THE OPEN BOOK SERIES 1

ANTS X
Proceedings of the Tenth Algorithmic Number Theory Symposium

Computing equations of curves with many points

Virgile Ducet and Claus Fieker

msp

THE OPEN BOOK SERIES 1 (2013)
Tenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2013.1.317

Computing equations of curves with many points

Virgile Ducet and Claus Fieker

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 seven new records over $\mathbb{F}_2$.

1. 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 subvector space of $\mathbb{F}_q^n$ of dimension k in which every nonzero vector has at least d nonzero 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, Goppa [7] proposed a method for constructing codes which is based on algebraic geometry. Let X be a (nonsingular 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 such that $2g-2 < \deg D_2 < n$. 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 for every differential ω let $\operatorname{res}_{P_i}(\omega)$ denote 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 $\omega \mapsto (\operatorname{res}_{P_1}(\omega), \ldots, \operatorname{res}_{P_n}(\omega))$. 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

MSC2010: primary 11R37; secondary 14H45.
Keywords: explicit class field theory, Kummer theory, Witt vectors, curves with many points, equations of abelian coverings.

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 [22]). His Harvard course notes [23] remain a very useful reference with a lot of material. Niederreiter and Xing continued the search for good curves and devoted many papers to finding and exploiting new techniques; in particular, they make use of the explicit description of ray class fields provided by the theory of Drinfel'd modules. Their book [18] includes all their work on the subject and much more. In a series of paper in the late 90s, Lauter [12; 13; 14] extended Serre's method and obtained new records by studying the degrees 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 Ph.D. thesis [1] or the ANTS paper [2] 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 ramified at most 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 can one deduce the equation of the curve from its theoretical construction; in particular, the so-called "explicit" description via Drinfel'd 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 we apply this method to the problem 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 from knowledge of the corresponding ray class group. In Section 4 we present an algorithm to find good curves, and we give an overview of our results in Section 5.

2. 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 [10], [15], or [25] 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, that is, 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 $\mathfrak{m}$":

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

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 that are ramified.

The existence theorem of class field theory guarantees, for every modulus $\mathfrak{m}$ and every 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, that 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, we have $\mathfrak{f}_{L_{\mathfrak{m}}(H_{\mathfrak{m}})/K} \leq \mathfrak{m}$.

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 $\overline{H} = H/P_{\mathfrak{m},1}$ of $\mathrm{Pic}_{\mathfrak{m}}$ of finite index. This correspondence is one-to-one, and furthermore we have an isomorphism $\mathrm{Pic}_{\mathfrak{m}}/\overline{H} \cong \mathrm{Div}_{\mathfrak{m}}/H$. 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 one-to-one 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* $\mathrm{Pic}_{\mathfrak{m}}/H \cong \mathrm{Gal}(L/K)$.

3. Computing the equation of an abelian covering

Throughout 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 [6], where one will find more algorithmic details; the computations of groups of units and ray class groups are explained in [8].

3.1. ***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 $\overline{H} = \mathrm{Div}_{\mathfrak{m}}/H$ as a finite product of cyclic groups $\overline{H} = \prod_{i=1}^{d} \overline{H}_i$, where each $\overline{H}_i$ is of the form $\mathrm{Div}_{\mathfrak{m}}/H_i$ for a subgroup $H \subseteq H_i \subseteq \mathrm{Div}_{\mathfrak{m}}$ such that $\overline{H}_i \cong \mathbb{Z}/p_i^{m_i}\mathbb{Z}$ 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 $\mathrm{Gal}(L_i/K) \cong \overline{H}_i$, 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 $L_1 L_2/K$.

