(2E))$ and

$$e_R^2(s_3) = e_R(s_1) \times e_R(s_2) \in \mathbf{K}[R].$$

So

$$s_3 = e_R^\star(e_R(s_1) \times e_R(s_2)) = e_R^\star(\perp(\top(e_R(s_1)) \diamond_\sigma \top(e_R(s_2))))$$

and the $\mathbf{K}$-bilinear map

$$e_B^2 \circ e_R^\star \circ \perp \circ \diamond_\sigma \circ (\top \times \top) \circ (e_R \times e_R) \circ (e_B^\star \times e_B^\star) : \mathbf{M} \times \mathbf{M} \to \mathbf{M}$$

is the multiplication map in $\mathbf{M}$. We observe that

$$\top \circ e_R \circ e_B^\star : \mathbf{M} \to \mathbf{K}[C]^\sigma$$

and

$$e_B^2 \circ e_R^\star \circ \perp : \mathbf{K}[C]^\sigma \to \mathbf{M}$$

are $\mathbf{K}[C]$-linear maps. We deduce that

$$\nu_q^{sym}(n_1, n_2) \leqslant \sigma.$$

13. A general bound

Let $\mathbf{K}$ be a finite field with q elements. Let $\bar{\mathbf{K}}$ be an algebraic closure of $\mathbf{K}$. Let $n \geqslant 2$ be a prime to q integer. Let n_1 and n_2 be two positive integers such that $n = n_1 n_2$. We would like to instantiate the construction in Section 12 so as to obtain a sharp bound for the equivariant symmetric complexity $\nu_q^{sym}(n_1, n_2)$ of multiplication in the degree n algebra over $\mathbf{K}$ defined in Section 9. Field extensions correspond to the case $n_2 = 1$. We let X be a smooth absolutely integral curve over $\mathbf{K}$ such that

$$X(\mathbf{K}) \neq \varnothing. \tag{9}$$

Let μ_n be a primitive n-th root of unity in $\bar{\mathbf{K}}$. Let $\mathbf{K}(\mu_n)$ be the field generated by μ_n over $\mathbf{K}$. We assume that the Jacobian J_X has a point

$$s \in J_X(\mathbf{K}(\mu_n)) \text{ of order } n, \text{ such that } F_q(s) = qs \tag{10}$$

where F_q is the Frobenius of $J_X/\mathbf{K}$. A sufficient condition for such an s to exist is that the characteristic polynomial $\chi(t)$ of F_q has a root in $\mathbf{Z}_\ell$ congruent to q modulo n, for every prime ℓ dividing n. This is granted if n divides the cardinality $\chi(1)$ of $J_X(\mathbf{K})$, and 1 is a simple root of χ modulo ℓ for every prime ℓ dividing n. That is

$$\chi(1) = 0 \bmod n \quad \text{and} \quad \gcd(\chi'(1), n) = 1 \tag{11}$$

where χ' is the derivative of the polynomial χ. We look for a curve X with smallest possible genus satisfying these conditions. Condition (11) cannot hold if $n > (1 + \sqrt{q})^{2g}$. On the other hand we heuristically expect to find a curve X with genus g_X equal to g and satisfying condition (11) provided

$$g \gg \log_q n.$$

Conditions (9) and (10) and Kummer theory imply the existence of a curve Y over $\mathbf{K}$ and an unramified Galois cover $\rho : Y \to X$ with cyclic Galois group of order n. We can even force a $\mathbf{K}$-point on X to split completely in Y. We take $a \in X(\mathbf{K})$, $B = \rho^{-1}(a)$, n_1, n_2, $\mathfrak{r}$, $R = \sum_{c \in C} c.\mathfrak{r}$, D, $E = \rho^{-1}(D)$, e_B and e_R as in Section 12. The condition

$$e_B \text{ is surjective and } e_R^2 \text{ is injective} \tag{12}$$

is granted if

$$\deg(E - B) > 2g_Y - 2 \text{ and } \deg(2E - R) < 0$$

or equivalently

$$\deg D \geqslant 2g_X \text{ and } \deg \mathfrak{r} \geqslant 2 \deg D + 1.$$

This last condition is easy to check but a bit restrictive. A more delicate sufficient condition for (12) is

$$E - B \text{ is non-special and } \dim H^0(Y, \mathcal{O}_Y(2E - R)) = 0.$$

Remind that a divisor D on a curve X of genus g_X is said to be **non-special** if the dimension of $H^0(X, \mathcal{O}_X(D))$ is $\deg D - g_X + 1$. Otherwise D is said to be **special**. We summarize the above discussion in the theorem bellow.

