Probability of System of Parameters

Notes by: Juliette Bruce

Given k homogenous polynomials in $n+1$ variables what do expect about the dimension of their zero set? Well a good guess would be that each polynomial imposes a dimension one condition and so their zero set should have dimension $n-(k+1)$. In this talk I will discuss how over a finite field may be able to put this intuition to the test. This is based on joint with Daniel Erman.

University of Wisconsin - Monday, February 29, 2016

Table of Contents

1. Introduction

1.1 Motivation

Suppose some one hands you homogenous polynomials $f_0,\dots,f_k \in S = k[x_0,\dots,x_n]$ of degree d, where k is a field, what do you expect about the dimension of $\mathbb{V}(f_0,\dots,f_k) \subset \mathbb{P}^n_k$? Well intuitively each polynomial *should* cut down one dimension, and so we would expect that:

$$\dim \mathbb{V}(f_0,\dots,f_k) = n-(k+1).$$

In fact by Krull's Height theorem we know that:

$$\dim \mathbb{V}(f_0,\dots,f_k) \geq n-(k+1).$$

Helpful Background:

Theorem 1.1.1 (Krull's Height Theorem). *If $x_1,\dots,x_c$ are elements in a Noetherian ring R and $P \subset R$ is a prime ideal minimal over $\langle x_1,\dots,x_c\rangle$ then:*

$$codim P = \dim R_P = \sup\left\{\begin{array}{c}\text{lengths of chains}\\ \text{of primes}\\ \text{descending from } P\end{array}\right\} \leq c.$$

Proof. We proceed by induction upon c with $c=1$ serving as the base case, itself know as Krull's Principal Ideal Theorem. In this case we begin by reducing to the case when R is local by letting $R = R_P$. Now letting $Q \subset P$ be a prime ideal it is enough to show that $\dim Q = 0$. Now we get a decending chain of ideals:

$$P \supset Q^{(1)} + \langle x_1\rangle \supset Q^{(2)} + \langle x_1\rangle \supset \cdots \supset Q^{(n)} + \langle x_1\rangle \supset Q^{(n+11)} + \langle x_1\rangle \supset \cdots,$$

which by a relation between minimality and Artinian stabilizes as $R/\langle x_1\rangle$ is Artinian. (Here $Q^{(n)}$ is the nth symbolic power i.e. $r \in R$ such that $sr \in Q^n$ for $s \in R\setminus Q$.)Hence we get that $Q^{(n)}+\langle x_1\rangle$ is equal to $Q^{(n+1)}+\langle x_1\rangle$. By chasing definitions using the minimality of P we find that $Q^{(n)} = Q^{(n+1)} + x_1 Q^{(n)}$ from which the desired result follows by Nakayama's Lemma being applied twice. (Once to show that $Q^{(n+1)} = Q^n$ and then using this to show R_Q is zero dimensional.)

In the inductive step we once again reduce to the local case by replacing R with R_P. Now let $P_1 \subsetneq P$ be a prime ideal such that there are no prime ideals between P_1 and P. This implies that $\dim P$ is equal to $\dim P_1 + 1$, and so by induction it suffices to show that P_1 is minimal over some set of elements $\langle y_1,\dots,y_{c-1}\rangle$. The ideal is to show that there exists an $N \gg 0$ such that $x_i^N = y_i + a_i x_i$ for $a_i \in R$ and $y_i \in P_1$. Finally one must show that P_1 is minimal over these y_i. (Note the proof uses characterizations of Artinian rings and Nakayama's Lemma in was I require the Noetherian assumption.) □

Remark 1.1.1. *Now by the Nullstellensatz we know that if $I \subset k[x_0,\dots,x_n]$ then $\dim I = \dim \mathbb{V}(I) - 1$. (The minus one arriving because we are in projective space.) Hence we see that Krull's Height Theorem says that*

$$n - \dim \mathbb{V}(I) = \dim \mathbb{V}(I) \leq (k+1),$$

which of course implies that $\dim \mathbb{V}(I)$ is bounded above by $n-(k+1)$. (Note here we are using the fact that $k[x_0,\dots,x_n]$ is an affine domain so that $\dim I + \dim I = n$. In general this need not hold for even affine rings.)

We call a collection of polynomials $f_0,\dots,f_k$, which achieves the expected dimension a **system of parameter**. The goal of this talk is to try and answer the following question:

Question 1.1.1. *Is our intuition any good? That is, are most collections of polynomials systems of parameters?*

1.2 Refining Our Question

Of course not every collection of polynomials $f_0,\dots,f_k$ are a system of parameters. For example, if $f_i = f_j$ then $f_0,\dots,f_k$ clearly cannot be a system of parameters. More concretely $f_0 = x^2 - y^2$ and $f_1 = x^2 - xy$ is not

a system of parameters. This is because f_0 and f_1 both vanish along the line $x = y$, and so their intersection is one dimensional not zero.

That said if the condition of whether or not $f_0, \ldots, f_k$ form a system of parameters is an algebraic one. Specifically we can view the set of homogenous polynomials of degree d as $\mathbb{A}^m$ where $m = \binom{n+d}{d}$. (We think of a point in $\mathbb{A}^m$ as giving the coefficients on each monomial of degree d.) Then the set of tuples in $(\mathbb{A}^m)^{k+1}$, which fail to be system of parameters is a Zariski closed subset. This is not the focus of my talk, and so I do not want to go into the details of showing why this is true. So instead proof by example!