3.2. ***Cyclic case: $l \neq p$.*** Now suppose that $\overline{H}$ 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 [10, Chapter XI, §2]), the idea consists of 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 refer to Figure 1; the solid lines in the figure 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', and hence there exists a nonzero 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, that is, 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, we have $U_S = \langle \epsilon_1, \ldots, \epsilon_s \rangle$ for independent elements ϵ_i $(1 \leq i \leq s-1)$ and a torsion unit ϵ_s. Set $M := K'(\sqrt[n]{U_S})$, so that $\mathrm{Gal}(M/K') = (\mathbb{Z}/n\mathbb{Z})^s$. For any place P of K' unramified in M/K', the Frobenius

[1] This is a general property of Kummer extensions, which follows from Hensel's lemma; see for example [17, Lemma V.3.3].

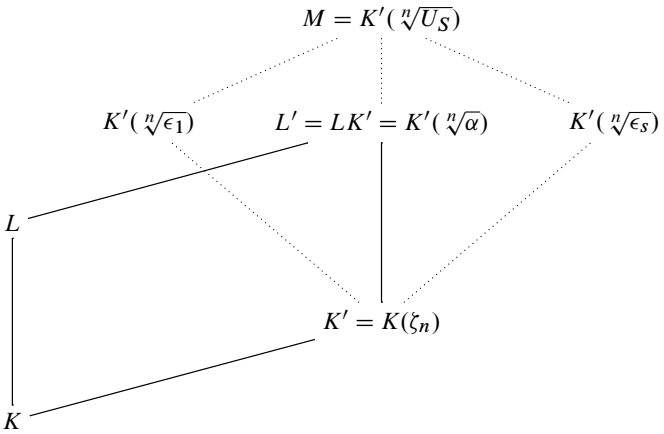

Figure 1. Fields used implicitly in the discussion.

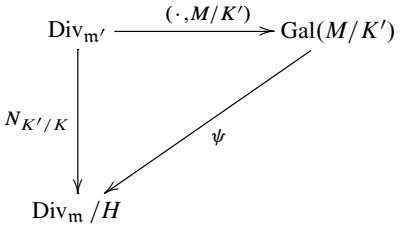

Figure 2. Definition of ψ.

$(P, M/K')$ at P is defined by its operation on the $\sqrt[n]{\epsilon_i}$. Since M/K' is unramified outside S, we see that 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 $\sqrt[n]{\epsilon_i}^N \equiv \zeta_n^{n_i}\sqrt[n]{\epsilon_i} \bmod P$, where N is 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-th roots of unity, and 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!

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 Figure 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 (see [6, §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 $\mathfrak{m}$).

3.3. ***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 an arbitrary 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 be used to 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 can be visualized as a tower:

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

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

$$\wp(\vec{\alpha}) = \vec{\alpha}^p - \vec{\alpha}.$$

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 [11, pp. 330–332]), every abelian extension of exponent p^r of k arises as $k(\wp^{-1}(\Delta_r))$ 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 $\vec{\gamma} \mapsto \vec{\gamma} + (1, 0, \ldots, 0)$ (see [21]).

So for our purposes we take $r = m$, and we 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 $\wp(\vec{y}) = \vec{x}$. Now we 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 write x for $\vec{x}$.

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, so we henceforth assume that $v_P(y) < 0$ and $p \mid v_P(y)$. 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 is a uniformizing element (that is, $v_P(\pi) = 1$). 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 also make 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 a 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 [24, Proposition 3.7.8] and Proposition 4 below), so λ_P does not depend on y. Thus, while Lemma 2 helps us understand the ramification in L/K, if we want to explicitly compute L we need to find a Riemann-Roch space containing the generator x. With this in mind, we combine Lemma 2 with the strong approximation theorem to get a global result.

