SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Search for function fields with many rational places

av

Erland Arctaedius

2015 - No 21

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET, 106 91 STOCKHOLM

Search for function fields with many rational places

Erland Arctaedius

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Karl Rökaeus

2015

Search for function fields with many rational places

Erland Arctaedius

September 28, 2015

Abstract

We will give a short introduction to function fields, aimed at providing us with tools to compute L-polynomials of hyperelliptic function fields. We use these tools to conclude the existence of extensions of these function fields for which we can both provide a lower limit on their number of rational places and compute their genus. Using these techniques we write a program in Java aimed at searching for function fields with a large number of rational places with respect to its genus. Finally we present the results of running the program over various small finite fields and genera.

1 Function fields

This chapter contains an algebraic introduction to function fields. Some theorems will have their proofs presented, but many will not. The proofs, and a much more detailed theory, is available in [STI].

There are other ways to approach the subject of function fields, and we will touch upon that in Section 1.5.

Definition 1. An *algebraic function field* F/K is an extension field F of K, that contains some x transcendental over K with $[F : K(x)] < \infty$.

The *field of constants* $\widetilde{K}$ of F/K are the elements in F that are algebraic over K; we will assume that we have K algebraically closed in F, so that $K = \tilde{K}$.

An important special case of function fields are when $F = K(x)$, where x is some element transcendental over K; if this is the case F/K is said to be a *rational function field*.

1.1 Places

Definition 2. A *discrete valuation* of F/K is a function $v : F \to \mathbb{Z} \cup \{\infty\}$ with the following properties:

1. $v(x) = \infty$ if and only if $x = 0$

2. $v(xy) = v(x) + v(y)$ for all $x, y \in F$

3. $v(x + y) \geq \min(v(x), v(y))$, for all $x, y \in F$

4. There is some element $z \in F$ such that $v(z) = 1$

5. $v(k) = 0$ for all $k \neq 0$ in K

We can use discrete valuations to define *places* of F/K, which will be one of the most important concepts in this text.

Definition 3. A *place* P of F/K with valuation v_P, where v_P is a discrete valuation, is a set $P = \{f \in F : v_P(f) > 0\}$.

To each place P of F/K corresponds a so called *valuation ring* O, with $K \subsetneqq O \subsetneqq F$, such that O is local with maximal ideal P (we often write this as O_P). The valuation ring O_P can be described by $O_P = \{f \in F : v_P(f) \geq 0\}$. For valuation rings the following hold: for each $f \in F$ either $f \in O$ or $f^{-1} \in O$. The set of all places of F/K is denoted by $\mathbb{P}_F$.

Definition 4. If P is a place of F/K and $x \in F$ we say that P is a *zero* of x if $v_P(x) > 0$, a *pole* if $v_P(x) < 0$. If x has a zero (pole) at P, that zero (pole) is said to be of order $v_P(x)$ $(-v_P(x))$.

Example 1. Consider the rational function field $\mathbb{F}_2(x)/\mathbb{F}_2$. In Example 2 we will discuss the places of $\mathbb{F}_2(x)/\mathbb{F}_2$ in more detail; here we give a concrete example of how places and valuations are connected. Let $p(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$ (note that p is irreducible) and consider the elements of $\mathbb{F}_2(x)$ as rational functions. Any non-zero element $f \in \mathbb{F}_2(x)$ can be written as $f = up^n$, where u has neither a zero nor a pole at the zeros of p, in a unique way. We then define $v_p(f) = n$, and we put $v_p(0) = \infty$. This fulfills all the criteria of a discrete valuation, so $P_{p(x)} = \{f : v_p(f) > 0\}$ is a place. The valuation ring O_P then consists of all $\frac{f(x)}{g(x)}$, with $f, g \in \mathbb{F}_2[x]$ and $p(x) \nmid g(x)$.

Since P is a maximal ideal in O_P, O_P/P must be a field. We denote by $x(P)$ the residue class of $x \in F$ in O_P/P, and if x is not in O_P we write $x(P) = \infty$.

Definition 5. Let $P \in \mathbb{P}_F$, and let O_P be the valuation ring corresponding to P. Then the *residue class field* F_P is defined by $F_P = O_P/P$. The mapping from F to $F_P \cup \{\infty\}$ given by $x \mapsto x(P)$ is known as the *residue class map* (with respect to P).

Definition 6. Let $P \in \mathbb{P}_F$. The *degree* of P is defined by $\deg P = [F_P : K]$. If $\deg P = 1$ we say that P is a *rational* place.

Theorem 1. *[STI, Prop. I.1.14] For each $P \in \mathbb{P}_F$ we have $\deg P \leq [F : K(f)] < \infty$, where $f \in P$ and $f \neq 0$. Thus every place has finite degree.*

Theorem 2. *[STI, Coro. I.1.19] Every $z \in F$ with z transcendental over K has at least one zero and one pole.*

Theorem 3. *[STI, Coro. I.1.19]* $\mathbb{P}_F \neq \emptyset$

Proof. This follows immediately from the previous theorem. □

In fact $\mathbb{P}_F$ is infinite for all F/K.

