Explicit points on Jacobians of superelliptic curves over global function fields

Lisa Berger, Chris Hall, René Pannekoek,
Jennifer Park, Rachel Pries, Shahed Sharif,
Alice Silverberg, Douglas Ulmer

Lausanne Workshop
November 15, 2012

Thanks to an AIM Workshop

This work was initiated at an AIM (American Institute of Mathematics) workshop on *Cohomological methods in abelian varieties* in Palo Alto, March 26–30, 2012.

Some Background

Ranks of elliptic curves over $\mathbb{F}_q(t)$ are unbounded.

- Tate & Shafarevich (1967): isotrivial
- Ulmer (2002): non-isotrivial

Some Background

Theorem (Ulmer, 2007)

For all $g > 0$, all primes p, and all R, there exist absolutely simple non-isotrivial abelian varieties of dimension g over $\mathbb{F}_p(t)$ with

$$\textit{analytic rank} = \textit{algebraic rank} > R.$$

Ulmer Example (2007)

If $p \nmid (2g+2)(2g+1)$, then the Jacobian of

$$y^2 = x^{2g+2} + x^{2g+1} + t^{p^n+1}$$

over $\mathbb{F}_p(t)$ is absolutely simple, non-isotrivial, and has rank $\geq p^n/2n$.

In particular, the Jacobian of

$$y^2 = x^{2g+2} + x^{2g+1} + t$$

has unbounded rank in the tower $\{\mathbb{F}_p(t^{1/d})\}$.

Some Background

Theorem (Ulmer (2007))

Roughly half the abelian varieties over $\mathbb{F}_q(t)$ have unbounded analytic rank in the tower

$$\{\mathbb{F}_q(t^{1/d})\}_{\gcd(d,q)=1}.$$

Ulmer's results gave families of abelian varieties of fixed dimension and unbounded (analytic and algebraic) rank over $\mathbb{F}_q(t)$, but didn't give explicit points.

Ulmer's *Legendre curve* paper

In Ulmer's preprint

Explicit points on the Legendre curve

he obtained high rank and explicit points on

$$y^2 = x(x+1)(x+t).$$

Our work

We generalize Ulmer's work to Jacobians of superelliptic curves of higher genus.

For a certain family, our goal is to determine as much as we can about the arithmetic, such as rank, torsion, explicit points, and BSD.

In particular, we obtain large rank.

BSD

Consider

$$C : y^r = x^{r-1}(x+1)(x+t)$$

over $\mathbb{F}_p(t)$ with p an odd prime, $p \nmid r$ ($r = 2$ is Ulmer's Legendre case). Then C has genus $r-1$. Let $J = \mathrm{Jac}(C)$. Note that

$$\mathbb{Z}[\zeta_r] \hookrightarrow \mathrm{End}(J)$$

via $\zeta_r \mapsto [(x, y) \mapsto (x, \zeta_r y)]$.

Theorem 1

The full Conjecture of Birch and Swinnerton-Dyer holds for J over $\mathbb{F}_q(t^{1/d})$, for all d and for all $q = p^a$.

Rank

For the remaining results, suppose that r is a prime divisor of d and $d = p^f + 1$ for some f. Take $q = p^a$ and let

$$K_d = \mathbb{F}_q(\boldsymbol{\mu}_d, t^{1/d}).$$

Theorem 2

$$rank_{\mathbb{Z}} J(K_d) = (r-1)(d-2)$$

Explicit Points

Let $u = t^{1/d}$, let $P_{0,0} := (u, u(u+1)^{d/r})$, and more generally let

$$P_{i,j} := (\zeta_d^i u, \zeta_d^{jd/r+i} u(\zeta_d^i u + 1)^{d/r}) \in C(K_d)$$

with i mod d and j mod r (giving dr points),

$$Q_\infty := \text{the point at infinity} \in C(K_d),$$

$$D_{i,j} := [P_{i,j}] - [Q_\infty] \in J(K_d).$$

Theorem 3

The $D_{i,j}$'s generate a subgroup of $J(K_d)$ of finite index.