Theorem 2. *Let $\mathbf{K}$ be a finite field with q elements. Let $n \geqslant 2$ be a prime to q integer. Let $\rho : Y \to X$ be an unramified Galois cover between two smooth absolutely integral curves over $\mathbf{K}$. We assume that the Galois group C of ρ is cyclic of order n. Let $a \in X(\mathbf{K})$. Let n_1 be the inertial degree of ρ at a. Let $B = \rho^{-1}(a)$ be the fiber of ρ above a. Let $n_2 = n/n_1$. Let $\mathfrak{r}$ be an effective divisor on Y such that $\mathfrak{r}$ and $c.\mathfrak{r}$ are disjoint for every c in C. Let $R = \sum_{c \in C} c.\mathfrak{r}$. Let D be a divisor on $X/\mathbf{K}$. Let $E = \rho^{-1}(D)$. We assume that*

$$\deg D \geqslant 2g_X \text{ and } \deg \mathfrak{r} \geqslant 2 \deg D + 1. \tag{13}$$

or

$$E - B \text{ is non-special and } \dim H^0(Y, \mathcal{O}_Y(2E - R)) = 0. \tag{14}$$

where g_X is the genus of X. Then $\nu_q^{sym}(n_1, n_2) \leqslant \sigma$ where

$$\sigma = S_{\mathbf{K}}(\times : \mathbf{K}[\mathfrak{r}] \times \mathbf{K}[\mathfrak{r}] \to \mathbf{K}[\mathfrak{r}])$$

is the symmetric bilinear complexity of multiplication in the residue ring of $\mathfrak{r}$.

If $\mathfrak{r}$ is $\deg \mathfrak{r}$ times a point in $Y(\mathbf{K})$, the symmetric bilinear complexity σ of $\mathbf{K}[\mathfrak{r}] \simeq \mathbf{K}[x]/x^{\deg \mathfrak{r}}$ is linear in the degree of $\mathfrak{r}$ according to Equation (2). If $\mathfrak{r}$ is reduced and irreducible then σ is linear in the degree of $\mathfrak{r}$ according to Theorem 1. If $\mathfrak{r}$ is a sum of $\deg \mathfrak{r}$ pairwise distinct $\mathbf{K}$-rational points then $\sigma = \deg \mathfrak{r}$.

14. Non-special divisors

In order to verify Condition (14) in Theorem 2, we need a simple criterion for a divisor to be non-special in this context. Let $\mathbf{K}$ be a field with characteristic p. Let $n \geqslant 2$ be a prime to p integer. Let $\bar{\mathbf{K}}$ be an algebraic closure of $\mathbf{K}$. Let μ_n be a primitive n-th root of unity in $\bar{\mathbf{K}}$. Let X and Y be two smooth absolutely integral curves over $\mathbf{K}$. We call g_X the genus of X and g_Y the genus of Y. Let $\rho : Y \to X$ be a Galois unramified cover with cyclic Galois group C of order

n. Let $\hat{\rho} : J_X \to J_Y$ be the induced map on Jacobian varieties. The kernel of $\hat{\rho}$ is a finite group scheme of degree n. There is a pairing

$$e_\rho : \operatorname{Ker} \hat{\rho} \times C \to \boldsymbol{\mu}_n$$

where $\boldsymbol{\mu}_n$ is the group scheme of n-th roots of unity. If γ is a divisor class in the kernel of $\hat{\rho}$ and $c \in C$, we let Γ be a divisor in γ and G a function on Y with divisor $\rho^{-1}(\Gamma)$. We set

$$e_\rho(\gamma, c) = \frac{G \circ c}{G}.$$

This is a non-degenerate pairing. As a consequence $\operatorname{Ker} \hat{\rho}$ is isomorphic to $\boldsymbol{\mu}_n$.

Let D be a divisor on X with degree $g_X - 1$. Let E be the pullback of D on Y. The degree of E is $n(g_X - 1) = g_Y - 1$. If E is special then the $\mathbf{K}[C]$-module $H^0(Y, \mathcal{O}_Y(E))$ is non-zero. Since p is prime to n, there exists an eigenvector φ for the action of C on $H^0(Y, \mathcal{O}_Y(E)) \otimes \mathbf{K}(\mu_n)$. Let N be the effective divisor on $Y \otimes \mathbf{K}(\mu_n)$ such that the principal divisor (φ) is $N - E$. Then N is the pullback of an effective divisor M on $X \otimes \mathbf{K}(\mu_n)$. And $M - D$ is in the the kernel of $\hat{\rho}$.

To summarize, if D is a divisor on X with degree $g_X - 1$, then the pullback $E = \rho^{-1}(D)$ has degree $g_Y - 1$. And E is special (its class is effective) if and only if there exists a degree $g_X - 1$ effective divisor M on $X \otimes \mathbf{K}(\mu_n)$ such that $D - M$ is in the kernel of $\hat{\rho}$.

15. Elliptic curves

In this section we adapt the general method of Section 12 to the special case of elliptic curves. The main reason for this restriction is that we have a good control on the group of rational points on an elliptic curve. Restricting to elliptic curves is not optimal but it enables us to prove such an asymptotic statement as Theorem 5.

