COMPUTING EQUATIONS OF CURVES WITH MANY POINTS

V. DUCET AND C. FIEKER

Abstract. We explain how to compute the equations of the abelian coverings of any curve defined over a finite field. Then we describe an algorithm which computes curves with many rational points with respect to their genus. The implementation of the algorithm provides 7 new records over $\mathbb{F}_2$.

Introduction

The motivation for finding curves defined over a finite field $\mathbb{F}_q$ with many rational points compared to their genus comes from the theory of error-correcting codes. Let C be a (n,k,d)-*code*, that is a sub-vector space of $\mathbb{F}_q^n$ of dimension k in which every non-zero vector has at least d non-zero coordinates in a fixed basis. For given parameters n and k, one wishes to find codes with the largest possible correction capacity $(d-1)/2$.

In a 1977 paper ([Gop77]), Goppa proposed a method for constructing codes which is based on algebraic geometry. Let X be a (non-singular projective irreducible) curve X defined over $\mathbb{F}_q$. Let $D_1 = P_1 + \cdots + P_n$ and D_2 be two divisors over X with disjoint support such that the points P_i are rational and $2g-2 < \deg(D_2) < n$ respectively. Let $\Omega_X(D_1 - D_2)$ be the space of differentials ω on X such that $\operatorname{div}(\omega) \geq D_2 - D_1$ and let $\operatorname{res}_{P_i}(\omega)$ be the residue of ω at P_i; the *Goppa code* $C(X, D_1, D_2)$ associated to this data is the image of the $\mathbb{F}_q$-linear map $\Omega_X(D_1 - D_2) \to \mathbb{F}_q^n$ defined by $\omega \mapsto (\operatorname{res}_{P_1}(\omega), ..., \operatorname{res}_{P_n}(\omega))$. For these codes, the Riemann-Roch Theorem shows that $k = g - 1 + n - \deg(D_2)$ and that

$$\frac{k}{n} + \frac{d}{n} \geq 1 + \frac{1}{n} - \frac{g}{n}.$$

By construction, n is bounded by the number of rational points $N(X)$ of X, and from the above inequality, for given n and k, the smaller the genus, the more efficient the code. So one would like to find, for every n, the smallest genus g such that there exists a curve $X/\mathbb{F}_q$ with at least n rational points. The moral of all this is that one must look for curves with many rational points compared to their genus, for every genus.

The idea of using Class Field Theory to construct abelian coverings with many rational points over a finite field comes from Serre (see [Ser83]). His Harvard course notes ([Ser85]) remain a very useful reference with a lot of material. Niederreiter and Xing continued the search for good curves and devoted many papers to find new techniques. One can quote in particular the explicit description of ray class fields provided by the theory of Drinfel'd modules. Their book ([NX01]) includes all their work on the subject and much more. In a series of paper of the late 90s ([Lau96], [Lau99a], [Lau99b]), Lauter extended Serre's method and obtained new records by studying the degree of certain abelian extensions of the rational function field ramified at a single rational place and totally split at the others. She also interpreted several known families of curves as particular class field theoretical constructions. Auer (see his PhD thesis [Aue99] or the ANTS paper [Aue00] for a summary of the results) extended Lauter's work and described an algorithm to compute the degree of the maximal abelian extension of any function field at most ramified at one place and with prescribed splitting behavior. This allowed him to find many new curves improving the known records. We conclude this historical survey by noting that only in a few cases one can deduce the equation of the curve from its theoretical construction, especially, the so called "explicit" description via Drinfeld modules is very difficult to use.

In the present article, we use explicit Class Field Theory to compute the equations of the abelian coverings of a curve defined over a finite field, and apply it to the problem consisting of finding curves with the maximum possible number of rational points compared to their genus. The paper is divided as follows: in the first section we explain the link between ray class groups and abelian coverings. Then we describe how to use explicit Class Field Theory to compute the equation of an abelian covering of a curve with knowledge of the corresponding ray class group. In section 3 we present an algorithm to find good curves and then give an overview of the results in section 4.

Acknowledgments. The first author would like to thank Everett Howe and his advisor David Kohel for their support during the preparation of the paper, as well as Jérémie Detrey and Emmanuel Thomé for their help with Magma.
Both authors thank the anonymous referees for their useful comments about a first version of the article.

1. Ray Class Groups

We first recall the main aspects of Class Field Theory in the classical language of ray class groups. The reader is referred to [Lan94], [Mil11b] or [Wei95] for the proofs.

Let K be a global function field defined over a finite field $\mathbb{F}_q$; K should be thought of as the function field of a curve X defined over $\mathbb{F}_q$. The set of places of K is denoted by Pl_K. Let $\mathfrak{m}$ be a *modulus* on K, *i.e.* an effective divisor over K. Let $\mathrm{Div}_\mathfrak{m}$ be the group of divisors of K whose support is disjoint from that of $\mathfrak{m}$, and let $P_{\mathfrak{m},1}$ be the subgroup of divisors of functions 'congruent to 1 modulo $\mathfrak{m}$':

$$P_{\mathfrak{m},1} = \{\mathrm{div}(f) : f \in K^\times \text{ and } v_P(f-1) \geq v_P(\mathfrak{m}) \text{ for all } P \in \mathrm{Pl}_K\}.$$

A subgroup H of $\mathrm{Div}_\mathfrak{m}$ of finite index is called a *congruence subgroup modulo* $\mathfrak{m}$ if H contains $P_{\mathfrak{m},1}$.

By the Artin Reciprocity Law, for every finite abelian extension L of K there exist a modulus $\mathfrak{m}$ and a congruence subgroup $H_\mathfrak{m}(L)$ modulo $\mathfrak{m}$ such that the Artin map provides an isomorphism of groups

$$\mathrm{Gal}(L/K) \cong \mathrm{Div}_\mathfrak{m}/H_\mathfrak{m}(L).$$

Such a $\mathfrak{m}$ is called an *admissible modulus for* L/K; it is not unique (whereas for a given $\mathfrak{m}$, $H_\mathfrak{m}(L)$ is), but there exists an admissible modulus $\mathfrak{f}_{L/K}$ for L/K, called the *conductor of* L/K, which is smaller than the others in the sense that every admissible modulus $\mathfrak{m}$ for L/K satisfies $\mathfrak{f}_{L/K} \leq \mathfrak{m}$ (as divisors). An important property of the conductor of an abelian extension is that its support consists of exactly those places which are ramified.

