Angle Ranks of Abelian Varieties

David Zureick-Brown (Amherst College)
with Taylor Dupuy
and Kiran Kedlaya

Alladi 70th birthday conference

March 19, 2026

Slides available at https://dmzb.github.io/

$$\Gamma := \langle \alpha_1, \ldots, \alpha_n \rangle \subset \overline{\mathbb{Q}}^*$$

Let $f(x) \in \mathbb{Z}[x]$ be monic, with nonzero roots $\alpha_1, \ldots, \alpha_n$.

Definition

$$\overline{\mathbb{Q}}^* \supset \Gamma := \langle \alpha_1, \ldots, \alpha_n \rangle \cong \mathbb{Z}^r \oplus T.$$
$$S^1 \supset \Gamma' := \langle \theta_1, \ldots, \theta_n \rangle \cong \mathbb{Z}^\delta \oplus T \qquad \left(\alpha_j = r_j e^{i\theta_i}\right)$$

Example

- $\Phi_n(x)$ cyclotomic $\Rightarrow \boxed{r = 0}$
- $x^n - b \Rightarrow \boxed{\text{r = 0 } or \text{ 1}}$.

Lemma

If $n > 3$ and $\operatorname{Gal} f \cong S_n$, then $\boxed{r = n \text{ or } n-1}$.

Proof.

Suppose $\alpha_1^{A_1} \cdots \alpha_n^{A_n} = 1$.

Apply $\tau = (ij)$ and divide to get $\left(\frac{\alpha_i}{\alpha_j}\right)^{A_i - A_j} = 1$. □

Weil Polynomials. Let $q = p^n$.

Definition

A q-*Weil Polynomial* $f(x) \in \mathbb{Z}[x]$ is a **monic** polynomial of **even degree** such that **all roots have complex absolute value** $\sqrt{q}$.

Definition

A q-*Weil number* α is a root of a q-Weil polynomial.

Roots

$$\alpha_1, \overline{\alpha_1}, \ldots, \alpha_g, \overline{\alpha_g} \in \overline{\mathbb{Z}}$$

$$\alpha_i \cdot \overline{\alpha_i} = q$$

Ranks

1. $r \leq g + 1$
2. $\delta = r - 1 \leq g$

Let $A/\mathbb{F}_q$ be an Abelian Variety of dimension g

Weil Conjectures.

1. Let $P_A(x)$ be the characteristic polynomial $P_A(x)$ of $F \in \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell A)$
2. Then $P_A(x)$ is a q-Weil polynomial.
3. $A(\mathbb{F}_q^n) = (\alpha_1^n + \overline{\alpha_1}^n + \cdots + \alpha_g^n + \overline{\alpha_g}^n) - \left(\alpha_1^n \alpha_2^n + \cdots + \alpha_{g-1}^n \alpha_g^n\right) + \cdots + q^g$

"Linear algebra"

$H^i(A) \cong \wedge^i H^1(A)$

Theorem (Honda tate)

The map

$$\left\{ \begin{array}{c} \textit{isogeny classes of} \\ \textit{simple abelian varieties over } \mathbb{F}_q \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \textit{conjugacy classes of} \\ q\textit{-Weil numbers} \end{array} \right\}$$

$$\textit{isogeny class of } A \longmapsto \textit{the set of zeros of } P_A(x)$$

is a bijection.

Galois group of a Weil Polynomial $f(x)$

Roots

$$\alpha_1, \overline{\alpha_1}, \ldots, \alpha_g, \overline{\alpha_g} \in \overline{\mathbb{Z}}$$

$$\alpha_i \cdot \overline{\alpha_i} = q$$

Definition

$W_{2g} = \mathrm{Aut}\{\{1, \overline{1}\}, \{2, \overline{2}\}, \ldots, \{g, \overline{g}\}\} \subset S_{2g}$

$$\begin{tikzcd} C \arrow[r, hook] \arrow[d, hook] & G \arrow[r, two heads] \arrow[d, hook] & \overline{G} \arrow[d, hook] \\ \mathbb{F}_2^g \arrow[r, hook] & W_{2g} \arrow[r, two heads] & S_g \end{tikzcd}$$

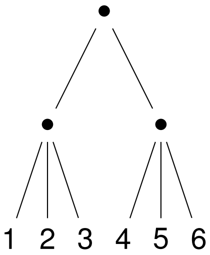
1. C is a **linear code**
2. C and $\dim_{\mathbb{F}_2} C$ are invariants of f (and A)

Theorem (Dupuy–Kedlaya–Zureick-Brown)

If $\#C > 2$, f is irreducible, and $G = \mathrm{Gal}\, f(x)$ is primitive, then $\boxed{\delta = g}$.

