# Notes on Poonen's Paper

Ziquan Yang

May 25, 2015

## Contents

# 1 Introduction

In his expositary paper 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* $\mu$ of a subset $S \subseteq \mathbb{N}$ id 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 care finitely many primes, i.e. sufficiently large $\mathcal{P}_{<r}$, and we have a good understanding of how to deal with finitely many primes. A standard application of 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.

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

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

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

This can be shown using pretty crude bounds:

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

Poonen used a similar sieve method to prove the following:

**Theorem 1.2.** *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 1.3.** 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 for Theorem 1.2. Not only does it provides the intuition for how the sieve argument works, but it itself could of rendered a corollary of Theorem 1.2.

# 2 Prelimiaries

## 2.1 Zeta functions

Let us recall the definition of the zeta function:

$$\zeta_X(s) = \prod_{x\in|X|} (1 - N(x)^{-s})^{-1}$$

where $|X|$ is the set of closed points in $X$ and $N(x)$ is the cardinality of the residue field at $x$.

We compute $\zeta(\text{Spec}\,\mathbb{F}_\text{p}[\text{t}], \text{s})$, as an example. Let $X = \text{Spec}\,\mathbb{F}_\text{p}[\text{t}]$. A point $x \in |X|$ is represented by a monic irreducible polynomial $f$. It is not hard to discern that $N(x)$ is simply $p^{\deg f}$. Now we have

$$\begin{aligned}
\zeta(\text{Spec}\,\mathbb{F}_\text{p}[\text{t}], \text{s}) &= \prod_{f \text{irred}} (1 - p^{-s\text{deg}\, f})^{-1} \\
&= \prod_{f \text{irred}} \sum_{m=0}^{\infty} p^{-sm \deg f} \\
&= \prod_{g\in\mathbb{F}_p[t] \text{monic}} p^{-s \deg g} \\
&= \prod_{d=0}^{\infty} p^{d-ds} \\
&= (1 - p^{1-s})^{-1}
\end{aligned}$$

Now let me explain the third equation. Consider the degree $n$ term in the expansion of the product

$$(\sum_{m_1=0}^{\infty} p^{-sm_1 \deg f_0})(\sum_{m_2=0}^{\infty} p^{-sm_2 \deg f_1})(\sum_{m_3=0}^{\infty} p^{-sm_3 \deg f_2})\cdots$$

To construct a term what we do is to select a term in each factor, indexed by an irreducible polynomial, so that the degrees add up to $n$. Note that all polynomials factor into a product of irreducible ones, so the degree $n$ term simply counts the number of monic polynomials of degree $n$.

## 2.2 Twisted sheaves

Let $X = \mathbb{P}^n_A = \operatorname{Proj} \mathrm{S}$ where $S = A[x_0, \cdots, x_n]$. For any $P \in X$ we define

$$\mathcal{O}_X(n)_P = \bigcup_{d \geq 0} \{\frac{f}{g} : f \in S_{d+n}, g \in S_d, g(P) \neq 0\}$$

Note that they are not polynomial functions near $P$. However, they can readily produce functions.

On an open subset $U \subseteq X$ we define

$$\mathcal{O}_X(n)(U) = \bigcap_{P \in U} \mathcal{O}_X(n)_P$$

. In particular, on $\mathcal{U}_i = D_+(x_i)$ we have

$$\mathcal{O}_X(n)(\mathcal{U}_i) = \bigcup_{d \geq 0} \{\frac{f}{x_i^d} : f \in S_{d+n}\}$$

We easily observe that

$$\mathcal{O}_X(\mathcal{U}_i)(n) \to \mathcal{O}_X(\mathcal{U}_i) \text{ defined by } \varphi \mapsto \varphi \cdot x_i^{-n}$$

gives an *isomorphism* $\mathcal{O}_X(\mathcal{U}_i)(n) \simeq \mathcal{O}_X(\mathcal{U}_i)$. I think of sections in $\mathcal{O}_X(n)$ as "primers of functions that carry the information of zeros and poles". For example, if $U \subseteq \mathcal{U}_i$, then the above isomorphism gives a real function on $U$. If $U \subseteq \mathcal{U}_j$ as well and we "untwist" using $x_j$ instead, they we would obtain another function on $U$, which differ from the previous one by a unit in $\mathcal{O}_X(U)^*$.

