Distribution of Frobenius polynomials of abelian varieties of extremely small order

Kiran S. Kedlaya

Department of Mathematics, University of California San Diego
kedlaya@ucsd.edu
These slides can be downloaded from https://kskedlaya.org/slides/.

Arithmetic, Geometry, Cryptography, and Coding Theory (AGC^{2}T)
CIRM (Centre international de rencontres mathématiques), Luminy, Marseille, France
June 11, 2025

Supported by (grant DMS-2401536) and UC San Diego (Warschawski Professorship).
I acknowledge that my workplace occupies unceded ancestral land of the Kumeyaay Nation.

Orders of abelian varieties over finite fields

Let A be an abelian variety of dimension g over $\mathbb{F}_q$. The characteristic polynomial of Frobenius on A has coefficients in $\mathbb{Z}$ and has the form

$$P_A(T) = \prod_{i=1}^{g} (T - \alpha_i)(T - \overline{\alpha}_i), \qquad \alpha_i \in \mathbb{C}, |\alpha_i| = q^{1/2}.$$

The group $A(\mathbb{F}_q)$ has order $P_A(1) = \prod_i (1 - \alpha_i)(1 - \overline{\alpha}_i) = \prod_i (q + 1 - \alpha_i - \overline{\alpha_i})$ and hence

$$\#A(\mathbb{F}_q) \geq (q + 1 - 2\sqrt{q})^g = (\sqrt{q} - 1)^{2g}.$$

For $q \geq 5$, $\sqrt{q} - 1 > 1$ and this lower bound is exponential. For $q \leq 4$, there is **no** exponential lower bound: there exists an elliptic curve E with $P_E(T) = T^2 - qT + q$ and hence $\#E(\mathbb{F}_q) = 1$, and any power $A = E^g$ satisfies $\#A(\mathbb{F}_q) = 1$ for all g.

The simple case

Now let A be a **simple** abelian variety of dimension g over $\mathbb{F}_q$. We get better bounds by applying Tate's theorem: for any fixed simple abelian variety B not isogenous to A,

$$|\operatorname{Res}_T(P_A(T), P_B(T))| \geq 1 \quad \text{and so} \quad 0 \leq \sum_{i=1}^{g} \log |P_B(\alpha_i)|^2.$$

For $q = 3, 4$, this can be used to deduce an exponential lower bound on $\#A(\mathbb{F}_q)$ by excluding E (Aubry–Haloui–Lachaud, Kadets, van Bommel–Costa–Poonen–Li–Smith). We will see a similar computation later.

However, for $q = 2$, there are **infinitely many** simple A with $\#A(\mathbb{F}_2) = 1$ (Madan–Pal). This occurs when $\beta_i := 3 - \alpha_i - \overline{\alpha}_i$ is an algebraic **unit** with all conjugates in $[3 - 2\sqrt{2}, 3 + 2\sqrt{2}]$. This means that $\beta_i + \beta_i^{-1}$ is an algebraic integer with all conjugates in $[2, 6]$; by Kronecker, it must be $4 + \zeta + \zeta^{-1}$ for some root of unity ζ.

Context: the relative class number m problem for function fields

For $C' \to C$ a finite separable morphism of classical[1] curves over $\mathbb{F}_q$, the relative class number $h(C')/h(C)$ can be interpreted as $\#A(\mathbb{F}_q)$ where A is the Prym variety for the covering.

For each r, let T_{A,q^r} be the q^r-Frobenius trace on A. Then

$$0 \leq \#C'(\mathbb{F}_{q^r}) = q^r + 1 - T_{J(C'),q^r} = q^r + 1 - T_{J(C),q^r} - T_{A,q^r} = \#C(\mathbb{F}_{q^r}) - T_{A,q^r}.$$

Say we want to bound g assuming that $h(C')/h(C) = m$. For each r we can write down an "explicit formulas" / "linear programming"[2] bound of the form

$$\#C(\mathbb{F}_{q^r}) \leq c_0 g + c_1.$$

We can thus win by finding a sufficiently good lower bound of the form

$$\sum_{r=1}^{s} a_r T_{A,q^r} \geq b_0 g - b_1.$$

[1] Smooth, projective, and geometrically irreducible. Sometimes also called "nice".

