Handbook of Finite Fields

by

Gary L. Mullen
Department of Mathematics
The Pennsylvania State University
University Park, PA 16802, U.S.A.
Email: mullen@math.psu.edu

and

Daniel Panario
School of Mathematics and Statistics
Carleton University
Ottawa, Ontario K1S 5B6, Canada
Email: daniel@math.carleton.ca

Foreward

To be written later.

Preface

To be written later.

Contents

1

Curves over finite fields

1.1 Introduction to function fields and curves

Arnaldo Garcia, IMPA
Henning Stichtenoth, Sabanci University

The theory of algebraic curves is essentially equivalent to the theory of algebraic function fields. The latter requires less background and is closer to the theory of finite fields; therefore we present here the theory of function fields. At the end of the section, we give a brief introduction to the language of algebraic curves. Our exposition follows mainly the book [40], other references are [13, 21, 24, 32, 31, 46].

Throughout this section, K denotes a *finite field*. However, almost all results of this section hold for arbitrary perfect fields.

1.1.1 Valuations and places

1.1.1 Definition An *algebraic function field over* K is an extension field F/K with the following properties:

1. There is an element $x \in F$ such that x is transcendental over K and the extension $F/K(x)$ has finite degree.
2. No element $z \in F \setminus K$ is algebraic over K.

The field K is the *constant field* of F.

1.1.2 Remark

1. We often use the term *function field* rather than *algebraic function field.*

2. Property 2 in Definition 1.1.1 is often referred to as: K is *algebraically closed in* F, or K is the *full constant field of* F.
3. If F/K is a function field, then the degree $[F : K(z)]$ is finite for *every* $z \in F \setminus K$.
4. Every function field F/K can be generated by *two* elements, $F = K(x, y)$, where the extension $F/K(x)$ is finite and separable.

Throughout this section, F/K always means a function field over K.

1.1.3 Example (*Rational function fields*) The simplest example of a function field over K is the *rational function field* $F = K(x)$, with x being transcendental over K. The elements of $K(x)$ are the *rational functions* $z = f(x)/g(x)$ where f, g are polynomials over K and g is not the zero polynomial.

1.1.4 Example (*Elliptic and hyperelliptic function fields*) Let F be an extension of the rational function field $K(x)$ of degree $[F : K(x)] = 2$. For simplicity we assume that $\mathrm{char} K \neq 2$. Then there exists an element $y \in F$ such that $F = K(x, y)$, and y satisfies an equation over $K(x)$ of the form

$$y^2 = f(x), \quad \text{with } f \in K[x] \text{ square-free}$$

(i.e., f is not divisible by the square of a polynomial $h \in K[x]$ of degree ≥ 1). One shows that F is rational if $\deg(f) = 1$ or 2. F is an *elliptic function field* if $\deg(f) = 3$ or 4, and it is a *hyperelliptic function field* if $\deg(f) \geq 5$. See also Definition 1.1.107 and Example 1.1.108. A detailed exposition of elliptic and hyperelliptic function fields is given in Sections **??** and **??**.

1.1.5 Remark In case of $\mathrm{char} K = 2$, the definition of elliptic and hyperelliptic function fields requires some modification, see [40, Chapters 6.1, 6.2].

1.1.6 Definition A *valuation* of F/K is a map $\nu : F \to \mathbb{Z} \cup \{\infty\}$ with the following properties:

1. $\nu(x) = \infty$ if and only if $x = 0$.
2. $\nu(xy) = \nu(x) + \nu(y)$ for all $x, y \in F$.
3. $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$ for all $x, y \in F$.
4. There exists an element $z \in F$ such that $\nu(z) = 1$.
5. $\nu(a) = 0$ for all $a \in K \setminus \{0\}$.

The symbol ∞ denotes an element not in $\mathbb{Z}$ such that $\infty + \infty = \infty + n = n + \infty = \infty$ and $\infty > m$ for all $m, n \in \mathbb{Z}$.

It follows that $\nu(x^{-1}) = -\nu(x)$ for every nonzero element $x \in F$. Property 3 above is called the *Triangle Inequality*. The following proposition is often useful.

1.1.7 Proposition (*Strict Triangle Inequality*) Let ν be a valuation of the function field F/K and let $x, y \in F$ such that $\nu(x) \neq \nu(y)$. Then $\nu(x + y) = \min\{\nu(x), \nu(y)\}$.

1.1.8 Remark For a valuation ν of F/K, consider the following subsets $\mathcal{O}, \mathcal{O}^*, P$ of F:

$$\mathcal{O} := \{z \in F \mid \nu(z) \geq 0\}, \ \mathcal{O}^* := \{z \in F \mid \nu(z) = 0\}, \ P := \{z \in F \mid \nu(z) > 0\}.$$

Then $\mathcal{O}$ is a ring, $\mathcal{O}^*$ is the group of invertible elements (*units*) of $\mathcal{O}$, and P is a maximal ideal of $\mathcal{O}$. In fact, P is the *unique* maximal ideal of $\mathcal{O}$, which means that $\mathcal{O}$ is a *local ring*. The ideal P is a *principal ideal*, which is generated by every element $t \in F$ with $\nu(t) = 1$.

For distinct valuations ν_1, ν_2, the corresponding ideals $P_1 = \{z \in F \mid \nu_1(z) > 0\}$ and $P_2 = \{z \in F \mid \nu_2(z) > 0\}$ are distinct.

1.1.9 Definition

1. A subset $P \subseteq F$ is a *place* of F/K if there exists a valuation ν of F/K such that $P = \{z \in F \mid \nu(z) > 0\}$. The valuation ν is uniquely determined by the place P. Therefore we write $\nu =: \nu_P$ and say that ν_P is the *valuation corresponding to the place* P.
2. If P is a place of F/K and ν_P is the corresponding valuation, then the ring $\mathcal{O}_P := \{z \in F \mid \nu_P(z) \geq 0\}$ is the *valuation ring of* F corresponding to P.
3. An element $t \in F$ with $\nu_P(t) = 1$ is a *prime element at the place* P.
4. Let $\mathbb{P}_F := \{P \mid P \text{ is a place of } F\}$.

1.1.10 Remark Since P is a maximal ideal of its valuation ring $\mathcal{O}_P$, the residue class ring $\mathcal{O}_P/P$ is a field. The constant field K is contained in $\mathcal{O}_P$, and $P \cap K = \{0\}$. Hence one has a canonical embedding $K \hookrightarrow \mathcal{O}_P/P$. We always consider K as a subfield of $\mathcal{O}_P/P$ via this embedding.

1.1.11 Definition Let P be a place of F/K.

1. The field $F_P := \mathcal{O}_P/P$ is the *residue class field of* P.
2. The degree of the field extension F_P/K is finite and is the *degree of the place* P. We write $\deg P := [F_P : K]$.
3. A place $P \in \mathbb{P}_F$ is *rational* if $\deg P = 1$. This means that $F_P = K$.
4. For $z \in \mathcal{O}_P$, denote by $z(P) \in F_P$ the residue class of z in F_P. For $z \in F \setminus \mathcal{O}_P$, set $z(P) := \infty$. The map from F to $F_P \cup \{\infty\}$ given by $z \mapsto z(P)$ is the *residue class map* at P.

1.1.12 Remark For a *rational* place $P \in \mathbb{P}_F$ and an element $z \in \mathcal{O}_P$, the residue class $z(P)$ is the (unique) element $a \in K$ such that $\nu_P(z - a) > 0$. In this case, one calls the map $z \mapsto z(P)$ from $\mathcal{O}_P$ to K the *evaluation map* at the place P. We note that the evaluation map is K-linear. This map plays an important role in the theory of *algebraic–geometry codes*, see Section **??**.

1.1.13 Example We want to describe all places of the rational function field $K(x)/K$.

1. Let $h \in K[x]$ be an irreducible monic polynomial. Every nonzero element $z \in K(x)$ can be written as
$$z = h(x)^r \cdot \frac{f(x)}{g(x)}$$
with polynomials $f, g \in K[x]$ which are relatively prime to h, and $r \in \mathbb{Z}$. Then the map $\nu_P : K(x) \to \mathbb{Z} \cup \{\infty\}$ with $\nu_P(z) := r$ (and $\nu_P(0) := \infty$) defines a valuation of $K(x)/K$. The corresponding place P is
$$P = \left\{ \frac{u(x)}{v(x)} \mid u, v \in K[x],\ h \text{ divides } u \text{ but not } v \right\}.$$
The residue class field of this place is isomorphic to $K[x]/(h)$ and therefore we have $\deg P = \deg(h)$.
2. Another valuation of $K(x)/K$ is defined by $\nu(z) = \deg(g) - \deg(f)$ for $z = f(x)/g(x) \neq 0$. The corresponding place is called the *place at infinity* and is

denoted by P_∞ or $(x = \infty)$. It follows from the definition that

$$P_\infty = \left\{ \frac{f(x)}{g(x)} \mid \deg(f) < \deg(g) \right\}.$$

The place P_∞ has degree one, that is, it is a rational place.

3. There are no places of $K(x)/K$ other than those described in Parts 1 and 2.
4. For $a \in K$, the polynomial $x - a$ is irreducible of degree 1 and defines a place P of degree one. We sometimes denote this place as $P = (x = a)$. The set $K \cup \{\infty\}$ is therefore in 1–1 correspondence with the set of rational places of $K(x)/K$ via $a \longleftrightarrow (x = a)$.
5. The residue class map corresponding to a place $P = (x = a)$ with $a \in K$ is given as follows: If $z = f(x)/g(x) \in \mathcal{O}_P$ then $g(a) \neq 0$ and

$$z(P) =: z(a) = f(a)/g(a) \in K.$$

In order to determine $z(\infty) := z(P)$ at the infinite place $P = P_\infty$, we write $f(x) = a_n x^n + \cdots + a_0$ and $g(x) = b_m x^m + \cdots + b_0$ with $a_n b_m \neq 0$. Then $z(\infty) = 0$ if $n < m$, $z(\infty) = \infty$ if $n > m$, and $z(\infty) = a_n/b_n$ if $n = m$.

1.1.2 Divisors and Riemann–Roch theorem

1.1.14 Remark [40, Corollary 1.3.2] Every function field F/K has infinitely many places.

1.1.15 Remark The following theorem states that distinct valuations of F/K are *independent* of each other.

1.1.16 Theorem (*Approximation Theorem*) [40, Theorem 1.3.1] Let $P_1, \ldots, P_n \in \mathbb{P}_F$ be pairwise distinct places of F. Let $x_1, \ldots, x_n \in F$ and $r_1, \ldots, r_n \in \mathbb{Z}$. Then there exists an element $z \in F$ such that

$$\nu_{P_i}(z - x_i) = r_i \quad \text{for} \quad i = 1, \ldots, n \ .$$

1.1.17 Definition Let F/K be a function field, $x \in F$ and $P \in \mathbb{P}_F$.

1. P is a *zero of* x if $\nu_P(x) > 0$, and the integer $\nu_P(x)$ is the *zero order* of x at P.
2. P is a *pole of* x if $\nu_P(x) < 0$. The integer $-\nu_P(x)$ is the *pole order* of x at P.

1.1.18 Remark

1. A nonzero element $a \in K$ has neither zeros nor poles.
2. For all $x \neq 0$ and $P \in \mathbb{P}_F$, P is a pole of x if and only if P is a zero of x^{-1}.

1.1.19 Theorem [40, Theorem 1.4.11] For $x \in F \setminus K$ the following hold:

1. x has at least one zero and one pole.
2. The number of zeros and poles of x is finite.
3. Let $P_1, \ldots, P_r$ and $Q_1, \ldots, Q_s$ be all zeros and poles of x, respectively. Then

$$\sum_{i=1}^{r} \nu_{P_i}(x) \deg P_i = \sum_{j=1}^{s} -\nu_{Q_j}(x) \deg Q_j = [F : K(x)] \ .$$

1.1.20 Definition

1. The *divisor group* of F/K is the free abelian group generated by the set of places of F/K. It is denoted by $\mathrm{Div}(F)$. The elements of $\mathrm{Div}(F)$ are *divisors* of F. That means, a divisor of F is a formal sum
$$D = \sum_{P \in \mathbb{P}_F} n_P P \quad \text{with} \quad n_P \in \mathbb{Z} \quad \text{and} \quad n_P \neq 0 \quad \text{for at most finitely many } P.$$
The set of places with $n_P \neq 0$ is the *support* of D and denoted as $\mathrm{supp}\, D$. If $\mathrm{supp}\, D \subseteq \{P_1, \cdots, P_k\}$ then D is also written as
$$D = n_1 P_1 + \ldots + n_k P_k \quad \text{where } n_i = n_{P_i}.$$
Two divisors $D = \sum_P n_P P$ and $E = \sum_P m_P P$ are added coefficientwise, that is $D + E = \sum_P (n_P + m_P) P$. The *zero divisor* is the divisor $0 = \sum_P r_P P$ where all $r_P = 0$.
2. A divisor of the form $D = P$ with $P \in \mathbb{P}_F$ is a *prime divisor*.
3. The *degree* of the divisor $D = \sum_P n_P P$ is
$$\deg D := \sum_{P \in \mathbb{P}_F} n_P \cdot \deg P.$$
We note that this is a finite sum since $n_P \neq 0$ only for finitely many P.
4. A partial order on $\mathrm{Div}(F)$ is defined as follows: if $D = \sum_P n_P P$ and $E = \sum_P m_P P$, then
$$D \leq E \text{ if and only if } n_P \leq m_P \quad \text{for all } P \in \mathbb{P}_F.$$
A divisor $D \geq 0$ is *positive* (or *effective*).

