Lower bounds on the maximal number of points on curves over finite fields

Jonas Bergström

Stockholm University

Joint with E. Howe, E. Lorenzo García and C. Ritzenthaler.

arXiv:2204.08551

AFDRTIII
October 5, 2022

Questions (from J-P. Serre)

Definition

Let $N_q(g)$ denote the maximal number of (rational) points on any (smooth and projective) curve of genus g over a finite field $\mathbb{F}_q$.

Question (1)

Fix g, does the value $N_q(g)$ remain at a bounded distance from the Hasse–Weil bound $1 + q + 2g\sqrt{q}$ for all q (as is the case for $g = 0, 1$ and 2)?

Question (2)

Is it possible to give, for each g, positive constants c, q_o such that for all $q > q_0$, we have $N_q(g) \geq 1 + q + c\sqrt{q}$?

Three approaches to Question 2

(1) Katz-Sarnak theory - which will give the optimal result of this kind when $q \to \infty$.

(2) Recursive constructions of double covers, starting with well chosen hyperelliptic curve of genus 2 or 3.

Theorem (B.L-G.H.R.)

For any q and $g \geq 2$, $N_q(g) \geq q + 1 + 4\sqrt{q} - 31$.

(3) Counts of points over $\mathbb{F}_q$ of moduli spaces of hyperelliptic curves - reproves the optimal result when $q \to \infty$, gives weaker bounds than with method 2 (with current knowledge about the moduli spaces).

Moduli spaces of curves

- For $g \geq 2$, let $\mathcal{M}_g$ denote the moduli space of curves of genus g which is defined over $\mathbb{Z}$.
- Let $\mathcal{M}_g(\mathbb{F}_q)$ denote the set of $\mathbb{F}_q$-isomorphism classes of curves over $\mathbb{F}_q$.
- If $C/\mathbb{F}_q$ is a curve of genus g, put

$$a_1(C) = \mathrm{Tr}\big(Fr_q, H^1_{\acute{e}t}(C, \mathbb{Q}_\ell)\big) = q + 1 - \#C(\mathbb{F}_q),$$

  and for $n \geq 1$,

$$S_n(q, \mathcal{M}_g) = \sum_{[C] \in \mathcal{M}_g(\mathbb{F}_q)} \frac{a_1(C)^n}{\#\mathrm{Aut}_{\mathbb{F}_q}(C)}.$$

- Let $\mathcal{H}_g \subset \mathcal{M}_g$ denote the subspace of hyperelliptic curves, and make the corresponding definitions.

Results from Katz-Sarnak theory

Theorem (Katz-Sarnak 1999)

Fix $g \geq 2, n \geq 1$. Let dm be the Haar measure on USp_{2g}, the compact symplectic group. Then we have,

$$\int_{m \in \mathrm{USp}_{2g}} \mathrm{Tr}(m)^n \, dm = \frac{S_n(q, \mathcal{M}_g)}{q^{\dim \mathcal{M}_g + n/2}} + O(q^{-1/2}).$$

Proposition (Katz-Sarnak/Lachaud 2016)

Fix $g \geq 2$. Put

$$A(x) := \sum_{\substack{C \in \mathcal{M}_g(\mathbb{F}_q) \\ a_1(C) \leq x\sqrt{q}}} \frac{1}{\#\mathrm{Aut}_{\mathbb{F}_q}(C)}$$

Then we have for any $-2g \leq x \leq 2g$,

$$A(x)/A(2g) = F(x) + O(q^{-1/2}),$$

for a strictly increasing function $F(x)$ with $F(2g) = 1$.

Katz-Sarnak theory: corollary

Corollary (B.L-G.H.R.)

Fix $g \geq 2$ and $\varepsilon > 0$. For all sufficiently large q we have,

$$N_q(g) > q + 1 + (2g - \varepsilon)\sqrt{q}.$$

Proof.