Example 1.2.1. *If we take $d = 1$ so that $f_0, \ldots, f_k$ are linear linear forms, i.e. they define hyperplanes, we see that whether the condition of whether they form a system of parameters is a determinantal one. In particular, by duality hyperplanes of dimension $n-1-k$ correspond to hyperplanes in $(\mathbb{P}^n)^\vee$ of dimension k. That is to say a hyperplane in $\mathbb{P}^n$ correspond to points in $(\mathbb{P}^n)^\vee$. Thus, hyperplanes $H_0, \ldots, H_k$ in $\mathbb{P}^n$ will intersect in the correct dimension if and only if the corresponding points in $(\mathbb{P}^n)^\vee$ are linearly independent. Therefore, if we let*

$$f_i = f_{i0}x_0 + f_{i1}x_1 + \cdots + f_{in}x_n$$

so that the f_{ij} are the coordinates of $(\mathbb{P}^n)^k$ then the locus of linear forms, which fail to be systems of parameters is given by:

$$\mathbb{V}\left(\begin{array}{c} (k+1)\times(k+1) \\ \text{minors of} \end{array} \begin{pmatrix} f_{00} & f_{01} & \cdots & f_{0n} \\ f_{10} & f_{11} & \cdots & f_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ f_{k0} & f_{k1} & \cdots & f_{kn} \end{pmatrix} \right) \subset (\mathbb{P}^n)^k.$$

So for example, if we let $k = 1$ and $n = 2$ we see that:

$$\left\{ \begin{array}{c} \text{locus corresponding to} \\ \text{linear forms } (f_0, f_1) \text{ on } \mathbb{P}^2 \\ \text{which are not parameters} \end{array} \right\} = \mathbb{V}\left(\begin{array}{c} 2\times 2 \\ \text{minors of} \end{array} \begin{pmatrix} f_{00} & f_{01} & f_{02} \\ f_{10} & f_{11} & f_{12} \end{pmatrix} \right)$$

$$= \mathbb{V}(f_{00}f_{11} - f_{01}f_{10},\ f_{00}f_{12} - f_{02}f_{10},\ f_{01}f_{12} - f_{02}f_{11}) \subset (\mathbb{P}^2)^2.$$

Note that the codimension of the determinantal variety given by $(k+1)\times(k+1)$ minors of a $(n+1)\times(k+1)$ matrix is $(n+1-(k+1)+1)(k+1-(k+1)+1) = (n-k+1)$. (The codimension of determinantal varieties was worked out by Jack Eagon in his thesis, and can be found as Exercises 10.9 and 10.10 in [Eis95].*)*

Helpful Background:

Definition 1.2.1. *If V is a finite dimensional vector space and $U \subset V$ a subspace then the **annihilator of** U is the subspace $U^o \subset V^\vee$ given by:*

$$U^o = \{\phi \in V^\vee \mid \phi(U) = 0\}.$$

Lemma 1.2.1. *If V is a n-dimensional vector space and $U \subset V$ a k-dimensional subspace then*

$$\dim V = \dim U + \dim U^o.$$

Proof. Let $e_1, \ldots, e_n$ be a basis for V such that $e_1, \ldots, e_k$ are a basis for U. Now if $\phi_1, \ldots, \phi_n$ are the dual basis for $V^\vee$ we see that $\phi_{k+1}, \ldots, \phi_n$ form a basis for U^o. □

Remark 1.2.1. *If we think geometrical and associate $V^\vee$ with $V^\perp$ via the inner product then this makes sense since $U^o = U^\perp$.*

Proposition 1.2.1. *Let V be an $n+1$ dimensional vector space. There is a one to one correspondence*

$$\left\{ \begin{array}{c} \text{Linear subspaces of } \mathbb{P}(V) \\ \text{of dim. } k \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{Linear subspaces of } \mathbb{P}(V^\vee) \\ \text{of dimension } n-m-1. \end{array} \right\}$$

Proof. If $H \subset \mathbb{P}(V)$ is an m-dimensional linear subspace then $H = \mathbb{P}(U)$ for some subspace $U \subset V$ of dimension $m+1$. Now by Lemma 1.2.1 we know that $U^o \subset V^\vee$ has dimension $(n+1)-(m+1) = n-m$. Hence $\mathbb{P}(U^o) \subset \mathbb{P}(V^\vee)$ is a linear subspace of dimension $n-m-1$. Finally using the fact that $(U^o)^o = U$ we see that this correspondence is in fact a bijection. □

Notice over an infinite field this says that our intuition is quite good. For example, if we are working over $\mathbb{C}$ then the space of things failing to be systems of parameters has Lesbuege measure zero. That said over a finite field things are quite different. It is still true that the set of tuples in $(\mathbb{A}^m)^{k+1}$, which fail to be system of parameters form a Zariski closed subset, but this no longer caries as much weight. In particular, over a finite field Zariski closed subsets can contain arbitrarily many of the points. For example, if $a, \dots, a_r \in \mathbb{F}_q$ then $f(x) = (x-a_1)\cdots(x-a_r)$ is a polynomial vanishing on all r points.

Hence over $\mathbb{F}_q$ the fact that failing to be a system of parameters is a Zariski closed condition is not a satisfying answer to Question 1.1.1. That said when working over a finite field it turns out it makes sense to discuss some notion of the "probability" of a collection $f_0, \dots, f_k$ of polynomials is a system of parameters. (Fair warning I am being intentionally vague here, and will clarify what precisely I mean shortly.)

Taking this perspective, work of Daniel Erman and myself, which should appear on the arXiv in the coming weeks, provides the following answer to motivating question.

Theorem 1.2.1 (Bruce-Erman,[BK12])**.**

$$\lim_{d\to\infty} \textbf{Prob}\begin{pmatrix}(f_0,\dots,f_k) \textit{ of degree } d\\ \textit{are parameters on } \mathbb{P}^n\end{pmatrix} = \begin{cases}1 & \textit{if } k<n\\ \zeta_{\mathbb{P}^n}(n+1)^{-1} & \textit{if } k=n\end{cases}$$

In the above theorem $\zeta_{\mathbb{P}^n}$ is the Hasse-Weil ζ-function of $\mathbb{P}^n$. Recalling that if X is a "nice variety" – i.e. a scheme of finite type over $\mathbb{F}_q$ – then the zeta function of X is defined to be:

$$\zeta_X(s) := Z_X(q^{-s}) = (\prod_{p\in X^c}\left(1-q^{-s\deg(p)}\right)^{-1} = \exp\left(\sum_{t=1}^{\infty}\frac{\#X(\mathbb{F}_{q^t})}{t}q^{-ts}\right)$$

where X^c is the closed points of X [Wei49]. In the case of $\mathbb{P}^n$ we see that:

$$\zeta_{\mathbb{P}^n}(s)^{-1} = (1-q^{-s})(1-q^{-s+1})\cdots(1-q^{-s+n}),$$

and so $\zeta_{\mathbb{P}^n}(n+1)^{-1}$ is some number between zero and one.

q \ n	2	3	6	10
2	$\frac{21}{64}$	$\frac{315}{1024}$	$\frac{78129765}{268435456}$	$\approx .2889$
3	$\frac{416}{792}$	$\frac{33280}{59049}$	$\frac{12816818094080}{22876792454961}$	$\approx .5601$
5	$\frac{11904}{15625}$	$\frac{7428096}{9765625}$	$\approx .7603$	$\approx .7603$
7	$\frac{98496}{117649}$	$\approx .8369$	$\approx .8363$	$\approx .8368$
191	$\approx .9947$	$\approx .9947$	$\approx .9947$	$\approx .9947$

FIGURE 1. Values of $\zeta_{\mathbb{P}^n}(n+1)^{-1}$ over $\mathbb{F}_q$ for various values of (n,q).