1.1.21 Remark Since every nonzero element $x \in F$ has only finitely many zeros and poles, the following definitions are meaningful.

1.1.22 Definition For a nonzero element $x \in F$, let Z and N denote the set of zeros and poles of x, respectively.

1. The divisor $(x)_0 := \sum_{P \in Z} \nu_P(x) P$ is the *zero divisor* of x.
2. The divisor $(x)_\infty := -\sum_{P \in N} \nu_P(x) P$ is the *divisor of poles* of x.
3. The divisor $\mathrm{div}(x) := \sum_{P \in \mathbb{P}_F} \nu_P(x) P = (x)_0 - (x)_\infty$ is the *principal divisor* of x.

1.1.23 Remark

1. We note that both divisors $(x)_0$ and $(x)_\infty$ are positive divisors. By Theorem 1.1.19, $\deg (x)_0 = \deg (x)_\infty$ and hence $\deg(\mathrm{div}(x)) = 0$.
2. For $x \in F \setminus K$ we have $\deg (x)_0 = \deg (x)_\infty = [F : K(x)]$. The principal divisor of a nonzero element $a \in K$ is the zero divisor. We observe that for the element $0 \in K$, no principal divisor is defined.
3. The sum of two principal divisors and the negative of a principal divisor are principal, since $\mathrm{div}(xy) = \mathrm{div}(x) + \mathrm{div}(y)$ and $\mathrm{div}(x^{-1}) = -\mathrm{div}(x)$. Therefore the principal divisors form a subgroup of the divisor group of F.

1.1.24 Example We consider again the *rational function field* $F = K(x)$. Let $f \in K[x]$ be a nonzero polynomial and write f as a product of irreducible polynomials,

$$f(x) = a \cdot p_1(x)^{r_1} \cdots p_n(x)^{r_n} \ ,$$

where $0 \neq a \in K$ and $p_1, \ldots, p_n$ are pairwise distinct, monic, irreducible polynomials. Let P_i be the place of $K(x)$ corresponding to the polynomial p_i (see Example 1.1.13), and P_∞ be the place at infinity. Then the principal divisor of f in $\mathrm{Div}(K(x))$ is

$$\mathrm{div}(f) = r_1P_1 + \cdots + r_nP_n - dP_\infty \quad \text{where} \quad d = \deg(f).$$

As every element of $K(x)$ is a quotient of two polynomials, we thus obtain the principal divisor for any nonzero element $z \in K(x)$ in this way.

1.1.25 Definition

1. Two divisors $D, E \in \mathrm{Div}(F)$ are *equivalent* if $E = D + \mathrm{div}(x)$ for some $x \in F$. This is an equivalence relation on the divisor group of F/K. We write

$$D \sim E \ \text{ if } D \text{ and } E \text{ are equivalent.}$$

2. $\mathrm{Princ}(F) := \{A \in \mathrm{Div}(F) \mid A \text{ is principal}\}$ is the *group of principal divisors* of F.
3. The factor group $\mathrm{Cl}(F) := \mathrm{Div}(F)/\mathrm{Princ}(F)$ is the *divisor class group* of F.
4. For a divisor $D \in \mathrm{Div}(F)$ we denote by $[D] \in \mathrm{Cl}(F)$ its class in the divisor class group.

1.1.26 Remark The equivalence relation $\sim$ as defined in Definition 1.1.25 is often denoted as *linear equivalence* of divisors.

1.1.27 Remark

1. It follows from the definitions that $D \sim E$ if and only if $[D] = [E]$.
2. $D \sim E$ implies $\deg D = \deg E$.
3. In a *rational* function field $K(x)$, the converse of Part 2 also holds. If F/K is *non-rational*, then there exist, in general, divisors of the same degree which are not equivalent.

1.1.28 Definition Let F/K be a function field and let $A \in \mathrm{Div}(F)$ be a divisor of F. Then the set

$$\mathcal{L}(A) := \{x \in F \mid \mathrm{div}(x) \geq -A \ \} \cup \{0\}$$

is the *Riemann–Roch space associated to the divisor A*.

1.1.29 Proposition $\mathcal{L}(A)$ is a finite-dimensional vector space over K.

1.1.30 Definition For a divisor A, the integer

$$\ell(A) := \dim \mathcal{L}(A)$$

is the *dimension* of A. We point out that $\dim \mathcal{L}(A)$ denotes here the dimension as a vector space over K.

1.1.31 Remark

1. If $A \sim B$ then the spaces $\mathcal{L}(A)$ and $\mathcal{L}(B)$ are isomorphic (as K-vector spaces). Hence $A \sim B$ implies $\ell(A) = \ell(B)$.
2. $A \leq B$ implies $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ and hence $\ell(A) \leq \ell(B)$.
3. $\deg A < 0$ implies $\ell(A) = 0$.
4. $\mathcal{L}(0) = K$ and hence $\ell(0) = 1$.

1.1.32 Remark The following theorem is one of the main results of the theory of function fields.

1.1.33 Theorem (*Riemann–Roch Theorem*) [40, Theorem 1.5.15] Let F/K be a funcion field. Then there exist an integer $g \geq 0$ and a divisor $W \in \mathrm{Div}(F)$ with the following property: for all divisors $A \in \mathrm{Div}(F)$,

$$\ell(A) = \deg A + 1 - g + \ell(W - A).$$

1.1.34 Definition The integer $g =: g(F)$ is the *genus* of F, the divisor W is a *canonical divisor* of F.

1.1.35 Remark [40, Proposition 1.6.1]

1. If $W' \sim W$, then the equation above also holds when W is replaced by W'.
2. Suppose that $g_1, g_2 \in \mathbb{Z}$ and $W_1, W_2 \in \mathrm{Div}(F)$ satisfy the equations $\ell(A) = \deg A + 1 - g_1 + \ell(W_1 - A) \ = \deg A + 1 - g_2 + \ell(W_2 - A)$ for all divisors A. Then $g_1 = g_2$ and $W_1 \sim W_2$.
3. As a consequence of 1 and 2, the canonical divisors of F/K form a uniquely determined divisor class $[W] \in \mathrm{Cl}(F)$, the *canonical class* of F.

1.1.36 Corollary [40, Corollary 1.5.16] Let W be a canonical divisor and $g = g(F)$ the genus of F. Then

$$\deg W = 2g - 2 \quad \text{and} \quad \ell(W) = g.$$

Conversely, every divisor C with $\deg C = 2g - 2$ and $\ell(C) = g$ is canonical.

1.1.37 Remark A slightly weaker version of the Riemann–Roch Theorem is often sufficient:

1.1.38 Theorem (*Riemann's Theorem*)[40, Theorem 1.4.17] Let F/K be a function field of genus g. Then for all divisors $A \in \mathrm{Div}(F)$,

$$\ell(A) \geq \deg A + 1 - g.$$

Equality holds for all divisors A with $\deg A > 2g - 2$.

1.1.39 Example Consider the *rational function field* $F = K(x)$. The following hold:

1. The genus of $K(x)$ is 0.
2. Let P_∞ be the infinite place of $K(x)$, see Example 1.1.13. For every $k \geq 0$ we obtain
$$\mathcal{L}(kP_\infty) = \{f \in K[x] \mid \deg(f) \leq k\}.$$
This shows that Riemann–Roch spaces are natural generalizations of spaces of polynomials.
3. The divisor $W = -2P_\infty$ is canonical.

1.1.40 Remark Conversely, if F/K is a function field of genus $g(F) = 0$, then there exists an element $x \in F$ such that $F = K(x)$. (This does not hold in general if K is not a finite field.)

1.1.41 Remark For divisors of degree $\deg A > 2g-2$, Riemann's Theorem gives a precise formula for $\ell(A)$. On the other hand, $\ell(A) = 0$ if $\deg A < 0$. For the interval $0 \le \deg A \le 2g-2$, there is no exact formula for $\ell(A)$ in terms of $\deg A$.

1.1.42 Theorem (*Clifford's Theorem*) [40, Theorem 1.6.13] For all divisors $A \in \mathrm{Div}(F)$ with $0 \le \deg A \le 2g-2$,

$$\ell(A) \le 1 + \frac{1}{2} \cdot \deg A \ .$$

1.1.43 Remark The genus $g(F)$ of a function field F is its most important numerical invariant. In general it is a difficult task to determine $g(F)$. Some methods are discussed in Subsection 1.1.3. Here we give upper bounds for $g(F)$ in some special cases.

1.1.44 Remark Assume that $F = K(x,y)$ is a function field over K, where x,y satisfy an equation $\varphi(x,y) = 0$ with an *irreducible* polynomial $\varphi(X,Y) \in K[X,Y]$ of degree d. Then

$$g(F) \le \frac{(d-1)(d-2)}{2}.$$

Equality holds if and only if the plane projective curve which is defined by the affine equation $\varphi(X,Y) = 0$, is nonsingular. (These terms are explained in Subsection 1.1.5)

1.1.45 Remark (*Riemann's Inequality*) [40, Corollary 3.11.4] Suppose that $F = K(x,y)$. Then

$$g(F) \le ([F : K(x)] - 1)([F : K(y)] - 1).$$

1.1.3 Extensions of function fields

1.1.46 Remark In this subsection we consider the following situation: F/K and F'/K' are function fields with $F \subseteq F'$ and $K \subseteq K'$. We always assume that K (respectively K') is algebraically closed in F (respectively in F') and that the degree $[F : F']$ is finite. As before, K is a *finite* field.

1.1.47 Remark The extension degree $[K' : K]$ divides $[F' : F]$.

1.1.48 Definition Let $P \in \mathbb{P}_F$ and $P' \in \mathbb{P}_{F'}$. The place P' is an *extension* of P (equivalently, P' *lies over* P, or P *lies under* P') if one of the following equivalent conditions holds:

1. $P \subseteq P'$,
2. $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$,
3. $P' \cap F = P$,
4. $\mathcal{O}_{P'} \cap F = \mathcal{O}_P$.

We write $P'|P$ to indicate that P' is an extension of P.

1.1.49 Remark If P' lies over P then the inclusion $\mathcal{O}_P \hookrightarrow \mathcal{O}_{P'}$ induces a natural embedding of the residue class fields $F_P \hookrightarrow F'_{P'}$. We therefore consider F_P as a subfield of $F'_{P'}$ via this embedding.

1.1.50 Definition Let P' be a place of F' lying above P.

1. There exists an integer $e \geq 1$ such that $\nu_{P'}(z) = e \cdot \nu_P(z)$ for all $z \in F$. This integer $e =: e(P'|P)$ is the *ramification index of* $P'|P$.
2. The degree $f(P'|P) := [F'_{P'} : F_P]$ is finite and is the *relative degree* of $P'|P$.

1.1.51 Remark Suppose that F''/K'' is another finite extension of F'/K'. Let P, P', P'' be places of F, F', F'' such that $P'|P$ and $P''|P'$. Then

$$e(P''|P) = e(P''|P') \cdot e(P'|P) \quad \text{and} \quad f(P''|P) = f(P''|P') \cdot f(P'|P).$$

1.1.52 Theorem (*Fundamental Equality*) [40, Theorem 3.1.11] Let P be a place of F/K. Then there exists at least one but only finitely many places of F' lying above P. If $P_1, \ldots, P_m$ are *all* extensions of P in F' then

$$\sum_{i=1}^{m} e(P_i|P) f(P_i|P) = [F' : F].$$

1.1.53 Corollary Let F'/F be an extension of degree $[F' : F] = n$, and let $P \in \mathbb{P}_F$. Then

1. For every place $P' \in \mathbb{P}_{F'}$ lying over P, $e(P'|P) \leq n$ and $f(P'|P) \leq n$.
2. There are at most n distinct places of F' lying over P.

1.1.54 Definition Let F'/F be an extension of degree $[F' : F] = n$, and let $P \in \mathbb{P}_F$.

1. A place $P' \in \mathbb{P}_{F'}$ over P is *ramified* if $e(P'|P) > 1$, and it is *unramified* if $e(P'|P) = 1$.
2. P is *ramified in* F'/F if there exists an extension of P in F' that is ramified. Otherwise, P is *unramified* in F'.
3. P is *totally ramified* in F'/F if there is a place P' of F' lying over P with $e(P'|P) = n$. It is clear that P' is then the *only* extension of P in F'.
4. P *splits completely* in F'/F if P has n distinct extensions $P_1, \ldots, P_n$ in F'. It is clear that P is then *unramified* in F'.

