A Summary of Summer's Work

Ziquan Yang

August 10th, 2015 (edited on Sep. 28th)

1 Introduction to sieve methods

In his expositary paper [4] Poonen discussed an easy application of the idea of sieve method in number theory to compute the density square-free integers. Since we are talking about an infinite subset of integers, we first need to define what we mean by density.

Definition 1.1. The *density* μ of a subset $S \subseteq \mathbb{N}$ is defined by

$$\mu(S) = \lim_{B\to\infty} \frac{|S \cap [1, B]|}{B}$$

Let $\mathcal{P}$ be the set of all primes, and we use $\mathcal{P}_{<r}$ to denote the set of primes $< r$. For every bounded B we only need to take care of finitely many primes, i.e. sufficiently large $\mathcal{P}_{<r}$, and we have a good understanding of how to deal with finitely many primes. With Chinese remainder theorem it is easy to compute the density of $S_r := \{n \in \mathbb{N} : p^2 \textit{ does not divide } n, \forall p \in \mathcal{P}_{<r}\}$:

$$\mu(S_r) = \prod_{p\in\mathcal{P}_{<r}} (1 - p^{-2})$$

However, the CRT argument breaks down for infinitely many primes. As S is the limit of S_r, i.e $S = \cap_{r=1}^{\infty} S_r$, we may want to push $r \to \infty$ and guess that $\mu(S) = \zeta(2)^{-1} = \pi^2/6$. It requires some nontrivial work to justify this switch of order of taking limits, i.e.

$$\lim_{B\to\infty} \frac{|S \cap [1, B]|}{B} = \lim_{B\to\infty} \frac{|\cap_r S_r \cap [1, B]|}{B} = \lim_{r\to\infty} \lim_{B\to\infty} \frac{|S_r \cap [1, B]|}{B}$$

The idea is to bound the error term $|\mu(S) - \mu(S_r)|$ and show it vanishes as $r \to \infty$. To be precise we want to show

$$\lim_{r\to\infty} \lim_{B\to\infty} \frac{|n \in S_r \cap [1, B] : n \textit{ divisible by some } p^2, p > r|}{B} = 0$$

This can be shown using pretty crude bounds:

$$\begin{aligned}
&|n \in B_r \cap [1,B] : n \textit{ divisible by some } p^2, p > r| \\
&\qquad \leq |n \in [1,B] : n \textit{ divisible by some } p^2, p > r| \\
&\qquad \leq \sum_{p>r} \lfloor \frac{B}{p^2} \rfloor \\
&\qquad \leq \sum_{m>r} \lfloor \frac{B}{m^2} \rfloor \\
&\qquad \leq B \int_r^\infty \frac{1}{x^2} dx \\
&\qquad = B/r
\end{aligned}$$

2 Poonen's work and extensions

Poonen used the idea of sieve method to prove the following:

Theorem 2.1. *Let X be a quasiprojective subscheme of $\mathbb{P}^n$ of dimension $m \geq 0$ over $\mathbb{F}_q$. Define*

$$\mathcal{P} := \{f \in S_{\text{homog}} : H_f \cap X \textit{ is smooth of dimension } m-1\}$$

Then $\mu(\mathcal{P}) = \zeta_X(m+1)^{-1}$.

Definition 2.2. Define the density of a subset $\mathcal{P} \subset S_{\text{homog}}$ by

$$\mu(\mathcal{P}) = \lim_{d\to\infty} \frac{|\mathcal{P} \cap S_d|}{|S_d|}$$

The density of square-free integers would serve as a benchmark example of an arithmetic analogue of Theorem 2.1.

Poonen's method has three main pieces:

1. An interpolation lemma
2. A bound on the density of those hypersurfaces that are bad at "medium degree points"
3. A bound on the density of those hypersurfaces that are bad at "high degree points"

Here is Poonen's interpolation lemma:

Lemma 2.3. *If Y be a finite subscheme of $\mathbb{P}^n$ over a field k, then the map*

$$\phi_d : S_d = H^0(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(d)) \to H^0(Y, \mathcal{O}_Y(d))$$

is sujective for $d \geq \dim H^0(Y, \mathcal{O}_Y(d)) - 1$.

