Totally positive integers of small trace and extreme orders of abelian varieties over finite fields

Alexander Smith

29 June 2021

Defining absolute trace

An *algebraic integer* α is a complex root to a monic polynomial

$$P(z) = z^d + a_{d-1}z^{d-1} + \cdots + a_0$$

with $a_0, \ldots, a_{d-1}$ rational integers.
Assume that this polynomial is irreducible, and take $\alpha_1 = \alpha, \ldots, \alpha_d$ to be its complex roots. We call α *totally positive* if these roots are all positive real numbers. We define the *absolute trace* of α by

$$\text{a.tr}(\alpha) = \frac{1}{d}(\alpha_1 + \cdots + \alpha_d) = -\frac{a_{d-1}}{d}.$$

Question

How small can the absolute trace of a totally positive algebraic integer be?

Totally positive algebraic integers with small absolute trace

For the polynomial $z - 1$, we have

$$\text{a.tr}(1) = \frac{1}{1}(1) = 1.$$

This is the limit: suppose the integral irreducible degree d polynomial P has real positive roots $\alpha_1, \ldots, \alpha_d$. Then, by the AM-GM inequality,

$$\text{a.tr}(\alpha_1) = \frac{1}{d}(\alpha_1 + \cdots + \alpha_d) \geq (\alpha_1 \ldots \alpha_d)^{1/d} = |P(0)|^{1/d}.$$

Since $P(0)$ is an integer, and since 0 is not a root of P, we can conclude that $\text{a.tr}(\alpha_1) \geq 1$.

Totally positive algebraic integers with small absolute trace

Some other examples:

- A root α of
$$z^2 - 3z + 1 \approx (z - .3820)(z - 2.6180)$$
has $\mathrm{a.tr}(\alpha) = 3/2$.
- A root α of
$$z^3 - 5z^2 + 6z - 1 \approx (z - .1981)(z - 1.5550)(z - 3.2470)$$
has $\mathrm{a.tr}(\alpha) = 5/3$.
- A root α of
$$z^4 - 7z^3 + 13z^2 - 7z + 1 \quad \text{or of}$$
$$z^4 - 7z^3 + 14z^2 - 8z + 1$$
has $\mathrm{a.tr}(\alpha) = 7/4$.

Best previous bound on absolute trace

Theorem (Liang–Wu, '11)

If α is a totally positive algebraic integer, then it is either one of the examples we have already mentioned, or

$$\mathrm{a.tr}(\alpha) \geq 1.79193.$$

On the other hand, for any odd prime q, the totally positive algebraic integer $\alpha_q = 4\cos^2(\pi/q)$ satisfies $\mathrm{a.tr}(\alpha_q) = 2 - 2/(q-1)$, so there are infinitely many totally positive algebraic integers with absolute trace < 2.

The Schur–Siegel–Smyth trace problem

For a given λ in $(0, 2)$, show that there are finitely many totally positive algebraic integers with absolute trace at most λ.

Progress on the Schur–Siegel–Smyth trace problem

Theorem (S. '21)

If α *is a totally positive algebraic integer, then the inequality*

$$\mathrm{a.tr}(\alpha) > \lambda$$

holds for $\lambda = 1.802$ *with finitely many exceptions.*

Timeline for bounds on a.tr

The bound λ	Reference
1.6487	Schur (1918)
1.7336	Siegel (1945)
1.7719	Smyth (1984)
1.7783786	McKee and Smyth (2004)
1.784109	Aguirre and Peral (2008)
1.78702	Flammang (2009)
1.79193	Liang and Wu (2011)
1.802	S. (2021)

The resultant

Suppose P is a degree d-integer polynomial. We have already noted $P(0)$ is an integer. Some similar examples include:

- $P(-1)$ and $P(2)$ are integers
- $3^d P(1/3)$ is an integer
- $P(i)P(-i)$ is an integer

More generally, if $Q(z) = b_e(z - \beta_1)\ldots(z - \beta_e)$ is an integral polynomial, then the *resultant*

$$\text{res}(Q, P) = b_e^d P(\beta_1)\ldots P(\beta_d)$$

is an integer.