Example 2. The simplest function fields are the rational ones. For rational function fields (i.e. $K(x)/K$) it's easy to determine the places. We can show that the places of $K(x)/K$ have valuation rings on the form

$$O_{p(x)} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x],\, p(x) \nmid g(x) \right\}$$

where $p\left(x\right)$ is an irreducible polynomial in $K\left[x\right]$. This could be recognized as the localization of $K[x]$ with respect to $S = \{g(x) : p(x) \nmid g(x)\} \subseteq K[x]$. The only valuation ring not on this form corresponds to the place at infinity, and can be written as

$$O_\infty = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x],\, \deg f \leq \deg g \right\}.$$

It can be shown that $\deg P_{p(x)} = \deg p$ and $\deg P_\infty = 1$, so that the rational places (excluding P_∞) correspond to $p(x) = x - \alpha \in K[x]$, which in turn correspond to the elements of K. Thus the rational places of a rational function field are in a one-to-one correspondence with $K \cup \{\infty\}$.

1.2 Divisors

Divisors will be critical to this paper; they allow us to define the *genus* of a function field, and later on the *zeta function*, from which we will find the *L-polynomial*. Much of the work we do will be to compute these L-polynomials and draw conclusions from them.

Definition 7. A *divisor* D of a function field F/K is a formal sum of places,

$$D = \sum_{P \in \mathbb{P}_F} n_P P,$$

with $n_P \in \mathbb{Z}$ and only finitely many n_P being non-zero. The set of all divisors $\mathbb{D}_F$ form an abelian group, with addition given by $D + D' = \sum_{P \in \mathbb{P}_F} (n_P + n'_P)P$. If $D = 1 \cdot P$ for some $P \in \mathbb{P}_F$, D is said to be a *prime divisor*.

For each $P \in \mathbb{P}_F$ we define $v_P : \mathbb{D}_F \to \mathbb{Z}$ as $v_P(D) = n_P$, so we may write $D = \sum_{P \in \mathbb{P}_F} v_P(D) \cdot P$. Using this we can give a partial order to $\mathbb{D}_F$, given by $D \leq D'$ if and only if $v_P(D) \leq v_P(D')$ for all $P \in \mathbb{P}_F$.

Definition 8. The *degree* of a divisor D is $\deg D = \sum_{P \in \mathbb{P}_F} v_P(D) \deg P$.

Theorem 4. *[STI, Coro. I.3.4] Any element $x \in F$ have only finitely many zeros (poles) in $\mathbb{P}_F$.*

Definition 9. For $0 \neq x \in F$, let Z be the set of zeros of x and N be the set of poles of x (so both Z and N are finite subsets of $\mathbb{P}_F$). Then we may define the following (using the valuations from Definition 3):

Zero divisor $(x)_0 = \sum_{P \in Z} v_P(x) P$

Pole divisor $(x)_\infty = \sum_{P \in N} \left(-v_P\left(x\right)\right) P$

Principal divisor $(x) = (x)_0 - (x)_\infty$

Note that from Definition 2 we have $(k) = 0 \Leftrightarrow k \in K \setminus \{0\}$.

Definition 10. The set $\mathcal{P}_F = \{(x) : x \in F\}$ is called the *group of principal divisors* of F (this is a subgroup of $\mathbb{D}_F$). The factor group $\mathcal{C}_F = \mathbb{D}_F / \mathcal{P}_F$ is known as the *divisor class group* of F.

Definition 11. For a divisor D we define $\mathcal{L}(D) = \{x \in F : (x) \geq -D\} \cup \{0\}$. $\mathcal{L}(D)$ is known as the *Riemann-Roch space* associated with D.

Note that $x \in \mathcal{L}\left(D\right)$ is equivalent to $v_P\left(x\right) \geq -v_P\left(D\right)$ for all $P \in \mathbb{P}_F$.

Theorem 5. *[STI, Lemma I.4.6] $\mathcal{L}\left(D\right)$ is a vector space over K*

Proof. If $x, y \in \mathcal{L}\left(D\right)$ and $a \in K$, we have, for all $P \in \mathbb{P}_F$, $v_P\left(x + y\right) \geq \min\left(v_P\left(x\right), v_P\left(y\right)\right)$, using Definition 2. Since $\min\left(v_P\left(x\right), v_P\left(y\right)\right) \geq -v_P(D)$ we must have $x + y \in \mathcal{L}\left(D\right)$. Also $v_P\left(ax\right) = v_P\left(a\right) + v_P\left(x\right) = v_P\left(x\right)$ by Definition 2, so $v_P\left(ax\right) \geq -v_P\left(D\right)$, and thus $ax \in \mathcal{L}\left(D\right)$. Since both $x + y$ and ax is in $\mathcal{L}\left(D\right)$ it must form a vector space. □

Definition 12. The *dimension* of a divisor $D \in \mathbb{D}_F$, denoted $\dim D$, is defined as the K-dimension of $\mathcal{L}\left(D\right)$.