There are plenty of cases in which we do not care about "differing be a unit". A classical senario that will come up later is the following: Let $P \in U$ be a point, where $U$ is a quasiprojective subscheme of $X$. Let $\mathfrak{m}_u$ be the ideal sheaf of $P$ on $U$ (note that this is different from the ideal sheaf of $P$ on $X$!) and $Y$ be the scheme of $U$ corresponding to the ideal sheaf $\mathfrak{m}_u^2$. Then given $f \in S_d = H^0(X, \mathcal{O}_X(n))$, $H_f \cap U$ is singular at $P$ if and only if the restriction of $f$ to a section of $\mathcal{O}_Y(d)$ is zero.

### 2.3 Degree and base extension

For each $r$, $\mathbb{P}^n$ over $\mathbb{F}_q$ contains only finitely many closed points of degree $\leq r$. Actually it suffices to check this on $\mathbb{A}^n$. When $n = 1$, a closed point corresponds to an irreducible $f \in \mathbb{F}_q[t]$ and we know there are only finitely many irreducible polynomials of a bounded degree. Now consider $\mathbb{A}^2$. It suffices to show there are only finitely many closed points of bounded degree on a fiber over the natural projection $\mathbb{A}^2 \to \mathbb{A}^1$. Given $\mathfrak{m} \subseteq \mathbb{F}_q[x_0, x_1]$, we have a two-step filtration

$$\mathbb{F}_q[x_0, x_1]/\mathfrak{m} = (\mathbb{F}_q[x_0, x_1]/\mathfrak{m} \cap \mathbb{F}_q[x_0])/\mathfrak{m}^e \simeq \mathbb{F}_{q^e}[x_1]/\mathfrak{m}'$$

for some $\mathfrak{m}'$ maximal ideal in $\mathbb{F}_{q^e}[x_1]$. If $\mathfrak{m} \cap \mathbb{F}_q[x_0]$ remain fixed, i.e. we restrict our attention to the fiber over $\mathbb{F}_q[x_0] \cap \mathfrak{m}$, then $\mathfrak{m}'$ is determined uniquely by $\mathfrak{m}$. Hence there are only finitely many of them of bounded degree. Conversely, we see that even $\mathbb{A}^1$ contains points of arbitrarily large degree.

Now let $X \subseteq \mathbb{P}^n$ be a quasiprojective subscheme over $\mathbb{F}_q$. We show that if $\deg X \geq 1$, for every $n_0$ there exists a closed point $P$ in $X$ with $\deg P \geq n_0$. By what we have shown above, it is equivalent to showing that $X$ contains infinitely many closed points. We may assume that $X$ is affine of finite type over $\mathbb{F}_q$ and Noether normalization tells us that there exists a surjection $X \to \mathbb{A}^1$ if $\dim X \geq 1$. Hence $X$ contains infinitely many closed points.

Note that a morphism never increase the degree of a point. To make precise, let $f : X \to Y$ be a morphism of schemes of finite type over $\mathbb{F}_q$, $P \in X$ be a closed point, then $\deg f(P) \leq \deg P$. Since $P$ gives a morphism $\operatorname{Spec} \mathrm{K(P)} \to \mathrm{X}$, where $K(P)$ is the residue field of $P$ on $X$. Compose it with $f$ we get $\operatorname{Spec} \mathrm{K(P)} \to \mathrm{Y}$, which in particular, is equipped with an *inclusion* $K(f(P)) \subseteq K(P)$. Hence $\deg f(P) \leq \deg P$.

## 3 The Main Result

Instead of proving the Bertini theorem over finite fields directly, we add a little twist to the statement and this will be the main result that we will prove:

**Theorem 3.1.** *Let $X$ be a quasiprojective subscheme of $\mathbb{P}^n$ over $\mathbb{F}_q$. Let $Z$ be a finite subscheme of $\mathbb{P}^n$ and assume $U = X - (Z \cap X)$ is smooth of dimension $m \geq 0$. Fix a subset $T \subseteq H^0(Z, \mathcal{O}_Z)$. Define*

$$\mathcal{P} = \{f \in S_{\text{homog}} : H_f \cap U \textit{ is smooth of dimension } m-1, \textit{and } f|_Z \in T\}$$

*Then*

$$\mu(\mathcal{P}) = \frac{\#T}{\#H^0(Z, \mathcal{O}_Z)} \zeta_U(m+1)^{-1}$$

Let me explain the notation $f|_Z$. Recall that on the level of sets $Z$ is a finite set of closed points. Suppose $Z_i \in Z$. We can readily untwist $f$ using $x_j$ to give a function near $i$ for some $j$ such that $Z_i \in D_+(x_j)$. For consistency we always choose the smallest possible such $j$, but this choice really does not matter.

