Analytic number theory for 0-cycles

BY WEIYAN CHEN
Department of Mathematics, University of Chicago, 5734 S. University Ave., Chicago, IL 60637, USA.
e-mail: chen@math.uchicago.edu, wchen7@uchicago.edu
(Received 12 September 2016; revised 05 April 2017)

Abstract

There is a well-known analogy between integers and polynomials over $\mathbb{F}_q$, and a vast literature on analytic number theory for polynomials. From a geometric point of view, polynomials are equivalent to effective 0-cycles on the affine line. This leads one to ask: Can the analogy between integers and polynomials be extended to 0-cycles on more general varieties? In this paper we study prime factorisation of effective 0-cycles on an arbitrary connected variety $V$ over $\mathbb{F}_q$, emphasizing the analogy between integers and 0-cycles. For example, inspired by the works of Granville and Rhoades, we prove that the prime factors of 0-cycles are typically Poisson distributed.

1. Introduction

Riemann’s zeta function encodes information about how a random integer factors into primes. The aim of this paper is to present concrete examples addressing the following question: what does the zeta function of a variety $V$ tell us about how a random 0-cycle on $V$ factors into “primes”? In this paper, we study prime factorisation of effective 0-cycles on a connected variety $V$ over $\mathbb{F}_q$, emphasising the analogy between integers and 0-cycles. For example, inspired by the works of Granville and Rhoades, we prove that the prime factors of 0-cycles are typically Poisson distributed.

1.1. Prime factorisation of 0-cycles

Let $q$ be a power of a prime number. Fix $V$ to be a geometrically connected variety over $\mathbb{F}_q$. By a “variety” we mean an integral, separated scheme of finite type. We do not require $V$ to be smooth or projective. An effective 0-cycle $C$ on $V$ over $\mathbb{F}_q$ (for brevity we will just call it a “0-cycle” in this paper) is a formal $\mathbb{N}$-linear sum

$$C = n_1P_1 + n_2P_2 + \cdots + n_lP_l,$$

where $n_i \in \mathbb{N}$, and of distinct closed points $P_i$’s on $V$. The degree of $C$ is $\deg(C) := \sum n_i \deg(P_i)$ where $\deg(P_i)$ denotes the degree of the closed point $P_i$. We view equation (1.1) as giving the prime factorisation of 0-cycles written additively, where closed points on $V$ play the role of “primes”. Let $A_n(V)$ denote the set of all 0-cycles on $V$ of degree $n$. Let $B_n(V)$ denote the set of all square-free 0-cycles on $V$, namely, those with each $n_i = 1$ in (1.1).

A 0-cycle on $V$ of degree $n$ can also be thought of as an $\mathbb{F}_q$-point on the $n$th symmetric power $\text{Sym}^n V$. Similarly, a square-free 0-cycle on $V$ of degree $n$ is equivalent to an $\mathbb{F}_q$-point
on the \( n \)th configuration space \( \text{Conf}_n V \). This viewpoint is important for our purposes. See Section 2 below for more discussion.

Let’s consider an example when \( V \) is the affine line \( \mathbb{A}^1 \). There is a natural bijection between closed points on \( \mathbb{A}^1 \) over \( \mathbb{F}_q \) of degree \( n \) and monic irreducible polynomials over \( \mathbb{F}_q \) of degree \( n \). This bijection extends via equation (1·1) to be between 0-cycles on \( \mathbb{A}^1 \) and monic polynomials. Adding two 0-cycles on \( \mathbb{A}^1 \) corresponds to multiplying two polynomials. Therefore, 0-cycles on a variety \( V \) generalise monic polynomials.

Furthermore, the analogy between integers and polynomials over \( \mathbb{F}_q \) can be extended to 0-cycles on a variety \( V \) over \( \mathbb{F}_q \). We summarise the correspondence in Table 1 below.

| Table 1. Integers vs. 0-cycles |
|--------------------------------|
| Positive integers \( x \)      | 0-cycles \( C \) on a variety \( V \) over \( \mathbb{F}_q \) |
| Multiplication                 | Formal addition                                    |
| \( \log x \)                   | \( \deg C \)                                      |
| \( \log(x \cdot y) = \log x + \log y \) | \( \deg(C + D) = \deg C + \deg D \) |
| Integers in \( (e^n, 2e^n) \)  | \( \mathcal{A}_n(V) \)                           |
| Square-free integers in \( (e^n, 2e^n) \) | \( \mathcal{B}_n(V) \)                          |
| Prime numbers                  | Closed points on \( V \)                         |
| Prime factorisation of integers| Prime factorisation of 0-cycles                  |

1.2. Summary of results

Even though integers and 0-cycles are apparently different objects, using the dictionary provided by Table 1 we will be able to translate analytic number theory into the study of 0-cycles. We study asymptotic statistics for the prime factorisation of 0-cycles on a geometrically connected variety \( V \) over \( \mathbb{F}_q \). Our results, to be summarised below, are analogs of classical results in analytic number theory, and also generalise previous works about polynomials over \( \mathbb{F}_q \). Among them, Theorem 4 is the most difficult to prove.

First, we start with the prime number theorem. The classical prime number theorem, proved by Hadamard and de la Vallée–Poussin, says that the probability for a uniformly chosen random integer in \( (e^n, 2e^n) \) to be prime is \( \sim 1/n \) as \( n \to \infty \).

We will give a similar result for 0-cycles with an explicit bound on the error. Though the result is relatively straightforward to prove, we include it here as a first example to illustrate how a theorem about integers would translate into one about 0-cycles using Table 1. Let \( Z(V, t) \) be the zeta function of \( V \) over \( \mathbb{F}_q \) and let \( \tilde{Z}(V, t) := Z(V, t)(1 - q^d t) \). Denote \( \Pi_n(V) := \{ C \in \mathcal{A}_n(V) : C \text{ is a single closed point} \} \).

**Theorem 1** (Prime number theorem for 0-cycles). Suppose \( V \) is a geometrically connected variety over \( \mathbb{F}_q \) of dimension \( d \geq 1 \),

\[
\frac{|\Pi_n(V)|}{|\mathcal{A}_n(V)|} = \frac{1}{n} \frac{1}{\tilde{Z}(V, q^{-d})} + O \left( \frac{1}{nq^{n/2}} \right), \quad \text{as} \ n \to \infty.
\]

The assumption for \( V \) to be geometrically connected implies that \( Z(V, t) \) has a unique pole at \( t = q^{-d} \), and thus \( \tilde{Z}(V, q^{-d}) \) is a well-defined number. See Section 2 below for more details. Theorem 1 in the case \( V = \mathbb{A}^1 \) is a classical and first proved by Gauss.
Analytic number theory for 0-cycles

Theorem 1 gives the asymptotic probability for a 0-cycle to be a “prime”. We further ask: what is the probability for a 0-cycle to be “almost prime” i.e. to factor into a product of large primes? and to be “highly composite”, i.e. to factor into a product of small primes? The answer to the two questions will be described asymptotically by the following two functions \( R_1 \rightarrow R_\geq 0 \) and the Dickman–de Bruijn function \( \rho \). See Section 4.2 below for their definitions. The two functions are important because of the following classical theorems in analytic number theory:

(i) (Buchstab [2]) For any \( u \geq 1 \), let \( \Phi(n, u) \) denote the number of integers \( x \in (e^n, 2e^n) \) with no prime factor smaller than \( x^{1/u} \). As \( n \rightarrow \infty \), we have

\[
\frac{\Phi(n, u)}{e^n} \sim \frac{\omega(u)u}{n}.
\]

(ii) (Dickman [7], with error term proved by Ramaswami [21]) For any \( u \geq 1 \), let \( \Psi(n, u) \) denote the number of integers \( x \in (e^n, 2e^n) \) with no prime factor larger than \( x^{1/u} \). As \( n \rightarrow \infty \), we have

\[
\frac{\Psi(n, u)}{e^n} = \rho(u) + O(1/n).
\]

We now consider the analogs for 0-cycles. For any \( u \geq 1 \), define \( \Phi_V(n, u) \) to be the number of 0-cycles of degree \( n \) on \( V \) containing no closed point of degree smaller than \( n/u \), and \( \Psi_V(n, u) \) to be the number of 0-cycles of degree \( n \) on \( V \) containing no closed point of degree larger than \( n/u \).

**Theorem 2** (No small/large factor). Suppose \( V \) is a geometrically connected variety over \( \mathbb{F}_q \) of dimension \( d \geq 1 \). As \( n \rightarrow \infty \), we have

\[
\frac{\Phi_V(n, u)}{|A_n(V)|} \sim \frac{\omega(u)u}{n}, \quad (1.2)
\]

\[
\frac{\Psi_V(n, u)}{|A_n(V)|} = \rho(u) + O(1/n). \quad (1.3)
\]

Theorem 2 in the case when \( V = \mathbb{A}^1 \) was proved in [3] and [18].

Next, we ask: fix a closed point \( P \), what is the probability for a random 0-cycle \( C \) to contain \( P \), when \( C \) is uniformly chosen in \( A_n(V) \)? More generally, how does the order of \( P \) i.e. the coefficients in (1.1) distribute as \( C \) varies in \( A_n(V) \)?

We first consider the same questions for integers. For a prime number \( p \), the \( p \)-adic order \( \nu_p \) (i.e. the order of \( p \) in the prime factorisation) can be viewed as a random variable on \( \mathbb{Z} \cap (e^n, 2e^n) \). A straightforward calculation gives the asymptotic distribution of \( \nu_p \) for a uniform integers, or square-free integers, in \( \mathbb{Z} \cap (e^n, 2e^n) \) as \( n \rightarrow \infty \):

(i) \( \operatorname{Prob}(\nu_p(x) = j : x \in (e^n, 2e^n)) \rightarrow p^{-j}(1 - p^{-1}) \), geometric distribution;

(ii) \( \operatorname{Prob}(\nu_p(x) = 1 : \text{square-free } x \in (e^n, 2e^n)) \rightarrow (p + 1)^{-1} \), Bernoulli distribution;

(iii) for all primes \( p \), the random variables \( \nu_p \) converge to mutually independent random variables on \( \mathbb{Z} \cap (e^n, 2e^n) \), or on square-free integers in \( (e^n, 2e^n) \).