The Existence Theorem of Class Field Theory guarantees for any modulus $\mathfrak{m}$ and any congruence subgroup $H_\mathfrak{m}$ modulo $\mathfrak{m}$ the existence of a unique global function field $L_\mathfrak{m}(H_\mathfrak{m})$, possibly defined over a constant field extension, which is a finite abelian extension of K such that

$$\mathrm{Gal}(L_\mathfrak{m}(H_\mathfrak{m})/K) \cong \mathrm{Div}_\mathfrak{m}/H_\mathfrak{m}.$$

The field $L_\mathfrak{m}(H_\mathfrak{m})$ is called the *class field* of $H_\mathfrak{m}$. Note that by definition of the conductor, $\mathfrak{f}_{L_\mathfrak{m}(H_\mathfrak{m})/K} \leq \mathfrak{m}$.

Instead of working with congruence subgroups modulo a certain $\mathfrak{m}$, it is sometimes more convenient to consider subgroups of the *ray class group modulo* $\mathfrak{m}$, which is the quotient group

$$\mathrm{Pic}_\mathfrak{m} = \mathrm{Div}_\mathfrak{m}/P_{\mathfrak{m},1}.$$

To each congruence subgroup H modulo $\mathfrak{m}$, one can associate the subgroup $\bar{H} = H/P_{\mathfrak{m},1}$ of $\mathrm{Pic}_\mathfrak{m}$ of finite index. This correspondence is one-to-one, and furthermore we have the isomorphism

$$\mathrm{Pic}_\mathfrak{m}/\bar{H} \cong \mathrm{Div}_\mathfrak{m}/H.$$

We can thus restate what has been said above as follows:

Theorem 1 (Main Theorem of Class Field Theory). *Let* $\mathfrak{m}$ *be a modulus. There is a 1-1 inclusion reversing correspondence between subgroups* H *of* $\mathrm{Pic}_\mathfrak{m}$ *of finite index and finite abelian extensions* L *of* K *with conductor less than* $\mathfrak{m}$*. Furthermore the Artin map provides an isomorphism*

$$\mathrm{Pic}_\mathfrak{m}/H \cong \mathrm{Gal}(L/K).$$

2. Computing the equation of an abelian covering

In all this section, K is a function field defined over a finite field $\mathbb{F}_q$. We fix a modulus $\mathfrak{m}$ and a congruence subgroup H modulo $\mathfrak{m}$, and we explain how to compute the class field L of H. The similar approach for number fields has been introduced by the second author in [Fie01], where one will find more algorithmic details, and the computations of groups of units and ray class groups are explained in [HPP03].

2.1. **Reduction to the cyclic case.**

First, we show that we can reduce the problem to the case of a cyclic extension of prime power degree. For this, we use the fundamental theorem of abelian groups to decompose $\bar{H} = \mathrm{Div}_\mathfrak{m}/H$ as a finite product of cyclic groups $\bar{H} = \prod_{i=1}^d \bar{H}_i$, where each $\bar{H}_i$ is of the form $\mathrm{Div}_\mathfrak{m}/H_i$ for a subgroup $H \subseteq H_i \subseteq \mathrm{Div}_\mathfrak{m}(K)$ such that $\bar{H}_i \cong \mathbb{Z}/(p_i^{m_i}\mathbb{Z})$ for some prime number p_i and some positive integer m_i. For every i, let L_i be the class field of H_i, so $\mathrm{Gal}(L_i/K) \cong \bar{H}_i$, and let L' be the composite field $L_1 L_2 \cdots L_d$. By general Galois theory, $\mathrm{Gal}(L'/K)$ is isomorphic to the subgroup of elements of $\prod_{i=1}^d \mathrm{Gal}(L_i/K)$ which agree on $L_1 \cap \cdots \cap L_d$. The functoriality of the Artin map implies that the previous condition is always true, so $\mathrm{Gal}(L'/K) \cong \prod_{i=1}^d \mathrm{Gal}(L_i/K)$. Thus $\mathrm{Gal}(L/K)$ and $\mathrm{Gal}(L'/K)$ are equal, and by the uniqueness property of the class field, we conclude that $L = \prod_{i=1}^d L_i$. Also, note that if we have equations for two abelian extensions L_1/K and L_2/K, then there are algorithms based on the theory of resultants to compute an equation of L_1L_2/K.

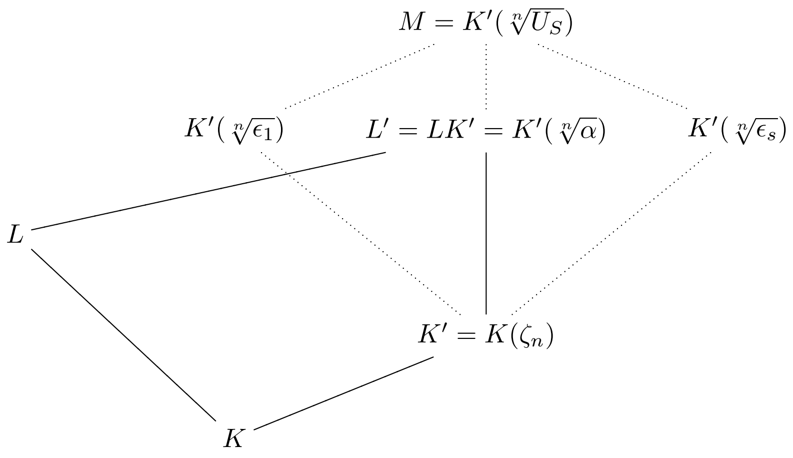
$M = K'(\sqrt[n]{U_S})$
$K'(\sqrt[n]{\epsilon_1})$
$L' = LK' = K'(\sqrt[n]{\alpha})$
$K'(\sqrt[n]{\epsilon_s})$
L
$K' = K(\zeta_n)$
K

Diagram 1. Fields used implicitly

2.2. **Cyclic case: $l \neq p$.** Now suppose that $\bar{H}$ is cyclic of prime power degree $n = l^m$ for a prime l different from p and an integer $m \geq 1$. As in the proof of the Existence Theorem (see [Lan94, Chap. XI, §2]), the idea consists in reducing to the case when K contains the n-th roots of unity, and then to use explicit Kummer theory. So let $K' = K(\zeta_n)$ and set $L' = LK'$: we will 'translate" the problem to the extension L'/K' (note that the extension K'/K is a constant field extension, hence it is unramified).

We will use the diagram 1 where solid lines connect fields that are actually constructed during the execution of the algorithm, while dotted lines connect fields that are only implicitly used.