Let $\mathbf{K}$ be a finite field with cardinality q and characteristic p. Let $n \geqslant 2$ be an integer. Let Y be an elliptic curve over $\mathbf{K}$. We assume that Y has a $\mathbf{K}$-point t of order n. Let C be the group generated by t. Let X be the quotient of Y by C. Let $\rho : Y \to X$ be the quotient isogeny. Let a in $X(\mathbf{K})$. Let n_1 be the inertial degree of ρ at a. Let $n_2 = n/n_1$. The fiber $B = \rho^{-1}(a)$ of ρ above a has n_2 irreducible components, each of degree n_1 above a. We call $\mathbf{M}$ the residue ring $\mathbf{K}[B]$ of B. Let v be a point in $X(\mathbf{K})$. We assume that $v - a$ is not in the kernel of the dual isogeny $\hat{\rho}$. We call D the degree 1 divisor on X consisting of the single point v with multiplicity 1. We call E the divisor $\rho^{-1}(D)$. We let u be a non-zero point in $\rho(Y(\mathbf{K}))$.We assume that $u - 2v$ is not in the kernel of $\hat{\rho}$. We let $\mathfrak{r}$ be the formal sum of one point in the fiber of ρ above u plus one point in the kernel of ρ. Let R be the closure of $\mathfrak{r}$ under the action of C. So R is the sum of the two split fibers of ρ above the origin o_X and u. We let ϵ be a local equation of D in a neighborhood of o_X, a and u. In this setting the evaluation map $e_B : H^0(Y, \mathcal{O}_Y(E)) \to \mathbf{M}$ is an isomorphism between two free $\mathbf{K}[C]$-modules of rank 1. The evaluation map $e_R^2 : H^0(Y, \mathcal{O}_Y(2E)) \to \mathbf{K}[R]$ is an isomorphism between two free $\mathbf{K}[C]$-modules of rank 2. The symmetric bilinear complexity of multiplication in $\mathbf{K}[\mathfrak{r}] \sim \mathbf{K} \times \mathbf{K}$ is 2. We deduce that $\nu_q^{sym}(n_1, n_2)$ is bounded by 2. In the special case when $n_1 = n \geqslant 2$ the residue ring $\mathbf{M}$ is a field and $\nu_q^{sym}(n_1, n_2) = \nu_q^{sym}(n)$. The latter cannot be equal to 1 then because $\mathbf{K}^n$ is not a field. So $\nu_q^{sym}(n) = 2$ in that case.

Theorem 3. *Let $\mathbf{K}$ be a field with cardinality q and characteristic p. Let $n \geqslant 2$ be an integer. Let Y be an elliptic curve over $\mathbf{K}$ having a $\mathbf{K}$-point t of order n. Let X be the quotient of Y*

by the group C generated by t. Let $\rho : Y \to X$ be the quotient isogeny. Let $a \in X(\mathbf{K})$. Let n_1 be the inertial degree of ρ at a. Let $n_2 = n/n_1$. Let u be a non-zero point in $\rho(Y(\mathbf{K}))$. Let $v \in X(\mathbf{K})$. We assume that neither $v - a$ nor $u - 2v$ are in the kernel of the dual isogeny $\hat{\rho}$. Then $\nu_q^{sym}(n_1, n_2) \leqslant 2$. In case $n_2 = 1$ then $\nu_q^{sym}(n) = 2$.

16. An asymptotic bound

Let $n \geqslant 2$ be an integer. Using Theorem 3 we now prove an asymptotic bound on the equivariant complexity $\nu_q^{sym}(n)$ without any restriction on q or n. We let $\mathbf{K}$ be a field with cardinality q and characteristic p. Let $n \geqslant 2$ be an integer. We first assume that

$$n^2 \leqslant 2\sqrt{q} \tag{15}$$

and

$$q \geqslant 37. \tag{16}$$

There are two consecutive multiples of n^2 in the Hasse interval $[q+1-2\sqrt{q}, q+1+2\sqrt{q}]$. At least one of them is not congruent to 1 modulo p. So there exists an elliptic curve Y over $\mathbf{K}$ such that $Y(\mathbf{K})$ is divisible by n^2. We deduce that Y has a $\mathbf{K}$-point of order n. Indeed the group $Y(\mathbf{K})$ is isomorphic to $(\mathbf{Z}/m_1\mathbf{Z}) \times (\mathbf{Z}/m_1m_2\mathbf{Z})$ where m_1 and m_2 are positive integer. And n^2 divides $\#Y(\mathbf{K}) = m_1^2m_2$. So n^2 divides $(m_1m_2)^2$. So n divides m_1m_2. So $Y(\mathbf{K})$, beeing isomorphic to $(\mathbf{Z}/m_1\mathbf{Z}) \times (\mathbf{Z}/m_1m_2\mathbf{Z})$, has an element t of order n. Let C be the group generated by t. We call X the quotient of Y by C. Let $\rho : Y \to X$ be the quotient isogeny. Let P be a point in $X(\mathbf{K})$. Let $\bar{\mathbf{K}}$ be an algebraic closure of $\mathbf{K}$. Let Q be any point in $Y(\bar{\mathbf{K}})$ such that $\rho(Q) = P$. We set $\kappa(P) = F_q(Q) - Q$ where F_q is the Frobenius endomorphism of $Y/\mathbf{K}$. We thus define a morphism

$$\begin{array}{rcl} \kappa & : & X(\mathbf{K})/\rho(Y(\mathbf{K})) \longrightarrow \operatorname{Ker}\rho = C \\ & & P \longmapsto F_q(Q) - Q \end{array}$$

which is easily seen to be a bijection. Let n_1 and n_2 be two positive integers such that $n = n_1n_2$. There exists at least one point a in $X(\mathbf{K})$ such that $\kappa(a) = n_2t$. The inertial degree of ρ above a is n_1. We call $B = \rho^{-1}(a)$ the fiber of ρ above a. It has n_2 irreducible components, each of degree n_1 above a. We call $\mathbf{M}$ the residue ring $\mathbf{K}[B]$ of B.