Theorem 6. *[STI, Lemma I.4.7(b)] If $D < 0$, where $D \in \mathbb{D}_F$, then $\mathcal{L}(D) = \{0\}$.*

Proof. If there is an x such that $0 \neq x \in \mathcal{L}\left(D\right)$ this would imply that $(x) \geq -D > 0$, which means that x has a zero but no pole, contradicting Theorem 2. □

We would like to show that the dimension of a divisor is finite.

Theorem 7. *[STI, Lemma I.4.8] If $A, B \in \mathbb{D}_F$ and $A \leq B$ we have $\mathcal{L}\left(A\right) \subseteq \mathcal{L}\left(B\right)$, and*

$$\dim\left(\mathcal{L}\left(B\right) / \mathcal{L}\left(A\right)\right) \leq \deg B - \deg A.$$

Proof. $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ means that $\{x \in F : (x) \geq -A\} \subseteq \{x \in F : (x) \geq -B\}$ and clearly $(x) \geq -A$ implies $(x) \geq -B$ if $A \leq B$, so the first statement follows.

We can assume that $B = A + P$ for some $P \in \mathbb{P}_F$, and then use induction to prove the general case. Let $t \in F$ be such that $v_P(t) = v_P(B) = v_P(A) + 1$. Then if $x \in \mathcal{L}(B)$ we have that $v_P(x) \geq -v_P(B) = -v_P(t)$, so $xt \in O_P$. We may thus define $\phi : \mathcal{L}(B) \to F_P$ by $\phi(x) = (xt)(P)$. Then ϕ is a K-linear map, with $\ker\phi = \{x \in \mathcal{L}(B) : v_P(xt) > 0\}$. However, $v_P(xt) > 0$ is equivalent to $v_P(x) \geq -v_P(A)$, so in fact $\ker\phi = \mathcal{L}(A)$, so there is a K-linear injective map from $\mathcal{L}(B)/\mathcal{L}(A)$ to F_P, which implies that $\dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq \dim F_P = \deg P = \deg B - \deg A$. □

Theorem 8. *[STI, Prop. I.4.9] For any $D \in \mathbb{D}_F$, $\mathcal{L}(D)$ is a finite dimensional vector space over K.*

Proof. We write $D = D^+ - D^-$, with $D^+ \geq 0$ and $D^- \geq 0$. Using the previous theorem we see that $\dim(\mathcal{L}(D^+)/\mathcal{L}(0)) \leq \deg D^+$. However, $\mathcal{L}(0) = K$ ($(x) = 0$ if $x \in K$, so $K \subseteq \mathcal{L}(0)$, while $0 \neq x \in \mathcal{L}(0)$ implies that $(x) \geq 0$, so x has no pole, thus $x \in K$ by Theorem 2), so $\dim(\mathcal{L}(D^+)) = \dim(\mathcal{L}(D^+)/\mathcal{L}(0)) + 1 \leq 1 + \deg D^+$. Since $D \leq D^+$, we have $\mathcal{L}(D) \subseteq \mathcal{L}(D^+)$, so

$$\dim \mathcal{L}(D) \leq \dim \mathcal{L}\left(D^+\right) \leq 1 + \deg D^+$$

so that $\mathcal{L}(D)$ is finite dimensional. □

Definition 13. For a function field F/K we define its *genus* (denoted g) to be

$$\max_{D \in \mathbb{D}_F} (\deg D - \dim D + 1)$$

Note that g is non-negative, which follows from letting $D = 0$, so that $\deg D - \dim D + 1 = 0$.

The genus of a function field is probably its most important characteristic. In general it's hard to determine, but for the classes of function fields that we will examine it is easy to compute.

Example 3. We once again consider the rational function fields, in order to determine their genus. Let $K(x)/K$ be a rational function field, and consider the pole divisor of x, $(x)_\infty$. Let $r \in \mathbb{N}$ and consider the vector space $L_r = \mathcal{L}(r(x)_\infty)$. We then have that $1, x, x^2, \ldots, x^r$ are all in L, so $r + 1 \leq \dim(L_r)$. We can also show that $\deg(x)_\infty = 1$ (in general, for any function field and $x \in F$ we have $\deg(x)_0 = \deg(x)_\infty = [F : K(x)]$). Thus $\deg(L_r) = r$. To proceed further we will need Riemann's Theorem:

Theorem 9. *[STI, Thm. I.4.17(b)] (Riemann) If F/K is a function field there is an integer c such that $\dim D = \deg D - g + 1$, whenever $\deg D \geq c$.*

We will not prove this. Using this we see that, for large enough r, we have $\dim(L_r) = \deg(L_r) - g + 1 = r - g + 1$, but since $r + 1 \leq \dim(L_r)$ we must have $g \leq 0$; we have already shown that $g \geq 0$ for any function field, so we must have $g = 0$ for rational function fields.