The interpolation lemma is not hard to prove, but it is of crucial importance in the method. First, it gives us reason to believe that when the degree of hypersurface is high enough, then its local behaviors at different points are relatively independent of each other. In fact, this surjectivity result invariably reduce the study of $H^0(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(d))$ to the study of $H^0(Y, \mathcal{O}_Y(d))$. Second, it sets up a criterion for "high degree", since after that we no longer have surjectivity.

The most technical part in the method is to bound the following two sets:

$$\mathcal{Q}_r^{\text{medium}} = \bigcup_{d \geq 0} \{f \in S_d : \exists P \in (H_f \cap U)^{bad} \text{ with } r \leq \deg P \leq \frac{d}{m+1}\}$$

and

$$\mathcal{Q}^{\text{high}} = \bigcup_{d \geq 0} \{f \in S_d : \exists P \in (H_f \cap U)^{bad} \text{ with } \deg P > \frac{d}{m+1}\}$$

where $P \in (H_f \cap U)^{bad}$ means that $P \in U$ and $H_f \cap U$ fails to be smooth of dimension $m-1$ at P. $\mathcal{Q}_r^{\text{medium}}$ and $\mathcal{Q}^{\text{high}}$ are "tail terms", and we see that $\mathcal{P} \subseteq \mathcal{P}_r \subseteq \mathcal{P} \cup \mathcal{Q}_r^{\text{medium}} \cup \mathcal{Q}^{\text{high}}$. Hence $\overline{\mu}(\mathcal{P})$ and $\underline{\mu}(\mathcal{P})$ each differ from $\mu(\mathcal{P}_r)$ by at most $\overline{\mu}(\mathcal{Q}_r^{\text{medium}}) + \overline{\mu}(\mathcal{Q}^{\text{high}})$. Our goal is to prove that $\overline{\mu}(\mathcal{Q}_r^{\text{medium}}) = \overline{\mu}(\mathcal{Q}^{\text{high}}) = 0$.

$\mathcal{Q}_r^{\text{medium}}$ is relatively easier to treat since surjectivity in the above lemma is still guaranteed. We may simply use the Lang-Weil bound to complete this part of the proof.

$\mathcal{Q}^{\text{high}}$ is much harder to deal with. The central piece in the proof is Poonen's decoupling trick: write a polynomial in $H^0(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(d))$ in the following form:

$$f = f_0 + g_1^p t_1 + \cdots + g_m^p t_m + h^p$$

where t_i's are local parameters and g_i's and h are auxilliary polynomials of appropriate degrees. The main point of doing so is to decouple partial derivatives.

When X is a projective subscheme of $\mathbb{P}^n$, let A be a very ample divisor that induces the inclusion $X \hookrightarrow \mathbb{P}^n$. We know that the restriction map

$$H^0(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(d)) \to H^0(X, \mathcal{O}_X(dA))$$

is surjective. Therefore we could have reduced to the study of $H^0(X, \mathcal{O}_X(dA))$, which is intrinsic of X.

Building on Poonen's work, Erman and Wood studied the case when the degree of the hypersurface is not increasing in the very ample direction. For example, consider $X = \mathbb{P}^1 \times \mathbb{P}^1$. We might be interested in studying hypersufaces (curves in this case) of bidegree (n, d) and we want to push d to infinity. Poonen's work only deals with the case when n and d are both increasing. Erman and Wood's work is basically following Poonen's idea, but it has greatly enriched the toolbox we have at hand.

3 My work

After I absorbed the main ideas of these papers, Prof. Schoen gave me a toy problem to think about, and I proved the following: In $\mathbb{P}^1 \times \mathbb{P}^1$, the asymptotic probability that a randomly chosen curve of bidegree $(3, d)$ is simply ramified is $\zeta_{\mathbb{P}^1}(2)^{-2}$ as $d \to \infty$. I extended Poonen's decoupling trick to treat second order partial derivatives. I also used the basic structure of Erman and Wood's arguments, although now I realized I could have made things a bit simpler.