Hence Theorem 3.1.1 in essence says that our intuition is correct, but wavers slightly in the maximal case when $k=n$.

Helpful Background:

Proposition 1.2.2. *If X is a scheme of finite type over $\mathbb{F}_q$ then*

$$\#X(\mathbb{F}_{q^t}) = \sum_{d|t} d\#\{x \in X^c \mid \deg(x) = d\}.$$

Proof. If we assume that X is a reduced scheme of finite type over $\mathbb{F}_q$ then there is an open affine cover $\{U_i\}$ of X such that $\mathcal{O}_X(U_i)$ is a finitely generated $\mathbb{F}_q$-algebra. Hence we see that for such a scheme if $x \in X$ is a closed point the **residue field** $k(x) = (\mathcal{O}_{X,x}/\mathfrak{m}_x)$ is a finite extension of $\mathbb{F}_q$. (This is because Jacobson version of the Nullstellensatz says a finitely generated algebra over a Jacobson ring is Jacobson, and the extension of residue fields is finite.) So we may define the degree $\deg(x) = [k(x) : \mathbb{F}_q]$.

Now the $\mathbb{F}_{q^t}$ points of X are in bijection with the $\mathbb{F}_q$-scheme morphisms $\operatorname{Spec}\mathbb{F}_{q^t} \longrightarrow X$, which means:

$$X(\mathbb{F}_{q^t}) = \operatorname{Hom}_{\mathbb{F}_q}(\operatorname{Spec}(\mathbb{F}_{q^t}, X) = \bigsqcup_{\deg(x)|t} \operatorname{Hom}_{\mathbb{F}_q}(k(x), \mathbb{F}_{q^t}).$$

Notice the Galois group $Gal(\mathbb{F}_{q^t}/\mathbb{F}_q)$ acts transitively upon $\operatorname{Hom}_{\mathbb{F}_q}(k(x), \mathbb{F}_{q^t})$ by post-composition. Moreover the things stabilizer of a point is exactly those automorphism of $\mathbb{F}_{q^t}$ fixing $k(x)$ i.e. the stabilizer is $Gal(\mathbb{F}_{q^t}/k(x))$. Thus, since $Gal(\mathbb{F}_{q^t}/\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/t\mathbb{Z}$ and $Gal(\mathbb{F}_{q^t}/k(x))$ is isomorphic to $\mathbb{Z}/(t/\deg(x))\mathbb{Z}$ we get that $\operatorname{Hom}_{\mathbb{F}_q}(k(x), \mathbb{F}_{q^t})$ has order $\deg(x)$. □

Proposition 1.2.3. *If X is a scheme of finite type over $\mathbb{F}_q$ then as formal power series:*

$$Z_X(t) = \exp\left(\sum_{m\geq 1} \frac{\#X(\mathbb{F}_{q^m})}{m} t^m\right) = \prod_{x \in X^c} \left(1 - t^{\deg(x)}\right)^{-1}.$$

Proof. Let n_d be equal to the number of closed points on X of degree d i.e.

$$n_d = \#\{x \in X^c \mid \deg(x) = d\}.$$

Now by Proposition 1.2.2 we have:

$$\log(Z_X(t)) = \sum_{m\geq 1} \frac{\#X(\mathbb{F}_{q^m})}{m} t^m = \sum_{m\geq 0}\left(\sum_{d|m} \frac{dn_d}{m}\right) t^m = \sum_{d\geq 1} n_d \left(\sum_{e\geq 1} \frac{t^{er}}{e}\right) = \sum_{d\geq 1} -n_d \log(1-t^d) = \log\left(\prod_{d\geq 1} (1-t^d)^{-n_d}\right).$$

□

Proposition 1.2.4. *If X is a scheme of finite type over $\mathbb{F}_q$ and $Y \subset X$ is a closed subscheme then letting $U = X \setminus Y$*

$$Z_X(t) = Z_Y(t) \cdot Z_U(t)$$

Example 1.2.2. *Using the above proposition we can easily compute the zeta function of $\mathbb{P}^n$ by induction upon n. In particular, recall we have a natural closed inclusion $\mathbb{P}^{n-1} \subset \mathbb{P}^n$, and the complement is $\mathbb{A}^n$ meaning that the above proposition implies:*

$$Z_{\mathbb{P}^n}(t) = \mathbb{Z}_{\mathbb{P}^{n-1}}(t) \cdot \mathbb{Z}_{\mathbb{A}^n}(t).$$

Now to compute the zeta function of $\mathbb{A}^n$ we just note that $\mathbb{A}^n(\mathbb{F}_{q^m}) = q^{mn}$, and so by definition

$$Z_{\mathbb{A}^n}(t) = \exp\left(\sum_{m\geq 0} \frac{\#\mathbb{A}^n(\mathbb{F}_{q^m}}{m} t^m\right) = \exp\left(\sum_{m\geq 0} \frac{q^{mn}}{m} t^m\right) = \frac{1}{1-q^n t}.$$

From this we see that

$$Z_{\mathbb{P}^n}(t) = \frac{1}{(1-t)(1-qt)\cdots(1-q^n t)}.$$

The goal for the remainder of this talk is to try understand Theorem 3.1.1 i.e. to understand how likely systems of parameters are over finite fields. Put somewhat more formally let:

$$S_d = \mathbb{F}_q[x_0,\dots,x_n]_d = \left\{\begin{matrix}\text{homogenous polynomials}\\ \text{of degree } d\end{matrix}\right\} = \text{Span}_{\mathbb{F}_q}\left\langle\begin{matrix}\text{monomial of degree } d\\ \text{in } x_0,\dots,x_n\end{matrix}\right\rangle = H^0(\mathbb{P}^n,\mathcal{O}_{\mathbb{P}^n}(d))$$

and

$$\mathcal{P}_{d,k} = \left\{\begin{matrix}(f_0,\dots,f_k)\\ \text{are parameters on } \mathbb{P}^n\end{matrix}\right\} \subset S_d^{k+1}.$$

