DISSERTATION

NUMBER-THEORETIC PROPERTIES OF THE BINOMIAL DISTRIBUTION WITH APPLICATIONS IN ARITHMETIC GEOMETRY

Submitted by

Eric Schmidt

Department of Mathematics

In partial fulfillment of the requirements

For the Degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Summer 2014

Doctoral Committee:

Advisor: Jeffrey Achter

Rachel Pries
Renzo Cavalieri
Wim Bohm

ABSTRACT

NUMBER-THEORETIC PROPERTIES OF THE BINOMIAL DISTRIBUTION WITH APPLICATIONS IN ARITHMETIC GEOMETRY

Alina Bucur et al. showed that the distribution of the number of points on a smooth projective plane curve of degree d over a finite field of order q is approximated by a particular binomial distribution. We generalize their arguments to obtain a similar theorem concerning hypersurfaces in projective m-space. We briefly describe Bucur and Kedlaya's generalization to complete intersections. We then prove theorems concerning the probability that a binomial distribution yields an integer of various certain properties, such as being prime or being squarefree. Finally, we show how to apply such a theorem, concerning a property P, to yield results concerning the probability that the numbers of points on random complete intersections possess property P.

ACKNOWLEDGEMENTS

Thanks to my advisor Jeff Achter for all his help. Thanks also to Leif Anderson for designing the document class used for this dissertation.

TABLE OF CONTENTS

CHAPTER 1

Introduction

The binomial distribution is a probability distribution that indicates the probability of obtaining t successes, given n independent trials with probability of success α. That is, if we fix n and α, we have the distribution

$$\text{Prob}(X = t) = B_{\alpha,n}(t) = \binom{n}{t}\alpha^t(1-\alpha)^{n-t}.$$

The starting point for my research is a paper by Alina Bucur et al. [3], concerning the distribution of the number of points on a smooth projective plane curve of degree d over a finite field of order q. Adapting arguments of Poonen [14], they showed that, in a suitable sense, this distribution is approximated by a particular binomial distribution, whose parameters n and α depend on q. More precisely, they proved, for each t, that the probability of choosing a curve with t points gets arbitrarily close to the estimate given by the binomial distribution, provided that d and q approach infinity and d is large relative to q. My first work was to understand their result and see that their arguments could be generalized to obtain a similar theorem concerning hypersurfaces in projective m-space.

My other work attempts to obtain information on the probability that the number of points on a complete intersection (or on multiple complete intersections chosen independently) will have a certain property. For instance, we might try to estimate the probability that the number of points will be prime, squarefree, and so on. There are two steps to this process. First, we consider picking an integer according to the binomial distribution, and we prove a theorem concerning the probability that this integer will be (say) prime. Second, we see that this theorem, together with the results concerning complete intersections, tells

us about the probability of picking a complete intersection with (say) a prime number of points.

I will now describe the progress made along these lines. J. E. Nymann and W. J. Leahey show [11] that the probability that k integers chosen according to the binomial distribution are relatively prime is $1/\zeta(k)$. This result is not directly applicable since Nymann and Leahey assume that the parameter α is fixed, whereas in our application we need it to vary with q. However, their arguments can be generalized to allow α to vary (with certain restrictions), and this provides a strong enough result to apply to complete intersections. We also present an argument giving the probability that an integer chosen according to the binomial distribution is kth-power free, which again turns out to be $1/\zeta(k)$. Jerry Hu has determined the probability that s integers chosen according to the uniform distribution are k-wise relatively prime [18]. His proof can be adapted to give an analogous result concerning the binomial distribution.

Using these results we can prove, for instance, that the number of points on a smooth hypersurface in $\mathbb{P}^m(\mathbb{F}_q)$ of degree d is squarefree with probability $6/\pi^2$, provided that q and d increase to infinity appropriately. See Chapter 4 for more general and precise statements.

It is more difficult to analyze the probability that an integer chosen according to the binomial distribution is prime. Ideally, we would find an analogue of the prime number theorem. After some time, I came up with the following plan. First, we will assume that the parameter α is constant, and let the number of trials n vary. Consider, for each n, the probability that an integer chosen according to the binomial distribution with n trials and parameter α will be prime. Form the exponential generating function from the sequence of probabilities for various n. We then wish to show that this generating function is *admissible* in a sense defined by W. K. Hayman [6]. This requires verifying some analytic properties

of the function. Hayman showed that once these properties have been proved, we obtain an asymptotic expression for the coefficients of the generating function. This would give our "binomial" prime number theorem. If we could get a sufficiently good error term, we might even be able to apply this to counting points on hypersurfaces or complete intersections. Section 3.8 describes this in more detail.

CHAPTER 2

The numbers of points on hypersurfaces and complete intersections

2.1. Introduction

Bjorn Poonen, in [14], analyzed the limiting probability that an intersection of a hypersurface with a given quasiprojective scheme of dimension m (over a finite field) is smooth of dimension $m-1$, as the degree of the hypersurface tends to infinity. Bucur et al. [3] used Poonen's ideas to show that the distribution of the number of points on a smooth projective plane curve is approximated by a binomial distribution. They did this by determining the error terms that arise in Poonen's argument. In Section 2.2 we follow Bucur et al., showing that essentially the same argument applies to the distribution of the number of points on a smooth projective hypersurface. At some points we have been more explicit about the hypotheses required for the various lemmas.

In a later paper [4], Alina Bucur and Kiran S. Kedlaya proved a similar result about complete intersections. We discuss this result in Section 2.3.

2.2. Hypersurfaces

Fix $m \geq 1$. Let S_d be the set of homogeneous polynomials $F(X_0, \ldots, X_m)$ of degree d over $\mathbb{F}_q$ and let S_d^{ns} be the subset of polynomials corresponding to smooth hypersurfaces $H_F = F(X_0, \ldots, X_m) = 0$.

For a prime power q, we let $n_q = \#\mathbb{P}^m(\mathbb{F}_q) = 1 + q + q^2 + \cdots + q^m$. We also denote by p the characteristic of $\mathbb{F}_q$.

Let Z be a finite subscheme of $\mathbb{P}^m$. Let $U = \mathbb{P}^m \setminus Z$. Then U is smooth of dimension m. We also let T denote a subset of $H^0(Z, \mathcal{O}_Z)$. Let r denote a real number. Let $U_{<r}$ be the closed points of U of degree less than r and $U_{>r}$ the ones with degree greater than r. Also, let $s = \#U_{<r}$.

Let $\mathcal{P}_{d,r} = \{F \in S_d : F|_Z \in T \text{ and } H_F \cap U \text{ is smooth of dimension } m-1 \text{ at all } P \in U_{<r}\}$. (We consider H_F to be smooth of every dimension at any point it does not contain.)

LEMMA 2.1. *For any subscheme $Y \subseteq \mathbb{P}^m$, the map $\phi_d : S_d = H^0(\mathbb{P}^m, \mathcal{O}_{\mathbb{P}^m}(d)) \longrightarrow H^0(Y, \mathcal{O}_Y(d))$ is surjective for $d \geq \dim H^0(Y, \mathcal{O}_Y) - 1$.*

PROOF. Lemma 2.1 in [14]. □

LEMMA 2.2. *For $d \geq (m+1)rs + \dim H^0(Z, \mathcal{O}_Z) - 1$, we have*

$$\frac{\#\mathcal{P}_{d,r}}{\#S_d} = \frac{\#T}{\#H^0(Z, \mathcal{O}_Z)} \prod_{P \in U_{<r}} \left(1 - q^{-(m+1)\deg P}\right).$$

PROOF. For each $P \in U_{<r}$, let $\mathfrak{m}_P$ be the ideal sheaf of P on U, and let V_P be the closed subscheme of U corresponding to the ideal sheaf $\mathfrak{m}_P^2$. That is, V_P is a first-order neighborhood of P; the restriction of a function $f \in H^0(U, \mathcal{O}_U)$ to V_P contains the information not only of the value of f at P but the first-order derivative at P. Then, $\dim H^0(V_P, \mathcal{O}_{V_P}) = (m+1)\deg P < (m+1)r$. Let $V = \bigcup V_P$.

Consider the map

$$\phi_d : S_d = H^0(\mathbb{P}^m, \mathcal{O}_{\mathbb{P}^m}(d)) \longrightarrow H^0(V \cup Z, \mathcal{O}_{V \cup Z}(d)) \simeq H^0(Z, \mathcal{O}_Z) \times \prod_{P \in U_{<r}} H^0(V_P, \mathcal{O}_{V_P}),$$

where we pick a (noncanonical) isomorphism between $H^0(V_P, \mathcal{O}_{V_P}(d))$ and $H^0(V_P, \mathcal{O}_{V_P})$. Then, the dimension of the codomain of ϕ_d is

$$\dim H^0(Z, \mathcal{O}_Z) + \sum_{P \in U_{<r}} (m+1) \deg P < \dim H^0(Z, \mathcal{O}_Z) + (m+1)rs.$$

Thus, since $d \geq (m+1)rs + \dim H^0(Z, \mathcal{O}_Z) - 1$, Lemma 2.1 implies that ϕ_d is surjective.

Now, H_F is not smooth of dimension $m-1$ at P if and only if the restriction of F to a section of $\mathcal{O}_{V_P}$ is 0. Thus, $\mathcal{P}_{d,r}$ is the inverse image of

$$T \times \prod_{P \in U_{<r}} \left(H^0(V_P, \mathcal{O}_{V_P}) \setminus \{0\} \right)$$

under ϕ_d.

We can conclude that

$$\begin{aligned} \frac{\#\mathcal{P}_{d,r}}{\#S_d} &= \frac{\#\left[T \times \prod_{P \in U_{<r}} \left(H^0(V_P, \mathcal{O}(V_P)) \setminus \{0\}\right)\right]}{\#[H^0(Z, \mathcal{O}_Z) \times \prod_{P \in U_{<r}} H^0(V_P, \mathcal{O}_{V_P})]} \\ &= \frac{\#T}{\#H^0(Z, \mathcal{O}_Z)} \prod_{P \in U_{<r}} \left(1 - q^{-(m+1)\deg P}\right). \end{aligned}$$

□

PROPOSITION 2.3. *To each $P \in \mathbb{P}^m(\mathbb{F}_q)$, associate a random variable Y_P taking the value 1 with probability $1/q$ and the value 0 with probability $(q-1)/q$, and let the random variables be independent. Then, for $d \geq n_q - 1$ and $t \geq 0$,*

$$\frac{\#\{F \in S_d : \#H_F(\mathbb{F}_q) = t\}}{\#S_d} = \text{Prob}\left(t = \sum Y_P\right).$$

PROOF. Take Z to be an $\mathfrak{m}_P$-neighborhood for each point $P \in \mathbb{P}^m(\mathbb{F}_q)$. Thus

$$H^0(Z, \mathcal{O}_Z) = \prod_{P \in \mathbb{P}^m(\mathbb{F}_q)} \mathcal{O}_P/\mathfrak{m}_P.$$

Now, the isomorphisms $\mathcal{O}_P/\mathfrak{m}_P \cong \mathbb{F}_q$ give an isomorphism

$$H^0(Z, \mathcal{O}_Z) \cong \bigoplus_{P \in \mathbb{P}^m(F_q)} \mathbb{F}_q. \tag{2.1}$$

Thus, we see that $\dim H^0(Z, \mathcal{O}_Z) = n_q$ and $\#H^0(Z, \mathcal{O}_Z) = q^{n_q}$. For $a \in H^0(Z, \mathcal{O}_Z)$, let $a_P \in \mathbb{F}_q$ denote the value of the P-component of the direct sum (2.1). (Note: we can interpret a as a function on Z, and a_P as the value of the function at P.) Suppose $R \subseteq \mathbb{P}^m(\mathbb{F}_q)$ has cardinality t. We want to count all hypersurfaces H_F such that $H_F(\mathbb{F}_q) = R$. Let

$$T = \{a \in H^0(Z, \mathcal{O}_Z) : \forall P \in \mathbb{P}^m(\mathbb{F}_q) \;\; a_P = 0 \Leftrightarrow P \in R\}.$$

Then $\#T = (q-1)^{n_q - t}$. By taking $r = 0$ in Lemma 2.2, we see that, when $d \geq n_q - 1$,

$$\begin{aligned} \frac{\{\#F \in S_d : H_F(\mathbb{F}_q) = R\}}{\#S_d} &= \frac{\#\mathcal{P}_{d,0}}{\#S_d} = \frac{\#T}{\#H^0(Z, \mathcal{O}_Z)} = \frac{(q-1)^{n_q - t}}{q^{n_q}} \\ &= \left(\frac{1}{q}\right)^t \left(\frac{q-1}{q}\right)^{n_q - t} = \text{Prob}(Y_P = 1 \Leftrightarrow P \in R). \end{aligned}$$

