Rational points on curves over finite fields and Drinfeld modular varieties

Alp Bassa

Sabancı University

Curves over Finite Fields

Let $\mathcal{C}$ be smooth, projective, absolutely irreducible curve over $\mathbb{F}_q$.

(alternatively $F/\mathbb{F}_q$ an algebraic function field with full constant field $\mathbb{F}_q$)

$\mathcal{C}(\mathbb{F}_q)$ set of rational points of $\mathcal{C}$.

$$\#\mathcal{C}(\mathbb{F}_q) \text{ is finite}$$

$$\#\mathcal{C}(\mathbb{F}_q) = ?$$

The Hasse–Weil bound

$\mathcal{C} \longrightarrow \zeta_{\mathcal{C}}$ Zeta function of $\mathcal{C}$

Theorem (Hasse–Weil)

The Riemann hypothesis holds for $\zeta_{\mathcal{C}}$.

Corollary (Hasse–Weil bound)

Let $\mathcal{C}/\mathbb{F}_q$ be a curve of genus $g(\mathcal{C})$. Then

$$\#\mathcal{C}(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q} \cdot g(\mathcal{C}).$$

How good is the Hasse–Weil bound?

Trivial improvement

$$\#\mathcal{C}(\mathbb{F}_q) \leq q + 1 + \lfloor 2\sqrt{q} \cdot g(\mathcal{C}) \rfloor.$$

Theorem (Serre)

$$\#\mathcal{C}(\mathbb{F}_q) \leq q + 1 + g(\mathcal{C}) \cdot \lfloor 2\sqrt{q} \rfloor.$$

If the genus $g(\mathcal{C})$ is small (with respect to q) $\longrightarrow$ Hasse–Weil bound is good.
It can be attained, *maximal curves*, for example over $\mathbb{F}_{q^2}$

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

Ihara, Manin: The Hasse–Weil bound can be improved if $g(\mathcal{C})$ is large (with respect to q).

Ihara's constant

Ihara:

$$A(q) = \limsup_{g(\mathcal{C})\to\infty} \frac{\#\mathcal{C}(\mathbb{F}_q)}{g(\mathcal{C})}$$

$\mathcal{C}$ runs over all absolutely irreducible, smooth, projective curves over $\mathbb{F}_q$.

Hasse–Weil bound	$\Longrightarrow A(q) \leq 2\sqrt{q}$
Ihara	$\Longrightarrow A(q) \leq \frac{1}{2}(\sqrt{8q+1}-1) \leq \sqrt{2q} \leq 2\sqrt{q}$
Drinfeld–Vladut	$\Longrightarrow A(q) \leq \sqrt{q}-1$

Lower bounds for $A(q)$

Serre (using class field towers):

$$A(q) > 0$$

Ihara, Tsfasman–Vladut–Zink (modular curves):
If $q = \ell^2$ then

$$A(\ell^2) \geq \sqrt{q} - 1 = \ell - 1$$

In fact $A(\ell^2) = \ell - 1$.

Zink (Shimura surfaces):
If $q = p^3$, p a prime number, then

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

(generalized by Bezerra–Garcia–Stichtenoth to all cubic finite fields)

$A(q)$ for non-prime q

B.–Beelen–Garcia–Stichtenoth
ℓ prime power, $n \geq 2$, $q = \ell^n$

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

- $n = 2$: $\ell - 1 \to$ Drinfeld-Vladut bound
- $n = 3$: $\frac{2(\ell^2-1)}{\ell+2} \to$ Zink's bound

ℓ prime power, $n = 2k+1 \geq 3$, $q = \ell^n$

$$A(\ell^{2k+1}) \geq \frac{2}{\frac{1}{\ell^k - 1} + \frac{1}{\ell^{k+1} - 1}} \geq \frac{2(\ell^{k+1} - 1)}{\ell + 1 + \epsilon}$$

with

$$\epsilon = \frac{\ell - 1}{\ell^k - 1}.$$

Note:

$$\ell^{k+\frac{1}{2}} - 1 \geq A(\ell^{2k+1}) \geq \frac{2}{\frac{1}{\ell^k - 1} + \frac{1}{\ell^{k+1} - 1}}.$$

$2^{15} \quad (2^3)^5 \quad (2^5)^3$

$q = 2^k$,k large,

$$\frac{\text{lower bound}}{\sqrt{q} - 1} \approx 94\%$$

How to obtain lower bounds for $A(q)$?