We now consider the analogs for 0-cycles. For a closed point \( P \) on \( V \) of degree \( k \) and a 0-cycle \( C \) on \( V \), define \( \nu_P(C) \) to be the order of \( P \) in the prime factorisation of \( C \) as in (1.1). Equip \( A_n(V) \) and \( B_n(V) \) with the uniform probability measure.
Theorem 3 (Asymptotic distribution of prime orders in 0-cycles). Suppose $V$ is a geometrically connected variety over $\mathbb{F}_q$ of dimension $d \geq 1$.

(i) The random variable $\nu_P$ on $A_n(V)$ converges to a geometric distribution as $n \to \infty$. Precisely, there exists a constant $b$ depending only on $V$ such that for any natural number $j$, we have

$$\text{Prob}(\nu_P(C) = j : C \in A_n(V)) = \left(\frac{1}{q^{dk}}\right)^j \left(1 - \frac{1}{q^{dk}}\right) + O\left(\frac{n^b}{q^n}\right).$$

(ii) The random variable $\nu_P$ restricted to $B_n(V)$ converges to a Bernoulli distribution as $n \to \infty$. Precisely, we have

$$\text{Prob}(\nu_P(C) = 1 : C \in B_n(V)) = \frac{1}{q^{dk} + 1} + O\left(\frac{1}{q^{n/2}}\right).$$

(iii) For all closed points $P$ on $V$, the random variables $\nu_P$ converge to mutually independent random variables on $A_n(V)$ or on $B_n(V)$ as $n \to \infty$.

Theorem 3 in the case $V = \mathbb{A}^1$ was proved by Arratia–Barbour–Tavaré [1, theorem 3.1]. Theorem 3 in the case when $V$ is the affine or the projective space can also be deduced from a theorem of Poonen [19, theorem 1.1]. Recently, Farb–Wolfson and the author independently generalised a theorem of Church–Ellenberg–Farb [5] about asymptotic arithmetic statistics on $\text{Conf}^n\mathbb{A}^1$ to that on $\text{Conf}^n V$ for $V$ a smooth variety (see [11, theorem B] and [4, corollary 4]). Theorem 3 gives a probabilistic interpretation and a new proof of this generalisation, and removes the assumption for $V$ to be smooth. See Section 3.4 below for more details.

Remark 1 (Erdős–Kac’s heuristic). Erdős and Kac made the following brilliant observation. Let $\Omega(n)$ denote the total number of prime factors of an integer $x \in (e^n, 2e^n)$, counted with multiplicities. Then $\Omega(x) = \sum_p \nu_p(x)$, summing over all prime numbers $p$. Since $\nu_p$’s converge to independent random variables as $n \to \infty$, heuristically $\Omega$ is a sum of independent random variables in the limit. By the Central Limit Theorem, one should expect $\Omega$ to converge to the normal distribution as $n \to \infty$. This observation leads Erdős and Kac to prove their celebrated theorem in [8] which roughly says that when $n$ is large, $\Omega$ on $\mathbb{Z}\cap(e^n, 2e^n)$ is approximately normally distributed with mean and variance $\log n$. Erdős–Kac theorem was originally about $\omega$, the number of distinct prime factors. But the same heuristic applies and the same result holds for $\Omega$.

Theorem 3 tells us that the exact same heuristic will also apply to 0-cycles! For a 0-cycle $C$, define $\Omega(C)$ to be the total number of closed points in $C$ counted with multiplicities. Then we have

$$\Omega(C) = \sum_{P \in V^{cl}} \nu_P(C),$$

where $V^{cl}$ is the set of all closed points of $V$. By Theorem 3 (iii), the sequence $(\nu_P)_{P \in V^{cl}}$ converges to a sequence of independent random variables as $n \to \infty$. As before, one should expect that $\Omega$ on $A_n(V)$ would be approximately normally distributed with mean and variance $\log n$ as $n \to \infty$. This heuristic is confirmed by a theorem of Liu [16, corollary 2].
Erdős-Kac’s heuristic and Liu’s theorem imply that on average, a 0-cycle $C$ would contain $\sim \log \deg C$ many closed points. Thus, for $C$ with prime factorisation $C = n_1 p_1 + \cdots n_i p_i$, 

$$\phi(C) := \{ \log \deg p_1, \log \deg p_2, \ldots, \log \deg p_i \}$$

is typically a collection of $\sim \log \deg C$ many real numbers in the interval $[0, \log \deg C]$. How should we expect $\phi(C)$ to distribute on the interval $[0, \log \deg C]$?

We first consider the same question for integers. Granville [12, theorem 1] proved that for almost all integers $x$, the sets of numbers 

$$\phi(x) := \{ \log(\log p) : p | x \}$$

are close to being “random” i.e. Poisson distributed. A sequence of finite sets $S_1, S_2, \ldots$ is said to be Poisson distributed (see [12]) if there exist functions $m_j, K_j, L_j \to \infty$ monotonically as $j \to \infty$ such that $S_j \subset [0, m_j]$ and $|S_j| \sim m_j$, and for all $L \in [1/L_j, L_j]$ and all integer $k \in [0, K_j]$, we have 

$$\Prob\left(t \in [0, m_j] : |S_j \cap [t, t + L]| = k\right) \sim e^{-L} \frac{L^k}{k!},$$

where $\Prob$ stands for probability with respect to the Lebesgue measure on the real line. For example, if $S_j$ is a set of $j$ real numbers chosen uniformly and independently in the interval $[0, j]$, then the sequence $S_j$ is almost surely Poisson distributed.

We prove the following analog of Granville’s theorem for 0-cycles.

**Theorem 4 (Prime factors in 0-cycles are Poisson distributed).** Suppose $V$ is a geometrically connected variety over $\mathbb{F}_q$ of dimension $d \geq 1$. The sets $\phi(C)$ are approximately Poisson distributed for almost all 0-cycle $C$ in $\mathcal{A}_n(V)$ as $n \to \infty$.

More precisely, there exist functions $K(n), L(n) \to \infty$ monotonically as $n \to \infty$ such that for any $\epsilon > 0$, for any $n$ sufficiently large depending on $\epsilon$, for all $L \in [1/L(n), L(n)]$ and all integer $k \leq K(n)$, for at least $(1 - \epsilon)|\mathcal{A}_n(V)|$ many 0-cycles $C$ in $\mathcal{A}_n(V)$, we have

$$(1 - \epsilon)e^{-L} \frac{L^k}{k!} \leq \Prob\left(t \in [0, \log n] : |\phi(C) \cap [t, t + L]| = k\right) \leq (1 + \epsilon)e^{-L} \frac{L^k}{k!}.$$

**Remark 2 (Related work).** Theorem 4 in the case when $V = \mathbb{A}^1$ was first proved by Rhoades [22, theorem 1-3]. Following the theme that integers and permutations should have similar statistical behaviors, Granville proved that the cycle lengths of permutations are also typically Poisson [14, theorem 1]. See Granville’s excellent survey [13] for more on the anatomy of integers and permutations. Our proof of Theorem 4 uses ideas from both Rhoades’ and Granville’s works.

**Remark 3 (Proof methods).** The key ingredient in the proofs of all the results above comes from the Riemann Hypothesis over finite fields, famously proved by Deligne. In addition, to prove Theorem 2, we use general results about decomposable combinatorial structures proved in [3] and [18]. In the proof of Theorem 4, we establish a comparison lemma (Lemma 16 below) relating statistics about permutations and about 0-cycles, and then use Granville’s theorem in [14] about cycle lengths in permutations.

2. Symmetric powers, Zeta function and the Weil conjectures

In this section we recall a version of Weil conjectures for $V$ not necessarily smooth or projective. All results presented in this section are previously known.
The zeta function of $V$ over $\mathbb{F}_q$ is
\[ Z(V, t) := \exp \left( \sum_{k=1}^{\infty} \frac{|V(\mathbb{F}_{q^k})|}{k} t^k \right). \] (2.1)

**THEOREM 5** (Dwork, Grothendieck and Deligne). Suppose $V$ is a geometrically connected variety over $\mathbb{F}_q$ of dimension $d \geq 1$.

(i) There exist polynomials $P_i(t)$ for $i = 0, \ldots, 2d$ such that
\[ Z(V, t) = \frac{P_1(t) \cdots P_{2d-1}(t)}{P_0(t) \cdots P_{2d}(t)}, \]
where $P_{2d}(t) = 1 - q^d t$.

(ii) For each $i$, for each $\alpha$ such that $P_i(\alpha) = 0$, there exists some $j \leq i$ such that $|\alpha| = q^{-j/2}$. It is possible that $j$ depends on $\alpha$.

When $V$ is smooth and projective, Theorem 5 is a part of the Weil conjectures, originally formulated by Weil [23]. In this case, the equality $j = i$ will be achieved for all $\alpha$ in (ii).

Part (ii) is due to Deligne (see [6, théorème I (3.3.1)]) and are often called the “Riemann Hypothesis over finite fields”; it will be especially important for our purposes. Theorem 5 has the following consequence:

**COROLLARY 6.** Suppose $V$ is a geometrically connected variety over $\mathbb{F}_q$ of dimension $d \geq 1$. We have
\[ \frac{|V(\mathbb{F}_{q^n})|}{q^{nd}} = 1 + O \left( \frac{1}{q^{n/2}} \right), \quad \text{as } n \to \infty. \] (2.2)

Corollary 6 in the case when $V$ is a quasi-projective variety was first proved by Lang–Weil [17, theorem 1], before Theorem 5 was proved.