1.1.55 Theorem [40, Corollary 3.5.5] If F'/F is a finite *separable* extension of function fields, then at most *finitely many* places of F are ramified in F'/F.

1.1.56 Remark More precise information about the ramified places in F'/F is given in Theorem 1.1.71.

1.1.57 Definition For $P \in \mathbb{P}_F$ one defines the *conorm* of P in F'/F as

$$\mathrm{Con}_{F'/F}(P) := \sum_{P'|P} e(P'|P) \cdot P'.$$

For an arbitrary divisor of F we define its conorm as

$$\mathrm{Con}_{F'/F}\left(\sum_P n_P P\right) := \sum_P n_P \cdot \mathrm{Con}_{F'/F}(P).$$

1.1.58 Remark $\mathrm{Con}_{F'/F}$ is a homomorphism from the divisor group of F to the divisor group of F', which sends principal divisors of F to principal divisors of F'.

1.1.59 Remark For every divisor $A \in \mathrm{Div}(F)$, one has

$$\deg \mathrm{Con}_{F'/F}(A) = \frac{[F' : F]}{[K' : K]} \cdot \deg A.$$

In particular, if $K' = K$ then $\deg \mathrm{Con}_{F'/F}(A) = [F' : F] \cdot \deg A$.

1.1.60 Definition Let F'/K' be a finite extension of F/K, let $P \in \mathbb{P}_F$ and $\mathcal{O}_P$ its valuation ring.

1. An element $z \in F'$ is *integral over* $\mathcal{O}_P$ if there exist elements $u_0, \ldots, u_{m-1} \in \mathcal{O}_P$ such that $z^m + u_{m-1}z^{m-1} + \cdots + u_1 z + u_0 = 0$. Such an equation is an *integral equation for* z over $\mathcal{O}_P$.
2. The set $\mathcal{O}'_P := \{z \in F' \mid z \text{ is integral over } \mathcal{O}_P\}$ is a subring of F'. It is the *integral closure of* $\mathcal{O}_P$ *in* F'.

1.1.61 Proposition [40, Chapter 3.2, 3.3] With notation as in Definition 1.1.60, the following hold:

1. $z \in F'$ is integral over $\mathcal{O}_P$ if and only if the coefficients of the minimal polynomial of z over F are in $\mathcal{O}_P$.
2. $\mathcal{O}'_P = \bigcap_{P'|P} \mathcal{O}_{P'}$.
3. There exists a basis $(z_1, \ldots, z_n)$ of F'/F such that $\mathcal{O}'_P = \sum_{i=1}^n z_i \mathcal{O}_P$, that is, every element $z \in F'$ which is integral over $\mathcal{O}_P$, has a unique representation $z = \sum x_i z_i$ with $x_i \in \mathcal{O}_P$. Such a basis $(z_1, \ldots, z_n)$ is an *integral basis* at the place P.
4. Every basis $(y_1, \ldots, y_n)$ of F'/F is an integral basis for *almost all* places $P \in \mathbb{P}_F$ (that is, for all P with only finitely many exceptions). In particular, if $F' = F(y)$ then $(1, y, \ldots, y^{n-1})$ is an integral basis for almost all P.

1.1.62 Remark Using integral bases one can often determine all extensions of a place $P \in \mathbb{P}_F$ in F'. In the following theorem, denote by $\bar{u} := u(P) \in F_P$ the residue class of an element $u \in \mathcal{O}_P$ in the residue class field $F_P = \mathcal{O}_P/P$. For a polynomial $\psi(T) = \sum u_i T^i \in \mathcal{O}_P[T]$ we set $\bar{\psi}(T) := \sum \bar{u}_i T^i \in F_P[T]$.

1.1.63 Theorem (*Kummer's Theorem*) [40, Theorem 3.3.7] Suppose that $F' = F(y)$ with y integral over $\mathcal{O}_P$. Let $\varphi \in \mathcal{O}_P[T]$ be the minimal polynomial of y over F and decompose $\bar{\varphi}$ into irreducible factors over F_P,

$$\bar{\varphi}(T) = \gamma_1(T)^{\epsilon_1} \cdots \gamma_r(T)^{\epsilon_r}$$

with distinct irreducible monic polynomials $\gamma_i \in F_P[T]$ and $\epsilon_i \geq 1$. Choose monic polynomials $\varphi_i \in \mathcal{O}_P[T]$ such that $\bar{\varphi}_i = \gamma_i$. Then the following hold:

1. For each $i \in \{1, \ldots, r\}$ there exists a place $P_i|P$ such that $\varphi_i(y) \in P_i$. The relative degree of $P_i|P$ satisfies $f(P_i|P) \geq \deg(\gamma_i)$.
2. If $(1, y, \ldots, y^{n-1})$ is an *integral basis* at P, then there exists for each $i \in \{1, \ldots, r\}$ a *unique* place $P_i|P$ with $\varphi_i(y) \in P_i$, and we have $e(P_i|P) = \epsilon_i$ and $f(P_i|P) = \deg(\gamma_i)$.
3. If $\bar{\varphi}(T) = \prod_{i=1}^n (T - a_i)$ with distinct elements $a_1, \ldots, a_n \in K$, then P splits completely in F'/F.

1.1.64 Example Consider a field K with $\mathrm{char}K \neq 2$ and a function field $F = K(x, y)$, where y satisfies an equation $y^2 = f(x)$ with a polynomial $f(x) \in K[x]$ of odd degree. Then $[F : K(x)] = 2$, and $\varphi(T) = T^2 - f(x)$ is the minimal polynomial of y over $K(x)$. Let $a \in K$.

1. If $f(a)$ is a nonzero square in K (that is, $f(a) = c^2$ with $0 \neq c \in K$), then the place $(x = a)$ of $K(x)$ (see Example 1.1.13) splits into two rational places of F.
2. If $f(a)$ is a non-square in K, then the place $(x = a)$ has exactly one extension Q in F, and $\deg Q = 2$.
3. If $a \in K$ is a simple root of the equation $f(x) = 0$, then the place $(x = a)$ of $K(x)$ is totally ramified in $F/K(x)$, and its unique extension $P \in \mathbb{P}_F$ is rational.

For more examples see Section 1.2.

1.1.65 Remark In what follows, we assume that F'/F is a *separable* extension of function fields of degree $[F' : F] = n$. As before, P denotes a place of F and $\mathcal{O}'_P$ is the integral closure of $\mathcal{O}_P$ in F'. By $\mathrm{Tr}_{F'/F} : F' \to F$ we denote the *trace mapping*. For information about separable extensions and the trace map, see any standard textbook on algebra, e.g. [29].

1.1.66 Definition

1. For $P \in \mathbb{P}_F$, the set

$$\mathcal{C}_P := \{z \in F' \mid \mathrm{Tr}_{F'/F}(z\mathcal{O}'_P) \subseteq \mathcal{O}_P\}$$

is the *complementary module* of P in F'.

2. There is an element $t_P \in F'$ such that $\mathcal{C}_P = t_P \mathcal{O}'_P$, and we define for $P' \in \mathbb{P}_{F'}$ with $P'|P$ the *different exponent of P' over P* as

$$d(P'|P) := -\nu_{P'}(t_P).$$

We observe that the element t_P is not unique, but the different exponent is well-defined (independent of the choice of t_P).

1.1.67 Lemma [40, Definition 3.4.3]

1. For all $P'|P$, $d(P'|P) \geq 0$.
2. For almost all $P \in \mathbb{P}_F$, $d(P'|P) = 0$ holds for all extensions $P'|P$ in F'.

1.1.68 Definition The *different* of a finite separable extension of function fields F'/F is the divisor of the function field F' defined as

$$\mathrm{Diff}(F'/F) := \sum_{P \in \mathbb{P}_F} \sum_{P'|P} d(P'|P)P' \ .$$

1.1.69 Theorem [40, Theorems 3.4.6, 3.4.13] Let F'/K' be a finite separable extension of F/K.

1. If W is a canonical divisor of F/K, then the divisor

$$W' := \mathrm{Con}_{F'/F}(W) + \mathrm{Diff}(F'/F)$$

is a canonical divisor of F'/K'.

2. (*Hurwitz Genus Formula*) The genera of F' and F satisfy the equation

$$2g(F') - 2 = \frac{[F' : F]}{[K' : K]}(2g(F) - 2) + \deg \mathrm{Diff}(F'/F).$$

1.1.70 Remark We note that Part 2 is an immediate consequence of Part 1 since the degree of a canonical divisor of F is $2g(F) - 2$. Next we give some results that help to compute the different exponents $d(P'|P)$.

1.1.71 Theorem (*Dedekind's Different Theorem*) [40, Theorem 3.5.1] Let F'/F be a finite separable extension of function fields, let $P \in \mathbb{P}_F$ and $P' \in \mathbb{P}_{F'}$ with $P'|P$. Then

1. $d(P'|P) \geq e(P'|P) - 1 \geq 0$.
2. $d(P'|P) = e(P'|P) - 1$ if and only if the characteristic of F does not divide $e(P'|P)$.

1.1.72 Remark In other words, the different of F'/F contains exactly the places of F' which are ramified in F'/F. In particular it follows that only finitely many places are ramified. The following definition is motivated by Dedekind's Different Theorem.

1.1.73 Definition Assume that $P'|P$ is ramified.

1. $P'|P$ is *tame* if the characteristic of F does not divide $e(P'|P)$.
2. $P'|P$ is *wild* if the characteristic of F divides $e(P'|P)$.

1.1.74 Lemma In a tower of separable extensions $F'' \supseteq F' \supseteq F$, the different is *transitive*, that is:

$$d(P''|P) = d(P''|P') + e(P''|P') \cdot d(P'|P) \text{ for } P'' \supseteq P' \supseteq P, \text{ and hence}$$
$$\mathrm{Diff}(F''/F) = \mathrm{Diff}(F''/F') + \mathrm{Con}_{F''/F'}(\mathrm{Diff}(F'/F)).$$

1.1.75 Proposition [40, Theorem 3.5.10] Let $F' = F(y)$ be a separable extension of degree $[F' : F] = n$. Let $P \in \mathbb{P}_F$ and assume that the minimal polynomial φ of y has all of its coefficients in $\mathcal{O}_P$. Let $P_1, \ldots, P_r$ be all extensions of P in F'. Then one has:

1. $0 \leq d(P_i|P) \leq \nu_{P_i}(\varphi'(y))$ for $i = 1, \ldots, r$.
2. $\{1, y, \ldots, y^{n-1}\}$ is an integral basis at P if and only if $d(P_i|P) = \nu_{P_i}(\varphi'(y))$ for $i = 1, \ldots, r$.

Here φ' denotes the derivative of φ in the polynomial ring $F[T]$.

1.1.76 Remark Recall that a finite field extension F'/F is *Galois* if the automorphism group $G := \{\sigma : F' \to F' \mid \sigma \text{ is an automorphism of } F' \text{ which is the identity on } F\}$ has order ord $G = [F' : F]$. In this case, $\mathrm{Gal}(F'/F) := G$ is the *Galois group* of F'/F.

1.1.77 Remark If F'/F is Galois and P is a place of F, the Galois group $\mathrm{Gal}(F'/F)$ acts on the set of extensions of P via $\sigma(P') = \{\sigma(z) \mid z \in P'\}$.

1.1.78 Proposition [40, Theorem 3.7.1] Suppose that F'/F is a *Galois* extension, and let $P \in \mathbb{P}_F$.

1. The Galois group acts *transitively* on the set of extensions of P in F'. That is, for any two extensions P_1, P_2 of P in F', there is an automorphism $\sigma \in \mathrm{Gal}(F'/F)$ such that $P_2 = \sigma(P_1)$.

2. If $P_1, \ldots, P_r$ are *all* extensions of P in F', then
$$e(P_i|P) = e(P_j|P), \quad f(P_i|P) = f(P_j|P), \text{ and } d(P_i|P) = d(P_j|P)$$
holds for all $i, j = 1, \ldots, r$.
3. Setting $e(P) := e(P_i|P)$ and $f(P) := f(P_i|P)$, we have the equality
$$e(P) \cdot f(P) \cdot r = [F' : F].$$

1.1.79 Proposition (*Kummer Extensions*) [40, Proposition 3.7.3] Let $F' = F(y)$ be an extension of function fields of degree $[F' : F] = n$, where the constant field of F is the finite field $\mathbb{F}_q$. Assume that
$$y^n = u \in F \;\text{ and } n \text{ divides } (q-1)\ .$$
Then F'/F is Galois, and the Galois group $\mathrm{Gal}(F'/F)$ is cyclic of order n.