Since $F(x)$ is strictly increasing for $-2g \leq x \leq 2g$, $F(2g - \varepsilon) < 1$. So, taking sufficiently large q we have

$$A(2g - \epsilon)/A(2g) < 1.$$

Hence, there is a curve $C/\mathbb{F}_q$ with $a_1(C) > (2g - \varepsilon)\sqrt{q}$. □

Note that the above results holds just as well when one replaces $\mathcal{M}_g$ with $\mathcal{H}_g$.

The idea is to construct double covers of hyperelliptic curves $C_n \to \ldots \to C_1$, with $\#C_{i+1}(\mathbb{F}_q) \geq \#C_i(\mathbb{F}_q)$ and increasing genus.

Lemma (B.L-G.H.R.)

Let q be odd and let $C/\mathbb{F}_q$ be a hyperelliptic curve of genus g (with fewer than q rational Weierstrass points). Then there is a hyperelliptic curve D of genus $2g+1$ that is a double cover of C and such that $\#D(\mathbb{F}_q) \geq \#C(\mathbb{F}_q)$.

Proof (sketch).

Say that C is given by $y^2 = f(x)$ of degree $2g+2$ and $f(0) \neq 0$, then $y^2 = f(x^2)$ and $y^2 = f(n \cdot x^2)$, with n a non-square in $\mathbb{F}_q$, gives D, D' such that $\#D(\mathbb{F}_q) + \#D'(\mathbb{F}_q) = 2\#C(\mathbb{F}_q)$. □

There is a similar lemma (with a more subtle proof), demanding that C has exactly two rational Weierstrass points, for covers of genus $2g$.

Recursive double covers: the base cases

Lemma (B.L-G.H.R.)

Let q be odd. Then there is a curve $C/\mathbb{F}_q$ of genus 2 with exactly two rational Weierstrass points such that

$$\#C(\mathbb{F}_q) > \begin{cases} 1+q+4\sqrt{q}-5 & \text{if } q < 512; \\ 1+q+4\sqrt{q}-32 & \text{if } q > 512. \end{cases}$$

Excerpts from the proof.

The result for $q < 512$ is found by computer counts.
For $q \equiv_3 4$, we can find an elliptic curve $E : y^2 = x(x-a)(x-b)$ such that $(a_1(E), q) = 1$, $a_1(E) \equiv_8 -q-1$ and $a_1(E) > 2\sqrt{q} - 16$.
Using results of Howe, Leprévost, Poonen, the curve $y^2 = h$ with:

$$h = c\left(x^2 + b/a\right)\left(x^2 - (a-b)/b\right)\left(x^2 - a/(b-a)\right),$$

has a Jacobian which is isogenous to $E \times E$ and which has exactly two rational Weierstrass points. $\square$

Recursive double covers: summing up

- There is a similar result in genus 3 (using double covers of curves of genus 2 constructed as in the previous lemma).
- With these base cases in genus 2 and 3 we can reach any genus g using towers as above.
- There are corresponding results when q is even.
- In summary we have (as we saw before):

Theorem (B.L-G.H.R.)

For any q and $g \geq 2$, $N_q(g) \geq q + 1 + 4\sqrt{q} - 31$.

Counting points on moduli spaces of hyperelliptic curves

Theorem (B. 2009)

For every $g \geq 2$ and q we have

$$S_2(q,\mathcal{H}_g) = [q^{2g}] - 1$$

$$S_4(q,\mathcal{H}_g) = \left[\frac{q^{2g}(3q^2+q+1)}{q+1}\right] - \frac{1}{2}(q-1)(q-2)(q+1)g^2 + \\ + \frac{1}{2}(-q^3+2q^2-7q+2)g - 3q + 2$$

$$S_6(q,\mathcal{H}_g) = \left[\frac{q^{2g}(15q^4+16q^2+2q+1)}{(q+1)^2}\right] + \ldots$$

where $[f_1/f_2]$ denotes the polynomial quotient in the Euclidean division of f_1 by f_2.