We need a point v in $X(\mathbf{K})$such that $v-a$ is not in the kernel of $\hat{\rho}$. There are at least $|X(\mathbf{K})|-n$ such points. So the existence of v is granted provided

$$|X(\mathbf{K})| - n \geqslant 1.$$

The latter inequality follows from Conditions (15) and (16). We also need a non-zero point u in $\rho(Y(\mathbf{K}))$ such that $u - 2v$ is not in the kernel of $\hat{\rho}$. There are at least

$$\frac{|X(\mathbf{K})|}{n} - n - 1$$

such points. So the existence of u is granted provided

$$\frac{|X(\mathbf{K})|}{n} - n \geqslant 2.$$

The later inequality follows again from Conditions (15) and (16). Applying Theorem 3 we deduce the following.

Theorem 4. *Let q be a prime power and $n \geqslant 2$ an integer. Let n_1 and n_2 be two positive integers such that $n = n_1 n_2$. If $q \geqslant 37$ and $n \leqslant \sqrt{2\sqrt{q}}$ then $\nu_q^{sym}(n_1, n_2) \leqslant 2$.*

We now can bound $\nu_q(n)$ without any restriction on n and q. We let m be the smallest integer such that $m \geqslant 4\log_q n$ and $m \geqslant 6$. We set $q' = q^m$ and check that (q', n) satisfy Conditions (15) and (16). Using Theorem 4 in conjunction with Equation (8) and Theorem 1 we deduce the following theorems.

Theorem 5. *Let q be a prime power and $n \geqslant 2$ an integer. Let m be the smallest integer such that $m \geqslant 4\log_q n$ and $m \geqslant 6$. Then $\nu_q^{sym}(n) \leqslant 2 \times \mu_q^{sym}(m)$.*

Theorem 6. *There exists an absolute constant $\mathcal{Q}$ such that the following is true. Let q be a prime power and $n \geqslant 2$ an integer. Then $\nu_q^{sym}(n) \leqslant \mathcal{Q} \times \lceil \log_q n \rceil$.*

The next theorem now follows from Theorem 6 and the existence of an algorithm to compute products in $\mathbf{K}[x]/(x^n - 1)$ at the expense of $O(n\log(n)|\log(\log(n))|)$ operations in $\mathbf{K}$. See [14, 5].

Theorem 7. *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 straight line program that computes the coordinates in $\mathcal{B}$ of 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.

Compared to [8, Theorem 4] we save a $\log n$ factor on both the running time and the size of the model. Theorem 7 is also more general since it applies to any normal basis and does not rely on any ad hoc redundant representation as in [8].

17. Bounding $\nu_q^{sym}(n)$

We explain how to use Theorems 3 and 2 to bound $\nu_q^{sym}(n)$ for given q and n. If we plan to use an elliptic curve, we look for the smallest integer m such that the Hasse interval

$$[\lceil q^m + 1 - 2q^{m/2} \rceil, \lfloor q^m + 1 + 2q^{m/2} \rfloor]$$

contains a multiple of n. We then look for an elliptic curve over a field with q^m elements satisfying the hypotheses of Theorem 3. We pick random curves and compute their cardinality using Schoof's algorithm and its variants [15], until we find a curve with order divisible by n. We then check for the existence of a point of order n.

If we want to use the general method of Section 12, we look for the smallest integer g such that $(\sqrt{q} + 1)^{2g}$ is reasonably larger than n. We then pick random curves of genus g over a field with q elements, until we find one whose Jacobian has order divisible by n. We then check the hypotheses of Theorem 2. We illustrate this method with a few examples in the following sections. We will see how to verify the hypotheses of Theorem 2 at the least computational cost. The knowledge of the zeta function suffices in many cases.

18. The case $q = 7$ and $n = 5$

Since 10 belongs to the Hasse interval

$$[\lceil 7+1-2\sqrt{7}\rceil, \lfloor 7+1+2\sqrt{7}\rfloor] = [3, 13]$$

there is an elliptic curve E such that $E(\mathbf{K}) \simeq \mathbf{Z}/10\mathbf{Z}$. We can take Y to be the smooth projective model of

$$y^2 = x^3 + x + 4.$$

The point $t = (6, 4) \in Y$ has order 5. The quotient of Y by the group C generated by t is the elliptic curve X with affine equation

$$y^2 = x^3 + 3x + 4.$$

Since the kernel of the quotient by C isogeny $\rho : Y \to X$ is split, the kernel of the dual isogeny $\hat{\rho}$ is isomorphic to $\boldsymbol{\mu}_5$. The only rational point in it is the origin o_X because n is prime to $q-1$. The image $\rho(Y(\mathbf{K}))$ has order 2. The point

$$a = (0, 2) \in X(\mathbf{K})$$

has order 5. So it does not belong to $\rho(Y(\mathbf{K}))$. The fiber $B = \rho^{-1}(a)$ contains no $\mathbf{K}$-point. So it is irreducible. We set

$$u = (6, 0) \in X(\mathbf{K})$$

the unique $\mathbf{K}$-rational point of order 2 on X. So u belongs to $\rho(Y(\mathbf{K}))$. We take

