*The Quarterly Journal of Mathematics*
**Quart. J. Math. 00 (2018), 1–22; doi:10.1093/qmath/hay053**

# ON LOCALLY REPEATED VALUES OF ARITHMETIC FUNCTIONS OVER $\mathbb{F}_q[T]$

*by* ZEÉV RUDNICK[†]
with an Appendix by Ron Peled

(*Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel*)

[Received 27 March 2018. Revised 3 September 2018]

**Abstract**

The frequency of occurrence of 'locally repeated' values of arithmetic functions is a common theme in analytic number theory, for instance in the Erdős–Mirsky problem on coincidences of the divisor function at consecutive integers, the analogous problem for the Euler totient function and the quantitative conjectures of Erdős, Pomerance and Sarkőzy and of Graham, Holt and Pomerance on the frequency of occurrences. In this paper, we introduce the corresponding problems in the setting of polynomials over a finite field, and completely solve them in the large finite field limit.

## 1. Introduction

The frequency of occurrence of 'locally repeated' values of arithmetic functions is a common theme in analytic number theory. For instance, the famous Erdős–Mirsky problem asked to show that there are infinitely many integers $n$ for which $d(n) = d(n+1)$, where $d(n)$ is the divisor function; and the number of such occurrences was the subject of a series of papers of Erdős, Pomerance and Sarkőzy. One can replace the divisor function $d(n)$ by the number $\omega(n)$ of distinct prime divisors of $n$; the problems turn out to be closely related. Replacing $d(n)$ by the Euler totient function $\varphi(n)$ leads to somewhat different problems. These questions have generated a large body of literature (some described below), with several open conjectures. In this paper, we introduce the corresponding problems in the setting of polynomials over a finite field, and completely solve them in the large finite field limit.

### 1.1. *The problem of Erdős and Mirsky*

We begin with an account of the state of the art for the problems over the integers.

The problem of Erdős and Mirsky [4] is to show that there are infinitely many integers $n$ such that $d(n) = d(n+1)$ where $d(n)$ is the number of divisors of $n$. This was proved by Heath-Brown [10] following an idea in Spiro's PhD thesis [16], who showed that $d(n) = d(n+5040)$ has infinitely many solutions, and Pinner [13] showed that for any $k \geq 1$, there are infinitely many integers $n$ with $d(n) = d(n+k)$. We now know much more, for instance Goldston *et al.* [8] show that there are infinitely many $n$'s so that both $n$ and $n+1$ have prime factorizations of the form $p_1^2 p_2 p_3 p_4$ with $p_j$ distinct primes, hence $d(n) = 24 = d(n+1)$.

[†]Corresponding author. E-mail: rudnick@post.tau.ac.il

The same problem arises for other arithmetic functions, such as $\Omega(n)$, the number of all prime divisors of $n$ [10], or $\omega(n)$, the number of distinct prime divisors of $n$ [15]. One can also ask about multiple shifts, for instance are there infinitely many solutions of

$$d(n) = d(n+1) = d(n+2)$$

of which nothing is currently known.

The quantitative aspect of the problem is to find the asymptotic of

$$S_\alpha(x) := \#\{n \le x : \alpha(n) = \alpha(n+1)\},$$

where $\alpha = d, \omega, \Omega$, and likewise for any shift. Erdős *et al.* [5] conjectured that the order of magnitude is given by

$$S_\alpha(x) \sim \frac{1}{2\sqrt{\pi}} \frac{x}{\sqrt{\log\log x}}. \tag{1.1}$$

They proved an upper bound $S_\alpha(x) \ll x/\sqrt{\log\log x}$ of the correct order of magnitude [6] and there is a lower bound which is not far from the upper bound $S_\alpha(x) \gg x/(\log\log x)^3$, due to Hildebrand [11].

One can more generally ask for the asymptotic frequency of coincidences of any number of shifts, that is given any distinct integers $a_1, \dots, a_r$, for

$$S_\alpha(a_1 \dots, a_r; x) := \#\{n \le x : \alpha(n+a_1) = \cdots = \alpha(n+a_r)\}$$

and using the same heuristic as in [5], namely that the shifts are statistically independent, combined with the Erdős–Kac theorem, one is led to conjecture that

$$S_\alpha(a_1 \dots, a_r; x) \sim \frac{1}{\sqrt{r}\,(\sqrt{2\pi})^{r-1}} \frac{x}{(\log\log x)^{(r-1)/2}}. \tag{1.2}$$

### 1.2. *Locally repeated value of the Euler totient function*

Given a non-zero integer $k \ge 1$, it was conjectured in [5] that there are infinitely many integers $n$ for which $\varphi(n) = \varphi(n+k)$. This is not known for any value of $k$. Let $P(k, x)$ be the number of such integers $n \le x$:

$$P(k, x) := \#\{n \le x : \varphi(n) = \varphi(n+k)\}.$$

For instance, when $x = 10^8$, we have [9]

$$P(1, 10^8) = 306, \quad P(2, 10^8) = 125986, \quad P(3, 10^8) = 2, \quad P(4, 10^8) = 69131.$$

In [5, 9], it is shown that $P(k, x) = o(x)$ for any $k \ge 1$.