Since L/K is cyclic of degree n, the field $L' := L(\zeta_n) = K'L$ is a Kummer extension of K', hence there exists a non-zero element $\alpha \in K'$ such that $L' = K'(\sqrt[n]{\alpha})$. Since L'/K has to be unramified outside places in the modulus $\mathfrak{m}$ of L/K, there exists a set S of places of K', depending only on $\mathfrak{m}$ and K', such that α can be chosen as an element of the S-units U_S, *i.e.* as an element that has no poles outside S; in particular, L'/K' is unramified[1] outside S. Let $\mathfrak{m}'$ be an admissible modulus for L'/K', and assume without loss of generality that $\mathfrak{m}'$ is supported on S. By the Dirichlet Unit Theorem, $U_S = \langle \epsilon_1, \ldots, \epsilon_s \rangle$ for independent elements ϵ_i $(1 \leq i \leq s-1)$ and a torsion unit ϵ_s. We set $M := K'(\sqrt[n]{U_S})$ and get $\mathrm{Gal}(M/K') = (\mathbb{Z}/n\mathbb{Z})^s$. For any place P of K' unramified in M/K', the Frobenius $(P, M/K')$ at P is defined by its operation on the $\sqrt[n]{\epsilon_i}$, thus since M/K' is unramified outside S, we get a map $\mathrm{Div}_{\mathfrak{m}'} \to (\mathbb{Z}/n\mathbb{Z})^s$ defined by $P \mapsto (n_i)$, where $\sqrt[n]{\epsilon_i} \mapsto \zeta_n^{n_i} \sqrt[n]{\epsilon_i}$ and $\sqrt[n]{\epsilon_i}^N \equiv \zeta_n^{n_i} \sqrt[n]{\epsilon_i} \bmod P$, with N the cardinality of the residue field $\mathbb{F}_P$ of K' at P. In particular, $N \equiv 1 \bmod n$ because $\mathbb{F}_P$ contains the n-roots of unity, thus n_i is defined by $\epsilon_i^{\lceil N/n \rceil} \equiv \zeta_n^{n_i} \bmod P$. To summarize: the Artin map from $\mathrm{Div}_{\mathfrak{m}'}$ to $(\mathbb{Z}/n\mathbb{Z})^s$ is explicit and can be computed in K' already!

[1] This is a general property of Kummer extensions, which follows from Hensel's lemma, see for example [Neu99, Lem. V.3.3].

$$\begin{tikzcd}
\mathrm{Div}_{\mathfrak{m}'} \arrow[r, "{(\cdot, M/K')}"] \arrow[d, "N_{K'/K}"'] & \mathrm{Gal}(M/K') \arrow[dl, "\psi"] . \\
\mathrm{Div}_{\mathfrak{m}}/H &
\end{tikzcd}$$

Diagram 2. Definition of ψ

Now, to find L' we need to find divisors $D \in \mathrm{Div}_{\mathfrak{m}'}$ such that $(D, M/K')$ fixes L'. By the Existence Theorem, this is equivalent to $D \in H'$, where H' is the congruence subgroup modulo $\mathfrak{m}'$ whose class field is L'. By standard properties of the Artin map, this reduces to $\mathrm{N}_{K'/K}(D) \in H$. We use this as summarized in diagram 2 to explicitly construct the map ψ: computing $(P, M/K')$ on the one side and $\mathrm{N}_{K'/K}(P) + H \in \mathrm{Div}_{\mathfrak{m}}/H$ on the other, we collect (small) places outside S until the full group $\mathrm{Gal}(M/K')$ can be generated. The field L' is then obtained as the field fixed by the kernel of ψ.

In order to find α we apply a similar idea again ([Fie01, §4] for details): L'/K is abelian and the Galois group can be computed explicitly. Once the automorphisms of L'/K are known, we can easily establish again an explicit Artin map, now from $\mathrm{Div}_{\mathfrak{m}}$ to $\mathrm{Gal}(L'/K)$, and find the subgroup fixing L as above. We note that the conductor of L' can be larger than the conductor of L/K, but since L' is obtained via a constant field extension, the ramified primes remain the same, hence the map is well defined and surjective (but the kernel may not be a congruence subgroup modulo $\mathfrak{m}$).

2.3. **Cyclic case: $l = p$.** Finally we turn to the case when L/K is cyclic of degree $n = p^m$, for an integer $m \geq 1$. To begin with, we recall some aspects of Artin-Schreier-Witt theory. Let k be any field and let $\bar{k}$ be an algebraic closure of k. Let r be an integer and let $\mathrm{W}_r(k)$ and $\mathrm{W}_r(\bar{k})$ be the rings of *Witt vectors of length* r with coefficients in k and $\bar{k}$ respectively. Then any $\vec{\alpha}$ in $\mathrm{W}_r(\bar{k})$ can generate an algebraic extension $k(\vec{\alpha})$ of k in the following way: if $\vec{\alpha} = (\alpha_1, \ldots, \alpha_r)$, then we set

$$k(\vec{\alpha}) = k(\alpha_1, \ldots, \alpha_r).$$

This construction is equivalent to that of the tower

$$\begin{array}{ccl}
k_r & = & k(\vec{\alpha}), \\
\uparrow & & \\
\vdots & & \\
\uparrow & & \\
k_2 & = & k_1(\alpha_2), \\
\uparrow & & \\
k_1 & = & k_0(\alpha_1), \\
\uparrow & & \\
k_0 & = & k
\end{array}$$

Suppose now that k has positive characteristic p. Let $\wp$ be the Artin-Schreier-Witt operator acting on $\vec{\alpha} \in \mathrm{W}_r(\bar{k})$ by

$$\wp(\vec{\alpha}) = \vec{\alpha}^p - \vec{\alpha} = (\alpha_1^p - \alpha_1, \dots, \alpha_r^p - \alpha_r).$$

Then for $\vec{\beta}$ in $\mathrm{W}_r(k)$ the equation $\wp(\vec{\alpha}) = \vec{\beta}$ is algebraic over k, so as above one can consider the extension $k(\wp^{-1}(\vec{\beta}))$. Actually, by explicit Artin-Schreier-Witt theory (see [Lan02, pp. 330-332]), every abelian extension of exponent p^r of k arises as a $k(\wp^{-1}(\Delta_r))$ for some subgroup $\Delta_r \subseteq \mathrm{W}_r(k)$ containing $\wp(\mathrm{W}_r(k))$. In particular, a cyclic extension of degree p^r of k is of the form $k(\vec{\gamma})$ for some $\vec{\gamma}$ in $\wp^{-1}(k) \subset \mathrm{W}_r(\bar{k})$, with Galois group generated by the automorphism $\vec{\gamma} \mapsto \vec{\gamma} + (1, 0, ..., 0)$ (see [Sch36]).