$$v = (0, 5) \in X(\mathbf{K}).$$

Since $2v$ has order 5, it must be different from u. Since the only $\mathbf{K}$-point in the kernel of $\hat{\rho}$ is o_X we easily check that $v - a$ and $u - 2v$ are not in this kernel. Applying Theorem 3 we deduce that

$$\nu_7^{sym}(5) = 2.$$

The following computer session implements this calculation in SageMath (Version 9.4) [18].

```
sage: q=7;K=GF(q);n=5
....: Y=EllipticCurve([K(1),K(4)]);Y.order()
10
sage: t=Y(6,4);n*t
(0 : 1 : 0)
sage: rho = Y.isogeny(t);X = rho.codomain()
Elliptic Curve defined by y^2 = x^3 + 3*x + 4
over Finite Field of size 7
sage: a=X(0,2);5*a
(0 : 1 : 0)
sage: u=X(6,0);v=X(0,5);u-2*v
(2 : 5 : 1)
```

19. The case $q = 11$ and $n = 239$

We try the general method first. We then see what can be achieved using elliptic curves and extension of scalars.

19.1. **Using a genus 2 curve.** Let X be the smooth projective model of the hyperelliptic curve with equation

$$y^2 = x^5 + x^3 + 2x^2 + 3.$$

This is a genus 2 curve. The characteristic equation of the Frobenius F_q of X is

$$\chi(t) = t^4 + 7t^3 + 33t^2 + 77t + 121.$$

So X has $q + 1 + 7 = 19$ points over $\mathbf{K}$. Its Jacobian has $\chi(1) = 239 = n$ points. This is a prime integer. The factorization of $\chi(t)$ modulo n is

$$\chi(t) = (t - 11)(t - 1)(t^2 + 19t + 11).$$

So there is a point s in $J_X[n]$ such that $F_q(s) = qs$. Let $w_0 \in X(\mathbf{K})$ be the unique place at infinity. The class of $2w_0$ is the unique divisor class of degree 2 on X having positive projective dimension. There exists a curve Y over $\mathbf{K}$ and a Galois cover $\rho : Y \to X$ with cyclic Galois group of order n such that the fiber of ρ above w_0 splits completely over $\mathbf{K}$. The kernel of $\hat{\rho} : J_X \to J_Y$ is the subgroup generated by the class s. We observe that the class of q generates a subgroup of index 2 in the multiplicative group $(\mathbf{Z}/n\mathbf{Z})^*$. So Galois action on the non-zero classes in the kernel of $\hat{\rho}$ has two orbits.

Let w_1 and w_2 be two points in $X(\mathbf{K})$ having distinct x-coordinates. The linear pencil of the divisor $w_1 + w_2$ has projective dimension zero, that is

$$H^0(X, \mathcal{O}_X(w_1 + w_2)) = \mathbf{K}.$$

Let v_1, v_2, v_3, v_4, v_5 be five points in $X(\mathbf{K})$. We assume that v_1, v_2, v_3, v_4, v_5, w_1, and w_2 are pairwise distinct. Since the cardinality of $J_X(\mathbf{K})$ is odd, the multiplication by two map is a bijection of it. We deduce the existence of five effective degree two divisors D_1, D_2, D_3, D_4, D_5 such that $2(D_i - 2w_0)$ is linearly equivalent to $w_1 + w_2 - v_i - w_0$ for $1 \leqslant i \leqslant 5$. The divisor $2D_i - 3w_0$ is linearly equivalent to $w_1 + w_2 - v_i$. It is a non-special divisor.

Let ξ be any non-zero divisor class in the kernel of $\hat{\rho}$. For each $1 \leqslant i \leqslant 5$, the divisor class $2D_i - 3w_0 - \xi$ is the class $w_1 + w_2 - v_i - \xi$. At most two among these five classes are effective. Otherwise the class $w_1 + w_2 - \xi$ would have positive projective dimension. So it would be the class of $2w_0$. Then $\xi = w_1 + w_2 - 2w_0$ would be $\mathbf{K}$-rational. A contradiction.

Since there are only two Galois orbits on the non-zero classes in $\operatorname{Ker}\rho$ we deduce that there exists a v among v_1, v_2, v_3, v_4, v_5 such that $w_1 + w_2 - v - \xi$ is ineffective for all ξ in this kernel. We call D the effective degree two divisor such that $2(D - 2w_0)$ is linearly equivalent to $w_1 + w_2 - v - w_0$.

Because n is a prime integer, every fiber of ρ above a rational point of X is either irreducible or completely split. Since de genus of Y is

$$g_Y = 1 + n(g_X - 1) = 1 + n = 240,$$

the number of $\mathbf{K}$-rational points on it is bounded from above by $q+1+2g_Y\sqrt{q}<1604$. So the number of split fibers is $\leqslant 1603/239<7$. So there are at least 13 points $(a_i)_{1\leqslant i\leqslant 13}$ in $X(\mathbf{K})$ with an irreducible fiber above them.

At most two among the $(a_i)_{1\leqslant i\leqslant 13}$ make the class of $D-a_i$ effective. Otherwise D would have positive projective dimension. So it would be linearly equivalent to $2w_0$. Then $w_1+w_2-v-w_0$ would be principal. But w_1+w_2 has projective dimension 0 and v is distinct from w_1 and w_2. A contradiction.

