Recursive Towers of Function Fields over Finite Fields

Dietrich Kuhn
(Carl von Ossietzky University Oldenburg)

March 11, 2022

Function Fields and their Extensions

Definition

- An algebraic **function field** F/k of one variable over k is an extension field $F \supset k$ such that F is a finite algebraic extension of $k(x)$ for some element $x \in F$ which is transcendental over k.
- The algebraic closure of k in F is called the **full constant field** of F.
- Let F' and F be function fields over the full constant fields k' and k, resp., such that $F' \supseteq F$ and $k' \supseteq k$. Then the extension F'/F of fields is called an **extension of function fields** if F'/F is algebraic.

Examples

Let $f(X,Y) := Y^2 - X(X^2+1) \in \mathbb{R}[X,Y]$ and let

$$(F_0, F_1, F_2) := (\mathbb{R}(x_0), \mathbb{R}(x_0, x_1), \mathbb{R}(x_0, x_1, x_2))$$

with $f(x_0, x_1) = 0$ and $f(x_1, x_2) = 0$.

Places and Genus

Let F be a function field over the full constant field k.

- A **place** P of F is the unique maximal ideal of some maximal discrete valuation ring $\mathcal{O}_P$ in F with $k \subsetneqq \mathcal{O}_P \subsetneqq F$.
- The **degree** $\deg(P)$ of a place P in F is defined as $[\mathcal{O}_P/P : k]$.
- $N(F)$ denotes the number of **rational** (i.e. degree one) places in F.
- $g(F) \in \mathbb{N}_0$ denotes the **genus** of F.

Examples

Let $f(X,Y) := Y^2 - X(X^2+1) \in \mathbb{R}[X,Y]$ and let

$$\mathcal{F}_0 := (F_0, F_1, F_2, \dots) := (\mathbb{R}(x_0), \mathbb{R}(x_0,x_1), \mathbb{R}(x_0,x_1,x_2), \dots)$$

with $f(x_n, x_{n+1}) = 0$ for all $n \in \mathbb{N}_0$. Then we have

$$(g(F_0), g(F_1), g(F_2), \dots) = (0,1,6,\dots) \text{ and } g(F_n) \to \infty.$$

Recursive Towers of Function Fields

Definition

Let $\mathcal{F} = (F_0, F_1, \ldots) = (F_\nu)_\nu$ be a sequence of function fields F_n over k.

(i) $\mathcal{F}$ is called a **tower** if each extension F_n/F_{n-1} is proper, finite and separable and $g(F_n) \to \infty$ as $n \to \infty$.

(ii) A tower $\mathcal{F}$ is called **recursively defined** by an absolutely irreducible polynomial $f(X, Y) \in k[X, Y]$ if there exist $x_n \in F_n$ s.t. for all n

- $F_n = k(x_0, x_1, \ldots, x_n)$ and $f(x_n, x_{n+1}) = 0$,
- $[F_{n+1} : F_n] = \deg_Y(f)$.

Examples

- $\mathcal{F}_0/\mathbb{R}$: $Y^2 - X(X^2+1)$.
- $\mathcal{F}_{2,a}/\mathbb{F}_2$: $X^2Y^2 + XY^2 + Y + a(X^2+1) + (a-1)X$ with $a \in \mathbb{F}_2$.
- $\mathcal{F}_5/\mathbb{F}_5$: $(X^6 + X + 2)(Y^5 - Y) - (X^5 - X)(Y^6 + Y^5 + 2Y + 3)$.

Good Towers

Let $\mathcal{F} = (F_\nu)_\nu$ be a tower over $\mathbb{F}_q$. Then we define

- $\nu(\mathcal{F}) := \lim_{n\to\infty} \frac{N(F_n)}{[F_n:F_0]} \in \mathbb{R}_{\geq 0}$ **(splitting rate)**
- $\gamma(\mathcal{F}) := \lim_{n\to\infty} \frac{g(F_n)}{[F_n:F_0]} \in \mathbb{R}_{>0} \cup \{\infty\}$ **(genus)**
- $\lambda(\mathcal{F}) := \frac{\nu(\mathcal{F})}{\gamma(\mathcal{F})} \in \mathbb{R}_{\geq 0}$ **(limit)**

and $\mathcal{F}$ is called **good** if $\lambda(\mathcal{F}) > 0$.