1.3 The zeta function and L-polynomial

In this part we will assume that $K = \mathbb{F}_q$, and denote the genus with g. We will also use the notation A_n, with $A_n = |\{D \in \mathbb{D}_F : D \geq 0 \, \text{and} \deg D = n\}|$. It would be good to know that the A_n:s are not infinite:

Theorem 10. *[STI, Lemma V.1.1]* $A_n < \infty$

Proof. A positive divisor can be written as a sum of prime divisors, so we need only show that $S = \{P \in \mathbb{P}_F : \deg P \leq n\}$ is finite. Pick any $x \in F \setminus \mathbb{F}_q$ and consider $S_0 = \left\{P \in \mathbb{P}_{\mathbb{F}_q(x)} : \deg P \leq n\right\}$. Clearly $P \cap \mathbb{F}_q(x) \in S_0$ for any $P \in S$. Also, any $P_0 \in S_0$ has only finitely many extensions in F, so if S_0 is finite we are done. From Example 2 we know that the places of $\mathbb{F}_q(x)/\mathbb{F}_q$ (a rational function field) correspond to monic, irreducible polynomials over $\mathbb{F}_q$ (and the place at infinity), so there are only finitely many places of $\mathbb{F}_q(x)$, implying that S_0 is also finite. □

Definition 14. For a function field $F/\mathbb{F}_q$ we define the *zeta function* as

$$Z(w) = \sum_{n=0}^{\infty} A_n w^n \in \mathbb{C}[[w]]$$

One can show that $Z(w)$ converges for $|w| < q^{-1}$, and we can then extend it to all of $\mathbb{C}$ (with a simple pole at $w = 1$). This is similar to the more famous Riemann zeta function (this is easier to see if we consider $Z(q^{-s})$).

Definition 15. The function defined by $L(t) = (1-t)(1-tq)Z(t)$ is known as the L-polynomial of $F/\mathbb{F}_q$.

It's not difficult to see that $L \in \mathbb{Z}[x]$.

Theorem 11. *[STI, Thm. V.1.15] For a function field $F/\mathbb{F}_q$ we have*

1. $\deg L = 2g$
2. *If $L(t) = a_{2g}t^{2g} + a_{2g-1}t^{2g-1} + \cdots + a_1 t + a_0$ we have*
   (a) $a_0 = 1$
   (b) $a_{2g} = q^g$
   (c) $a_{2g-i} = q^{g-i}a_i$ *for* $i \in \{0, 1, \cdots, g\}$
   (d) $a_1 = N - (q+1)$, *where* $N = |\{P \in \mathbb{P}_F : \deg P = 1\}|$, *the number of places of degree one in F.*

In order to compute the L-polynomial, we will need so called *constant field extensions.*

Definition 16. A *constant field extension* F_r ($r \in \mathbb{Z}^+$) of a function field $F/\mathbb{F}_q$ is a function field over $\mathbb{F}_{q^r}$ with $F_r = F\mathbb{F}_{q^r}$, the composite field of F and the new field of constants, $\mathbb{F}_{q^r}$.

(A brief remainder of what a composite field is: if Φ, A, B are all fields, with A and B being subfields of Φ, then the composite field of A and B, denoted AB, is the intersection of all subfields of Φ that contain both A and B.)

The following theorem will be used later to compute the L-polynomials.

Theorem 12. *[STI, Coro. V.1.17] Let N_r be the number of places of degree one in the constant field extension F_r of $F/\mathbb{F}_q$, i.e. $N_r = |\{P \in \mathbb{P}_{F_r} : \deg P = 1\}|$, and let $S_r = N_r - (q^r + 1)$. If $L(t) = t^{2g}a_{2g} + t^{2g-1}a_{2g-1} + \cdots + ta_1 + a_0$ is the L-polynomial of $F/\mathbb{F}_q$ we then have*

$$a_0 = 1$$

and

$$ia_i = S_i a_0 + S_{i-1}a_1 + \cdots + S_1 a_{i-1}$$

for $i \in \{1, 2, \ldots, g\}$. [STI, Corollary V.1.17]

1.4 Hyperelliptic function fields

Throughout this section we will assume that $\mathrm{char}K \neq 2$, since most of the following need some special treatment when $\mathrm{char}K = 2$. (Mostly, but not solely, this is done by replacing y^2 with $y^2 + y$ in the text below.)

We saw in Example 3 that the rational function field has genus 0, and conversely any function field with genus 0 and at least one divisor of degree one is rational. Elliptic function fields, which have genus one, are thus the simplest non-rational function fields.

Definition 17. If F/K is a function field, with $g = 1$ and at least one divisor of degree 1, then it is said to be an *elliptic function field.*

If K is algebraically closed or finite (we will always use finite fields) we are guaranteed to have at least one divisor of degree one, so that all function fields of genus one are elliptic.

Theorem 13. *[STI, Props. VI.1.2, VI.1.3] If F/K is an elliptic function field there exist $x, y \in F$ and $f \in K[x]$, f square free and $\deg f = 3$, such that*

$$y^2 = f(x)$$

and

$$F = K(x, y)$$

The converse also holds, i.e. every square free polynomial of degree three over K gives an elliptic function field.

Hyperelliptic function fields are a reasonable next step in our studies after elliptic function fields.

Definition 18. A *hyperelliptic function field* is a function field F/K with $g \geq 2$, such that there exists a rational subfield $K(x) \subseteq F$ with $[F : K(x)] = 2$.