Rank

Theorem 4

$$rank_{\mathbb{Z}} J(\mathbb{F}_q(t^{1/d})) = (r-1)\left[\sum_{e|d} \frac{\varphi(e)}{o_q(e)} - \frac{2}{o_q(r)}\right]$$

where

$$o_q(e) := \textit{the order of } q \textit{ in } (\mathbb{Z}/e\mathbb{Z})^*.$$

Rank

Therefore over (fixed) $\mathbb{F}_q(u)$, Jacobians of curves of genus $r-1$ have unbounded rank.

(This is for r and p such that $r \mid (p^f+1)$ for some f,
i.e., such that the order of p mod r is even,
i.e., $-1 \in \langle p \rangle \subset (\mathbb{Z}/r\mathbb{Z})^*$.
For each r, we get at least half the primes p.
Later we'll see a different example without this restriction.)

Torsion

Theorem 5

As $\mathbb{Z}[\zeta_r]$-modules,

$$J(K_d)_{\mathrm{tors}} \cong \mathbb{Z}[\zeta_r]/(\zeta_r - 1) \times \mathbb{Z}[\zeta_r]/(\zeta_r - 1)^2.$$

So as abelian groups,

$$J(K_d)_{\mathrm{tors}} \cong \begin{cases} (\mathbb{Z}/r\mathbb{Z})^3 & \text{if } r > 2, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \text{if } r = 2. \end{cases}$$

Decomposition and Endomorphisms

Theorem 6

If $r > 2$ *then*

$$J \sim B^2$$

where B *is an* $(r-1)/2$*-dimensional absolutely simple abelian variety with real multiplication by* $\mathbb{Q}(\zeta_r)^+$*.*

Theorem 7

If $r > 2$ *then*

$$\mathrm{End}(J) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathrm{M}_2(\mathbb{Q}(\zeta_r)^+)$$
$$\mathrm{End}_{\bar{\mathbb{F}}_q(t)}(J) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}(\zeta_r).$$

L-function

Theorem 8

$$L(J/\mathbb{F}_q(t), s) = 1,$$
$$L(J/K_d, s) = (1 - q_1^{1-s})^{(r-1)(d-2)}$$

where $q_1 = |\mathbb{F}_q(\boldsymbol{\mu}_d)|$, *i.e., with* $T = q_1^{-s}$ *we have*

$$L(T, J/K_d) = (1 - q_1 T)^{(r-1)(d-2)} \in \mathbb{Z}[T]$$

Ulmer's Legendre curve

The case $r = 2$ gives the Legendre curve. For that case, all these results were shown earlier by Ulmer.

We generalize his statements and proofs.

Conjecture of Birch & Swinnerton-Dyer

Conjecture (BSD I)

$$\mathit{rank}_{\mathbb{Z}} J(K) = \mathrm{ord}_{s=1} L(J, s)$$

Conjecture (BSD II)

As $s \to 1$,

$$L(J, s) \sim \frac{R|Ш|\tau}{|J(K)|^2_{\mathrm{tors}}}(s-1)^r$$

where r is the analytic rank, R is the regulator, Ш is the Tate-Shafarevich group, and τ is the Tamagawa number.

For function fields it's known that $\mathrm{rank}_{\mathbb{Z}} J(K) \leq \mathrm{ord}_{s=1} L(J, s)$ and that BSD I $\Longrightarrow$ BSD II, by Tate, Milne, ..., Kato, Trihan.

Sketch of Proof of BSD

Theorem 1

The full Conjecture of Birch and Swinnerton-Dyer holds for J over $\mathbb{F}_q(t^{1/d})$, for all d and for all $q = p^a$.

$$C \cong y^r = \frac{(x+1)(x+t)}{x}$$

Let

$$C_d : \beta^d = \alpha^r - 1,$$

$$D_d : \delta^{-d} = \gamma^r - 1.$$

Then

$$C_d \times D_d \dashrightarrow y^r = \frac{(x+1)(x+u^d)}{x}$$

$$(\alpha, \beta, \gamma, \delta) \mapsto (x, y, u) = (\alpha^r - 1, \alpha\gamma, \beta/\delta)$$

Sketch of Proof of BSD

Thus, the surface $y^r = (x+1)(x+u^d)/x$ over $\mathbb{F}_q$ is dominated by a product of curves $C_d \times D_d$.