So for our purpose we take $r = m$ and can assume that the cyclic extension of degree p^m of K is of the form $L = K(\vec{y})$ for some $\vec{x} \in \mathrm{W}_m(K)$ and $\vec{y} \in \mathrm{W}_m(\bar{K})$ satisfying $\wp(\vec{y}) = \vec{x}$, and we now explain how to compute $\vec{x}$. It is clear that the Artin-Schreier-Witt extension does not change if one replaces $\vec{x}$ with $\vec{x} + \wp(\vec{z})$ for some $\vec{z}$ in $\mathrm{W}_m(K)$, so one will look for $\vec{x}$ as an element of $\mathrm{W}_m(K)/\wp(\mathrm{W}_m(K))$.

We first look at the case $m = 1$; hence we assume that L/K is a cyclic extension of degree p, and denote $\vec{x} = x$.

Lemma 2. *Let $y \in K$ be arbitrary. For every place P of K there exists an element $u_P \in K$ such that either $v_P(y + u_P^p - u_P)$ is negative and coprime to p, or $v_P(y + u_P^p - u_P) \geq 0$.*

Proof. If $v_P(y) \geq 0$ or $v_P(y)$ is coprime to p then $u_P := 0$ works, hence assume $v_P(y) < 0$ and $p | v_P(y)$. Let $\bar{y} := (y\pi^{-v_P(y)})(P) \in \mathbb{F}_P$, where $\mathbb{F}_P$ is the residue class field of K at P and π a uniformizing element (*i.e.* $v_P(\pi) = 1$). Since the p-power Frobenius is surjective, we can find a $\bar{u} \in \mathbb{F}_P$ such that $\bar{u}^p = -\bar{y}$. Now let u be a lift of $\bar{u}$ in K: there exists $a \in K$ with $v_P(a) > v_P(y)$ such that $y + u^p\pi^{v_P(y)} = a$. Then, since $v_P(y) < v_P(y)/p < 0$, we have $v_P(y + (u\pi^{v_P(y)/p})^p - u\pi^{v_P(y)/p}) \geq \min\{v_P(a), v_P(y)/p\} > v_P(y)$ (note that $v_P(u) = 0$), and we can recurse. □

We make also use of the fact that the ramified places P in L/K (which appear in the support of $\mathfrak{m}$) are exactly those for which there exists u_P as above such that $\lambda_P := -v_P(y + u_P^p - u_P)$ is positive and coprime to p; furthermore, the conductor $\mathfrak{f}_{L/K}$ verifies $v_P(\mathfrak{f}_{L/K}) = \lambda_P + 1$ (use [Sti09, Prop. 3.7.8] and Proposition 4 below), so λ_P does not depend on y. Thus Lemma 2 is useful to understand the ramification in L/K, but to compute explicitly L, we need to find a Riemann-Roch space containing the generator x. So we combine Lemma 2 with the Strong Approximation Theorem to get a global result:

Lemma 3. *Let $y \in K$. For every place P, let u_P and λ_P be as above. Let S be the set of places P of K such that $\lambda_P > 0$, and let $S' := \{P \in \mathrm{Pl}_K : v_P(y) < 0\}$, so $S \subseteq S'$. Fix an arbitrary place $P_0 \notin S'$, and let n_0 be a positive integer such that $D := n_0 P_0 - \sum_{P \in S'} 2P$ is non-special. Then there exists some u such that $v_P(y + u^p - u) = -\lambda_P$ for $P \in S$, $v_P(y + u^p - u) \geq 0$ for $P \notin S \cup \{P_0\}$, and $v_{P_0}(y + u^p - u) \geq -pn_0$.*

Proof. By the Strong Approximation Theorem and its proof (see [Sti09, Theo. 1.6.5.]), there exists an element u in K such that $v_P(u - u_P) = 1$ for $P \in S'$, $v_P(u) \geq 0$ for $P \notin S' \cup \{P_0\}$, and $v_{P_0}(u) \geq -n_0$. We have:

$$\begin{aligned} v := v_P(y + u^p - u) &= v_P(y + u_P^p - u_P + (u - u_P)^p + (u_P - u)) \\ &\geq \min\{v_P(y + u_P^p - u_P), pv_P(u - u_P), v_P(u_P - u)\}, \end{aligned}$$

which provides that $v = -\lambda_P$ if $P \in S$, and $v \geq 0$ if $P \in S' \setminus S$. In the same way,

$$\begin{array}{rcl} v & = & v_P(y + u_P^p - u_P + (u^p - u) - (u_P^p - u_P)) \\ & \geq & \min\{v_P(y + u_P^p - u_P), v_P(u^p - u), v_P(u_P^p - u_P)\}, \end{array}$$

so we also have that $v \geq 0$ if $P \notin S' \cup \{P_0\}$, and $v \geq -pn_0$ if $P = P_0$ (note that $u_P = 0$ when $P \notin S'$). □

Thus we have that $x := y + u^p - u$ is an element of the Riemann-Roch space

$$\mathcal{L}(pn_0P_0 + \sum_S \lambda_P P) = \{f \in K : \operatorname{div}(f) \geq -pn_0P_0 - \sum_S \lambda_P P\}.$$

We now turn back to our hypothesis that L/K is a cyclic extension of degree p^m, for some $m \geq 1$, with primitive element $\vec{x}$. Following [Sch36], we study the vector $\lambda_P := -v_P(\vec{x}) := (-v_P(x_1), \ldots, -v_P(x_m))$. By adding elements of the form $\wp(0, \ldots, 0, x, 0, \ldots, 0)$ we can assume that there exist sets $S_i \subset \operatorname{Supp}(\mathfrak{m})$, places $P_{0,i}$ not in S_i and positive integers $n_{0,i}$ such that x_i is in $\mathcal{L}(pn_{0,i}P_{0,i} + \sum_{S_i} \lambda_{P,i}P)$, where $\lambda_{P,i} := -v_P(x_i) > 0$ and $\gcd(\lambda_{P,i}, p) = 1$ for $P \in S_i$.

Setting $M_P := \max\{p^{m-i}\lambda_{P,i} : 1 \leq i \leq m\}$, we obtain $v_P(\mathfrak{f}_{L/K}) = M_P + 1$ from [Sch36, p. 163]. Given that we already know a modulus $\mathfrak{m}$ such that $\mathfrak{f}_{L/K} \leq \mathfrak{m}$, we immediately get $\lambda_{P,i} \leq (v_P(\mathfrak{m}) - 1)p^{i-m}$. If $\mathfrak{m} = \sum_P n_P P$, then we set $D_i := pn_{0,i}P_{0,i} + \sum_{S_i}(n_P - 1)p^{i-m}P$. With these notations, we see that x_i is an element of $\mathcal{L}(D_i)$.