As we can see this version of the theorem introduces two more variables: a finite subscheme $Z$, which we could think of as a finite set of points, and a subset $T \subseteq H^0(Z, \mathcal{O}_Z)$. The idea is to loosen the condition that $H_f \cap X$ is smooth by taking off a finite set of points ($Z \cap X$), but retain some control over the local behavior of $f$ at $Z$.

Just as in the case of using Sieve method to compute the density of square free integers, the main goal of the proof is to justify the following exchange of order of taking limits:

$$\lim_{d\to\infty} \frac{\#(\mathcal{P} \cap S_d)}{\#S_d} = \lim_{d\to\infty} \frac{\#((\cap_r \mathcal{P}_r) \cap S_d)}{\#S_d} = \lim_{r\to\infty} \lim_{d\to\infty} \frac{\#(\mathcal{P}_r \cap S_d)}{\#S_d}$$

that is

$$\mu(\mathcal{P}) = \lim_{r\to\infty} \mu(\mathcal{P}_r)$$

In other to do this we introduce the following two sets

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

and

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

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 $\overline{\mu}(\mathcal{Q}_r^{\text{medium}}) + \overline{\mu}(\mathcal{Q}^{\text{high}})$.

# 4 Lemmas and Proofs

## 4.1 Singular points of low degree

**Lemma 4.1.** *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 $d \geq \dim H^0(Y, \mathcal{O}_Y(d)) - 1$.*

*Proof.* Let $\mathcal{I}_Y$ be the ideal sheaf of $Y \subseteq \mathbb{P}^n$. Then $\operatorname{coker} \phi_d \subseteq H^1(\mathbb{P}^n, \mathcal{I}_Y(d))$ which vanishes for $d >> 1$ by Theorem III.5.2b of Hartshorne. Thus $\phi_d$ will be surjective eventually. Enlarge $\mathbb{F}_q$ if necessary (why can we do this?) we may assume $Y \subseteq \mathbb{A}^n = \{x_0 \neq 0\}$ and we dehomogenize at $x_0$. Then $\phi_d$ can be identified with a map $A_{\leq d} \to B := H^0(Y, \mathcal{O}_Y)$. Let $B_i$ be the image of $A_{\leq i}$ in $B$. Then we have a chain $0 = B_{-1} \subseteq B_0 \subseteq B_1 \subseteq \cdots$. If some $B_j = B_{j+1}$, then

$$B_{j+2} = B_{j+1} + \sum_{i=1}^{n} x_i B_{j+1} = B_{j+1} + \sum_{i=1}^{n} x_i B_j = B_{j+1}$$

that is, the chain will stabilize after then. Since we know the chain *has to* stabilize to $B$ and the dimension over $\mathbb{F}_q$ has to increase for strict inclusions, we obtain the desired conclusion. □

Now we show the following:

$$\mu(\mathcal{P}_r) = \frac{\#T}{\#H^0(Z, \mathcal{O}_Z)} \prod_{P \in U_{<r}} (1 - q^{-(m+1)\deg P})$$

as in the setting of the main theorem.

Let $U_{<r} = \{P_1, \cdots, P_s\}$. Let $\mathfrak{m}_i$ be the ideal sheaf of $P_i$ on $U$. Let $Y_i$ be the closed subscheme of $U$ defined by the ideal sheaf $\mathfrak{m}_i^2$ and $Y = \bigcup Y_i$. For $f$ with $\deg f = d$, $H_f \cap U$ is singular at $P_i$ if and only if the restriction of $f$ to a section of $\mathcal{O}_{Y_i}(d)$ is zero. Hence $\mathcal{P}_r \cap S_d$ is the inverse image of

$$T \times \prod_{i=1}^{s} (H^0(Y_i, \mathcal{O}_{Y_i}) - \{0\})$$

under the $\mathbb{F}_q$-linear composition

$$\phi_d : S_d = H^0(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(d)) \to H^0(Y \cup Z, \mathcal{O}_{Y \cup Z}(d)) \simeq H^0(Z, \mathcal{O}_Z) \times \prod_{i=1}^{s} H^0(Y_i, \mathcal{O}_{Y_i})$$

Note that $Y$ and $Z$ are two *disjoint* set of closed points, so $H^0(Y \cup Z, \mathcal{O}_{Y \cup Z}(d))$ naturally splits to the above direct product after we untwist the sections individually for each point. The isomorphism is not canonical though since we may an arbitrary choice when untwisting.