[2] See Serre, *Rational points on curves over finite fields*, Chapters 6–7.

Relative class number m for function fields (continued)

For $q = 3, 4$, we get a lower bound on traces by writing $A \sim E^r \times B$ where B does not have E have an isogeny factor; bounding $\dim(B)$ in terms of m; then applying the Weil bound to T_{B,q^r}. The resulting bound is good enough to solve the relative class number m problem for $q > 2$ when $m = 1$ (K.) or $m = 2$ (Arango-Piñeros–Chara–Hamakiotes–K.–Rama).

For $q = 2, m = 1$, one can write down a bound of the form $\sum_{r=1}^{4} a_r T_{A,2^r} \geq b_0 g - b_1$ for all A with $\#A(\mathbb{F}_2) = 1$; it suffices to achieve this for simple A which we have already classified. This is good enough to solve the relative class number 1 problem (K.).

We now explain how to derive similar bounds for $q = 2$ and general m, where no classification exists. This leads to an effective upper bound for the relative class number m problem for $q = 2$ (ACHKR).

A converse problem is to establish **existence** of many simple abelian varieties over $\mathbb{F}_2$ of fixed order. See my upcoming talk at René 25.

A qualitative result

For A a simple abelian variety over $\mathbb{F}_2$ with $\dim(A) = g$, define the Radon measure μ_A on $[3 - 2\sqrt{2}, 3 + 2\sqrt{2}]$ as an average of Dirac measures:

$$\mu_A := \frac{1}{g} \sum_{i=1}^{g} \delta_{3-\alpha_i-\overline{\alpha}_i}.$$

Theorem

There exists a measure μ with the property: for any sequence of A with $g \to \infty$ and $\frac{1}{g} \log \#A(\mathbb{F}_2) \to 0$, the sequence μ_A converges in measure to μ.

The measure μ is symmetric via $\beta \mapsto \beta^{-1}$, so it pulls back along $\beta \mapsto 4 - \beta - \beta^{-1}$ from a measure on $[-2, 2]$. The latter is the pushforward of the uniform measure on the unit circle along $\zeta \mapsto \zeta + \zeta^{-1}$.

The proof uses (a little) **capacity theory** as in Serre's Seminaire Bourbaki from March 2018.

Quantitative estimates

For a function $f(x)$ with $f(x) \geq a - b\log(3-x)$ for $[-2\sqrt{2}, 2\sqrt{2}]$, integrating against μ_A yields

$$\sum_{i=1}^{g} f(\alpha_i + \overline{\alpha}_i) \geq ag - b\log \#A(\mathbb{F}_2).$$

In particular, this holds with

$$f(x) = x + 0.2456(x^2 - 4) + 0.0887(x^3 - 6x) + 0.0295(x^4 - 8x + 8),\ a = 1.1691,\ b = 1.9169.$$

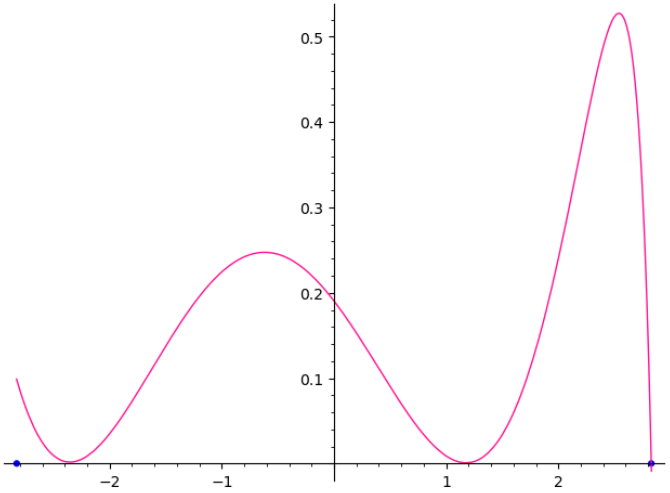
We thus have the following estimate (ACHKR): for any abelian variety A over $\mathbb{F}_2$,

$$T_{A,2} + 0.2456\, T_{A,2^2} + 0.0887\, T_{A,2^3} + 0.0295\, T_{A,2^4} \geq 1.1691 \dim(A) - 1.9169 \log \#A(\mathbb{F}_2).$$