Find sequences $\mathcal{F} = (\mathcal{C}_i)_{i \geq 0}$ with $\mathcal{C}_i / \mathbb{F}_q$ and $g(\mathcal{C}_i) \to \infty$ such that

$$\lambda(\mathcal{F}) = \lim_{i \to \infty} \frac{\#\mathcal{C}_i(F_q)}{g(\mathcal{C}_i)} \text{ is large.}$$

since

$$0 < \lambda(\mathcal{F}) \leq A(q) \leq \sqrt{q} - 1$$

$$\lambda(\mathcal{F}) : \text{limit of } \mathcal{F} = (\mathcal{C}_i)_{i \geq 0}.$$

How to construct good sequences

Various approaches:

- Class field towers (over prime fields)
- Modular curves (Elliptic, Shimura, Drinfeld) (over $\mathbb{F}_{q^2}$)
- Explicit equations (recursively defined)

Modular towers

$X_0(N)/\mathbb{Q}$ modular curve parametrizing elliptic curves with a cyclic N-isogeny.

Good reduction at primes $p \nmid N$.

$g(X_0(N))$ are known (formula).

$X_0(N)/\mathbb{F}_{p^2}$ has many $\mathbb{F}_{p^2}$-rational points (why?).

Supersingular points

Fact: E/k supersingular $\longrightarrow j(E) \in \mathbb{F}_{p^2}$,
where p is the characteristic of k.

isomorphism classes of supersingular elliptic curves give rise to $\mathbb{F}_{p^2}$-rational points on $X_0(N)/k$

Fix a prime p.
$(N_i)_{i\geq 0}$ with $N_i \to \infty$, $p \nmid N_i$.

$$C_{N_i} = (X_0(N_i) \pmod{p})$$

- $\#C_{N_i}(\mathbb{F}_{p^2})$ is large (supersingular points)
- $g(C_{N_i})$ can be calculated

$$\frac{\#C_{N_i}(\mathbb{F}_{p^2})}{g(C_{N_i})} \to \sqrt{p^2} - 1 = p - 1 \quad \text{(Drinfeld-Vladut bound)}$$

Recursively defined towers

Fix $f(U,V) \in \mathbb{F}_q[U,V]$.
Let $\mathcal{C}_n$ be the curve defined by

$$f(x_0, x_1) = 0$$

$$f(x_1, x_2) = 0$$

$$\cdots$$

$$f(x_{n-1}, x_n) = 0$$

$\mathcal{F} = (\mathcal{C}_n)_{n \geq 1}$ tower recursively defined by f.
We obtain a covering of curves

$$\cdots \to \mathcal{C}_{n+1} \to \mathcal{C}_n \to \cdots \to \mathcal{C}_1 \to \mathcal{C}_0 = \mathbb{P}^1.$$

Example

There are several examples of recursively defined towers, with large limit (even optimal).
Garcia–Stichtenoth, 1996, Norm-Trace tower
$q = \ell^2$

$$V^\ell + V = \frac{U^{\ell+1}}{U^\ell + U}$$

$$\lambda = \sqrt{q} - 1$$

Attains the Drinfeld–Vladut bound.
Genus computation is difficult (wild ramification)
Why many rational points?