Lemma 3. *Let y be an element of K. For every place P of K, 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 that $S \subseteq S'$. 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 nonspecial. 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 [24, Theorem 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 shows that $v = -\lambda_P$ if $P \in S$, and $v \geq 0$ if $P \in S' \setminus S$. In the same way,

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

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

$$\mathcal{L}\left(pn_0 P_0 + \sum_S \lambda_P P\right) = \left\{f \in K : \operatorname{div}(f) \geq -pn_0 P_0 - \sum_S \lambda_P P\right\}.$$

We now return 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 [21], 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 [21, 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 the dimension of this space over $\mathbb{F}_p$. We compute an $\mathbb{F}_p$-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 subvector space of $\mathcal{L}_K(D)$ generated by the f_i, and we have

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

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 as in 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 $\vec{y}$ via the formula

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

(see [21]), where the last term is in $\mathrm{W}_m(\mathbb{F}_p) \cong \mathbb{Z}_p \bmod p^m$ and satisfies

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

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

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

and this is made explicit via the Frobenius: Every $\mathrm{Gal}(M_m(0, \ldots, 0, \wp^{-1}(f_i))/M_m)$ 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

$$\mathrm{Gal}(M_m(0, \ldots, 0, \wp^{-1}(f_i))/M_m) \cong \mathrm{Gal}(K(\wp^{-1}(f_i))/K),$$

the generating isomorphisms 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 (see [21]), we have

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

and so the isomorphism $\mathrm{Gal}(M/M_m) \cong (\mathbb{Z}/p\mathbb{Z})^d$ is made 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 $\mathrm{Gal}(M/M_m)$ 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 explicit Artin map.

4. 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 the same finite field $\mathbb{F}_q$ such that the number of rational places of the field L is greater than or equal to the corresponding entry in the table[2] (as it was in June 2011). Furthermore, with the aid of the theory of Section 3, 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*

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

Proof. By the Riemann-Hurwitz genus formula, this comes down to showing that the degree of the different $\mathfrak{D}_{L/K}$ 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 $\deg \mathrm{N}(\mathfrak{D}_{L/K}) = \deg \mathfrak{D}_{L/K}$. By the conductor-discriminant formula, $\mathrm{N}(\mathfrak{D}(L_K))$ is equal to $\mathfrak{f}_{L/K}^{l-1}$, so by taking degrees we obtain the proposition. □

From Proposition 4, the genus of a cyclic 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 the other hand, $\mathfrak{f}_{L/K}$ 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 cyclic 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

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

[2]Note that L will be defined over $\mathbb{F}_q$ if at least one rational place of K splits totally in L, which will be the case when we are looking for L with many rational places.

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 extension of function fields. 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, *that is*,

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

Proof. From [16, Corollary 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, this 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. □

We see that 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 of its "best" coverings reaching or improving a lower bound in www.manypoints.org, start the process again on these coverings, and so on. We summarize the process in Algorithm 1. 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.

[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 rational points. This number of points is denoted $N_q(g)$.

Algorithm 1 (Good abelian coverings).

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 and conductor $\mathfrak{m}$.
  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. 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 $l \mid q^{\deg P} - 1$. 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 whose dimension depends again on the total number of places. The computation of the number of rational places requires the computation of 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.

Name	f
D_1	y^2+y+x^3+x
D_2	$y^2+(x^3+x+1)y+x^5+x^4+x^3+x$
D_3	$y^3+x^2y^2+(x^3+1)y+x^2+x$
D_4	$y^4+(x+1)y^2+(x^3+x)y+x^7+x^3$
D_5	$y^4+(x^2+x+1)y^2+(x^2+x)y+x^7+x^6+x^5+x^4$
D_6	$y^4+(x^6+x^5+x^4+1)y^2+(x^7+x^4+x^3+x^2)y+x^{11}+x^{10}+x^3+x^2$
D_7	$y^4+(x^7+x^6+x^4+x^2+1)y^2+(x^8+x^6+x^5+x^4)y+x^{10}+x^8+x^6+x^4$
D'_1	y^2+xy+x^3+x
D'_2	y^2+y+x^5+x
D'_3	$y^4+(x^2+x+1)y^2+(x^2+x)y+x^6+x^5$
D'_4	$y^4+xy^2+(x+1)y+x^5+x^4+x^3+x^2$
D'_5	$y^4+(x^3+1)y^2+(x^4+x^2)y+x^9+x^5$
D'_6	$y^4+(x^3+x+1)y^2+(x^3+x)y+x^9+x^8+x^5+x^4$
D'_7	$y^4+x^7y^2+(x^7+1)y+x^5+x$

Table 1. Equations $f=0$ for the base curves over $\mathbb{F}_2$ used in our calculations. The curves D_g have genus g and are maximal; the curves D'_g have genus g and satisfy $|D'_g(\mathbb{F}_2)| = N_2(g)-1$.