The $n$th symmetric power of a variety $V$ is the quotient $\text{Sym}^n V := V^n/S_n$, where the symmetric group $S_n$ acts on $V^n$ by permuting the coordinates. $\text{Sym}^n V$ is also a variety over $\mathbb{F}_q$ (see [20, page 66]). The zeta function $Z(V, t)$ satisfies the following equation:
\[ Z(V, t) = 1 + \sum_{n=1}^{\infty} |\text{Sym}^n V(\mathbb{F}_q)| t^n, \] (2.3)
where $\text{Sym}^n V(\mathbb{F}_q)$ is the set of $\mathbb{F}_q$-points on $\text{Sym}^n V$. An $\mathbb{F}_q$-point in $\text{Sym}^n V$ is a 0-dimensional subvariety of $V$ of degree $n$ defined over $\mathbb{F}_q$, which is equivalently a multiset $\{x_1, \ldots, x_n\}$ of possibly repeated points in $V(\mathbb{F}_q)$ such that the action of Frobenius on $V(\mathbb{F}_q)$ preserves the multiset. Thus, $\{x_1, \ldots, x_n\}$ decomposes into a union of orbits of Frobenius, possibly with repetition. Note that there is a natural bijection between orbits of Frobenius on $V(\mathbb{F}_q)$ of size $k$ and closed points on $V$ of degree $k$. This bijection extends via equation (1.1) to a bijection between $\mathbb{F}_q$-points on $\text{Sym}^n V$ and 0-cycles on $V$ of degree $n$ over $\mathbb{F}_q$. Therefore, we have $\text{Sym}^n V(\mathbb{F}_q) \cong A_n(V)$. Similarly, the $n$th configuration space of $V$ is defined to be
\[ \text{Conf}^n V := \{ (x_1, \ldots, x_n) \in V^n : x_i \neq x_j, \forall i \neq j \}/S_n, \]
where $S_n$ also acts on permuting the coordinates. $\text{Conf}^n V$ is a subvariety of $\text{Sym}^n V$. There is a bijection between $\text{Conf}^n V(\mathbb{F}_q)$ and $B_n(V)$. 
If we adopt the convention that \(|A_0(V)| = |B_0(V)| = 1\) (the only 0-cycle of degree 0 is the empty one), then we have
\[
\sum_{n=0}^{\infty} |A_n(V)| t^n = Z(V, t) \quad (2.4)
\]
\[
\sum_{n=0}^{\infty} |B_n(V)| t^n = \frac{Z(V, t)}{Z(V, t^2)} \quad (2.5)
\]
The later equation follows from the fact that every 0-cycle \(C\) can be written uniquely as a sum \(C = 2A + B\) where \(B\) is square-free.

3. Prime number theorem and asymptotic distribution of prime orders

In this section, we prove Theorem 1 and Theorem 3 stated in the Introduction.

3.1. Proof of Theorem 1

We will first proved two lemmas estimating the sizes of \(A_n(V)\) and \(\Pi_n(V)\), respectively.

**Lemma 7.** Suppose \(V\) is a geometrically connected variety over \(\mathbb{F}_q\) of dimension \(d \geq 1\). There exists a constant \(b\) depending only on \(V\) such that
\[
\frac{|A_n(V)|}{q^{nd}} = \tilde{Z}(V, q^{-d}) + O \left( \frac{n^b}{q^n} \right) \quad (3.1)
\]
Recall that \(\tilde{Z}(V, t) := Z(V, t)(1 - t^{-d})\). Theorem 5 implies that \(\tilde{Z}(V, t)\) is a rational function in \(t\) with no pole in the disk \(|z| < q^{-\frac{2d-1}{2}} = q^{-(d-1)}\). In particular, \(\tilde{Z}(V, t)\) converges at \(t = q^{-d}\). We decompose \(Z(V, t)\) into the following sum:
\[
Z(V, t) = \frac{\tilde{Z}(V, q^{-d})}{1 - q^{-d}t} + \frac{\tilde{Z}(V, t) - \tilde{Z}(V, q^{-d})}{1 - q^{-d}t} \quad (3.2)
\]
The dominating term in (3.2), which is a geometric series, tells that \(|A_n(V)|\) grows like \(\tilde{Z}(V, q^{-d})q^{nd}\), contributing to the first summand in (3.1). The remainder in (3.2) is a rational function in \(t\) with no pole in the disk \(|z| < q^{-\frac{2d-1}{2}} = q^{-(d-1)}\). Thus, its \(n\)th Taylor coefficient grows like \(O(n^b q^{(d-1)})\) where \(b\) is the number of poles with norm \(q^{-(d-1)}\) (see [9, theorem IV.9]), which after normalisation contributes to the error term in (3.1). This completes the proof of Lemma 7.

**Remark 4** (The constant \(b\)). In general, the poles of \(Z(V, t)\) are determined by the compactly supported étale cohomology of \(V\). In the proof, the constant \(b\) is equal to the number of poles of \(Z(V, t)\) with norm \(q^{-(d-1)}\), which further depends on the compactly supported étale cohomology of \(V\) in dimension \(2d - 2\).

**Lemma 8.** Suppose \(V\) is a geometrically connected variety over \(\mathbb{F}_q\) of dimension \(d\), then
\[
\frac{|\Pi_n(V)|}{q^{nd}} = \frac{1}{n} + O \left( \frac{1}{nq^{n/2}} \right) \quad (3.3)
\]
**Proof.** Each \(\mathbb{F}_q\)-point on \(V\) comes from a closed point on \(V\) of degree \(k\) for some \(k|n\). Thus,
\[
|V(\mathbb{F}_q)| = \sum_{k|n} k|\Pi_k(V)|.
\]
Let $\mu$ be the Möbius function. Applying Möbius inversion, we obtain

$$|\Pi_n(V)| = \frac{1}{n} \sum_{k|n} \mu(n/k)|V(\mathbb{F}_q)|.$$  \hspace{1cm} (3.3)

This formula together with Corollary 6 establishes Lemma 8.

Theorem 1 follows by taking the quotient of $|\mathcal{A}_n(\mathcal{V})|$ and $|\Pi_n(V)|$, which were estimated in Lemma 7 and Lemma 8, respectively.

3.2. Proof of Theorem 3

Let $P$ be a closed point of $\mathcal{V}$ of degree $k$.

(i) $\nu_P$ on $\mathcal{A}_n(\mathcal{V})$. For any $\mathcal{C} \in \mathcal{A}_n(\mathcal{V})$ and any natural number $j$,

$$\nu_P(\mathcal{C}) \geq j \iff \mathcal{C} = jP + \mathcal{C}' \text{ for some } \mathcal{C}' \in \text{Sym}^{n-jk}V(\mathbb{F}_q).$$

Therefore, we have

$$\text{Prob}(\nu_P \geq j : \mathcal{A}_n(\mathcal{V})) = \frac{|\mathcal{A}_{n-jk}(\mathcal{V})|}{|\mathcal{A}_n(\mathcal{V})|} = \frac{1}{q^{jk}d} + O\left(\frac{n^b}{q^n}\right), \quad \text{by Lemma 7.}$$

Part (i) is established by taking

$$\text{Prob}\left(\nu_P = j : \mathcal{A}_n(\mathcal{V})\right) = \text{Prob}(\nu_P \geq j : \mathcal{A}_n(\mathcal{V})) - \text{Prob}(\nu_P \geq j + 1 : \mathcal{A}_n(\mathcal{V})).$$

(ii) $\nu_P$ on $\mathcal{B}_n(\mathcal{V})$. We first prove a lemma bounding the size of $|\mathcal{B}_n(\mathcal{V})|$.

**Lemma 9.** If $\mathcal{V}$ is a geometrically connected variety over $\mathbb{F}_q$ of dimension $d \geq 1$, then

$$\frac{|\mathcal{B}_n(\mathcal{V})|}{q^{nd}} = \frac{Z(\mathcal{V}, q^{-d})}{Z(\mathcal{V}, q^{-2d})} + O(q^{-n/2}), \quad \text{as } n \to \infty. \hspace{1cm} (3.4)$$

**Proof.** Similarly as in the proof of Lemma 7, we separate the generating function for $|\mathcal{B}_n(\mathcal{V})|$, calculated in equation (2.5), as:

$$\frac{Z(\mathcal{V}, t)}{Z(\mathcal{V}, t^2)} = \frac{1}{1 - q^dt} \frac{\hat{Z}(\mathcal{V}, q^{-d})}{\hat{Z}(\mathcal{V}, q^{-2d})} + \frac{1}{1 - q^dt} \left[ \hat{Z}(\mathcal{V}, t) - \frac{\hat{Z}(\mathcal{V}, q^{-d})}{\hat{Z}(\mathcal{V}, q^{-2d})} \right]. \hspace{1cm} (3.5)$$

The dominating term in (3.5) implies that $|\mathcal{B}_n(\mathcal{V})| \sim \hat{Z}(\mathcal{V}, q^{-d})q^{nd}/Z(\mathcal{V}, q^{-2d})$. The error is controlled by the smallest possible absolute value of poles of $R(t)$, which by Theorem 5 (i) is $q^{-(2d-1)/4}$ if $d = 1$, and is $q^{-(2d-2)/2}$ if $d \geq 2$. Hence, by the same argument as the proof of Lemma 7, we have

- if $d = 1$, then
  $$\frac{|\mathcal{B}_n(\mathcal{V})|}{q^n} = \frac{Z(\mathcal{V}, q^{-1})}{Z(\mathcal{V}, q^{-2})} + O\left(\frac{n^a}{q^{3n/4}}\right), \quad \text{for some constant } a;$$

- if $d \geq 2$, then
  $$\frac{|\mathcal{B}_n(\mathcal{V})|}{q^{nd}} = \frac{\hat{Z}(\mathcal{V}, q^{-d})}{Z(\mathcal{V}, q^{-2d})} + O\left(\frac{n^b}{q^n}\right), \quad \text{for some constant } b.$$

In either case, (3.4) holds.
In particular, Lemma 9 implies that when $m \to \infty$ and $n \to \infty$ with $n \geq m$,

$$\frac{|B_n(V)|}{|B_n(V)|} = q^{-(n-m)d} + q^{-(n-m)(d-1/2)}O(q^{-n/2}), \quad (3.6)$$

where the implied constant is independent of $n$ and $m$.