The Smyth approach to the Schur–Siegel–Smyth trace problem

Smyth pioneered an approach to the trace problem that just uses this fact about resultants; this is the only approach to the problem that has improved the bound since. These results fit in the following template:

Theorem

Take λ, N from any row of the table on the next slide. There is then an explicit list of N irreducible integer polynomials $Q_1, \ldots, Q_N$ so that, if a given real polynomial

$$P(z) = (z - \alpha_1)(z - \alpha_2) \ldots (z - \alpha_d)$$

has positive roots and satisfies $|\text{res}(Q_i, P)| \geq 1$ for all $i \leq N$, then the roots must also satisfy

$$\tfrac{1}{d}(\alpha_1 + \cdots + \alpha_d) > \lambda.$$

The Smyth approach to the Schur–Siegel–Smyth trace problem

The bound λ	Polynomial count N	Reference
1.0	1	Folklore use of AM-GM
1.7719	≈ 15	Smyth (1984)
1.7783786	18	McKee and Smyth (2004)
1.780022	24	Aguirre, Bilbao and Peral (2006)
1.783622	28	Aguirre and Peral (2007)
1.784109	31	Aguirre and Peral (2008)
1.78702	35	Flammang (2009)
1.78839	70	McKee (2011)
1.79193	86	Liang and Wu (2011)

What can we use besides the resultant?

We can use the discriminant; the discriminant of the monic polynomial $P(z) = (z - \alpha_1) \dots (z - \alpha_d)$ is defined by

$$\Delta(P) = \prod_{1 \le i < j \le d} (\alpha_i - \alpha_j)^2.$$

If P is an integer polynomial, this is an integer. If P is also squarefree, we have $|\Delta(P)| \geq 1$.

Discriminant information is not so useful in small degrees, but becomes increasingly useful as d increases.

Polynomials to measures

Given complex numbers $\alpha_1, \ldots, \alpha_d$, we associate the polynomial $P(z) = (z - \alpha_1) \ldots (z - \alpha_d)$ with the probability measure μ_P defined by

$$\mu_P(Y) = \frac{1}{d} \cdot \#(Y \cap \{\alpha_1, \ldots, \alpha_d\}).$$

This is a Borel measure on $\mathbb{C}$.
For any polynomial Q, we have

$$\frac{1}{d} \log |\mathrm{res}(P, Q)| = \frac{1}{d} \sum_{i \leq d} \log |Q(\alpha_i)| = \int_{\mathbb{C}} \log |Q(z)| d\mu_P(z).$$

We also have

$$\frac{1}{d}(\alpha_1 + \cdots + \alpha_d) = \int_{\mathbb{C}} z \, d\mu_P(z).$$

Polynomials to measures

For any Borel probability measure μ on $\mathbb{C}$ with compact support, we define

$$\text{log.res}(\mu, Q) = \int_{\mathbb{C}} \log|Q(z)|\,d\mu(z) \quad \text{and} \quad \text{a.tr}(\mu) = \int_{\mathbb{C}} z\,d\mu(z).$$

If $\mu = \mu_P$, where P is an irreducible monic integer polynomial , we have

$$\text{log.res}(\mu, Q) \geq 0 \quad \text{for } Q \text{ an integer polynomial unless } P|Q.$$

Additionally, if α is a totally positive root of P, then $\text{a.tr}(\mu) = \text{a.tr}(\alpha)$.