1. For $P \in \mathbb{P}_F$ define $r_P := \gcd(n, \nu_P(u))$, the greatest common divisor of n and $\nu_P(u)$. Then
$$e(P'|P) = \frac{n}{r_P} \;\text{ and }\; d(P'|P) = \frac{n}{r_P} - 1 \;\text{ for all }\; P'|P.$$
2. Denote by K (K', respectively) the constant field of F (F', respectively). Then
$$g(F') = 1 + \frac{n}{[K' : K]}\left(g(F) - 1 + \frac{1}{2}\sum_{P \in \mathbb{P}_F}\left(1 - \frac{r_P}{n}\right)\deg P\right).$$
3. If $K = K'$ and $F = K(x)$ is a rational function field, then
$$g(F') = -n + 1 + \frac{1}{2}\sum_{P \in \mathbb{P}_F}(n - \gcd(n, \nu_P(u)))\deg P.$$

1.1.80 Remark Let F'/F be a Galois extension of function fields of degree $[F' : F] = n$ whose Galois group is cyclic. Suppose that n divides $q-1$ (where the constant field of F is $\mathbb{F}_q$). Then $F' = F(y)$ with some element y satisfying $y^n \in F$. So Proposition 1.1.79 applies.

1.1.81 Example Assume that the characteristic of K is *odd*. Let $F = K(x, y)$ with $y^2 = f(x)$, where $f \in K[x]$ is a square-free polynomial of degree $\deg(f) = 2m+1$. This means that $f = f_1 \cdots f_s$ with pairwise distinct irreducible polynomials $f_i \in K[x]$. Let $P_i \in \mathbb{P}_{K(x)}$ be the place corresponding to f_i, $i = 1, \ldots, s$, and P_∞ be the pole of x in $K(x)$. For $P \in \{P_1, \ldots, P_s, P_\infty\}$ we have $\gcd(2, \nu_P(f)) = 1$, and for all other places $Q \in \mathbb{P}_{K(x)}$ we have $\nu_Q(f) = 0$. Then Part 3 of the Proposition above yields $g(F) = (\deg(f) - 1)/2 = m$. Hence for every integer $m \geq 0$ there exist function fields F/K of genus $g(F) = m$.

1.1.82 Proposition (*Artin–Schreier Extensions*) [40, Proposition 3.7.8] Let F/K be a function field, where K is a finite field of characteristic p. Let $F' = F(y)$ with $y^p - y = u \in F$. We assume that *for all poles* P of u in F, p does not divide $\nu_P(u)$, and that $u \notin K$. Then the following hold:

1. F'/F is Galois of degree $[F' : F] = p$, and F, F' have the same constant field.
2. Exactly the poles of u are ramified in F'/F (in fact, they are *totally ramified*), all other places of F are unramified.
3. Let P be a pole of u in F and let P' be the unique place of F' lying over P. Then the different exponent of $P'|P$ is $d(P'|P) = (p-1)(-\nu_P(u) + 1)$.

4. The genus of F' is given by the formula

$$g(F') = p \cdot g(F) + \frac{p-1}{2}\left(-2 + \sum_{P:\ \nu_P(u)<0} (-\nu_P(u)+1)\cdot \deg P\right).$$

1.1.83 Remark Every Galois extension F'/F of degree $[F' : F] = p = \mathrm{char}K$ can be written as $F' = F(y)$, where y satisfies an equation of the form $y^p - y = u \in F$. If moreover $F = K(x)$ is a *rational* function field, one can choose u in such a way that for all poles P of u in $K(x)$, p does not divide $\nu_P(u)$.

1.1.84 Example Suppose that $\mathrm{char}K = p$ and $F = K(x, y)$, where $y^p - y = f(x) \in K[x]$, $\deg(f) = m$ and m is not divisible by p. Then $F/K(x)$ is Galois of degree p and K is algebraically closed in F. The pole of x is the only place of $K(x)$ that is ramified in $F/K(x)$, and the genus of F is $g(F) = (p-1)(m-1)/2$.

1.1.85 Definition The function field F'/K' is called a *constant field extension* of F/K, if $F' = FK'$ (that is, if $K' = K(\alpha)$ then $F' = F(\alpha)$).

1.1.86 Remark If E/K' is a finite extension of F/K (meaning that E/F is a finite extension and K' is the constant field of E), we consider the intermediate field $F \subseteq F' := FK' \subseteq E$. Then F'/K' is a constant field extension of F/K, and E/F' is an extension of function fields having the same constant field K'.

1.1.87 Theorem [40, Chapter 3.6] Let $F' = FK'$ be a constant field extension of F. Then the following hold:

1. $[F' : F] = [K' : K]$, and K' is algebraically closed in F'.
2. F'/F is unramified, that is, all $P \in \mathbb{P}_F$ are unramified in F'/F.
3. $g(F') = g(F)$.
4. For every divisor $A \in \mathrm{Div}(F)$, $\deg \mathrm{Con}_{F'/F}(A) = \deg A$ and $\ell(\mathrm{Con}_{F'/F}(A)) = \ell(A)$.

1.1.4 Differentials

1.1.88 Remark In this subsection we consider a function field F/K where $K = \mathbb{F}_q$ is a finite field of characteristic p. The aim is to give an interpretation of the *canonical divisors* of F.

1.1.89 Remark The set $F^p := \{z^p \mid z \in F\}$ is a subfield of F which contains K. The extension F/F^p has degree $[F : F^p] = p$ and is *purely inseparable*. An element $z \in F \setminus F^p$ is called a *separating element* for F/K. For every separating element z, the extension $F/K(z)$ is finite and separable.

1.1.90 Remark Recall that a *module* over a field L is just a vector space over L.

1.1.91 Definition Let M be a module over F. A *derivation* of F into M is a map $\delta : F \to M$, which is K-linear and satisfies the *product rule*

$$\delta(u \cdot v) = u \cdot \delta 5. + v \cdot \delta(u) \quad \text{for all} \quad u, v \in F\ .$$

1.1.92 Remark Let $\delta : F \to M$ be a derivation of F, $z \in F$ and $n \geq 0$. Then $\delta(z^n) = nz^{n-1} \cdot \delta(z)$. In particular, $\delta(z^p) = 0$ for all $z^p \in F^p$.

1.1.93 Proposition [40, Proposition 4.1.4] Let x be a separating element for F/K. Then there exists a unique derivation $\delta_x : F \to F$ with the property $\delta_x(x) = 1$. We call δ_x the *derivation of F with respect to x.*

1.1.94 Proposition [40, Chapter 4.1] There is a one–dimensional F-module Ω_F and a derivation $d : F \to \Omega_F$ (written as $z \mapsto dz$) with the following properties:

1. $dz \neq 0$ for every separating element $z \in F$.
2. $dz = \delta_x(z) \cdot dx$ for every $z \in F$ and $x \in F \setminus F^p$.

The pair (Ω_F, d) is the *differential module* of F/K, the elements of Ω_F are *differentials* of F/K.

1.1.95 Remark

1. If $z \in F$ is not separating then $dz = 0$.
2. Given a separating element $x \in F$, every differential $\omega \in \Omega_F$ has a unique representation $\omega = udx$ with $u \in F$, since Ω_F is a one-dimensional F-module.
3. Suppose that $\omega, \eta \in \Omega_F$ and $\omega \neq 0$. Then there is a unique element $u \in F$ such that $\eta = u\omega$. We write then $u = \eta/\omega$.
4. Item 2 in Proposition 1.1.94 says that, for a separating element $x \in F$,

$$\delta_x(z) = \frac{dz}{dx} \quad \text{for all } z \in F.$$

1.1.96 Remark One can attach a divisor to every nonzero differential $\omega \in \Omega_F$ as follows.

1.1.97 Definition [40, Theorem 4.3.2(e)] Let $\omega \in \Omega_F$, $\omega \neq 0$.

1. Let $P \in \mathbb{P}_F$ and let t be a P-prime element (that is, $\nu_P(t) = 1$). Then t is a separating element of F/K, and we can write $\omega = u \cdot dt$ with $u \in F$. We define

$$\nu_P(\omega) := \nu_P(u).$$

   This definition is independent of the choice of the prime element t, and one can show that $\nu_P(\omega) = 0$ for almost all $P \in \mathbb{P}_F$.
2. The divisor

$$\operatorname{div}(\omega) := \sum_{P \in \mathbb{P}_F} \nu_P(\omega) P$$

   is the *divisor of* ω.

1.1.98 Remark Divisors have the property $\operatorname{div}(u\omega) = \operatorname{div}(u) + \operatorname{div}(\omega)$ for $u \in F \setminus \{0\}$ and $\omega \in \Omega_F \setminus \{0\}$. Therefore $\operatorname{div}(\omega) \sim \operatorname{div}(\eta)$ for any two nonzero differentials $\omega, \eta \in \Omega_F$.

1.1.99 Remark Recall that the divisor of poles of an element $0 \neq x \in F$ is denoted by $(x)_\infty$.

1.1.100 Proposition [40, Chapter 4.3] Let $x \in F$ be a separating element for F/K. Then

$$\operatorname{div}(dx) = -2(x)_\infty + \operatorname{Diff}(F/K(x)).$$

1.1.101 Theorem [40, Chapter 4.3] Let $\omega \in \Omega_F$ be a nonzero differential of F/K. Then the divisor $W := \operatorname{div}(\omega)$ is a *canonical divisor* of F. In particular,

$$2g(F) - 2 = \deg(\operatorname{div}(\omega)).$$

1.1.102 Definition For every divisor $A \in \mathrm{Div}(F)$, we define the set

$$\Omega_F(A) := \{\omega \in \Omega_F \mid \mathrm{div}(\omega) \geq A\}.$$

1.1.103 Remark $\Omega_F(A)$ is a finite-dimensional K-vector space.

1.1.104 Theorem (*Riemann–Roch Theorem, 2nd version*) For every divisor $A \in \mathrm{Div}(F)$,

$$\ell(A) = \deg A + 1 - g(F) + \dim \Omega_F(A),$$

where $\dim \Omega_F(A)$ means the dimension as a K-vector space.

1.1.105 Corollary We have $\dim \Omega_F(0) = g(F)$.

1.1.106 Remark We finish this subsection with examples of function fields that will be discussed in detail in Sections **??** and **??**.

1.1.107 Definition

1. A function field F/K of genus $g(F) = 1$ is an *elliptic function field.*
2. A function field F/K is *hyperelliptic* if $g(F) \geq 2$, and there exists an element $x \in F$ such that $[F : K(x)] = 2$.

1.1.108 Example [40, Chapters 6.1, 6.2] Let K be a finite field of characteristic $\neq 2$, and let F/K be an elliptic or hyperelliptic function field of genus g. Assume that F has at least one rational place P. Then there exist $x, y \in F$ such that $F = K(x, y)$ and $y^2 = f(x)$ with a square-free polynomial $f \in K[x]$ of degree $2g + 1$. The differentials

$$\omega_i := \frac{x^i}{y} dx \ , \quad i = 0, \ldots, g-1$$

form a basis of $\Omega_F(0)$.

1.1.5 Function fields and curves

1.1.109 Remark There is an alternative *geometric* approach to function fields via *algebraic curves.* We give here only a very brief (and incomplete) introduction. For more information we refer to [13, 23, 32].

1.1.110 Remark Let K be a finite field, and denote by $\bar{K}$ the algebraic closure of K. Let $K[X_1, \ldots, X_n]$ be the ring of polynomials in n variables over K.

1.1.111 Definition

1. The n-*dimensional affine space* $\mathbf{A}^n = \mathbf{A}^n(\bar{K})$ *over* $\bar{K}$ is the set of all n-tuples of elements of $\bar{K}$. An element $P = (a_1, \ldots, a_n) \in \mathbf{A}^n$ is a *point*, and $a_1, \ldots, a_n$ are its *coordinates.*
2. Let $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$ be polynomials. Then the set $V := \{P \in \mathbf{A}^n \mid f_1(P) = \cdots = f_m(P) = 0\}$ is the *affine algebraic set defined by* $f_1 = \cdots = f_m = 0$. We say that V is *defined over* K since the polynomials $f_1, \ldots, f_m$ have coefficients in K.

3. Let V be as in 2. The set $I(V) := \{f \in \bar{K}[X_1, \ldots, X_n] \mid f(P) = 0 \text{ for all } P \in V\}$ is an ideal of $\bar{K}[X_1, \ldots, X_n]$, which is the *ideal of* V.
4. The algebraic set V is *absolutely irreducible* if $I(V)$ is a prime ideal of $\bar{K}[X_1, \ldots, X_n]$. Then the residue class ring $\Gamma(V) := \bar{K}[X_1, \ldots, X_n]/I(V)$ is an integral domain, and its quotient field $\bar{K}(V) := \mathrm{Quot}(\Gamma(V))$ is the *field of rational functions on* V. The residue class of X_i in $\bar{K}(V)$ is the *i-th coordinate function on* V and is denoted by x_i. The subfield $K(V) := K(x_1, \ldots, x_n) \subseteq \bar{K}(V)$ is the field of *K-rational functions on* V.
5. An absolutely irreducible affine algebraic set V is an *absolutely irreducible affine algebraic curve over* K (briefly, an *affine curve over* K), if the field $K(V)$ as defined in 4 has transcendence degree one over K. This means that $K(V)$ is an *algebraic function field* over K, as defined in Definition 1.1.1. The curve V is a *plane affine curve* if $V \subseteq \mathbf{A}^2$.
6. Let V be an affine curve over K. A point $P \in V$ is *K-rational* if all its coordinates are in K. We set $V(K) := \{P \in V \mid P \text{ is } K\text{-rational}\}$.
7. Two affine curves V_1 and V_2 are *birationally equivalent* if their function fields $K(V_1)$ and $K(V_2)$ are isomorphic.