There is a significant difference between $k$ being even or odd, due to the ability to find solutions to the problem when $k$ is even: Leo Moser [12] observed that for integers of the form $n = 2(2p-1)$ where $p$ is a prime such that $2p-1$ is also prime, then $\varphi(n) = 2p-2 = \varphi(4p) = \varphi(n+2)$, and Schinzel [14] extended this observation to the family $n = k(2p-1)$ where $p$ is a prime for which $2p-1$ is also prime, and both are coprime to $k$. Therefore, assuming a suitable quantitative version of the twin prime conjectures gives at least $\gg x/(\log x)^2$ solutions when $k$ is even. However, when $k$ is odd, we have a smaller upper bound

$$P(k,x) \ll x/\exp\{(\log x)^{1/3}\}, \qquad k \text{ odd}.$$

It is also conjectured [5] that for any $k \geq 1$, there is a lower bound of $P(k,x) \gg x^{1-\epsilon}$.

Graham *et al.* [9] systematized these observations and used them to conjecture that for $k$ even,

$$\frac{1}{x}P(k,x) \sim \frac{A(k)}{(\log x)^2} \quad \text{as} \quad x \to \infty, \tag{1.3}$$

where $A(k) = 2C_2 \cdot c(k)$, with $C_2 = \prod_{p>2}(1-(p-1)^{-2}) = 0.6601\ldots$ is the twin prime constant, and

$$c(k) = \sum_{\substack{j,j+k \\ \text{same prime divisors}}} \frac{\gcd(j,j+k)}{j(j+k)} \prod_p{}^{*} \frac{p-1}{p-2},$$

where the sum is over all $j$'s so that $j$ and $j+k$ have the same prime factors, and the product is over primes $p > 2$ dividing $jk(j+k)/\gcd(j,j+k)^3$. For instance, $c(2) = 1/2$.

One can more generally ask the same question for multiple shifts, and to replace the Euler totient function $\varphi$ by the sum-of divisors function $\sigma(n) = \sum_{d|n} d$.

### 1.3. *The problem of Erdős and Mirsky over* $\mathbb{F}_q[T]$

Let $\mathbb{F}_q$ be a finite field of $q$ elements, and $\mathbb{F}_q[T]$ the ring of polynomials with coefficients in $\mathbb{F}_q$. For $n \geq 0$, let $M_n \subset \mathbb{F}_q[T]$ be the set of monic polynomials of degree $n$. Let $\alpha$ be an arithmetic function, that is a complex-valued function on the set of monic polynomials. For each finite field $\mathbb{F}_q$, we are given $r$ distinct polynomials $a_1, \ldots, a_r \in \mathbb{F}_q[T]$ of degree $<n$. We want to compute the probability that $\alpha(f+a_1) = \ldots = \alpha(f+a_r)$ for random $f \in M_n$, as $q \to \infty$. That is, setting

$$S_\alpha(\overrightarrow{a}; n, q) := \#\{f \in M_n \colon \alpha(f+a_1) = \ldots = \alpha(f+a_r)\}$$

then

$$\text{Prob}\{f \in M_n \colon \alpha(f+a_1) = \cdots = \alpha(f+a_r)\} = \frac{1}{q^n} S_\alpha(\overrightarrow{a}; n, q).$$

We treat the case when the arithmetic function $\alpha$ is such that for squarefree $f$, the value $\alpha(f)$ depends univalently on the number $\omega(f)$ of distinct prime (monic irreducible) divisors of $f$, that is for squarefree $f, g \in M_n$, $\alpha(f) = \alpha(g)$ if and only if $\omega(f) = \omega(g)$. Examples are: $\Omega(f)$ the

number of all prime divisors, $d(f)$ the number of monic divisors of $f$, and more generally $d_k(f) = \#\{(g_1,\dots,g_k): f = cg_1\dots g_k,\ g_j \text{ monic}, c \in \mathbb{F}_q^\times\}$, the number of ways of factoring $f$ as a product of $k$ factors.

The result is

THEOREM 1.1 *Let $\alpha = \omega, \Omega$, or $d_k$. For any $r$ distinct polynomials, $a_1,\dots,a_r \in \mathbb{F}_q[T]$ of degree $<n$*

$$\lim_{q\to\infty} \frac{1}{q^n} S_\alpha(\overrightarrow{a}; n, q) \sim \frac{c_r}{(\log n)^{(r-1)/2}}, \quad n \to \infty,$$

*with*

$$c_r = \frac{1}{(2\pi)^{(r-1)/2}\sqrt{r}}.$$

If we make the translation $X \leftrightarrow q^n$, $\log x \leftrightarrow n$, then we see that we have an analog for the conjecture (1.1) of Erdős, Pomerance and Sarkőzy (including the same constant).