Discriminant of a measure

For any Borel probability measure μ on $\mathbb{C}$ with compact support, we define

$$\log.\Delta(\mu) = \int\int \log|z - w| d\mu(z) d\mu(w).$$

This is $-\infty$ for any measure coming from a polynomial; however, if $Q_1, Q_2, \ldots$ is a sequence of squarefree monic integer polynomials, and if the measures $\mu_{Q_1}, \mu_{Q_2}, \ldots$ converge in an appropriate sense to the Borel measure μ, then

$$\log.\Delta(\mu) \geq 0.$$

The implications from measures

Proposition

Choose $\lambda > 0$ *and a finite list of integer polynomials* $Q_1, \ldots, Q_N$. *Suppose that every Borel measure* μ *on* $[0, \infty]$ *satisfying*

$$\text{log.}\Delta(\mu) \geq 0, \quad \text{log.res}(\mu, Q_i) \geq 0$$

also satisfies $\text{a.tr}(\mu) > \lambda$. *Then there are finitely many totally positive algebraic integers* α *that satisfy*

$$\text{a.tr}(\alpha) \leq \lambda.$$

Our goal is to minimize $\text{a.tr}(\mu)$ subject to the discriminant condition and some set of resultant conditions

Schur's result

Proposition (Schur 1918)

Suppose a given probability measure μ on $[0,\infty]$ satisfies $\log.\Delta(\mu) \geq 0$. *Then*

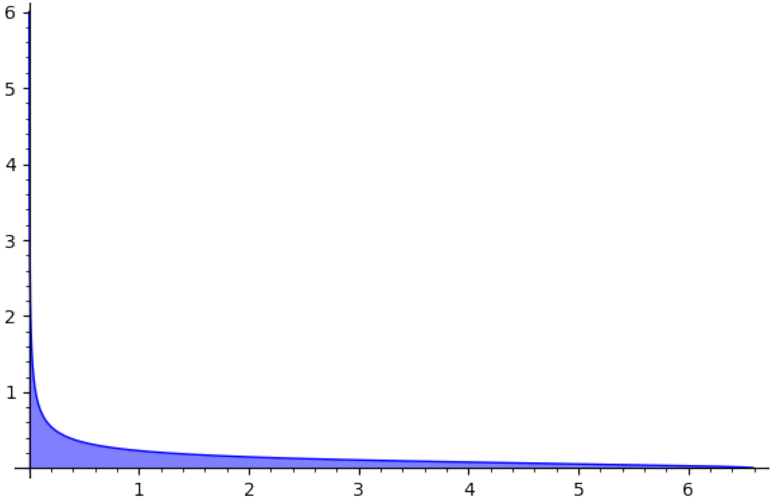
$$\mathrm{a.tr}(\mu) \geq e^{1/2} \approx 1.6487.$$

So, for any $\epsilon > 0$, we conclude that there are finitely many totally positive algebraic integers satisfying $\mathrm{a.tr}(\alpha) \leq e^{1/2} - \epsilon$.
The probability measure

$$d\mu(x) = \frac{1}{2e^{1/2}\pi}\sqrt{\frac{4e^{1/2} - x}{x}}dx$$

is the unique measure for which this inequality is sharp.