If we sum over all $R \subseteq \mathbb{P}^m(\mathbb{F}_q)$ with $\#R = t$, we obtain

$$\frac{\#\{F \in S_d : \#H_F(\mathbb{F}_q) = t\}}{\#S_d} = \sum_{\#R = t} \text{Prob}(Y_P = 1 \Leftrightarrow P \in R) = \text{Prob}\left(t = \sum Y_P\right).$$

□

LEMMA 2.4. *For any sequence $\{x_i\}$ of nonnegative real numbers with $\sum x_i < 1$, we have*

$$1 \le \prod_{i=1}^{\infty}(1-x_i)^{-1} \le \frac{1}{1-\sum x_i}.$$

PROOF. The first inequality is evident. To prove the second, for any k, we have

$$\prod_{i=1}^{k}(1-x_i)^{-1} = \prod_{i=1}^{k}\sum_{j=0}^{\infty} x_i^j = \sum_{a_1,\dots,a_k\ge 0} x_1^{a_1}\cdots x_k^{a_k} < \sum_{j=0}^{\infty}(x_1+\cdots+x_k)^j = \frac{1}{1-(x_1+\cdots+x_k)}.$$

Letting k increase to infinity, we obtain the result. □

Define

$$\zeta_U(z) = \prod_{P \text{ closed point of } U} (1-q^{-z\deg P})^{-1}.$$

PROPOSITION 2.5. *The product $\zeta_U(z)$ converges absolutely for $\operatorname{Re} z > m$.*

PROOF. Fix z such that $\operatorname{Re} z > m$. The number of closed points of degree e in U is less than $2q^{me}$. Hence, for any $r \ge 0$, we have $\sum_{P\in U_{>r}} |q^{-z\deg P}| < 2\sum_{j>r} |q^{(m-z)j}|$, which converges since $\operatorname{Re}(m-z) < 0$. Thus, we can choose r so that $\sum_{P\in U_{>r}} |q^{-z\deg P}| < 1$. To prove the absolute convergence of $\zeta_U(z)$, it suffices to prove this with finitely many terms removed from the product. Thus, since

$$\prod_{P\in U_{>r}} |(1-q^{-z\deg P})^{-1}| \le \prod_{P\in U_{>r}} (1-|q^{-z\deg P}|)^{-1}$$

converges by Lemma 2.4, the result is proved. □

LEMMA 2.6. *We have, for $r > \log_q \frac{2q}{q-1}$ and $d \ge (m+1)rs + \dim H^0(Z,\mathcal{O}_Z) - 1$,*

$$1 \le \frac{\#\mathcal{P}_{d,r}}{\#S_d} \Big/ \frac{\#T}{\zeta_U(m+1)\#H^0(Z,\mathcal{O}_Z)} \le 1 + \frac{2q^{-r}}{1-q^{-1}-2q^{-r}}.$$

PROOF. Suppose first that r is an integer. Similarly to Proposition 2.5, since the number of closed points of degree e in U is less than $2q^{me}$, we have that

$$\sum_{\deg P \geq r} q^{-(m+1)\deg P} < 2\sum_{j \geq r} q^{-j} = \frac{2q^{-r}}{1-q^{-1}} < 1.$$

Then, by Lemma 2.4,

$$1 \leq \prod_{\deg P \geq r} (1 - q^{-(m+1)\deg P})^{-1} \leq \frac{1}{1 - \frac{2q^{-r}}{1-q^{-1}}} = 1 + \frac{2q^{-r}}{1 - q^{-1} - 2q^{-r}}.$$

Thus,

$$1 \leq \zeta_U(m+1) \prod_{P \in U_{<r}} (1 - q^{-(m+1)\deg P}) \leq 1 + \frac{2q^{-r}}{1 - q^{-1} - 2q^{-r}}.$$

If r is not an integer, we can obtain the same inequality by applying the above reasoning to $\lceil r \rceil$. To complete the proof, compare this with Lemma 2.2. □

Note: In the previous lemma, if we only care about integral values of r, then for $q = 2$ we have the condition $r \geq 3$, for $q = 3$ the condition $r \geq 2$, and for $q \geq 4$ the condition $r \geq 1$.

LEMMA 2.7. *For a closed point $P \in U$ of degree $e \leq d/(m+1)$, we have*

$$\frac{\#\{F \in S_d : H_F \cap U \text{ is not smooth of dimension } m-1 \text{ at } P\}}{\#S_d} = q^{-(m+1)e}.$$

PROOF. Special case of Lemma 2.3 of [14]. □

Let $\mathcal{Q}_{d,r}$ be the set of all $F \in S_d$ such that there exists a closed point $P \in U$ with $r \leq \deg P \leq d/(m+1)$ and $H_F \cap U$ not smooth of dimension $m-1$ at P.

LEMMA 2.8.

$$\frac{\#\mathcal{Q}_{d,r}}{\#S_d} \leq \frac{2q^{-r}}{1-q^{-1}}.$$

PROOF. As in the proof of Lemma 2.6, by replacing r by $\lceil r \rceil$ we reduce to the case where r is an integer. We have, by definition of $\mathcal{Q}_{d,r}$,

$$\frac{\#\mathcal{Q}_{d,r}}{\#S_d} \leq \sum_{P \in U, r \leq \deg P \leq d/(m+1)} \frac{\#\{F \in S_d : H_F \cap U \text{ is not smooth of dimension } m-1 \text{ at } P\}}{\#S_d}.$$

Thus, using Lemma 2.7 and the fact that the number of closed points of degree e in U is bounded above by $2q^{me}$, we have

$$\frac{\#\mathcal{Q}_{d,r}}{\#S_d} \leq \sum_{P \in U, r \leq \deg P \leq d/(m+1)} q^{-(m+1)e} \leq 2 \sum_{e=r}^{d/(m+1)} q^{-e} \leq 2 \sum_{e=r}^{\infty} q^{-e} = \frac{2q^{-r}}{1-q^{-1}}.$$

□

Let $A_{\leq d}$ denote the set of polynomials in $\mathbb{F}_q[x_1, \ldots, x_m]$ of degree at most d.

LEMMA 2.9. *If $P \in A^m(\mathbb{F}_q)$ is of degree e, then*

$$\frac{\#\{f \in A_{\leq d} : f(P) = 0\}}{\#A_{\leq d}} \leq q^{-\min(d+1,e)}.$$

PROOF. Lemma 2.5 in [14]. □

In what follows we will use the following notation. Let $\gamma = \lfloor (d-1)/p \rfloor$ and $\eta = \lfloor d/p \rfloor$. If we have polynomials $f_0 \in A_{\leq d}$, $g_1, \ldots, g_m \in A_{\leq \gamma}$ and $h \in A_{\leq \eta}$, then we define the polynomial $f \in A_{\leq d}$ by $f = f_0 + g_1^p x_1 + \cdots + g_m^p x_m + h^p$. The ith partial derivative is given by $D_i = \frac{\partial}{\partial x_i}$. Define $W_0 = U$ and, for each $1 \leq i \leq m$, define $W_i = U \cap \{D_1 f = \cdots = D_i f = 0\}$. Notice that $D_i f = D_i f_0 + g_i^p$ for $1 \leq i \leq m$, so even if we have only specified f_0 and $g_1, \ldots, g_i$, the partial derivatives $D_1 f, \ldots, D_i f$ (and hence the schemes $W_1, \ldots, W_i$) are determined, even though f itself is not. Hence the statement of the following lemma makes sense.

LEMMA 2.10. *If we have* $0 \leq i < m$ *and have fixed* f_0 *and* $g_1, \ldots, g_i$ *so that* $\dim W_i \leq m - i$*, then*

$$\frac{\#\{g_{i+1} \in A_{\leq \gamma} : \dim W_{i+1} = \dim W_i\}}{\#A_{\leq \gamma}} \leq (d-1)^i q^{\gamma - 1}.$$

PROOF. If $\dim W_{i+1} = \dim W_i$, then $(W_{i+1})_{\mathrm{red}}$ must contain some $(m-i)$-dimensional component of $(W_i)_{\mathrm{red}}$. By Bézout's theorem, the number of such components is at most $(d-1)^i$, as $\deg D_i f \leq d-1$ and $\deg \bar{U} = 1$ (where $\bar{U}$ is the Zariski closure of U.). Consider some $(m-i)$-dimensional component V. Since $\dim V \geq 1$, there is some coordinate x_j such that $x_j(V)$ is a 1-dimensional subscheme of $\mathbb{A}^1$. Then, since any nonzero polynomial in x_j does not vanish on all of $\mathbb{A}^1$, such a polynomial does not vanish on V. From the formula $D_i f = D_i f_0 + g_i^p$, we see that the set $\{g_{i+1} : (W_{i+1})_{\mathrm{red}} \supseteq V\}$ is either empty or a coset of the subspace $\{g_{i+1} : g_{i+1}(P) = 0, \forall P \in V\}$. Since this subspace cannot contain nonzero polynomials in the variable x_j alone, its dimension is at most $\dim A_{\leq \gamma} - (\gamma + 1)$. Since there are at most $(d-1)^i$ choices for V, the number of choices for g_{i+1} for which $\dim W_{i+1} = \dim W_i$ is at most $(d-1)q^{\dim A_{\leq \gamma} - (\gamma+1)}$. This proves the result. □

LEMMA 2.11. *If we have fixed* f_0 *and* $g_1, \ldots, g_m$ *so that* $\dim W_m = 0$*, then*

$$\frac{\#\{h \in A_{\leq \eta} : H_f \cap W_m \cap U_{>d/(m+1)} = \varnothing\}}{\#A_{\leq \eta}} \leq (d-1)^m q^{-\min(\eta+1, d/(m+1))}.$$

PROOF. For any $P \in W_m \cap U_{>d/(m+1)}$, the set $\{h \in A_{\leq \eta} : P \in H_f\}$ is either empty or a coset of $\{h_0 \in A_{\leq \eta} : h_0(P) = 0\}$. Hence, by Lemma 2.9,

$$\frac{\#\{h \in A_{\leq \eta} : P \in H_f\}}{\#A_{\leq \eta}} \leq q^{-\min(\eta+1, d/(m+1))}.$$

By Bézout's theorem, $\#W_m \leq (d-1)^m$. The proof is complete. □

Define $\mathcal{Q}_d^{\text{high}}$ to be the set of all $F \in S_d$ such that there exists a closed point $P \in U$ with $\deg P > d/(m+1)$ and $H_F \cap U$ not smooth of dimension $m-1$ at P.

LEMMA 2.12. *Suppose $d \geq 3$. Then,*

$$\frac{\#\mathcal{Q}_d^{\text{high}}}{\#S_d} \leq (m+1)(d-1)^m q^{-\min(\eta+1, d/(m+1))} + 2(m+1)(d-1)^{m-1} q^{-\gamma-1}.$$

PROOF. We can find a bound for $\mathcal{Q}_d^{\text{high}}$ by assuming that $U \subseteq \mathbb{A}^m$ and multiplying the result by $m+1$. We will pick f_0, $g_1, \ldots, g_m$, and h uniformly at random, in that order. This determines f itself uniformly at random, since for each fixed choice of $g_1, \ldots, g_m$ and h, each f is determined by exactly one f_0. We are looking to bound the number of $f \in A_{\leq d}$ such that f is not smooth of dimension $m-1$ at some $P \in U_{>d/(m+1)}$. For each P, this is equivalent to asserting that $f(P) = (D_1 f)(P) = \cdots = (D_m f)(P) = 0$, or $P \in H_f \cap W_m$. We thus seek to bound $\text{Prob}(H_f \cap W_m \cap U_{>d/(m+1)} = \varnothing)$, which is bounded above by

$$\text{Prob}(\dim W_m > 0) + \text{Prob}(H_f \cap W_m \cap U_{>d/(m+1)} = \varnothing \,|\, \dim W_m = 0).$$

Now, $\dim W_m > 0$ implies that $W_i = W_{i+1}$ for some i. Thus, by summing the result of Lemma 2.10 for all $0 \leq i < m$, we obtain an upper bound for the first summand in the above expression. Lemma 2.11 gives an upper bound for the second summand. Thus by combining Lemma 2.10 and Lemma 2.11 we determine the desired upper bound. (To obtain a simpler expression we replace $1 + (d-1) + \cdots + (d-1)^{m-1}$ with $2(d-1)^{m-1}$.) □

Let $\mathcal{P}$ denote the set of all $F \in S_d$ such that $H_F \cap U$ is smooth of dimension $m-1$ and $F|_Z \in T$.