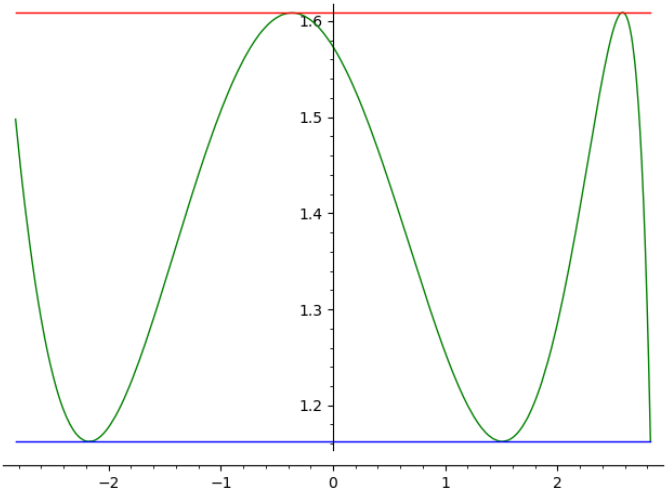
Using similar logic (with a different function), we obtain

$$1.162g \leq T_{A,2} + 0.2417\, T_{A,4} + 0.0878\, T_{A,8} + 0.0454\, T_{A,16} + 1.9815 \log \#A(\mathbb{F}_2) \leq 1.6085g.$$

Plot of $f(x) - a + b\log(3 - x)$ for $x \in [-2\sqrt{2}, 2\sqrt{2}]$ (first bound)



Plot of $f(x) - a + b\log(3 - x)$ for $x \in [-2\sqrt{2}, 2\sqrt{2}]$ (second bound)



How to obtain similar bounds

In this example, the coefficients of $b^{-1}(a - f(x))$ are chosen to give a good low-degree polynomial approximation to $\log(3 - x)$ on the interval $[-2\sqrt{2}, 2\sqrt{2}]$. We can find good higher-degree approximations using the Fourier series for $\log(3 - \sqrt{2}(e^{2\pi i\theta} - e^{-2\pi i\theta}))$.

Quantitative estimates with exceptions

To obtain lower-degree estimates (e.g., bounds on $T_{A,2}$ alone), we again should allow a finite number of exceptions.

For any integer polynomial $P(x)$ with $P(3 - \alpha_i + \overline{\alpha_i}) \neq 0$, the resultant of P with $\prod_{i=1}^{g}(x - (3 - \alpha_i - \overline{\alpha_i}))$ is a nonzero integer. Hence

$$\sum_{i=1}^{g} \log(x - (3 - \alpha_i - \overline{\alpha_i}) \geq 0.$$

Sample application: if $\pm\sqrt{2}$ are not roots of $P_A(x)$, then

$$T_{A,2} \geq 0.4752g - 2.2523 \log m.$$

The class of optimization problems arising here has a long history in algebraic number theory, dating back to its role in the study of totally positive algebraic integers with small trace (the **Schur–Siegel–Smyth problem**).

Closing thoughts

For small g, we have tabulated the Weil polynomials corresponding to simple abelian varieties of dimension g over $\mathbb{F}_2$ of order 2. (We use some of the aforementioned estimates to truncate the search, but it seems difficult to go further.)

g	1	2	3	4	5	6	7	8	9	10	11
Count	1	3	4	10	9	28	24	54	50	86	63

What is the asymptotic behavior here? And is it feasible to use analytic arguments to get lower bounds? (We are looking for lattice points in small misshapen regions.)

One partial result: the count is always positive (for order 2, and for some other fixed orders). For more details, come to Tahiti...