Let ξ be any non-zero class in the kernel of $\hat{\rho}$. At most two among the $(a_i)_{1\leqslant i\leqslant 13}$ make $D-a_i-\xi$ effective. Otherwise $D-\xi$ would have positive projective dimension. So it would be linearly equivalent to $2w_0$. Then ξ would be the class of $D-2w_0$ and it would therefore be $\mathbf{K}$-rational. A contradiction.

Since Galois action has two orbits on the non-zero classes in the kernel of $\hat{\rho}$, we deduce that at least $13-2-2\times 2=7$ rational points a_i on X have irreducible fiber $\rho^{-1}(a_i)$ and make $D-a_i+\xi$ non-special for every ξ in $\operatorname{Ker}\hat{\rho}$. We let a be any of them.

We let $\mathfrak{r}$ be the three times any point on Y above w_0. The ring $\mathbf{K}[\mathfrak{r}]$ is isomorphic to $\mathbf{K}[x]/x^3$. Since $\mathbf{K}$ has $q\geqslant 4$ elements the symmetric bilinear complexity of multiplication in $\mathbf{K}[\mathfrak{r}]$ is 5. Applying Theorem 2 we deduce

$$\nu_{11}^{sym}(239)\leqslant 5.$$

The following computer session implements this calculation in SageMath (Version 9.4) [18].

```
sage: q=11;K=GF(q);Kx.<x>=FunctionField(K);Kxy.<y>=Kx[];
KX.<y> = Kx.extension(y^2-x^5-x^3-K(2)*x^2-K(3))
g = KX.genus();LP=KX.L_polynomial();t=LP.parent().gen()
sage: chi=LP(1/t)*t^(2*g)
t^4 + 7*t^3 + 33*t^2 + 77*t + 121
sage: n=numerator(chi(1))
239
sage: Fnt.<t> = PolynomialRing(GF(n));factor(Fnt(chi))
(t + 228)*(t + 238)*(t^2 + 19*t + 11)
```

19.2. **Using an elliptic curve and extension of scalars.** We now try to bound $\nu_{11}^{sym}(239)$ using the method in Section 15. We let m be the smallest integer such that the Hasse interval

$$[\lceil q^m+1-2q^{m/2}\rceil,\lfloor q^m+1+2q^{m/2}\rfloor]$$

contains a multiple of n. For $m=1$ we find the interval $[9,15]$. For $m=2$ we find the interval $[111,133]$. For $m=3$ we find the interval $[1296,1368]$. None of these three intervals contain a multiple of 239. So we must take $m\geqslant 4$. The best we can hope with this method is to prove that

$$\nu_{11}^{sym}(239)\leqslant 2\mu_q^{sym}(4).$$

Since $q\geqslant 6$ we have $\mu_q^{sym}(4)=7$. So $\nu_{11}^{sym}(239)\leqslant 14$. This is not as good as the bound already obtained in Section 19.1.

20. The case $q = 13$ and $n = 4639$

Let X be the smooth projective plane quartic with homogeneous equation

$$y^3z + x^3y + 2xyz^2 + yz^3 + 11x^3z + 9x^2z^2 + 10xz^3.$$

This is a genus 3 curve. The characteristic equation of the Frobenius F_q of X is

$$\chi(t) = t^6 + 9t^5 + 51t^4 + 197t^3 + 663t^2 + 1521t + 2197.$$

So X has $q + 1 + 9 = 23$ points over $\mathbf{K}$. Its Jacobian has $\chi(1) = 4639 = n$ points. This is a prime integer. The factorization of $\chi(t)$ modulo n is

$$\chi(t) = (t - 13)(t - 1)(t + 2195)(t + 3726)(t^2 + 3380t + 13).$$

So there is a point s in $J_X[n]$ such that $F_q(s) = qs$. Let $w_0 \in X(\mathbf{K})$ be the point $(0 : 0 : 1)$. There exists a curve Y over $\mathbf{K}$ and a Galois cover $\rho : Y \to X$ with cyclic Galois group of order n such that the fiber of ρ above w_0 splits completely over $\mathbf{K}$. The kernel of $\hat{\rho} : J_X \to J_Y$ is the subgroup generated by the class s. We observe that the class of q generates the multiplicative group $(\mathbf{Z}/n\mathbf{Z})^*$. So Galois action is transitive on the non-zero classes in the kernel of $\hat{\rho}$.

Let w_1, w_2 and w_3 be three non-colinear points in $X(\mathbf{K})$. The linear pencil of the divisor $w_1 + w_2 + w_3$ has projective dimension zero, that is

$$H^0(X, \mathcal{O}_X(w_1 + w_2 + w_3)) = \mathbf{K}.$$

Let $v_1, \ldots, v_7$ be seven points in $X(\mathbf{K})$. We assume that v_1, v_2, v_3, v_4, v_5, v_6, v_7, w_1, w_2 and w_3 are pairwise distinct. Since the cardinality of $J_X(\mathbf{K})$ is odd, the multiplication by two map is a bijection of it. We deduce the existence of seven effective degree three divisors $D_1, \ldots, D_7$ such that $2(D_i - 3w_0)$ is linearly equivalent to $w_1 + w_2 + w_3 - v_i - 2w_0$ for $1 \leqslant i \leqslant 7$. The divisor $2D_i - 4w_0$ is linearly equivalent to $w_1 + w_2 + w_3 - v_i$. It is non-special.