Now we can invoke the previous lemma to see that when $d >> 1$, $\phi_d$ is surjective. Hence

$$\frac{\#(\mathcal{P}_r \cap S_d)}{\#(S_d)} = \frac{\#[T \times \prod_{i=1}^{s} (H^0(Y_i, \mathcal{O}_{Y_i}) - \{0\})]}{\#[H^0(Z, \mathcal{O}_Z) \times \prod_{i=1}^{s} H^0(Y_i, \mathcal{O}_{Y_i})]}$$

since the cardinality of $\ker \phi_d$ is cancelled out on the LHS. The RHS turns out to be the desired

$$\frac{\#T}{\#H^0(Z, \mathcal{O}_Z)} \prod_{i=1}^{s} (1 - q^{-(m+1)\deg P_i})$$

## 4.2 Singular points of medium degree

We prove $\overline{\mu}(\mathcal{Q}_r^{\text{medium}}) \to 0$ as $r \to \infty$.

**Lemma 4.2.** *Let $U \subseteq \mathbb{P}^n$ be a smooth quasiprojective subscheme of dimension $m \geq 0$ over $\mathbb{F}_q$. If $P \in U$ is a closed point of degree $e \leq d/(m+1)$, then the fraction $f \in S_d$ such that $H_f \cap U$ is not smooth of dimension $m-1$ at $P$ equals $q^{-(m+1)e}$.*

*Proof.* Let $\mathfrak{m}$ be the ideal sheaf of $P$ on $U$ and let $Y$ be the subsheme with ideal sheaf $\mathfrak{m}^2$. Then the kernel of $\phi_d : H^0(\mathbb{P}^n, \mathcal{O}(d)) \to H^0(Y, \mathcal{O}_Y(d))$ is exactly those $f$ such that $H_f \cap U$ is not smooth of dimension $m-1$ at $P$. By lemma 4.1, $\phi_d$ is surjective. Then the conclusion follows from $\operatorname{codim} \phi_d = (m+1)e$. □

We invoke the crude bound $|U(\mathbb{F}_{q^e}| \leq cq^{em})$ for some $c > 0$ depending only on $U$. Note that $U(\mathbb{F}_{q^e})$ means the set of *geometric points* on $U$, i.e. morphisms $\mathrm{Spec}\,\mathrm{F_{q^e}} \to \mathrm{U}$. A point on a scheme may corresponds to many geometric points, so the bound is rather crude, but it suffices for our purposes here.

$$\begin{aligned}
\frac{|\mathcal{Q}_r^{\text{medium}} \cap S_d|}{|S_d|} &\leq \sum_{e=r}^{\lfloor d/(m+1) \rfloor} |\{P \in U : \deg P = e\}| q^{-(m+1)e} \\
&\leq \sum_{e=r}^{\lfloor d/(m+1) \rfloor} |U(\mathbb{F}_{q^e})| q^{-(m+1)e} \\
&\leq \sum_{e=r}^{\infty} cq^{em} q^{-(m+1)e} \\
&= \frac{cq^{-r}}{1-q^{-1}}
\end{aligned}$$

Then the conclusion follows.

## 4.3 Singular points of high degree

As promised, now we want to prove $\overline{\mu}(\mathcal{Q}^{\text{high}}) = 0$, but first we prove a simple lemma:

**Lemma 4.3.** *Let $P$ be a closed point of degree $e$ in $\mathbb{A}^n$ over $\mathbb{F}_q$. Then the fraction of $f \in A_{\leq d}$ that vanishes on $P$ is at most $q^{-\min(d+1,e)}$.*

*Proof.* The idea is very simple: $P$ corresponds to a maximal ideal $\mathfrak{m}$ in $\mathbb{F}_q[t_1, \cdots, t_n]$, and $\deg P$ is large means $\mathfrak{m}$ is small. To be precise, the isomorphism $\mathbb{F}_q[t_1, \cdots, t_n]/\mathfrak{m} \to \mathbb{F}_{q^e}$, which in particular is a $\mathbb{F}_q$-linear map, restricts to a map $\mathfrak{m}/(A_{\leq d} \cap \mathfrak{m}) \to \mathbb{F}_{q^e}$. Then the conclusion is obvious. □