Examples

- $0 \leq \lambda(\mathcal{F}_{2,a}) \leq \sqrt{2} - 1 \approx 0,414\ldots$
- $0,666\ldots = \frac{2}{5-2} \leq \lambda(\mathcal{F}_5) \leq \sqrt{5} - 1 \approx 1,236\ldots$

Known Bounds for the Limit

Upper bounds:

- $A(q) := \limsup_{\mathcal{F}} \lambda(\mathcal{F})$ Ihara's Constant
- $0 \leq \lambda(\mathcal{F}) \leq A(q) \leq \sqrt{q} - 1$ (Drinfeld-Vladut, 1983)

Some lower bounds:

- q square: $A(q) = \sqrt{q} - 1$ (Tsfasman-Vladut-Zink, modular curves, 1982; Garcia-Stichtenoth, recursive towers, 1995)
- $q = p^{2m+1}$ with p prime and $m \geq 1$: $A(q) \geq \frac{2(p^{m+1}-1)}{p+1+\frac{p-1}{p^m-1}}$
  (Bassa-Beelen-Garcia-Stichtenoth, recursive towers, 2013)
- $q \neq 2, 3$: $A(q) \geq \frac{2}{q-2}$ (Bassa-Ritzenthaler, recursive towers, 2020)
- q, l arbitrary: $A(q^l) \geq c\frac{l^2 \log(q)^2}{l+\log(q)}$ (Temkine, class field towers, 2001)
- $A(2) \geq 0.316999$, $A(3) \geq 0.492876$ (Duursma-Mak, cft, 2012)

Applications and Open Problems

Towers of function fields over finite fields have applications in the construction of error-correcting codes and cryptography (e.g. encryption, secret sharing, multi-party-computation).

Open problems:

- Find/Construct good recursive towers for $q = 2, 3$.
- Find/Construct better/other recursive towers with more specific properties (e.g. F_n / F_0 Galois for all $n \in \mathbb{N}_0$) and classify them.
- Elkies's 'Fantasia' (1998): Any optimal recursive tower has a modular interpretation.
- Find better lower and upper bounds for the limit of a recursive tower or even determine its precise value.

Open Problems

Definition

Let $\mathcal{F} = (F_\nu)_\nu$ be a recursive tower over a finite field. Then we define

- $\mathrm{Split}(\mathcal{F}/F_0)$ as the set of all rational places $P \in \mathbb{P}_{F_0}$ which split in F_n/F_0 for all $n \in \mathbb{N}$ and
- $\mathrm{Ram}(\mathcal{F}/F_0)$ as the set of all places $P \in \mathbb{P}_{F_0}$ which ramify in F_n/F_0 for some $n \in \mathbb{N}$.

Conjecture (Beelen-Garcia-Stichtenoth, 2004)

Let $\mathcal{F} = (F_\nu)_\nu$ be a recursive tower over a finite field of degree d.

(C1) *If* $\nu(\mathcal{F}) = \lim_{n\to\infty} \frac{N(F_n)}{d^n} > 0$, *then* $\#\mathrm{Split}(\mathcal{F}/F_0) > 0$.

(C1') $\nu(\mathcal{F}) = \#\mathrm{Split}(\mathcal{F}/F_0)$.

(C2) *If* $\gamma(\mathcal{F}) = \lim_{n\to\infty} \frac{g(F_n)}{d^n} < \infty$, *then* $\#\mathrm{Ram}(\mathcal{F}/F_0) < \infty$.

Tower Graphs and a Partial Solution for Conjecture 1

Definition

Let $\mathcal{F} = (F_\nu)_\nu$ be a recursive tower over the field k which is defined by the polynomial $f(X, Y)$. Then we call the directed graph $\Gamma_\mathcal{F}$ with

- the vertex set $V(\Gamma_\mathcal{F}) := k \cup \{\infty\}$,
- the edge set $E(\Gamma_\mathcal{F}) := \{(x, y) \in V(\Gamma_\mathcal{F})^2 : f(x, y) = 0\}$,
- edge map : $E(\Gamma_\mathcal{F}) \to V(\Gamma_\mathcal{F})^2$, $(x, y) \mapsto (x, y)$

the **tower graph** of $\mathcal{F}$.