Then Prof. Schoen let me consider consider hypersurfaces in $\mathbb{P}^2 \times \mathbb{P}^1$ of bidegree $(3, d)$. These hypersurfaces are parametrized by $P = \mathbb{P}V$, where

$$V = H^0(\mathbb{P}^2 \times \mathbb{P}^1, \mathcal{O}(3, d))$$

Let P^0 be the subscheme parametrizing those non-singular ones:

$$P^0 = \{f \in P : H_f \textit{ is non-singular } \}$$

Let $\pi : \mathbb{P}^2 \times \mathbb{P}^1 \to \mathbb{P}^1$ be projection to the second component. If H_f is non-singular, then fibers of $\pi|_{H_f}$ are cubic curves in $\mathbb{P}^2$. This makes H_f an elliptic surface. The analogy of being simply ramified for H_f has to do with singular fibers of the map $\pi : H_f \to \mathbb{P}^1$. Smooth fibers are all isomorphic to the smooth cubic curve. It is customary for some literature to call an irredcucible cubic curve, together with a specified point as the base point, an elliptic curve. There are many types of singular fibers. If the fiber is irreducible, then it is either a nodal curve (e.g. $y^2 = x^2 - x^3$), or a cuspidal curve (e.g. $y^2 = x^3$). If the fiber is not irreducible, then it may be a union of a conic curve and a line, or a union of three lines and there are many different configurations of irreducible components. An analogue of a simply ramified curve would be a hypersurface whose singular fibers are all nodal curves. Hence we are primarily concerned with the following subset of P^0:

$$D = \{f \in P^0 : \textit{all singular fibers of } H_f \textit{ are nodal curves}\}$$

The conjecture is as $d \to \infty$, then density of D will be close to 1.

To attack the problem I need to consider reducibility of fibers, which is not normally a local property like smoothness. However, with the hint from Prof. Schoen, I figured out how to partially classify the degree 3 curves in $\mathbb{P}^2$ using its local behavior at the singularity (if there is one).

The Poonen type sieve methods in [3] and [2] depend heavily on linear algebraic arguments. In particular, at the end of the day we need linear equations with respect to partial derivatives, although sometimes nonlinear equations may naturally comes up. For example, the most natural way to describe the condition the plane curve described by $f = 0$ has a double line as tangent cone at a point P is to require:

$$f = \frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = 0, \, (\frac{\partial^2 f}{\partial x \partial y})^2 = (\frac{\partial^2 f}{\partial x^2})(\frac{\partial^2 f}{\partial y^2})$$

at P, but the second equation is nonlinear. We circumvented the problem by introducing a new variable $(u : v) \in \mathbb{P}^1$ and look at the equation

$$\frac{\partial^2 f}{\partial x^2}u^2 + 2\frac{\partial^2 f}{\partial x \partial y}uv + \frac{\partial^2 f}{\partial y^2}v^2$$

Therefore, instead of working directly with $\mathbb{A}^2 \times \mathbb{A}^1 \subseteq \mathbb{P}^2 \times \mathbb{P}^1$, we worked with $\mathbb{P}^1 \times \mathbb{A}^2 \times \mathbb{A}^1$, where $\mathbb{P}^1$ serves to parametrize the auxilliary variables $(u : v)$.

