Computing Equations of Curves with Many Points

Virgile Ducet[1] Claus Fieker[2]

[1]Institut de Mathématiques de Luminy

[2]Fachbereich Mathematik Universität Kaiserslautern

Journées Codage et Cryptographie 2012, 8-12 octobre 2012

Motivation

Let $X/\mathbb{F}_q$ be a genus g curve. 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

$$\Omega_X(D_1 - D_2) = \{\omega \in \mathrm{Diff}(X) : \mathrm{div}(\omega) \geq D_2 - D_1\}.$$

The *Goppa code* $C(X, D_1, D_2)$ *is the image of the* $\mathbb{F}_q$*-linear map* $\Omega_X(D_1 - D_2) \to \mathbb{F}_q^n$ *defined by*

$$\omega \mapsto (\mathrm{res}_{P_1}(\omega), ..., \mathrm{res}_{P_n}(\omega)).$$

Motivation

Let $X/\mathbb{F}_q$ be a genus g curve. 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

$$\Omega_X(D_1 - D_2) = \{\omega \in \mathrm{Diff}(X) : \mathrm{div}(\omega) \geq D_2 - D_1\}.$$

The *Goppa code* $C(X, D_1, D_2)$ *is the image of the* $\mathbb{F}_q$*-linear map* $\Omega_X(D_1 - D_2) \to \mathbb{F}_q^n$ *defined by*

$$\omega \mapsto (\mathrm{res}_{P_1}(\omega), ..., \mathrm{res}_{P_n}(\omega)).$$

Let (n, k, d) *be the parameters of the code; then* $k = g - 1 + n - \deg(D_2)$ *and*

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

Bounds on the Number of Points of Curves over $\mathbb{F}_q$

Let $C/\mathbb{F}_q$ be a curve. Set $N(C) = |C(\mathbb{F}_q)|$.

QUESTION: How big can $N(C)$ be?

Bounds on the Number of Points of Curves over $\mathbb{F}_q$

Let $C/\mathbb{F}_q$ be a curve. Set $N(C) = |C(\mathbb{F}_q)|$.

QUESTION: How big can $N(C)$ be?

Introduce $N_q(g) = \max\limits_{\substack{C/\mathbb{F}_q \\ g(C)=g}} N(C)$.

Bounds on the Number of Points of Curves over $\mathbb{F}_q$

Let $C/\mathbb{F}_q$ be a curve. Set $N(C) = |C(\mathbb{F}_q)|$.

QUESTION: How big can $N(C)$ be?

Introduce $N_q(g) = \max_{\substack{C/\mathbb{F}_q \\ g(C)=g}} N(C)$.

UPPER BOUNDS:

- Hasse-Weil-Serre bound:

$$|N_q(g) - q - 1| \leqslant g \cdot \lfloor 2\sqrt{q} \rfloor;$$

- Oesterlé bounds;
- articles of Howe and Lauter ('03, '12),...

Lower bounds: Find curves with as many points as possible.

LOWER BOUNDS: Find curves with as many points as possible.

POSSIBLE METHODS:

- curves with explicit equations: Hermitian curves, Ree curves, Suzuki curves,...
- curves defined by explicit coverings: Artin-Schreier-Witt, Kummer,...
- curves with modular structure: elliptic or Drinfel'd modular curves,...
- curves defined by a non-explicit covering: abelian coverings (Class Field Theory, Drinfel'd modules),...

LOWER BOUNDS: Find curves with as many points as possible.

POSSIBLE METHODS:

- curves with explicit equations: Hermitian curves, Ree curves, Suzuki curves,...
- curves defined by explicit coverings: Artin-Schreier-Witt, Kummer,...
- curves with modular structure: elliptic or Drinfel'd modular curves,...
- curves defined by a non-explicit covering: abelian coverings (Class Field Theory, Drinfel'd modules),...

OUR APPROACH: Class Field Theory.

Function Fields

Let K be an algebraic function field over $\mathbb{F}_q$, that is a finite algebraic extension of $\mathbb{F}_q(X)$ for an indeterminate X.