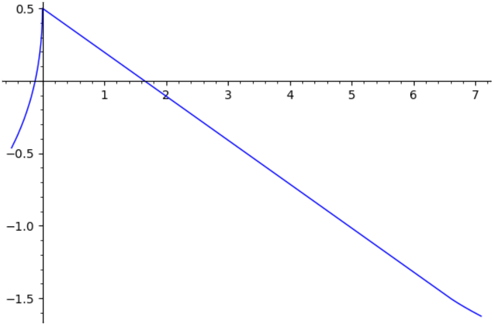
Schur's distribution



The potential of Schur's distribution

With μ as above, we define the potential U^μ of μ on $\mathbb{C}$ by

$$U^\mu(z) = -\int \log|z-w| d\mu(z).$$



Siegel's result

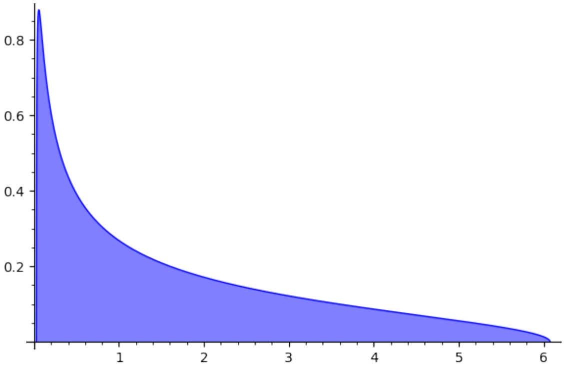
Proposition (Siegel 1945)

Suppose the probability measure μ *on* $[0,\infty]$ *satisfies* $\mathrm{log.}\Delta(\mu) \geq 0$ *and* $\mathrm{log.res}(\mu, z) \geq 0$*. Then*

$$\mathrm{a.tr}(\mu) > 1.7336.$$

This implies that there are finitely many totally positive algebraic integers of absolute trace at most 1.7336

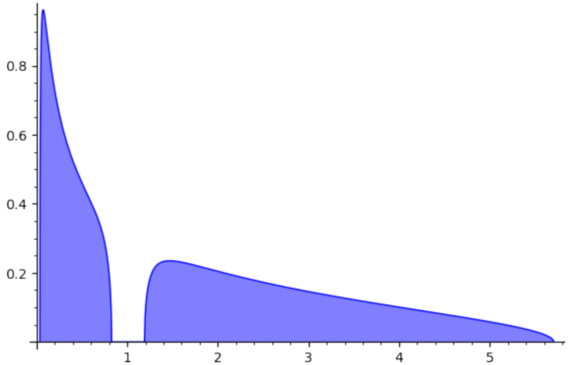
Siegel's optimal measure



Density approximately proportional to

$$\frac{\sqrt{(x-0.028)(6.01-x)}}{x}$$

Add the restriction log.res$(\mu, z-1) \geq 0$

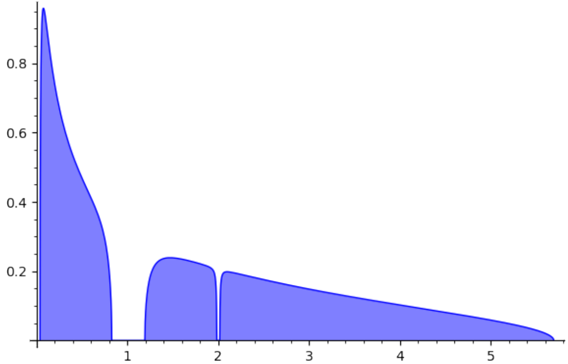


Density approximately proportional to

$$\frac{\sqrt{(x-0.036)(.828-x)(x-1.19)(5.71-x)}}{x(x-1)}$$

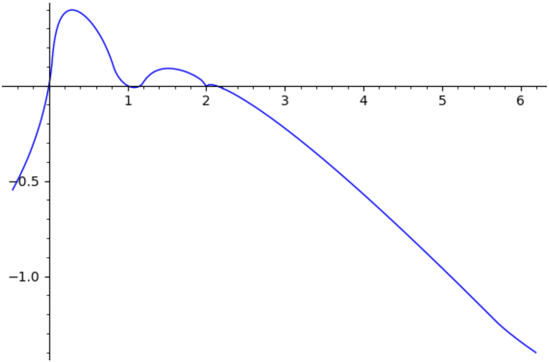
Shows that a.tr$(\alpha) > 1.7773$ with finitely many exceptions.