Let $\phi_{d,r} = \left(\#\mathcal{Q}_{d,r} + \#\mathcal{Q}_d^{\text{high}}\right)/(\#S_d)$.

LEMMA 2.13. *Suppose $d \geq 3$. Then, we have*

$$0 \leq \phi_{d,r} \leq \frac{2q^{-r}}{1-q^{-1}} + (m+1)(d-1)^m q^{-\min(\eta+1, d/(m+1))} + 2(m+1)(d-1)^{m-1}q^{-\gamma-1}.$$

Moreover, for $r > \log_q \frac{2q}{q-1}$ and $d \geq (m+1)rs + \dim H^0(Z, \mathcal{O}_Z) - 1$,

$$1 \leq \left(\frac{\#\mathcal{P}}{\#S_d} + \phi_{d,r}\right) \Big/ \frac{\#T}{\zeta_U(m+1)\#H^0(Z,\mathcal{O}_Z)} \leq 1 + \frac{2q^{-r}}{1-q^{-1}-2q^{-r}}.$$

PROOF. Since $\mathcal{P} = \mathcal{P}_{d,r} \setminus (\mathcal{Q}_{d,r} \cup \mathcal{Q}_d^{\mathrm{high}})$, this is the result of combining Lemmas 2.6, 2.8, and 2.12. □

Let $\psi_d = \phi_{d,(\log_q d)/(m+1)}$.

The next lemma estimates the probability that a hypersurface is smooth.

LEMMA 2.14. *If $d \geq 3$, then*

$$0 \leq \psi_d \leq \frac{2d^{-1/(m+1)}}{1-q^{-1}} + (m+1)(d-1)^m q^{-\min(\eta+1, d/(m+1))} + 2(m+1)(d-1)^{m-1}q^{-\gamma-1}.$$

Moreover, there exists d_m depending only on m such that for all $d \geq d_m$,

$$1 \leq \left(\frac{\#S_d^{\mathrm{ns}}}{\#S_d} + \psi_d\right) \Big/ \zeta_{\mathbb{P}^m}(m+1)^{-1} \leq 1 + \frac{2d^{-1/(m+1)}}{1-q^{-1}-2d^{-1/(m+1)}}.$$

PROOF. Let $r = \frac{\log_q d}{m+1}$. If $d > 4^{m+1}$, then $d > (2q/(q-1))^{m+1}$, so that $r > \log_q \frac{2q}{q-1}$. Also, from $s < 2q^{mr}$ and $\log_q d \leq \log_2 d$, we obtain $(m+1)rs < 2d^{m/(m+1)} \log_2 d$, which is $o(d)$ as $d \to \infty$. Hence, if d is sufficiently large, we may apply Lemma 2.13 with $Z = \varnothing$ and $T = \{0\}$ to obtain the result. □

THEOREM 2.15. *To each $P \in \mathbb{P}^m(\mathbb{F}_q)$, associate a random variable X_P taking the value 1 with probability $(n_q - q^m)/n_q$ and the value 0 with probability q^m/n_q, and let the random*

variables be independent. Then, for $d \geq (m+1)n_q - 1$ and $t \geq 0$,

$$\left| \frac{\#\{F \in S_d^{\mathrm{ns}} : \#H_F(\mathbb{F}_q) = t\}/(\#S_d^{\mathrm{ns}})}{\mathrm{Prob}\,(t = \sum X_P)} - 1 \right|$$
$$\leq cq^t(d^{-1/(m+1)} + (d-1)^m q^{-\min(\lfloor d/p \rfloor + 1, d/(m+1))} + (d-1)^{m-1} q^{-\lfloor (d-1)/p \rfloor - 1}),$$

where c depends only on m.

PROOF. Take Z to be an $\mathfrak{m}_P^2$-neighborhood for each point $P \in \mathbb{P}^m(\mathbb{F}_q)$. Thus

$$H^0(Z, \mathcal{O}_Z) = \prod_{P \in \mathbb{P}^m(\mathbb{F}_q)} \mathcal{O}_P/\mathfrak{m}_P^2.$$

Now, consider the $\mathbb{F}_q$-module isomorphisms $\mathcal{O}_P/\mathfrak{m}_P^2 \cong \mathbb{F}_q^{m+1}$ given by

$$(b_0 + b_1 x_1 + \cdots + b_m x_m) \mapsto (b_0, b_1, \ldots, b_m),$$

where we have chosen coordinates so that $P = 0$. These give an isomorphism

$$H^0(Z, \mathcal{O}_Z) \cong \bigoplus_{P \in \mathbb{P}^m(\mathbb{F}_q)} \mathbb{F}_q^{m+1}. \tag{2.2}$$

Thus, we see that $\dim H^0(Z, \mathcal{O}_Z) = (m+1)n_q$ and $\#H^0(Z, \mathcal{O}_Z) = q^{(m+1)n_q}$. For $a \in H^0(Z, \mathcal{O}_Z)$, let $a_P = (a_{P,0}, \ldots, a_{P,m}) \in \mathbb{F}_q^{m+1}$ denote the value of the P-component of the direct sum (2.2). Suppose $R \subseteq \mathbb{P}^m(\mathbb{F}_q)$ has cardinality t. We want to count all hypersurfaces H_F such that F is smooth and $H_F(\mathbb{F}_q) = R$. Let

$$T = \{a \in H^0(Z, \mathcal{O}_Z) : \forall P \in \mathbb{P}^m(\mathbb{F}_q)\ (a_P \neq 0 \text{ and } (a_{P,0} = 0 \Leftrightarrow P \in R))\}.$$

Then $\#T = (q^m-1)^t(q-1)^{n_q-t}q^{m(n_q-t)}$. Let $r = \frac{\log_q d}{m+1}$. By using these values of Z, T, and r in Lemma 2.13, we find (for $d \geq (m+1)n_q - 1$)

$$1 \leq \left(\frac{\#\{F \in S_d^{\mathrm{ns}} : H_F(\mathbb{F}_q) = R\}}{\#S_d} + \psi_d \right) \Big/ Y \leq 1 + M, \tag{2.3}$$

where

$$M = \frac{2d^{-1/(m+1)}}{1 - q^{-1} - 2d^{-1/(m+1)}}$$

and

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

We want to combine this with Lemma 2.14 to find an estimate for $(\#\{F \in S_d^{\mathrm{ns}} : H_F(\mathbb{F}_q) = R\})/(\#S_d^{\mathrm{ns}})$. Now, using (2.3), we can find an upper bound for $\frac{\#\{F \in S_d^{\mathrm{ns}} : H_F(\mathbb{F}_q) = R\}}{\#S_d}$, and using Lemma 2.14 we can find a lower bound for $\frac{\#S_d^{\mathrm{ns}}}{\#S_d}$. By dividing these, we find that

$$\frac{\#\{F \in S_d^{\mathrm{ns}} : H_F(\mathbb{F}_q) = R\}}{\#S_d^{\mathrm{ns}}} \Big/ (Y\zeta_{\mathbb{P}^m}(m+1)) \leq \frac{1 + M - \frac{\psi_d}{Y}}{1 - \psi_d \zeta_{\mathbb{P}^m}(m+1)}.$$

The latter expression is equal to

$$1 + \frac{M - \frac{\psi_d}{Y} + \psi_d \zeta_{\mathbb{P}^m}(m+1)}{1 - \psi_d \zeta_{\mathbb{P}^m}(m+1)}. \tag{2.4}$$

From this, we find that an upper bound for (2.4) is

$$1 + c_1(d^{-1/(m+1)} + (d-1)^m q^{-\min(\lfloor d/p \rfloor + 1, d/(m+1))} + (d-1)^{m-1} q^{-\lfloor (d-1)/p \rfloor - 1}). \tag{2.5}$$

for some $c_1 > 0$. (The denominators appearing in (4), in M and in the upper bound for ϕ_d are bounded away from 0, so by making c large enough we may omit them.)

Similarly, to obtain a lower bound, we find that

$$\frac{\#\{F \in S_d^{\mathrm{ns}} : H_F(\mathbb{F}_q) = R\}}{\#S_d^{\mathrm{ns}}} \Big/ (Y\zeta_{\mathbb{P}^m}(m+1)) \geq \frac{1 - \frac{\psi_d}{Y}}{1 + M - \psi_d \zeta_{\mathbb{P}^m}(m+1)},$$

which equals

$$1 - \frac{M - \psi_d \zeta_{\mathbb{P}^m}(m+1) + \frac{\psi_d}{Y}}{1 + M - \psi_d \zeta_{\mathbb{P}^m}(m+1)}.$$

Now, Y is a rational expression in q of degree $-t$. From this, we find that a lower bound for the above is

$$1 - c_2 q^t (d^{-1/(m+1)} + (d-1)^m q^{-\min(\lfloor d/p \rfloor + 1, d/(m+1))} + (d-1)^{m-1} q^{-\lfloor (d-1)/p \rfloor - 1}), \tag{2.6}$$

for some $c_2 > 0$.

Since

$$\frac{\zeta_{\mathbb{P}^m}(m+1)}{\zeta_U(m+1)} = \zeta_Z(m+1) = \left(\frac{1}{1 - q^{-m-1}}\right)^{n_q} = \left(\frac{q^{m+1}}{q^{m+1} - 1}\right)^{n_q},$$

we have

$$\begin{aligned} Y\zeta_{\mathbb{P}^m}(m+1) &= \left(\frac{q^{m+1}}{q^{m+1}-1}\right)^{n_q} \frac{(q^m - 1)^t (q-1)^{n_q - t} q^{m(n_q - t)}}{q^{(m+1)n_q}} \\ &= \left(\frac{n_q - q^m}{n_q}\right)^t \left(\frac{q^m}{n_q}\right)^{n_q - t} \\ &= \mathrm{Prob}(X_P = 1 \Leftrightarrow P \in R). \end{aligned}$$

If we sum the latter expression over all $R \subseteq \mathbb{P}^m(\mathbb{F}_q)$ with $\#R = t$, we obtain $\mathrm{Prob}\,(t = \sum X_P)$.

Now, $Y\zeta_{\mathbb{P}^m}(m+1)$ multiplied by (2.5) is an upper bound for

$$\frac{\#\{F \in S_d^{\mathrm{ns}} : H_F(\mathbb{F}_q) = R\}}{\#S_d^{\mathrm{ns}}},$$

and so summing over all R with $\#R = t$, we find that $\mathrm{Prob}\,(t = \sum X_P)$ multiplied by (2.5) is an upper bound for

$$\frac{\#\{F \in S_d^{\mathrm{ns}} : \#H_F(\mathbb{F}_q) = t\}}{\#S_d^{\mathrm{ns}}}.$$

Similarly, $\mathrm{Prob}\,(t = \sum X_P)$ multiplied by (2.6) is a lower bound for the same expression. This completes the proof. □

2.3. Complete intersections

While the work in the previous section was being done Alina Bucur and Kiran S. Kedlaya, in [4], proved a result about complete intersections analogous to the prior result of [3] about plane curves. Here we simply record the special case we will use.

Theorem 2.16. *Let $1 \le j \le m$ be an integer, and consider tuples $\mathbf{d} = (d_1, \dots, d_j)$ of positive integers such that $(m+1)n_q - 1 \le d_1 \le \cdots \le d_j$. For any $\mathbf{f} = (f_1, \dots, f_j) \in S_{d_1} \times \cdots \times S_{d_j}$, let $H_{\mathbf{f}} = H_{f_1} \cap \cdots H_{f_j}$. Consider some $R \subseteq \mathbb{P}^m(\mathbb{F}_q)$ of size t. Suppose $q, d_1, \dots, d_j$ vary such that $d_1 \to \infty$, $d_1 \ge (m+1)n_q$ and $d_j = o((q^{d_1/\max(m+1,p)})^{1/m})$. Then, the probability that a smooth $H_{\mathbf{f}}$ of dimension $m-j$ contains the points of R but no other point of $\mathbb{P}^m(\mathbb{F}_q)$ is*

$$\left(\frac{q^{-j}L(q,m,j)}{1-q^{-j}+q^{-j}L(q,m,j)}\right)^t \left(\frac{1-q^{-j}}{1-q^{-j}+q^{-j}L(q,m,j)}\right)^{n_q-t}$$
$$+ O((d_1 - n_q + 1)^{(-2j-1)/m} + d_j^m q^{-d_1/\max(m+1,p)}),$$

where

$$L(q,m,j) = \prod_{i=1}^{j-1}(1 - q^{-(m-i)}).$$

Proof. This follows from Theorem 1.2 and Corollary 1.3 of [4]. (Our notation is a bit different.) □

CHAPTER 3

Statistics on binomial distributions

3.1. Introduction

In the previous section, we saw that the distribution of points on a random smooth hypersurface (or, more generally, a smooth complete intersection) is approximated by a binomial distribution. This provides a possible avenue of answering various statistical questions about complete intersections. For instance, if we wish to determine the probability that the number of points on a complete intersection is squarefree, we could determine the same probability for integers chosen according to a binomial distribution, and we will obtain the same probability (in the limit) for complete intersections. See Chapter 4 for more details on this process.