By induction, we assume that the x_i have been computed for $1 \leq i \leq m-1$ and explain how to find x_m. Set $M_m := K(\wp^{-1}(x_1, \ldots, x_{m-1}))$ and $D := D_m$; as remarked above, we can identify x_m as an element of the $\mathbb{F}_q$-vector space

$$\overline{\mathcal{L}_K}(D) = \mathcal{L}_K(D)/\wp(\mathcal{L}_K(D)).$$

Let d be its dimension over $\mathbb{F}_p$. Then we compute a $\mathbb{F}_p$-basis of $\overline{\mathcal{L}_K}(D)$, and lift it to a set of d elements $\{f_1, \ldots, f_d\}$ of $\mathcal{L}_K(D)$. Hence x_m is an element of the sub-vector space of $\mathcal{L}_K(D)$ generated by the f_i:

$$x_m = \sum_{i=1}^d a_i f_i$$

for some unknown elements a_i of $\mathbb{F}_p$. Next, we set

$$M := K(\wp^{-1}((x_1, \ldots, x_{m-1}, \mathcal{L}_K(D)))) = M_m(\wp^{-1}(0, \ldots, 0, \mathcal{L}_K(D))),$$

so that we have a tower $K \subset M_m \subset L \subset M$. Note that similar to the Kummer case, neither M nor M_m is actually ever constructed. We will use the explicit action of the Frobenius automorphisms on Witt vectors of length m, so we identify $(x_1, \ldots, x_{m-1})$ with $(x_1, \ldots, x_{m-1}, 0) \in \mathrm{W}_m(K)$ and f_i with $(0, \ldots, 0, f_i) \in \mathrm{W}_m(K)$. Let P be an unramified place of K; then the Frobenius automorphism $(P, L/K)$ acts on $\vec{y}$ as follows (see [Sch36]):

$$(P, L/K)(\vec{y}) = \vec{y} + \left\{\frac{\vec{x}}{P}\right\},$$

where the last term is in $\mathrm{W}_m(\mathbb{F}_p) \cong \mathbb{Z}_p \bmod p^m$ and verifies

$$\left\{\frac{\vec{x}}{P}\right\} = \operatorname{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\vec{x} + \vec{x}^q + \cdots + \vec{x}^{\frac{\mathrm{N}(P)}{q}} \bmod P).$$

We now compute $\operatorname{Gal}(M/M_m)$. We have canonical isomorphisms

$$\operatorname{Gal}(M/M_m) \cong \prod_{i=1}^{d} \operatorname{Gal}(M_m(0,\ldots,0,\wp^{-1}(f_i))/M_m) \cong (\mathbb{Z}/p\mathbb{Z})^d,$$

and this is explicit via the Frobenius: every $\operatorname{Gal}(M_m(0,\ldots,0,\wp^{-1}(f_i))/M_m)$ is generated by the isomorphisms $(Q, M_m(0,\ldots,0,\wp^{-1}(f_i))/M_m)$, where Q is a place of M_m. Because of the canonical isomorphism $\operatorname{Gal}(M_m(0,\ldots,0,\wp^{-1}(f_i))/M_m) \cong \operatorname{Gal}(K(\wp^{-1}(f_i))/K)$, they are of the form

$$y_i \mapsto y_i + \left\{\frac{f_i}{P}\right\},$$

where y_i is a primitive element of $K(\wp^{-1}(f_i))/K$ and P is the place of K below Q. Since the symbol $\{\cdot\}$ is additive ([Sch36]), we have

$$\operatorname{Gal}(K(\wp^{-1}(f_i))/K) \cong \left\langle \left\{\frac{f_i}{P}\right\} \right\rangle,$$

and so the isomorphism $\operatorname{Gal}(M/M_m) \cong (\mathbb{Z}/p\mathbb{Z})^d$ is explicit via the map

$$(Q, M/M_m) \mapsto \left(\left\{\frac{f_1}{P}\right\},\ldots,\left\{\frac{f_d}{P}\right\}\right).$$

We lift the terms in $\{\cdot\}$ from $\mathrm{W}_m(\mathbb{F}_p)$ to $\mathbb{Z}_p$, and if we can find enough places P_i such that the $\mathbb{Z}_p$-vectors

$$\left(\left\{\frac{f_1}{P_i}\right\},\ldots,\left\{\frac{f_d}{P_i}\right\}\right)_i$$

form a matrix of rank d over $\mathbb{Z}_p$, then we are done, because by Class Field Theory every element of $\operatorname{Gal}(M/M_m)$ is a Frobenius automorphism for some place Q. The generator is now obtained in exactly the same way as in the previous section for Kummer extensions – for which all that is necessary is an explict Artin map.

3. An algorithm to find curves with many points

We now turn to the explicit applications of the theory described in the preceding sections, and switch between the language of curves and function fields when necessary. Our aim here is to find curves of low genus ($g \leq 50$) defined over a small finite field ($q \leq 100$) such that the number of rational points is the maximum possible; the current records can be found at `www.manypoints.org`. So we will only be interested in the abelian extensions L/K defined over a same finite field $\mathbb{F}_q$ such that the number of rational places of the field L is greater or equal to the corresponding entry in the table[2]. Furthermore, with the theory of §2, we will be able to find the equations of such extensions.

Proposition 4. *Let L/K be a cyclic extension of prime degree l of function fields defined over a finite field $\mathbb{F}_q$. Then the genus of L satisfies:*

$$g_L = 1 + l(g_K - 1) + \frac{1}{2}(l-1)\deg(\mathfrak{f}_{L/K}).$$

[2] Note that L is defined over $\mathbb{F}_q$ as soon as at least one rational place of K splits totally in L, which will be the case to find a L with many rational places.