- The part $[\cdot]$ is the contribution from the stable cohomology.
- We also prove a formula for $S_8(q,\mathcal{H}_g) = 105q^{2g+3} + \ldots$.

Point counting corollary

Theorem (B.L-G.H.R.)

For $g \geq 2$, q and (even) $n \geq 2$, let

$$a_{q,n}(g) := (S_n(q, \mathcal{H}_g)/q^{\dim \mathcal{H}_g + n/2})^{1/n}.$$

Then $N_q(g) \geq q + 1 + a_{q,n}(g)\sqrt{q}$.

Proof (sketch).

There are q^{2g-1}, $\overline{\mathbb{F}}_q$-isomorphism classes of hyperelliptic genus-g curves defined over $\mathbb{F}_q$. Each such can be represented by a curve $C_1, \ldots, C_{q^{2g-1}}$ over $\mathbb{F}_q$ and a positive integer $s_n(C_i)$ such that $a_1(C_i)^n \geq s_n(C_i)$ and $S_n(q, \mathcal{H}_g) = \sum_{i=1}^{q^{2g-1}} s_n(C_i)$. So, there has to be a curve C_j such that $a_1(C_j)^n \geq S_n(q, \mathcal{H}_g)/q^{2g-1}$. □

- For $n = 8$, $g \geq 3$ and odd $q \geq 11$ this gives the corollary,
$$N_q(g) \geq q + 1 + 1.71\sqrt{q}.$$

The main term when point counting

Theorem (B.L-G.H.R.)

For $g \geq 2$ and (even) $n \geq 2$ let

$$\mathfrak{a}_n(g) := \lim_{q \to \infty} S_n(q, \mathcal{H}_g)/q^{\dim \mathcal{H}_g + n/2}.$$

Then $\mathfrak{a}_n(g)$ is equal to the number of times the trivial representation appears in the USp_{2g}-representation $V^{\otimes n}$ with V the standard representation.

Proof (sketch).

See the Katz-Sarnak theorem. $\square$

Theorem (B.L-G.H.R.)

For every $g \geq 2$, we have

$$\lim_{n \to \infty} \left(\mathfrak{a}_{2n}(g)\right)^{1/2n} = 2g\,.$$

Representations and local systems

- From now on work in progress (and less directly connected to $N_q(g)$).
- The irreducible representations $V_\lambda(j)$ of GSp_{2g} are indexed by $\lambda = (\lambda_1, \ldots, \lambda_g)$ with $\lambda_1 \geq \ldots \geq \lambda_g \geq 0$ and an integer j.
- Put $|\lambda| = \lambda_1 + \ldots + \lambda_g$ and note that $V_\lambda^\vee \cong V_\lambda(|\lambda|)$.
- Let $V = V_{(1)}(-1)$ be the standard representation.
- From the universal curve $\pi : \mathcal{H}_{g,1} \to \mathcal{H}_g$ we define the local system $\mathbb{V} := R^1\pi_*\mathbb{Q}_\ell$.
- For $[C] \in \mathcal{H}_g$ we have $\mathbb{V}_{[C]} \cong H^1(C, \mathbb{Q}_\ell)$ and from the symplectic pairing we get induced local systems $\mathbb{V}_\lambda(j)$.

Lefschetz trace formula and cohomology of local systems

- For any n, there are integers $c_{\lambda,n} \geq 0$ such that,

$$V^{\otimes n} \cong \bigoplus_{|\lambda| \leq n} V_\lambda^{\oplus c_{\lambda,n}}\big((-n+|\lambda|)/2\big).$$