Throughout Chapter 3, we will consider $\alpha \in (0,1)$, and put $\beta = 1 - \alpha$. For each $n \geq 0$, the probability measure of the binomial distribution is

$$B_{\alpha,n}(\{t\}) = \binom{n}{t} \alpha^t \beta^{n-t}$$

on the set of nonnegative integers. This gives the probability of t successes when running n independent trials, each of whose probability of success is α. To simplify the notation, we will generally write just $B_n(t)$. Thus, in the theorems that follow, we allow α to vary with n, which is necessary for our application. (We do, however, assume that α is bounded away from 1, since allowing α to approach 1 would be not be useful for us.) We will write α_n and β_n to emphasize the dependence on n.

Sometimes, it will be convenient to approximate the binomial distribution with a normal distribution, with pdf

$$N_n(x) = (2\pi n\alpha_n\beta_n)^{-1/2}e^{-\frac{1}{2}u^2(x)},$$

where $u(x) = (x-a)/\sigma$, $\sigma = (n\alpha_n\beta_n)^{1/2}$, and $a = \alpha_n n$. (Here a and σ are the mean and standard deviation, respectively, of N_n.) The relationship between the binomial distribution and the normal approximation is given by the following.

THEOREM 3.1. *There is a constant $\lambda_2 \in \mathbb{R}$ such that,*

$$\sum_{x\in\mathbb{Z}} |B_n(x) - N_n(x)| = |\beta_n - \alpha_n|\sigma^{-1}\lambda_2 + O(\sigma^{-2}).$$

PROOF. This is Theorem 3 of [15], which also determines explicitly the value of λ_2. □

3.2. Coprime integers

Nymann and Leahey [11] calculated the probability that integers chosen according to the binomial distribution are coprime. However, they assumed that α was constant as n approached infinity. This is unsuitable for us, so here we generalize their argument to allow α to vary, with certain restrictions.

Our result in this section is the following.

THEOREM 3.2. *Suppose that α_n is bounded away from 1, and that $\alpha_n = \omega((\log n)^b/n)$, where $b = 1$ if $k \geq 3$ and $b = 2$ if $k = 2$. Then, as n goes to infinity, the probability that k integers chosen according to the binomial distribution, with n Bernoulli trials with probability of success α_n, are coprime tends to $1/\zeta(k)$.*

The lower bound on α_n could probably be improved. However, the result fails for $\alpha_n = 1/n$ (see Section 3.7), so we are close to the true range in which the theorem holds.

Throughout this section, we will assume, unless stated otherwise, that the restrictions on α_n hold. Note that for $k = 2$ there is a stronger hypothesis on α_n. Most of the time, this stronger hypothesis is not needed. The places where we must appeal to it are explicitly noted.

Let $I_n = \{m \in \mathbb{Z} : 0 \leq m \leq n\}$. If P_n is a probability measure on I_n and k is a positive integer, then P_n^k is the k-fold product measure on I_n^k. Let $S_n^k = \{(x_1, \ldots, x_k) \in I_n^k : \gcd(x_1, \ldots, x_k) = 1\}$. For an integer $d > 0$, let $A_n(d) = \{j \in I_n : j \equiv 0 \pmod{d}\}$.

LEMMA 3.3. *Let $n \geq 1$. For any probability distribution P_n on I_n, we have*

$$P_n^k(S_n^k) = \sum_{d=1}^{n} \mu(d) \left[(P_n(A_n(d)))^k - (P_n(\{0\}))^k \right].$$

PROOF. Lemma 1 of [11]. □

From now on we specialize to the binomial distribution B_n. Fix an integer $k \geq 2$. Let $\varepsilon_n(d) = B_n(A_n(d)) - d^{-1}$.

LEMMA 3.4.

$$B_n^k(S_n^k) = \sum_{d=1}^{n} \mu(d) d^{-k} + \sum_{j=1}^{k} \binom{k}{j} \sum_{d=1}^{n} \mu(d) d^{j-k} (\varepsilon_n(d))^j - (1 - \alpha_n)^{kn} \sum_{d=1}^{n} \mu(d).$$

PROOF. By Lemma 3.3,

$$B_n^k(S_n^k) = \sum_{d=1}^{n} \mu(d) \left[(d^{-1} + \varepsilon_n(d))^k - \beta_n^{kn} \right].$$

We obtain the result by applying the binomial theorem to the first term in the brackets. □

The first summand in Lemma 3.4, $\sum_{d=1}^{n} \mu(d) d^{-k}$, approaches $1/\zeta(k)$ as $n \to \infty$. Thus, Theorem 3.2 will be established if we show that the remaining terms go to 0.

LEMMA 3.5.

$$\lim_{n\to\infty} \beta_n^{kn} \sum_{d=1}^{n} \mu(d) = 0.$$

PROOF. Let $u_n = \alpha_n^{-1}$. We have, for all sufficiently large n,

$$\left|\beta_n^{kn} \sum_{d=1}^{n} \mu(d)\right| < n\beta_n^{kn} = n(1-u_n^{-1})^{u_n\alpha_n kn}$$

$$< ne^{-\alpha_n kn} < ne^{-k\log n} = n^{1-k},$$

which goes to 0 as $n \to \infty$. □

LEMMA 3.6. *If α_n is bounded away from 1 but has no other restrictions, we have $|\varepsilon_n(d)| = O((\alpha_n n)^{-1/2})$ uniformly in d as $n \to \infty$.*

PROOF. Nymann and Leahey show, in the proof of Lemma 3 of [11] that

$$|\varepsilon_n(d)| \le 3B_n(s),$$

where $s = \lfloor \alpha_n(n+1) \rfloor$. The result follows from Theorem 3.1. □

LEMMA 3.7. *For $1 \le j < k$,*

$$\lim_{n\to\infty} \sum_{d=1}^{n} \mu(d) d^{j-k} (\varepsilon_n(d))^j = 0.$$

PROOF. It suffices to show that $\sum d^{j-k}|\varepsilon_n(d)|^j \to 0$. Suppose first that $j-k > 1$. By Lemma 3.6, the sum is $O((\alpha_n n)^{-j/2})$, which is $o((\log n)^{-j/2})$ by our hypothesis on α_n. Hence the value approaches 0. If $j-k=1$, the sum is $O((\alpha_n n)^{-j/2}\log n)$, which again approaches 0. (If $j=1$, then $k=2$ and we use our stronger hypothesis on α_n.) □

We will fix a function $h : \mathbb{N} \longrightarrow \mathbb{R}$ with the property that $\sqrt{(\log n)/\alpha_n} = o(h(n))$ and $h(n) = o(\sqrt{n}\,)$. (For instance, we could take h to be the geometric mean.)

For the next lemma we will, like Nymann and Leahey, need the following theorem ([10], p. 266):

THEOREM 3.8. *Let $\{X_k\}_{1\leq k\leq n}$ be independent random variables. Put $S = \sum_{k=1}^{n} X_k$. Let s be the standard deviation of S and let c be the maximum value of $|X_k/s|$. Fix some $\varepsilon > 0$ such that $\varepsilon c \leq 1$. Then,*

$$\text{Prob}(S/s > \varepsilon) < \exp\left(-\frac{\varepsilon^2}{2}\left(1 - \frac{\varepsilon c}{2}\right)\right).$$

The next lemma shows that the probability of being a certain distance from the mean decays more rapidly than $1/n$.

LEMMA 3.9.

$$\sum_{|k-\alpha_n n|>\alpha_n h(n) n^{1/2}} B_n(k) = o(n^{-1}).$$

PROOF. To apply the theorem, for each $1 \leq k \leq n$, let X_k be a random variable taking the value $1-\alpha_n$ with probability α_n and $-\alpha_n$ with probability $1-\alpha_n$. (Thus the X_k are identically distributed with mean 0.) Let $\varepsilon = h(n)\sqrt{\alpha_n/(1-\alpha_n)}$. We have $s = \sqrt{n\alpha_n(1-\alpha_n)}$ and $c = a/s$, where $a = \max(\alpha_n, 1-\alpha_n)$. Thus, we see that $\varepsilon c = ah(n)n^{-1/2} \leq 1$ for $n \gg 0$. Hence, Theorem 3.8 applies, and yields

$$\begin{aligned}\text{Prob}(S > \alpha_n h(n) n^{1/2}) &< \exp\left(-\frac{h^2(n)\alpha_n}{2(1-\alpha_n)}\left(1 - \frac{ah(n)n^{-1/2}}{2}\right)\right) \\ &< \exp(\alpha_n(h^3(n)n^{-1/2} - h^2(n))).\end{aligned}$$

We claim that the last expression is $o(n^{-1})$, which is equivalent to claiming that

$$\alpha_n h^3(n) n^{-1/2} - \alpha_n h^2(n) + \log n$$

tends to $-\infty$. Our hypotheses on h show that $h^2(n) = \omega(h^3(n)n^{-1/2})$ and $\alpha_n h^2(n) = \omega(\log n)$, so this is true. Now, the random variable S is a sum of n random variables taking either the value $1 - \alpha_n$ or $-\alpha_n$, and S itself has the value $k - \alpha_n n$, where k is the number of times that $1 - \alpha_n$ was chosen. Moreover the probability that S has this value is $B_n(k)$. Hence, we have shown that

$$\sum_{k - \alpha_n n > \alpha_n h(n) n^{1/2}} B_n(k) = o(n^{-1}).$$

By repeating the same argument with X_k replaced with $-X_k$, we obtain the result. □

LEMMA 3.10. *If $1 \le d \le n$ such that no multiple of d lies in $(\alpha_n(n - h(n)n^{1/2}), \alpha_n(n + h(n)n^{1/2}))$, we have, uniformly in d, that $|\varepsilon_n(d)| = O(d^{-1})$.*

PROOF. Consider the sum $\sum_{k \equiv 0 \pmod d} B_n(k)$. The previous lemma shows that the sum is $o(n^{-1})$, and since $n^{-1} \le d^{-1}$, we are done. □

LEMMA 3.11. *If K_n is the number of integers $d \in [\alpha_n h(n) n^{1/2}, \alpha_n(n - h(n)n^{1/2})]$, for which some multiple lies in $(\alpha_n(n - h(n)n^{1/2}), \alpha_n(n + h(n)n^{1/2}))$, then*

$$K_n = O(\alpha_n h(n) n^{1/2} \log(n^{1/2}/h(n))).$$

PROOF. Let $u = \alpha_n n$, $v = \alpha_n h(n) n^{1/2}$, and $s = (u + v)/v$. Suppose $kd \in (u - v, u + v)$. Since $d \le u - v$, $k \ge 2$. Also, since $d \ge v$, we have $kv \le u + v$, and so $k \le s$. Thus there are $s - 1$ possible values for k. For each possible k, the corresponding d's lie in the interval

$((u-v)/k, (u+v)/k))$, which contains at most $2v/k+1$ integers. So, a bound for K_n is given by

$$\sum_{k=2}^{s}(2v/k+1) \le 2v\log s + (s-1) = 2\alpha_n h(n) n^{1/2}\log(n^{1/2}/h(n)+1) + n^{1/2}/h(n)$$
$$= O(\alpha_n h(n) n^{1/2}\log(n^{1/2}/h(n))).$$

□

Proof of Theorem 3.2. By Lemmas 3.4, 3.5, and 3.7, it suffices to show that

$$\lim_{n\to\infty}\sum_{d=1}^{n}|\varepsilon_n(d)|^k = 0.$$

To do this, define $n_1 = \lfloor \alpha_n h(n) n^{1/2}\rfloor$, $n_2 = \lfloor \alpha_n(n - h(n)n^{1/2})\rfloor$, and $n_3 = \lfloor \alpha_n(n+h(n)n^{1/2})\rfloor$. For sufficiently large n, we have $n_1 < n_2 < n_3 < n$, so we can express the sum as

$$\sum_{d=1}^{n} = \sum_{d=1}^{n_1} + \sum_{d=n_1+1}^{n_2} + \sum_{d=n_2+1}^{n_3} + \sum_{d=n_3+1}^{n}.$$

We will show that each of these four sums goes to 0.