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

Remark. It is possible to extend the algorithm to coverings of nonprime degrees, to include Artin-Schreier-Witt extensions for example, and this is what we have implemented in Magma. The genus and the conductor can then be computed using techniques from [8]. Note however that the computations then are much longer. This is the reason why we presented the algorithm only for cyclic extensions of prime degree: Since their arithmetic is simpler, the algorithm works best for them and can thus be used more efficiently over finite fields of size greater than 2 or 3.

5. Results

In this section we present the explicit results we obtained by implementing our algorithm. All of our computations were carried out in Magma [4], using a class field theory library implemented by the second author.

We restrict our attention here to the case where the base field is $\mathbb{F}_2$.

In Table 1 we give the equations for the base curves to which we applied our algorithm. The curves D_g have genus g and are maximal; the curves D'_g have genus g and satisfy $|D'_g(\mathbb{F}_2)| = N_q(g)-1$. Note that Rigato [19] has shown that the maximal curves of genus 1, 2, 3, 4, and 5 over $\mathbb{F}_2$ are unique.

g	N	Oesterlé bound	Base curve	Conductor $\mathfrak{f}$	Galois group G	$\lvert S\rvert$	$\lvert T\rvert$	$\lvert R\rvert$
14	16	16	D_4	$2P_7$	$\mathbb{Z}/2\mathbb{Z}$	16	0	0
17	18	18	D_2	$4P_1+6P_1$	$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$	16	2	0
24	23	23	D_4'	$2P_1+4P_1+2P_2$	$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$	20	1	2
29	26	27	D_4	$4P_1+8P_1$	$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$	24	2	0
41	34	35	D_3'	$4P_1+4P_1$	$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$	32	2	0
45	34	37	D_2	$4P_1+8P_1$	$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$	32	2	0
46	35	38	D_3	$3P_1+8P_1$	$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$	32	1	2

Table 2. New results over $\mathbb{F}_2$. For each genus g in the leftmost column, we give the largest number N for which we have constructed a genus-g curve over $\mathbb{F}_2$ having N rational points. The other columns are explained in the text.

Table 2 presents data on the curves we constructed that improved the previous records for the number of points on a genus-g curve over $\mathbb{F}_2$. The first two columns in the table give the genus g and the number of rational points N on the abelian coverings we construct. The third column gives the Oesterlé bound on the number of rational points of a genus-g curve defined over $\mathbb{F}_2$; in the cases we consider this is the best upper bound known. The fourth column gives the name (from Table 1) of the base curve used in the construction. The fifth column gives the conductor of the covering; a summand of the form $n_i P_i$ means that there is a place of degree i occurring in the conductor with weight n_i. The final four columns give the Galois group G of the covering, the number $|S|$ of totally split places, the number $|T|$ of totally ramified places, and the number $|R|$ of partially ramified places. In some cases we obtained the same values of g and N by applying our algorithm to different base curves; in these cases, we only make one entry in our table, corresponding to the construction using the base curve with the smallest genus. Finally, we mention that the average bound on the degree of the possible conductors we have tested was 14.