- Note that $c_{\lambda,n} = 0$ if $|\lambda| \not\equiv_2 n$.
- The Lefschetz trace formula gives us,

$$S_n(q,\mathcal{H}_g) = \sum_{i=0}^{2\dim \mathcal{H}_g} (-1)^i \,\mathrm{Tr}\big(\mathrm{Fr}_q, H_c^i(\mathcal{H}_g \otimes \overline{\mathbb{F}}_q, \mathbb{V}_1^{\otimes n})\big) =$$

$$= \sum_{|\lambda| \leq n} c_{\lambda,n} \sum_{i=0}^{2\dim \mathcal{H}_g} (-1)^i \,\mathrm{Tr}\big(\mathrm{Fr}_q, H_c^i(\mathcal{H}_g \otimes \overline{\mathbb{F}}_q, \mathbb{V}_\lambda)\big)\, q^{(n-|\lambda|)/2}.$$

The zeroeth cohomology group

- Deligne's theory of weights tells us that that the trace of Frobenius on $H_c^j(\mathcal{H}_g \otimes \overline{\mathbb{F}}_q, \mathbb{V}_\lambda)$ is equal (after choosing an embedding of $\overline{\mathbb{Q}}_\ell$ in $\mathbb{C}$) to a sum of complex numbers with absolute value at most $q^{(j+|\lambda|)/2}$.
- So only when $j = 2\dim\mathcal{H}_g$ can we get a contribution to $\mathfrak{a}_n(\mathcal{H}_g)$.
- Poincaré duality gives

$$H^0(\mathcal{H}_g \otimes \overline{\mathbb{F}}_q, \mathbb{V}_\lambda) \cong H_c^{2\dim\mathcal{H}_g}(\mathcal{H}_g \otimes \overline{\mathbb{F}}_q, \mathbb{V}_\lambda)(\dim\mathcal{H}_g).$$

- But $H^0(\mathcal{H}_g \otimes \overline{\mathbb{F}}_q, \mathbb{V}_\lambda)$ is non-zero precisely if $\mathbb{V}_\lambda$ is trivial and Frobenius acts as multiplication by 1, hence we reprove that: $\mathfrak{a}_n(\mathcal{H}_g)$ is equal to the number of times the trivial representation appears in the USp_{2g}-representation $V^{\otimes n}$.
- Note that this is also the argument by Katz-Sarnak.

The first cohomology group and even n

- We will now return to $\mathcal{M}_g$.
- Take $g \geq 3$. From the work of Johnson 83' and Hain 95' we know that $H^1(\mathcal{M}_g, \mathbb{V}_\lambda)$ is non-zero if and only if $\lambda = (1,1,1)$.
- By comparison theorems the same holds (in étale cohomology) for $H^1(\mathcal{M}_g \otimes \overline{\mathbb{F}}_q, \mathbb{V}_\lambda)$.
- The same type of argument using Deligne's theory of weights gives the following,

Theorem (B.L-G.H.R.)

For any $g \geq 3$ and even $n \geq 2$,

$$\int_{m \in \mathrm{USp}_{2g}} \mathrm{Tr}(m)^n \, dm = \frac{S_n(q, \mathcal{M}_g)}{q^{\dim \mathcal{M}_g + n/2}} + O(q^{-1}).$$

The first cohomology group and odd n

- For odd n and $g \geq 3$ let us define
$$\mathfrak{b}_n(\mathcal{M}_g) := -\lim_{q\to\infty} \frac{S_n(q, \mathcal{M}_g)}{q^{\dim \mathcal{M}_g + (n-1)/2}}.$$
- The cohomology group $H^1(\mathcal{M}_g \otimes \overline{\mathbb{F}}_q, \mathbb{V}_{(1,1,1)})$ is of dimension one and generated by the Gross-Schoen cycle, so the action of Fr_q on this cohomology group is by multiplication by q.
- Using again Deligne's theory of weights we get,

Theorem (B.L-G.H.R.)

For any $g \geq 3$ and odd $n \geq 1$, $\mathfrak{b}_n(\mathcal{M}_g)$ equals the number of times the representation $V_{(1,1,1)}$ appears in the USp_{2g}-representation $V^{\otimes n}$ with V the standard representation.