First sum. Lemma 3.6 gives

$$\sum_{d=1}^{n_1} = O(n_1(\alpha_n n)^{-k/2}) = O(n_1(\alpha_n n)^{-1}) = O(h(n)n^{-1/2}).$$

Second sum. We further divide this sum into two components. The first is that over those d for which no multiple lies in $(\alpha_n(n-h(n)n^{1/2}), \alpha_n(n+h(n)n^{1/2}))$. By Lemma 3.10, this sum is

$$(\alpha_n n)^{(1-k)/2} O\left(\sum_{n_1+1}^{n_2} d^{-1}\right) = O((\alpha_n n)^{(1-k)/2}\log n),$$

which goes to 0. (If $k = 2$, we use the stronger hypothesis on α_n.) For the rest of the d's, we apply Lemma 3.11 to find that the sum over those d's is

$$O(\alpha_n h(n) n^{1/2} \log(n^{1/2}/h(n))(\alpha_n n)^{-k/2}) = O(h(n) n^{-1/2} \log(n^{1/2}/h(n))).$$

We will show that the latter expression goes to 0. To do this, for each $n > 0$, define the function $g_n(x) = x \log(n^{1/2}/x)$ for $x > 0$. The functions g_n are increasing on $(0, n^{1/2}/e)$. Now, by hypothesis, we have $h(n) = o(n^{1/2})$. Hence, for any $\varepsilon > 0$, we have $h(n) < \varepsilon n^{1/2}$ for sufficiently large n. So if we further have $\varepsilon < 1/e$, we find that $h(n) n^{-1/2} \log(n^{1/2}/h(n)) < n^{-1/2} g_n(\varepsilon n^{1/2}) = -\varepsilon \log \varepsilon$, which goes to 0 as $\varepsilon \to 0$.

Third sum. Similar to first sum.

Fourth sum. Apply Lemma 3.10 as in the first part of the second sum. □

3.3. Integers that are k-free

For $k \geq 2$, a positive integer is said to be k-free if it is not divisible by the kth power of a prime. Nymann and Leahey determined in [12] the probability that an integer chosen according to the binomial distribution is k-free, assuming that α is constant. Here, we prove the same by a different method, while allowing α to vary. We will call a quantity *negligible* if it is $O((\alpha_n n)^{-c})$ for all $c \in \mathbb{R}$. In this section, we make use of the normal approximation N_n to the binomial distribution, discussed at the beginning of Chapter 3. N_n decays quite rapidly as the distance from the mean increases. In particular, if a function $f(n)$ has the property $|f(n) - \alpha_n n| \geq (\alpha_n n)^{1/2+\varepsilon}$, then $N_n(f(n))$ is negligible. If P is a polynomial and $f(n)$ is negligible, then $f(n)P(\alpha_n n)$ is also negligible, and (provided α_n is bounded away from 1) $N_n(n)P(n)$ is negligible.

THEOREM 3.12. *Let α_n be bounded away from 1, and suppose $\alpha_n = \omega(1/n)$. As $n \to \infty$, the probability of an integer chosen according to the binomial distribution being k-free tends to $1/\zeta(k)$.*

PROOF. Let $S_k(x)$ be the set of all k-free integers at most x and $f_k(x)$ the number of k-free integers at most x. Using Theorem 3.1, we have $B_n(S_k(n)) = N_n(S_k(n)) + O((\alpha_n n)^{-1/2})$. Applying summation by parts, we have

$$N_n(S_k) = N_n(n) f_k(n) - \int_1^n N_n'(t) \left(\frac{t}{\zeta(k)} + R_k(t) \right) dt,$$

where $R_k(t)$ is a remainder term to be described. The term $N_n(n) f_k(n)$ is negligible. Moreover,

$$-\int_1^n N_n'(t) \frac{t}{\zeta(k)}\, dt = \frac{1}{\zeta(k)} \left(-(N_n(n)n - N_n(1)) + \int_1^n N_n(t)\, dt \right).$$

Here, $N_n(n)n$ and $N_n(1)$ are negligible. In order to show

$$\lim_{n\to\infty} \int_1^n N_n(t)\, dt = 1, \tag{3.1}$$

perform a change of variables $t = \sigma v + a$ to obtain

$$\frac{1}{\sqrt{2\pi}} \int_{(1-a)/\sigma}^{(n-a)/\sigma} e^{-\frac{1}{2}v^2}\, dv.$$

Since the restrictions on α_n show that the limits of integration approach $-\infty$ and ∞ respectively as $n \to \infty$, (3.1) is established.

Now we consider the remainder term. We have $R_k(t) = O(t^{1/k})$ ([16], p. 213). So the error is at most a constant times

$$\int_1^n |N_n'(t)| t^{1/k}\, dt = \int_1^a N_n'(t) t^{1/k}\, dt - \int_a^n N_n'(t) t^{1/k}\, dt,$$

which is, ignoring negligible terms,

$$2N_n(a)a^{1/k} - \frac{1}{k}\int_1^n N_n(t) t^{1/k-1}\, dt.$$

The term on the left is $O((\alpha_n n)^{1/k-1/2})$. For the integral on the right, we may replace it with

$$\int_\ell^n N_n(t) t^{1/k-1}\, dt,$$

where $\ell = a - a^{3/4}$. (The error is negligible since the integrand is negligible on the excluded interval, and the width of the excluded interval is less than a.) This latter integral is bounded above by

$$\ell^{1/k-1}\int_\ell^n N_n(t)\, dt,$$

which goes to 0 since ℓ increases without bound. Hence, provided $k > 2$, we have our result. To handle the case $k = 2$, we use the stronger bound $R_2(t) = O(f(t))$ where $f(t) = t^{1/2}\exp(-A\log^{1/2} t)$ for some A ([16], p. 213). Thus, in this case, the error is at most a constant times

$$\int_1^n |N_n'(t)| f(t)\, dt.$$

Since $f(t) = o(t^{1/2})$ and $f'(t) = O(t^{-1/2})$, we may make a similar argument to show that this integral goes to 0. □

3.4. The number-of-divisors function

The result here is not a probability calculation, but it is of a similar flavor, and we will use it later. It concerns the function $\tau(n)$, the number of divisors of n. For a function f, we write $f_{(1)}(x) = f(x+1) - f(x)$ for the first differences of f. Similarly $f_{(2)}$ denotes the first differences of $f_{(1)}$. The mth derivative of f will be denoted $f^{(m)}$. In this section we will denote N_n by simply N. We will write

$$T(x) = \sum_{1 \le j \le x} \tau(j).$$

Dirichlet showed that

$$T(x) = x \log x + (2\gamma - 1)x + \Delta(x),$$

where $\Delta(x) = O(\sqrt{x})$ and γ is Euler's constant [17]. We will establish an analogue of this for the binomial distribution. Our argument here is similar to that of the previous section, but more complicated. First, we need the following.

Lemma 3.13. *For α_n bounded away from 1 and $\alpha_n = \omega(1/n)$, and for $t \in \mathbb{Z}$ and $c \in \mathbb{R}$,*

$$\sum_{x=t}^{n} N(x) = 1 + O((\alpha_n n)^{-c}).$$

Proof. What follows is similar to pp. 43–44 of [5], but we give the complete argument. Fix an integer $m > 0$. The Euler–Maclaurin summation formula ([5], pp. 40–42) yields

$$\begin{aligned}\sum_{x=t}^{n} N(x) = \int_t^n N(x)\,dx + \frac{1}{2}(N(n) - N(t)) + \sum_{k=1}^{m} \frac{\tilde{B}_{2k}}{(2k)!}(N^{(2k-1)}(n) - N^{(2k-1)}(t)) \\ - \int_t^n N^{(2m)}(x) \frac{\tilde{B}_{2m}(x - \lfloor x \rfloor)}{(2m)!}\,dx,\end{aligned}$$

where $\tilde{B}_{2m}$ (the Bernoulli numbers) and $\tilde{B}_{2m}(x)$ (the Bernoulli polynomials) satisfy

$$|\tilde{B}_{2m}(x - \lfloor x \rfloor)| \leq |\tilde{B}_{2m}|. \tag{3.2}$$

For each $j > 0$, the jth derivative of N is of the form $N(x)$ multiplied by a polynomial. This shows that the error terms are negligible, with the exception of the integral

$$R = \int_t^n N^{(2m)}(x) \frac{\tilde{B}_{2m}(x - \lfloor x \rfloor)}{(2m)!}\, dx.$$

Using (3.2), the integral has magnitude at most

$$\frac{|\tilde{B}_{2m}|}{(2m)!} \int_t^n |N^{(2m)}(x)|\, dx = \frac{|\tilde{B}_{2m}|\sigma^{1/2-m}}{(2m)!} \int_{u(t)}^{u(n)} \left| \frac{d^{2m}}{dy^{2m}} e^{-\frac{1}{2}y^2} \right| dy,$$

where we have substituted $x = \sigma y + a$. The integrand does not depend on n, and since the derivatives of f are bounded, so is the integral. Hence $R = O((\alpha_n n)^{1/2-m})$. Letting m increase, we obtain

$$\sum_{x=t}^{n} N(x) = \int_t^n N(x)\, dx + O((\alpha_n n)^{-c}), \quad c \in \mathbb{R}.$$

We may replace the range of integration with $(-\infty, +\infty)$ with negligible error, as in the proof of Theorem 3.12. Thus, we are done. □

The main claim of this section is:

THEOREM 3.14. *For α_n bounded away from 1 and (for some $\varepsilon > 0$) $\alpha_n = \omega(n^{-1+\varepsilon})$,*

$$\sum_{j=1}^{n} B_n(j)\tau(j) = \log(\alpha_n n) + 2\gamma + O((\alpha_n n)^{-1/4}).$$

PROOF. By Theorem 3.1 and the estimate $\tau(x) = o(x^\eta)$ for any $\eta > 0$ ([2], p. 296), we have

$$\sum_{j=1}^{n} B_n(j)\tau(j) = \sum_{x=1}^{n} N(x)\tau(x) + o((\alpha_n^{-1/2} n^{-1/2+\eta})).$$

The restrictions on α_n show that the error term is $O((\alpha_n n)^{-1/4})$. Summation by parts yields

$$\sum_{x=1}^{n} N(x)\tau(x) = N(n)T(n) - \sum_{x=1}^{n-1} N_{(1)}(x)T(x).$$

The term $N(n)T(n)$ is negligible, so we are left to describe the asymptotics of

$$-\sum_{x=1}^{n-1} N_{(1)}(x)T(x). \tag{3.3}$$

Now we write $T(x)$ as $x\log x + (2\gamma - 1)x + \Delta(x)$. Each of the terms yields a sum to examine. First, we have

$$-\sum_{x=1}^{n-1} N_{(1)}(x)x\log x = -N(n)n\log n + \sum_{x=1}^{n-1} N(x+1)(x\log x)_{(1)}, \tag{3.4}$$

Similar to before, $-N(n)n\log n$ is negligible. As for the sum on the right, the mean value theorem implies that $\log(x) + 1 \leq (x\log x)_{(1)} \leq \log(x+1) + 1$. Therefore, a lower bound for this sum is

$$\sum_{x=2}^{n} N(x)(\log(x-1) + 1). \tag{3.5}$$

Writing $\log(x-1) + 1$ as $(\log a + 1) + (\log(x-1) - \log a)$, the sum breaks up into

$$\sum_{x=2}^{n} N(x)(\log a + 1),$$

which by Lemma 3.13 is $\log a + 1$ with negligible error, and

$$\sum_{x=2}^{n} N(x)(\log(x-1) - \log a).$$

With negligible error, we contract the range of summation to $(a - a^c, a + a^c)$, for some c in $(1/2, 3/4)$. (Proof of negligibility: $N(x)$ is negligibly small on the excluded intervals, the logarithmic term is $O(n)$, and the range excluded has length less than n. The restrictions on α_n imply that $n = o((\alpha_n n)^{1/\varepsilon})$). By the mean value theorem, $|\log(x-1) - \log(a)| \leq |(x-1) - a|/a$. For x in the new range of summation, $|(x-1) - a|/a \leq a^{c-1} + 1/a$. Hence, the sum is $o((\alpha_n n)^{-1/4})$. Therefore, (3.5) converges to $\log a + 1$ with error $o((\alpha_n n)^{-1/4})$. A similar argument shows that the upper bound

$$\sum_{x=2}^{n} N(x)(\log x + 1)$$

also converges to $\log a + 1$ with the same error bound. Hence (3.4) itself does.