For each row of Table 2, let C_g denote the covering curve of genus g corresponding to that row. We present explicit equations for each C_g next; these are equations for the C_g as coverings of their base curves, so the equations for the base curves (given in Table 1) are left unstated here. We have attempted to present the equations so that the structure of each cover as a tower of Artin-Schreier covers is clear.

$$C_{14}: \begin{cases} 0 = (x^7+x^3+1)(z^2+z) \\ \qquad + y^3 + (x^4+x)y^2 + (x^4+x^2+1)y + (x^8+x^6+x^5+x^4) \end{cases}$$

$$C_{17}: \begin{cases} 0 = z^2 + x^2 z \\ \qquad + x(x+1)(x^3+x^2+1)y + x^2(x+1)^2(x^4+x^3+x^2+x+1) \\ 0 = w^2 + xw + x(x+1)(x^2+x+1)y + x^2(x+1) \end{cases}$$

$$C_{24}: \begin{cases} 0 = z^2 + x^2(x+1)z \\ \qquad + x(x^3+x^2+1)y^3 + x^3(x+1)^4y^2 + x^2(x^4+x^3+1)y \\ \qquad + x(x+1)(x^7+x^6+x^3+x^2+1) \\ 0 = w^2 + x^2w + x(x+1)y^3 \\ \qquad + x^3(x+1)^2y^2 + x^2(x+1)^2y + x(x+1)(x^2+x+1) \end{cases}$$

$$C_{29}: \begin{cases} 0 = z^2 + x^2(x+1)^4z \\ \qquad + (x+1)(x^6+x^5+x^4+x^3+1)y^3 \\ \qquad + x(x+1)^3(x^5+x^4+x^3+x^2+1)y^2 + (x+1)^2(x^6+x^2+1)y \\ \qquad + x^2(x+1)^3(x^5+x^4+x^3+x^2+1) \\ 0 = w^2 + x^2(x+1)^5w \\ \qquad + (x+1)(x^9+x^8+x^5+x^4+1)y^3 \\ \qquad + x(x+1)^3(x^9+x^8+x^6+x^5+x^4+x^2+1)y^2 \\ \qquad + (x+1)^2(x^9+x^8+x^3+x^2+1)y \\ \qquad + x^2(x+1)^3(x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+x^2+1) \end{cases}$$

$$C_{41}: \begin{cases} 0 = z^2 + \big[x^6(x^2+x+1)y^3 + x^7(x^4+x^3+x^2+x+1)y^2 \\ \qquad + x^6(x+1)(x^2+x+1)y + x^{10}(x+1)^4\big]z \\ \qquad + x(x+1)^7(x^{13}+x^{12}+x^{11}+x^9+x^6+x^4+1)y^3 \\ \qquad + x^2(x+1)^3(x^{17}+x^{15}+x^{12}+x^{11}+x^9+x^3+1)y^2 \\ \qquad + x(x+1)^6(x^{17}+x^{15}+x^{14}+x^{13}+x^4+x^2+1)y \\ \qquad + x^5(x+1)^4(x^{17}+x^{16}+x^{12}+x^{11}+x^6+x^3+1) \\ 0 = v^2 + x^7v + xz \\ 0 = w^2 + x^2w + xy^2 + x^2y \end{cases}$$

$$C_{45}: \begin{cases} 0 = z^2 + (x+1)^2(xy+1)z + x^2(x^{13}+x^{11}+x^9+x+1)y \\ \qquad + x^9(x^8+x^6+x^4+x^3+x^2+x+1) \\ 0 = v^2 + (x+1)^2v + x(x+1)z + x^7(x^4+x+1) \\ 0 = w^2 + (x+1)^2w + (x+1)(x^5+x^2+x)y + (x+1)(x^8+x^5+x^4) \end{cases}$$

$$C_{46}: \begin{cases} 0 = z^2 + \big[(x+1)y^2 + (x^3+x^2+1)y + (x^4+x^3+x^2+x+1)\big]z \\ \qquad + (x+1)^2(x^{11}+x^8+x^6+x+1)y^2 + (x+1)^6(x^9+x^2+1)y \\ \qquad + x^7(x+1)^2(x^7+x^5+x^4+x^3+1) \\ 0 = v^2 + v + x(x+1)z + x^5(x+1) \\ 0 = w^2 + w + xy^2 + x^2(x^3+x^2+1)y \end{cases}$$