Let ξ be any non-zero divisor class in the kernel of $\hat{\rho}$. For each $1 \leqslant i \leqslant 7$, the divisor class $2D_i - 4w_0 - \xi$ is the class $w_1 + w_2 + w_3 - v_i - \xi$. At most three among these seven classes are effective. Otherwise the class $w_1 + w_2 + w_3 - \xi$ would have positive projective dimension. So it would be the class $K - P_\xi$ where K is the canonical class and P_ξ is a point on X. Because Galois action is transitive on the non-zero classes in the kernel of $\hat{\rho}$, there would exist for every such class ξ a point P_ξ such that $w_1 + w_2 + w_3 - \xi$ is the class $K - P_\xi$. We consider the points P_s, P_{2s}, P_{3s}, P_{4s} associated with s, $2s$, $3s$, $4s$, where s is a generator of the kernel of $\hat{\rho}$. These are four pairwise distinct points and $P_{2s} - P_s$ is linearly equivalent to $P_{4s} - P_{3s}$. So the linear series of $P_s + P_{4s}$ has positive projective dimension. A contradiction because X is not hyperelliptic.

So we can assume that $w_1 + w_2 + w_3 - v_i - \xi$ is ineffective for $1 \leqslant i \leqslant 4$. Since the Galois group of $\mathbf{K}$ acts transitively on the non-zero classes in the kernel of $\hat{\rho}$ we deduce that $2D_i - 4w_0 - \xi$ is ineffective for any ξ in $\operatorname{Ker} \hat{\rho}$ and any $1 \leqslant i \leqslant 4$.

At least one among D_1, D_2, D_3, D_4 has projective dimension zero. Otherwise there would exist four points P_1, P_2, P_3, P_4 such that D_i is linearly equivalent to $K - P_i$ for $1 \leqslant i \leqslant 4$. So $2(K - P_i)$ is linearly equivalent to $w_1 + w_2 + w_3 + 4w_0 - v_i$. We deduce that $2P_2 + v_1 \sim 2P_1 + v_2$ and $2P_3 + v_1 \sim 2P_1 + v_3$ and $2P_4 + v_1 \sim 2P_1 + v_4$. So these classes have positive projective dimension. There exist three points Q_2, Q_3, and Q_4 such that $2P_1 + v_2 \sim K - Q_2$, $2P_1 + v_3 \sim K - Q_3$, and $2P_1 + v_4 \sim K - Q_4$. So $v_2 + Q_2 \sim v_3 + Q_3 \sim v_4 + Q_4$. A contradiction because X is not hyperelliptic.

We call D one among D_1, D_2, D_3, D_4 having projective dimension zero. And let v be the point such that $2(D-3w_0)$ is linearly equivalent to $w_1+w_2+w_3-v-2w_0$.

Because n is a prime integer, every fiber of ρ above a rational point of X is either irreducible or completely split. Since de genus of Y is

$$g_Y = 1+n(g_X-1) = 1+2n = 9279,$$

the number of $\mathbf{K}$-rational points on it is bounded from above by $q+1+2g_Y\sqrt{q} < 66926$. So the number of split fibers is $\leqslant 66925/9279 < 15$. So there are at least 9 points $(a_j)_{1\leqslant j\leqslant 9}$ in $X(\mathbf{K})$ with an irreducible fiber above them.

Let ξ be any non-zero class in the kernel of $\hat{\rho}$. At most three among the $(a_i)_{1\leqslant i\leqslant 9}$ make $D-a_i-\xi$ effective. Otherwise $D-\xi$ would have positive projective dimension. So it would be linearly equivalent to $K-P_\xi$ for some point P_ξ on X. Because Galois action is transitive on the non-zero classes in the kernel of $\hat{\rho}$, there would exist for every such class ξ a point P_ξ such that $D-\xi$ is the class $K-P_\xi$. We consider the points P_s, P_{2s}, P_{3s}, P_{4s} associated with s, $2s$, $3s$, $4s$, where s is a generator of the kernel of $\hat{\rho}$. These are four pairwise distinct points and $P_{2s}-P_s$ is linearly equivalent to $P_{4s}-P_{3s}$. So the linear series of P_s+P_{4s} has positive projective dimension. A contradiction because X is not hyperelliptic. So at least six among the $(a_i)_{1\leqslant i\leqslant 9}$ make $D-a_i-\xi$ ineffective for the chosen non-zero ξ and thus for all its conjugates. So we can assume that $D-a_i-\xi$ is ineffective for any $1\leq i\leq 6$ and any non-zero ξ in the kernel of $\hat{\rho}$.

At most three among the $(a_i)_{1\leqslant i\leqslant 6}$ make $D-a_i$ special. Otherwise D would have positive projective dimension. A contradiction.

