Statistics of random hypersurfaces (mod p)

Victor Wang

January 4, 2021 Tea

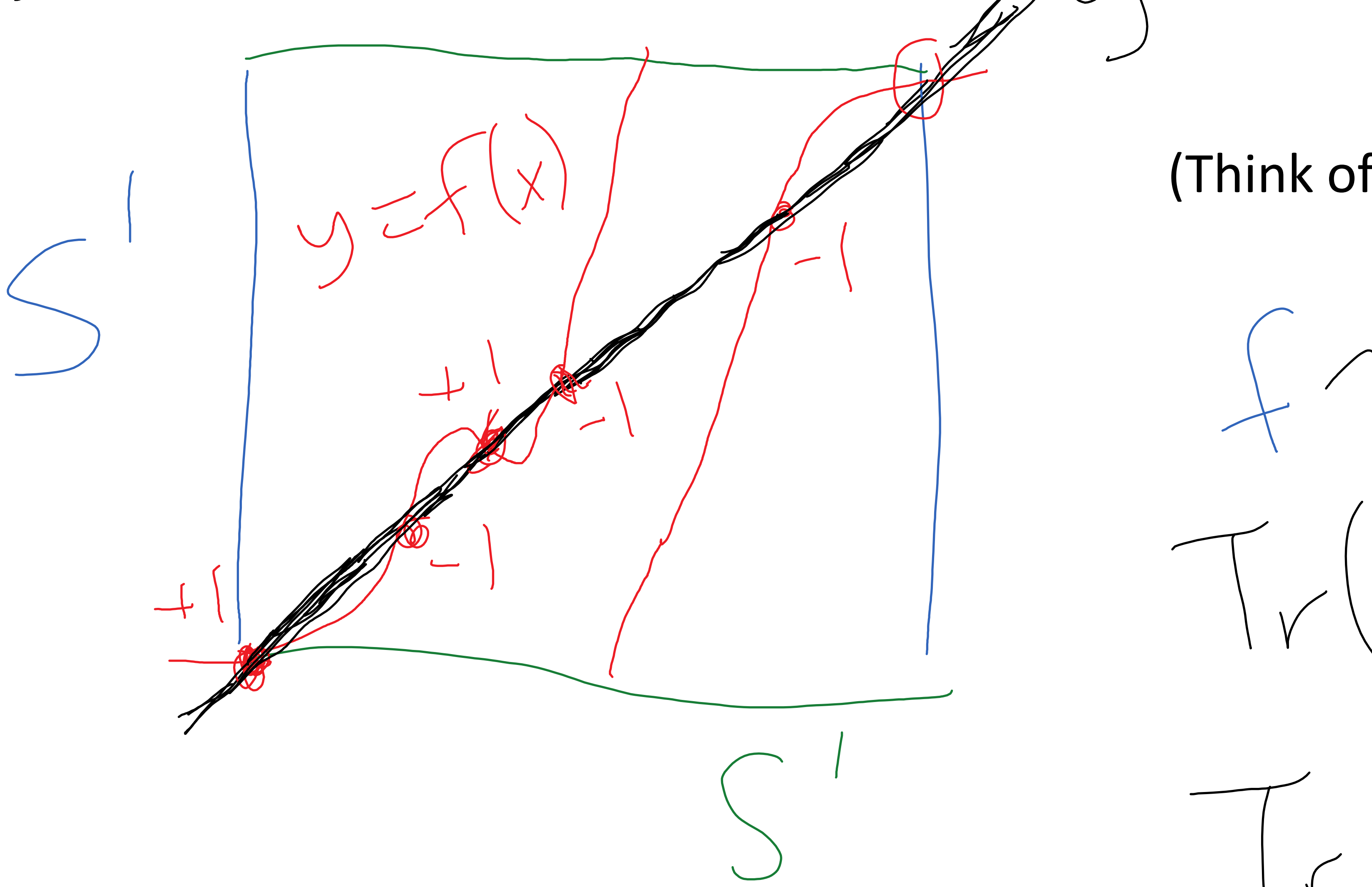
Last modified: 2021-09-19

LTF: Point counts vs. (co-)homology actions

- Note that $X(F_p) = Fix\left[Frob_p \mid X\left(\overline{F_p}\right)\right]$.[!]
- So, we can count points using the (Grothendieck–)**Lefschetz fixed-point formula (LTF)**: $Fix[-] = \sum(-1)^i \cdot Tr\left(Frob_p \,\middle|\, H_c^i\left(X \times \overline{F_p}\right)\right)$.
- Why (co-)homology? To visualize fixed points, we can intersect the "graph" of $Frob$, with the "diagonal":
- $Fix\left[Frob_p \mid X\left(\overline{F_p}\right)\right] = \{(x, y)\colon\ y = Frob_p(x)\} \cap \{(x, y)\colon\ x = y\}$.
- If you imagine "wiggling" or "deforming" $Frob_p$, then the RHS should stay the same. This is morally why (co-)homology comes up in the LTF.

[!] I will be loose with notation in these slides; consult other references for more careful notation.

Let $f: S^1 \to S^1$ be continuous.



(Think of S^1 as “reals mod 1”.)

$f \sim 2x$

$Tr(f|_{H_0(S^1)}) = 1$

$Tr(f|_{H_1(S^1)}) = 2$

The (signed) number of fixed points is detected by $f \mid H_*(S^1)$:
here $+1 - 1 + 1 - 1 - 1 = Tr(f \mid H_0) - Tr(f \mid H_1)$.

Assumption for rest of talk: Projectivity

- For simplicity, I will always work with projective varieties (this is morally a “compactness” assumption; cf. topological spaces).
- In principle, non-projective cases can be reduced to projective cases.
- Ex: Counting points on $x^2 + y^2 = 1$ boils down to $x^2 + y^2 = z^2$ plus a separate analysis of $x^2 + y^2 = 0$. (The latter two are projective.)
- (Whereas a smooth projective conic always has exactly $p + 1$ points $mod\ p$, the answer for a smooth affine conic is messier.)