Remark. After this article was written, a preprint of Karl Rökaeus appeared in which he undertakes similar computations over the finite fields of size 2, 3, 4, and 5 (see [20]). Over $\mathbb{F}_2$ he recovers our genus-17 record, and he improves our genus-45 bound to 36 points. (He obtains the record-setting genus-45 curve as an abelian

cover of a genus-2 curve D with $|D(\mathbb{F}_2)| = N_2(2) - 2$.) In private communication, Rökaeus indicated that he also found a genus-46 curve over $\mathbb{F}_2$ with 36 points.

Remark. As mentioned above, we have restricted our search to curves over the field $\mathbb{F}_2$. However, our code works over other fields as well, and while we were testing it we found a curve of genus 11 over $\mathbb{F}_3$ with 21 rational points. This curve is a degree-2 cover of the genus-4 maximal curve defined by

$$C : y^4 - y^2 + x^6 + x^4 + x^2 = 0.$$

With notations as above, the conductor of the cover is of the form $P_1 + P_1 + P_1 + P_5$, and we have $|S| = 9$, $|R| = 3$, and $|T| = 0$. The resulting cover C' is given by the equation

$$\begin{aligned} z^2 = &-(x^5+x^4+x^3-x^2+x+2)\cdot(y+x^2+x)\cdot(y^2+(-x+1)y+x^3-x^2-x+1) \\ &\cdot\big((x^7+x^6+x^5-x^3-1)y^3+(-x^8+x^6+x^5-x^4-x^3-x)y^2 \\ &+(-x^{10}-x^9-x^8+x^5+x^4+x^3-x^2+1)y \\ &-x^{12}-x^9-x^8+x^6+x^4+x\big). \end{aligned}$$

Acknowledgments

The first author would like to thank his advisor David Kohel and Everett Howe 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.

References

[1] Roland Auer, *Ray class fields of global function with many rational places*, Ph.D. thesis, Carl-von-Ossietzky-Universität Oldenburg, 1999. http://oops.uni-oldenburg.de/volltexte/1999/457/

[2] ———, *Curves over finite fields with many rational points obtained by ray class field extensions*, in Bosma [3], 2000, pp. 127–134. MR 2002h:11053

[3] Wieb Bosma (ed.), *Algorithmic number theory: Proceedings of the 4th International Symposium (ANTS-IV) held at the Universiteit Leiden, Leiden, July 2–7, 2000*, Lecture Notes in Computer Science, no. 1838, Berlin, Springer, 2000. MR 2002d:11002

[4] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system, I: The user language*, J. Symbolic Comput. **24** (1997), no. 3–4, 235–265. MR 1484478

[5] Henri Cohen (ed.), *Algorithmic number theory: Proceedings of the 2nd International Symposium (ANTS-II) held at the Université Bordeaux I, Talence, May 18–23, 1996*, Lecture Notes in Computer Science, no. 1122, Berlin, Springer, 1996. MR 97k:11001

[6] Claus Fieker, *Computing class fields via the Artin map*, Math. Comp. **70** (2001), no. 235, 1293–1303. MR 2002e:11153

[7] V. D. Goppa, *Codes that are associated with divisors*, Problemy Peredači Informacii **13** (1977), no. 1, 33–39. MR 58 #15672

[8] Florian Hess, Sebastian Pauli, and Michael E. Pohst, *Computing the multiplicative group of residue class rings*, Math. Comp. **72** (2003), no. 243, 1531–1548. MR 2004f:11126

[9] David Kohel and Robert Rolland (eds.), *Arithmetic, geometry, cryptography and coding theory 2009: Papers from the 12th Conference (AGC^{2}T 12) held in Marseille, March 30–April 3, 2009, the 1st Geocrypt Conference held in Pointe-à-Pitre, April 27–May 1, 2009, and the European Science Foundation Exploratory Workshop on Curves, Coding Theory and Cryptography held in Marseille, March 25–29, 2009*, Contemporary Mathematics, no. 521, American Mathematical Society, Providence, RI, 2010. MR 2011g:11003

