An analogue of the Brauer-Siegel theorem for some families of elliptic curves over function fields

RICHARD GRIFFON, Institut de Mathématiques de Jussieu - Université Paris Diderot

Introduction

Let E be an elliptic curve over the function field $K = \mathbb{F}_q(t)$.
The arithmetic of E is (or should be) encoded in three objects:

- $E(K)$, its **Mordell-Weil group**: a finitely generated group equipped with the canonical Néron-Tate height pairing $\langle \cdot, \cdot \rangle_{NT}$.
- $Ш(E/K)$, its **Shafarevich-Tate group**: conjecturally a finite group.
- $L(E/K, s)$, its L-function and the **special value at** $s = 1$, which appears in the Birch & Swinnerton-Dyer conjecture:

$$L^*(E/K, 1) := \lim_{s \to 1} \frac{L(E/K, s)}{(s-1)^{\mathrm{ord}_{s=1} L(E/K,s)}}.$$

Recall that the **Néron-Tate regulator** is defined as

$$\mathrm{Reg}(E/K) := \det\left(\langle P_i, P_j \rangle_{NT}\right)_{1 \le i,j \le r}$$

where $P_1, \ldots, P_r$ denotes a basis of the free part of $E(K)$.

General diophantine problem: bounding the size of $E(K)$ and $Ш(E/K)$ in terms of the exponential differential height $H(E/K)$ (or in terms of the conductor $\mathcal{N}_{E/K}$). But individual bounds are hard to obtain: for example,

- Lang's conjecture: $\mathrm{Reg}(E/K) \gg (\log H(E/K))^{\mathrm{rk}\ E(K)}$.
- Szpiro's conjecture: $\# Ш(E/K) \ll_\epsilon \mathcal{N}_{E/K}{}^{1/2+\epsilon} \ll_\epsilon H(E/K)^{1+\epsilon}$.

Following [Hindry], we consider the **Brauer-Siegel ratio of** E/K:

$$\mathfrak{Bs}(E/K) := \frac{\log\left(\mathrm{Reg}(E/K) \cdot \# Ш(E/K)\right)}{\log H(E/K)}.$$

In a sense, $\mathfrak{Bs}(E/K)$ quantifies the difficulty of finding rational points on E and of computing a basis for the Mordell-Weil group of E.

- **What is the behaviour of $\mathfrak{Bs}(E/K)$ when $H(E/K) \to \infty$?**
- **Is it always true that $\mathfrak{Bs}(E/K) \to 1$?**

Remark 1: $\mathfrak{Bs}(A/K)$ makes sense for any abelian variety A over a global field K (provided its $Ш$ is finite). What is the behaviour of $\mathfrak{Bs}(A/K)$ when $H(A/K) \to \infty$ with $\dim A$ fixed?
Remark 2: Note the analogy with the Brauer-Siegel theorem, which says that

$$\mathfrak{Bs}(K/\mathbb{Q}) := \frac{\log\left(\mathrm{Reg}(\mathcal{O}_K^\times) \cdot \# \mathcal{C}\ell(\mathcal{O}_K)\right)}{\log \sqrt{\Delta_K}} \xrightarrow[{[K:\mathbb{Q}]\text{ fixed}}]{\Delta_K \to \infty} 1.$$

Analytic proof: (1) Link $\mathfrak{Bs}(K/\mathbb{Q})$ with the residue $\mathrm{res}_{s=1}\zeta_K(s)$.
(2) Study the behaviour of $\zeta_K(s)$ around $s = 1$.

This analogy suggests to study the behaviour of $L(E/K, s)$ around $s = 1$.

Previous results

Little is known about $\mathfrak{Bs}(E/K)$. [Hindry & Pacheco] show (conditional to $Ш$ being finite) that

$$0 \le \liminf_{E \in \mathcal{E}} \mathfrak{Bs}(E/K) \le \limsup_{E \in \mathcal{E}} \mathfrak{Bs}(E/K) \le 1 \qquad \text{as } H(E/K) \to +\infty$$

where $\mathcal{E} = \{\text{all elliptic curves over } K\}$.