Role of smoothness in Weil conjectures (given projectivity)

- (*Neither* is important for "rationality" of the local zeta function.)
  - (Point counts for a variety over $F_p, F_{p^2}, \ldots$ always satisfy a linear recurrence. The LTF always applies in some form.)
- "Comparing" cohomology of X_{F_p} and X_C, if X has an integral model.
  - *Non-example*: $x^2 - y^2 + (pz)^2 = 0$ is irred.$/C$, but not $/F_p$ (for odd p). So, $\dim H^2$'s differ, either by an indirect point-counting argument, or in principle directly…
- Poincare "duality".
  - Morally, "diff. forms" only "pair cleanly" on smooth (i.e., locally "$\approx$ linear") spaces.
- "Purity" of the action of $Frob_q \mid H^i\left(X \times \overline{F_q}\right)$: eigenvalues are all size $q^{\frac{i}{2}}$.
  - Morally, the elements of H^i have "units" of dim. i, which could "drop" for sing. X…
- Consequence of "purity" (+ "comparison"): **naïve square-root cancellation** when counting points <u>on certain classes of varieties</u>.

What if we drop smoothness? (Abstract generalities)

- For singular X/F_p, our current understanding of ℓ-adic cohomology is poor.
- Morally, H^* should only depend on "concrete geometry" like point counts.
- But it remains open (?) in general that $\dim H^*(X \times \overline{F_p})$ is independent of the (auxiliary!) choice of ℓ.
- See D. Wan, "Algorithmic theory of zeta functions over finite fields" (2008): https://www.math.leidenuniv.nl/~psh/ANTproc/17wan.pdf
- If the Hasse–Weil zeta function (defined "naively" as $\prod \zeta_p(s, X_p)$ over almost all primes p) is meromorphic for all cubic hypersurfaces X/Q (possibly singular!), then it is meromorphic for all varieties X/Q.
- Moral: Singular stuff can be interesting, but poorly understood in general.