For each $n$, define a subset $B^p_n(V) := \{C \in B_n(V) : \nu_p(C) = 1\}$. We have a bijection:

$$B_{n-k}(V) \setminus B^p_{n-k}(V) \to B^p_n(V)$$

$$C' \mapsto C' + P.$$

The bijection gives the following equations:

$$|B^p_n(V)| = |B_{n-k}(V)| - |B^p_{n-k}(V)|$$

$$= |B_{n-k}(V)| - |B_{n-2k}(V)| + |B_{n-3k}(V)| - |B_{n-4k}(V)| + \cdots$$

Therefore, we have:

$$\text{Prob}(\nu_p = 1 : B_n(V)) = \frac{|B^p_n(V)|}{|B_n(V)|}$$

$$= \left[ \sum_{i=1}^{\lfloor n/2k \rfloor} (1)^{i+1} \frac{|B_{n-k}(V)|}{|B_n(V)|} \right] + O \left( \frac{|B^p_{n-(\lfloor n/2k \rfloor)}(V)|}{|B_n(V)|} \right)$$

$$= \sum_{i=1}^{\lfloor n/2k \rfloor} (1)^{i+1} \left[ q^{-ikd} + q^{-(ik-1/2)d}O(q^{-n/2}) \right] + O(q^{-nd/2}) \quad \text{by (3.6)}$$

$$= \sum_{i=1}^{\lfloor n/2k \rfloor} (1)^{i+1} q^{-kd} + \left[ \sum_{i=1}^{\lfloor n/2k \rfloor} (1)^{i+1} q^{-(ik-1/2)d} \right] \cdot O(q^{-n/2}) + O(q^{-nd/2})$$

$$= q^{-kd} \cdot \frac{1 + O(q^{-nd/2})}{1 + q^{-kd}} + O(q^{-n/2}) + O(q^{-nd/2})$$

$$= \frac{1}{q^{kd} + 1} + O(q^{-n/2}) \quad \text{since } d \geq 1.$$

(iii) Independence. To prove that $\nu_P$ are mutually independent as $n \to \infty$, it suffices to check that for any finite collection of distinct closed points $P_1, \ldots, P_m$ on $V$ of degree $\deg(P_i) = r_i$ for each $i$, and for any sequence of natural numbers $k_1, \ldots, k_m$, and for any $n \geq \sum_{i=1}^{m} r_i$, we have

$$\prod_{i=1}^{m} \text{Prob}(\nu_{P_i} \geq k_i : A_n(V)) = \text{Prob}(\nu_{P_i} \geq k_i, \forall 0 \leq i \leq m : A_n(V)) + O(n^b q^{-n}). \quad (3.7)$$

By the same argument as in the proof of (i), we have for each $i$,

$$\text{Prob}(\nu_{P_i} \geq k_i : A_n(V)) = \frac{|A_{n-r_i}(V)|}{|A_n(V)|} = q^{-r_i d} + O(n^b q^{-n}). \quad (3.8)$$

Similarly, if we let $h$ abbreviate $\sum_{i=1}^{m} r_i$, then when $n \geq h$, we have

$$\text{Prob}(\nu_{P_i} \geq k_i, \forall 0 \leq i \leq m : A_n(V)) = \frac{|A_{n-h}(V)|}{|A_n(V)|} = q^{-hd} + O(n^b q^{-n}). \quad (3.9)$$

Equation (3.7) follows by applying equations (3.8) and (3.9) to the two sides, respectively.

One can prove a similar equation as (3.7) with $A_n(V)$ replaced by $B_n(V)$, using a similar argument but with the estimate in (3.6).
3-3. 0-cycles, permutations, and integer partitions

In this section, we discuss the connections among 0-cycles, permutations, and partitions of an integer. These viewpoints will be useful for the later sections.

The prime factorisation of a 0-cycle \( C \in \mathcal{A}_n(V) \) into a sum of closed points (possibly with repetition) \( C = P_1 + \cdots + P_l \) gives a partition \( \lambda_C \) of the integer \( n \) by

\[
\lambda_C : n = \deg(P_1) + \cdots + \deg(P_l).
\]  

Similarly, the decomposition of a permutation \( \sigma \in S_n \) into a product of disjoint cycles \( \sigma = c_1 \cdot c_2 \cdots c_l \) gives a partition \( \lambda_\sigma \) of the integer \( n \) by

\[
\lambda_\sigma : n = |c_1| + \cdots + |c_l|,
\]

where \(|c_i|\) stands for the order of the cycle \( c_i \). Furthermore, \( \lambda_\sigma \) completely determines the conjugacy class of \( \sigma \). Thus, partitions of \( n \) parametrise both permutations and 0-cycles as in the following diagram:

\[
\begin{array}{ccc}
S_n & \cong & \{ \text{conjugacy classes in } S_n \} \\
\mathcal{A}_n(V) & \longrightarrow & \{ \text{partitions of } n \}.
\end{array}
\]

Hence, every class function \( \chi : S_n \to \mathbb{Q} \) can be evaluated at partitions of \( n \), and thus induces a map \( \mathcal{A}_n(V) \to \mathbb{Q} \) via \( C \mapsto \chi(\lambda_C) \). To simplify notation, we will use \( \chi(C) \) to abbreviate \( \chi(\lambda_C) \) and use the same \( \chi \) to denote the induced map on \( \mathcal{A}_n(V) \). What we mean will be clear from context.

Note that if \( C \in \mathcal{B}_n(V) \) is square-free, then there is a natural conjugacy class of \( S_n \) associated to \( C \) coming from permutation induced by the action of Frobenius on \( C \). The partition associated to this conjugacy class is precisely \( \lambda_C \).

3-4. Statistics weighted by character polynomials

In this section, we discuss a consequence of Theorem 3 which is related to recent works of [5] and [11] on representation stability and arithmetic statistics.

For each positive integer \( k \), define a function

\[
X_k : S_n \to \mathbb{N}
\]

\[
X_k(\sigma) := \text{the number of cycles of order } k \text{ in the cycle decomposition of } \sigma \in S_n.
\]

A character polynomial is a polynomial \( P \in \mathbb{Q}[X_1, X_2, \ldots] \). It defines a class function on \( S_n \) for all \( n \), and hence, by Section 3-3, induces a function on \( \mathcal{A}_n(V) \) for all \( n \). We view \( P \) as a random variable on \( \mathcal{A}_n(V) \) and on \( \mathcal{B}_n(V) \), both under the uniform probability measure.

For any finite sequence of nonnegative integers \( \lambda = (\lambda_1, \ldots, \lambda_l) \), define a character polynomial:

\[
\binom{X}{\lambda} := \prod_{k=1}^{l} \binom{X_k}{\lambda_k}.
\]

Character polynomials of the form \( \binom{X}{\lambda} \) give a basis for the vector space \( \mathbb{Q}[X_1, X_2, \ldots] \). The following results give explicit formulas for the expected values of the basis character polynomial \( \binom{X}{\lambda} \) on \( \mathcal{A}_n(V) \) and on \( \mathcal{B}_n(V) \) asymptotically as \( n \to \infty \).
COROLLARY 10. Suppose \( V \) is a geometrically connected variety over \( \mathbb{F}_q \) of dimension \( d \geq 1 \). As before, let \(|\pi_n(V)|\) for each \( n \) be as in Theorem 1. Let both \( A_n(V) \) and \( B_n(V) \) have the uniform probability measure. Let \( \mathbb{E}[\chi; S] \) denote the expected value of a random variable \( \chi \) on the finite set \( S \) under the uniform probability measure. For any finite sequence of nonnegative integers \( \lambda = (\lambda_1, \ldots, \lambda_l) \), we have

\[
\lim_{n \to \infty} \mathbb{E}\left[\left(\binom{X}{\lambda}\right); A_n(V)\right] = \prod_{k=1}^{l} \left(\frac{|\pi_k(V)| + \lambda_k - 1}{\lambda_k}\right) \frac{1}{(q^{kd} - 1)^{\lambda_k}} \quad (3.14)
\]

\[
\lim_{n \to \infty} \mathbb{E}\left[\left(\binom{X}{\lambda}\right); B_n(V)\right] = \prod_{k=1}^{l} \left(\frac{|\pi_k(V)|}{\lambda_k}\right) \frac{1}{(q^{kd} + 1)^{\lambda_k}} \quad (3.15)
\]

In particular, the limits on the left-hand side exist.

**Proof.** We first prove (3.14). By the definition of \( X_k(C) \), we have

\[
X_k(C) = \text{the number of closed points in } C \text{ of degree } k, \text{ counted with multiplicities}
\]

\[
= \sum_{P \in V^{cl}; \deg P = k} \nu_P(C),
\]

where \( \nu_P \) is as in Theorem 3 and the sum is over all closed points \( P \) on \( V \) of degree \( k \). Theorem 3 says that each \( \nu_P \) on \( A_n(V) \) converges in probability to mutually independent and identically distributed (i.i.d.) geometric random variables. Thus, \( X_k \) on \( A_n(V) \) converges in probability and consequently also in distribution to a sum of \(|\pi_k(V)|\)-many i.i.d geometric random variables, which is precisely the negative binomial distribution. The right-hand side of (3.14) is exactly the factorial moments of the negative binomial.

The proof of (3.15) is completely the same, if we replace “geometric” by “Bernoulli”, and replace “negative binomial” by “binomial” in the proof above.

In [5], Church–Ellenberg–Farb related a stability phenomenon in representation theory, which they called “representation stability”, to the convergence of various statistics on algebraic varieties over finite fields. Part of Theorem 1 in [5] says that for any character polynomial \( P \), the following limit

\[
\lim_{n \to \infty} \mathbb{E}[P; B_n(A^1)]
\]

always exists. Since every character polynomial \( P \) can be written as a linear combination of polynomials of the form \( \binom{X}{\lambda} \), our Corollary 10 in particular implies that \( \lim_{n \to \infty} \mathbb{E}[P; B_n(V)] \) converges for any character polynomial \( P \), and thus generalises their result from \( A^1 \) to any geometrically connected variety \( V \) of positive dimension. Similar generalisation with an additional assumption for \( V \) to be smooth was also proved by Farb–Wolfson [11, theorem C] using the stability of étale cohomology of Conf\( n \) \( V \) with twisted coefficients, and by Chen [4, corollary 4] using the zeta function of \( V \). Corollary 10 gives a probabilistic interpretation of the limit, and furthermore removes the assumption for \( V \) to be smooth (as was needed in [11] and [4]).

4. 0-cycles as decomposable combinatorial structures

In this section we prove Theorem 2 using the general axiomatic results from the theory of decomposable combinatorial structures in [3] and [18].
4.1. Abstract decomposable combinatorial structures

Consider the following general set-up. Let $\mathcal{P}$ be a disjoint union $\bigcup_{n=1}^{\infty} \mathcal{P}_n$ where each $\mathcal{P}_n$ is a finite set. An element in $\mathcal{P}_n$ is said to have “degree” $n$. Define $\mathcal{C}$ to be the set of all finite multisets of elements in $\mathcal{P}$. The degree of each multiset is defined to be the sum of the degrees of its elements, summing with multiplicities. Write $\mathcal{C} = \bigcup_{n=1}^{\infty} \mathcal{C}_n$ as disjoint unions according to the degrees. The triple $(\mathcal{P}, \mathcal{C}, \text{degree})$ is called a decomposable combinatorial structure (see §10, introduction). Objects in $\mathcal{P}$ can be viewed as “primes”. Objects in $\mathcal{C}$ can be viewed as “composites”. Define the following generating functions:

$$P(t) := 1 + \sum_{n=1}^{\infty} |\mathcal{P}_n| t^n,$$
$$C(t) := 1 + \sum_{n=1}^{\infty} |\mathcal{C}_n| t^n. \quad (4.1)$$

See §10 for many examples of decomposable combinatorial structures that arise naturally in different areas of mathematics. In this paper, we will focus on the following example.