A quasiprojective subscheme of $\mathbb{P}^n$ is quasicompact, it suffices to show this for a neighborhood of an arbitrary point. We first assume $U \subseteq \mathbb{A}^n$ is affine. Given $u \in U$, choose a system of local parameters $t_1, \cdots, t_n$ such that $t_{m+1} = t_{m+2} = \cdots = t_n = 0$ defines $U$ locally at $u$. Hence $dt_i$'s form a basis for $\Omega_{\mathbb{A}^n/\mathbb{F}_q,u}$ and let $\partial_i$'s be the dual basis for $\mathcal{T}_{\mathbb{A}^n/\mathbb{F}_q,u}$. Choose $s \in A$ to clear the denominators so that each $D_i = s\partial_i$ gives a global derivation $A \to A$. $\Omega_{\mathbb{A}^n/\mathbb{F}_q,u}$ is locally free since $U$ is smooth. So we may further restrict $U$ so that $\Omega_{\mathbb{A}^n/\mathbb{F}_q,u}$ is actually free and $s$ is invertible on $U$.

Now $H_f \cap U$ fails to be smooth of dimension $m-1$ at a point $P \in U$ if and only if $f(P) = (D_1 f)(P) = \cdots = (D_m f)(P)$. For future use we define

$$W_i = U \cap \{D_1 f = \cdots D_i f = 0\}$$

. Let $T_d = \{f \in A_{\leq d} : \dim U \cap W_m = 0 \textit{ and } H_f \cap W_m \cap U_{>d/(m+1)} = \emptyset\}$. Then $T_d \subseteq A_{\leq d} - (A_{\leq d} \cap \mathcal{Q}^{\text{high}})$. We will show that $|T_d|/|A_{\leq d}| \sim 1 - o(1)$ as $d \to \infty$. This would suffice for our conclusion although the inclusion might be strict.

Here I am trying to rewrite Poonen's decoupling trick to make the central argument clearer to myself, but they are really the same. Set $F = A_d, G_i = A_{\leq \gamma}, H = A_{\leq \eta}$ where

$$\tau = \max_i(\deg t_i), \gamma = \lfloor \frac{d-\tau}{p} \rfloor, \eta = \lfloor \frac{d}{p} \rfloor$$

Then we consider the following map

$$\varphi : \mathcal{D} := F \times \prod_{i=1}^{n} G_i \times H \to A_{\leq d}$$

defined by

$$\varphi(f_0, g_1, \cdots, g_m, h) = f_0 + g_1^p t_1 + \cdots + g_m^p t_m + h^p$$

To simplify notation we may write $\widetilde{g}$ in place of $(g_1, \cdots, g_m)$ later. $\varphi$ is obviously linear and surjective so

$$\frac{|\{f \in A_{\leq d} - \mathcal{Q}^{\text{high}}\}|}{|A_{\leq d}|} = \frac{|\{(f_0, \widetilde{g}, h) \in \mathcal{D} : \varphi(f_0, \widetilde{g}, h) \in A_{\leq d} - \mathcal{Q}^{\text{high}}\}|}{|\mathcal{D}|}$$

The point of this complication is that it is easier to check whether $\varphi(f_0, \widetilde{g}, h) \in A_{\leq d} - \mathcal{Q}^{\text{high}}$ on the level of $\mathcal{D}$. Note that $D_i f = (D_i f_0) + g_i^p s$ so in particular $D_i f$ depends only on $g_i$ once $f_0$ is fixed. *Step 1:* For any fixed $f_0$, we give a bound for the fraction of $(g_0, \cdots, g_m)$ such that $\dim W_m = 0$.

We observe that $\dim W_m = 0$ if and only if each $D_i f$ cuts out a fresh dimension, so we proceed stepwise: Suppose $g_1, \cdots, g_i$ are chosen such that

$\dim W_i \leq m-i$ what is the fraction of $g_{i+1}$ such that $\dim W_{i+1} \leq m-i-1$? Suppose $V_1, \cdots, V_l$ are the $(m-i)$-dimensional $\mathbb{F}_q$ irreducible components of $(W_i)_{\mathrm{red}}$. We obtain a bound on $l$ by applying Bezout theorem:

$$l \leq (\deg \overline{U})(\deg D_1 f) \cdots (\deg D_i f)$$

where $\overline{U}$ is the projective closure of $U$, but all that we care is that it is a constant independent of $d$. We can easily see the RHS is bounded by $c_0 d^i$ for some constant $c_0$.