Proof. By the Riemann-Hurwitz Genus Formula, this comes down to showing that the degree of the different $\mathcal{D}_{L/K}$ of L/K is $(l-1)\deg(\mathfrak{f}_{L/K})$. Let Q be a place of L and let P be the place of K below Q. The extension being Galois, the inertia degree of P relatively to Q is independent of Q, so we denote it f_P. Let $\mathrm{N} = \mathrm{N}_{L/K} : \mathrm{Div}(L) \to \mathrm{Div}(K)$ be the norm map defined by linearizing the formula $\mathrm{N}(Q) = f_P P$. From the general relation $\deg(Q) = f_P \deg(P)$, we note that $\deg(\mathrm{N}(\mathcal{D}_{L/K})) = \deg \mathcal{D}_{L/K}$. By the Conductor-Discriminant Formula, $\mathrm{N}(\mathcal{D}(L_K))$ is equal to $\mathfrak{f}_{L/K}^{l-1}$, so by taking degrees we obtain the proposition. □

From Proposition 4, the genus of an abelian extension of global function fields L/K of prime degree is exactly determined by its conductor $\mathfrak{f}_{L/K}$, or even simply by its degree. On another side, $\mathfrak{f}_{L/K}$ identifies L as the only field such that the Galois group of L/K is a quotient of the ray class group modulo $\mathfrak{f}_{L/K}$ by a certain subgroup of finite index. So, starting from a prime number l and a modulus $\mathfrak{m}$ defined over a global function field K with field of constants $\mathbb{F}_q$, one can enumerate all the abelian extensions L of K of degree l and of conductor $\mathfrak{f}_{L/K}$ less than $\mathfrak{m}$ by computing all the subgroups of index l of $\mathrm{Pic}_{\mathfrak{m}}$. We also know in advance that the genus of these extensions will be less than

$$1 + l(g_K - 1) + \frac{1}{2}(l-1)\deg(\mathfrak{m}).$$

Since l is a prime, all places which ramify have the same ramification type: either they are all wildly ramified, or they are all tamely ramified. The following proposition thus describes what kind of $\mathfrak{m}$ one should test for a given l:

Proposition 5. *Let L/K be an abelian function field extension. Let P be a place of K. Then P is wildly ramified in L/K if and only if P appears in the conductor of L/K with multiplicity greater than 2, i.e.*

$$P \text{ is wildly ramified if and only if } \mathfrak{f}_{L/K} \geq 2P.$$

Proof. From [Mil11a, Cor. 7.59], we see that a place P is tamely ramified if and only if the first ramification group in upper numbering is trivial, and from the local-global property of the conductor, it amounts to saying that P has weight one in $\mathfrak{f}_{L_K}$. So a place with weight at least two must be wildly ramified. □

So if l is prime to the characteristic p of K, then $\mathfrak{m}$ must be of the form

$$\mathfrak{m} = \sum_{i=1}^{n} P_i,$$

whereas if l equals p, then $\mathfrak{m}$ must be of the form

$$\mathfrak{m} = \sum_{i=1}^{n} m_i P_i,$$

where $m_i \geq 2$.

Because we want the greatest possible number of rational places for the field L, and because of the formula

$$N(L) = l|S| + r$$

(where S is the set of rational places of K which split in L and r is the number of rational places in the support of $\mathfrak{f}_{L/K}$), it seems reasonable to start from a field K which itself has many rational points compared to its genus. In this way, we will find curves with many points and their equations recursively: we start from the projective line or a maximal[3] elliptic curve, compute all its 'best' coverings reaching or improving a lower bound in `www.manypoints.org`, and start the process again on these coverings, and so on. We summarize the process in Algorithm 1 below. Note that a reasonable restriction, especially when the size of the constant field increases, could be to take only conductors with places of degree 1 in their support.

Algorithm 1 Good Abelian Covering

```
Input: A function field $K/\mathbb{F}_q$, a prime $l$, an integer $G$.
Output: The equations of all cyclic extensions of $K$ of degree $l$ and genus less than
    $G$ whose number of $\mathbb{F}_q$-rational points improves the best known records.
Compute all the moduli of degree less than $B = (2G-2-l(2g(K)-2))/(l-1)$
using Proposition 5.
for each such modulus $\mathfrak{m}$ do
    Compute the ray class group $\mathrm{Pic}_{\mathfrak{m}}$ modulo $\mathfrak{m}$.
    Compute the set $S$ of subgroups of $\mathrm{Pic}_{\mathfrak{m}}$ of index $l$.
    for every $s$ in $S$ do
        Compute the genus $g$ and the number of rational places $n$ of the class field
        $L$ of $s$.
        if $n$ is greater or equal to the known record for a genus $g$ curve defined
        over $\mathbb{F}_q$ then
            Update $n$ as the new lower bound on $N_q(g)$.
            Compute and output the equation of $L$.
        end if
    end for
end for
```

The complexity of the algorithm is linear in the number of fields (or pairs of divisors and subgroups) we need to consider. The total number of divisors of degree bounded by B is roughly $O(q^B)$ since this is the estimate for the number of irreducible polynomials of degree bounded by B already. The number of subgroups to consider depends on the structure of the ray class group. For tamely ramified extensions, the group is the extension of the divisor class group by the product of the multiplicative groups of the divisors (modulo constants), so the number of cyclic factors depends on the number of places such that $l|q^{\deg P}-1$. For wild extensions, the number of ramified places provides the same information. In the wild case, the number is bounded by $B/2$, so the total number of fields to investigate is roughly $O(q^B \cdot q^{B/2})$. For each pair we have to compute the genus and the number of rational places. The computation of the genus can be seen to run in time quartic in the number of (potentially) ramified places: for each place we need to check if it divides the conductor. This test is done by some $\mathbb{Z}$-HNF computation of a matrix of dimension depending on the total number of places again. The number of rational places requires to compute discrete logarithms in the divisor class group for every rational place of the base field. Assuming a small degree, this depends linearly on the number of ramified places.

[3] We call a curve of genus g defined over $\mathbb{F}_q$ *maximal* if no genus g curve defined over $\mathbb{F}_q$ has more points. This number of points is denoted $N_q(g)$.

To summarize: the total complexity is essentially exponential in the genus bound, thus limited in scope.

Remark 6. *It is possible to extend the algorithm to coverings of non-prime degrees, to include Artin-Schreier-Witt extensions for example, and this is what has been implemented in Magma. The genus and the conductor can then be computed using techniques from* [HPP03].