Then our question of interest, which we will try and answer in this talk is:

Question 1.2.1. *Does the following limit exist and if so what is it and its asymtoptics:*

$$\lim_{d\to\infty} \textbf{Prob}\left(\begin{matrix}f_0,\dots,f_k \text{ of degree } d\\ \text{are parameters on } \mathbb{P}^n\end{matrix}\right) = \lim_{d\to\infty} \textbf{Prob}(\mathcal{P}_{d,k}) := \lim_{d\to\infty} \frac{\#\mathcal{P}_{d,k}}{\#S_d^{k+1}}?$$

Helpful Background:

Theorem 1.2.2. *Let $S = A[x_0,\dots,x_n]$ where A is a ring then there is a natural isomorphism*

$$\Gamma_*(\mathbb{P}^n,\mathcal{O}_{\mathbb{P}^n}) = \bigoplus_{d\in\mathbb{Z}} \mathbb{H}^0(\mathbb{P}^n,\mathcal{O}_{\mathbb{P}^n}(d)) \cong S$$

Proof. Let $\{\mathcal{U}_i\}$ be the standard affine open cover of $\mathbb{P}^n$ i.e. $\mathcal{U}_i = D_+(x_i)$. Now the sheaf axioms giving a global section $s \in \Gamma(\mathbb{P}^n,\mathcal{O}_{\mathbb{P}^n}(d))$ is equivalent to giving a collection of sections $s_i \in \mathcal{O}_{\mathbb{P}^n}(d)(\mathcal{U}_i)$ such that s_i and s_j agree on the intersection $\mathcal{U}_i \cap \mathcal{U}_j = D_+(x_ix_j)$. By construction such s_i is just homogenous element of degree d in $S[x_i^{-1}]$ and its restriction to $\mathcal{U}_i \cap \mathcal{U}_j = D_+(x_ix_j)$ is just the image of s_i under the localization map

$$S[x_i^{-1}] \longrightarrow S[(x_ix_j)^{-1}].$$

Hence we see that we may identify $\Gamma_*(\mathbb{P}^n,\mathcal{O}_{\mathbb{P}^n})$ is tuples $(s_0,\dots,s_n)$ such that $s_i \in S[x_i^{-1}]$ subject to the restraint that s_i and s_j have the smae image under the localization map above. That is we have the following diagram

$$\Gamma_*(\mathbb{P}^n,\mathcal{O}_{\mathbb{P}^n}) \hookrightarrow \bigoplus_{i=0}^{n} S\left[\frac{1}{x_i}\right] \hookrightarrow \bigoplus_{i,j} S\left[\frac{1}{x_ix_j}\right] \hookrightarrow S\left[\frac{1}{x_0\cdots x_n}\right]$$

where the arrows are all inculsions because the x_i are non-zero divisors and hence all the localization maps are in fact injective. Hence $\Gamma_*(\mathbb{P}^n,\mathcal{O}_{\mathbb{P}^n})$ is the intersection of $S[x_i^{-1}]$ as subsets of $S[(x_0\cdots x_n)^{-1}]$. Now an element of $S[(x_0\cdots x_n)^{-1}]$ can be written as $x_0^{e_0}\cdots x_n^{e_n}f$ where f is a homogenous polynomial not divisible by x_i and $e_i \in \mathbb{Z}$. However, from this it is clear that an element of $S[(x_0\cdots x_n)^{-1}]$ is in $S[x_i^{-1}]$ if and only if $l_i \geq 0$, from which the claim is clear. □

Theorem 1.2.3.

$$H^k(\mathbb{P}^n,\mathcal{O}_{\mathbb{P}^n}(d)) = \begin{cases} k[x_0,\dots,x_n]_d & \text{if } k = 0\\ \left(\frac{1}{x_0\cdots x_n}k\left[\frac{1}{x_0},\cdots,\frac{1}{x_n}\right]\right)_d & \text{if } k \equiv n\\ 0 & \text{else}\end{cases}$$

Corollary 1.2.1.

$$h^k(\mathbb{P}^n,\mathcal{O}_{\mathbb{P}^n}(d)) = \begin{cases} \binom{n+d}{d} & \text{if } k = 0\\ \binom{-(d+1)}{-(n+d+1)} & \text{if } k \equiv n, d \leq -(d+1)\\ 0 & \text{else}\end{cases}$$

Helpful Background:

Example 1.2.3. *Warning if $Z \subset \mathbb{P}^n$ is a projective variety it is generally not the case that $\Gamma^*(Z,\mathcal{O}_Z)$ is isomorphic to its homogenous coordinate ring R. (Recall the homogenous coordinate ring is defined as S/I where $I = \Gamma_*(\mathbb{P}^n,\mathcal{I}_Z)$ where $\mathcal{I}_Z$ is the ideal sheaf defining Z.) For example, let $Z \subset \mathbb{P}^3$ be the image of the following morphism:*

$$\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^3 \qquad \text{given by} \qquad [s:t] \longmapsto [s^4 : s^3t : st^3 : t^4]$$

Now from the usual short exact sequence we get a long exact sequence of sheaves:

$$0 \longrightarrow H^0(Z,\mathcal{I}_Z(1)) \longrightarrow H^0(\mathbb{P}^3,\mathcal{O}_{\mathbb{P}^3}(1)) \longrightarrow H^0(Z,\mathcal{O}_Z(1)) \longrightarrow H^1(Z,\mathcal{I}_Z(1)) \longrightarrow H^1(\mathbb{P}^3,\mathcal{O}_{\mathbb{P}^3}(1)) \longrightarrow \cdots$$

Notice that since ϕ is a closed embedding of degree four $\mathcal{O}_Z(1) \cong \mathcal{O}_{\mathbb{P}^1}(4)$. Using Theorem 1.2.3:

$$\begin{aligned} h^1(Z,\mathcal{I}_Z(1)) &= h^0(Z,\mathcal{I}_Z(1)) - h^0(\mathbb{P}^3,\mathcal{O}_{\mathbb{P}^3}(1)) + h^0(Z,\mathcal{O}_Z(1)) \\ &= h^0(Z,\mathcal{I}_Z(1)) - h^0(\mathbb{P}^3,\mathcal{O}_{\mathbb{P}^3}(1)) + h^0(\mathbb{P}^1,\mathcal{O}_{\mathbb{P}^1}(4)) = h^0(Z,\mathcal{I}_Z(1)) - \binom{3+1}{1} + \binom{1+4}{4} \geq 1 \end{aligned}$$