$$q = \ell^2 \qquad V^\ell + V = \frac{U^{\ell+1}}{U^\ell + U}$$

$$X_n^\ell + X_n = \frac{X_{n-1}^{\ell+1}}{X_{n-1}^\ell + X_{n-1}}, \ldots, X_3^\ell + X_3 = \frac{X_2^{\ell+1}}{X_2^\ell + X_2},\ X_2^\ell + X_2 = \frac{X_1^{\ell+1}}{X_1^\ell + X_1}$$

$$X_1 = a_1 \in \mathbb{F}_q \text{ s.t. } Tr_{\mathbb{F}_q/\mathbb{F}_\ell}(a_1) \neq 0$$

$$(\ell^2 - \ell \text{ choices})$$

$$X_2 = a_2 \text{ with } a_2^\ell + a_2 = \frac{a_1^{\ell+1}}{a_1^\ell + a_1} \in \mathbb{F}_\ell \backslash \{0\}$$

$$\ell \text{ choices with } a_2 \in \mathbb{F}_q,\ Tr_{\mathbb{F}_q/\mathbb{F}_\ell}(a_2) \neq 0)$$

$$X_3 = a_3 \text{ with } a_3^\ell + a_3 = \frac{a_2^{\ell+1}}{a_2^\ell + a_2} \in \mathbb{F}_\ell \backslash \{0\}$$

$$\ell \text{ choices with } a_3 \in \mathbb{F}_q,\ Tr_{\mathbb{F}_q/\mathbb{F}_\ell}(a_3) \neq 0)$$

$\cdots\ \cdots$ so $\#\mathcal{C}_n(\mathbb{F}_q) \geq (\ell^2 - \ell)\ell^{n-1}$

Elkies has shown that all known optimal recursive towers are modular (Elliptic, Shimura, Drinfeld).

Elkies: Fix s. The sequence $X_0(s^k)$ is recursively defined.

A point $z \in Y_0(s^k) = X_0(s^k) - \{\text{cusps}\}$ represents an equivalence class of

- the pairs (E, C_{s^k}) of elliptic curve E and cyclic subgroup C_{s^k} of order s^k.
- isogenies $E \to E/C_{s^k}$

C_{s^k} is cyclic, so it has a unique filtration of the form

$$C_{s^k} \supset C_{s^{k-1}} \supset \cdots \supset C_s \supset \{e\}$$

In terms of isogenies:

$$E_0 = E \to E_1 = E/C_s \to \cdots \to E_k = E/C_{s^k}.$$

For $i = 0, 1, \ldots, k-1$, E_i and E_{i+1} are related by a cyclic s-isogeny. So

$$\Phi_s(j(E_i), j(E_{i+1})) = 0,$$

where $\Phi_s(U, V)$ is the modular polynomial of level s.

So we iterate the correspondence

$$\begin{tikzcd}
 & X_0(s) \arrow[dl] \arrow[dr] & \\
X(1) & & X(1)
\end{tikzcd}$$

$$\begin{tikzcd}
 & X_0(s^2) \arrow[dl] \arrow[dr] & & \\
X_0(s) \arrow[dl] \arrow[dr] & & X_0(s) \arrow[dl] \arrow[dr] & \\
X(1) & X(1) & & X(1)
\end{tikzcd}$$

Drinfeld Modular Varieties

$$
\begin{array}{ccc}
 & & C_\infty \\
 & & | \\
\mathbb{C} & & \bar{k}_\infty \\
| & & | \\
\mathbb{R} & & k_\infty \\
| & & | \\
\mathbb{Q} & & \mathbb{F}_\ell(T) \\
| & & | \\
\mathbb{Z} & & \mathbb{F}_\ell[T]
\end{array}
$$

$\mathbb{Z}$-lattices inside $\mathbb{C}$ $\quad\rightarrow$ rank 1 or 2

$\mathbb{F}_\ell[T]$-lattices inside C_∞ $\quad\rightarrow$ arbitrary high rank possible

