Rational points on curves over finite fields and Drinfeld modular varieties

Alp Bassa

Sabancı University
Curves over Finite Fields

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

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

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

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

$\#C(\mathbb{F}_q) = ?$
The Hasse–Weil bound

$C \longrightarrow \zeta_C$  Zeta function of $C$

Theorem (Hasse–Weil)
The Riemann hypothesis holds for $\zeta_C$.

Corollary (Hasse–Weil bound)
Let $C/\mathbb{F}_q$ be a curve of genus $g(C)$. Then

$$\#C(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q} \cdot g(C).$$
How good is the Hasse–Weil bound?

**Trivial improvement**

\[ \#C(\mathbb{F}_q) \leq q + 1 + \lceil 2\sqrt{q} \cdot g(C) \rceil. \]

**Theorem (Serre)**

\[ \#C(\mathbb{F}_q) \leq q + 1 + g(C) \cdot \lceil 2\sqrt{q} \rceil. \]

If the genus \( g(C) \) is small (with respect to \( q \)) \( \rightarrow \) 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 \( g(C) \) is large (with respect to \( q \)).
Ihara’s constant

Ihara:

\[ A(q) = \limsup_{g(C) \to \infty} \frac{\#C(F_q)}{g(C)} \]

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

Hasse–Weil bound \( \implies A(q) \leq 2\sqrt{q} \)

Ihara \( \implies A(q) \leq \frac{1}{2}(\sqrt{8q + 1} - 1) \leq \sqrt{2q} \leq 2\sqrt{q} \)

Drinfeld–Vladut \( \implies A(q) \leq \sqrt{q} - 1 \)
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, \( n \geq 2, q = ℓ^n \)

\[
A(ℓ^n) \geq \frac{2}{\frac{1}{ℓ-1} + \frac{1}{ℓ^{n-1}-1}}
\]

- \( n = 2 \): \( ℓ - 1 \rightarrow \) Drinfeld-Vladut bound
- \( n = 3 \): \( \frac{2(ℓ^2-1)}{ℓ+2} \rightarrow \) Zink’s bound
\( \ell \) 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:

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

\[
2^{15} \ (2^3)^5 \ (2^5)^3
\]

\( q = 2^k, k \) large,

\[
\frac{\text{lower bound}}{\sqrt{q - 1}} \approx 94\%
\]
How to obtain lower bounds for $A(q)$?

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

$$\lambda(\mathcal{F}) = \lim_{i \to \infty} \frac{\#C_i(F_q)}{g(C_i)}$$

is large.

since

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

$\lambda(\mathcal{F})$ : limit of $\mathcal{F} = (C_i)_{i \geq 0}$. 
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 \( C_n \) be the curve defined by

\[
\begin{align*}
  f(x_0, x_1) &= 0 \\
  f(x_1, x_2) &= 0 \\
  \vdots \\
  f(x_{n-1}, x_n) &= 0
\end{align*}
\]

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

\[
\cdots \to C_{n+1} \to C_n \to \cdots \to C_1 \to C_0 = \mathbb{P}^1.
\]
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?
\[ q = \ell^2 \quad V^\ell + V = \frac{U^{\ell+1}}{U^\ell + U} \]

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

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

\[ (\ell^2 - \ell \text{ choices}) \]

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

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

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

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

\[ \cdots \cdots \text{ so } \# C_n(\mathbb{F}_q) \geq (\ell^2 - \ell)\ell^{n-1} \]
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 $E \to E/C_{s^k}$
$C_{sk}$ is cyclic, so it has a unique filtration of the form

$$C_{sk} \supset C_{sk-1} \supset \cdots \supset C_s \supset \{e\}$$

In terms of isogenies:

$$E_0 = E \to E_1 = E/C_s \to \cdots \to E_k = E/C_{sk}.$$ 

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

\[ X_0(s) \]
\[ \downarrow \quad \downarrow \]
\[ X(1) \quad X(1) \]

\[ X_0(s^2) \]
\[ \downarrow \quad \downarrow \]
\[ X_0(s) \quad X_0(s) \]
\[ \downarrow \quad \downarrow \quad \downarrow \]
\[ X(1) \quad X(1) \quad X(1) \]
Drinfeld Modular Varieties

- $C_\infty$
- $\bar{k}_\infty$
- $k_\infty$
- $\mathbb{F}_\ell(T)$
- $\mathbb{F}_\ell[T]$

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

$\mathbb{F}_\ell[T]$-lattices inside $C_\infty$ \rightarrow arbitrary high rank possible
Drinfeld Modular Curves

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

\[ \mathbb{F}_P = A/ \langle P \rangle = \mathbb{F}_{\ell^d} \]

where \( d = \text{deg} \ P. \)

\( \mathbb{F}_P^{(2)}: \) 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 $\rightarrow$ Shimura curves
Drinfeld modular curves $\rightarrow$ 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 $\rightarrow$ defined over $\mathbb{F}_p^{(2)}$.

In general:

**Theorem (Gekeler)**

Any supersingular Drinfeld module $\phi$ 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 $\phi$ be a normalized rank $n$ Drinfeld Module of characteristic $T - 1$.

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

$\phi$ is supersingular if $\phi_{T-1}$ is a purely inseparable map of degree $\ell^n$, i.e.,

$$\phi_{T-1} = \tau^n,$$

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 $\phi$ weakly supersingular, if $\phi_{T-1}$ is a map of inseparability at least $\ell^{n-1}$, i.e.,

$$\phi_{T-1} = \tau^n + g_1 \tau^{n-1},$$

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

$$\tau - u$$

whose kernel is annihilated by $T$.

$$\exists \mu = \tau^{n-1} + a_2\tau^{n-2} + \cdots + a_{n-1}\tau + a_n, \text{ s.t.}$$

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

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: \( \lambda \cdot \phi = \psi \cdot \lambda \)

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

\[ g_1^\ell - u = h_1 - u^{\ell n} \]

\[ -ug_1 = -h_1 u^{\ell n-1} \]
\[-g_1 = \frac{N_n(1/u) + 1}{(1/u)^{\ell^u n^{-1}}} , \]
\[-h_1 = \frac{N_n(1/u) + 1}{1/u} \]

Letting \( v_0 = 1/u \)

\[
\mathbb{F}_q(v_0)
\]

\[
\begin{array}{c}
\mathbb{F}_q(g_1) \\
\mathbb{F}_q(h_1)
\end{array}
\]
\[
\frac{N_n(V) + 1}{V^{\ell n^{-1}}} = \frac{N_n(U) + 1}{U}.
\]
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: $Tr_n(t) = t + t^{\ell} + \cdots + t^{\ell^{n-1}}$, $N_n(t) = t^{1+\ell+\ell^2+\cdots+\ell^{n-1}}$

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

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

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

- $n = 2$: $\ell - 1 \rightarrow$ Drinfeld-Vladut bound
- $n = 3$: $\frac{2(\ell^2-1)}{\ell+2} \rightarrow$ Zink’s bound
$\mathcal{F}_6/\mathbb{F}_q$, $q = \ell^n$, $n = 2k + 1 \geq 3$

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

\[
\frac{V^{\ell^n} - V}{V^{\ell^k}} = -\frac{(1/U)^{\ell^n} - (1/U)}{U^{\ell^{k+1}}}
\]
\( \mathcal{F}_6 / \mathbb{F}_q, \ q = \ell^n, \ n = 2k + 1 \)

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

with

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

Note:

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

\[2^{15} \quad (2^3)^5 \quad (2^5)^3\]

\(q = 2^k, k \) large,

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