The Tate Conjecture for the surface then follows, and this in turn implies (full) BSD for the Jacobian of the curve $y^r = (x+1)(x+u^d)/x$ over $\mathbb{F}_q(u)$, for all $q = p^a$.

This gives (full) BSD for J over $\mathbb{F}_q(t^{1/d})$, for all $q = p^a$ and all d.

Recall Theorems on Rank and Points

Recall: r is prime, $r \mid d = p^f + 1$ for some f, $q = p^a$, $K_d = \mathbb{F}_q(\boldsymbol{\mu}_d, t^{1/d})$, $u = t^{1/d}$.

Theorem 2

$$rank_{\mathbb{Z}} J(K_d) = (r-1)(d-2)$$

Theorem 3

The $D_{i,j}$'s generate a subgroup of $J(K_d)$ of finite index, where

$$D_{i,j} := [P_{i,j}] - [Q_\infty] \in J(K_d)$$

with

$$P_{i,j} := (\zeta_d^i u, \zeta_d^{jd/r+i} u(\zeta_d^i u + 1)^{d/r}) \in C(K_d)$$

(i mod d and j mod r).

Sketch of Proof of Theorems 2 and 3

We compute the dimension of the image of $\langle D_{i,j} \rangle$ under the $(\zeta_r - 1)$-descent map (Poonen-Schaefer's $(x - T)$ map):

$$
\begin{aligned}
(x - T) : J(K_d)/(\zeta_r - 1)J(K_d) &\hookrightarrow H^1(K_d, J[\zeta_r - 1]) \\
&\xrightarrow{\sim} \left[(K_d[T]/(T(T+1)(T+t)))^* \,/\, (\ldots)^r \right]_1 \\
&\xrightarrow{\sim} \left[(K_d^*/(K_d^*)^r)^3 \right]_1
\end{aligned}
$$

$$(x, y) \in C(K_d) \mapsto (x, x+1, x+t)$$

where $[\,\cdot\,]_1$ denotes the kernel of the weighted norm map

$$(x, y, z) \mapsto x^{r-1} yz = yz/x \in K_d^*/(K_d^*)^r.$$

Sketch of Proof of Theorems 2 and 3

$$\begin{aligned}\operatorname{rank}_{\mathbb{Z}[\zeta_r]} J(K_d) &= \\ &\dim_{\mathbb{F}_r} J(K_d)/(\zeta_r - 1) - \dim_{\mathbb{F}_r} J(K_d)_{\text{tors}}/(\zeta_r - 1) \\ &\qquad \geq \dim_{\mathbb{F}_r}((x - T)(\langle D_{i,j}\rangle)) - 2 = d - 2\end{aligned}$$

giving

$$\operatorname{rank}_{\mathbb{Z}} J(K_d) = (r-1)\operatorname{rank}_{\mathbb{Z}[\zeta_r]} J(K_d) \geq (r-1)(d-2).$$

Sketch of Proof of Theorems 2 and 3

Then

$$\begin{aligned}(r-1)(d-2) &\leq \text{rank} \\ &\leq (= \text{with BSD}) \text{ analytic rank} \\ &\leq \text{degree of } L\text{-function} \\ &= (r-1)(d-2)\end{aligned}$$

giving a different proof of BSD.

A sketch of the proof of the last equality is as follows:

Sketch of Proof of Theorems 2 and 3

Combining work of Ulmer, Milne, and others, one gets that the degree of the L-function is

$$-4\dim(J) + \deg(\mathrm{cond}(J[\ell]))$$

for any prime $\ell \nmid 2pr$, and

$$\mathrm{cond}(J[\ell]) = \sum_{x \in \mathbb{P}^1} (t_x + 2u_x)[x]$$

where t_x is the dimension of the toric part of the special fiber (over x) of the Néron model of J, and u_x is the dimension of the unipotent part.

