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 $X(F_p) = \text{Fix} \left[ \text{Frob}_p \mid X \left( \overline{F_p} \right) \right]$.\(^1\)

• So, we can count points using the (Grothendieck–)Lefschetz fixed-point formula (LTF): $\text{Fix}[-] = \sum (-1)^i \cdot \text{Tr} \left( \text{Frob}_p \mid H_c^i \left( X \times \overline{F_p} \right) \right)$.

• Why (co-)homology? To visualize fixed points, we can intersect the “graph” of Frob, with the “diagonal”:

• $\text{Fix} \left[ \text{Frob}_p \mid X \left( \overline{F_p} \right) \right] = \{ (x, y) : y = \text{Frob}_p(x) \} \cap \{ (x, y) : x = y \}$.

• If you imagine “wiggling” or “deforming” Frob, then the RHS should stay the same. This is morally why (co-)homology comes up in the LTF.

\(^1\) 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”.)

The (signed) number of fixed points is detected by \( f | H_*(S^1) \):
here \(+1 - 1 + 1 - 1 - 1 = Tr(f | H_0) - Tr(f | H_1)\).
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 $F_p, F_{p^2}, ...$ 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 “$≈$ linear”) spaces.

• “Purity” of the action of $Frob_q | H^i (X \times \overline{F_q})$: 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 on certain classes of varieties.
What if we drop smoothness? (Abstract generalities)

• For singular $X/F_p$, our current understanding of $\ell$-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 $\ell$.
• 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: $x_1, x_2, ..., x_m$. (Assume $m \geq 3$.)
• So $V := \{F = 0\}$ is a hypersurface in $P^{m-1}/F_q$. (Assume $F \neq 0$.)
• Let $d = \text{deg}(F)$.
• Level 1: Points on linear hypersurfaces.
  • If $d = 1$, then $V(F_q)$ (e.g., $x_m = 0$) has exactly $|P^{m-2}(F_q)| = \frac{q^{m-1}-1}{q-1} = q^{m-2} + q^{m-3} + \cdots + q + 1$ points.
  • Fix $m, d$. Naïve heuristic: $F = 0$ has $|P^{m-2}(F_q)| + O\left(\frac{m-2}{q^2}\right)$ 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: $x_1, x_2, \ldots, x_m$. (Assume $m \geq 3$.)

• So $V := \{F = 0\}$ is a hypersurface in $P^{m-1}/F_q$.

• Let $d = \deg(F)$.

• Fix $m, d$. Naïve heuristic: $F = 0$ has $|P^{m-2}(F_q)| + O\left(\frac{m-2}{2}\right)$ 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 $O\left(\frac{m-3}{2} \cdot \frac{m-2}{2}\right)$.

• But the exceptional $F$ occur with probability at most $O\left(q^{-1}\right)$.
  • Such $F$ must be singular (so $\nabla F: \overline{F_q}^m \rightarrow \overline{F_q}^m$ 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 $x_1, \ldots, x_m$.

• Fix $m$. Naïve heuristic: $F = 0$ has $|P^{m-2}(F_q)| + O\left(\frac{m-2}{q}\right)$ points.

• Assume $p \neq 2$. This lets us complete the square:

• WLOG $F = a_1x_1^2 + \cdots + a_rx_r^2$, with $r := \text{rank}(F)$ and $a_1, \ldots, a_r \in F_q^\times$.

• For such “diagonal” $F$, Weil (1949) computed $|V(F_q)|$ explicitly (when $r = m$) as evidence when formulating the Weil conjectures.

• This implies $|V(F_q)| = |P^{m-r-1}(F_q)| + q^{m-r} \cdot \left( |P^{r-2}(F_q)| \pm 1 \right) \left(2r \right) \cdot \left( q^{\frac{r-2}{2}} \right)$.

• Sign (“bias”): $\left( \frac{-1}{F_q} \frac{1}{r} a_1 \cdots a_r \right) = \left( \frac{-1}{F_q} \frac{1}{r} \text{det}(F) \right)$, 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 $|P^{m-2}(F_q)| + O\left(\frac{m-2}{q^2}\right)$ points.

• Rigorously: If $p \neq 2$ and $r := rank(F) \in [1, m]$, then

  $|V(F_q)| = |P^{m-2}(F_q)| \pm q^{\frac{m-r}{2}} \cdot q^{\frac{m-2}{2}} \cdot 1_{2|r}$.

  • So, if $m$ is odd, then the “naïve heuristic” fails with probability $\approx q^{-1}$.
  • Or, if $m$ is even, then $\ldots$ 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 $F_0 := x_1^3 + x_2^3 + x_3^3 + x_4^3$ in 4 variables.
• For $c \in F_q^4 - \{0\}$, let $V_c := \{F_0 = c \cdot x = 0\}$ be “basically in 3 variables”.
• If $V_c \times \overline{F_q}$ (“basically a plane cubic”) is irreducible, then $\left| |V_c(F_q)| - |P^1(F_q)| \right| \leq 18(3 + 3)^3 \cdot q^2$ (Lang–Weil, but with a lazily chosen constant).
• **Observation**: Here $V_c \times \overline{F_q}$ is reducible if and only if
  • $V_c \times \overline{F_q}$ contains a line over $\overline{F_q}$, if and only if
  • $c$ is orthogonal 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 $F_0 := x_1^3 + x_2^3 + x_3^3 + x_4^3 + x_5^3 + x_6^3$ in 6 variables.
• For $c \in F_q^6 - \{0\}$, let $V_c := \{F_0 = c \cdot x = 0\}$ be "basically in 5 variables".
• Conjecture/Challenge (W., 2020): ∃ closed $E \subset A_Z^6$, with $\text{codim}(E_Q, A_Q^6) \geq 4$, ...
• ... such that for any given prime power $q$ and tuple $c \in F_q^6 - E(F_q)$, we have
  • $|V_c(F_q)| - |P^3(F_q)| \leq 18(3 + 3)^5 \cdot q^2$, 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 \(\text{deg}(F) = 3, 4, \ldots\)
  • The role of \(m \pmod{2}\) also deserves more thought.
• Recent works of a similar statistical flavor:
  • ???
• Thanks for your time!