Function Fields

Let K be an algebraic function field over $\mathbb{F}_q$, that is a finite algebraic extension of $\mathbb{F}_q(X)$ for an indeterminate X.

To a curve $C/\mathbb{F}_q$ one can associate its function field $\mathbb{F}_q(C)$.

Function Fields

Let K be an algebraic function field over $\mathbb{F}_q$, that is a finite algebraic extension of $\mathbb{F}_q(X)$ for an indeterminate X.

To a curve $C/\mathbb{F}_q$ one can associate its function field $\mathbb{F}_q(C)$.

EXAMPLE:
If $C = V(P(x, y))$, then $\mathbb{F}_q(C) = \mathbb{F}_q(x)[y]/P(x, y)$.

Function Fields

Let K be an algebraic function field over $\mathbb{F}_q$, that is a finite algebraic extension of $\mathbb{F}_q(X)$ for an indeterminate X.

To a curve $C/\mathbb{F}_q$ one can associate its function field $\mathbb{F}_q(C)$.

EXAMPLE:
If $C = V(P(x, y))$, then $\mathbb{F}_q(C) = \mathbb{F}_q(x)[y]/P(x, y)$.

THEOREM:
The two categories are equivalent.

We thus have totally equivalent notions of genus, divisors,... The equivalent of a point P of a curve is a *place and is also denoted (by abuse)* P.

For a point P of C, consider the subring of its function field

$$\mathcal{O}_P = \{f \in \mathbb{F}_q(C) : P \text{ is not a pole of } f\}$$

with unique maximal ideal

$$\mathcal{M}_P = \{f \in \mathbb{F}_q(C) : P \text{ is a zero of } f\}.$$

The *residue field at P is*

$$\mathbb{F}_P = \mathcal{O}_P/\mathcal{M}_P.$$

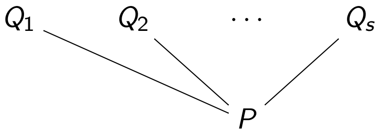
The degree of P is

$$\deg(P) = [\mathbb{F}_P : \mathbb{F}_q].$$

We let $N(K)$ be the number of places of degree 1 of K.

Ramification Theory

In a function field extension L/K we have places of L above P:



For each place Q_i above P, we define the following two positive integers:

$$\mathcal{M}_P \mathcal{O}_Q = \mathcal{M}_Q^{e(Q_i/P)} \text{ (\textit{ramification index})}$$

$$f(Q_i/P) = [\mathbb{F}_{Q_i} : \mathbb{F}_P] \text{ (\textit{inertia degree}).}$$

L/K is *ramified* (*resp.* *totally ramified*) *at* P *if there exists* i *such that* $e(Q_i/P) > 1$ *(resp.* $s = 1$ *and* $e(Q_1/P) = [L : K]$*).* P *is* *totally split* *in* L *if* $s = [L : K]$*.*

Why use Class Field Theory?

Remark:

Let L/K be an algebraic extension of algebraic function fields defined over $\mathbb{F}_q$. Then

$$N(L) \geqslant [L : K]\#\mathrm{Split}_{\mathbb{F}_q}(L/K) + \#\mathrm{TotRam}_{\mathbb{F}_q}(L/K).$$

Class Field Theory describes the abelian extensions of K in terms of data intrinsic to K and provides a good control on the ramification and decomposition behavior in the extension.

Why use Class Field Theory?

Remark:
Let L/K be an algebraic extension of algebraic function fields defined over $\mathbb{F}_q$. Then

$$N(L) \geqslant [L:K]\#\mathrm{Split}_{\mathbb{F}_q}(L/K) + \#\mathrm{TotRam}_{\mathbb{F}_q}(L/K).$$

Class Field Theory describes the abelian extensions of K in terms of data intrinsic to K and provides a good control on the ramification and decomposition behavior in the extension.

Problem: One does not know in general the equations of the abelian coverings of K (problematic for applications, for example to coding theory).

Why use Class Field Theory?

Remark:
Let L/K be an algebraic extension of algebraic function fields defined over $\mathbb{F}_q$. Then

$$N(L) \geqslant [L:K]\#\mathrm{Split}_{\mathbb{F}_q}(L/K) + \#\mathrm{TotRam}_{\mathbb{F}_q}(L/K).$$

Class Field Theory describes the abelian extensions of K in terms of data intrinsic to K and provides a good control on the ramification and decomposition behavior in the extension.