I think I have treated the high degree points in the setting of this problem. However, in order to compute the exact density of D we would need the following:

Let $P \in \mathbb{P}^1_{\mathbb{F}_q}$ be a fixed point. Let $r(s)$ be the irreducible polynomial of degree e such that the second infinitestimal neighborhood $P^{(2)} = \mathrm{Spec}\, \mathbb{F}_\mathrm{q}[\mathrm{s}]/\mathrm{r(s)}^2$. As $d \to \infty$, what is the probability that the image of a randomly chosen $f \in H^0(\mathbb{P}^2 \times \mathbb{P}^1, \mathcal{O}(3, d))$ under the restriction

$$H^0(\mathbb{P}^2 \times \mathbb{P}^1, \mathcal{O}(3, d)) \to H^0(\mathbb{P}^1_{\mathbb{F}_q[s]/r(s)^2}, \mathcal{O}(3))$$

shows that the hypersurface H_f is smooth at all points on the fiber over P and the fiber $(H_f)_P$ is either smooth or a nodal curve. As $d \to \infty$, the above restriction map will eventually be a surjection and hence we reduce to studying $H^0(\mathbb{P}^2_{\mathbb{F}_q[s]/r(s)^2}, \mathcal{O}(3))$. As in [2], We have the isomorphism

$$H^0(\mathbb{P}^2_{\mathbb{F}_q[s]/r(s)^2}, \mathcal{O}(3)) \simeq H^0(\mathbb{P}^2_{\mathbb{F}_{q^e}}, \mathcal{O}(3))^2$$

as vector spaces over $\mathbb{F}_{q^e}$. We are concerned with the probability that a randomly chosen pair $(F_1, F_2) \in H^0(\mathbb{P}^2_{\mathbb{F}_{q^e}}, \mathcal{O}(3))^2$ satisfies one of the following:

1. F_1 describes a smooth curve in $\mathbb{P}^2_{\mathbb{F}_{q^e}}$.
2. F_1 describes a nodal curve in $\mathbb{P}^2_{\mathbb{F}_{q^e}}$ but F_2 does not vanish at the node.

In the end we did not compute the exact fractions. However, we were still able to use Lang-Weil bounds to show that at least, the density of D should be positive. Therefore, if N is sufficiently large, then for all $d \geq N$, there exists a smooth hypersurface of degree d in D. If we replace $\mathbb{F}_q$ by $\mathbb{F}_{q^l}$, then the density goes to 1 as $l \to \infty$. In fact, D contains an open subset of $\mathbb{P}V$. If we are working with algebraically closed fields, then this already says that the density of D is 1. Therefore as the base field approaches its algberaic closure, the density of D also approaches that of its algebraic closure.

4 Future work

I am interested in how we can use sieve methods to systematically treat global properties that cannot be tested locally, for example, irreducibility. I know Prof. Poonen has already written an article on this, introducing new ideas that I have not yet absorbed. Probably I can write something on the semiample version of his Bertini irreducibility theorems.

At the end of his expository aritle, Poonen posed the following questions:

1. There seems to be a general principle that if an existence result about polynomials or n-tuples of polynomials over an infinite field can be proved by dimension counting, then a corresponding result over finite fields can be proved by the closed point sieve. Can this principle be formalized and proved?

2. What other theorems currently require the hypothesis Assume that k is an infinite field? Hopefully the closed point sieve could be used to eliminate the hypothesis in many of these.

My research is basically following this theme. We treated the simply ramified curves and elliptic surface by first demonstrating a dimension counting argument and then converting the argument into a sieve method. An interesting phenomenon that I noticed is that sometimes there are more than one natural ways to do the dimension counting argument, but not all of them can be easily converted to a sieve argument.

Prof. Schoen suggests that I read about ruled surfaces and see how my results for curves $\mathbb{P}^1 \times \mathbb{P}^1$ extend.

References

[1] B. Poonen, *Bertini irreducibility theroems over finite fields*, available at *http://www-math.mit.edu/ poonen/papers/bertini_irred.pdf*

[2] D. Erman and M.M. Wood, *Semiample Bertini theorems over finite fields*, Duke Mathematical Journal 164(2015), no. 1, 1-38

[3] B. Poonen, *Bertini theorems over finite fields*, Ann. of Math. (2) 160 (2004), no. 3, 1099-1127.

[4] B. Poonen, *Sieve methods for varieties over finite fields and arithmetic schemes*, J. Theor. Nombres Bordeaux, 19(1):221229, 2007.