Explicit generating sets of Jacobians of curves over finite fields

Banff

February 10, 2007

Hannes Grund
Florian Hess

Technical University Berlin

Introduction

Let C be a complete geometrically irreducible curve over $\mathbb{F}_q$ of genus g and J its Jacobian.

Assume there is $Q \in C(\mathbb{F}_q)$ and let $C \to J$ with respect to Q.

We are interested in explicitly describeable subsets of $C(\mathbb{F}_q)$ whose images generate $J(\mathbb{F}_q)$, in the asymptotics $q \to \infty$ and g constant.

Uses a combination of well-known techniques, generalises work of Kohel and Shparlinski.

Observations

Have $\#C(\mathbb{F}_q) \sim q$ and $\#J(\mathbb{F}_q) \sim q^g$.

Upper bound for cardinality of minimal generating sets:

- $O(\log(q^g))$, for general groups.
- $O(g)$, observing group structure of $J(\mathbb{F}_q)$.

Theorem (Erdös, Renyi).

Let G be an abelian group and $n = \#G$. Choose k elements $a_1, \ldots, a_k$ from G uniformly and independently at random.
If $k \geq \log_2(n) + 2\log(\log(n))$, then $G = \{\sum_{i=1}^k \lambda_i a_i \mid \lambda_i \in \{0,1\}\}$ with probability tending to 1 for $n \to \infty$.

Cannot apply this to $C(\mathbb{F}_q)$, unless $C(\mathbb{F}_q)$ ”sufficiently random” in $J(\mathbb{F}_q)$.

Explicit generating sets

Let B be a subgroup of $\mathbb{F}_q^+$ and $\alpha \in \mathbb{F}_q$. Let $I = \cup_{i=r}^{s}(B + \alpha i)$ for $r, s \geq 0$.

Let $f \in \mathbb{F}_q(C)^\times$ be a function with at least one pole order not divisible by p, where $p^n = q$. Such f exists with $\deg(f) = O(g)$.

Let $S = \text{supp}((f)_\infty)$ and $T = \{P \in C(\mathbb{F}_q) \backslash S \mid f(P) \in I\}$.

Theorem 1.

If $\#I = \theta^\sim(q^{1/2})$ for $q \to \infty$ and $g = O(1)$ then:

- $\#T = O^\sim(q^{1/2})$,
- T generates $J(\mathbb{F}_q)$,
- T contains a generator for every cyclic factor group of $J(\mathbb{F}_q)$.

Discussion

Possible motivation:

- Obtain deterministic algorithms.
- Useful for some statements about pseudo-random number generators.

Case $q = O(1)$ and $g \to \infty$:

- Then use closed points up to degree $O(\log_q(g))$, yields generating set of size polynomial in $\log(q)$ and g.

Comparison with finite fields:

- Can find generating sets of size $O(q^{1/4})$.
- Can find polynomial size generating sets if $p = O(1)$.

Incomplete character sums

With the notation from before, Theorem 1 is a corollary of the following theorem.

Theorem 2.

Let $\chi \in J(\mathbb{F}_q)^\vee$. Then

$$\sum_{P \in T} \chi(P) = \begin{cases} \#I + O(gq^{1/2}\log(p)) & \text{for } \chi = 1, \\ O(gq^{1/2}\log(p)) & \text{otherwise.} \end{cases}$$

Proof of Thm 1

Because of Thm 2, the set I can be chosen within the bounds such that the character sums are different for $\chi = 1$ and all $\chi \neq 1$. Hence we have that $\chi(P) = 1$ for all $P \in T$ implies $\chi = 1$, and T generates $J(\mathbb{F}_q)$.