**Example 1 (0-cycles as decomposable combinatorial structures).** For each $n$, let $\mathcal{P}_n := \Pi_n(V)$ as in Theorem 1 and let $\mathcal{C}_n := A_n(V)$. Then the prime factorisation of 0-cycles in (1.1) says that $(\mathcal{C}, \mathcal{P}, \text{deg})$ is a decomposable combinatorial structure. In this case, $C(t)$ is precisely the zeta function $Z(V, t)$ of the variety $V$.

Therefore, we can apply general results about decomposable combinatorial structures to study 0-cycles.

4.2. Proof of Theorem 2

First, we state the definitions of the Buchstab and the Dickman–de Bruijn functions.

**Definition 1.** The Buchstab function $\omega : \mathbb{R}_{\geq 1} \to \mathbb{R}_{\geq 0}$ is the unique continuous function satisfying the differential-difference equations:

$$\omega(u) = 1/u, \quad 1 \leq u \leq 2,$$
$$\omega(u) + u\omega'(u) = \omega(u - 1), \quad u \geq 2.$$

The Dickman–de Bruijn function $\rho : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is the unique continuous function satisfying the differential-difference equations:

$$\rho(u) = 1 \quad 0 \leq u \leq 1,$$
$$u\rho'(u) + \rho(u - 1) = 0 \quad u \geq 2.$$

Theorem 2 will be a consequence of Lemma 7 and Lemma 8 together with the following general theorems about decomposable combinatorial structures. Given a decomposable combinatorial structure $(\mathcal{C}, \mathcal{P}, \text{deg})$ as in the previous section, define

$$X(n,m) := |\{c \in \mathcal{C}_n : c \text{ contains no prime of degree smaller than } m\}|,$$
$$Y(n,m) := |\{c \in \mathcal{C}_n : c \text{ contains no prime of degree larger than } m\}|.$$
Theorem 11 (Bender–Mashatan–Panario–Richmond, Omar–Panario–Richmond–Whitely). Suppose $(\mathcal{C}, \mathcal{P}, \deg)$ is a decomposable combinatorial structure such that there exist constants $K$ and $R$ satisfying
\begin{equation}
|\mathcal{P}_n| \sim \frac{1}{n} R^n \quad \text{and} \quad |\mathcal{C}_n| \sim K R^n \quad \text{as } n \to \infty. \tag{4.2}
\end{equation}

(i) [3, theorem 1.1]. For any $\epsilon > 0$, and any $m, n$ with $\epsilon \leq m/n \leq 1$,
\[
\frac{X(n, m)}{|\mathcal{P}_n|} \sim \frac{n \omega(m/n)}{m}.
\]

(ii) [18, theorem 1]. For any $\epsilon > 0$ and any $m, n$ with $\epsilon \leq m/n \leq 1$,
\[
\frac{Y(n, m)}{|\mathcal{C}_n|} = \rho(n/m) + O(1/m).
\]

We apply Theorem 11 to our case when $\mathcal{P}_n = \Pi_n(V)$ and $\mathcal{C}_n = A_n(V)$ as in Example 1. As $n \to \infty$,
\[
|\Pi_n(V)| \sim \frac{q^{d_u}}{n}, \quad \text{by Lemma 8},
\]
\[
|A_n(V)| \sim \tilde{Z}(V, q^{-d})q^{nd}, \quad \text{by Lemma 7}.
\]

Thus, conditions (4.2) are satisfied. Theorem 11 then implies that for any $u \geq 1$, as $n \to \infty$,
\[
\Phi_V(n, u) = \frac{X(n, n/u)|\Pi_n(V)|}{|A_n(V)|} \sim \frac{n \omega(u)}{n/u} \cdot \frac{1}{n} = \frac{u \omega(u)}{n},
\]
\[
\Psi_V(n, u) = \frac{Y(n, n/u)|\mathcal{C}_n|}{|A_n(V)|} = \rho(u) + O(1/n).
\]

5. Prime factors of 0-cycles are Poisson distributed

In this section we prove Theorem 4 by proving the following quantitative statement:

Theorem 12. Suppose $V$ is a geometrically connected variety over $\mathbb{F}_q$, of dimension $d \geq 1$. For every $n$ large enough, let $y := \log \log n/(\log \log \log n)^2$. There exists a subset $\Sigma_n \subset A_n(V)$ with $|\Sigma_n| \leq |A_n(V)| 2^{-y/7}$ such that for every $C \in A_n(V) \setminus \Sigma_n$, for every $L \in [1/y, y/20]$, and for every $r \leq y(\log y)^{-2}$,
\begin{equation}
\frac{1}{\log n} \nu\left( \left\{ t \in [0, \log n] : \left| \phi(C) \cap [t, t + L] \right| = k \right\} \right) = e^{-L} \frac{L'}{r!} \left[ 1 + O\left( \frac{1}{2^{y/15}} \right) \right], \tag{5.1}
\end{equation}
where $\nu$ denotes the Lebesgue measure and $\phi(C)$ is as in Theorem 4.

Proof. We will prove Theorem 12 in three steps: first, we prove a general lemma comparing statistics about 0-cycles and about permutations; second, we apply the comparison lemma to a theorem of Granville about permutations, and obtain an estimate for the left-hand side of (5.1); finally, we construct the set $\Sigma_n \subset A_n(V)$, following an argument due to Rhoades [22]. The key step in the proof is to establish Lemma 16.

Step 1. Compare permutations and square-free 0-cycles. We showed in Section 3.3 that any class function on $S_n$ gives a function, viewed as a random variable, on $A_n(V)$. The main aim in this step is to prove Lemma 16, which roughly says that statistics on square-free 0-cycles are controlled by the corresponding statistics on permutations.
For any real number $A$ and any positive integer $k$, define
\[
\binom{A}{k} := \frac{A(A+1) \cdots (A+k-1)}{k!}.
\]
For $A$ a positive integer, $\binom{A}{k} = \binom{A+k-1}{k}$ is the number of ways to choose $k$ elements from a set of size $A$, allowing repetition.

**Lemma 13.** For any real number $A$ and any positive integer $k$, we have
\[
\sum_{i=0}^{k-1} \binom{A}{i} A = \binom{A}{k} k.
\]

**Proof.** We will prove by induction on $k$. The case when $k = 1$ is easily checked. For induction, we have
\[
\sum_{i=0}^{k-1} \binom{A}{i} A = \binom{A}{k-1} A + \sum_{i=0}^{k-2} \binom{A}{i} A
= \binom{A}{k-1} A + \binom{A}{k-1} (k-1)
= \binom{A}{k} k.
\]

**Lemma 14.** For any positive integer $n$, any real number $t$ and any $A > 0$, we have
\[
\frac{1}{n!} \sum_{\sigma \in S_n} \prod_{j=1}^{n} (1 + At^j)^{X_j(\sigma)} = \sum_{i=0}^{n} \binom{A}{i} t^i.
\]

*(The function $X_j$ was defined in (3.13).)*

**Proof.** We will prove by induction on $n$. The case when $n = 1$ is easily checked. We will show that if equation (5.2) holds for all $k < n$, then it also holds for $n$.

For an arbitrary $\sigma \in S_n$ decomposed into a product of disjoint cycles, the number $n$ appears in a unique cycle of length $l$, for some $l = 1, \ldots, n$. Moreover, for each $l$, define $R_l := \{\sigma \in S_n : n \text{ is contained in an } l\text{-cycle of } \sigma\}$.

\[
|R_l| = (n-l)!(l-1)! \binom{n-1}{l-1} = (n-1)!.
\]

Let $E_n$ denote the left hand side of (5.2), which is a sum over $S_n$. We rewrite the sum over $R_l$, for each $1 \leq l \leq n$:
\[
E_n := \frac{1}{n!} \sum_{\sigma \in S_n} \prod_{j=1}^{n} (1 + At^j)^{X_j(\sigma)}
= \frac{1}{n!} \sum_{l=1}^{n} \left[ \sum_{\sigma \in R_l} \prod_{j=1}^{n} (1 + At^j)^{X_j(\sigma)} \right]
= \frac{1}{n!} \sum_{l=1}^{n} \left[ \frac{|R_l|}{|S_{n-1}|} (1 + At^l) \sum_{r \in S_{n-1}} \prod_{j=1}^{n} (1 + At^j)^{X_j(r)} \right]
\]
Analytic number theory for 0-cycles

\[= \frac{1}{n} \sum_{l=1}^{n} \left[ (1 + At^l) E_{n-1}^l \right] \]

\[= \frac{1}{n} \sum_{l=1}^{n} \left[ (1 + At^l) \sum_{i=0}^{n-l} \left( \binom{A}{i} \right) t^l \right] \quad \text{by induction hypothesis} \]

\[= \frac{1}{n} \sum_{l=1}^{n} \sum_{i=0}^{n-l} \left( \binom{A}{i} \right) t^l + \frac{1}{n} \sum_{l=1}^{n} \sum_{i=0}^{n-l} \left( \binom{A}{i} \right) At^l. \]

We simplify the two summands on the last line separately. The first summand can be simplified to be:

\[\frac{1}{n} \sum_{l=1}^{n} \sum_{i=0}^{n-l} \left( \binom{A}{i} \right) t^l = \frac{1}{n} \sum_{i=0}^{n-1} (n - i) \left( \binom{A}{i} \right) t^l \]

(5-3)

The second summand can be simplified to be

\[\frac{1}{n} \sum_{l=1}^{n} \sum_{i=0}^{n-l} \left( \binom{A}{i} \right) At^l = \frac{1}{n} \sum_{k=1}^{n} \left[ (\sum_{i=0}^{k-1} \left( \binom{A}{i} \right) ) A \right] t^k \]

\[= \frac{1}{n} \sum_{k=1}^{n} k \left( \binom{A}{k} \right) t^k \quad \text{by Lemma 13.} \]

(5-4)

Combining (5-3) and (5-4), we get:

\[E_n = \frac{1}{n} \sum_{i=0}^{n-1} (n - i) \left( \binom{A}{i} \right) t^l + \frac{1}{n} \sum_{i=1}^{n} i \left( \binom{A}{i} \right) t^l \]

\[= \sum_{i=0}^{n} \left( \binom{A}{i} \right) t^i. \]

Lemma 14 is thus proved.