Definition

1. **Primitive** means “no blocks”.
2. A “**Block**” is $B \subset \{\alpha_1, \overline{\alpha_1}, \ldots, \alpha_g, \overline{\alpha_g}\}$ such that $1 < |B| < 2g$ and such that for all $\sigma \in G$, $S \cap \sigma(B) = B$ or $\emptyset$.



$\mathrm{Aut}\, T \subset \{1, \ldots, 6\}$ is transitive, but not primitive.

$B = \{1, 2, 3\}$ is a block.

Theorem (Dupuy–Kedlaya–Zureick-Brown)

We construct a representation $V \in$ Rep G such that $\dim V = \delta$.

This recovers all previous work.

1. [Tankeev]: g prime $\Rightarrow \delta \in \{1, g-1, g\}$.
2. [Lenstra–Zarhin]: A “almost ordinary” $\Rightarrow \delta \in \{g-1, g\}$.
3. [DKZB]: If f is irreducible and $C = \mathbb{F}_2^g$, then $\delta = g$.

Database of Weil polynomials (Dupuy–Kedlaya–Roe–Vincent)

1. Many improved tools for fast computation
2. Disproof of Shparlinski’s conjecture (ordinary $\Rightarrow \delta = g$).

Why Bother?

1. The **Tate Conjecture** is true for all powers of such A.
2. **Arithmetic Statistics**: distribution of $\#A(\mathbb{F}_q^n)$ (Arango—Bhadmidipati–Sankar)
3. **Inverse Galois** for Weil polynomials (Arango–Frengly–Vemulapalli)
4. More new cases of the **Tate Conjecture** (Arango–Frengly–Vemulapalli)

Observations

(0) If $\prod \alpha_i^{A_i} = q^N$, then $\prod \overline{\alpha}_i^{A_i} = q^N$

(1) Let $\beta_i = \alpha_i / \overline{\alpha_i}$, and divide (0) to get $\prod \beta_i^{A_i} = 1$

(2) Applying v_q gives $\sum A_i v_q(\beta_i) = 0$.

Let $\sigma \in G$.

(3) If $\prod \beta_i^{A_i} = 1$, then $\prod \sigma(\beta_i)^{A_i} = 1$, so $\boxed{\sum A_i v_q(\sigma(\beta_i)) = 0}$.

Main point: the converse holds [Zarhin, Zywina]

If $A_1, \ldots, A_g \in \mathbb{Z}$ satisfy (3) for all $\sigma \in G$, then

$$\prod \beta_i^{A_i} = \zeta.$$

“Newton hyperplane” representation

(3) If $\prod \beta_i^{A_i} = 1$, then $\prod \sigma(\beta_i)^{A_i} = 1$, so $\boxed{\sum A_i v_q(\sigma(\beta_i)) = 0}$.

$$M = (v_q(\sigma(\beta_j))) = \begin{pmatrix} v_q(\beta_1) & v_q(\beta_2) & \cdots & v_q(\beta_g) \\ v_q(\sigma(\beta_1)) & v_q(\sigma(\beta_2)) & \cdots & v_q(\sigma(\beta_g)) \\ \vdots & \vdots & \ddots & \vdots \\ v_q(\sigma'(\beta_1)) & v_q(\sigma'(\beta_2)) & \cdots & v_q(\sigma'(\beta_g)) \end{pmatrix}$$

$\mathbb{Q}^g \supset V = \text{Span}\,\langle v_q(\sigma(\overline{\beta})) : \sigma \in G \rangle$

Proposition (Let $\overline{A} = (A_1, \ldots, A_g)$)