Remark 1.2.2. *Before moving on let me take a quick moment for some preemptive disambiguation:*

- *I am (almost) always working over a finite field $\mathbb{F}_q$ with q-elements.*
- *By variety I mean projective reduced scheme over $\mathbb{F}_q$, but do not assume irreducibility i.e. $\mathbb{P}^n = \mathbb{P}^n_{\mathbb{F}_q}$.*
- *When I say "polynomial" I mean homogenous polynomial of positive degree.*
- *If you replace $\mathbb{P}^n$ with a projective scheme X of dimension n everything works essentially the same way.*

2. A First Guess

2.1 Local Probabilities

Now $f_0,\ldots,f_k$ form a system of parameters if and only if $\mathbb{V}(f_0,\ldots,f_k)$ has dimension $n-(k+1)$ i.e. so long as $f_0,\ldots,f_k$ do not vanish along a subvariety of dimension $n-(k+1)+1 = n-k$. With this in mind it will be useful for us to understand the probability $(k+1)$ randomly chosen polynomials vanish along a fixed $(n-k)$-dimensional variety$Z$. This is exactly what the following lemma does:

Lemma 2.1.1. *If $Z \subseteq \mathbb{P}^n$ is a projective variety over $\mathbb{F}_q$ with ideal sheaf $\mathcal{I}_Z$ then for all $d > reg(\mathcal{I}_Z)$ where $reg(\mathcal{I}_Z)$ is the Custulunvo-Mumuford regularity:*

$$\textbf{Prob}\begin{pmatrix} f_0,\ldots,f_k \text{ of degree } d \\ \text{vanish along } Z \end{pmatrix} = q^{-(k+1)h^0(Z,\mathcal{O}_Z(d))}.$$

Proof. From the short exact sequence of sheaves:

$$0 \longrightarrow \mathcal{I}_Z(d)^{\oplus(k+1)} \longrightarrow \mathcal{O}_{\mathbb{P}^n}(d)^{\oplus(k+1)} \longrightarrow \mathcal{O}_Z(d)^{\oplus(k+1)} \longrightarrow 0,$$

we get the following associated long exact sequence on cohomology:

$$0 \longrightarrow H^0(Z,\mathcal{I}_Z(d))^{\oplus(k+1)} \longrightarrow H^0(\mathbb{P}^n,\mathcal{O}_{\mathbb{P}^n}(d))^{\oplus(k+1)} \longrightarrow H^0(Z,\mathcal{O}_Z(d))^{\oplus(k+1)} \longrightarrow H^1(Z,\mathcal{I}_Z(d))^{\oplus(k+1)} \longrightarrow \cdots.$$

Now when $d > \text{reg}(\mathcal{I}_Z)$ we have that $H^1(Z,\mathcal{I}_Z(d))$ vanishes meaning the above becomes the following short exact sequence:

$$0 \longrightarrow H^0(Z,\mathcal{I}_Z(d))^{\oplus(k+1)} \xrightarrow{\phi} H^0(\mathbb{P}^n,\mathcal{O}_{\mathbb{P}^n}(d))^{\oplus(k+1)} \longrightarrow H^0(\mathcal{O}_Z(d))^{\oplus(k+1)} \longrightarrow 0.$$

After having identified S_d with $H^0(\mathbb{P}^,\mathcal{O}_{\mathbb{P}^n}(d))$ we see that $f_0,\dots,f_k$ vanish along Z if and only if it is in $H^0(Z,\mathcal{I}_Z(d))^{\oplus(k+1)}$ i.e. in the kernel of ϕ.So we have that:

$$\textbf{Prob}\left(\begin{matrix}f_0,\dots,f_k \text{ of degree } d\\ \text{vanish along } Z\end{matrix}\right) = \frac{\#H^0(Z,\mathcal{I}_Z(d))^{\oplus(k+1)}}{\#H^0(\mathbb{P}^n,\mathcal{O}_{\mathbb{P}^n}(d))^{\oplus(k+1)}} = q^{(k+1)(h^0(Z,\mathcal{I}_Z(d))-h^0(\mathbb{P}^n,\mathcal{O}_{\mathbb{P}^n}(d)))} = q^{-(k+1)h^0(Z,\mathcal{O}_Z(d))}.$$

Notice the last equality follows from the fact that dimension is additive in short exact sequences of vector spaces, and so the short exact sequence above gives us:

$$h^0(\mathbb{P}^n,\mathcal{O}_{\mathbb{P}^n}(d)) - h^0(Z,\mathcal{I}_Z(d)) = h^0(Z,\mathcal{O}_Z(d)).$$

□

Before moving on let us briefly recall a few facts regarding $h^0(Z,\mathcal{O}_Z(d))$ as a function of d, which we will summarize in the following propoisition:

Proposition 2.1.1. *Let $Z \subset \mathbb{P}^n$ be a closed subvariety then there exists a polynomial $P_Z(d)$ such that $P_Z(d) = h^0(Z,\mathcal{O}_Z(d))$ for $d \gg 0$. Moreover we know that:*

(a) $P_Z(d) = \frac{\deg(Z)}{\dim Z!}d^{\dim Z} + O(Z^{\dim Z-1})$

(b) $\chi(Z,\mathcal{O}_Z(d)) = P_Z(d)$

For us the important take away from this is that if $Z \subset \mathbb{P}^n$ has dimension $(n-k)$ and degree e then $h^0(Z,\mathcal{O}_Z(d))$ is asymptotic to $\frac{e}{(n-k)!}d^{n-k}$.

Helpful Background:

Lemma 2.1.2. *If f is an integer function and $\delta(f) = f(n) - f(n-1)$ is a polynomial of degree d then f is a polynomial of degree $d+1$.*

Proposition 2.1.2. *If $\mathcal{F}$ is a coherent sheaf on a projective scheme $Z \subset \mathbb{P}^n$ then $\chi(Z,\mathcal{F}(d))$ is a polynomial of degree* $\dim(supp(\mathcal{F}))$.