Example: For all n prime to q, let $E_n/K : Y^2 + XY = X^3 - t^n$. The finiteness of $Ш(E_n/K)$ is due to [Ulmer], and [Hindry & Pacheco] show that E_n/K satisfies

$$H(E_n/K) \xrightarrow[n \to \infty]{} \infty, \quad \mathfrak{Bs}(E_n/K) \xrightarrow[n \to \infty]{} 1.$$

So the lim sup above is actually 1. **What is the** $\liminf \mathfrak{Bs}(E/K)$**? Is it** < 1**?**

Theorem

Write $K = \mathbb{F}_q(t)$. *We always assume* $\mathrm{char}(\mathbb{F}_q) > 3$.
Let $E_0 : y^2 = x^3 + ax + b$ be an elliptic curve over $\mathbb{F}_q$; let E be the constant elliptic curve $E = E_0 \times_{\mathbb{F}_q} \mathbb{F}_q(t)$. For $d \in \mathbb{N}^*$, prime to q, let $E^{(d)}/K$ be the quadratic twist of E by $D(t) = t^d + 1$:

$$E^{(d)} : D(t) \cdot Y^2 = X^3 + aX + b.$$

One has $H(E^{(d)}/K) = q^{\lfloor \frac{d-1}{2} \rfloor + 1}$.

Theorem (G.) Consider the family of quadratic twists of constant elliptic curves over K by $D(t) = t^d + 1$ with $d \in \mathbb{N}^*$ prime to q:

$$\mathcal{E} := \left\{ E^{(d)},\ E/\mathbb{F}_q(t) \text{ constant ell. curve } \& \ d \in \mathbb{N}^* \text{ with } \gcd(d, q) = 1 \right\}.$$

Then $Ш(E^{(d)}/K)$ *is finite for all* $E^{(d)} \in \mathcal{E}$ and

$$o(1) \le \mathfrak{Bs}(E^{(d)}/K) \le 1 + o(1) \qquad (d \to \infty). \qquad (*)$$

Moreover, in the "supersingular case", *i.e.* when d runs through the (infinite) set $\mathcal{D}_q := \left\{ d \in \mathbb{N}^* \,\middle|\, \exists n \in \mathbb{N}^* \text{ such that } d \text{ divides } q^n + 1 \right\}$, one has

$$\mathfrak{Bs}(E^{(d)}/\mathbb{F}_q(t)) \xrightarrow[d \in \mathcal{D}_q,\ d \to \infty]{} 1.$$

Comments & future works

This is a work in progress.

- Can we also compute $\lim \mathfrak{Bs}(E^{(d)}/K)$ when d is not necessarily in the "supersingular set" $\mathcal{D}_q$? Is it still true that $\mathfrak{Bs}(E^{(d)}/K) \to 1$?
- One can also twist the constant curve E by any squarefree polynomial $D(t) \in \mathbb{F}_q[t]$ instead of $D(t) = t^d + 1$. In which case, we can easily prove that

  $$o(1) \le \mathfrak{Bs}(E^D/K) \le 1 + o(1) \qquad (\deg D \to \infty).$$

  For which families of such D can we explicitly compute $\lim \mathfrak{Bs}(E^D/K)$? Equivalently, can we compute the zeroes of the zeta-function of $C_D : Y^2 = D(X)$?
- For which families of non-constant elliptic curves over $\mathbb{F}_q(t)$ can we compute (unconditionally) the limit of the Brauer Siegel ratio?
- Is there one such family of elliptic curves for which $\lim \mathfrak{Bs}(E/K)$ is < 1? is 0?
- In general, if B&SD is known for E/K, bounding $\mathfrak{Bs}(E/K)$ is equivalent to finding good upper and lower bounds for $|L^*(E/K, 1)|$. The size of $|L^*(E/K, 1)|$ depends on how the zeroes of $L(E/K, s)$ are distributed on the line $\Re(s) = 1$. The main contribution comes from the "small zeroes".