1.1.112 Example Let F/K be an algebraic function field. Then there exist elements $x, y \in F$ such that $F = K(x, y)$, and there is an irreducible polynomial $f \in K[X, Y]$ such that $f(x, y) = 0$. Let $V \subseteq \mathbf{A}^2$ be the plane affine curve defined by $f = 0$. Then $K(V) = F$.

1.1.113 Definition

1. Let V be an affine curve as in Definition 1.1.111, and let $P \in V$. A rational function $\varphi \in \bar{K}(V)$ is *defined at* P if $\varphi = g(x_1, \ldots, x_n)/h(x_1, \ldots, x_n)$ with $g, h \in \bar{K}[x_1, \ldots, x_n]$ and $g(P) \neq 0$. The set $\mathcal{O}_P(V)$ of all rational functions on V which are defined at P, is a ring and it is the *local ring of* V *at* P.
2. The point P is *non-singular* if its local ring is *integrally closed*. This means, by definition, that every $z \in \bar{K}(V)$ which satisfies an *integral equation* over $\mathcal{O}_P(V)$, is in $\mathcal{O}_P(V)$, see Definition 1.1.60.
3. The curve V is *non-singular* if all of its points are non-singular.

1.1.114 Remark Let $f \in K[X, Y]$ be an *absolutely irreducible polynomial* (that is, f is irreducible in $\bar{K}[X, Y]$). Then the equation $f = 0$ defines a plane affine curve $\mathcal{C} \subseteq \mathbf{A}^2(\bar{K})$. A point $P \in \mathcal{C}$ is non-singular if and only $f_X(P) \neq 0$ or $f_Y(P) \neq 0$, where $f_X(X, Y)$ and $f_Y(X, Y)$ denote the partial derivatives with respect to X and Y, respectively.

1.1.115 Example Let $n > 0$ be relatively prime to the characteristic of K. Then the *Fermat curve* $\mathcal{C}$ which is defined by the equation $f(X, Y) = X^n + Y^n - 1 = 0$, is non-singular.

1.1.116 Remark In a sense, affine curves are not "complete", one has to add a finite number of points "at infinity". To be precise, one introduces the projective space $\mathbf{P}^n$ over $\bar{K}$ and the "projective closure" of an affine curve in $\mathbf{P}^n$. This leads to the concept of a *projective curve*. We do not give details here and refer to textbooks on algebraic geometry, e.g. [13, 23, 32].

1.1.117 Remark

1. Two projective curves are *birationally equivalent* if their function fields are isomorphic.

2. For every projective curve $\mathcal{C}$ there exists a *non-singular* projective curve $\mathcal{X}$ which is birationally equivalent to $\mathcal{C}$. The curve $\mathcal{X}$ is uniquely determined up to isomorphism and it is *the non-singular model of* $\mathcal{C}$.

1.1.118 Remark There is a 1–1 correspondence between {algebraic function fields F/K, up to isomorhism} and {absolutely irreducible, non-singular, projective curves $\mathcal{X}$ defined over K, up to isomorphism}. Under this correspondence, extensions F'/F of function fields correspond to coverings $\mathcal{X}' \to \mathcal{X}$ of curves, composites of function fields $E = F_1F_2$ correspond to fibre products of curves, etc. What corresponds to a place P of a function field F/K? If P is rational, then it corresponds to a K-rational point of the associated projective curve. Now let $K = \mathbb{F}_q$ and let P be a place of F with $\deg P = n$. Then P corresponds to exactly n points on the associated projective curve, with coordinates in the field $\mathbb{F}_{q^n}$. These points form an orbit under the Frobenius map, which is the map that raises the coordinates of points to the q-th power. For details, see [32].

References Cited: [13, 21, 23, 24, 29, 32, 31, 40, 46]

1.2 Rational points on curves

Arnaldo Garcia, IMPA
Henning Stichtenoth, Sabanci University

1.2.1 Remark In this section we use the language of function fields rather than algebraic curves, see Section 1.1. A simple way for switching from function fields to algebraic curves is as follows.

A *function field* $F/\mathbb{F}_q$ *of genus* g corresponds to a *curve* $\mathcal{X}$ *of genus* g *over* $\mathbb{F}_q$, that is an absolutely irreducible, non-singular, projective curve which is defined over $\mathbb{F}_q$. If $F = \mathbb{F}_q(x, y)$ and x, y satisfy the equation $\varphi(x, y) = 0$ for an irreducible polynomial $\varphi(X, Y) \in \mathbb{F}_q[X, Y]$, then $\mathcal{X}$ is a non-singular, projective model of the plane curve which is defined by $\varphi(X, Y) = 0$. By abuse of notation, we say briefly that the curve $\mathcal{X}$ is given by $\varphi(x, y) = 0$. *Rational places* of the function field correspond to $\mathbb{F}_q$*-rational points* of $\mathcal{X}$.

1.2.1 Rational places

1.2.2 Remark Let F be a function field over $\mathbb{F}_q$. Then F has only finitely many rational places.

1.2.3 Definition Define $N(F) := |\{P \mid P \text{ is a rational place of } F\}|$.

1.2.4 Example For the *rational function field* $F = \mathbb{F}_q(x)$ we have $N(F) = q + 1$. The rational places are the zeros of $x - a$ with $a \in \mathbb{F}_q$, and the pole P_∞ of x.

1.2.5 Lemma [40, Lemma 5.1] Let F'/F be a finite extension of function fields having the same constant field $\mathbb{F}_q$. Then the following hold.

1. Let P be a place of F and P' a place of F' lying above P. If P' is rational, then P is rational.
2. $N(F') \leq [F' : F] \cdot N(F)$.

1.2.6 Remark The following special case of Kummer's Theorem [40, Theorem 3.3.7] is often useful to determine rational places of a function field.

1.2.7 Lemma Let P be a rational place of F and let $\mathcal{O}_P$ be its valuation ring. Consider a finite extension $E = F(y)$ of F such that $\mathbb{F}_q$ is also the full constant field of E. Assume that the minimal polynomial $\varphi(T)$ of y over F has all its coefficients in $\mathcal{O}_P$ (that is, y is integral over $\mathcal{O}_P$). Suppose that the reduction $\bar{\varphi}(T)$ of $\varphi(T)$ modulo P (which is a polynomial over the residue class field $\mathcal{O}_P/P = \mathbb{F}_q$) splits over $\mathbb{F}_q$ as follows:

$$\bar{\varphi}(T) = (T - a_1) \cdots (T - a_s) \cdot p_1(T) \cdots p_r(T)$$

with distinct elements $a_1, \ldots, a_s \in \mathbb{F}_q$ and distinct irreducible polynomials $p_1, \ldots, p_r \in \mathbb{F}_q[T]$ of degree > 1. Then there are exactly s rational places $P_1, \ldots, P_s$ of E lying over P.

1.2.8 Example Assume that $q = 2^m$ with $m \geq 2$, and consider the function field $F = \mathbb{F}_q(x, y)$ with

$$y^2 + y = x^{q-1}.$$

The pole P_∞ of x is totally ramified in the extension $F/\mathbb{F}_q(x)$, this gives one rational place of F. Next we consider the place $P = (x = a)$ of $\mathbb{F}_q(x)$ which is the zero of $x - a$ with

$a \in \mathbb{F}_q$. The reduction of the minimal polynomial $\varphi(T) = T^2 + T + x^{q-1}$ modulo P is then

$$\bar{\varphi}(T) = \begin{cases} T^2 + T + 1 & \text{if } a \neq 0, \\ T^2 + T & \text{if } a = 0. \end{cases}$$

The polynomial $T^2 + T = T(T+1)$ splits over $\mathbb{F}_q$ into linear factors. If m is odd, then $T^2 + T + 1$ is irreducible over $\mathbb{F}_q$, and for m even, $T^2 + T + 1$ splits into two distinct linear polynomials over $\mathbb{F}_q$. Therefore

$$N(F) = \begin{cases} 3 & \text{if } m \text{ is odd}, \\ 2q + 1 & \text{if } m \text{ is even}. \end{cases}$$

1.2.2 The Zeta function of a function field

1.2.9 Definition Throughout this subsection we use the following notations:

1. F is an algebraic function field over $\mathbb{F}_q$ of genus $g(F) = g$, and $\mathbb{F}_q$ is algebraically closed in F,
2. $\mathbb{P}_F$ is the set of places of $F/\mathbb{F}_q$,
3. $N(F)$ is the number of rational places of F,
4. $\mathrm{Div}(F)$ is the divisor group of F,
5. $\mathrm{Div}^0(F) := \{A \in \mathrm{Div}(F) \mid \deg A = 0\}$ is the *group of divisors of degree zero*, and $\mathrm{Princ}(F) \subseteq \mathrm{Div}^0(F)$ is the *group of principal divisors* of F,
6. $\mathrm{Cl}^0(F) := \mathrm{Div}^0(F)/\mathrm{Princ}(F)$ is the *class group* of F. In terms of algebraic curves $\mathcal{X}$, the class group corresponds to the rational points of the *Jacobian of* $\mathcal{X}$ and is then denoted as $\mathrm{Jac}(\mathcal{X})(\mathbb{F}_q)$.

1.2.10 Lemma [40, Proposition 5.1.3]

1. For every $n \geq 0$, there are only finitely many divisors $A \geq 0$ with $\deg A = n$.
2. The class group $\mathrm{Cl}^0(F)$ is a finite group.

1.2.11 Definition The number $h := h_F := \mathrm{ord}(\mathrm{Cl}^0(F))$ is the *class number of* F.

1.2.12 Definition The *Zeta function* of F is defined by the power series in $\mathbb{C}[[t]]$ below (here $\mathbb{C}$ is the complex number field):

$$Z(t) := \sum_{n=0}^{\infty} A_n t^n,$$

where A_n denotes the number of *positive* divisors $D \in \mathrm{Div}(F)$ of degree n.

1.2.13 Theorem [40, Theorem 5.1.15]

1. The power series $Z(t)$ converges for all $t \in \mathbb{C}$ with $|t| < q^{-1}$.

2. $Z(t)$ can be written as

$$Z(t) = \frac{L(t)}{(1-t)(1-qt)}$$

with a polynomial $L(t) = a_0 + a_1 t + \cdots + a_{2g} t^{2g} \in \mathbb{Z}[t]$ of degree $2g$. This polynomial is the *L-polynomial of F*.

3. (*Functional Equation of the L-polynomial*) The coefficients of the L-polynomial of F satisfy
   (1) $a_0 = 1$ and $a_{2g} = q^g$,
   (2) $a_{2g-i} = q^{g-i} a_i$ for $0 \le i \le g$.
4. $N(F) = a_1 + (q+1)$.
5. $L(1) = h_F$ is the class number of F.

1.2.14 Lemma [40, Theorem 5.1.15]

1. The L-polynomial factors into linear factors over $\mathbb{C}$ as follows:

$$L(t) = \prod_{j=1}^{2g} (1 - \omega_j t)$$

with *algebraic integers* $\omega_j \in \mathbb{C}$. As $L(\omega_j^{-1}) = 0$, the complex numbers ω_j are the *reciprocals of the roots of* $L(t)$.

2. One can arrange $\omega_1, \ldots, \omega_{2g}$ in such a way that $\omega_j \cdot \omega_{g+j} = q$ for $1 \le j \le g$.

1.2.15 Remark The reciprocal polynomial $P(t) := t^{2g} \cdot L(1/t)$ has an interpretation as the *characteristic polynomial of the Frobenius endomorphism* acting on the Tate module T_ℓ; see [30, 42]. The roots of $P(t)$ are just the reciprocals of the roots of $L(t)$. Therefore, the complex numbers ω_j in Lemma 1.2.14 are also called the *eigenvalues of the Frobenius endomorphism*.

1.2.16 Remark The following theorem is fundamental for the theory of function fields over finite fields. It was first proved by Hasse for $g = 1$; the generalization to all $g \ge 1$ is due to Weil.

1.2.17 Theorem (*Hasse–Weil Theorem*) [40, Theorem 5.2.1]. The reciprocals of the roots of the L-polynomial satisfy

$$|\omega_j| = q^{1/2} \quad \text{for} \quad 1 \le j \le 2g \ .$$

1.2.18 Remark The Hasse–Weil Theorem is often referred to as the *Riemann Hypothesis for function fields over finite fields.*

1.2.3 Bounds for the number of rational places

1.2.19 Remark The next result is an easy consequence of the Hasse–Weil Theorem 1.2.17.

1.2.20 Theorem (*Hasse–Weil Bound*) [40, Theorem 5.2.3]. The number $N = N(F)$ of rational places of a function field $F/\mathbb{F}_q$ of genus g satisfies the inequality

$$|N - (q+1)| \le 2gq^{1/2} \ .$$

If q is not a square, this bound can be improved as follows.