Given $V_k$ we want to bound

$$G^{bad}_{i+1,k} = \{g_{i+1} \in G_{i+1} : D_{i+1} f = (D_{i+1} f_0) + g^p_{i+1} s \text{ vanishes identically on } V_k\}$$

If $g_{i+1}, g'_{i+1} \in G^{bad}_k$, then $g_{i+1} - g'_{i+1}$ vanishes identically on $V_k$. Hence if $G^{bad}_{i+1,k} \neq \emptyset$, it is a coset of the kernel of the restriction map $\mathrm{res}_k : G_{i+1} = A_{\leq \gamma} \to \Gamma(V_k, \mathcal{O}_{V_k})$. codim $\ker \mathrm{res}_k = \dim \mathrm{Im}\, \mathrm{res}_k \geq \gamma + 1$ since some $x_j$ do not vanish on $V_k$ (and hence none of nonzero polynomial in $x_j$ vanishes identically on $V_k$). (Recall that we have already dehomogenized from $\mathbb{P}^n$.) Therefore we conclude if $\dim W_i \leq m-i$

$$\frac{|\{g_{i+1} \in G_{i+1} : \dim W_{i+1} \leq m-i-1\}|}{|G_{i+1}|} = \frac{|\cup_k G^{bad}_{i+1,k}|}{|G_{i+1}|} \leq l q^{\gamma+1} \sim o(1)$$

as $d \to \infty$.

*Step 2:* If $f_0, \widetilde{g}$ satisfies the above condition, we give a bound for the fraction of $h$ such that $H_f \cap W_m \cap U_{>d/(m+1)}$. This step is easier. Use the same Bezout's argument with $W_m$ we see that $|W_m| \sim O(d^m)$. For $P \in W_m$, we define $H^{bad}_P$ anagolously, then it is a coset of the kernel of $\mathrm{ev}_P : H = A_{\leq eta} \to k(P)$. If $P > d/(m+1)$, then the lemma says that $|H^{bad}_P|/|H| \leq q^{-v}$, where $v = \min(\eta+1, d/(m+1))$. Hence

$$\frac{|\{h \in H : H_f \cap W_m \cap U_{>d/(m+1)} \neq \emptyset\}|}{|H|} \leq |W_m| q^{-v} \sim O(d^m q^{-v}) = o(1)$$

as $d \to \infty$.

Step 1 and 2, together with previous discussion, shows that

$$\frac{|\{(f_0, \widetilde{g}, h) \in \mathcal{D} : \varphi(f_0, \widetilde{g}, h) \notin \mathcal{Q}^{\text{high}}|}{|\mathcal{D}|} \sim \prod_{i=1}^{m} (1 - o(1))(1 - o(1)) = 1 - o(1)$$

In case in is confusing, recall that $\varphi(\mathcal{D}) = S_d$ and $\mathcal{D}$ depends on $d$. That is, we used a family $\mathcal{D}_d$ but we suppressed the supscript before.

# 5 Applications

## 5.1 Anti-Bertini theorem

Theorem 3.1 yields the following theorem, which Poonen calls the Anti-Bertini theorem:

**Theorem 5.1.** *Given a finite field $\mathbb{F}_q$ and integers $n \geq 2, d \geq 1$, there exists a smooth projective geometrically integral hypersurface $H_g \subseteq \mathbb{P}^n$ over $\mathbb{F}_q$ such that for each $f \in S_1 \cup \cdots \cup S_d$, $H_f \cap H_g$ fails to be smooth of dimension $n-2$.*

*Proof.* Let $H^{(1)}, \cdots, H^{(l)}$ be a list of the $H_f$ arising from $f \in S_1 \cup \cdots \cup S_d$. For each $i, 1 \leq i \leq l$, we choose a point $P_i \in H^{(i)}$ distinct from $P_j$ for $j < i$. In Theorem 3.1, we take $X = \mathbb{P}^n$. Now we use exactly the same trick as in the proof of Lemma 4.2. Let $\mathfrak{m}_i$ be the ideal sheaf of $P_i$ and let $Y_i$ be the subscheme corresponding to $\mathfrak{m}_i^2$. Take $Z = \cup Y_i$. $Z$ holds the information of the tangent space of $H_g$ at $P_i$'s. Let $T$ be the subset of sections whose tangent space at $P_i$ coincides with that of $H^{(i)}$. Note that we care concerned it there is a $g$ whose *image* in $T$ has the desired tangent spaces, but $T$ itself is nonempty since we may choose components in $H^0(Z, \mathcal{O}_Z) = \prod_i H^0(Y, \mathcal{O}_Y)$ separately. As in Theorem 3.1, we define

$$\mathcal{P} = \{g \in S_{\text{homog}} : H_g \cap U \textit{ is smooth of dimension } m-1 \textit{ and } f \mid_Z \in T\}$$