The following theorem is a analogue to Theorem 13.

Theorem 14. *[STI, Prop. VI.2.3] Let F/K be a hyperelliptic function field with genus g. Then there exist a square free polynomial $f \in K[x]$, with $\deg f$ being either $2g+2$ or $2g+1$, and elements $x, y \in F$ such that*

$$y^2 = f(x)$$

and

$$F = K(x, y)$$

Conversely, if $F = K(x, y)$ and $y^2 = f(x)$ for some square free polynomial f with degree $d \geq 4$, then F/K is a hyperelliptic function field with genus

$$g = \begin{cases} \frac{d-1}{2} & \text{if } 2 \nmid d \\ \frac{d-2}{2} & \text{if } 2 | d \end{cases}$$

1.5 Parallels in other subjects

A geometric view of function fields starts with an algebraic curve V; the function field is then the set of all rational functions on V. Conversely, to every function field corresponds a unique, projective, non-singular algebraic curve (there may be many curves with the same function field, but only one of them is non-singular). Results in one of these domains can be carried over to the other. An example is the genus; a function field has the same genus as its corresponding curve. This is in turn is related to the genus of topology; if we consider curves over $\mathbb{C}$ we will have a real surface; the number of holes in it is equal to its genus.

Algebraic function fields (i.e. function fields over finite fields) are also closely related to number fields in number theory (for brevity we will drop the "algebraic" prefix for the rest of this section). Number fields and function fields are collectively known as *global fields.* A number field is a subfield F of $\mathbb{C}$ with $[F : \mathbb{Q}] < \infty$; this is similar to Definition 1. One example of their close relation is the Z-function. In Definition 14 we stated that $Z(w) = \sum_{n=0}^{\infty} A_n w^n$ for a function field $F/\mathbb{F}_q$ and $|w| < q^{-1}$. We can rewrite Z as

$$Z(w) = \prod_{P \in \mathbb{P}_F} \left(1 - w^{\deg P}\right)^{-1} \tag{1}$$

since every factor in the product can be written as a geometric sum. (This takes a perhaps more familiar form if we substitute w with q^{-s}.) For a number field K we define the ring of integers O_K as the ring of all integral elements in K (an integral element is the solution to some monic polynomial in $\mathbb{Z}[x]$). We may then define the Dedekind zeta function as the analytic continuation of

$$\zeta_K(s) = \sum_{I \subseteq O_K, I \neq (0)} ||I||^{-s}$$

where I runs through the non-zero ideals of O_K and $||I||$ denotes the index of I, i.e. $||I|| = |O_K/I|$ (which is always finite and well-defined). We can rewrite this in a way similar to what we did in the function field case, to arrive at

$$Z(s) = \prod_{P \subseteq O_K} \left(1 - ||P||^{-s}\right)^{-1} \tag{2}$$

where P ranges over the prime ideals of O_K. The prime ideals in the ring of integers are used instead of places in function fields. We can define valuations v_P by letting $v_P(t)$ be the smallest n such that $t \in P^n$. In the world of function fields, we could have started with valuation rings of F/K (rather than with valuations, as was done in this text) and defined valuation corresponding to a valuation ring O_P as follows: select a prime element t for P; for every $0 \neq z \in F$ there is a unique representation $z = ut^n$, where $u \in O_P \setminus P$ and $n \in \mathbb{Z}$; we say that the valuation of z at P is $v_P(z) = n$.

In fact the prime ideals of O_K act as the prime ideals of C_x, the integral closure of K in $K[x]$. However, different choices of x gives rise to different embeddings, which in turn gives rise to different C_x and thus different prime ideals. By using the places instead of the prime ideals, we avoid these problems. In the geometric view the places correspond to the whole projective space, while the various C_x correspond to affine pieces of it. If we take the intersection of a place P and some C_x we will have either prime ideal of C, or K; e.g. $P_\infty \cap C_x = K$, while $P_0 \cap C_{1/x} = K$.

ζ-functions exist in many areas of mathematics and are characterized by formal similarities. They are complex valued, and take complex arguments. At first they are often only defined for some complex numbers, but can sometimes be analytically extended to almost all of $\mathbb{C}$, usually to some meromorphic function. We can sometimes rewrite them as an Euler product, which is to say a product where the index runs over some kind of primes (e.g. primes numbers, prime ideals). (1) and (2) above are examples of Euler products. Both C_x and O_K are Dedekind domains, which means that their ideals factor into prime ideals in a unique way, which is what enables us to write the ζ-functions as Euler products. Usually we would like to find some kind of functional equation for the ζ-functions (for a Z-function of $F/\mathbb{F}_q$ it takes the form $Z(w) = q^{g-1}w^{2g-2}Z\left(\frac{1}{qw}\right)$, which is essentially the Riemann-Roch theorem). The original ζ-function, due to Riemann, is defined as the analytical continuation of

$$\zeta(s) \quad = \quad \sum_{n=1}^{\infty} \frac{1}{n^s}$$

with Euler product

$$\zeta(s) = \prod_{p\,\text{prime}} \frac{1}{1 - p^{-s}}$$

and functional equation

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s)\, \zeta(1-s)$$

(where Γ denotes the gamma function).