Let $U \subseteq J(\mathbb{F}_q)$ such that $J(\mathbb{F}_q)/U$ is cyclic, and let $n = \#J(\mathbb{F}_q)/U$. For $d \mid n$ let $\chi \in J(\mathbb{F}_q)^\vee$ with $\ker(\chi) \supseteq U$ of order d. Let $T_d = T \cap \ker(\chi)$, the elements of order n/d in T. Then

$$\begin{aligned} \#T_d &= \sum_{P \in T_d} 1 = \frac{1}{d}\sum_{P \in T}\sum_{i=0}^{d-1} \chi^i(P) = \frac{1}{d}\sum_{P \in T} 1 + \frac{1}{d}\sum_{i=1}^{d-1}\sum_{P \in T}\chi^i(P) \\ &= \frac{1}{d}\#T + O(gq^{1/2}\log(p)). \end{aligned}$$

Iwaniec's shifted sieve implies that the number of generators of $J(\mathbb{F}_q)/U$ in T is greater than or equal to

$$c_1\#T/(\log(\log(n)) + 1)^2 - c_2\log(n)^2 gq^{1/2}\log(p). \qquad \square$$

Proof of Thm 2 - Character sums

Let $X \to C$ be an abelian covering of C, $G(X/C)$ its Galois group and $(\cdot, X/C)$ its Artin symbol. Let $\chi \in G(X/C)^\vee$ be a character and $\mathfrak{f}(\chi)$ the conductor.

Then by Hasse-Weil

$$\begin{aligned} &\sum_{P \in C \setminus \mathfrak{f}(\chi),\, \deg(P) \mid d} \deg(P) \cdot \chi((P, X/C))^{d/\deg(P)} \\ &\qquad = \begin{cases} q^d + O(gq^{d/2}) & \text{for } \chi = 1, \\ O((g + \deg \mathfrak{f}(\chi))q^{d/2}) & \text{otherwise.} \end{cases} \end{aligned}$$

These are "complete" character sums.

Setup

Assume that X represents a Hilbert class field of C.

Instead of $\chi \in J(\mathbb{F}_q)^\vee$ and $\sum_{P\in T}\chi(P)$ we consider $\chi \in G(X/C)^\vee$ and $\sum_{P\in T}\chi((P,X/C))$.

Let $Y \to C$ be an abelian covering linearly disjoint from $X \to C$ and ramified in $S \subseteq C$.

Choose a set $I \subseteq G(Y/C)$ and define $T = \{P \in C(\mathbb{F}_q)\backslash S \mid (P,Y/C) \in I\}$ (will be brought in accordance with I and T from Theorem 1 later).

$$h_I(\sigma) := \frac{1}{\#G(Y/C)} \sum_{\psi\in G(Y/C)^\vee} \sum_{\tau\in I} \psi(\sigma\tau^{-1}) = \begin{cases} 1 & \text{for } \sigma \in I, \\ 0 & \text{otherwise.} \end{cases}$$

Expression

$$\begin{aligned}
\sum_{P\in T}\chi(P) &= \sum_{P\in C(\mathbb{F}_q)\backslash S} \chi(P) h_I(P) \\
&= \frac{1}{\#G(Y/C)} \sum_{P\in C(\mathbb{F}_q)\backslash S} \sum_{\psi\in G(Y/C)^\vee} \sum_{\tau\in I} \chi(P)\psi(P)\psi(\tau^{-1}) \\
&= \frac{\#I}{\#G(Y/C)} \sum_{P\in C(\mathbb{F}_q)} \chi(P) - \frac{\#I}{\#G(Y/C)} \sum_{P\in S} \chi(P) + \\
&\quad \frac{1}{\#G(Y/C)} \sum_{\psi\in G(Y/C)^\vee\backslash\{1\}} \left(\sum_{P\in C(\mathbb{F}_q)\backslash S} \chi(P)\psi(P) \right) \left(\sum_{\tau\in I} \psi(\tau^{-1}) \right)
\end{aligned}$$

(Automatically applying Artin symbols as required.)

Expression

Because of the assumptions, $P \mapsto \chi(P)\psi(P)$ is equal to $P \mapsto (\chi\times\psi)(P)$, where $\chi\times\psi \in G(X \times_C Y/Y)^\vee\backslash\{1\}$.

Also, $\mathfrak{f}(\chi\times\psi) = \mathfrak{f}(\psi)$ and $\mathrm{supp}(\mathfrak{f}(\psi)) \subseteq S$.