1.2.21 Theorem (*Serre Bound*) [36], [40, Theorem 5.3.1].

$$|N-(q+1)| \leq g \cdot \left\lfloor 2q^{1/2} \right\rfloor ,$$

where $\lfloor \alpha \rfloor$ means the integer part of the real number α.

1.2.22 Definition For every $g \geq 0$, we define

$$N_q(g) := \max\{N \in \mathbb{N} \mid \text{there is a function field } \ F/\mathbb{F}_q \text{ of genus } \ g \text{ with } N(F) = N\}.$$

1.2.23 Remark Clearly $N_q(g) \leq q+1+g \cdot \left\lfloor 2q^{1/2} \right\rfloor$. Further improvements of this bound can be obtained.

1.2.24 Proposition (*Serre's Explicit Formulas*) [37], [40, Proposition 5.3.4]. Suppose that $u_1, \ldots, u_m$ are non-negative real numbers, not all of them equal to zero, satisfying $1+\sum_{n=1}^{m} u_n \cos n\theta \geq 0$ for all $\theta \in \mathbb{R}$. Then

$$N_q(g) \leq 1 + \frac{2g + \sum_{n=1}^{m} u_n q^{n/2}}{\sum_{n=1}^{m} u_n q^{-n/2}}.$$

1.2.25 Remark The results of the examples and tables below are proved in the following way. First one derives upper bounds for $N_q(g)$ using Serre's Explicit Formulas. In some cases, these upper bounds can be improved slightly by rather subtle arguments [25]. Lower bounds for $N_q(g)$ are usually obtained by providing explicit examples of function fields having that number of rational places. Many methods of construction have been proposed, see [26, 31, 45] for some of them.

1.2.26 Example (*The case* $g = 1$) [36]. Let $q = p^e$ with a prime number p.

1. If e is odd, $e \geq 3$ and p divides $\left\lfloor 2q^{1/2} \right\rfloor$, then $N_q(1) = q + \left\lfloor 2q^{1/2} \right\rfloor$.
2. $N_q(1) = q+1+\left\lfloor 2q^{1/2} \right\rfloor$, otherwise.

1.2.27 Example (*The case* $g = 2$). For all prime powers q,

$$q-2+2\cdot \left\lfloor 2q^{1/2} \right\rfloor \leq N_q(2) \leq q+1+2\cdot \left\lfloor 2q^{1/2} \right\rfloor .$$

In fact, the exact value of $N_q(2)$ is known in all cases [36].

1.2.28 Example (*The case* $g = 3$) The value of $N_q(3)$ is known for many but not for all q. For instance, one knows $N_q(3)$ for all $q \leq 169$ and for all $q = 2^k$ with $k \leq 20$. For details we refer to [33].

1.2.29 Remark The following tables show $N_q(g)$ for some small values of q and g. Updated tables can be found on the website http://www.manypoints.org/, see [26].

1.2.30 Example (*Values of* $N_q(g)$ *for* $q = 2, 4, 8$ *and small* g). In the tables below, an entry like $21-24$ means that the exact value of $N_4(8)$ is not known; one knows only that $21 \leq N_4(8) \leq 24$ (at the time of printing).

g	0	1	2	3	4	5	6	7	8	9	10	20
$N_2(g)$	3	5	6	7	8	9	10	10	11	12	13	19-21
$N_4(g)$	5	9	10	14	15	17	20	21	21-24	26	27	40-45
$N_8(g)$	9	14	18	24	25	29	33-34	34-38	35-42	45	42-49	76-83

1.2.31 Example (*Values of $N_q(g)$ for $1 \leq g \leq 4$ and prime numbers $q \leq 43$*) (at the time of printing).

q	2	3	5	7	11	13	17	19	23	29	31	37	41	43
$N_q(1)$	5	7	10	13	18	21	26	28	33	40	43	50	54	57
$N_q(2)$	6	8	12	16	24	26	32	36	42	50	52	60	66	68
$N_q(3)$	7	10	16	20	28	32	40	44	48	60	62	72	78	80
$N_q(4)$	8	12	18	24	33	38	46	48-50	57	67-70	72	82	88-90	92

1.2.32 Remark If the genus $g(F)$ is large with respect to q, the Hasse–Weil bound can be improved considerably.

1.2.33 Proposition (*Ihara's Bound*) [27], [40, Proposition 5.3.3]. Suppose that $N_q(g) = q + 1 + 2gq^{1/2}$. Then $g \leq q^{1/2}(q^{1/2} - 1)/2$.

1.2.34 Example Let q be a square. Then there exists a function field of genus $g = q^{1/2}(q^{1/2} - 1)/2$ having $q + 1 + 2gq^{1/2}$ rational places. For more about function fields which attain the Hasse–Weil upper bound, see Subsection 1.2.4.

1.2.35 Example

1. For $q = 2^{2m+1}$ with $m \geq 1$, and $g = 2^{3m+1} - 2^m$, one knows that $N_q(g) = q^2 + 1$.
2. Similarly, for $q = 3^{2m+1}$ with $m \geq 1$ and $g = 3^{m+1}(3^{4m+2} + 3^{3m+1} - 3^m - 1)/2$ one has $N_q(g) = q^3 + 1$.

The function fields which attain the values $N_q(g)$ in this example, correspond to the *Deligne–Lusztig curves* associated to the *Suzuki group* and to the *Ree group*, respectively [5, 22, 38].

1.2.4 Maximal function fields

1.2.36 Definition A function field $F/\mathbb{F}_q$ is *maximal* if $g(F) > 0$ and $N(F)$ attains the Hasse-Weil upper bound $N(F) = q + 1 + 2gq^{1/2}$.

1.2.37 Remark It is clear that q must be the square of a prime power, if there exists a maximal function field $F/\mathbb{F}_q$. Therefore we assume in this subsection that $q = \ell^2$ is a square. By Ihara's bound 1.2.33, the genus of a maximal function field F over $\mathbb{F}_{\ell^2}$ satisfies $1 \leq g(F) \leq \ell(\ell - 1)/2$.

1.2.38 Example [40, Lemma 6.4.4] Let $H := \mathbb{F}_{\ell^2}(x, y)$ where x, y satisfy the equation $y^\ell + y = x^{\ell+1}$. Then H is a maximal function field over $\mathbb{F}_{\ell^2}$ with $g(H) = \ell(\ell - 1)/2$ and $N(H) = \ell^3 + 1 = \ell^2 + 1 + 2g(H)\ell$. The field H is called the *Hermitian function field over* $\mathbb{F}_{\ell^2}$.

1.2.39 Remark The rational places of the Hermitian function field H are the following: there is a unique common pole of x and y, and for any $\alpha, \beta \in \mathbb{F}_{\ell^2}$ with $\alpha^\ell + \alpha = \beta^{\ell+1}$ there is a unique common zero of $y - \alpha$ and $x - \beta$. In this way one obtains all $1 + \ell^3$ rational places of H.

1.2.40 Remark There are generators u, v of the Hermitian function field H which satisfy the equation $u^{\ell+1} + v^{\ell+1} = 1$. Hence the Hermitian function field is a special case of a *Fermat function field*, which is defined by an equation $u^n + v^n = 1$ with $\gcd(n, q) = 1$.

1.2.41 Proposition

1. Suppose that $F/\mathbb{F}_{\ell^2}$ is a maximal function field of genus $g(F) = \ell(\ell - 1)/2$. Then F is isomorphic to the Hermitian function field H [34].

2. There is no maximal function field $E/\mathbb{F}_{\ell^2}$ whose genus satisfies $\frac{1}{4}(\ell-1)^2 < g(E) < \frac{1}{2}\ell(\ell-1)$ for ℓ odd (and $\frac{1}{4}\ell(\ell-2) < g(E) < \frac{1}{2}\ell(\ell-1)$ for ℓ even) [12].
3. Up to isomorphism there is a unique maximal function field $E/\mathbb{F}_{\ell^2}$ of genus $g(E) = \frac{1}{4}(\ell-1)^2$ for ℓ odd (and $g(E) = \frac{1}{4}\ell(\ell-2)$ for ℓ even) [1, 11].

1.2.42 Proposition (*Serre*) [28]. Let F be a maximal function field over $\mathbb{F}_q$. Then every function field E of positive genus with $\mathbb{F}_q \subset E \subseteq F$ is also maximal over $\mathbb{F}_q$.

1.2.43 Remark The Hermitian function field $H/\mathbb{F}_{\ell^2}$ has a large automorphism group G. Every subgroup $U \subseteq G$ whose fixed field is not rational, provides then an example of a maximal function field H^U over $\mathbb{F}_{\ell^2}$. Most known examples of maximal function fields over $\mathbb{F}_{\ell^2}$ have been constructed in this way, see [5, 18, 20], [24, Chapter 10].

1.2.44 Example [19] Over the field $\mathbb{F}_q$ with $q = r^6$, consider the function field $F = \mathbb{F}_q(x, y, z)$ which is defined by the equations

$$x^r + x = y^{r+1} \quad \text{and} \quad y \cdot \frac{x^{r^2} - x}{x^r + x} = z^{\frac{r^3+1}{r+1}}.$$

Here F is the *Giulietti–Korchmáros function field*; it is maximal over $\mathbb{F}_q$ of genus $g(F) = (r-1)(r^4 + r^3 - r^2)/2$. It is (at the time of printing) the only known example of a maximal function field over $\mathbb{F}_q$ which is *not* a subfield of the Hermitian function field $H/\mathbb{F}_q$.

1.2.45 Remark [41] An important ingredient in many proofs of results on maximal function fields (for example, Parts 2 and 3 of Proposition 1.2.41) is the *Stöhr–Voloch theory* which sometimes gives an improvement of the Hasse–Weil upper bound. The method of Stöhr–Voloch involves the construction of an auxiliary function which has zeros of high order at the $\mathbb{F}_q$-rational points of the corresponding non-singular curve. We illustrate this method in the case of plane curves. Let $f(X, Y) \in \mathbb{F}_q[X, Y]$ be an absolutely irreducible polynomial that defines a non-singular projective plane curve. Recall that an affine point (a, b) with $f(a, b) = 0$ is non-singular if at least one of the partial derivatives $f_X(X, Y)$ or $f_Y(X, Y)$ does not vanish at the point (a, b). The auxiliary function $h(X, Y)$ in this case is obtained from the equation of the tangent line as $h(X, Y) = (X - X^q)f_X(X, Y) + (Y - Y^q)f_Y(X, Y)$. Suppose now that $f(X, Y)$ does not divide $h(X, Y)$. Then

$$N(F) \leq d(d + q - 1)/2 \;,$$

where $F = \mathbb{F}_q(x, y)$ with $f(x, y) = 0$ is the corresponding function field, and d denotes the degree of the polynomial $f(X, Y)$.
As an example consider the case $d = 4$. The genus of F is $g(F) = (d-1)(d-2)/2 = 3$. The bound above gives $N(F) \leq 2q + 6$ which is better than the Hasse–Weil upper bound for all $q \leq 23$. We note that $N_q(3) = 2q + 6$ for $q = 5, 7, 11, 13, 17$ and 19, see Example 1.2.31.

1.2.5 Asymptotic bounds

1.2.46 Remark In this subsection we give some results about the asymptotic growth of the numbers $N_q(g)$, see 1.2.22. As was mentioned in Proposition 1.2.33, the Hasse-Weil upper bound $N_q(g) \leq q + 1 + 2gq^{1/2}$ cannot be attained if the genus is large with respect to q.

1.2.47 Definition The real number $A(q) := \limsup_{g\to\infty} N_q(g)/g$ is *Ihara's quantity.*

1.2.48 Remark As follows from the Hasse–Weil bound, $A(q) \leq 2q^{1/2}$. The following bound is a significant improvement of this estimate.

1.2.49 Theorem (*Drinfeld–Vlăduţ Bound*) [40, Theorem 7.1.3],[47].

$$A(q) \leq q^{1/2} - 1.$$

1.2.50 Remark The proof of the Drinfeld–Vlăduţ bound is a clever application of Serre's explicit formulas 1.2.24. If q is a square, the Drinfeld–Vlăduţ bound is sharp.

1.2.51 Theorem (*Ihara, Tsfasman–Vlăduţ–Zink*) [27, 43].

$$A(q) = q^{1/2} - 1 \quad \text{if } q \text{ is a square.}$$

1.2.52 Remark If q is a non-square, the exact value of $A(q)$ is not known. The lower bounds for $A(q)$, given below, are proved by providing specific sequences of function fields $F_n/\mathbb{F}_q$ such that $\lim_{n\to\infty} N(F_n)/g(F_n) > 0$. Every such sequence gives then a lower bound for $A(q)$. For details, see Section 1.3.