Proof. First we reduce to the case of an infinite field using the fact cohomology respects base change i.e.

$$h^i(Z,\mathcal{F}(d)) \otimes_k \overline{k} = h^i(Z_{\overline{k}},\mathcal{F} \otimes_k \overline{k}(d)).$$

Now we proceed by induction upon $\dim \text{supp}(\mathcal{F})$. Now since $\mathcal{F}$ has finitely many associated points – i.e. associated primes corresponding of the module corresponding to $\mathcal{F}$ – there exists $x \in \Gamma(Z,\mathcal{O}_Z(1))$ missing these points. (This amounts to a prime avoidance type argument to show there is a degree one element, which is a non-zero divisor on $\Gamma_*(Z,\mathcal{F})$.) Hence we get the following short exact sequence:

$$0 \to \mathcal{F}(-1) \xrightarrow{\times x} \mathcal{F} \to \mathcal{G} \to 0$$

where $\mathcal{G}$ is the cokernel of this map. Since Euler characteristics add in exact sequences we see that this means

$$\chi(Z,\mathcal{F}(d)) - \chi(Z,\mathcal{F}(d-1)) - \chi(Z,\mathcal{G})$$

However, Krull's Height Theorem we know that $\dim(\text{supp}(\mathcal{G})) = \dim(\text{supp}(\mathcal{F})) - 1$ since x misses the associated points i.e. is a non-zero divisor on $\Gamma_*(Z,\mathcal{F})$. Hence by induction we have that $\chi(Z,\mathcal{G})$ is a polynomial of degree $\dim(\text{supp}(\mathcal{F})) - 1$. Thus, the result follows by Lemma 2.1.2. □

Helpful Background:

Theorem 2.1.1. *If $\mathcal{F}$ is a coherent sheaf on a projective scheme $Z \subset \mathbb{P}^n$ then $h^0(Z,\mathcal{F}(d)) = \chi(Z,\mathcal{F}(d))$ for $d \gg 0$ i.e. $h^0(Z,\mathcal{F}(d))$ is a numerical polynomial.*

Proof. By Proposition 2.1.2 we know that $\chi(Z,\mathcal{F}(d))$ is a polynomial of degree $\dim(\mathrm{supp}(\mathcal{F}))$ and so all we must show is $h^0(Z,\mathcal{F}(d))$ is equal to $\chi(Z,\mathcal{F}(d))$ that for sufficiently large $d \gg$. However, by Serre Vanishing since $\mathcal{F}$ is coherent we know that for large enough d $h^i(Z,\mathcal{F}(d)) = 0$ for all $i > 0$. □

Example 2.1.1. *If $Z \subset \mathbb{P}^n$ is a smooth curve and D is a divisor on Z then Reimann-Roch implies that*

$$\chi(Z,\mathcal{O}_Z(D)) = \deg(D) + \chi(Z,\mathcal{O}_Z) = \deg(D) + 1 - g.$$

Recall that for a curve $\chi(Z,\mathcal{O}_Z) = 1 - g$ essentially by dimensional vanishing and Serre Duality. Hence if $|H| : Z \hookrightarrow \mathbb{P}^n$ is the complete linear system giving the embedding of Z then by letting $H = D$ we have that:

$$\chi(Z,\mathcal{O}_Z(dH)) = \deg(dH) + \chi(Z,\mathcal{O}_Z) = d\deg(Z) + 1 - g$$

meaning the Hilbert polynomial for a curve is a linear polynomial whose leading coefficient is $\deg(Z)$ and whose constant term is $1 - g$.

2.2 A Simple Example

Now that we know the probability $(k+1)$ randomly chosen polynomials of vanish along a fixed subvariety of dimension $(n-k)$ we would like a way to stitch these probabilities together to form an answer. Towards this it is informative to work through a simple example in detail. Hence let's consider the case when X is the union of three lines ℓ_0, ℓ_1, and ℓ_2 where each line $\ell_i \subset \mathbb{P}^2$ is given by $\mathbb{V}(x_i)$ (see Figure 2).

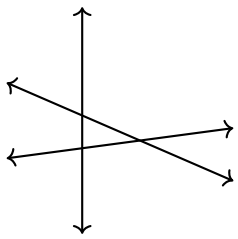


Figure 2. When curves intersect, the values of functions along those curves are not asymptotically independent for $d \gg 0$. For instance the probability that a function of degree vanishes along a line is $q^{-(d+1)}$. But if we knew that a function vanished along two of the three lines in this figure, then the probability would rise to $q^{-(d-1)}$.

Since X is one dimensional $f \in H^0(X,\mathcal{O}_X(d))$ is a parameter on X if and only if $\mathbb{V}(f_d)$ is zero dimensional i.e. $\mathbb{V}(f)$ does not vanish along ℓ_0, ℓ_1, or ℓ_2. Hence we see by inclusion-exclusion that for sufficiently large d:

$$\begin{aligned}
\mathbf{Prob}\Big(f \text{ is a parameter on } X\Big) &= 1 - \mathbf{Prob}\Big(f \text{ is not a parameter on } X\Big) \\
&= 1 - \mathbf{Prob}\left(\begin{matrix} f \text{ vanishes along} \\ \ell_0 \text{ or } \ell_1 \text{ or } \ell_2 \end{matrix}\right) \\
&= 1 - \Big[3\mathbf{Prob}(\ell_i \subset \mathbb{V}(f_d)) - 3\mathbf{Prob}(\ell_i \cup \ell_j \subset \mathbb{V}(f_d)) + \mathbf{Prob}(X \subset \mathbb{V}(f_d))\Big] \\
&= 1 - 3q^{-(d+1)} + 3q^{-(2d+1)} - q^{-3d}
\end{aligned}$$

Notice the exponents come from computing the Hilbert polynomials of ℓ_i, $\ell_i \cup \ell_j$ and X, which may be done by Example 2.1.1.