2 The program

The source code is available at algebra.ethna.se. The program is written in Java; with hindsight this might not have been the best choice of language, due to the lack of support for symbolic mathematics in Java. Java seems to lack solid libraries (or built in support) for symbolic mathematics, so large parts of the program are used to represent finite fields and polynomials over them. Java is an object oriented language, so the program is organized into classes. When we below refer to the classes we have italicized their names.

The results from the program are compared with data from manYPoints.org, where tables of upper and lower bounds for the largest algebraic function fields of given genus over a given finite field are available.

2.1 Theory

2.1.1 Information about extensions from the L-polynomial

In order to prove the existence of function fields with N large with respect to g we consider hyperelliptic function fields. Hyperelliptic function fields are useful to us since we can easily find their genus and L-polynomials. Using the L-polynomial of a hyperelliptic function field we can find some information about extensions of them, including the genus and a lower limit on the number of rational places. The following theorem is central to this paper:

Theorem 15. *Let $F/\mathbb{F}_q$ be a hyperelliptic function field, defined by $y^2 = f(x)$, with genus g and N rational places and L-polynomial $L(t)$. Then there exists an extension F' of F with degree $d = L(-1)$, such that $F'/\mathbb{F}_{q^2}$ is a function field with genus $d(g-1)+1$ and at least dN rational places.*

The proofs of these formulas depend on class field theory, which we will not cover. We will try to give some motivation however. At the core of this is the class group from Definition 10; one can prove that subgroups of the class group corresponds to extensions of F. If we find the index of one such subgroup, we know that this is the degree of the extension corresponding to the subgroup. We then know that every rational place of F must split completely in the extension F', so N' (the number of rational places in $\mathbb{P}_{F'}$) must be at least dN (where N is the number of rational places in $\mathbb{P}_F$).

At the same time we can show that $d = [F' : F] = \prod_{\zeta^n=1,\zeta\neq 1} L_F(\zeta)$, where L_F is the L-polynomial of F, and F' has field of constants $\mathbb{F}_{q^n}$; in our case we use $n = 2$, so $d = L_F(-1)$. (Note that we could use another n and that way find other extensions, e.g. over $\mathbb{F}_{q^3}$. We restrict ourselves to $n = 2$ for simplicity.)

The L-polynomial of F/K is connected to the class group by $h = L(1) = \operatorname{ord}\{[A] \in \mathcal{C}_F : \deg[A] = 0\}$, h is known as the class number of $F/\mathbb{F}_q$. $[A]$ is the element in $\mathcal{C}_F = \mathbb{D}_F/\mathcal{P}_F$ corresponding to A in $\mathbb{D}_F$, and $\deg[A] = \deg A$ (it can be shown that this definition of degree is independent of the chosen representative A). The group $\mathcal{C}_F^0 = \{[A] \in \mathcal{C}_F : \deg[A] = 0\}$ (obviously a subgroup of $\mathcal{C}_F$) is thus the group of divisor classes of degree zero, and can be shown to be finite (so that $h \in \mathbb{N}$).

A more detailed account of this section can be found in [GEER] or [RÖK].

2.1.2 What we're looking for

There are various bounds on the maximal number of rational places of a function field with genus g over $\mathbb{F}_q$.

Theorem 16. *[STI, Thm. V.2.3] (Hasse-Weil bound) For a function field $F/\mathbb{F}_q$ with N rational places and genus g, we have $|N - (q+1)| \leq 2g\sqrt{q}$*

Various improvements can be made, including the Serre bound, $|N - (q+1)| \leq g\lfloor 2\sqrt{q}\rfloor$.

At manYPoints.org tables are kept for certain q (all primes under 100 and some powers of 2, 3, 5, 7, 11, 13, 17, 19), and $g \leq 50$.

We are however interested in finding lower bounds. In order to be entered into the tables at manYPoints.org the bound need to be greater than $b_{q,g}/\sqrt{2}$, where $b_{q,g}$ is the current best greater bound for function field over $\mathbb{F}_q$ with genus g. Thus it's not enough just to find any lower bound to fill in the blanks (e.g. at $q = 5^4$, where most g lack lower bounds, we cannot enter any bound we find).

2.1.3 Program sketch

A high level sketch of the program:

```
Input: q, g
P:={square-free polynomials in GF(q)[x] with degree 2g+2
    or 2g+1}

for(p in P){
 FF := HyperEllipticFunctionField(p, GF(q))
 N := #RationalPlaces(FF)

 L(t) := LPolynomial(FF)

 d := L(-1)
 g' := d*(g-2)/2
 N' := d*N

 if(N' > CurrentLowerLimit(g', q^2))
  print FF+" has an extension with at least "+N'+"
      rational places and genus "+g'+" over GF("+(q^2)+"),
       which is better than the current know lower limit."
}
```

2.1.4 Finding the L-polynomial

In order to find the L-polynomial of $F/\mathbb{F}_q$ we use Theorem 12. This means that we need to be able to find the number of rational places of F and of the constant field extensions F_r, for $0 \leq r \leq g$ (the numbers N_r in the theorem). We saw in Example 2 that the places of $K(x)/K$ correspond to $K \cup \{\infty\}$. So the rational places of $K(x,y)/K$, which is an extension of $K(x)$, must all "lie over" the rational places of $K(x)$. Since we know that $y^2 = f(x)$ we can find the rational places of $K(x,y)/K$ by finding the number of solutions $(x,y) \in K$ to $y^2 = f(x)$ and accounting for the place at infinity. If we wish to find the rational places of F_r we allow x and y to be in $\mathbb{F}_{q^r}$ instead of $\mathbb{F}_q$.