1.2.53 Theorem

1. (*Serre*) [31, Theorem 5.2.9],[37] There is an absolute constant $c > 0$ such that $A(q) > c \cdot \log q$ for all prime powers q.
2. (*Zink, Bezerra–Garcia–Stichtenoth*) [4, 48]

$$A(q^3) \geq 2(q^2 - 1)/(q + 2).$$

1.2.54 Example [2, 6] The best known lower bounds for $A(q)$ for $q = 2, 3, 5$ were obtained from class field towers:

$$\begin{aligned} A(2) &\geq 0.316999\ldots, \\ A(3) &\geq 0.492876\ldots, \\ A(5) &\geq 0.727272\ldots. \end{aligned}$$

1.2.55 Remark A counterpart to Ihara's quantity $A(q)$ is the following quantity.

1.2.56 Definition We set $A^-(q) := \liminf_{g\to\infty} N_q(g)/g$.

1.2.57 Proposition [9] $A^-(q) > 0$ for all q. More precisely,

1. $A^-(q) \geq (q^{1/2} - 1)/4$, if q is a square.
2. There is an absolute constant $d > 0$ such that $A^-(q) \geq d \cdot \log q$ for all q.

References Cited: [1, 2, 4, 5, 6, 9, 11, 12, 13, 18, 19, 20, 22, 24, 25, 26, 27, 28, 30, 31, 33, 34, 36, 37, 38, 40, 41, 42, 43, 45, 46, 47, 48]

1.3 Towers

Arnaldo Garcia, IMPA
Henning Stichtenoth, Sabanci University

We use terminology as in Sections 1.1 and 1.2, see also [40]. Some methods are discussed how to get *lower bounds* for Ihara's quantity $A(q)$, see Definition 1.2.47. Such bounds have a great impact in applications, for instance in coding theory, see Section **??**.

1.3.1 Introduction to towers

1.3.1 Remark Lower bounds for $A(q)$ are usually obtained in the following way: one constructs a sequence of function fields $(F_i/\mathbb{F}_q)_{i\geq 0}$ with $g(F_i) \to \infty$ such that the limit $\lim_{i\to\infty} N(F_i)/g(F_i)$ exists. If this limit is > 0, then it provides a non-trivial lower bound for $A(q)$.

1.3.2 Remark Essentially three methods are known for constructing such sequences of function fields: *modular towers, class field towers* and *explicit towers.* In the following two remarks we give a very brief description of the first two methods.

1.3.3 Remark (*Modular towers*) [3, 7, 8, 27, 43] Modular towers were introduced by Ihara, and independently by Tsfasman, Vlăduţ and Zink. Let N be a positive integer and p a prime number not dividing N. There exists an affine algebraic curve $Y_0(N)$ defined over $\mathbb{F}_p$ such that, for any field K of characteristic p, $Y_0(N)$ parametrizes the set of isomorphy classes of pairs (E, C), where E is an elliptic curve (see Section **??**) and C is a cyclic subgroup of E of order N, defined over K, in a functorial way. The construction of $Y_0(N)$ is independent of p and can be done in characteristic zero also. The complete curve obtained from $Y_0(N)$ is denoted $X_0(N)$. If $\ell \neq p$ is another prime, then the curves $X_0(\ell^n)$, $n = 1, 2, \ldots$ form a tower with the maps sending (E, C) to (E, C') where C' is the unique subgroup of C of index ℓ. Over $\mathbb{F}_{p^2}$, the supersingular elliptic curves **??** together with all their cyclic subgroups of order ℓ^n give rational points on $X_0(\ell^n)(\mathbb{F}_{p^2})$, because Frobenius is multiplication by $-p$ on those curves. This gives a tower of curves over $\mathbb{F}_{p^2}$ which attains the Drinfel'd–Vlăduţ bound.

For $\mathbb{F}_{q^2}$, with q arbitrary, a similar construction can be made using Shimura curves which parametrize abelian varieties of higher dimension with additional structure.

1.3.4 Remark (*Class field towers*) [6, 31, 35, 37] Starting with any function field F_0 of genus $g_0 \geq 2$ and a set S_0 of rational places of F_0, one defines inductively the field F_{n+1} to be the maximal abelian unramified extension of F_n in which all places of S_n split completely, and S_{n+1} to be the set of all places of F_{n+1} which lie over S_n. If $F_n \subsetneq F_{n+1}$ for all n (which is not always the case), the tower thus obtained is called a *class field tower*, and its limit (see Definition 1.3.8) is at least $|S_0|/(g_0 - 1)$. The hard part is to choose F_0, S_0 so that the tower is infinite. This is analogous to the corresponding problem in the number field case of infinite class field towers which was solved by Golod and Shafarevich. A choice of F_0, S_0 then can be used to show that $A(p) \geq c \cdot \log p$, for p prime, with an absolute constant $c > 0$. This approach which is due to Serre [37], is so far the only way to prove that $A(p) > 0$ holds for prime numbers p.

1.3.5 Remark (*Explicit towers of function fields*) These towers were introduced by Garcia and Stichtenoth [14, 40]. The method, which is more elementary than modular towers and class field towers, is presented below in some detail.

1.3.6 Definition A *tower* $\mathcal{F}$ *over* $\mathbb{F}_q$ is an infinite sequence $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ of function fields $F_i/\mathbb{F}_q$ (with $\mathbb{F}_q$ algebraically closed in all F_i) such that

1. $F_0 \subsetneqq F_1 \subsetneqq F_2 \subsetneqq \cdots \subsetneqq F_n \subsetneqq \cdots$,
2. each extension F_{n+1}/F_n is finite and separable,
3. for some $n \geq 0$, the genus $g(F_n)$ is ≥ 2.

1.3.7 Remark Items 2 and 3 imply that $g(F_i) \to \infty$ as $i \to \infty$. The following limit exists for every tower over $\mathbb{F}_q$ [40, Lemma 7.2.3].

1.3.8 Definition Let $\mathcal{F} = (F_0, F_1, \ldots)$ be a tower of function fields over $\mathbb{F}_q$. The limit $\lambda(\mathcal{F}) := \lim_{i\to\infty} N(F_i)/g(F_i)$ is called the *limit of the tower* $\mathcal{F}$.

1.3.9 Remark We note that the inequalities $0 \leq \lambda(\mathcal{F}) \leq A(q)$ hold for every tower over $\mathbb{F}_q$.

1.3.10 Definition A tower $\mathcal{F}/\mathbb{F}_q$ is *asymptotically good* if $\lambda(\mathcal{F}) > 0$. It is *asymptotically bad* if $\lambda(\mathcal{F}) = 0$.

1.3.11 Remark The notion of asymptotically good (bad) towers is related to the notion of asymptotically good (bad) sequences of codes, see Section **??**. The remark below follows immediately from the definitions.

1.3.12 Remark As $A(q) \geq \lambda(\mathcal{F})$, every asymptotically good tower $\mathcal{F}$ over $\mathbb{F}_q$ provides a non-trivial lower bound for Ihara's quantity.

1.3.13 Remark Most towers turn out to be asymptotically bad and some effort is needed to find asymptotically good ones. We discuss now some criteria which ensure that a tower is good.

1.3.14 Definition Let $\mathcal{F} = (F_0, F_1, \ldots)$ be a tower over $\mathbb{F}_q$.

1. A place P of F_0 is *ramified in* $\mathcal{F}/F_0$, if there is some $n \geq 1$ and some place Q of F_n lying over P with ramification index $e(Q|P) > 1$. Otherwise, P is *unramified* in $\mathcal{F}$.
2. A *rational* place P of F_0 *splits completely in* $\mathcal{F}/F_0$, if P splits completely in the extensions F_n/F_0, for all $n \geq 1$.
3. The set $\mathrm{Ram}(\mathcal{F}/F_0) := \{P \mid P$ is a place of F_0 which is ramified in $\mathcal{F}/F_0\}$ is the *ramification locus* of $\mathcal{F}$ over F_0.
4 The set $\mathrm{Split}(\mathcal{F}/F_0) := \{P \mid P$ is a rational place of F_0 splitting completely in $\mathcal{F}/F_0\}$ is the *splitting locus* of $\mathcal{F}$ over F_0.

1.3.15 Remark The splitting locus is alway finite (it may be empty). The ramification locus is finite or infinite.

1.3.16 Theorem [40, Theorem 7.2.10] Assume that the tower $\mathcal{F} = (F_0, F_1, \ldots)$ over $\mathbb{F}_q$ has the following properties.

1. The splitting locus $\mathrm{Split}(\mathcal{F}/F_0)$ is non-empty.
2. The ramification locus $\mathrm{Ram}(\mathcal{F}/F_0)$ is finite.

3. For every $P \in \mathrm{Ram}(\mathcal{F}/F_0)$ there is a constant $c_P \in \mathbb{R}$ such that for all $n \geq 0$ and all places Q of F_n lying over P, the different exponent $d(Q|P)$ is bounded by

$$d(Q|P) \leq c_P \cdot (e(Q|P) - 1).$$

Then the tower $\mathcal{F}$ is asymptotically good, and its limit satisfies the inequality

$$\lambda(\mathcal{F}) \geq \frac{s}{g(F_0) - 1 + r},$$

where

$$s := \left|\ \mathrm{Split}(\mathcal{F}/F_0)\ \right| \quad \text{and} \quad r := \frac{1}{2} \sum_{P \in \mathrm{Ram}(\mathcal{F}/F_0)} c_P \cdot \deg P.$$

1.3.17 Remark Of course, one should choose the constant c_P as small as possible (if it exists). In general it is a difficult task to prove its existence in towers having wild ramification.

1.3.18 Remark A tower $\mathcal{F}/F_0$ is *tame* if all places $P \in \mathrm{Ram}(\mathcal{F}/F_0)$ are tame in all extensions F_n/F_0; that is, the ramification index $e(Q|P)$ is relatively prime to q for all places Q of F_n lying over P. For a tame tower, the constants c_P in Theorem 1.3.16 can be chosen as $c_P = 1$. Hence a tame tower with finite ramification locus and non-empty splitting locus is asymptotically good, and the inequality for $\lambda(\mathcal{F})$ given in Theorem 1.3.16 holds with

$$r := \frac{1}{2} \sum_{P \in \mathrm{Ram}(\mathcal{F}/F_0)} \deg P.$$

1.3.19 Remark All *known* asymptotically good towers of function fields have the properties 1, 2, 3 of Theorem 1.3.16.

1.3.2 Examples of towers

1.3.20 Definition Let $f(Y) \in \mathbb{F}_q(Y)$ and $h(X) \in \mathbb{F}_q(X)$ be non-constant rational functions, and let $\mathcal{F} = (F_0, F_1, \ldots)$ be a tower of function fields over $\mathbb{F}_q$. The tower $\mathcal{F}$ is *recursively defined by the equation* $f(Y) = h(X)$, if there exist elements $x_i \in F_i$ $(i = 0, 1, \ldots)$ such that

1. $F_0 = \mathbb{F}_q(x_0)$ is a rational function field,
2. $F_i = F_{i-1}(x_i)$ for all $i \geq 1$,
3. for all $i \geq 1$, the elements x_{i-1}, x_i satisfy the equation $f(x_i) = h(x_{i-1})$,

1.3.21 Example [40, Proposition 7.3.2] Let $q = \ell^2$ be a square, $\ell > 2$. Then the equation

$$Y^{\ell-1} = 1 - (X + 1)^{\ell-1}$$

defines an asymtotically good tame tower $\mathcal{F}$ over $\mathbb{F}_q$. The ramification locus of this tower is the set of all places $(x_0 = \alpha)$ with $\alpha \in \mathbb{F}_\ell$, and the place $(x_0 = \infty)$ splits completely. By Theorem 1.3.16 the limit satisfies the inequality

$$\lambda(\mathcal{F}) \geq 2/(\ell - 2).$$

For $q = 9$ this limit attains the Drinfeld–Vlăduţ bound $\lambda(\mathcal{F}) = 2 = \sqrt{9} - 1$.

1.3.22 Example [40, Proposition 7.3.3] Let $q = \ell^e$ with $e \geq 2$ and set $m := (q-1)/(\ell-1)$. Then the equation

$$Y^m = 1 - (X+1)^m$$

defines an asymptotically good tame tower $\mathcal{F}$ over $\mathbb{F}_q$ with limit

$$\lambda(\mathcal{F}) \geq 2/(q-2).$$

This gives a simple proof that $A(q) > 0$ for all non-prime values of q. For $q = 4$ the tower attains the Drinfeld–Vlăduţ bound $\lambda(\mathcal{F}) = 1 = \sqrt{4} - 1$.