Add the restriction log.res$(\mu, z-2) \geq 0$

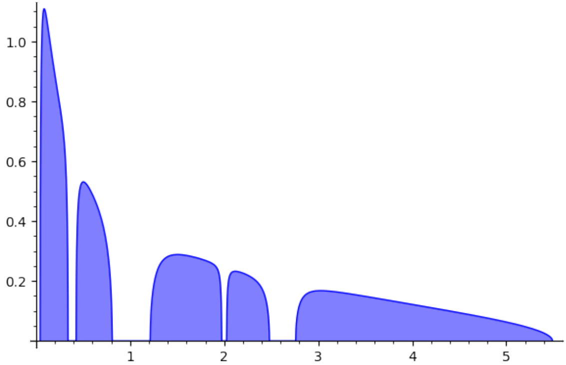


Shows that a.tr$(\alpha) > 1.7778$ with finitely many exceptions.

The potential of this measure

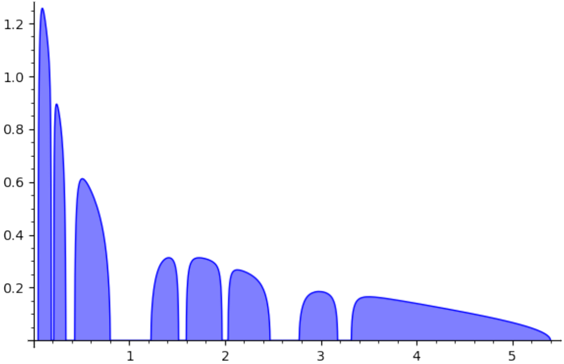


Add the restriction log.res$(\mu, z^2 - 3z + 1) \geq 0$



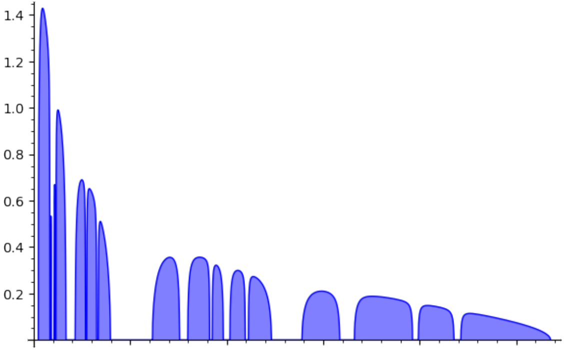
Shows that a.tr$(\alpha) > 1.7941$ with finitely many exceptions, beating the prior best bound.

Add the restriction log.res($\mu, z^3 - 5z^2 + 6z - 1) \geq 0$



Shows that a.tr(α) > 1.7999 with finitely many exceptions

Add restrictions for the two exceptional quartics



Shows that a.tr$(\alpha) > 1.8021$ with finitely many exceptions

The road to 2

We cannot extend this method more than a couple hundreths beyond 1.8021.
I do not currently think this reflects a limitation of the method.

Conjecture

Take μ to be a Borel probability measure supported on a compact subset Σ of $\mathbb{R}$. Suppose

$$\text{log.res}(\mu, Q) \geq 0 \quad \textit{for all nonzero integer polynomials } Q.$$

Then there is a sequence of monic integer polynomials $P_1, P_2, \ldots$ with roots in Σ so $\mu_{P_1}, \mu_{P_2}, \ldots$ have limit μ.

Serre's result

The first person who realized that Smyth's method could not solve the trace problem for $\lambda < 2$ was Serre. His proof used potential theory, and took advantage of the fact that, for an integral polynomial P, $|P(0)|$ is either 0 or at least 1.

Proposition

There is a Borel probability distribution approximately given by

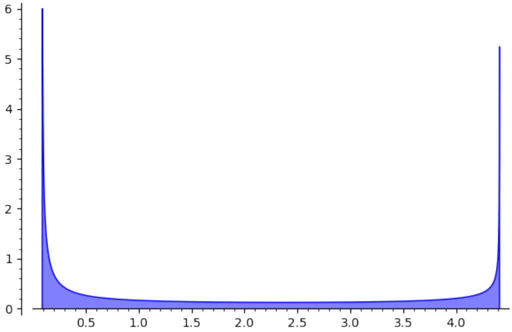
$$d\mu(x) = \frac{.25x + .043}{x\sqrt{(4.41 - x)(x - 0.087)}}dx \quad \textit{on} \ \approx [.087, 4.41]$$