3. The Answer

3.1 Main Result

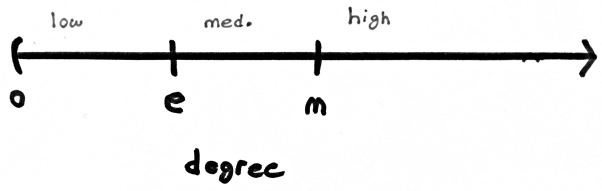
Notice this gives us a hint for how we might proceed. In particular, if as in the example there were only finitely many subvarieties of dimension $(n-k)$ we could do what we did above an apply an inclusion-exclusion type argument. However, $\mathbb{P}^n$ has dimension $(n-k)$ subvarieties of every degree, and so there is no way we could naively accomplish this. That said notice that leading term of the actual probability in Example 2.2 arrises from the subvarieties of minimal degree i.e. linear things:

$$\mathbf{Prob}\Big(f_d \text{ is a parameter on } X\Big) = 1 - \underbrace{3q^{-(d+1)}}_{\deg=1} + \underbrace{3q^{-(2d+1)}}_{\deg=2} - \underbrace{q^{-3d}}_{\deg=3}.$$

More generally the probability $f_0,\dots,f_k$ vanish along an $(n-k)$-dimensional subvariety decrease as hte degree increases. In particular, by Proposition 2.1.1 we know that $h^0(Z,\mathcal{O}_Z(d))$ is asymptotic to $\frac{\deg Z}{(n-k)!}d^{n-k}$ meaning

$$\mathbf{Prob}\left(\begin{matrix} f_0,\dots,f_k \text{ of degree } d \\ \text{vanish along } Z \end{matrix}\right) = q^{-(k+1)h^0(Z,\mathcal{O}_Z(d))} \sim q^{-\frac{(k+1)\deg Z}{(n-k)!}d^{n-k}} \qquad d \gg 0.$$

Thus, if we wished to compute the probability up to some error term we could try to do a inclusion-exclusion argument on all subvareities of dimension $(n-k)$ and degree less than or equal to e, and then wash the remaining varieties into an error term.



This turns approach turns out to work, and leads us to the main new theorem of this talk.

Theorem 3.1.1. *Fix some e and let $k < n$. For sufficiently large d we have that:*

$$\mathbf{Prob}\left(\begin{matrix} f_0,\dots,f_k \text{ of degree } d \\ \text{are parameters} \end{matrix}\right) = 1 - \sum_{\substack{Z\subseteq\mathbb{P}^n \text{reduced} \\ \dim Z \equiv n-k \\ \deg Z \leq e}} (-1)^{|Z|-1} q^{-(k+1)h^0(Z,\mathcal{O}_Z(d))} + o\left(q^{-e(k+1)\binom{n-k+d}{n-k}}\right).$$

Notice the sum is over all varieties *including* reducible varieties. When we write $\dim Z \equiv (n-k)$ we mean Z is equidimensional of dimension $(n-k)$. Further $|Z|$ denotes the irreducible components of Z.

Remark 3.1.1. *Recall given two functions $f,g:\mathbb{R}\to\mathbb{R}$ we say $f \in o(g)$ if*

$$\lim_{x\to\infty}\left|\frac{f(x)}{g(x)}\right| = 0,$$

and we say $f \in O(g)$ if

$$\limsup_{x\to\infty}\left|\frac{f(x)}{g(x)}\right| < \infty.$$

So for example, $3x \in O(x)$, but $3x$ is not in $o(x)$. More generally, if f and g are polynomials then $q^f \in O(q^g)$ if and only if the leading coefficient of $f-g$ is negative. Likewise $q^f \in o(q^g)$ if and only if $f-g$ is nonconstant with negative leading coefficient.

Using the above theorem we can final provide an answer to the motivating question of this talk.

Corollary 3.1.1.

$$\lim_{d\to\infty} \mathbf{Prob}\left(\begin{matrix}(f_0,\dots,f_k) \text{ of degree } d\\ \text{are parameters on } \mathbb{P}^n\end{matrix}\right) = \begin{cases} 1 & \text{if } k < n \\ \zeta_{\mathbb{P}^n}(n+1)^{-1} & \text{if } k = n \end{cases}$$

Proof of Corollary 3.1.1. As noted previously when $k = n$ this is a theorem of Bucur and Kedlaya [BK12]; so I will not discuss this here. (Note: We also have a proof of this, which although similar seems to be independent.)

In the case when $k < n$ Theorem 3.1.1 tells us that

$$\lim_{d\to\infty} \mathbf{Prob}\left(\begin{matrix}f_0,\dots,f_k \text{ of degree } d\\ \text{are parameters}\end{matrix}\right) = 1 - \lim_{d\to\infty} \sum_{\substack{Z\subseteq\mathbb{P}^n \text{reduced}\\ \dim Z\equiv n-k\\ \deg Z\leq e}} (-1)^{|Z|-1} q^{-(k+1)h^0(Z,\mathcal{O}_Z(d))} + o\left(q^{-e(k+1)\binom{n-k+d}{n-k}}\right).$$

However, by Proposition 2.1.1 we know

$$q^{-(k+1)h^0(Z,\mathcal{O}_Z(d)} \sim q^{-\frac{(k+1)\deg Z}{(n-k)!}d^{n-k}} \qquad d \gg 0.$$

Thus, since $k < n$ as d goes to infinity each term in the above sum converges to zero proving the claim. □

Another immediate corollary of Theorem 3.1.1 is that the the coefficient of the leading term is controlled by the geometry of $\mathbb{P}^n$. That is to say the probability $f_0,\dots,f_k$ is a system of parameters is proportional to the number of $(n-k)$-hyperplanes.

Corollary 3.1.2. *Let $k < n$ then:*

$$\lim_{d\to\infty} \frac{\mathbf{Prob}\left(\begin{matrix}(f_0,\dots,f_k) \text{ of degree } d\\ \text{are } \underline{\text{not}} \text{ parameters on } \mathbb{P}^n\end{matrix}\right)}{q^{-(k+1)\binom{n-k+d}{n-k}}} = \#\left\{(n-k)\text{-planes } L \subseteq \mathbb{P}^r_{\mathbb{F}_q}\right\}.$$

3.2 The Case When $k = n$

Much of this work was motivated by Poonen's work on Bertini theorems over finite fields. In fact, work in recent years has lead to the following heuristic for probabilistic questions about varieties over finite fields, which may be of use to stitch the local probabilities together. Put vaguely

Heuristic 3.2.1. *The probability a randomly chosen variety X has a property $\mathcal{P}$ should behave asymptotically like the product of the probability X has $\mathcal{P}$ locally.*

This heuristic arose from Poonen's work on Bertini theorems of finite fields and has since been applied in many other cases [Poo04], [EW15], [BK12]