Theorem (K, 2021)

Let $\mathcal{F} = (F_\nu)_\nu$ be a recursive tower over a finite field and let $\Gamma_\mathcal{F}^{\mathrm{ram}}$ be the ramification subgraph of its tower graph $\Gamma_\mathcal{F}$. If $\Gamma_\mathcal{F}^{\mathrm{ram}}$ has no finite weakly connected component which is also strongly connected and only has circles with balanced ramification indices, then $\nu(\mathcal{F}) = \#\mathrm{Split}(\mathcal{F}/F_0)$.

Consequences of the Partial Solution for Conjecture 1

- $0 = \lambda(\mathcal{F}_{2,a}) \leq \sqrt{2} - 1$. More generally, there are no good recursive towers of degree two over $\mathbb{F}_2$ by [7] (Stichtenoth-Tutdere, 2015).
- $0,666\cdots = \frac{2}{5-2} = \lambda(\mathcal{F}_5) \leq \sqrt{5} - 1$. More generally, the recursive towers in [8] (Bassa-Ritzenthaler, 2020) have the precise limit $\frac{2}{q-2}$.
- Improvements of results in
  - [2] Beelen-Garcia-Stichtenoth, 2004
  - [4] Maharaj-Wulftange, 2005
  - [5] Bassa-Garcia-Stichtenoth, 2008
  - [6] Hallouin-Perret, 2012
  - [7] Stichtenoth-Tutdere, 2015
  - [8] Bassa-Ritzenthaler, 2020
  - ...

  For all tame recursive towers $\mathcal{F}$, the theorem provides their precise limits $\lambda(\mathcal{F})$ and, for all wild recursive towers $\mathcal{F}$, it at least provides the precise splitting rate $\nu(\mathcal{F})$.

Techniques of the Proof and a Further Remark

Techniques:

- Virtual Abhyankar's Lemma
- Adjacency matrices of finite digraphs with weighted edges in $\mathbb{R}_{\geq 0}$
- Perron-Frobenius Theory
- Complex analysis (Maximum Modulus Principle)
- A new interpretation of the characteristic polynomial in terms of circles of the graph.

Further remark:
For a tame recursive tower $\mathcal{F} = (F_\nu)_\nu$ such that $\Gamma_{\mathcal{F}}^{\mathrm{ram}}$ is finite and satisfies a further 'mild' graph theoretical condition, there is an algorithm to compute an explicit formula for $g(F_n)$.

[1] Noam D. Elkies, *Explicit Modular Towers*, Proceedings of the Thirty-Fifth [1997] Annual Allerton Conference on Communication, Control and Computing, 1998, pp. 23–32.

[2] Peter Beelen, Arnaldo Garcia, and Henning Stichtenoth, *On Towers of Functions Fields Over Finite Fields* (2004).

[3] Peter Beelen, *Graphs and recursively defined towers of function fields*, Journal of Number Theory **108** (2004), no. 2, 217 - 240, DOI http://dx.doi.org/10.1016/j.jnt.2004.05.011.

[4] Hiren Maharaj and Jörg Wulftange, *On the construction of tame towers over finite fields*, Journal of Pure and Applied Algebra **199** (2005), no. 1 - 3, 197 - 218, DOI http://dx.doi.org/10.1016/j.jpaa.2004.12.008.

[5] Alp Bassa, Arnoldo Garcia, and Henning Stichtenoth, *A new tower over cubic finite fields*, Moscow Mathematical Journal (2008).

[6] Emmanuel Hallouin and Perret Marc, *Recursive Towers of Curves over Finite Fields using Graph Theory*, Moscow Mathematical Journal **14** (2012), DOI 10.17323/1609-4514-2014-14-4-773-806.

[7] Henning Stichtenoth and Seher Tutdere, *Quadratic recursive towers of function fields over* $\mathbb{F}_2$, Turkish Journal of Mathematics **39** (2015), 665-682.

[8] Alp Bassa and Christophe Ritzenthaler, *Good recursive towers over prime fields exist*, Mathematische Annalen **378** (2020), no. 1, 599–604.