satisfying

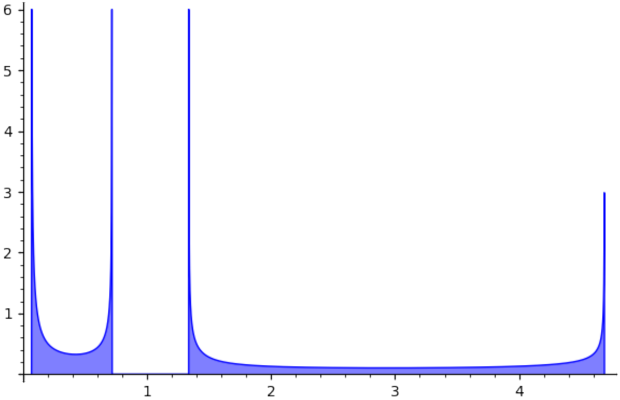
- $\text{log.res}(\mu, z) \geq 0$*;*
- $\text{log.res}(\mu, P) \geq 0$ *for any complex polynomial* P *with* $|P(0)| \geq 1$*; and*
- $\text{a.tr}(\mu) \approx 1.898$*.*

More on this measure

In particular, this measure satisfies log.res$(\mu, P) \geq 0$ for any nonzero integer polynomial P.
If the above conjecture holds, it would imply a.tr$(\alpha) < 1.9$ holds for infinitely many α .

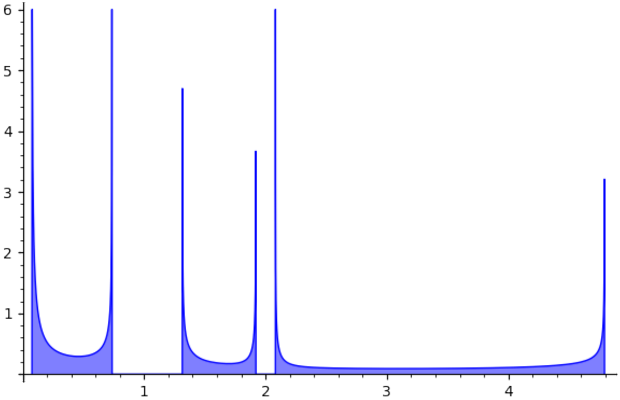


Using the value at 1



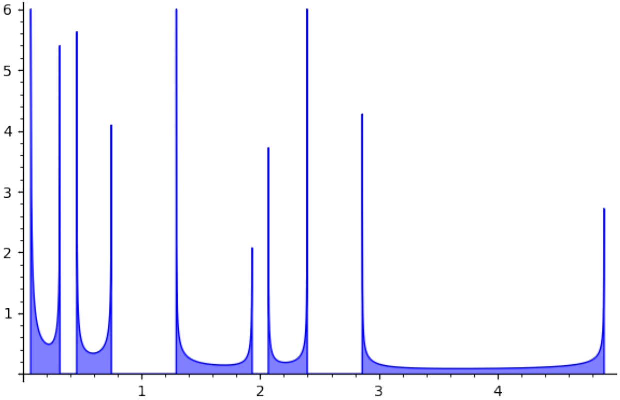
This measure has a.tr$(\mu) \approx 1.847$.

Using the value at 2



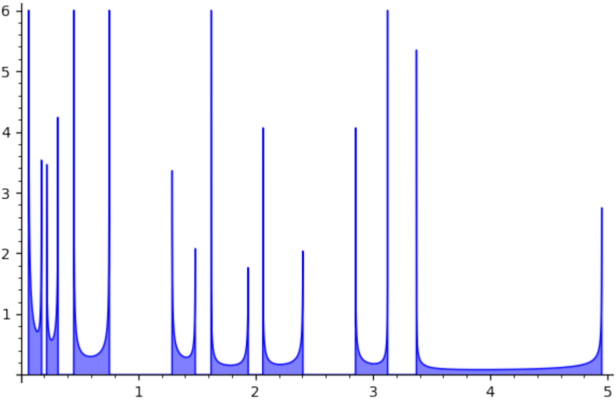
This measure has a.tr(μ) ≈ 1.836.