So

$$\begin{aligned}
\sum_{P\in C(\mathbb{F}_q)\backslash S} \chi(P)\psi(P) &= \sum_{P\in C(\mathbb{F}_q)\backslash \mathfrak{f}(\psi)} \chi(P)\psi(P) - \sum_{P\in S\backslash \mathfrak{f}(\psi)} \chi(P)\psi(P) \\
&= \sum_{P\in C(\mathbb{F}_q)\backslash \mathfrak{f}(\chi\times\psi)} (\chi\times\psi)(P) - \sum_{P\in S\backslash \mathfrak{f}(\psi)} \chi(P)\psi(P) \\
&= O((g + \deg \mathfrak{f}(\psi)) q^{1/2} + \#S).
\end{aligned}$$

Estimation

Using $b = \frac{1}{\#G(Y/C)} \sum_{\psi\in G(Y/C)^\vee\backslash\{1\}} \left|\sum_{\tau\in I}\psi(\tau^{-1})\right|$:

$$\sum_{P\in T}\chi(P) = \begin{cases} \frac{\#I}{\#G(Y/C)} q + O\big(\#S(1+b) + (g + \max_\psi \deg \mathfrak{f}(\psi)) q^{1/2} b\big) & \text{for } \chi = 1, \\ O\big(\#S(1+b) + (g + \max_\psi \deg \mathfrak{f}(\psi)) q^{1/2} b\big) & \text{otherwise.} \end{cases}$$

Hence can (hope to) get generating set T with $\#T = O(\#S(1+b) + (g + \max_\psi \deg \mathfrak{f}(\psi)) q^{1/2} b)$.

Find suitable Y, I such that $\#S = O(g)$, $\max_\psi \deg(\mathfrak{f}(\psi)) = O(g)$, $b = O(\log(p))$ and make things explicit.

Apparently have $b \geq 1/2$ for $I \neq \emptyset$ and $I \neq G(Y/C)$, so cannot be better than $\#T = O(gq^{1/2})$.

Slide from before with Thm 2

Let B be a subgroup of $\mathbb{F}_q^+$ and $\alpha \in \mathbb{F}_q$. Let $I = \cup_{i=s}^{s+r}(B + \alpha i)$ for $r, s \geq 0$.

Let $f \in \mathbb{F}_q(C)^\times$ be a function with at least one pole order not divisible by p, where $p^n = q$. Such f exists with $\deg(f) = O(g)$.

Let $S = \mathrm{supp}((f)_\infty)$ and $T = \{P \in C(\mathbb{F}_q) \backslash S \mid f(P) \in I\}$.

Theorem 2.

Let $\chi \in J(\mathbb{F}_q)^\vee$. Then

$$\sum_{P \in T} \chi(P) = \begin{cases} \#I + O(gq^{1/2}\log(p)) & \text{for } \chi = 1, \\ O(gq^{1/2}\log(p)) & \text{otherwise.} \end{cases}$$

Use Artin-Schreier covering

Make things explicit, use $Y \to C$ defined by $\mathbb{F}_q(Y) = \mathbb{F}_q(C)(\wp^{-1}(D))$ where $\wp(y) = y^p - y$ and $D = \{\alpha f \mid \alpha \in \mathbb{F}_q\}$.

Then

- $Y \to C$ is ramified only at $S = \mathrm{supp}((f)_\infty)$, linear disjoint from $X \to C$.
- $\#S = O(g)$,
- $\mathfrak{f}(\psi) \leq \sum_{P \in S}(1 - v_P(f))P$, hence $\deg(\mathfrak{f}(\psi)) = O(g)$.
- There is an isomorphism $u : \mathbb{F}_q^+ \to G(Y/C)$ such that $(P, Y/C) = u(f(P))$ for all $P \in C(\mathbb{F}_q) \backslash S$.

So can assume $I \subseteq \mathbb{F}_q^+$ and replace "$(P, Y/C) \in I$" by "$f(P) \in I$".

Theorem 2 now follows since $b = \frac{1}{q}\sum_{\psi \in (\mathbb{F}_q^+)^\vee \backslash \{1\}} \left|\sum_{\tau \in I} \psi(\tau^{-1})\right| \leq 1 + \log(p)$ for the given choice of I. $\square$