Ingredients of the proof

Let $\mathcal{C}_d/\mathbb{F}_q$ be the smooth hyperelliptic curve defined by

$$\mathcal{C}_d : Y^2 = X^d + 1.$$

Put $g_d = \left\lfloor \frac{d-1}{2} \right\rfloor = \mathrm{genus}(\mathcal{C}_d)$ and write the L-function of E_0 as

$$L(E_0/\mathbb{F}_q, T) = (1 - \alpha T)(1 - \bar{\alpha} T), \quad |\alpha| = \sqrt{q}.$$

(1) [Milne] showed that the $Ш$ of any twist E' of a constant elliptic curve is finite and that the full B&SD conjecture is true for E':

$$L^*(E'/K, 1) = \frac{\mathrm{Reg}(E'/K) \cdot \# Ш(E'/K)}{(\# E'(K)_{\mathrm{tors}})^2 \cdot H(E'/K)} \cdot \mathrm{Tam}(E'/K).$$

(2) Here, $\# E^{(d)}(K)_{\mathrm{tors}} = \mathcal{O}(1)$ and $\mathrm{Tam}(E^{(d)}/K) = o(g_d)$. Thus, when $g_d \to \infty$,

$$\mathfrak{Bs}(E^{(d)}/K) = 1 + \frac{\log |L^*(E^{(d)}/K, 1)|}{g_d \cdot \log q} + o(1).$$

(3) Easy bounds for $|L^*(E^{(d)}/K, 1)|$ imply $(*)$:

$$-g_d \cdot \log q \le \log |L^*(E^{(d)}/K, 1)| \le 2 \log g_d.$$

(4) [Milne] also proved that

$$L^*(E^{(d)}/K, 1) = (\log q)^{\mathrm{rk}\ E^{(d)}(K)} \cdot |L_d^{\neq}(\alpha^{-1})|^2,$$

where $L_d^{\neq}(T) \in \mathbb{Z}[T]$ is the numerator $L_d(T)$ of

$$Z(\mathcal{C}_d/\mathbb{F}_q, T) = \frac{\prod_{j=1}^{2g_d}(1 - \beta_j T)}{(1 - T)(1 - qT)}, \quad |\beta_j| = \sqrt{q}$$

with the factors vanishing at α^{-1} or $\bar{\alpha}^{-1}$ removed.

(5) Using the explicit formulae, one can show that

$$\mathrm{rk}\ E^{(d)}(K) = \mathcal{O}(d/\log d) = o(g_d).$$

(6) It follows from computations of [Weil] that

$$L_d(T) = \prod_m (1 - J(m) T^{u(m)}) \qquad (m \in (\mathbb{Z}/d\mathbb{Z} \smallsetminus \{0, d/2\})/\langle q \bmod d \rangle),$$

where $u(m) = \mathrm{order}(q \bmod d/\gcd(d, m))$ and $J(m)$ is a Jacobi sum.

(7) If d divides $q^n + 1$ for some n, [Shafarevich & Tate] proved that $u(m)$ is even and $J(m) = -q^{u(m)/2}$. So $L_d(T)$ has the form $L_d(T) = \prod_{j=1}^{h_d}(1 + q^{v_j} T^{2v_j})^{m_j}$.

(8) At some point, we use Baker-Wüstholz theorem. Write $\alpha = \sqrt{q} \cdot e^{i\theta}$, then for all $n \in \mathbb{N}^*$: either $\log|\cos(n\theta)| = 0$ or $\log|\cos(n\theta)| \gg_q \log(n)$.

References

[Hindry] M. Hindry, *Why is it difficult to compute the Mordell-Weil group?*, in Diophantine geometry, CRM Series, Ed. Norm. Pisa **4** (2007), 197-219.

[Hindry & Pacheco] M. Hindry & A. Pacheco, *An analogue of the Brauer-Siegel theorem for abelian varieties in positive characteristic*, Preprint (2015).

[Milne] J. Milne, *The Tate-Shafarevich group of a constant abelian variety*, Invent. Math. **6** (1968), 91-105.

[Shafarevich & Tate] I. Shafarevich & J. Tate, *The rank of elliptic curves*, Dokl. Akad. Nauk SSSR **175** (1967), 770-773.

[Ulmer] D. Ulmer, *Elliptic curves with high rank over function fields*, Annals of Math. **155** (2002), 295-315.

[Weil] A. Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497-508.

Contact

Richard Griffon – *PhD Student*
(Supervisor: Marc Hindry)
Institut de Mathématiques de Jussieu
Université Paris Diderot
✉ : richard.griffon@imj-prg.fr

PARIS DIDEROT   IMJ-PRG