Sketch of Proof of Theorems 2 and 3

We compute that the reduction of J at $u = 0$ and $u = \infty$ is totally multiplicative and the reduction at the d places $u^d = 1$ is half good and half additive. Thus,

$$\deg(\mathrm{cond}(J[\ell])) = \sum_{x \in \mathbb{P}^1} (t_x + 2u_x) =$$

$$(r-1) + (r-1) + d \cdot 2 \cdot \frac{r-1}{2} = (r-1)(d+2)$$

so

$$\deg(L\text{-function}) = -4\dim(J) + \deg(\mathrm{cond}(J[\ell])) =$$

$$-4(r-1) + (r-1)(d+2) = (r-1)(d-2).$$

Recall other Ranks Theorem

Theorem 4

$$rank_{\mathbb{Z}} J(\mathbb{F}_q(t^{1/d})) = (r-1)\left[\sum_{e|d} \frac{\varphi(e)}{o_q(e)} - \frac{2}{o_q(r)}\right]$$

where $o_q(e)$ is the order of q in $(\mathbb{Z}/e\mathbb{Z})^*$.

Sketch of Proof: We know how $\mathrm{Gal}(K_d/\mathbb{F}_q(t^{1/d}))$ acts on the $P_{i,j}$'s and we know all the relations among the $P_{i,j}$'s (from our rank calculations), so we can compute

$$\langle P_{i,j}\rangle^{\mathrm{Gal}(K_d/\mathbb{F}_q(t^{1/d}))}.$$

Recall Theorem on Torsion

Theorem 5

$$J(K_d)_{\mathrm{tors}} \cong \mathbb{Z}[\zeta_r]/(\zeta_r - 1) \times \mathbb{Z}[\zeta_r]/(\zeta_r - 1)^2$$

In particular,

$$J(K_d)_{\mathrm{tors}} = J(K_d)[r^\infty]$$

and

$$J(K_d)[\ell] = 0$$

for all primes $\ell \neq r$.

Sketch of Proof of Theorem 5

Let $Q_0 = (0,0)$, $Q_1 = (-1,0)$, $Q_t = (-t,0)$. Then $[Q_i] - [Q_\infty]$ are $(\zeta_r - 1)$-torsion points for $i = 0, 1, t$.

We found a divisor $D \in \langle D_{i,j} \rangle$ such that

$$(\zeta_r - 1)D \sim [Q_0] - [Q_\infty].$$

We show that the $\mathbb{F}_r$-dimension of the image of the known $(\zeta_r - 1)^\infty$-torsion under the $(\zeta_r - 1)$-descent map is 2; this shows we have all of it.

It's generated over $\mathbb{Z}[\zeta_r]$ by $[Q_1] - [Q_\infty]$ and D, so

$$J(K_d)[r] \cong \mathbb{Z}[\zeta_r]/(\zeta_r - 1) \times \mathbb{Z}[\zeta_r]/(\zeta_r - 1)^2.$$

Sketch of Proof of Theorem 5

To show

$$J(K_d)[\ell] = 0$$

for all $\ell \nmid 2pr$:

Use the geometry of the Néron model and group theory to understand the image of the mod ℓ representation

$$\mathrm{Gal}(\bar{\mathbb{F}}_q(t)(J[\ell])/\bar{\mathbb{F}}_q(t)) \hookrightarrow \mathrm{GL}_{2(r-1)}(\mathbb{F}_\ell).$$

We show $J(L)[\ell] = 0$ for all solvable extensions L of $\bar{\mathbb{F}}_q(t)$.

Sketch of Proof of Theorem 5

To show

$$J(K_d)[p] = 0 :$$

We show that J is ordinary, i.e.,

$$\#J(\overline{\mathbb{F}_q(t)})[p] = p^{r-1},$$

and calculate the Kodaira-Spencer map to show that

$$J(\mathbb{F}_p(t)^{sep})[p] = 0.$$

Sketch of Proof of Theorem 5

To show

$$J(K_d)[2] = 0:$$

Use that C is isomorphic to the hyperelliptic curve

$$\begin{aligned} y^2 &= x^{2r} - 2(t+1)x^r + t^2 - 2t + 1 \\ &= (x^r - (u^{d/2}+1)^2)(x^r - (u^{d/2}-1)^2) \end{aligned}$$

and apply a 2001 paper of Cornelissen, *Two-torsion in the Jacobian of hyperelliptic curves over finite fields*.

Decomposition and Endomorphisms

For $r > 2$:

Theorem 6

$J \sim B^2$ where B is an $(r-1)/2$-dimensional absolutely simple abelian variety with real multiplication by $\mathbb{Q}(\zeta_r)^+$.