Recall from (3·10) and (3·11) that there is a partition \(\lambda_C\) (or \(\lambda_\sigma\)) associated to a 0-cycle \(C \in B_n(V)\) (or to a permutation \(\sigma \in S_n\)).

**Lemma 15.** Suppose \(V\) is a geometrically connected variety over \(\mathbb{F}_q\) of dimension \(d \geq 1\). For each positive integer \(n\), define a class function \(g_n\) of \(S_n\) by

\[g_n(\sigma) := \frac{\text{Prob}(C \in B_n(V) : \lambda_C = \lambda_\sigma)}{\text{Prob}(\tau \in S_n : \lambda_\tau = \lambda_\sigma)}.\]

Then the expected value \(\mathbb{E}[g_n^2, S_n]\) is bounded as \(n \to \infty\).

**Proof.** For each positive integer \(j\), let \(\Pi_j(V)\) be as in Theorem 1 and let \(X_j\) be as in (3·13). Cauchy’s formula gives that

\[\text{Prob} (\tau \in S_n : \lambda_\tau = \lambda_\sigma) = \left( \prod_{j=1}^{n} j^{X_j(\sigma)} X_j(\sigma)! \right)^{-1}.\]
By the prime factorisation of 0-cycles (1·1), we have
\[
\text{Prob}(C \in \mathcal{B}_n(V) : \lambda_C = \lambda) = \frac{1}{|\mathcal{B}_n(V)|} \prod_{j=1}^{n} \left( \frac{|\Pi_j(V)|}{X_j(\sigma)} \right).
\]

Therefore, we can take the quotient of the two formulas above and obtain
\[
\mathbb{E}[g_n^2, S_n] = \frac{1}{n!} \sum_{\sigma \in S_n} \left( \frac{q^{nd}}{|\mathcal{B}_n(V)|} \prod_{j=1}^{n} \left( \frac{|\Pi_j(V)|}{X_j(\sigma)} \right) \frac{j^{X_j(\sigma)}X_j(\sigma)!}{q^{d j X_j(\sigma)}} \right)^2
\]
\[
= \left( \frac{q^{nd}}{|\mathcal{B}_n(V)|} \right)^2 \frac{1}{n!} \sum_{\sigma \in S_n} \left( \prod_{j=1}^{n} \left( \frac{|\Pi_j(V)|}{X_j(\sigma)} \right) \frac{j^{X_j(\sigma)}X_j(\sigma)!}{q^{d j X_j(\sigma)}} \right)^2
\]
\[
\leq \left( \frac{q^{nd}}{|\mathcal{B}_n(V)|} \right)^2 \left( \frac{1}{n!} \sum_{\sigma \in S_n} \prod_{j=1}^{n} \left( \frac{j^{X_j(\sigma)}}{q^{d j}} \right)^{2X_j(\sigma)} \right).
\]

We will bound each of the two factors in (5·5) separately. Lemma 9 implies that \(q^{nd}/|\mathcal{B}_n(V)|\) converges as \(n \to \infty\) and therefore is bounded. Lemma 8 implies that there exists some constant \(A\) depending only on \(V\) such that
\[
\forall j, \quad \frac{j|\Pi_j(V)|}{q^{d j}} \leq 1 + Aq^{-j/2}.
\]

Therefore, we have
\[
\frac{1}{n!} \sum_{\sigma \in S_n} \prod_{j=1}^{n} \left( \frac{j|\Pi_j(V)|}{q^{d j}} \right)^{2X_j(\sigma)} \leq \frac{1}{n!} \sum_{\sigma \in S_n} \prod_{j=1}^{n} \left( 1 + Aq^{-j/2} \right)^{X_j(\sigma)}
\]
\[
\leq \sum_{i=0}^{n} \binom{A}{i} q^{-i/2}
\]
\[
\leq \sum_{i=0}^{\infty} \binom{A}{i} q^{-i/2} = (1 - q^{-1/2})^{-A}.
\]

Hence, \(\mathbb{E}[g_n^2, S_n]\) is bounded.

Recall from (3·12) that every class function \(f_n\) of \(S_n\) can be evaluated at a partition \(\lambda\) of \(n\) and at a 0-cycle \(C \in \mathcal{A}_n(V)\). The following lemma relates the expected value of \(f_n\) on the two probability spaces \(S_n\) and \(\mathcal{B}_n(V)\).

**Lemma 16 (Comparison Lemma).** Suppose \(V\) is a geometrically connected variety over \(\mathbb{F}_q\) of dimension \(d \geq 1\). For any sequence \(f_n : S_n \to [0, 1]\) of class functions of \(S_n\), we have
\[
\mathbb{E}[f_n, \mathcal{B}_n(V)] = O\left(\sqrt{\mathbb{E}[f_n, S_n]}\right),
\]
where the implied constant is independent of the sequence \(f_n\).
Proof. We have
\[
\mathbb{E}[f_n, B_n(V)] = \frac{1}{|B_n(V)|} \sum_{C \in B_n(V)} f_n(C)
\]
\[
= \sum_{\lambda \in \Lambda_n} f_n(\lambda) \cdot \text{Prob}\left(C \in B_n(V) : \lambda_C = \lambda\right)
\]
\[
= \sum_{\lambda \in \Lambda_n} f_n(\lambda) \cdot g_n(\lambda) \cdot \text{Prob}\left(\sigma \in S_n : \lambda_\sigma = \lambda\right) \quad \text{with } g_n \text{ as in Lemma 15}
\]
\[
= \frac{1}{|S_n|} \sum_{\sigma \in S_n} f_n(\sigma) g_n(\sigma)
\]
\[
= \mathbb{E}[f_n \cdot g_n, S_n]
\]
\[
\leq \mathbb{E}[g_n^2, S_n]^{1/2} \cdot \mathbb{E}[f_n^2, S_n]^{1/2} \quad \text{by Cauchy–Schwarz inequality}
\]
\[
\leq \mathbb{E}[g_n^2, S_n]^{1/2} \cdot \mathbb{E}[f_n, S_n]^{1/2}
\]
\[
\text{since } 0 \leq f_n \leq 1.
\]
By Lemma 15, \(\mathbb{E}[g_n^2, S_n]\) is bounded. Hence, we have
\[
\mathbb{E}[f_n, B_n(V)] = O\left(\sqrt{\mathbb{E}[f_n, S_n]}\right),
\]
where the implied constant is \(\mathbb{E}[g_n^2, S_n]\) and thus is independent of the sequence \(f_n\).

One can ask if the same comparison lemma would hold if \(B_n(V)\) is replaced by the super-set \(A_n(V)\). Our proof would not work in this case because the inequality in (5.5) no longer holds if \(B_n(V)\) is replaced by \(A_n(V)\).

Remark 5 (Comparing measures on \(S_n\)). The set of conjugacy classes in \(S_n\) admits a standard probability measure, namely, the measure induced from the uniform measure on \(S_n\). On the other hand, for each variety \(V\) over finite fields, the pushforward of the uniform probability measure on \(B_n(V)\) via the map \(C \mapsto \lambda_C\) as in (3.12) gives another probability measure on the conjugacy classes of \(S_n\). The proof of Lemma 16 is a direct comparison of these measures. In the case when \(V = \mathbb{A}^1\), the pushforward of the uniform measure on the set \(B_n(\mathbb{A}^1)\) of monic square-free polynomials over \(\mathbb{F}_q\) to \(S_n\) is precisely what Hyde–Lagarias [15] called the polynomial \(q\)-splitting measure on \(S_n\).

Step 2. Approximate the left-hand side of (5.1). For each partition \(\lambda\) of \(n\) give by \(\lambda : n = \lambda_1 + \cdots + \lambda_l\), define a subset \(\phi(\lambda) := \{\log \lambda_1, \ldots, \log \lambda_l\}\) of the interval \([0, \log n]\). For any \(M\) and \(N\) with \(0 < M < N < n\), and for any \(r, L > 0\), define
\[
\mu_{r,L}(\lambda) := \frac{1}{\log(N/M)} \cdot \nu\left(\left\{t \in [\log M, \log N] : \left|\phi(\lambda) \cap [t, t + L]\right| = r\right\}\right),
\]
where again \(\nu\) denotes the Lebesgue measure. Though \(\mu_{r,L}\) also depends on \(M\) and \(N\), for simplicity we will suppress \(M\) and \(N\) in our notation.

As in (3.12), we can evaluate \(\mu_{r,L}\) on permutations and \(0\)-cycles:
\[
\forall \sigma \in S_n, \quad \mu_{r,L}(\sigma) := \mu_{r,L}(\lambda_\sigma),
\]
\[
\forall C \in A_n(V), \quad \mu_{r,L}(C) := \mu_{r,L}(\lambda_C).
\]
Moreover, \(\mu_{r,L}(C)\) approximates the left-hand side of (5.1) in Theorem 12. Our main goal in this step is to prove Proposition 19 below.
PROPOSITION 17. For any $N, M$ satisfying $M \leq \sqrt{n} \leq N \leq n$, let $m := (10 \log \log N)/(\log \log \log N)^2$ and, for any $r, L$ with $r \leq m/10$, and $(\log \log N)/M < L \leq m/10$, we have

$$\mathbb{E}\left[\left|\mu_{r,L} - \frac{e^{-L}L^r}{r!}\right|, B_n(V)\right] = O\left(\frac{\sqrt{e^{-L}L^r 1}}{2^{m}}\right), \quad \text{as } n \to \infty.$$  

Proof. Granville proved in [14, equation (4.1)] that for any $N, M, m, r, L$ satisfying the assumptions of this proposition,

$$\mathbb{E}\left[\left|\mu_{r,L} - \frac{e^{-L}L^r}{r!}\right|, B_n(V)\right] = O\left(\frac{e^{-L}L^r 1}{r! 2^{m}}\right), \quad \text{as } n \to \infty.$$  

Proposition 17 now follows by applying Lemma 16 to Granville’s estimate.

In order to obtain a similar statement but replacing $B_n(V)$ by $A_n(V)$, we will prove the following lemma.