Drinfeld Modular Curves

$A = \mathbb{F}_\ell[T]$, P a prime of A,

$$\mathbb{F}_P = A/ < P >= \mathbb{F}_{\ell^d}$$

where $d = \deg P$.
$\mathbb{F}_P^{(2)}$: The unique quadratic extension of $\mathbb{F}_P$.
For $N \in \mathbb{F}_\ell[T]$ we have

$$X_0(N)$$

an algebraic curve defined over $\mathbb{F}_\ell(T)$, Drinfeld modular curve, parametrizing rank 2 Drinfeld modules together with a cyclic N-isogeny.
$X_0(N)$ has good reduction at all primes $P \nmid N$.

$$X_0(N)/\mathbb{F}_P$$

Many points on Drinfeld modular curves

$X_0(N)/\mathbb{F}_P$ has many rational points over $\mathbb{F}_P^{(2)} = \mathbb{F}_{\ell^{2d}}$, where $d = \deg P$. Asymptotically:

Theorem (Gekeler)

$P \in \mathbb{F}_\ell[T]$ prime of degree d
$(N_k)_{k \geq 0}$: sequence of polynomials in $\mathbb{F}_\ell[T]$ with

- $P \nmid N_k$
- $\deg N_k \to \infty$

Then the sequence of curves

$$X_0(N_k)/\mathbb{F}_P$$

attains the Drinfeld–Vladut bound over $\mathbb{F}_P^{(2)} = \mathbb{F}_{\ell^{2d}}$.

Elkies: $X_0(Q^n)$ recursive.
Norm trace tower is related to (degree $\ell - 1$ cover of)

$$X_0(T^n)/\mathbb{F}_{T-1}$$

elliptic modular curves $\to$ Shimura curves
Drinfeld modular curves $\to$ modular curves of $\mathcal{D}$-elliptic sheaves

Papikian has shown that modular curves of $\mathcal{D}$-elliptic sheaves attain the Drinfeld–Vladut bound.

Many points over non-quadratic fields

Many points come from the supersingular points

$$\longrightarrow \text{defined over } \mathbb{F}_P^{(2)}.$$

In general:

Theorem (Gekeler)

Any supersingular Drinfeld module ϕ of rank r and characteristic P is isomorphic to one defined over L, where L is an extension $\mathbb{F}_P^{(r)}$ of $\mathbb{F}_P$ of degree r.

Idea: Look at space parametrizing rank r Drinfeld modules
Problem: The corresponding space is higher dimensional ($(r-1)$-dimensional), not a curve!
Idea': Look at curves on those spaces, passing through the many $\mathbb{F}_P^{(r)}$-rational points.

Let ϕ be a normalized rank n Drinfeld Module of characteristic $T-1$.

$$\phi_T = \tau^n + g_1\tau^{n-1} + g_2\tau^{n-2} + \cdots + g_{n-1}\tau + 1.$$

ϕ is supersingular if ϕ_{T-1} is a purely inseparable map of degree ℓ^n, i.e.,

$$\phi_{T-1} = \tau^n, \text{ i.e.,}$$

$$g_1 = g_2 = \cdots = g_{n-1} = 0.$$

We want a

- one dimensional sublocus,
- passing through $g_1 = g_2 = \cdots = g_{n-1} = 0$
- invariant under isogenies (to obtain a recursive tower)

We call ϕ weakly supersingular, if ϕ_{T-1} is a map of inseparability at least ℓ^{n-1}, i.e.,

$$\phi_{T-1} = \tau^n + g_1\tau^{n-1}, \text{ i.e.,}$$

$$g_2 = \cdots = g_{n-1} = 0.$$

Note that the property of being weakly supersingular is invariant under isogenies!
Look at the space of weakly supersingular normalized Drinfeld modes.