Note that $H_g \in \mathcal{P}$ is guaranteed to be smooth on $U = \mathbb{P}^n - Z$ directly, we know they are also smooth on $Z$ simply because we required the tangent space at these points to be of dimension $n-1$. Therefore hypersurfaces in $\mathcal{P}$ are smooth actually everywhere. □

**Remark 5.2.** The above proof shows it is useful to retain some control over the local behavior using $T$ as in Theorem 3.1. In my interpretation of Poonen's proof is correct, then I guess it is more rigorous to say we pick $P_i$'s at which $H^{(i)}$ is *smooth* of dimension $n-1$. It is always possible to do so it does not matter that much though.

**Conjecture 5.3.** *Let $X$ be an integral quasiprojective subscheme of $\mathbb{P}^n_{\mathbb{Z}}$ that is smooth over $\mathbb{Z}$ of relative dimension $r$. There exists $c > 0$ such that if $d, p >> 0$,*

$$\frac{\#\{f \in S_{d,p} : \dim (H_f \cap X_p)_{\text{sing}} \geq 1\}}{\# S_{d,p}} < \frac{c}{p^2}$$

Recall that $\operatorname{Spec} \mathbb{F}_{\text{p}} \to \operatorname{Spec} \mathbb{Z}$ is a closed immersion and closed immersion is stable under base extension. Therefore $X_p \to X$, and hence $X_p \to \mathbb{P}^n_{\mathbb{Z}}$ is a closed immersion.

new paragraph

# 6 Reflections

## 6.1 Degree and smoothness

I think the driving force for Theorem 3.1 to be true is encoded in Lemma 4.1.

Let us first look back at the benchmark example. For $p, q$ two different primes, CRT tells us that

$$\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/q^2\mathbb{Z}$$

The surjectivity means that "modulo $p^2$" and "modulo $q^2$" are independent events. Clearly, say $\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ is not surjective since it is impossible to be $0 \mod 4$ and $3 \mod 6$. CRT treats $\mathbb{Z}$ as a whole so are actually saved of the trouble to take the limit as in the definition of $\mu(S_r)$ when computing it. However, if we think about $\mu(S_r)$ in terms of its definition we do find that "divisible by $p^2$" and "divisible by $q^2$" are *not* independent events for $\mathbb{N} \cap [1, B]$ instead of all of $\mathbb{N}$. For example among numbers $1, 2, \cdots, 10$, "divisible by 2" does tell us something about "divisible by 3" since the probability that a randomly chosen number is 6 becomes higher once conditioned on "divisible by 2". However, we see that this interference vanishes once $[1, B]$ gets closer and closer to all of $\mathbb{N}$. In short, CRT first justifies our intuition that "divisible by $p^2$" and "divisible by $q^2$" are independent. Then we justify intuition when we generalize to infinitely many primes.

If we compare the two definitions of $\mu$, we find that, roughly speaking, "asympotically good for $B \to \infty$" is replaced by "asympotically good for $d \to \infty$".

Invoking the powerful theorem by Serre is certainly to quick way to prove Lemma 4.1 in great generality. However, I would like to point out my guess of the intuitive reason that this should be true. Recall that if $Y \to \operatorname{Spec} \mathrm{k}$ is a finite morphism, then $Y$ is a finite union of points with discrete topology, and the residue field of each of the points in $Y$ is a finite extension of $k$. By Nullstellensatz $Y$ is actually a finite set of *closed* points on $\mathbb{P}^n$ and again we further assume that $Y \subseteq \mathbb{A}^n_0$. In the special case when $k$ is algebraically closed and $n = 1$ we see that the surjectivity can be shown directly by Lagrange interpolation.

As the degree of a polynomial gets higher, we can infer less and less of the value of a point out of its values at other points. And I think this is the intuitive reason that allows us to think of "smooth at P" and "smooth at Q" as being independent events for $H_f$, $\deg f >> 0$ from the first place. Overall, Lemma 4.1 assumes a function similar to that of CRT in the proof.