Example 3.2.1. *A nice example of this heuristic arrises if we let X_d be a randomly chosen plane cuvre of degree d and $\mathcal{P}$ be the property that X_d is smooth. In this case since smoothness may be checked at closed points – we use X_d^c to denote the set of closed points of X_d – this heuristic says that:*

$$\begin{aligned}\lim_{d\to\infty} \mathbf{Prob}\left(X_d \text{ is smooth}\right) &= \lim_{d\to\infty} \prod_{p\in X_d^c} \mathbf{Prob}\left(X_d \text{ is smooth at } s\right)\\ &= \zeta_{\mathbb{P}^2}(3)^{-1} = (1-q^{-1})(1-q^{-2})(1-q^{-3}).\end{aligned}$$

In fact, as is noted in [EW15] *Poonen's work on Bertini theorems shows Heuristic 3.2.1 correct* [Poo04]. *Properties for which Heuristic 3.2.1 apply are often said to be* ***asymptotically independent****.*

Remark 3.2.1. *Poonen's work was substantially more general, and revolved around computing the probability a randomly chosen hypersurface intersects a smooth variety smoothly. In particular, he shows that if $X \subset \mathbb{P}^n$ is a smooth quasi-projective variety then*

$$\lim_{d\to\infty} \mathbf{Prob}\left(\begin{matrix} f \text{ of degree } d \\ \mathbb{V}(f)\cap X \text{ is smooth}\end{matrix}\right) = \lim_{d\to\infty}\prod_{p\in X}\mathbf{Prob}\left(\begin{matrix}\mathbb{V}(f)\cap X \text{ smooth at } p \\ \text{for } f \text{ of degree } d\end{matrix}\right) = \zeta_X(\dim X+1)^{-1}.$$

The above example is the special case of this theorem when we let $X = \mathbb{P}^2 \subset \mathbb{P}^2$, and interoperate a random plane curve of degree d to mean a randomly chosen homogenous polynomial of degree d.

With this in mind how might we apply this Heuristic 3.2.1 to our problem at hand? When k is equal to $n = \dim \mathbb{P}^n$ the question of whether or not $f_0,\dots,f_n$ form a system of parameters on $\mathbb{P}^n$ amounts to asking whether or not $\mathbb{V}(f_0,\dots,f_n) = \emptyset$. Thus, the above heuristic would suggest the following:

$$\lim_{d\to\infty}\mathbf{Prob}\left(\begin{matrix} f_0,\dots,f_n \text{ of degree } d \\ \text{are parameters on } \mathbb{P}^n\end{matrix}\right) = \lim_{d\to\infty}\prod_{p\in\mathbb{P}^n}\mathbf{Prob}\left(\begin{matrix} p\notin\mathbb{V}(f_0,\dots,f_k) \\ \text{for } f_0,\dots,f_n \text{ of degree } d\end{matrix}\right).$$

It turns out that in this turns out to be true. In particular, building on the work of Poonen, Buccur and Kedlaya proved the following result:

Theorem 3.2.1 ([BK12])**.** *When the $k = n$ the following limits exist and are equal:*

$$\begin{aligned}\lim_{d\to\infty}\mathbf{Prob}\left(\begin{matrix} f_0,\dots,f_n \text{ of degree } d \\ \text{are parameters on } \mathbb{P}^n\end{matrix}\right) &= \lim_{d\to\infty}\prod_{p\in\mathbb{P}^n}\mathbf{Prob}\left(\begin{matrix} p\notin\mathbb{V}(f_0,\dots,f_n) \\ \text{for } f_0,\dots,f_n \text{ of degree } d\end{matrix}\right)\\ &= \zeta_{\mathbb{P}^n}(n+1)^{-1}\\ &= \left(1-q^{-(n+1)}\right)(1-q^{-n})\cdots\left(1-q^{-1}\right).\end{aligned}$$

Remark 3.2.2. *Buccur and Kedlaya's results are actually substantially more general than stated above. They were actually interested in computing the probability of a having smooth complete intersection on any projective variety over $\mathbb{F}_q$. However, in the case that $k = n$ this reduces to the above theorem.*

With this in mind we might reasonably hope to adapt Heuristic 3.2.1 to the case when $k < n$. Noting that the question of whether or not $f_0,\dots,f_k$ form a system of parameters on $\mathbb{P}^n$ amounts to whether $\mathbb{V}(f_0,\dots,f_k)$ contains a subvariety of dimension $(n-k)$ we see we may generalize the above to the following guess of an answer to Question 1.2.1:

$$\mathbf{Prob}\left(\begin{matrix} f_0,\dots,f_k \text{ of degree } d \\ \text{are parameters on } \mathbb{P}^n\end{matrix}\right) = \prod_{\substack{Z\subset\mathbb{P}^n \\ \dim Z = n-k}}\mathbf{Prob}\left(\begin{matrix} Z\not\subset\mathbb{V}(f_0,\dots,f_k) \\ \text{for } f_0,\dots,f_n \text{ of degree } d\end{matrix}\right) + o(\text{lower order}).$$

References

[BK12] Alina Bucur and Kiran S. Kedlaya, *The probability that a complete intersection is smooth*, J. Théor. Nombres Bordeaux **24** (2012), no. 3, 541–556 (English, with English and French summaries). ↑

[Eis95] David Eisenbud, *Commutative algebra*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995. With a view toward algebraic geometry. ↑

[EW15] Daniel Erman and Melanie Matchett Wood, *Semiample Bertini theorems over finite fields*, Duke Math. J. **164** (2015), no. 1, 1–38. ↑

[Har77] Robin Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, vol. 52, Springer-Verlag, New York, 1977. With a view toward algebraic geometry. ↑

[Mus11] Mircea Mustaţă, *Zeta functions in algebraic geometry* (2011). Available at `http://www.math.lsa.umich.edu/~mmustata/zeta_book.pdf`. ↑

[Nag62] Masayoshi Nagata, *Local rings*, Interscience Tracts in Pure and Applied Mathematics, No. 13, Interscience Publishers a division of John Wiley & Sons New York-London, 1962. ↑

[Poo04] Bjorn Poonen, *Bertini theorems over finite fields*, Ann. of Math. (2) **160** (2004), no. 3, 1099–1127. ↑

[Ser65] Jean-Pierre Serre, *Zeta and L functions*, Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963), Harper & Row, New York, 1965, pp. 82–92. ↑

[Wei49] André Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508. ↑