What if we drop smoothness? (Concrete point counting)

- For the rest of the talk, focus on *(projective) hypersurfaces* $F = 0$.
- Let m be the number of variables: $x_1, x_2, \ldots, x_m$. (Assume $m \geq 3$.)
- So $V := \{F = 0\}$ is a hypersurface in P^{m-1}/F_q. (Assume $F \neq 0$.)
- Let $d = \deg(F)$.
- Level 1: Points on linear hypersurfaces.
  - If $d = 1$, then $V(F_q)$ (e.g., $x_m = 0$) has exactly $\left|P^{m-2}(F_q)\right| = \frac{q^{m-1}-1}{q-1} = q^{m-2} + q^{m-3} + \cdots + q + 1$ points.
- Fix m, d. Naïve heuristic: $F = 0$ has $\left|P^{m-2}(F_q)\right| + O\left(q^{\frac{m-2}{2}}\right)$ points.
  - Always true (by Lang–Weil) if $m = 3$ and F is absolutely irreducible.

What if we drop smoothness? (Point counting, cont'd)

- Let m be the number of variables: $x_1, x_2, \dots, x_m$. (Assume $m \geq 3$.)
- So $V \coloneqq \{F = 0\}$ is a hypersurface in P^{m-1}/F_q.
- Let $d = \deg(F)$.
- Fix m, d. Naïve heuristic: $F = 0$ has $\left|P^{m-2}(F_q)\right| + O\left(q^{\frac{m-2}{2}}\right)$ points.
- For $m \geq 4$, this is *false in general*, even if F is absolutely irreducible.
  - Lang–Weil would only give an error term of $O\left(q^{\frac{m-3}{2}} \cdot q^{\frac{m-2}{2}}\right)$.
- But the **exceptional** F occur with probability **at most** $O(q^{-1})$.
  - Such F must be *singular* (so $\nabla F\colon \overline{F_q}^m \to \overline{F_q}^m$ must have a *nontrivial* zero).#

The latter is *equivalent* to the former if char(k) is coprime to deg(F).

Level 2: Points on quadratic hypersurfaces

- Let $V := \{F = 0\} \subset P^{m-1}/F_q$, with F a **quadratic form** in $x_1, \dots, x_m$.
- Fix m. Naïve heuristic: $F = 0$ has $\left|P^{m-2}(F_q)\right| + O\left(q^{\frac{m-2}{2}}\right)$ points.
- Assume $p \neq 2$. This lets us *complete the square*:
- WLOG $F = a_1 x_1^2 + \cdots + a_r x_r^2$, with $r := rank(F)$ and $a_1, \dots, a_r \in F_q^\times$.
- For such "diagonal" F, Weil (1949) computed $\left|V(F_q)\right|$ explicitly (when $r = m$) as evidence when formulating the Weil conjectures.
- This implies $\left|V(F_q)\right| = \left|P^{m-r-1}(F_q)\right| + q^{m-r} \cdot \left(\left|P^{r-2}(F_q)\right| \pm \mathbf{1}_{2|r} q^{\frac{r-2}{2}}\right)$.
  - Sign ("bias"): $\left(\frac{(-1)^{\frac{r}{2}} a_1 \cdots a_r}{F_q}\right) = \left(\frac{(-1)^{\frac{r}{2}} \det(F)}{F_q}\right)$, e.g., $+1$ for $x_1^2 - x_2^2 + x_3^2 - x_4^2 = 0$.

Level 2: Quadratic hypersurfaces (summary)

- Fix m. Naïve heuristic: $F = 0$ has $\left|P^{m-2}(F_q)\right| + O\left(q^{\frac{m-2}{2}}\right)$ points.
- Rigorously: If $p \neq 2$ and $r \coloneqq rank(F) \in [1, m]$, then
- $\left|V(F_q)\right| = \left|P^{m-2}(F_q)\right| \pm q^{\frac{m-r}{2}} \mathbf{1}_{2|r} \cdot q^{\frac{m-2}{2}}$.
  - So, if m is **odd**, then the "naïve heuristic" fails with probability $\asymp q^{-1}$.
  - Or, if m is **even**, then ——————————— fails with probability $\ll q^{-2}$.
  - (Calculations for "diagonal" F. But similar flavor for the "full" family.)
- What's next? Any guesses for what happens for cubic hypersurfaces?
- (As a power of q^{-1}, how often should the "naïve heuristic" fail?)