## 6.2 Medium degree vs. high degree

I am curious why the degrees were divided in such way. In this section I am trying to understand what such division into cases is necessary or advisable.

## 6.3 Poonen's decoupling trick

I am trying to make the decoupling trick appear in a more natural way, since at first I found the trick completely magic. We make sure that all $f$ will be covered by inserting $f_0$, so $f_0$ could be seen as the "base" and those $g_i$'s and $h$ appear at first to be pretty arbitrary pertubations, in the sense that they only affect certain coefficients of $f_0$, and the aesthetic appeal is further hurt by $\lfloor\ \rfloor$ operation. Throughout the proof we worked hard on $g_i$'s and $h$ and then harvest a powerful conclusion on $f$. That is why I found the proof even a bit striking at first.

Let us the recall overall strategy in Poonen's decoupling trick. From a vector space $A$, we constructed another vector $\mathcal{D}$, and two projections $p_1$ and $\varphi$:

$$\begin{tikzcd}
\mathcal{D} \arrow[d, "p_1"] \arrow[dr, "\varphi"] & \\
F \arrow[r, "="] & A
\end{tikzcd}$$

where $F$ is simply just another copy of $A$. Now there is a subset $T \subseteq A$ and we are interested in bounding the fraction $|T|/|A|$. However, we bounded the fraction

$$\frac{|p_1^{-1}(P) \cap \varphi^{-1}(A)|}{|p_1^{-1}(P)|}$$

for a generic $P \in F$.

This senario can appear in a differential geometric setting as well. Consider the tangent bundle $TS^2$ of $S^2$. There are two natural ways to project $TS^2 \to S^2$. One is of course, straightforward $(p, v) \mapsto p$. The other one is to use the exponential map. Actually to obtain a better analogy we may feel free to replace $TS^2$ by any sub-bundle ot it. Now consider a subset $T \subseteq S^2$. To grab distribution of $T$ directly is hard, but we have some information of the orbits of a point under certain classes of variations (encoded by the sub-bundle), then we may go to the bundle and reconstruct the information on $T$.

Under this point of view I may call it "twisted scanning trick" and I see a possibility that we can generalize this idea.

## 6.4 Possible directions of generalization

We often construct new schemes out of old ones. How does $\mu(\mathcal{P})$ behave under classical constructions? Here are some questions that I can think of

1. Say $X$ is a curve with a node, so it is in particular smooth. Can we obtain information on $\mu(\mathcal{P}_X)$ from $\mu(\mathcal{P}_{X'})$ where $X'$ is the blow up at the singularity? Well I guess the singular case was not treated in classical Bertini either.

Some possible directions for future work may have a computational concern.

1. Is there an incidence that for a smooth $X$ as in Theorem 1.2, $\mu(\mathcal{P})$ is easier to compute from definition, or via other means, than $\zeta_X(m+1)^{-1}$?

2. If $\mu(\mathcal{P})$ behaves better than $\zeta_X(m+1)^{-1}$ for certain classical constructions, at least when doing proofs, then indeed it is not impossible to make inference backwards. Plus to compute $\zeta_X(m+1)^{-1}$ we may have to know the exact distribution of degrees of points, but it would then allow us to compute $\zeta_X(s)$ for arbitrary $s$. It is possible that $s = m+1$ happens to behave well in some circumstances?

## 6.5 Intrinsic?

As Poonen has remarked, one observation of Theorem 1.2 is that $\mu(\mathcal{P})$ is intrinsic in the sense that it is independent of the choice of embedding $X \hookrightarrow \mathbb{P}^n$. Can we see the fact without the full power of Theorem 1.2?

We note that $H_f \cap X$ is in particular a subscheme of $X$? Is there an intrinsic description of "all possible hypersuface sections when embedded in a projective space"? I think it makes an intuitive sense. Suppose $X \subset \mathbb{A}^n$ is affine, then $H_f \cap X$ could be understood as the subscheme cut out by the untwisting of $f$, which restricts to a regular function on $X$. But once $X \hookrightarrow \mathbb{P}^n$, $\mathcal{O}_{\mathbb{P}^n} \to \mathcal{O}_X$ is surjective anyways.

## 6.6 Questions

1. I got confused with the $U$ as in Theorem 3.1 when I was writing the proof for Theorem 5.1. Do we first think of $U$ as the open set on $X$ at first and then give it the open subscheme structure.