[10] Serge Lang, *Algebraic number theory*, 2nd ed., Graduate Texts in Mathematics, no. 110, Springer, New York, 1994. MR 95f:11085

[11] ———, *Algebra*, 3rd ed., Graduate Texts in Mathematics, no. 211, Springer, New York, 2002. MR 2003e:00003

[12] Kristin Lauter, *Ray class field constructions of curves over finite fields with many rational points*, in Cohen [5], 1996, pp. 187–195. MR 98a:11076

[13] ———, *Deligne-Lusztig curves as ray class fields*, Manuscripta Math. **98** (1999), no. 1, 87–96. MR 2000a:11163

[14] ———, *A formula for constructing curves over finite fields with many rational points*, J. Number Theory **74** (1999), no. 1, 56–72. MR 99k:11088

[15] J. S. Milne, *Class field theory (version 4.01)*, course notes, 2011. http://www.jmilne.org/math/CourseNotes/cft.html

[16] ———, *Algebraic number theory (version 3.04)*, course notes, 2012. http://www.jmilne.org/math/CourseNotes/ant.html

[17] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften, no. 322, Springer, Berlin, 1999. MR 2000m:11104

[18] Harald Niederreiter and Chaoping Xing, *Rational points on curves over finite fields: Theory and applications*, London Mathematical Society Lecture Note Series, no. 285, Cambridge University Press, 2001. MR 2002h:11055

[19] Alessandra Rigato, *Uniqueness of low genus optimal curves over $\mathbb{F}_2$*, in Kohel and Rolland [9], 2010, pp. 87–105. MR 2011m:11129

[20] Karl Rökaeus, *New curves with many points over small finite fields*, Tech. Report, 2012. arXiv 1204.4355 [math.NT]

[21] Hermann Ludwig Schmid, *Zur Arithmetik der zyklischen p-Körper*, J. Reine Angew. Math. **176** (1936), 161–167 (German). Zbl 0016.05205

[22] 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** (1983), no. 9, 397–402. http://gallica.bnf.fr/ark:/12148/bpt6k55351747/f35 MR 85b:14027

[23] ———, *Rational points on curves over finite fields*, unpublished notes by Fernando Q. Gouvéa of lectures at Harvard University, 1985.

[24] Henning Stichtenoth, *Algebraic function fields and codes*, 2nd ed., Graduate Texts in Mathematics, no. 254, Springer, Berlin, 2009. MR 2010d:14034

[25] André Weil, *Basic number theory*, Grundlehren der mathematischen Wissenschaften, no. 144, Springer, Berlin, 1973. MR 96c:11002

VIRGILE DUCET: virgile.ducet@gmail.com
Institut de Mathématiques de Luminy, Campus de Luminy, Case 907, 13288 Marseille Cedex 9, France

CLAUS FIEKER: fieker@mathematik.uni-kl.de
Fachbereich Mathematik, Universität Kaiserslautern, Postfach 3049, 67653 Kaiserslautern, Germany

VOLUME EDITORS

Everett W. Howe
Center for Communications Research
4320 Westerra Court
San Diego, CA 92121-1969
United States

Kiran S. Kedlaya
Department of Mathematics
University of California, San Diego
9500 Gilman Drive #0112
La Jolla, CA 92093-0112

Front cover artwork based on a detail of
Chicano Legacy 40 Años ©2010 Mario Torero.

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-00-2 (print), 978-1-935107-01-9 (electronic)

First published 2013.

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org **http://msp.org**

THE OPEN BOOK SERIES 1

Tenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the tenth ANTS meeting, held July 9–13, 2012, at the University of California, San Diego. It includes revised and edited versions of the 25 refereed papers presented at the conference, together with extended abstracts of two of the five invited talks.

TABLE OF CONTENTS