Problem: One does not know in general the equations of the abelian coverings of K (problematic for applications, for example to coding theory).

This Talk: we explain how to find these equations and describe an algorithm to find good curves (look at www.manypoints.org).

The Artin Map

Let L/K be an abelian extension. Let P be a place of K and Q be a place of L over P. Let $\mathbb{F}_P$ (resp. $\mathbb{F}_Q$) be the residue field of K at P (resp. of L at Q).

When P is unramified the reduction map $\mathrm{Gal}_Q(L/K) \to \mathrm{Gal}(\mathbb{F}_Q/\mathbb{F}_P)$ is an isomorphism. The pre-image of Frobenius is independent of Q; one denotes it by $(P, L/K)$ and call it the *Frobenius automorphism at P.*

DEFINITION:

The map $P \mapsto (P, L/K) \in \mathrm{Gal}(L/K)$ *can be extended linearly to the set of divisors supported outside the ramified places of* L/K*. The resulting map is called the Artin map and is denoted* $(\cdot\ , L/K)$*.*

Class Field Theory

DEFINITION:

A *modulus* on K *is an effective divisor.*

Let $\mathfrak{m}$ *be a modulus supported on a set* $S \subset \mathrm{Pl}_K$*, we denote by* $\mathrm{Div}_\mathfrak{m}$ *the group of divisors which support is disjoint from* S*. Set*

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

DEFINITION:

A congruence subgroup modulo $\mathfrak{m}$ *is a subgroup* $H < \mathrm{Div}_\mathfrak{m}$ *of finite index such that* $P_{\mathfrak{m},1} \subseteq H$.

EXISTENCE THEOREM:

For every modulus $\mathfrak{m}$ *and every congruence subgroup* H *modulo* $\mathfrak{m}$*, there exists a unique abelian extension* L_H *of* K*, called the class field of* H*, such that the Artin map provides an isomorphism*

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

Artin Reciprocity Law:

For every abelian extension L/K, there exists an *admissible modulus* $\mathfrak{m}$ *and a unique congruence subgroup $H_{L,\mathfrak{m}}$ modulo $\mathfrak{m}$, such that the Artin map provides an isomorphism*

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

Definition:

The conductor of L/K, denoted $\mathfrak{f}_{L/K}$, is the smallest admissible modulus. It is supported on exactly the ramified places of L/K.

Main Theorem of Class Field Theory:

Let $\mathfrak{m}$ be a modulus. There is a 1-1 inclusion reversing correspondence between congruence subgroups H modulo $\mathfrak{m}$ and finite abelian extensions L of K of conductor smaller than $\mathfrak{m}$. Furthermore the Artin map provides an isomorphism

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

Computing Abelian Extensions

DATA: Let $\mathfrak{m}$ be a modulus over K and H be a congruence subgroup modulo $\mathfrak{m}$.

Computing Abelian Extensions

DATA: Let $\mathfrak{m}$ be a modulus over K and H be a congruence subgroup modulo $\mathfrak{m}$.

GOAL: Compute the class field L of H.

Computing Abelian Extensions

DATA: Let $\mathfrak{m}$ be a modulus over K and H be a congruence subgroup modulo $\mathfrak{m}$.

GOAL: Compute the class field L of H.

ASSUMPTION: $\mathrm{Div}_{\mathfrak{m}}/H \cong \mathbb{Z}/\ell^m\mathbb{Z}$ for a prime number ℓ and an integer $m \geqslant 1$. Two cases: $\ell = p \overset{def}{=} \mathrm{char}(K)$ or $\ell \neq p$.

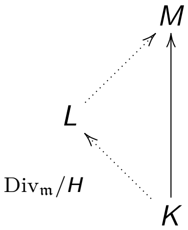
Computing Abelian Extensions

DATA: Let $\mathfrak{m}$ be a modulus over K and H be a congruence subgroup modulo $\mathfrak{m}$.

GOAL: Compute the class field L of H.