The second sum from (3.3) to examine is

$$-\sum_{x=1}^{n-1} N_{(1)}(x)(2\gamma - 1)x = (2\gamma - 1)\left(-N(n)n + \sum_{x=1}^{n} N(x)\right).$$

The term $-N(n)n$ is negligible and so by Lemma 3.13 we obtain $2\gamma - 1$ in the limit.

So far, we have found the main term $\log(\alpha_n n) + 2\gamma$. In analyzing (3.3) it remains to examine the sum

$$-\sum_{x=1}^{n-1} N_{(1)}(x)\Delta(x). \tag{3.6}$$

We show that (3.6) is $O((\alpha_n n)^{-1/4})$. To do this, we write it as

$$-N_{(1)}(n-1)\Delta_2(n-1) + \sum_{x=1}^{n-2} N_{(2)}(x)\Delta_2(x),$$

where $\Delta_2(x) = \sum_{y=1}^{x} \Delta(y)$. As usual, $-N_{(1)}(n-1)\Delta_2(n-1)$ is negligible. For the sum on the right we use a result from [17]:

$$\Delta_2(x) = \frac{1}{2}x\log x + \left(\gamma - \frac{1}{4}\right)x + O(x^{3/4}).$$

Again, after substituting for $\Delta_2(x)$, we divide into cases. First, letting $f(x) = x\log x$, we have

$$\sum_{x=1}^{n-2} N_{(2)}(x)f(x) = N_{(1)}(n-1)f(n-1) - \sum_{x=1}^{n-2} N_{(1)}(x+1)f_{(1)}(x).$$

Here $N_{(1)}(n-1)f(n-1)$ is negligible, and the expression that remains is

$$-N(n)f_{(1)}(n-1) + N(2)f(2) + \sum_{x=1}^{n-2} N(x+1)f_{(2)}(x). \tag{3.7}$$

Ignoring the negligible terms, we consider the sum that remains. By the mean value theorem,

$$f_{(2)}(x) \le \sup_{y\in[x,x+1]} f'_{(1)}(y) \le \sup_{z\in[x,x+2]} f''(z) = 1/x.$$

(There is no ambiguity, because $(f_{(1)})' = (f')_{(1)}$.) Hence, by restricting the range of summation, we can prove that (3.7) is $O(1/(\alpha_n n))$. Next,

$$\sum_{x=1}^{n-2} N_{(2)}(x)x$$

is negligible, as $x_{(2)} = 0$. Finally, we must consider

$$\sum_{x=1}^{n-2} N_{(2)}(x) O(x^{3/4}).$$

This is bounded above by a constant times

$$\sum_{x=1}^{n-2} |N_{(2)}(x)| x^{3/4}. \tag{3.8}$$

Now, the mean value theorem implies that $\sup |N_{(1)}(x)| \leq \sup |N'(x)| = O(1/(\alpha_n n))$. Moreover, $N''(x)$ has exactly two zeros. Therefore, if we define $S = \{x \in \mathbb{Z} \mid \operatorname{sgn} N_{(2)}(x) \neq \operatorname{sgn} N_{(2)}(x+1)\}$, then the size of S is bounded above by a constant independent of n. Now, (3.8) is bounded above by the sum of the usual negligible terms, and

$$2 \sum_{x \in S} |N_{(1)}(x+1)| x^{3/4} + \sum_{x=1}^{n-2} |N_{(1)}(nx+1)| (x^{3/4})_{(1)}.$$

The left sum is $O((\alpha_n n)^{-1/4})$. Since $(x^{3/4})_{(1)} \leq x^{-1/4}$, the sum on the right is, besides negligible terms, bounded above by

$$2 \sum_{x \in U} N(x+1) x^{-1/4} + \sum_{x=1}^{n-2} N(x+1) (x^{-1/4})_{(1)},$$

where $U = \{x \in \mathbb{Z} \mid \operatorname{sgn} N_{(1)}(x) \neq \operatorname{sgn} N_{(1)}(x+1)\}$. Since $N'(x)$ has a single root at $x = a$, the sum on the left is $O((\alpha_n n)^{-3/4})$. By restricting the range of summation, we see that the sum on the right is $O((\alpha_n n)^{-5/4})$.

This completes the proof. □

3.5. Integers k-wise relatively prime

In [18], László Tóth determined the probability that a tuple of s integers is pairwise coprime. Jerry Hu, in [7], generalizes this to the situation in which any k of the chosen integers are coprime. We here follow Hu, showing that his argument can be made to apply to a binomial distribution instead of a uniform distribution.

A tuple of s integers is defined to be k-wise relatively prime if any k of them are relatively prime, and to be k-wise relatively prime to an integer u if any k of them are prime to u. The probability of s integers being k-wise relatively prime when chosen according to the binomial distribution is the same as that found by Hu for the uniform distribution:

$$A_{s,k} = \prod_p \left(1 - \sum_{m=k}^{s} B_{1/p,n}(m)\right).$$

We use notation similar to Hu's. Namely, for a tuple $\mathbf{u} = (u_1, \ldots, u_{k-1})$, let $S_{s,k}^{(\mathbf{u})}(n)$ denote the set of s-tuples of integers $(a_1, \ldots, a_s)$ in $[1, n]$ that are k-wise relatively prime and i-wise relatively prime to u_i for $1 \le i \le k-1$. Define

$$Q_{s,k}^{(\mathbf{u})}(n) = B_n^s(S_{s,k}^{(\mathbf{u})}(n)).$$

For integers a,$b > 0$, Hu defines $(a, b]$ to be the product, over primes p dividing a, of the largest power of p dividing b. Put $[b, a) = (a, b]$. Define, for any positive integer j,

$$j * \mathbf{u} = \left(\frac{u_1(j, u_2)}{(j, u_1]}, \ldots, \frac{u_{k-2}(j, u_{k-1})}{(j, u_{k-1}]}, \frac{j u_{k-2}}{(\prod_{i=2}^{k-1}[j, u_i))(j, u_{k-1}]}\right).$$

(Here (x, y) denotes $\gcd(x, y)$.) Importantly, if $\mathbf{u}$ is a pairwise coprime tuple of positive integers, then so is $j * \mathbf{u}$.

LEMMA 3.15. *For* $\mathbf{u}$ *pairwise coprime,*

$$Q_{s+1,k}^{(\mathbf{u})}(n) = \sum_{\substack{j=1 \\ (j,u_1)=1}}^{n} B_n(j) Q_{s,k}^{(j*\mathbf{u})}(n).$$

PROOF. Hu ([7], p. 1065) observes that

> $s+1$ positive integers $a_1, a_2, \ldots, a_{s+1}$ are k-wise relatively prime and are i-wise relatively prime to u_i for $i = 1, 2, \ldots, k-1$ if and only if the first s positive integers $a_1, a_2, \ldots, a_s$ are k-wise relatively prime and are i-wise relatively prime to u_i and (a_{s+1}, u_{i+1}) for $i = 1, 2, \ldots, k-2$ and are $(k-1)$-wise relatively prime to u_{k-1} and a_{s+1}, and $(a_{s+1}, u_1) = 1 \ldots$

This justifies the equalities

$$Q_{s+1,k}^{(\mathbf{u})}(n) = \sum_{\substack{a_{s+1}=1 \\ (a_{s+1},u_1)=1}}^{n} B_n(a_{s+1}) Q_{s,k}^{(a_{s+1}*'\mathbf{u})}(n) = \sum_{\substack{j=1 \\ (j,u_1)=1}}^{n} B_n(j) Q_{s,k}^{(j*'\mathbf{u})}(n),$$

where

$$j *' \mathbf{u} = (u_1(j, u_2), \ldots, u_{k-2}(j, u_{k-1}), j u_{k-1}).$$

To complete the proof, we need only show that $S_{s,k}^{(j*'\mathbf{u})}(n) = S_{s,k}^{(j*\mathbf{u})}(n)$. The argument is contained in Hu [7]. (He only claims that the sets have the same cardinality, but his argument shows that they are the same set.) □

LEMMA 3.16. *Suppose* α_n *is bounded away from* 1. *Then, for integers* u, $m \geq 1$ *with* $(m, u) = 1$, *we have*

$$\sum_{\substack{a=1 \\ (a,u)=1 \\ m|a}}^{n} B_n(a) = \frac{\varphi(u)}{mu} + O((\alpha_n n)^{-1/2} \theta(u)),$$

where $\theta(u)$ *is the number of squarefree divisors of* u.

PROOF. The desired sum equals

$$\sum_{\substack{a=1\\ m|a}}^{n} B_n(a) \sum_{d|(a,u)} \mu(d) = \sum_{\substack{a=1\\ m|a}}^{n} B_n(a) \sum_{\substack{d|a\\ d|u}} \mu(d) = \sum_{d|u} \mu(d) \sum_{\substack{j\geq 1\\ md|j}} B_n(j).$$

Applying Lemma 3.6, this is

$$\sum_{d|u} \mu(d) \left(\frac{1}{md} + O((\alpha_n n)^{-1/2}) \right) = \frac{1}{m} \sum_{d|u} \frac{\mu(d)}{d} + O((\alpha_n n)^{-1/2} \theta(u)).$$

Since $\sum_{d|u} \mu(d)/d = \varphi(u)/u$, we are done. □

LEMMA 3.17. *Define*

$$f_{s,k,i}(u_i) = \prod_{p|u_i} \left(1 - \frac{\sum_{m=i}^{k-1} \binom{s}{m} (p-1)^{k-1-m}}{\sum_{m=0}^{k-1} \binom{s}{m} (p-1)^{k-1-m}} \right)$$

and

$$g_{s,i}(d) = d^i \prod_{p|d} \sum_{m=0}^{i} \binom{s}{m} \left(1 - \frac{1}{p}\right)^{i-m} \frac{1}{p^m}.$$

Then, we have

$$\frac{f_{s,k,i}(u_i)}{f_{s,k,i+1}(u_i)} = \sum_{d|u_i} \frac{\mu(d) \binom{s}{i}^{\omega(d)}}{g_{s,i}(d)}, \qquad i = 1, \ldots, k-2$$

and

$$f_{s,k,k-1}(u_{k-1}) = \sum_{d|u_{k-1}} \frac{\mu(d) \binom{s}{k-1}^{\omega(d)}}{g_{s,k-1}(d)},$$

PROOF. This is Lemma 4 of Hu [7]. □

THEOREM 3.18. *Let $\delta(s,k)$ be the maximum value of $\binom{s-1}{i}$ for $1 \leq i \leq k-1$. Suppose α_n is bounded away from 1 and $\alpha_n = \omega(n^{-1+\varepsilon})$. For $s \geq 1$ and $k \geq 2$, then uniformly in u_i*

with the u_i coprime, we have

$$Q_{s,k}^{(\mathbf{u})}(n) = A_{s,k} \prod_{i=1}^{k-1} f_{s,k,i}(u_i) + O((\alpha_n n)^{-1/2} \theta(u_1) \log^{\delta(s,k)} n).$$

PROOF. By induction on s. For $s = 1$, Lemma 3.16 shows that

$$Q_{s,k}^{(\mathbf{u})}(n) = \frac{\varphi(u_1)}{u_1} + O((\alpha_n n)^{-1/2} \theta(n)),$$

from which the result follows since $A_{1,k} = 1$, $f_{1,k,1}(u_1) = \phi(u_1)/u_1$ and $f_{1,k,i}(u_1) = 1$ for $i > 1$.