Using the resultant with $z^2 - 3z + 1$



This measure has $\text{a.tr}(\mu) \approx 1.820$.

Using the resultant with $z^3 - 5z^2 + 6z - 1$



This measure has $\text{a.tr}(\mu) \approx 1.817$.

Conjecture

There are infintely many totally positive algebraic integers with absolute trace at most 1.818*.*

Connection to abelian varieties over finite fields

Choose a prime power q, and take P to be a monic integer polynomial with all roots in the interval $[-2\sqrt{q}, 2\sqrt{q}]$. As a consequence of the Honda–Tate theorem, there is an abelian variety $A/\mathbb{F}_q$ so

$$\#A(\mathbb{F}_q)^{1/\dim A} = P(q+1)^{1/\deg(P)}.$$

Theorem (van Bommel– Costa– Li– Poonen–S.)

Fix a prime power q. Then, for n sufficiently large, every integer in the interval

$$\left[\left(q - 2q^{1/2} + 3 - q^{-1}\right)^n, \left(q + 2q^{1/2} - 3 - q^{-1}\right)^n\right]$$

is the order of a geometrically simple ordinary principally polarized abelian variety of dimension n over $\mathbb{F}_q$.

Our main goal

With q fixed and n tending to infinity, we would like to better understand how far $\#A(\mathbb{F}_q)$ can be beyond endpoints of the interval given above for $A/\mathbb{F}_q$ a simple n-dimensional abelian variety.

Here, our work is more incomplete.

The corresponding problem on Borel measures

Problem

For a fixed q *and a fixed list of integer polynomials* $Q_1, \ldots, Q_N$, *determine the probability measure* μ *on* $[-2\sqrt{q}, 2\sqrt{q}]$ *for which* $\mathrm{log.res}(\mu, q+1-z)$ *is maximized/minimized, subject to the restrictions*

$$\mathrm{log}.\Delta(\mu) \geq 0 \quad \textit{and} \quad \mathrm{log.res}(\mu, Q_i) \geq 0 \textit{ for } i \leq N.$$

For a fixed q and list of polynomials $Q_1, \ldots, Q_N$, this can be attacked using the same techniques that worked for the trace problem.

A natural Q_1 for the minimization problem would be $z - \lfloor 2\sqrt{q} \rfloor$. The effect of the restriction $\mathrm{log.res}(\mu, Q_1) \geq 0$ on μ then depends heavily on $2\sqrt{q}$ mod 1. On the other hand, the discriminant condition has no such cyclical behavior.

The case of square q

In the case where q is a square, $2\sqrt{q}$ is an integer. The limit over square q actually returns to the trace problem.

Theorem (S.)

Fix an square prime power q. For sufficiently large n, there is no simple abelian variety $A/\mathbb{F}_q$ of dimension n satisfying

$$\#A(\mathbb{F}_q) \leq (q - 2q^{1/2} + 1 + 1.802)^n \quad \textit{or}$$
$$\#A(\mathbb{F}_q) \geq (q + 2q^{1/2} + 1 - 1.802)^n.$$

On the other hand, if our above conjecture holds, then there is a simple abelian variety $A/\mathbb{F}_q$ of dimension n satisfying

$$\#A(\mathbb{F}_q) \leq (q - 2q^{1/2} + 1 + 1.817)^n$$

and another satisfying

$$\#A(\mathbb{F}_q) \geq (q + 2q^{1/2} + 1 - 1.817)^n.$$

Thank you!