2.1.5 Representation of $\mathbb{F}_q$

A fundamental part of the program must be the representation of $\mathbb{F}_q$, since most computations happen in some finite field. If q is prime this is easy (we need only integer computations modulo q), but if $q = p^n$, with $n > 1$, we need to be more sophisticated. In this case we have $\mathbb{F}_q = \frac{\mathbb{F}_p[x]}{(s)}$, where $s \in \mathbb{F}_p[x]$ is irreducible in $\mathbb{F}_p$ and has degree n. The first problem is then to find s; the approach we use is to pick a random monic polynomial with the correct degree until we find one that is irreducible. To test for irreducibility we use Rabin's test, detailed in appendix A.1.

The simplest approach, where e.g. $\mathbb{F}_{81}$ and $\mathbb{F}_9$ are both represented as extensions of $\mathbb{F}_3$ carries with it some problems; it is not trivial to take an element in $\mathbb{F}_9$ and map it to $\mathbb{F}_{81}$. One would have to find a homomorphism ϕ from $\mathbb{F}_9$ to $\mathbb{F}_{81}$ such that $\phi(\mathbb{F}_9)$ is a subfield of $\mathbb{F}_{81}$. Instead of doing that we could represent $\mathbb{F}_{81}$ as $\frac{\mathbb{F}_9[x]}{(r)}$, where $r \in \mathbb{F}_9[x]$ is irreducible and of degree 2. If we represent $\mathbb{F}_{81}$ this way the required homomorphism is simply the identity map.

This picture shows two different "towers" of finite fields, both having their base in $\mathbb{F}_3$, but leading to two different representations of $\mathbb{F}_{81}$, both having $\mathbb{F}_9$ as a subfield (of course), but how $\mathbb{F}_9$ is embedded in $\frac{\mathbb{F}_3[x]}{(x^4+x+2)}$ is not obvious.

$$\begin{array}{ccccc} \frac{\mathbb{F}_3[x]}{(x^4+x+2)} & & & & \\ \cup & & & & \\ \mathbb{F}_3 & \subset & \frac{\mathbb{F}_3[x]}{(x^2+1)} & \subset & \frac{\mathbb{F}_9[y]}{(y^2+x+1)} \end{array}$$

The code thus has two different classes for representing finite fields:

- *GF*(p,n), which represents $\mathbb{F}_{p^n}$ as a direct extension of $\mathbb{F}_p$
- *ExtGF*($\mathbb{F}_q$,n), which represents a degree n extension of $\mathbb{F}_q$.

2.2 Practical details

Listing all square-free polynomials of a given degree is done by first listing all polynomials, and then checking for squares. We list the polynomials recursively, first listing all polynomials of degree $n-1$ and then adding all possible ax^n terms to them.

Internally the program represents the elements of $\mathbb{F}_p$ (p prime) as the integers $0, 1, \cdots, p-1$. Addition and multiplication is carried out modulo p, the additive inverse of a is computed as $p - a$, and multiplicative inverses are found using the extended euclidean algorithm.

The elements of $\mathbb{F}_{p^n}$, p prime, $n > 1$ are represented as polynomials over $\mathbb{F}_p$ with degree less that n. If we denote by m the polynomial used to extend $\mathbb{F}_p$ to $\mathbb{F}_{p^n}$ we find the multiplicative inverse of an element by using the euclidean algorithm, like when $n = 1$, the main difference being the use of the polynomial euclidean algorithm rather than the ordinary one. We also need to be able to do long division using polynomials in order to do multiplication, in order to find the remainder when we divide the product with m.

This means that the program contains a total of three different classes representing polynomials:

1. *FieldElement*, polynomials over the integers, used to represent elements of $\mathbb{F}_q$
2. *Polynomial*, polynomials over the elements of some finite field, also used to represent the elements in *ExtGF*, e.g. the elements of $\frac{\mathbb{F}_9[y]}{(y^2+x+1)}$
3. *SPolynomial*, polynomials over some *ExtGF*. While the above two serve as both elements of various fields and as polynomials, *SPolynomial* are never considered as elements of a field.

There are three classes which represent finite fields:

1. *SimpleGF*, used for fields $\mathbb{F}_p$, p prime
2. *GF*, used for fields $\mathbb{F}_q$. No obvious embedding of e.g. $\mathbb{F}_9$ into $\mathbb{F}_{81}$
3. *ExtGF*, replaces *GF* when you need a specific embedding of some subfield

The *ExtMath* class contains various methods, mostly the euclidean algorithm for integers, *FieldElement*s and *Polynomial*s.