Next, we will prove the result for $s+1$ assuming it for s. We obtain, using Lemma 3.15,

$$\begin{aligned}
Q_{s+1,k}^{(\mathbf{u})}(n) &= \sum_{\substack{j=1 \\ (j,u_1)=1}}^{n} B_n(j) Q_{s,k}^{(j*\mathbf{u})}(n) \\
&= \sum_{\substack{j=1 \\ (j,u_1)=1}}^{n} B_n(j) A_{s,k} \prod_{i=1}^{k-2} f_{s,k,i}\left(\frac{u_1(j,u_2)}{(j,u_1]}\right) f_{s,k,k-1}\left(\frac{j u_{k-1}}{(\prod_{i=2}^{k-1}[j,u_i))(j,u_{k-1}]}\right) \\
&\quad + O(B_n(j)(\alpha_n n)^{-1/2} \theta(u_1(j,u_2)) \log^{\delta(s,k)} n) \\
(*) \qquad &= A_{s,k} \prod_{i=1}^{k-1} f_{s,k,i}(u_i) \sum_{\substack{j=1 \\ (j,u_1)=1}}^{n} B_n(j) \prod_{i=1}^{k-2} \frac{f_{s,k,i}((j,u_{i+1}))}{f_{s,k,i+1}((j,u_{i+1}))} f_{s,k,k-1}\left(\frac{j}{\prod_{i=2}^{k-1}[j,u_i)}\right) \\
&\quad + O\left((\alpha_n n)^{-1/2} \theta(u_1) \log^{\delta(s,k)} n \sum_{j=1}^{n} B_n(j)\theta(j)\right).
\end{aligned}$$

Using Theorem 3.14, we have $\sum_{j=1}^{n} B_n(j)\theta(j) \le \sum_{j=1}^{n} B_n(j)\tau(j) = O(\log n)$. We also have

$$\sum_{\substack{j=1 \\ (j,u_1)=1}}^{n} B_n(j) \prod_{i=1}^{k-2} \frac{f_{s,k,i}((j,u_{i+1}))}{f_{s,k,i+1}((j,u_{i+1}))} f_{s,k,k-1}\left(\frac{j}{\prod_{i=2}^{k-1}[j,u_i)}\right)$$

$$= \sum_{\substack{j=1\\(j,u_1)=1}}^{n} B_n(j) \prod_{i=1}^{k-2} \sum_{d_i|(j,u_{i+1})} \frac{\mu(d_i)\binom{s}{i}^{\omega(d_i)}}{g_{s,i}(d_i)} \sum_{d_{k-1}|\frac{j}{\prod_{i=2}^{k-1}[j,u_i)}} \frac{\mu(d_{k-1})\binom{s}{k-1}^{\omega(d_{k-1})}}{g_{s,k-1}(d_{k-1})}$$

$$= \sum_{\substack{d_1\cdots d_{k-1}e=j\le n\\ d_i|(j,u_{i+1}),i=1,\dots,k-2\\ d_{k-1}|\frac{j}{[j,u_2)\cdots[j,u_{k-1})}\\ (j,u_1)=1}} B_n(j) \prod_{i=1}^{k-1} \frac{\mu(d_i)\binom{s}{i}^{\omega(d_i)}}{g_{s,i}(d_i)}$$

$$= \sum_{\substack{d_1\cdots d_{k-1}\le n\\ d_i|u_{i+1},i=1,\dots,k-2\\ (d_{k-1},u_i),i=1,\dots,k-1}} \sum_{\substack{e\le\frac{n}{d_1\cdots d_{k-1}}\\ (e,u_1)=1}} B_n(d_1\cdots d_{k-1}e) \prod_{i=1}^{k-1} \frac{\mu(d_i)\binom{s}{i}^{\omega(d_i)}}{g_{s,i}(d_i)}.$$

Using Lemma 3.16, we have

$$\sum_{\substack{j=1\\(j,u_1)=1}}^{n} B_n(j) \prod_{i=1}^{k-2} \frac{f_{s,k,i}((j,u_{i+1}))}{f_{s,k,i+1}((j,u_{i+1}))} f_{s,k,k-1}\left(\frac{j}{\prod_{i=2}^{k-1}[j,u_i)}\right)$$

$$= \sum_{\substack{d_1\cdots d_{k-1}\le n\\ d_i|u_{i+1},i=1,\dots,k-2\\ (d_{k-1},u_i),i=1,\dots,k-1}} \prod_{i=1}^{k-1} \frac{\mu(d_i)\binom{s}{i}^{\omega(d_i)}}{g_{s,i}(d_i)} \left(\frac{\varphi(u_1)}{u_1 d_1\cdots d_{k-1}} + O((\alpha_n n)^{-1/2}\theta(u_1))\right)$$

$$= \frac{\varphi(u_1)}{u_1} \sum_{\substack{d_1\cdots d_{k-1}\le n\\ d_i|u_{i+1},i=1,\dots,k-2\\ (d_{k-1},u_i),i=1,\dots,k-1}} \prod_{i=1}^{k-1} \frac{\mu(d_i)\binom{s}{i}^{\omega(d_i)}}{d_i g_{s,i}(d_i)} + O\left((\alpha_n n)^{-1/2}\theta(u_1)\sum_{d\le n}\frac{\delta(s+1,k)^{\omega(d)}}{d}\right),$$

as $g_{s,i}(d_i) \ge d_i$.

This may be expressed as

$$\frac{\varphi(u_1)}{u_1} \sum_{\substack{d_i|u_{i+1},i=1,\dots,k-2\\ (d_{k-1},u_i),i=1,\dots,k-1}} \prod_{i=1}^{k-1} \frac{\mu(d_i)\binom{s}{i}^{\omega(d_i)}}{d_i g_{s,i}(d_i)}$$

$$= \frac{\varphi(u_1)}{u_1} \prod_{i=2}^{k-1} \prod_{p|u_i} \left(1 - \frac{\binom{s}{i-1}}{p\sum_{m=0}^{i-1}\binom{s}{m}(p-1)^{i-1-m}}\right) \prod_{p\nmid u_1\cdots u_{k-1}} \left(1 - \frac{\binom{s}{k-1}}{p\sum_{m=0}^{k-1}\binom{s}{m}(p-1)^{k-1-m}}\right)$$

$$= \prod_{i=1}^{k-1} \prod_{p|u_i} \left(1 - \frac{\binom{s}{i-1}}{p\sum_{m=0}^{i-1}\binom{s}{m}(p-1)^{i-1-m}}\right)\left(1 - \frac{\binom{s}{k-1}}{p\sum_{m=0}^{k-1}\binom{s}{m}(p-1)^{k-1-m}}\right)^{-1}$$
$$\times \prod_{p} \left(1 - \frac{\binom{s}{k-1}}{p\sum_{m=0}^{k-1}\binom{s}{m}(p-1)^{k-1-m}}\right),$$

together with the error terms

$$O\left(\sum_{d>n} \frac{\delta(s+1,k)^{\omega(d)}}{d^2}\right) = O\left(\sum_{d>n} \frac{\tau_{\delta(s+1,k)}(d)}{d^2}\right) = O(n^{-1}\log^{\delta(s+1,k)-1} n),$$

by Lemma 3(b) of [18], and

$$O\left((\alpha_n n)^{-1/2}\theta(u_1)\sum_{d\le n} \frac{\delta(s+1,k)^{\omega(d)}}{d}\right) = O\left((\alpha_n n)^{-1/2}\theta(u_1)\sum_{d\le n} \frac{\tau_{\delta(s+1,k)}(d)}{d}\right)$$
$$= O((\alpha_n n)^{-1/2}\theta(u_1)\log^{\delta(s+1,k)} n),$$

by Lemma 3(a) of [18]. We substitute into (*) to get

$$\begin{aligned} Q^{(\mathbf{u})}_{s+1,k}(n) &= A_{s,k}\prod_{p}\left(1 - \frac{\binom{s}{k-1}}{p\sum_{m=0}^{k-1}\binom{s}{m}(p-1)^{k-1-m}}\right) \\ &\quad \times \prod_{i=1}^{k-1} f_{s,k,i}(u_i)\prod_{p|u_i}\left(1 - \frac{\binom{s}{i-1}}{p\sum_{m=0}^{i-1}\binom{s}{m}(p-1)^{i-1-m}}\right) \\ &\quad \times \left(1 - \frac{\binom{s}{k-1}}{p\sum_{m=0}^{k-1}\binom{s}{m}(p-1)^{k-1-m}}\right)^{-1} \\ &\quad + O(n^{-1}\log^{\delta(s+1,k)-1} n) + O((\alpha_n n)^{-1/2}\theta(u_1)\log^{\delta(s+1,k)} n) \\ &\quad + O\left((\alpha_n n)^{-1/2}\theta(u_1)\log^{\delta(s,k)+1} n\right) \\ &= A_{s+1,k}\prod_{i=1}^{k-1} f_{s+1,k,i}(u_i) + O((\alpha_n n)^{-1/2}\theta(u_1)\log^{\delta(s+1,k)} n). \end{aligned}$$

This establishes the claim for $s+1$. □

COROLLARY 3.19. *If α_n is bounded away from 1 and $\alpha_n = \omega(n^{-1+\varepsilon})$, then the probability that s integers chosen according to the binomial distribution are k-wise relatively prime approaches $A_{s,k}$ as $n \to \infty$.*

3.6. PRIME NUMBERS

Let Π be the set of all prime numbers. Here we seek information on the behavior of $B_n(\Pi)$ as $n \to \infty$. We can show that $B_n(\Pi) \to 0$. If we use the prime number theorem, we can deduce a bit more:

THEOREM 3.20. *If α_n is bounded away from 1 and $\alpha_n = \omega(1/n)$, then*

$$\limsup_{n\to\infty} B_n(\Pi) \log\log(\alpha_n n) \leq 1.$$

PROOF. (The germ of this proof is found in [1], pp. 101–103.) Let $x = (\alpha_n n)^{1/2}$. For any j denote by $j\#$ the primorial, the product of all primes at most j. Let p_m denote the mth prime. For any n, let m be such that $p_m\#$ is the largest primorial less than x. Let $y = p_{m+1}\#$. Now, for $m \gg 0$, we have $p_m\# > p_{m+1}^2$ ([16], p 246). Therefore, for $n \gg 0$, we have $p_{m+1} < x^{1/2}$, so $y < x^{3/2}$. Write

$$B_n(\Pi) = \sum_{2\leq p\leq y} B_n(p) + \sum_{p>y} B_n(p).$$

Using Theorem 3.1, we obtain

$$\sum_{2\leq p\leq y} B_n(p) \leq \sum_{j=2}^{y} B_n(j) = \sum_{j=2}^{y} N_n(j) + O((\alpha_n n)^{-1/2}).$$

The sum on the right is bounded by $yN_n(y)$. Since $y < a^{3/4}$, we see that $yN_n(y)$ is negligible.

Now, for primes $p > y$, we have $(p, y) = 1$. Hence, by Lemma 3.16,

$$\sum_{p>y} B_n(p) \leq \sum_{\substack{j=1 \\ (j,y)=1}}^{n} B_n(j) = \frac{\varphi(y)}{y} + O((\alpha_n n)^{-1/2}\theta(y)).$$

We know $\theta(y) = o(y^{\varepsilon})$, so the error term is $O((\alpha_n n)^{-1/2+\varepsilon})$. According to one version of the prime number theorem ([2], p. 79), $p_{m+1} \sim \log y$, so

$$\frac{\varphi(y)}{y} = \prod_{i=1}^{m+1}\left(1 - \frac{1}{p_i}\right) \leq \left(\sum_{j=1}^{p_{m+1}} \frac{1}{j}\right)^{-1} \sim \frac{1}{\log p_{m+1}}$$
$$\sim \frac{1}{\log\log y} < \frac{1}{\log\log x} \sim \frac{1}{\log\log(\alpha_n n)}.$$

□

3.7. The case $\alpha_n = 1/n$

In our results so far, we have assumed that if α_n goes to 0, then it goes to 0 more slowly than $1/n$. Indeed, it is known, and it is not difficult to prove, that if $\alpha_n = \lambda/n$, and if S is any set of nonnegative integers, then

$$\lim_{n\to\infty} B_n(S) = e^{-\lambda} \sum_{j\in S} \frac{\lambda^j}{j!}.$$

(This fact is mentioned on pp. 152–153 of [9].) For example, if we put $\alpha_n = 1/n$ and $S = \Pi$, the limiting value is $\exp_{\Pi}(1)/e$, rather than 0 as in Theorem 3.20. To get an intuitive understanding of why there is a difference if $\alpha_n = 1/n$, note that the mode of the binomial distribution is approximately $\alpha_n n$. So, with $\alpha_n = 1/n$, a significant part of the distribution remains close to 1, whereas if α_n goes to 0 more slowly, the mode goes to infinity. In general, we cannot expect the same behavior in this case.