Level 3: Points on cubic hypersurfaces

- We could again discuss "universal families" of hypersurfaces.
- But for certain reasons, I want to focus on a different, smaller family.
- Fix $F_0 \coloneqq x_1^3 + x_2^3 + x_3^3 + x_4^3$ in 4 variables.
- For $\boldsymbol{c} \in F_q^4 - \{0\}$, let $V_{\boldsymbol{c}} \coloneqq \{F_0 = \boldsymbol{c} \cdot \boldsymbol{x} = 0\}$ be "basically in 3 variables".
- If $V_{\boldsymbol{c}} \times \overline{F_q}$ ("basically a plane cubic") is <u>irreducible</u>, then $\left|\left|V_{\boldsymbol{c}}(F_q)\right| - \left|P^1(F_q)\right|\right| \leq 18(3+3)^3 \cdot q^{\frac{1}{2}}$ (Lang–Weil, but with a lazily chosen constant).
- **Observation**: Here $V_{\boldsymbol{c}} \times \overline{F_q}$ is <u>reducible</u> if and only if
- … $V_{\boldsymbol{c}} \times \overline{F_q}$ <u>contains a line</u> over $\overline{F_q}$, if and only if
- … $\boldsymbol{c}$ is <u>orthogonal</u> to some line on $\{F_0 = 0\}$ (a cubic surface) over $\overline{F_q}$, if and only if
- … $c_i^3 - c_j^3 = c_k^3 - c_l^3 = 0$ for some permutation (i, j, k, l) of $[4]$.

Level 3: Cubic hypersurfaces (conjecturally)

- Note: $c_i^3 - c_j^3 = c_k^3 - c_l^3 = 0$ is a “codimension 2” condition.
- What if we increase the number of variables? (But keep the parity the same…)
- Fix $F_0 \coloneqq x_1^3 + x_2^3 + x_3^3 + x_4^3 + x_5^3 + x_6^3$ in 6 variables.
- For $\boldsymbol{c} \in F_q^6 - \{0\}$, let $V_{\boldsymbol{c}} \coloneqq \{F_0 = \boldsymbol{c} \cdot \boldsymbol{x} = 0\}$ be “basically in 5 variables”.
- **Conjecture/Challenge** (W., 2020): ∃ closed $E \subset A_Z^6$, with $\operatorname{codim}\left(E_Q, A_Q^6\right) \geq 4$, …
- … such that *for any given* prime power q and tuple $\boldsymbol{c} \in F_q^6 - E(F_q)$, we have
- $\left|\left|V_{\boldsymbol{c}}\left(F_q\right)\right| - \left|P^3\left(F_q\right)\right|\right| \leq 18(3+3)^5 \cdot q^{\frac{3}{2}}$, **or else**
- $c_i^3 - c_j^3 = c_k^3 - c_l^3 = c_m^3 - c_n^3 = 0$ for some permutation (i, j, k, l, m, n) of $[6]$.
- Prelim. evidence: https://github.com/wangyangvictor/singular_cubic_threefolds

Final remarks

- Possible moral/heuristic: "Randomness increases with $\deg(F)$".
  - Holds in our $\deg 2$ & 3 examples, at least. (Ignore the triv./degen. $\deg 1$ case.)
- There seems to be much left to explore, for $\deg(F) = 3, 4, \ldots$.
  - The role of $m \ (mod\ 2)$ also deserves more thought.
- Recent works of a similar statistical flavor:
  - Lindner, *Hypersurfaces with defect* ('20): https://arxiv.org/abs/1610.04077
  - Slavov, *[… rand(slicing) to count pts…]* ('17): https://arxiv.org/abs/1703.05062
  - Poonen & —, *[Excep. locus in Bert…]* ('20): https://arxiv.org/abs/2001.08672
  - ???
- Thanks for your time!