$\prod \beta_i^{A_i} = 1 \Leftrightarrow M \cdot \overline{A} = 0$

Corollary

$\delta = \operatorname{rank} M = \dim_{\mathbb{Q}} V.$

Example with G cyclic and A ordinary

Suppose that $\#C = 2$, and $G \cong \langle \sigma = (123456) \rangle$.
Re-index the roots so that σ acts as (123456). Then both

$$v_q(\overline{\beta}) = (1, 1, 1, -1, -1, -1) \text{ or } (1, -1, 1, -1, 1, -1) \text{ are possible.}$$

In the first case, $\delta = 6$, and in the second case, $\delta = 2$

One can't "simultaneously choose" coordinates for both Σ and v_q.

Sample Corollary

Suppose that $\#C = \mathbb{F}_2^g$ and f is irreducible. Then $\delta = g$.

Proof.

Note that for any $e_i \in C$, $e_i(\beta_j) = \beta_j^{(-1)^{\delta_{i,j}}}$.

Thus $v_q(e_i(\beta_j)) = (-1)^{\delta_{i,j}} v_q(\beta_j)$.

Now, if $(a_1, \ldots, a_j, \ldots, a_g) \in V$, then $(a_1, \ldots, -a_j, \ldots, a_g) \in V$. $\square$

Thank You!

$$\langle \alpha_1, \ldots, \alpha_n \rangle \subset \overline{\mathbb{Q}}^*$$

$$\begin{tikzcd} C \arrow[r, hook] \arrow[d, hook] & G \arrow[r, two heads] \arrow[d, hook] & \overline{G} \arrow[d, hook] \\ \mathbb{F}_2^g \arrow[r, hook] & W_{2g} \arrow[r, two heads] & S_g \end{tikzcd}$$

$$\begin{pmatrix} v_q(\beta_1) & v_q(\beta_2) & \cdots & v_q(\beta_g) \\ v_q(\sigma(\beta_1)) & v_q(\sigma(\beta_2)) & \cdots & v_q(\sigma(\beta_g)) \\ \vdots & \vdots & \ddots & \vdots \\ v_q(\sigma'(\beta_1)) & v_q(\sigma'(\beta_2)) & \cdots & v_q(\sigma'(\beta_g)) \end{pmatrix}$$

Proposition (Let $\overline{A} = (A_1, \ldots, A_g)$)

$\prod \beta_i^{A_i} = 1 \Leftrightarrow M \cdot \overline{A} = 0$

Corollary

$\delta = \operatorname{rank} M = \dim_{\mathbb{Q}} V.$

Tate conjecture

1. **Tate Conjecture**: $H^{2j}(A)(q^j)$ is algebraic
2. **Theorem**: $H^2(A)(q)$ is algebraic

1. $H^i(A) = \wedge^i H^1(A)$

1. If $H^{2j}(A)(q^j) = \wedge^i H^2(A)(q)$, then the Tate Conjecture is true.
2. This can fail, and such a class in $H^{2j}(A)(q^j)$ which does not come from degree 2 is called **exceptional**.

1. $\delta = g$ implies that there are no exceptional classes.
2. Idea: if $\alpha_i^2 \alpha_j^2 = q^2$, then there is an exceptional class in the image of
$$H^2(A)(\alpha_j^2) \wedge H^2(A)(\alpha_j^2) \to H^4(A)(q^2)$$
(see Zarhin).

Lemma: one can uniquely partition

$$\{1,\ldots,g\} = \bigsqcup_{i=1}^{m} T_i \text{ such that}$$

$\sigma \in C$ is constant on each T_i and each T_i is maximal for this property.

Write:

$$\mathbb{Q}^g = \bigoplus_{i=1}^{m} \mathbb{Q}^{\oplus T_i}$$

Corollary: suppose that $g > 1$ and set $g' = g/m$.

Then $\delta = im$ for some $i \in \{1,\ldots,g'\}$; $\delta \geq m$.

When $\overline{G}$ is not primitive, analyze $H_i = \mathrm{Stab}_{\overline{G}}\, T_i$

Theorem

1. *If g/m is prime, then $\delta \in \{m, g-m, g\}$.*
2. *If H_i acts 2-transitively on T_i, then $\delta \in \{g, g-m\}$.*