LEMMA 18. If $0 < M < N \leq n$ and $r, L > 0$ and $j$ is a positive integer, then for any $C \in A_n(V)$ and any $D \in A_j(V)$, we have

$$|\mu_{r,L}(C + D) - \mu_{r,L}(C)| \leq \frac{\log j}{\log(N/M)}.$$  

Proof. We have

$$\mu_{r,L}(C + D) = \frac{1}{\log(N/M)} v\left(\{t \in [\log M, \log N] : \phi(C + D) \cap [t, t + L] = r\}\right).$$  

Notice that $\phi(C + D) = \phi(C) \cup \phi(D)$, where $\phi(D) \subset [0, \log j]$. Therefore, the two sets $\phi(C + D)$ and $\phi(C)$ coincide except possibly on the interval $[0, \log j]$. Thus, we have

$$\left|v\left(\{t \in [\log M, \log N] : \phi(C + D) \cap [t, t + L] = r\}\right) - v\left(\{t \in [\log M, \log N] : \phi(C) \cap [t, t + L] = r\}\right)\right| \leq \log j$$

which gives that

$$|\mu_{r,L}(C + D) - \mu_{r,L}(C)| \leq \frac{\log j}{\log(N/M)}.$$  

PROPOSITION 19. For every $\epsilon > 0$ and every $M, N$ satisfying $0 \leq M \leq \sqrt{n^{1-\epsilon}}$ and $\sqrt{n} \leq N \leq n^{1-\epsilon}$, for $m := (10 \log \log N)/(\log \log \log N)^2$, for every $r, L$ satisfying $r \leq m/10$ and $(\log \log N)/M < L \leq m/10$, we have

$$\mathbb{E}\left[\left|\mu_{r,L} - \frac{e^{-L}L^r}{r!}\right|, A_n(V)\right] = O\left(\frac{\sqrt{e^{-L}L^r 1}}{2^{m}}\right), \quad \text{as } n \to \infty.$$  

Proof. The proof below despite its technicalities follows a very simple idea: $A_n(V)$ can be partitioned iteratively using $B_k(V)$ of smaller $k$ so we can apply Proposition 17.
Every 0-cycle $C \in A_n(V) \setminus B_n(V)$ can be written uniquely as a sum $C + 2D$ where $C$ is square-free. This gives the following partition of $A_n(V)$:

$$A_n(V) = \bigcup_{j=0}^{[n/2]} B_{n-2j}(V) \times A_j(V),$$

where again we adopt the convention that $B_0(V) = A_0(V) = \{0\}$. Therefore, we have

$$\mathbb{E}\left[\mu_{r,L} - \frac{e^{-L}L^r}{r!}, A_n(V)\right] = \sum_{j=0}^{[n/2]} \frac{|B_{n-2j}(V) \times A_j(V)|}{|A_n(V)|} \cdot \mathbb{E}\left[\mu_{r,L} - \frac{e^{-L}L^r}{r!}, B_{n-2j}(V) \times A_j(V)\right].$$

By Lemmas 9 and 7, we know that there exists a constant $A > 0$ such that for all $n, j \in \mathbb{Z}_{\geq 0}$

$$\frac{|B_{n-2j}(V) \times A_j(V)|}{|A_n(V)|} \leq A q^{-jd}.$$ 

Thus, (5.6) gives

$$\mathbb{E}\left[\mu_{r,L} - \frac{e^{-L}L^r}{r!}, A_n(V)\right] \leq \sum_{j=0}^{[n/2]} A q^{-jd} \cdot \mathbb{E}\left[\mu_{r,L} - \frac{e^{-L}L^r}{r!}, B_{n-2j}(V) \times A_j(V)\right]$$

$$= A \cdot \mathbb{E}\left[\mu_{r,L} - \frac{e^{-L}L^r}{r!}, B_n(V)\right]$$

$$+ A \cdot \sum_{j=1}^{[n/2]} \mathbb{E}\left[\mu_{r,L} - \frac{e^{-L}L^r}{r!}, B_{n-2j}(V) \times A_j(V)\right] q^{-jd}.$$ 

Proposition 17 tells us that

$$(*) = O\left(\sqrt{\frac{e^{-L}L^r}{r!} \frac{1}{2^m}}\right).$$

Thus the proof will be complete if we show that (**) satisfies the same bound as above.

$$(***) = A \cdot \sum_{j=1}^{[n/2]} \frac{q^{-jd}}{|B_{n-2j}(V) \times A_j(V)|} \sum_{C \in B_{n-2j}(V)} \sum_{D \in A_j(V)} \left|\mu_{r,L}(C + 2D) - \frac{e^{-L}L^r}{r!}\right|$$

$$\leq A \cdot \sum_{j=1}^{[n/2]} \frac{q^{-jd}}{|B_{n-2j}(V) \times A_j(V)|} \sum_{C \in B_{n-2j}(V)} \sum_{D \in A_j(V)} \left|\mu_{r,L}(C) - \frac{e^{-L}L^r}{r!}\right| + \frac{\log 2j}{\log(N/M)}$$

by Lemma 18

$$= A \frac{\log(N/M)}{\log(N/M)} \sum_{j=1}^{[n/2]} \log(2j)q^{-jd} + A \cdot \sum_{j=1}^{[n/2]} \mathbb{E}\left[\mu_{r,L} - \frac{e^{-L}L^r}{r!}, B_{n-2j}(V)\right] q^{-jd}.$$
To complete the proof, it suffices to show each of the following asymptotics:

\[ e^{-(\log n)/2} = O\left(\sqrt{\frac{e^{-L} L^r}{r!} \frac{1}{2^m}}\right), \quad (5.7) \]

\[ (\dagger) = O\left(e^{-(\log \log n)/2}\right), \quad \text{and thus} \quad (\dagger) = O\left(\sqrt{\frac{e^{-L} L^r}{r!} \frac{1}{2^m}}\right) \quad \text{by (5.7)} \tag{5.8} \]

\[ (\ddagger) = O\left(\sqrt{\frac{e^{-L} L^r}{r!} \frac{1}{2^m}}\right). \tag{5.9} \]

**Remark 6** (on the big-O notation). In the argument below, since we will be using the transitivity of the big-O relation repeatedly, for brevity we will follow the widely-used convention to write \(O(f) = O(g) = O(h)\) to mean that \(f = O(g)\) and \(g = O(h)\), and thus \(f = O(h)\). However, the equal sign in this notation does not imply reflexivity! Indeed, \(O(n^{-2}) = O(n^{-1})\) is true but \(O(n^{-1}) = O(n^{-2})\) is false. We advise the reader to treat the equal sign as an inequality in the context of big-O relation.

First, we prove (5.7). We will bound the following factors appearing on the right-hand side of (5.7).

\[ m = 10 \log \log N/(\log \log N)^2 \implies 2^m = O(e^{(\log \log N)/3}) \]

\[ L \leq \frac{m}{10} \implies e^L = O(e^{(\log \log N)/3}) \]

\[ r \leq \frac{m}{10} \implies r! \leq r^r = O(e^{m \log m}) = O(e^{(\log \log N)/3}). \]

Thus, we obtain

\[ \frac{r!}{e^{-L} L^r} 2^m \leq e^L \cdot 2^m \cdot r! = O(e^{\log \log N}) = O(e^{\log \log n}) \]

which implies (5.7) by taking reciprocal and square root.

Next, we prove (5.8). Since the infinite series \(\sum_{j=1}^{\infty} \log(2j) q^{-jd}\) converges, we have

\[ (\dagger) = O\left(\frac{1}{\log(N/M)}\right) = O(e^{-\log \log(N/M)}) \]

\[ = O\left(e^{-\log \log(n^{1/2})}\right) \quad \text{since} \quad N \geq \sqrt{n} \quad \text{and} \quad M \leq \sqrt{n^{1-\epsilon}} \]

\[ = O\left(e^{-(\log \log n)/2}\right). \]

Finally, we prove (5.9). In order to bound (\ddagger), we divide the summation over \(j\) into two parts: when \(j \leq (n-n^{1-\epsilon})/2\) and when \(j > (n-n^{1-\epsilon})/2\). When \(j \leq (n-n^{1-\epsilon})/2\), we have \(n - 2j \geq n^{1-\epsilon}\). Since \(M\) and \(N\) satisfy \(M \leq \sqrt{n^{1-\epsilon}} \leq N \leq n^{1-\epsilon}\), we can apply Proposition 17 to \(B_{n-2j}(V)\) to conclude that if \(n\) is large, then \(n - 2j \geq n^{1-\epsilon}\) is also large, and therefore

\[ \mathbb{E}\left[\left|\mu_{r,C} - \frac{e^{-L} L^r}{r!}\right|, B_{n-2j}(V)\right] = O\left(\sqrt{\frac{e^{-L} L^r}{r!} \frac{1}{2^m}}\right). \]

As explained above, this asymptotic bound holds long as \(n\) is large enough and does not depend on \(j\). Thus, by Cauchy–Schwarz we have

\[ \sum_{j \leq (n-n^{1-\epsilon})/2} \mathbb{E}\left[\left|\mu_{r,C} - \frac{e^{-L} L^r}{r!}\right|, B_{n-2j}(V)\right] q^{-jd} = O\left(\sqrt{\frac{e^{-L} L^r}{r!} \frac{1}{2^m}}\right). \]

\[ \sum_{j \geq (n-n^{1-\epsilon})/2} \mathbb{E}\left[\left|\mu_{r,C} - \frac{e^{-L} L^r}{r!}\right|, B_{n-2j}(V)\right] q^{-jd} = O\left(\sqrt{\frac{e^{-L} L^r}{r!} \frac{1}{2^m}}\right). \]
When \( j > (n - n^{1-\epsilon})/2 \), we have

\[
\sum_{j > (n - n^{1-\epsilon})/2} \mathbb{E} \left[ \left| \mu_{r,L}(C) - \frac{e^{-L} L^r}{r!} \right|, B_{n-2j}(V) \right] q^{-jd} = O \left( \sum_{j > (n - n^{1-\epsilon})/2} q^{-jd} \right) \\
= O \left( q^{-d(n-n^{1-\epsilon})/2} \right) = O \left( e^{-(\log \log n)/2} \right) \\
= O \left( \sqrt{\frac{e^{-L} L^r}{r!} \frac{1}{2^m}} \right) \quad \text{by (5.7).}
\]

Proposition 19 is established.

**Step 3. Deduce Theorem 12 from Proposition 19.**

We claim that Proposition 19 can be applied with appropriate choices of \( \epsilon, M, N \) to prove Theorem 12.

**Claim.** Choose \( \epsilon := \frac{(\log \log n)^2}{\log n} \) and \( M := n^{\epsilon} \) and \( N := n^{1-\epsilon} \). Then any \( r \) and \( L \) satisfying the assumptions of Theorem 12 will also satisfy the assumptions of Proposition 19, when \( n \) is large enough.