Serre's obstruction and experiments in genus three

- In genus $g \geq 3$ there are non-hyperelliptic curves and for such curves, the quadratic twist of its Jacobian is never a Jacobian. This is called *Serre's obstruction*.
- Define,

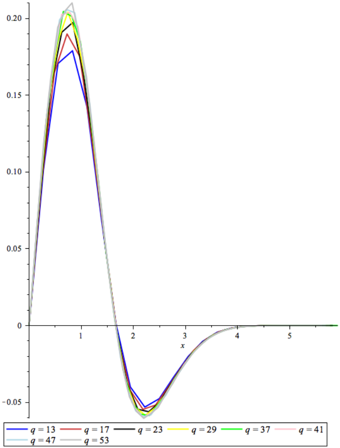
$$\mathcal{N}_{q,g}(x) := \frac{1}{q^{\dim \mathcal{M}_g}} \cdot \sum_{\substack{C \in \mathcal{M}_g(\mathbb{F}_q) \\ a_1(C) = \lfloor x\sqrt{q} \rfloor}} \frac{1}{\#\mathrm{Aut}_{\mathbb{F}_q}(C)},$$

  and

$$\mathcal{V}_{q,g}(x) := \sqrt{q}\,\big(\mathcal{N}_{q,g}(x) - \mathcal{N}_{q,g}(-x)\big),$$

  to measure this obstruction.
- Concrete data for $\mathcal{V}_{q,3}(x)$ for small q seems to indicate that it follows a common distribution:

Linear interpolation of $\mathcal{V}_{q,3}(x)$.



Heuristics for $\mathcal{V}_{q,3}(x)$.

- This data (and graph) was found by Lercier, Ritzenthaler, Rovetta, Sijsling, Smith 19' and they gave a heuristic argument that the distribution $\mathcal{V}_{q,3}(x)$ is related to the function

$$\mathcal{V}_3^{\lim}(x) = x(1 - x^2/3) \cdot \left(\frac{1}{2\sqrt{\pi}} e^{-x^2/2} \right).$$

- This relates to our older considerations since for *odd* n,

$$\sum_{-2g\sqrt{q} \leq t \leq 2g\sqrt{q}} \left(\frac{t}{\sqrt{q}} \right)^n \mathcal{V}_{q,g}\left(\frac{t}{\sqrt{q}} \right) = \frac{2 \cdot S_n(q, \mathcal{M}_g)}{q^{\dim \mathcal{M}_g + (n-1)/2}},$$

so letting q go to ∞ this expression goes to $-2\mathfrak{b}_n(g)$.

- Let now $\nu_3^{\lim}$ be of the form $P(x) \cdot \left(\frac{1}{\sqrt{2\pi}} e^{-x^2/2} \right)$ with P an odd polynomial of degree 5, with odd moments matching $-2\mathfrak{b}_n(3)$ for $n \leq 5$, we seem to get get an even better approximation:

Comparisons with $\mathcal{V}_{53,3}(x)$.

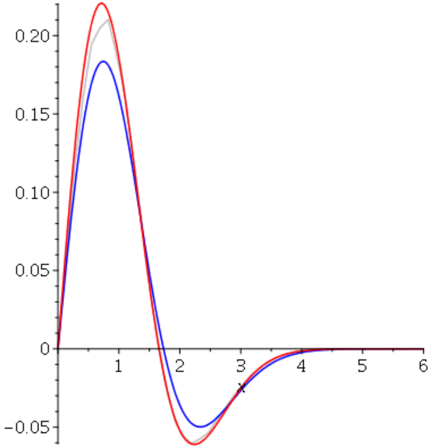


Figure: $\mathcal{V}_{53,3}$ in grey, $\mathcal{V}_3^{\lim}$ in blue and $\nu_3^{\lim}$ in red.

And finally:

Thank you for listening!