4. Results

We now present the results we have obtained. We have restricted to the case of $\mathbb{F}_2$. The computations have been performed with Magma, thanks to a Class Field Theory library implemented by the second author. The results are summarized in the table below. The notations are as follows: g_0 is the genus of the base curve and g and N are the genus and the number of rational points of the abelian covering respectively. The Oesterlé bound on the number of rational points of a genus g curve defined over $\mathbb{F}_q$ corresponds to the "OB" column. The conductor of the covering is added in the column "$\mathfrak{f}$": in this column, $n_i P_i$ means that there is a place of degree i occurring in the conductor with weight n_i. The Galois group of the covering is G, the number of totally split places is $|S|$, the number of totally ramified places is $|T|$ and the number of non-totally ramified places is $|R|$. When the result has been obtained using a non-maximal base curve, we denote the corresponding genus "g_0'" (see below for the equations of the base curves we have used). Note also that several results have been obtained by more than one means; however, we have entered in the table only the data corresponding to the smallest base genus. We have used the 7 following maximal curves over $\mathbb{F}_2$ as base curves whose equations have been computed by Algorithm 1 (the genus of the i-th curve is i):

(1) $y^2 + y - x^3 - x$
(2) $y^2 + (x^3 + x + 1)y + x^5 + x^4 + x^3 + x$
(3) $x^3y + x^2y^2 + x + x^2 + y^3 + y$
(4) $y^4 + (x + 1)y^2 + (x^3 + x)y + x^7 + x^3$
(5) $y^4 + (x^2 + x + 1)y^2 + (x^2 + x)y + x^7 + x^6 + x^5 + x^4$
(6) $y^4 + (x^6 + x^5 + x^4 + 1)y^2 + (x^7 + x^4 + x^3 + x^2)y + x^{11} + x^{10} + x^3 + x^2$
(7) $y^4 + (x^9 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2)y^2 + (x^{11} + x^9 + x^8 + x^7 + x^5 + x^4)y + x^{14} + x^{12} + x^{11} + x^7$

We have also used the following 7 base curves whose number of rational points is $\mathbb{N}_q(g) - 1$ (the genus of the i-th curve is again i):

(1) $y^2 + xy + x^3 + x$
(2) $y^2 + y + x^5 + x$
(3) $y^4 + (x^2 + x + 1)y^2 + (x^2 + x)y + x^6 + x^5$
(4) $y^4 + xy^2 + (x + 1)y + x^5 + x^4 + x^3 + x^2$
(5) $y^4 + (x^3 + 1)y^2 + (x^4 + x^2)y + x^9 + x^5$
(6) $y^4 + (x^3 + x + 1)y^2 + (x^3 + x)y + x^9 + x^8 + x^5 + x^4$
(7) $y^4 + x^7y^2 + (x^7 + 1)y + x^5 + x$

At last, we mention that the average bound on the degree of the possible conductors we have tested was 14. The results are summarized in Table 1.

Due to the size of the equations, we only give an explicit model for the maximal curves of genus 14, 17 and 24 that we have found:

(1) $y^8 + (x^{10} + x^8 + x^6 + x^4 + x^3 + x)y^6 + (x^{17} + x^{15} + x^9 + x^7 + x^3 + x)y^5 + (x^{28} + x^{23} + x^{22} + x^{19} + x^{18} + x^{16} + x^{14} + x^{12} + x^{11} + x^{10} + x^9 + x^7 + x^5 + x^4 + x^2 + x + 1)y^4 + (x^{31} + x^{29} + x^{15} + x^{13} + x^3 + x)y^3 + (x^{40} + x^{37} + x^{36} + x^{30} + x^{24} + x^{21} + x^{20} + x^{14} + x^{12} + x^9 + x^8 + x^2)y^2 + (x^{47} + x^{45} + x^{39} + x^{37} + x^{33} + x^{29} + x^{23} + x^{21} + x^{19} + x^{15} + x^{11} + x^9 + x^5 + x^3)y + x^{60} + x^{58} + x^{53} + x^{51} + x^{49} + x^{47} + x^{46} + x^{45} + x^{44} + x^{43} + x^{41} + x^{38} + x^{36} + x^{32} + x^{31} + x^{29} + x^{27} + x^{26} + x^{23} + x^{22} + x^{20} + x^{18} + x^{15} + x^{14} + x^{13} + x^{10} + x^9 + x^8 + x^7 + x^5;$

(2) $y^8 + (x^{20} + x^{13} + x^{10} + x^9 + x^2)y^4 + (x^{26} + x^{24} + x^{22} + x^{19} + x^{18} + x^{17} + x^{13} + x^{11} + x^{10} + x^4)y^2 + (x^{27} + x^{25} + x^{20} + x^{19} + x^{18} + x^{16} + x^{14} + x^{13} + x^{11} + x^7)y + x^{33} + x^{31} + x^{30} + x^{28} + x^{27} + x^{26} + x^{25} + x^{24} + x^{22} + x^{21} + x^{20} + x^{16} + x^{12} + x^{10} + x^9 + x^8;$

(3) $y^{16} + (x^{18} + x^{17} + x^{15} + x^{14} + x^{10} + x^8)y^{12} + (x^{28} + x^{27} + x^{26} + x^{22} + x^{21} + x^{14})y^{10} + (x^{31} + x^{30} + x^{29} + x^{27} + x^{26} + x^{25} + x^{23} + x^{19})y^9 + (x^{48} + x^{43} + x^{39} + x^{38} + x^{37} + x^{34} + x^{33} + x^{32} + x^{31} + x^{30} + x^{29} + x^{28} + x^{27} + x^{25} + x^{23} + x^{22} + x^{21} + x^{20} + x^{18})y^8 + (x^{48} + x^{47} + x^{46} + x^{40} + x^{34} + x^{33} + x^{32} + x^{26}) * y^6 + (x^{51} + x^{50} + x^{49} + x^{43} + x^{39} + x^{38} + x^{37} + x^{31})y^5 + (x^{72} + x^{71} + x^{70} + x^{69} + x^{68} + x^{67} + x^{65} + x^{59} + x^{58} + x^{56} + x^{51} + x^{49} + x^{47} + x^{45} + x^{42} + x^{41} + x^{40} + x^{38} + x^{36} + x^{34} + x^{33} + x^{31} + x^{30} + x^{28})y^4 + (x^{57} + x^{56} + x^{55} + x^{48} + x^{47} + x^{41})y^3 + (x^{82} + x^{81} + x^{77} + x^{76} + x^{75} + x^{73} + x^{72} + x^{69} + x^{68} + x^{67} + x^{64} + x^{61} + x^{58} + x^{57} + x^{55} + x^{54} + x^{53} + x^{50} + x^{49} + x^{48} + x^{45} + x^{44} + x^{40} + x^{39} + x^{38} + x^{37} + x^{36} + x^{34})y^2 + (x^{85} + x^{84} + x^{81} + x^{77} + x^{75} + x^{74} + x^{72} + x^{71} + x^{70} + x^{69} + x^{68} + x^{65} + x^{63} + x^{62} + x^{60} + x^{59} + x^{58} + x^{57} + x^{55} + x^{54} + x^{53} + x^{50} + x^{48} + x^{46} + x^{44} + x^{42} + x^{41} + x^{39})y + x^{108} + x^{97} + x^{96} + x^{95} + x^{91} + x^{90} + x^{88} + x^{87} + x^{86} + x^{83} + x^{82} + x^{81} + x^{78} + x^{76} + x^{75} + x^{72} + x^{70} + x^{69} + x^{68} + x^{64} + x^{63} + x^{58} + x^{55} + x^{53} + x^{52} + x^{51} + x^{50} + x^{46}.$

g	N-OB	g_0	$\mathfrak{f}$	G	$\lvert S\rvert$	$\lvert T\rvert$	$\lvert R\rvert$
14	16	4	$2P_7$	$\mathbb{Z}/2\mathbb{Z}$	16	0	0
17	18	2	$4P_1 + 6P_1$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	16	2	0
24	23	$4'$	$2P_1 + 4P_1 + 2P_2$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	20	1	2
29	$26-27$	4	$4P_1 + 8P_1$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	24	2	0
41	$34-35$	$3'$	$4P_1 + 4P_1$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	32	2	0
45	$34-37$	2	$4P_1 + 8P_1$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	32	2	0
46	$35-38$	3	$3P_1 + 8P_1$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	32	1	2