We let a be one among $(a_i)_{1\leq i\leq 6}$ such that $D-a$ is non-special. We let $\mathfrak{r}$ be the divisor consisting of four times any point on Y above w_0. The ring $\mathbf{K}[\mathfrak{r}]$ is isomorphic to $\mathbf{K}[x]/x^4$. Since $\mathbf{K}$ has $q\geqslant 6$ elements the symmetric bilinear complexity of multiplication in $\mathbf{K}[\mathfrak{r}]$ is 7. Applying Theorem 2 we deduce

$$\nu_{13}^{sym}(4639)\leqslant 7.$$

The following computer session implements this calculation in SageMath (Version 9.4) [18].

```
sage: q=13;K=GF(q);Kx.<x>=FunctionField(K);Kxy.<y>=Kx[];
KX.<y> = Kx.extension(y^3+y*(K(1)+K(2)*x+x^3)+K(10)*x
+K(9)*x^2+K(11)*x^3)
g=KX.genus();LP=KX.L_polynomial();t=LP.parent().gen();
sage: chi=LP(1/t)*t^(2*g)
t^6 + 9*t^5 + 51*t^4 + 197*t^3 + 663*t^2 + 1521*t + 2197
sage: n=numerator(chi(1))
4639
Fnt.<t> = PolynomialRing(GF(n));factor(Fnt(chi))
(t+2195)*(t+3726)*(t+4626)*(t+4638)*(t^2+3380*t+13)
```

21. Remarks and questions

The symmetric equivariant complexity $\nu_q^{sym}(n)$ provides a good control on the computational difficulty of multiplying two elements in a degree n extension of a field $\mathbf{K}$ with q-elements, given by their coordinates in any normal basis. We have shown how to bound $\nu_q^{sym}(n)$ using points

of order n in Jacobians over $\mathbf{K}$. We need a Jacobian with smallest possible dimension having a point of order n. A natural question is : given q and n, which is the smallest possible g such that there exists a Jacobian of dimension g over a field with q elements, having a rational point of order n ? Are there asymptotic families that are good with this respect ? Modular towers produce curves with many points but they have too much ramification to be useful here.

In practice, we pick random curves of genus g over a field with q elements, until we find some whose Jacobian has order divisible by n. A difficulty is that for large g we do not have a convenient model for a universal curve of genus g. We could restrict to hyperelliptic curves but their Jacobians tend to be smaller, so this restriction affects the efficiency of the method.

We may wonder if Theorem 6 is optimal, even roughly. Given q and some bound C, are there only finitely many n such that $\nu_q^{sym}(n) \leqslant C$? such that $\nu_q^{sym}(n) \leqslant C|\log(\log(n))|$ for example ?

REFERENCES

[1] S. Ballet, J. Pieltant, M. Rambaud, H. Randriambololona, R. Rolland, and J. Chaumine. On the tensor rank of multiplication in finite extensions of finite fields and related issues in algebraic geometry. *Uspekhi Mat. Nauk*, 76(1(457)):31–94, 2021.

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

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

[4] 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.

[5] David G. Cantor and Erich Kaltofen. On fast multiplication of polynomials over arbitrary algebras. *Acta Inform.*, 28(7):693–701, 1991.

[6] 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.

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

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

[9] S. Gao, J. von zur Gathen, and D. Panario. Gauss periods, primitive normal basis, and fast exponentiation in finite fields. *Lecture Notes in Computer Science*, 911:311–322, 1995.

[10] Shuhong Gao and David Thomson. Complexity of normal bases. In Gary L. Mullen and Daniel Panario, editors, *Handbook of Finite Fields*, Discrete mathematics and its applications, pages 117–127. CRC Press, 2013.

[11] Michael T. Heideman. *Multiplicative complexity, convolution, and the DFT*. Springer-Verlag, New York, 1988.

[12] R.C. Mullin, I.M. Onyszchuk, S.A. Vanstone, and R.M. Wilson. Optimal normal basis in $GF(p^n)$. *Discrete Applied Math.*, 22:149–161, 1989.

[13] Hugues Randriambololona. Bilinear complexity of algebras and the Chudnovsky-Chudnovsky interpolation method. *J. Complexity*, 28(4):489–517, 2012.

[14] A. Schönhage and V. Strassen. Schnelle Multiplikation grosser Zahlen. *Computing (Arch. Elektron. Rechnen)*, 7:281–292, 1971.

[15] René Schoof. Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordeaux*, 7(1):219–254, 1995. Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993).

[16] Mohammad Amin Shokrollahi. Optimal algorithms for multiplication in certain finite fields using elliptic curves. *SIAM J. Comput.*, 21(6):1193–1198, 1992.

[17] 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.

[18] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.4)*, 2021. `https://www.sagemath.org`.

[19] Joachim von zur Gathen and Jürgen Gerhard. *Modern computer algebra*. Cambridge University Press, Cambridge, third edition, 2013.

[20] S. Winograd. Some bilinear forms whose multiplicative complexity depends on the field of constants. *Math. Systems Theory*, 10(2):169–180, 1976/77.

JEAN-MARC COUVEIGNES, UNIV. BORDEAUX, CNRS, INRIA, BORDEAUX-INP, IMB, UMR 5251, F-33400 TALENCE, FRANCE.

Email address: `Jean-Marc.Couveignes@u-bordeaux.fr`

TONY EZOME, UNIVERSITÉ DES SCIENCES ET TECHNIQUES DE MASUKU, FACULTÉ DES SCIENCES, DÉPARTEMENT DE MATHÉMATIQUES ET INFORMATIQUE, BP 943 FRANCEVILLE, GABON.

Email address: `tony.ezome@gmail.com`