Frobenius on the first étale cohomology

Madhavan Venkatesh
with Diptajit Roy and Nitin Saxena

IIT Kanpur

ANTS XVI, July 2024

Theorem (M.V. , Diptajit Roy, Nitin Saxena)

Let $X \subset \mathbb{P}^N$ be a smooth projective variety over $\mathbb{F}_q$ of degree D and let $P_1(X/\mathbb{F}_q, T) := \det(1 - TF_q^\star \mid \mathrm{H}^1(X, \mathbb{Q}_\ell))$. There exists:

- randomised algorithm to compute $P_1(X/\mathbb{F}_q, T)$ for fixed D in time $O((\log q)^\Delta)$,
- quantum algorithm to compute $P_1(X/\mathbb{F}_q, T)$ in time polynomial in $D \log q$. Can also certify (in the sense of Arthur-Merlin protocols) with similar time complexity.

Above algorithms, in surface case, also output second Betti number.

Algorithm

- Reduce to surface-case via weak-Lefschetz.
- Let $(X_t)_{t\in\mathbb{P}^1}$ be a Lefschetz pencil of hyperplane sections on X.
- Sample smooth curves X_{u_1}, X_{u_2} for $u_1, u_2 \in \mathbb{F}_Q$, poly-bounded extn.
- Compute their zeta functions and take gcd of the numerators. With high prob this is $P_1(X/\mathbb{F}_Q, T)$. Recover $P_1(X/\mathbb{F}_q, T)$ from many such using Kedlaya's recipe.

Proof

- Big mod-ℓ monodromy of vanishing cycles.
- Equidistribution of Frobenius mod-ℓ.