TABLE 1. New results over $\mathbb{F}_2$

Remark 7. *Since the article has been written, a preprint of Karl Rökaeus has appeared in which he undertakes similar computations over the finite fields of size* 2*,* 3*,* 4 *and* 5 *(see* [Rök12]*). Over* $\mathbb{F}_2$ *he recovers the genus* 17 *record, and improves our genus* 45 *bound to* 36 *points (he also wrote us that he found a genus* 46 *curve with* 36 *points).*

Remark 8. *As mentionned above, we have restricted the search to $\mathbb{F}_2$. However, a curve of genus 11 with 21 points has been found over $\mathbb{F}_3$ while testing the code. It is a degree 2 cover of the genus 4 maximal curve defined by*

$$C : y^4 + 2y^2 + x^6 + x^4 + x^2.$$

With notations as above, the conductor is of the form $P_1 + P_1 + P_1 + P_5$. The resulting curve has equation as follows:

$$\begin{aligned} C' : {} & y^8 + (2x^{10} + x^9 + 2x^7 + x^6 + 2x^5 + 2x^4 + x^3 + x^2)y^6 + (2x^{20} + 2x^{19} + 2x^{18} + \\ & x^{17} + x^{16} + x^{15} + 2x^{14} + 2x^{12} + 2x^{11} + x^{10} + 2x^9 + 2x^8 + x^7 + 2x^6 + x^4)y^4 + \\ & (x^{30} + 2x^{28} + x^{24} + x^{23} + 2x^{22} + x^{21} + x^{20} + 2x^{19} + x^{18} + x^{17} + 2x^{16} + x^{15} + \\ & x^{14} + 2x^{13} + x^{11} + x^9 + x^8 + 2x^7)y^2 + x^{40} + x^{39} + 2x^{37} + x^{35} + 2x^{32} + x^{31} + \\ & x^{30} + x^{29} + 2x^{28} + 2x^{22} + 2x^{21} + x^{19} + 2x^{17} + x^{14} + 2x^{13} + 2x^{12} + 2x^{11} + x^{10}. \end{aligned}$$

References

[Aue99] Roland Auer. *Ray Class Fields of Global Function Fields with Many Rational Places.* PhD thesis, Carl-von-Ossietzky-Universität Oldenburg, 1999.

[Aue00] Roland Auer. Curves over finite fields with many rational points obtained by ray class field extensions. In *Algorithmic number theory (Leiden, 2000)*, volume 1838 of *Lecture Notes in Comput. Sci.*, pages 127–134. Springer, Berlin, 2000.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[Cas67] J. W. S. Cassels. Global fields. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 42–84. Thompson, Washington, D.C., 1967.

[Fie01] Claus Fieker. Computing class fields via the Artin map. *Math. Comp.*, 70(235):1293–1303 (electronic), 2001.

[Fie06] Claus Fieker. Applications of the class field theory of global fields. In *Discovering mathematics with Magma*, volume 19 of *Algorithms Comput. Math.*, pages 31–62. Springer, Berlin, 2006.

[Gop77] V. D. Goppa. Codes that are associated with divisors. *Problemy Peredači Informacii*, 13(1):33–39, 1977.

[HPP03] Florian Hess, Sebastian Pauli, and Michael E. Pohst. Computing the multiplicative group of residue class rings. *Math. Comp.*, 72(243):1531–1548 (electronic), 2003.

[Lan94] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1994.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, third edition, 2002.

[Lau96] Kristin Lauter. Ray class field constructions of curves over finite fields with many rational points. In *Algorithmic number theory (Talence, 1996)*, volume 1122 of *Lecture Notes in Comput. Sci.*, pages 187–195. Springer, Berlin, 1996.

[Lau99a] Kristin Lauter. Deligne-Lusztig curves as ray class fields. *Manuscripta Math.*, 98(1):87–96, 1999.

[Lau99b] Kristin Lauter. A formula for constructing curves over finite fields with many rational points. *J. Number Theory*, 74(1):56–72, 1999.

[Mil11a] J. S. Milne. Algebraic number theory (v3.03), 2011. Available at www.jmilne.org/math/.

[Mil11b] J.S. Milne. Class field theory (v4.01), 2011. Available at www.jmilne.org/math/.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences].* Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[NX01] Harald Niederreiter and Chaoping Xing. *Rational points on curves over finite fields: theory and applications*, volume 285 of *London Mathematical Society Lecture Note Series.* Cambridge University Press, Cambridge, 2001.

[Rök12] Karl Rökaeus. New curves with many points over small finite fields. 2012. Available at "arXiv:1204.4355".

[Sch36] H.L. Schmid. Zur Arithmetik der zyklischen p-Körper. *Journal für die reine und angewandte Mathematik*, 176:161–167, 1936.

[Ser83] Jean-Pierre Serre. Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini. *C. R. Acad. Sci. Paris Sér. I Math.*, 296(9):397–402, 1983.

[Ser85] Jean-Pierre Serre. *Rational Points on Curves over Finite Fields*. September to December 1985. Lecture notes given at Harvard University. Notes by Fernando Q. Gouvéa.

[Sti09] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[Wei95] André Weil. *Basic number theory*. Classics in Mathematics. Springer-Verlag, Berlin, 1995. Reprint of the second (1973) edition.

Institut de Mathématiques de Luminy, Campus de Luminy, Case 907, 13288 MARSEILLE Cedex 9

E-mail address: `virgile.ducet@gmail.com`

Fachbereich Mathematik, Universität Kaiserslautern, Postfach 3049, 67653 Kaiserslautern

E-mail address: `fieker@mathematik.uni-kl.de`

URL: `http://www.mathematik.uni-kl.de/~fieker/`