3.8. Future directions

Can we describe the behavior of $B_n(\Pi)$ more precisely? One might think that one could use a summation by parts, as in Theorem 3.12, to handle this question. Unfortunately, the error term in the prime number theorem is not small enough for this to work, even if we assume the Riemann hypothesis. To be more precise, we may define the logarithmic integral

$$\mathrm{Li}(x) = \int_2^x \frac{1}{\log t}\, dt,$$

and state the prime number theorem as

$$\pi(x) = \mathrm{Li}(x) + R(x).$$

If we assume the Riemann hypothesis, then we have $R(x) = O(x^{1/2} \log x)$ ([8], p. 193). If we proceeded analogously to Theorem 3.12, we would need to estimate the integral

$$\int_2^n N_n'(t)\pi(t)\, dt.$$

When we substitute for $\pi(x)$, the term $\mathrm{Li}(x)$ causes no difficulty, but $R(x)$ does. We need to use the upper bound for $|R(x)|$ to obtain an upper bound for

$$\int_2^n N_n'(t)R(t)\, dt,$$

but since $N_n'(t)$ changes sign, doing this requires splitting the integral in two, and, similarly to Theorem 3.12, we would obtain the term $2N_n(a)R(a)$, which, using the estimate for $R(x)$ above, cannot even be shown to be $o(1)$, and hence we obtain no information.

In the rest of this section we describe a different possible method of approaching this problem, as well as the difficulties involved. If we define $b_n = B_n(\Pi)$, then the exponential generating function of b_n is

$$F(z) = \sum_{n=0}^{\infty} \frac{b_n z^n}{n!} = \exp_{\Pi}(\alpha_n z) \exp(\beta_n z),$$

where

$$\exp_{\Pi}(z) = \sum_{p} \frac{z^p}{p!}.$$

Hayman [6] defined a class of "admissible functions", and gave an asymptotic formula for the power series coefficients of such functions. Thus, if we show that the exponential generating function F is admissible, we will obtain an asymptotic formula for $b_n/n!$, and hence for b_n by applying Stirling's formula. We here give Hayman's result, as described in [13], pp. 1178–1179. A function of the form

$$f(z) = \sum_{z=0}^{\infty} f_n z^n$$

is admissible if

(i) $f(z)$ is analytic for $|z| < R$ for some $0 < R \leq \infty$,

(ii) $f(z) \in \mathbb{R}$ if $z \in \mathbb{R}$ for $|z| < R$,

(iii) for $R_0 < r < R, \max_{|z|=r} |f(z)| = f(r)$,

(iv) for

$$a(r) = r\frac{f'(r)}{f(r)}, \qquad b(r) = ra'(r)$$

there is a function $\delta(r)$ defined for $R_0 < r < R$ such that $0 < \delta(r) < \pi$, and the following hold:

(a) $f(re^{i\theta}) \sim f(r) \exp(i\theta a(r) - \theta^2 b(r)/2)$ as $r \to R$ uniformly for $|\theta| < \delta(r)$,

(b) $f(re^{i\theta}) = o(f(r)b(r)^{-1/2})$ as $r \to R$ uniformly for $\delta(r) \leq |\theta| \leq \pi$,

(c) $b(r) \to \infty$ as $r \to R$.

Then, Hayman proved the following.

THEOREM 3.21. *If f is admissible, then*

$$f_n \sim (2\pi b(r_n))^{-1/2} f(r_n) r_n^{-n} \text{ as } n \to \infty,$$

where $a(r_n) = n$.

We want to apply this to our function F. Conditions (i), (ii), and (iii) are obvious. In order to verify condition (iv), we would need good information on the behavior of $a(r)$ and $b(r)$, which devolves onto information about $\exp_\Pi$. Unfortunately, obtaining such information seems to be quite difficult. We would like to know how fast $\exp_\Pi(x)$ grows as $x \to \infty$. If we try to determine this using summation by parts, we run into essentially the same problem we discussed above. Based on numerical computation, however, the function appears to approximate $\exp(x)/\log(x)$. Let us suppose we know that $\exp_\Pi(x) \sim \exp(x)/\log(x)$. One conclusion we could make is that all the derivatives of $\exp_\Pi$ have the same rate of growth as $\exp_\Pi$. To prove this, we need the following.

PROPOSITION 3.22. *Let*

$$f(x) = \sum_{n=0}^{\infty} a_n \frac{x^n}{n!},$$

and set

$$A_n = \sum_{m=0}^{n} a_n.$$

Suppose that, for some M, we have $|A_n| \leq M$ for all n. Then, $f(x) = O(e^x/\sqrt{x})$ as $x \to \infty$.

PROOF. Applying summation by parts, we have

$$f(x) = \sum_{k=0}^{\infty} A_k \left(\frac{x^k}{k!} - \frac{x^{k+1}}{(k+1)!} \right) \leq \sum_{k=0}^{\infty} s_k \left(\frac{x^k}{k!} - \frac{x^{k+1}}{(k+1)!} \right),$$

where $s_k = -M$ for $0 \leq k \leq x-1$ and $s_k = M$ for $k > x-1$. Thus, applying summation by parts again, $f(x) \leq -M + 2Mx^{\lceil x-1 \rceil}/(\lceil x-1 \rceil)!$, and the desired bound follows by Stirling's formula. The same argument establishes an upper bound for $-f(x)$, so we are done. $\square$

Now we can show our claim. We have

$$\frac{\exp'_\Pi(x)}{\exp_\Pi(x)} - 1 = \frac{\exp'_\Pi(x) - \exp_\Pi(x)}{\exp_\Pi(x)}.$$

By the preceding proposition, $\exp'_\Pi(x) - \exp_\Pi(x) = O(e^x/\sqrt{x})$, and since this grows slower than $\exp(x)/\log(x)$, we have established, on the assumption that $\exp_\Pi(x) \sim \exp(x)/\log(x)$, that $\exp_\Pi(x) \sim \exp'_\Pi(x)$. We can, of course, now make an inductive argument to show that all the derivatives are also asymptotic to each other. Additionally, since

$$a(r) = r \left(\frac{\alpha_n \exp'_\Pi(\alpha_n r)}{\exp_\Pi(\alpha_n r)} + \beta_n \right),$$

we can conclude that $a(r) \sim r$. This, however, is where the chain of deductions stops. We can compute $b(r)$ to be

$$a(r) + (\alpha_n r)^2 \frac{\exp'_\Pi(\alpha_n r)}{\exp_\Pi(\alpha_n r)} \left(\frac{\exp''_\Pi(\alpha_n r)}{\exp'_\Pi(\alpha_n r)} - \frac{\exp'_\Pi(\alpha_n r)}{\exp_\Pi(\alpha_n r)} \right).$$

Our assumption on the growth of $\exp_\Pi(x)$ implies that the expression in parentheses on the right goes to 0. If we knew further that this expression is $o(1/r)$, it would follow that $b(r) \sim r$. I have not found a way to do this, however.

In conclusion, this method of attack leads to difficulties similar to that of the more direct method.

CHAPTER 4

Statistics on the number of points on complete intersections

By combining the results in Chapters 2 and 3, we can obtain probabilistic information about the numbers of points on complete intersections. When doing this, we need to make restrictions on the behavior of the degrees of the hypersurface sections relative to the order q of the field, so that the error term goes to 0. Here are two examples.

Theorem 4.1. *Fix $m \geq 2$ and $1 \leq j \leq m-1$. Suppose $\{q_i\}_{i\geq 1}$ is a sequence of prime powers increasing to infinity and suppose the integers $d_{i,1} \leq \cdots \leq d_{i,j}$ go to infinity in such a way that $d_{i,1} > 2^{1+mn_{q_i}/(2j+1)}$ and $d_{i,j} = o((2^{-n_{q_i}} q_i^{d_{i,1}/\max(m+1,p)})^{1/m})$. For a fixed $k \geq 2$, the probability that a smooth complete intersection (formed by intersecting hypersurfaces of degrees $d_{i,1}, \ldots, d_{i,j}$) has the number of points k-free is, in the limit, $1/\zeta(k)$.*

Proof. For any $n \geq q_1$, let the integer $r(n)$ be maximal such that $n_{q_{r(n)}}$ does not exceed n. Let $\alpha_n = (q_{r(n)}^{-j} L(q_{r(n)}, m, j))/(1 - q_{r(n)}^{-j} + q_{r(n)}^{-j} L(q_{r(n)}, m, j))$. We have $\alpha_n = \Omega(n^{-j/m})$, and so Theorem 3.12 tells us that as $n \to \infty$ the probability of integers chosen according to the binomial distribution being k-free approaches $1/\zeta(k)$. By Theorem 2.16, this is also true of the number of points on a smooth complete intersection, since our hypotheses ensure that the error term in the theorem (multiplied by $2^{n_{q_{r(i)}}}$, the maximum number of choices for R in the theorem) goes to 0. □

Theorem 4.2. *Fix $m \geq 2$, $s \geq 2$, $k \geq 2$ and $1 \leq j \leq m-1$. Suppose $\{q_i\}_{i\geq 1}$ is a sequence of prime powers increasing to infinity and suppose the integers $d_{i,1} \leq \cdots \leq d_{i,j}$ go to infinity in such a way that $d_{i,1} > 2^{1+mn_{q_i}/(2j+1)}$ and $d_{i,j} = o((2^{-n_{q_i}} q_i^{d_{i,1}/\max(m+1,p)})^{1/m})$.*

The probability that s smooth complete intersections $H_1, \ldots, H_s$ (formed by intersecting hypersurfaces of degrees $d_{i,1}, \ldots, d_{i,j}$) have the numbers of points on $H_1, \ldots, H_s$ to be k-wise relatively is, in the limit, $A_{s,k}$.

PROOF. Similar to the previous theorem. □

The restrictions on q_i, $d_{i,1}, \ldots, d_{i,j}$ in the previous theorems depend heavily on the error term in Theorem 1.2 of [4]. If a better error term were found, this would correspondingly imply a relaxation on these restrictions. If $j = m$, these theorems do not apply. However, in the case $j = m = 1$, the parameter in the binomial distribution is $1/(q+1)$, and $n_q = q + 1$, so we can take $\alpha_n = 1/n$ and apply Section 3.7 instead.

BIBLIOGRAPHY

[1] George E. Andrews. *Number Theory*. Dover, New York, 1994.

[2] Tom M. Apostol. *Introduction to Analytic Number Theory*. Springer-Verlag, New York–Heidelberg, 1976.

[3] Alina Bucur, Chantal David, Brooke Feigon, and Matilde Lalín. Fluctuations in the number of points on smooth plane curves over finite fields. *Journal of Number Theory*, 130(11):2528–2541, 2010.

[4] Alina Bucur and Kiran S. Kedlaya. The probability that a complete intersection is smooth. *J. Théor. Nombres Bordeaux*, 24(3):541–556, 2012.

[5] N. G. de Bruijn. *Asymptotic Methods in Analysis*. North-Holland Publishing Co., Amsterdam, 2nd edition, 1961.

[6] W. K. Hayman. A generalisation of Stirling's formula. *J. Reine Angew. Math.*, 196:67–95, 1956.

[7] Jerry Hu. The probability that random positive integers are k-wise relatively prime. *International journal of number theory*, 9(5):1263–1271, 2013.

[8] G. J. O. Jameson. *The Prime Number Theorem*. Cambridge University Press, 2003.

[9] Norman L. Johnson, Samuel Kotz, and Adrienne W. Kemp. *Univariate Discrete Distributions*. John Wiley & Sons, New York, 2nd edition, 1992.

[10] Michel Loève. *Probability Theory I*. Springer-Verlag, New York, 4th edition, 1977.

[11] J. E. Nymann and W. J. Leahey. On the probability that integers chosen according to the binomial distribution are relatively prime. *Acta Arithmetica*, 31(3):205–211, 1976.

[12] J. E. Nymann and W. J. Leahey. On the probability that an integer chosen according to the binomial distribution be k-free. *Rocky Mountain Journal of Mathematics*, 7(4):769–774, 1977.

[13] A. M. Odlyzko. Asymptotic enumeration methods. In Ronald L. Graham, Martin Grötschel, and László Lovász, editors, *Handbook of Combinatorics*, volume 2, pages 1063–1229. Elsevier, Amsterdam, 1995.

[14] Bjorn Poonen. Bertini theorems over finite fields. *Annals of Mathematics (2)*, 160(3):1099–1127, 2004.

[15] Yu. V. Prohorov. Asymptotic behavior of the binomial distribution. *Selected translations in mathematical statistics and probability*, 1:87–95, 1961.

[16] J. Sándor, B. Crstici, and Dragoslav S. Mitrinović. *Handbook of Number Theory I.* Kluwer Academic, Dordrecht, 2006.

[17] Sanford Segal. A note on the average order of number-theoretic error terms. *Duke mathematical journal*, 32:279–284, 1965.

[18] László Tóth. The probability that k positive integers are pairwise relatively prime. *Fibonacci Quarterly*, 40(1):13–18, 2002.