1.3.23 Example [17] Let $q = p^2$ where p is an *odd prime*. Then the equation

$$Y^2 = \frac{X^2+1}{2X}$$

defines a tame tower $\mathcal{F}$ over $\mathbb{F}_q$. Its ramification locus is

$$\mathrm{Ram}(\mathcal{F}/F_0) = \{(x_0 = \alpha) \mid \alpha^4 = 1 \text{ or } \alpha = 0 \text{ or } \alpha = \infty\ \}.$$

There are $2(p-1)$ rational places of F_0 which split completely in the tower. The inequality in Theorem 1.3.16 gives $\lambda(\mathcal{F}) \geq p-1$ which coincides with the Drinfeld–Vlăduţ bound. So,

$$\lambda(\mathcal{F}) = p - 1.$$

The fact that the splitting locus of this tower has cardinality $2(p-1)$ is not easy to prove. For $p = 3, 5$ one can check directly that the places $(x_0 = \alpha)$ with $\alpha^4 + 1 = 0$ (for $p = 3$) and $\alpha^8 - \alpha^4 + 1 = 0$ (for $p = 5$) split completely in $\mathcal{F}$.

1.3.24 Remark Now we give some examples of *wild towers*, that is, there are some places of F_0 whose ramification index in some extension F_n/F_0 is divisible by the characteristic of $\mathbb{F}_q$. In wild towers, it is usually difficult to find a bound, if it exists, for the different exponents in terms of ramification indices (see Theorem 1.3.16).

1.3.25 Example [14] Let $q = \ell^2$ be a square and define the tower $\mathcal{F} = (F_0, F_1, \ldots)$ over $\mathbb{F}_q$ as follows: $F_0 := \mathbb{F}_q(x_0)$ is the rational function field, and for all $n \geq 0$, set $F_{n+1} := F_n(x_{n+1})$ with

$$(x_{n+1}x_n)^\ell + x_{n+1}x_n = x_n^{\ell+1}.$$

The ramification locus of $\mathcal{F}$ is $\mathrm{Ram}(\mathcal{F}/F_0) = \{\ (x_0 = 0),\ (x_0 = \infty)\ \}$, and all other rational places of F_0 split completely in the tower. We note however that Theorem 1.3.16 is not directly applicable to determine the limit $\lambda(\mathcal{F})$. One can show that

$$\lambda(\mathcal{F}) = \ell - 1,$$

so this tower attains the Drinfeld–Vlăduţ bound.

1.3.26 Example [15] The equation

$$Y^\ell + Y = \frac{X^\ell}{X^{\ell-1}+1}$$

defines a tower over $\mathbb{F}_q$ with $q = \ell^2$, whose limit attains the Drinfeld–Vlăduţ bound $\lambda(\mathcal{F}) = \ell - 1$. The determination of the splitting locus and the ramification locus for this tower is easy. The hard part is to show that $c_P = 2$ for all ramified places (for the definition of c_P see Theorem 1.3.16).

1.3.27 Example [4, 44] Over the field $\mathbb{F}_q$ with $q = \ell^3$, the equation

$$Y^\ell - Y^{\ell-1} = 1 - X + X^{-(\ell-1)}$$

defines an asymptotically good tower $\mathcal{F}$ with limit

$$\lambda(\mathcal{F}) \geq \frac{2(\ell^2-1)}{\ell+2}.$$

It follows that

$$A(\ell^3) \geq \frac{2(\ell^2-1)}{\ell+2},$$

for all prime powers ℓ (see Theorem 1.2.53).

1.3.28 Remark None of the towers in Examples 1.3.21 - 1.3.27 is Galois over F_0, that is, not all of the extensions F_n/F_0, $n \geq 0$ are Galois extensions. In some special cases however, one can prove that the tower $\hat{\mathcal{F}} := (\hat{F}_0, \hat{F}_1, \ldots)$, where $\hat{F}_n$ is the Galois closure of F_n/F_0, is also asymptotically good, see [16, 39].

1.3.29 Remark There are examples of function fields with many rational points which are *abelian extensions* of a rational function field (for instance, the Hermitian function field H, see Example 1.2.38). Other abelian extensions over $\mathbb{F}_q(x)$ having many rational places can be obtained via the method of *cyclotomic function fields* [31]. However, abelian extensions $F/\mathbb{F}_q(x)$ of *large* genus have only few rational places. More precisely, if $(F_i)_{i\geq 0}$ is a sequence of abelian extensions of a rational function field with $g(F_i) \to \infty$, then $\lim_{i\to\infty} N(F_i)/g(F_i) = 0$, see [10].

1.3.30 Remark We conclude this section with a warning: not every irreducible equation $f(Y) = h(X)$ defines a recursive tower. For instance, if one replaces $X+1$ by X in Examples 1.3.21 and 1.3.22, one just gets a finite extension $\mathcal{F}/F_0$ but not a tower. Also, one has to show that $\mathbb{F}_q$ is algebraically closed in each field F_i of the tower. In most of the examples above this follows from the fact that there is some place which is totally ramified in all extensions F_i/F_0.

References Cited: [3, 4, 6, 7, 8, 10, 14, 15, 16, 17, 27, 29, 31, 35, 37, 39, 40, 43, 44]

Bibliography

[1] M. Abdón and F. Torres. On maximal curves in characteristic two. *Manuscripta Math.*, 99(1):39–53, 1999. <24, 25>

[2] B. Angles and C. Maire. A note on tamely ramified towers of global function fields. *Finite Fields Appl.*, 8(2):207–215, 2002. <25>

[3] P. Beelen and I. I. Bouw. Asymptotically good towers and differential equations. *Compos. Math.*, 141(6):1405–1424, 2005. <26, 30>

[4] J. Bezerra, A. Garcia, and H. Stichtenoth. An explicit tower of function fields over cubic finite fields and Zink's lower bound. *J. Reine Angew. Math.*, 589:159–199, 2005. <25, 29, 30>

[5] E. Çakçak and F. Özbudak. Subfields of the function field of the Deligne-Lusztig curve of Ree type. *Acta Arith.*, 115(2):133–180, 2004. <23, 24, 25>

[6] I. Duursma and K.-H. Mak. On lower bounds for the Ihara constants A(2) and A(3). *arXiv:1102.4127v2[math.NT]*, 2011. <25, 26, 30>

[7] N. D. Elkies. Explicit modular towers. *Proceedings of the 35th Allerton conference on communication, control and computing*, pages 23–32, 1998. <26, 30>

[8] N. D. Elkies. Explicit towers of Drinfeld modular curves. In *European Congress of Mathematics, Vol. II (Barcelona, 2000)*, volume 202 of *Progr. Math.*, pages 189–198. Birkhäuser, Basel, 2001. <26, 30>

[9] N. D. Elkies, E. W. Howe, A. Kresch, B. Poonen, J. L. Wetherell, and M. E. Zieve. Curves of every genus with many points. II. Asymptotically good families. *Duke Math. J.*, 122(2):399–422, 2004. <25>

[10] G. Frey, M. Perret, and H. Stichtenoth. On the different of abelian extensions of global fields. In *Coding theory and algebraic geometry (Luminy, 1991)*, volume 1518 of *Lecture Notes in Math.*, pages 26–32. Springer, Berlin, 1992. <30>

[11] R. Fuhrmann, A. Garcia, and F. Torres. On maximal curves. *J. Number Theory*, 67(1):29–51, 1997. <24, 25>

[12] R. Fuhrmann and F. Torres. The genus of curves over finite fields with many rational points. *Manuscripta Math.*, 89(1):103–106, 1996. <24, 25>

[13] W. Fulton. *Algebraic curves*. Advanced Book Classics. Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1989. An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original. <1, 16, 17, 18, 25>

[14] A. García and H. Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlăduţ bound. *Invent. Math.*, 121(1):211–222, 1995. <26, 29, 30>

[15] A. Garcia and H. Stichtenoth. On the asymptotic behaviour of some towers of function fields over finite fields. *J. Number Theory*, 61(2):248–273, 1996. <29, 30>

[16] A. Garcia and H. Stichtenoth. On the Galois closure of towers. In *Recent trends in coding theory and its applications*, volume 41 of *AMS/IP Stud. Adv. Math.*, pages 83–92. Amer. Math. Soc., Providence, RI, 2007. <30>

[17] A. Garcia, H. Stichtenoth, and H.-G. Rück. On tame towers over finite fields. *J. Reine Angew. Math.*, 557:53–80, 2003. <29, 30>

[18] A. Garcia, H. Stichtenoth, and C.-P. Xing. On subfields of the Hermitian function field. *Compositio Math.*, 120(2):137–170, 2000. <24, 25>

[19] M. Giulietti and G. Korchmáros. A new family of maximal curves over a finite field. *Math. Ann.*, 343(1):229–245, 2009. <24, 25>

[20] M. Giulietti, G. Korchmáros, and F. Torres. Quotient curves of the Suzuki curve. *Acta Arith.*, 122(3):245–274, 2006. <24, 25>

[21] D. M. Goldschmidt. *Algebraic functions and projective curves*, volume 215 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2003. <1, 18>

[22] J. P. Hansen and J. P. Pedersen. Automorphism groups of Ree type, Deligne-Lusztig curves and function fields. *J. Reine Angew. Math.*, 440:99–109, 1993. <23, 25>

[23] R. Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52. <16, 17, 18>

[24] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres. *Algebraic curves over a finite field*. Princeton Series in Applied Mathematics. Princeton University Press, Princeton, NJ, 2008. <1, 18, 24, 25>

[25] E. Howe and K. Lauter. Improved upper bounds for the number of points on curves over finite fields. *Ann. Inst. Fourier (Grenoble)*, 53(6):1677–1737, 2003. <22, 25>

[26] E. Howe, K. Lauter, C. Ritzenthaler, and G. van der Geer. manYPoints - table of curves with many points. *http://www.manypoints.org/*. <22, 25>

[27] Y. Ihara. Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 28(3):721–724 (1982), 1981. <23, 25, 26, 30>

[28] G. Lachaud. Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis. *C. R. Acad. Sci. Paris Sér. I Math.*, 305(16):729–732, 1987. <24, 25>

[29] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002. <11, 18, 30>

[30] D. Lorenzini. *An invitation to arithmetic geometry*, volume 9 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1996. <21, 25>

[31] H. Niederreiter and C. Xing. *Rational points on curves over finite fields: theory and applications*, volume 285 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2001. <1, 18, 22, 25, 26, 30>

[32] H. Niederreiter and C. Xing. *Algebraic geometry in coding theory and cryptography*. Princeton University Press, Princeton, NJ, 2009. <1, 16, 17, 18>

[33] C. Ritzenthaler. Optimal curves of genus 1,2 and 3. *Publ. Math. Besancon (PMB)*, 2011. <22, 25>

[34] H.-G. Rück and H. Stichtenoth. A characterization of Hermitian function fields over finite fields. *J. Reine Angew. Math.*, 457:185–188, 1994. <23, 25>

[35] R. Schoof. Algebraic curves over $\mathbf{F}_2$ with many rational points. *J. Number Theory*, 41(1):6–14, 1992. <26, 30>

[36] J.-P. Serre. Nombres de points des courbes algébriques sur $\mathbf{F}_q$. In *Seminar on number theory, 1982–1983 (Talence, 1982/1983)*, pages Exp. No. 22, 8. Univ. Bordeaux I, Talence, 1983. <22, 25>

[37] J.-P. Serre. Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini. *C. R. Acad. Sci. Paris Sér. I Math.*, 296(9):397–402, 1983. <22, 25, 26, 30>

[38] J.-P. Serre. Quel est le nombre maximum de points rationnels que peut avoir une courbe algébrique de genre g sur un corps fini? *Annuaire du Collége de France*, 84:397–402, 1984. <23, 25>

[39] H. Stichtenoth. Transitive and self-dual codes attaining the Tsfasman-Vlăduţ-Zink bound. *IEEE Trans. Inform. Theory*, 52(5):2218–2224, 2006. <30>

[40] H. Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009. <1, 2, 4, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 18, 19, 20, 21, 22, 23, 25, 26, 27, 28, 29, 30>

[41] K.-O. Stöhr and J. F. Voloch. Weierstrass points and curves over finite fields. *Proc. London Math. Soc. (3)*, 52(1):1–19, 1986. <24, 25>

[42] J. Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966. <21, 25>

[43] M. A. Tsfasman, S. G. Vlăduţ, and T. Zink. Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. *Math. Nachr.*, 109:21–28, 1982. <25, 26, 30>

[44] G. van der Geer and M. van der Vlugt. An asymptotically good tower of curves over the field with eight elements. *Bull. London Math. Soc.*, 34(3):291–300, 2002. <29, 30>

[45] G. van der Geer and M. van der Vlugt. Tables of curves with many points. *http://www.science.uva.nl/ geer/tables-mathcomp21.pdf*, 2009. <22, 25>

[46] G. D. Villa Salvador. *Topics in the theory of algebraic function fields*. Mathematics: Theory & Applications. Birkhäuser Boston Inc., Boston, MA, 2006. <1, 18, 25>

[47] S. G. Vlăduţ and V. G. Drinfeld. The number of points of an algebraic curve. *Funktsional. Anal. i Prilozhen.*, 17(1):68–69, 1983. <25>

[48] T. Zink. Degeneration of Shimura surfaces and a problem in coding theory. In *Fundamentals of computation theory (Cottbus, 1985)*, volume 199 of *Lecture Notes in Comput. Sci.*, pages 503–511. Springer, Berlin, 1985. <25>

Index