Theorem 7

$$\mathrm{End}(J) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathrm{M}_2(\mathbb{Q}(\zeta_r)^+)$$
$$\mathrm{End}_{\bar{\mathbb{F}}_q(t)}(J) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}(\zeta_r).$$

Decomposition and Endomorphisms

We decompose

$$J \sim \ker(\sigma - 1) \times \operatorname{im}(\sigma - 1) \sim B^2$$

for the involution

$$\sigma : (x, y) \mapsto (-1 - \frac{v^r}{x+1}, \frac{v^2}{y})$$

where $v^r = t - 1$, and use group theory to show that B is absolutely simple and has endomorphism algebra $\mathbb{Q}(\zeta_r)^+$.

The isogeny, and all endomorphisms, are defined over $\mathbb{F}_q(\boldsymbol{\mu}_r, v) = \mathbb{F}_q(\zeta_r, (t-1)^{1/r})$.

L-function

Theorem 8

$$L(J/\mathbb{F}_q(t), s) = 1,$$
$$L(T, J/K_d) = (1 - q_1 T)^{(r-1)(d-2)} \in \mathbb{Z}[T],$$
$$L(J/K_d, s) = (1 - q_1^{1-s})^{(r-1)(d-2)}$$

where $q_1 = |\mathbb{F}_q(\mu_d)|$.

This follows since we showed that

$$\deg(L(T, J/K_d)) = (r-1)(d-2)$$
$$= \mathrm{rank}_{\mathbb{Z}} J(K_d) = \text{analytic rank}$$

and we can similarly show that $\deg(L(T, J/\mathbb{F}_q(t))) = 0$.

Another Example

We started with:

$$y^2 = x \prod_{i=1}^{g} (x + a_i)(a_i x + t)$$

or more generally

$$C : y^2 = xh(x) x^g h(t/x)$$

where the genus g is odd, $h(x) \in \mathbb{F}_q[x]$ has degree g and distinct roots, $h(0) \neq 0$, $q = p^a$ with p an odd prime.
Let

$$J = \mathrm{Jac}(C).$$

Another Example

If

- $d = p^f + 1$ for some f,
- h splits completely over $\mathbb{F}_q(\boldsymbol{\mu}_d, t^{1/d})$, and
- $u^d = t$,

then

$$(\zeta_d^i u, (\zeta_d^i u)^{\frac{g+1}{2}} h(\zeta_d^i u)^{d/2}) \in C(K_d).$$

Another Example

We computed the image of the points we know, under the 2-descent map:

$$J(K_d)/2J(K_d) \hookrightarrow H^1(K_d, J[2]) \cong \left[\left(K_d[T]/(h(T)h(t/T)T^{g+1})\right)^* /(\ldots)^2\right]_1$$

$$D \mapsto [\sigma \mapsto \sigma(D_1) - D_1] \text{ where } 2D_1 \sim D$$

$$\begin{aligned}\dim_{\mathbb{F}_2}(\text{image}) &\leq \dim_{\mathbb{F}_2}(J(K_d)/2J(K_d)) \\ &= \operatorname{rank} J(K_d) + \dim_{\mathbb{F}_2}(J(K_d)[2])\end{aligned}$$

We showed

$$\operatorname{rank} J(K_d) \geq d - 2.$$

Another Example

This gives unbounded rank over $\mathbb{F}_p(t)$ for all primes p, for dimension g abelian varieties.

But the degree of the L-function is large compared to $d - 2$, so the rank might be a lot larger than $d - 2$.

That's why we decided to consider a different example.

Possible Future Work

- Compute the regulator of the subgroup generated by the known points.
- Compute the index (in the full Mordell-Weil group) of the points we know.
- Compute other BSD data, such as Ш. (A full $(\zeta_r - 1)$-descent would give $|\text{Ш}[\zeta_r - 1]|$).

Explicit points on Jacobians of superelliptic curves over global function fields

Lisa Berger, Chris Hall, René Pannekoek,
Jennifer Park, Rachel Pries, Shahed Sharif,
Alice Silverberg, Douglas Ulmer

Lausanne Workshop
November 15, 2012