ASSUMPTION: $\mathrm{Div}_{\mathfrak{m}}/H \cong \mathbb{Z}/\ell^m\mathbb{Z}$ for a prime number ℓ and an integer $m \geqslant 1$. Two cases: $\ell = p \overset{def}{=} \mathrm{char}(K)$ or $\ell \neq p$.

STRATEGY: Using respectively Artin-Shreier-Witt and Kummer theories, find an abelian extension M of K containing L for which we can compute explicitly the Artin map. Then compute L as the subfield of M fixed by the image of H.



REMARK:

Let $P \in \mathrm{Pl}_K$. Then $(P, M/K)|_L = (P, L/K)$.

So

$$\begin{aligned}(H, M/K) &= \{(P, M/K) : P \in H\} \\ &= \{\sigma \in \mathrm{Gal}(M/K) : \sigma|_L = \mathrm{Id}_L\} \\ &= \mathrm{Gal}(M/L).\end{aligned}$$

Galois Theory implies $L = M^{(H, M/K)}$.

Cyclic Extensions of Prime Degree

PROPOSITION:

Let L/K be a cyclic extension of prime degree ℓ and of conductor $\mathfrak{f}_{L/K}$. Assume that they are defined over $\mathbb{F}_q$. Then the genus of L verifies:

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

Cyclic Extensions of Prime Degree

PROPOSITION:

Let L/K be a cyclic extension of prime degree ℓ and of conductor $\mathfrak{f}_{L/K}$. Assume that they are defined over $\mathbb{F}_q$. Then the genus of L verifies:

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

REMARK:

There seems to be no dependence on the ramification type of the extension (tame or wild), but in fact:

Cyclic Extensions of Prime Degree

PROPOSITION:

Let L/K be a cyclic extension of prime degree ℓ and of conductor $\mathfrak{f}_{L/K}$. Assume that they are defined over $\mathbb{F}_q$. Then the genus of L verifies:

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

REMARK:

There seems to be no dependence on the ramification type of the extension (tame or wild), but in fact:

PROPOSITION:

A place P of K is wildly ramified in L if and only if $\mathfrak{f}_{L/K} \geqslant 2P$ (and thus tamely ramified if and only if $v_P(\mathfrak{f}_{L/K}) = 1$).

The Algorithm

Input: A function field $K/\mathbb{F}_q$, a prime ℓ, an integer G.

Output: The equations of all cyclic extensions L of K of degree ℓ such that $g(L) \leqslant G$ and $N(L)$ improves the best known record.

Compute all the moduli of degree less than $B = (2G - 2 - \ell(2g(K) - 2))/(\ell - 1)$.
FOR each such modulus $\mathfrak{m}$ DO
    Compute the ray class group $\mathrm{Pic}_{\mathfrak{m}} \cong \mathrm{Div}_{\mathfrak{m}}/P_{\mathfrak{m},1}$.
    Compute the set T of subgroups of $\mathrm{Pic}_{\mathfrak{m}}$ of index ℓ.
    FOR every H in T DO
        Compute $g(L)$ and $n = N(L)$, where L is the class field of H.
        IF n is greater than the best known record THEN
            Update n as the new lower bound on $N_q(g(L))$.
            Compute the equation of L.
        END IF
    END FOR
END FOR

New Results over $\mathbb{F}_2$

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

g: genus of the covering.
N: number of F_2-rational points. OB: Oesterlé bound.
g_0: genus of the base curve. $\mathfrak{f}$: conductor of the extension.
G: Galois group. S: totally split places.
T: totally ramified places. R: (non-totally) ramified places.

EXAMPLE:

Take the genus 2 maximal curve C_0 with equation

$$y^2 + (x^3 + x + 1)y + x^5 + x^4 + x^3 + x.$$

Then the new curve of genus 17 with 18 rational points is a fiber product of Artin-Schreier coverings of C_0 with equations

$$\begin{cases} z^2 + z + (x^4 + x^2 + x + 1)/x^3y + (x^6 + x^5 + x + 1)/x^2; \\ w^2 + w + (x^3 + 1)/xy + x + 1. \end{cases}$$