Isogenies

Let $\lambda : \phi \to \psi$ be an isogeny of the form

$$\tau - u$$

whose kernel is annihilated by T.
$\exists \mu = \tau^{n-1} + a_2\tau^{n-2} + \cdots + a_{n-1}\tau + a_n$, s.t.

$$\mu \cdot \lambda = \phi_T$$

Then

$$N_n(u) + g_1 \cdot N_{n-1}(u) + 1 = 0$$

Notation: $N_k(x) = x^{1+\ell+\cdots+\ell^{k-2}+\ell^{k-1}}$

Equations for the isogenous Drinfeld module

$\lambda : \phi \to \psi$

$$\psi_T = \tau^n + h_1 \cdot \tau^{n-1} + 1$$

Isogeny: $\lambda \cdot \phi = \psi \cdot \lambda$

$$(\tau - u) \cdot (\tau^n + g_1 \tau^{n-1} + 1) = (\tau^n + h_1 \tau^{n-1} + 1) \cdot (\tau - u)$$

$$g_1^\ell - u = h_1 - u^{\ell^n}$$

$$-ug_1 = -h_1 u^{\ell^{n-1}}$$

$$-g_1 = \frac{N_n(1/u) + 1}{(1/u)^{\ell^{n-1}}},$$

$$-h_1 = \frac{N_n(1/u) + 1}{1/u}$$

Letting $v_0 = 1/u$

$$\begin{tikzcd}
 & \mathbb{F}_q(v_0) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{F}_q(g_1) & & \mathbb{F}_q(h_1)
\end{tikzcd}$$

$$\frac{N_n(V)+1}{V^{\ell^{n-1}}} = \frac{N_n(U)+1}{U}.$$

A new family of towers over all non-prime fields

B.–Beelen–Garcia–Stichtenoth
$\mathcal{F}_5$ over $\mathbb{F}_{\ell^n}$, $n \geq 2$:

Notation: $Tr_n(t) = t + t^{\ell} + \cdots + t^{\ell^{n-1}}$, $N_n(t) = t^{1+\ell+\ell^2+\ldots+\ell^{n-1}}$

$$\frac{N_n(V)+1}{V^{\ell^{n-1}}} = \frac{N_n(U)+1}{U}.$$

Splitting: $N_n(\alpha) = -1$

$$\lambda(\mathcal{F}_5) \geq \frac{2}{\frac{1}{\ell-1} + \frac{1}{\ell^{n-1}-1}}$$

- $n = 2$: $\ell - 1 \to$ Drinfeld-Vladut bound
- $n = 3$: $\frac{2(\ell^2-1)}{\ell+2} \to$ Zink's bound

$\mathcal{F}_6/\mathbb{F}_q,\ q = \ell^n,\ n = 2k+1 \geq 3$

$$\frac{Tr_k(V) - 1}{(Tr_{k+1}(V) - 1)^{\ell^k}} = \frac{(Tr_k(U) - 1)^{\ell^{k+1}}}{(Tr_{k+1}(U) - 1)}$$

$$\frac{V^{\ell^n} - V}{V^{\ell^k}} = -\frac{(1/U)^{\ell^n} - (1/U)}{U^{\ell^{k+1}}}$$

$\mathcal{F}_6/\mathbb{F}_q,\ q=\ell^n,\ n=2k+1$

$$\lambda(\mathcal{F}_6) \geq \frac{2}{\frac{1}{\ell^k-1}+\frac{1}{\ell^{k+1}-1}} \geq \frac{2(\ell^{k+1}-1)}{\ell+1+\epsilon}$$

with

$$\epsilon = \frac{\ell-1}{\ell^k-1}.$$

Note:

$$\ell^{k+\frac{1}{2}}-1 \geq A(\ell^{2k+1}) \geq \frac{2}{\frac{1}{\ell^k-1}+\frac{1}{\ell^{k+1}-1}}.$$

$2^{15} \quad (2^3)^5 \quad (2^5)^3$
$q=2^k$,k large,

$$\frac{\lambda(\mathcal{F}_5)}{\sqrt{q}-1} \approx 94\%$$