**Proof.** It suffices to verify the following three inequalities for large \( n \):

\[
\frac{(\log \log N)}{M} \leq \frac{1}{y} \quad (5.10) \\
\frac{y}{20} \leq \frac{m}{10} \quad (5.11) \\
\frac{y}{(\log y)} \leq \frac{m}{10}. \quad (5.12)
\]

We always assume that \( n \) is a number large enough. (5.10) follows from taking the quotient of the two inequalities \( \log \log N \leq \log \log n \) and \( M = n^{\epsilon} \geq (\log \log n)^2 \). (5.11) follows from

\[
\frac{y}{20} = \frac{1}{20} \frac{\log \log n}{(\log \log n)^2} \leq \frac{\log n^{1-\epsilon}}{(\log \log n^{1-\epsilon})^2} = \frac{(\log \log n) + \log(1 - \epsilon)}{(\log((\log \log n) + \log(1 - \epsilon)))^2}.
\]

(5.12) follows from (5.11).

Thus, Proposition 19 implies that with our choices of \( \epsilon, M, N \) and for all \( r, L \) considered in Theorem 12,

\[
\mathbb{E} \left[ \left| \mu_{r,L} - \frac{e^{-L} L^r}{r!} \right|, A_n(V) \right] = O \left( \sqrt{\frac{e^{-L} L^r}{r!} \frac{1}{2^m}} \right). \quad (5.13)
\]

The deduction below will mimic the deduction of theorem 1.3 from proposition 4.2 in [22]. We now construct the subset \( \Sigma_n \subset A_n(V) \). For nonnegative integers \( j \) and \( r \), we set \( L_j := m^{-1}(1 + 2^{-m/6})^j \) and define

\[
\Sigma_{j,r} := \left\{ C \in A_n(V) : \left| \mu_{r,L_j}(C) - e^{-L_j} \frac{L^r}{r!} \right| \geq \frac{1}{2^{m/6+1}} \left( e^{-L_j} \frac{L^r}{r!} \right)^{1/2} \right\}. \quad (5.14)
\]

Equation (5.13) implies that

\[
|\Sigma_{j,r}| = |A_n(V)| O(2^{-m/3}).
\]
We set $\Sigma_n := \bigcup_{j,r} \Sigma_{j,r}$ for $0 \leq j \leq 2^{m/6+1} \log m$ and $r \leq m(\log m)^{-2}$. The total number of such pairs $(j, r)$ are at most

$$2^{m/6+1} \log m \cdot m(\log m)^{-2} = \frac{m}{\log m} 2^{m/6+1}.$$ 

Thus,

$$|\Sigma_n| = |A_n(V)| \cdot O\left(\frac{m}{\log m} 2^{-m/6}\right),$$

which is within the claimed error in Theorem 12.

Next, we show that all $C \in A_n(V) \setminus \Sigma_n$ satisfy (5.1). For any $L \in [1/m, m/20]$, there is some $j$ such that $L_j \leq L < L_{j+1}$, and thus we have

$$\mu_{r,L}(C) = \sum_{i \leq r} \mu_{i,L}(C) - \sum_{i \leq r-1} \mu_{i,L}(C)$$

$$\leq \sum_{i \leq r} \mu_{i,L}(C) - \sum_{i \leq r-1} \mu_{i,L_{j+1}}(C)$$

$$\leq \sum_{i \leq r} \left[ e^{-L_{j+1}} \frac{L_{j+1}^i}{i!} + \frac{1}{2^{m/6+1}} \left( e^{-L_j} \frac{L_j^i}{i!} \right)^{1/2} \right]$$

$$- \sum_{i \leq r-1} \left[ e^{-L_{j+1}} \frac{L_{j+1}^i}{i!} - \frac{1}{2^{m/6+1}} \left( e^{-L_j} \frac{L_j^i}{i!} \right)^{1/2} \right]$$

$$\leq e^{-L_{j+1}} \frac{L_{j+1}^r}{r!} + O\left( \frac{m}{2^{m/6}} \sum_{i \leq r} \left( e^{-L_j} \frac{L_j^i}{i!} \right)^{1/2} \right)$$

since $e^{-L_j} \frac{L_j^i}{i!} = e^{-L_{j+1}} \frac{L_{j+1}^i}{i!} \left( 1 + O\left( \frac{m}{2^{m/6}} \right) \right)$.

Notice that $(\ast) = O(r) = O(m)$.

Thus, we have

$$\mu_{r,L}(C) \leq e^{-L} \frac{L^r}{r!} + O\left( \frac{m^2}{2^{m/6}} \right).$$

The error term above can be bounded as

$$\frac{m^2}{2^{m/6}} = \frac{1}{2^{m/15}} \cdot O\left( 2^{-m/11} \right) = \frac{1}{2^{m/15}} \cdot O\left( e^{\log \log n} \right) = \frac{1}{2^{m/15}} \cdot O\left( \frac{e^{-L} L^r}{r!} \right),$$

where the last equality follows from (5.7). Thus, we have

$$\mu_{r,L}(C) \leq e^{-L} \frac{L^r}{r!} \left[ 1 + O\left( \frac{1}{2^{m/15}} \right) \right].$$

The lower bound

$$\mu_{r,L}(C) \geq e^{-L} \frac{L^r}{r!} \left[ 1 + O\left( \frac{1}{2^{m/15}} \right) \right]$$

can be obtained in a similar way by considering

$$\mu_{r,L}(C) \geq \sum_{i \leq r} \mu_{i,L_{j+1}}(C) - \sum_{i \leq r-1} \mu_{i,L_j}(C).$$
Since we chose \( m \) and \( y \) such that \( m \leq y \), combining the lower and the upper bounds, we have

\[
\mu_{r,L}(C) = e^{-\frac{L'}{r!}} \left[ 1 + O\left( \frac{1}{2^{m/15}} \right) \right] = e^{-\frac{L'}{r!}} \left[ 1 + O\left( \frac{1}{2^{y/15}} \right) \right].
\]

Finally, to establish (5.1), we notice that

\[
\frac{1}{\log n} \nu \left( \left\{ t \in [0, \log n] : \phi(C) \cap [t, t + L] = k \right\} \right) = \mu_{r,L}(C) + O(\epsilon).
\]

The \( \epsilon \) we have chosen is so small that

\[
\epsilon = O\left( \frac{e^{-\frac{L'}{r!}} \frac{1}{2^{y/15}}}{r!} \right).
\]

Theorem 12 is thus proved.

6. Further questions

In Table 1, we see that multiplication of integers corresponds to the formal addition of 0-cycles. Is there any operation on 0-cycles that corresponds to addition of integers? Can one do additive number theory for 0-cycles? For example, how would a twin prime conjecture for 0-cycles state?

Acknowledgments. The author would like to thank Andrew Barbour, Jordan Ellenberg, Matthew Emerton, Andrew Granville, Sean Howe, Dan Petersen and Jesse Wolfson for helpful conversations, and to thank Sean Howe, Jeffrey Lagarias, Andrew Sutherland and an anonymous referee for suggestions on earlier drafts. The author is deeply grateful to his advisor Benson Farb, both for his kind support of this project and for his detailed comments on drafts of this paper.

REFERENCES

[1] R. Arratia, A. Barbour and S. Tavaré. On random polynomials over finite fields. Math. Proc. Cambridge Philos. Soc. 114 (1993), 347–368.
[2] A. Buchstab. Asymptotic estimation of a general number-theoretic function. Mat. Sb. (in Russian), 2(44) (6) (1937), 1239–1246.
[3] E. Bender, A. Mashatan, D. Panario and B. Richmond. Asymptotics of combinatorial structures with large smallest component. J. Combin. Theory Ser. A 107 (2004), 117–125.
[4] W. Chen. Twisted cohomology of configuration spaces and spaces of maximal tori via point-counting. Preprint, arXiv:1603.03931 (2016).
[5] T. Church, J. Ellenberg and B. Farb. Representation stability in cohomology and asymptotics for families of varieties over finite fields. Contemp. Math. 620 (2014), 1–54.
[6] P. Deligne. La conjecture de Weil: II. Publ. Math. Inst. Hautes Études Sci. 52 (1980), 137–252.
[7] K. Dickman. On the frequency of numbers containing prime factors of a certain relative magnitude. Arkiv för Matematik, Astronomi och Fysik 22A (1930), (10) 1–14.
[8] P. Erdős and M. Kac. The Gaussian law of errors in the theory of additive number theoretic functions. Amer. J. Math. 62 (1940), 738–742.
[9] P. Flajolet and R. Sedgewick. Analytic Combinatorics (Cambridge University Press, Cambridge, 2009).
[10] P. Flajolet and M. Soria. Gaussian limiting distributions for the number of components in combinatorial structures. J. Combin. Theory Ser. A 153 (1990), 165–182.
[11] B. Farb and J. Wolfson. Étale homological stability and arithmetic statistics. Preprint arXiv:1512.00415 (2015).
[12] A. Granville. Prime divisors are Poisson distributed. Int. J. Number Theory 03 (01), (2011).
[13] A. Granville. The anatomy of integers and permutations. Preprint (2008).
[14] A. Granville. Cycle lengths in a permutation are typically Poisson distributed. Electron. J. Combin. 13 (2006).
[15] T. Hyde and J. Lagarias. Polynomial splitting measures and cohomology of the pure braid group. Preprint, arXiv:1604.05359 (2016).
[16] Y. Liu. A generalisation of the Erdős–Kac theorem and its applications. Canad. Math. Bull. 47 (2004), 589–606.
[17] S. Lang and A. Weil. Number of points of varieties in finite fields, in Amer. J. Math. 76 (1954), 819–827.
[18] M. Omar, D. Panario, B. Richmond and J. Whately. Asymptotics of largest components in combinatorial structures. Algorithmica 46 (3) (2006), 493–503.
[19] B. Poonen. Bertini theorems over finite fields. Ann. of Math. (2004), 1099–1127.
[20] D. Mumford. Abelian Varieties. Tata Inst. Fund. Research Stud. Math. (Oxford University Press, 1970).
[21] V. Ramaswami. On the number of positive integers less than $x$ and free of prime divisors greater than $x^c$. Bull. Amer. Math. Soc. 55 (12) (1949), 1122–1127.
[22] R. Rhoades. Statistics of prime divisors in function fields. Int. J. Number Theory 05 (2009), 141.
[23] A. Weil. Numbers of solutions of equations in finite fields. Bull. Amer. Math. Soc. 55 (1949), 497–508.