ZPolynomial represents a polynomial over $\mathbb{Z}$; such polynomials cannot be accommodated in the other polynomial classes since $\mathbb{Z}$ doesn't form a field. The L-polynomials are stored as *ZPolynomial*s.

FunctionField contains information on a specific hyperelliptic function field, and methods to compute its L-polynomials and other metrics, e.g. N.

Main ties the other components together, and is responsible for output to the user. This is also where the data from manYPoints.org is loaded into the program, enabling results from the program to be automatically checked against the current best know values.

3 Results and discussion

[GEER] and [RÖK] have already done similar searches. While [RÖK] only searched through $q = 5$, $q = 7$ and $q = 11$ (thus the results where over $\mathbb{F}_{25}$, $\mathbb{F}_{49}$

and $\mathbb{F}_{121}$), [GEER] seems to have done a more comprehensive search. (Quite a few of the lower bounds found at manYPoints.org come from these two papers, which should show the usability of this approach.) In short, no new results have been found. The following values were searched:

q	d (degree of defining polynomial)
3	5,6
5	5,6,7
7	5,6
9	5
11	5
25	3

For some of these a list of all L-polynomials found was saved, for possible further analysis.

The foremost limit of this approach is the time needed to search trough all curves. Different polynomials over $\mathbb{F}_q$ with degree d might give rise to the same hyperelliptic curve, but we only do trivial reductions to remove these doubles. The number of polynomials we search trough for a given degree d and finite field $\mathbb{F}_q$ is $2q^d$ (the number of polynomials of degree $d \geq 0$ is q^{d+1}, but we restrict the first coefficient to either 1 or some random non-square in $\mathbb{F}_q$, since substitution allows us to transform any polynomial into one of these forms). Some of these polynomials are discarded since they are not square free; there are $\left(1 - \frac{1}{q}\right) q^d$ monic square free polynomials of degree d (see e.g. [YUAN]), so we need to compute the L-polynomials of $2\left(1 - \frac{1}{q}\right) q^d$ (*not* distinct) function fields. With the computation of an L-polynomial as the “computational unit” we thus have time-complexity $\mathcal{O}\left(q^d\right)$. This complexity is to be considered bad.

The computations required to compute an L-polynomial depend on q and the genus g of the function field. From theorem 12 we see that every increase in g leads to an exponential increase in the size of the field where we look for solutions (x, y) to $y^2 = f(x)$. The time required for L-polynomial computation increases very rapidly with g (there's a notable delay in computing the L-polynomial for a single genus three curve).

From theorem 15 we see that increases in g leads directly to greater genus g' of the extension. Since we are interested in $g' \leq 50$ we cannot increase g very much. For example, with $q = 5$ and $g = 3$ we have most g' greater than 100, so a search with $q = 5$ and $g = 4$ can be expected to find very few extensions with genus $g' \leq 50$. A similar problem occurs if we try to fill the gaps in $q' = 25$, $31 \leq g' \leq 50$; a search with $q = 5$ and $g = 2$ gives curves with to few points (less than $1/\sqrt{2}$ of the greater bound) while $g = 3$ leads to g' mostly being greater than 50.

The running time of the program isn't very impressive. While it's written in Java, which might itself be faster than e.g. Mathematica, Maple or Magma, the lack of good libraries for handling finite fields or function fields drags it down. It is much more time consuming when you have to develop this functionality yourself. Also, much time and thought have probably been put into optimizing these functions in e.g. Magma, while we've done very little in that regard. The problems in Section 2.1.5 could have been avoided with a smarter selection of irreducible polynomials for constructing the finite fields, and potentially affect performance.

References

[STI] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, 1993

[GEER] G. van der Geer, *Hunting for curves with many points*, IWCC 2009, Lecture Notes in Computes Science 5557 (2009), p. 82-96

[RÖK] K. Rökaeus, *Computer search for curves with many points through families over* $\mathbb{F}_{25}$ *and* $\mathbb{F}_{49}$

[MAR] D. Marcus, *Number Fields*, Springer-Verlag, 1977

[BB] J. Beachy & W. Blair, *Abstract Algebra*, Waveland Press, 3rd ed., 2006

[REID] M. Reid, *Undergraduate Commutative Algebra*, Cambridge University Press, 1995

[MANY] manypoints.org, lists of known upper and lower limits for the maximum number of rational places on a function field of given genus and over a given finite field

[YUAN] http://math.stackexchange.com/questions/93553/squarefree-polynomials-over-finite-fields

A Appendices

A.1 Rabin's irreducibility test

```
Inputs:
f - monic polynomial in GF(q)[x] of degree n
p[i] - distinct prime factors of n, 0<i<k+1
Output:
true - if f is irreducible over GF(q)
false - if f is reducible over GF(q)

r[i] := n/p[i] for 0<i<k+1

for i=1,...,k
  h := x^(q^r[i]) - x (mod f)
  if gcd(h, f) != 1
    exit(false)

h := x^(q^n) - x (mod f)
if h = 0
  exit(true)
else
  exit(false)
```