We prove Theorem 1.1 in two steps: for a permutation $\sigma \in S_n$ on $n$ letters, let $\omega_n$ be the number of (disjoint) cycles of $\sigma$. We set

$$E_r(n) = \frac{1}{(n!)^r} \#\{(\sigma_1,\dots,\sigma_r) \in (S_n)^r: \omega_n(\sigma_1) = \dots = \omega_n(\sigma_r)\}$$

which is the probability that $r$ random permutations on $n$ letters all have the same number of cycles.

THEOREM 1.2 *For any $n \geq 1$, there is some $c_{r,n} > 0$ so that for any choice of distinct $a_1,\dots,a_r \in \mathbb{F}_q[T]$, with $\max_j \deg a_j < n$,*

$$|S_\omega(\overrightarrow{a}; n, q) - E_r(n) q^n| \leq c_{r,n} q^{n-1/2}.$$

Our key tool for this is the independence of cycle structure for shifted polynomials [1], see Theorem 2.1.

We then show that

$$E_r(n) \sim \frac{c_r}{(\log n)^{(r-1)/2}}, \quad n \to \infty, \qquad c_r = \frac{1}{(2\pi)^{(r-1)/2}\sqrt{r}} \tag{1.4}$$

(the case $r = 2$ is due to Wilf [17]) which will prove Theorem 1.1.

### 1.4. *Locally repeated values of $\varphi$ in $\mathbb{F}_q[T]$*

The Euler totient function for $\mathbb{F}_q[T]$ over the finite field $\mathbb{F}_q$ is defined as $\varphi(f) = \#(\mathbb{F}_q[T]/(f))^\times$, the number of invertible residues modulo $f$. Fix $r \geq 2$. Given $r$ distinct polynomials $a_1[T],,\dots,a_r[T] \in \mathbb{F}_q[T]$, all of degree $\deg a_j < n$, let

$$S_\varphi(\overrightarrow{a}; n, q) = \#\{f \in M_n : \varphi(f + a_1) = \varphi(f + a_2) = \cdots = \varphi(f + a_r)\}.$$

Given a permutation $\sigma \in S_n$, one says that the *cycle structure* of $\sigma$ is $(\lambda_1, \ldots, \lambda_n)$ if $\sigma$ has $\lambda_i$ cycles of length $i$ (the notation $\lambda = (1^{\lambda_1} 2^{\lambda_2} \ldots n^{\lambda_n})$ is also used in the literature). Thus $n = \sum_i i\lambda_i$, and the number of cycles is $\omega(\sigma) = \sum_i \lambda_i$. Let $W_r(n)$ be the probability that $r$ random permutations on $n$ letters have the same cycle structure and

$$A_r = \sum_{m=1}^{\infty} W_r(m).$$

We have

$$A_2 = 4.2634, \quad A_3 = 2.59071\ldots, \quad A_4 = 2.23647\ldots$$

THEOREM 1.3 *For any choice of distinct* $a_1(T), \ldots, a_r(T) \in \mathbb{F}_q[T]$, *with* $\deg a_j < n$,

$$\lim_{q \to \infty} \frac{1}{q^n} S_\varphi(\overrightarrow{a}; n, q) \sim \frac{A_r}{n^r}, \quad \text{as } n \to \infty.$$

This is in analogy with the conjecture (1.3), once we use the dictionary $x \leftrightarrow q^n = X$, and $\log x \leftrightarrow n = \log_q X$.

The same result holds if we replace $\varphi$ with any arithmetic function $\alpha$ for which there is $q_n$ so that if $f, g \in M_n \subset \mathbb{F}_q[T]$ are both squarefree, then for all $q > q_n$, $\alpha(f) = \alpha(g)$ is equivalent to $f$ and $g$ having the same cycle structure: $\lambda(f) = \lambda(g)$. Examples are the sum-of-divisors function $\sigma(f) = \sum_{d|f} |d|$ (the sum over monic divisors), where $|d| = \#\mathbb{F}_q[T]/(d) = q^{\deg d}$, or more generally $\sigma_s(f) = \sum_{d|f} |d|^s$.

We prove Theorem 1.3 in two steps. First, we fix $n$, and show:

THEOREM 1.4 *For any* $n \geq 1$, *there is some* $C_{r,n} > 0$ *so that for any choice of distinct* $a_1, \ldots, a_r \in \mathbb{F}_q[T]$, *with* $\max_j \deg a_j < n$,

$$|S_\varphi(\overrightarrow{a}; n, q) - W_r(n) q^n| \leq C_{r,n} q^{n-1/2}.$$

It remains to asymptotically evaluate $W_r(n)$. This was done by Flajolet *et al.* [7, Section 4.2] for $r = 2$ (see also [3]). In Section 4.3, we sketch an adaptation of their method for general $r$, and show

$$W_r(n) \sim \frac{A_r}{n^r}, \quad \text{as } n \to \infty. \tag{1.5}$$

Thus we obtain Theorem 1.3. Appendix A, by Ron Peled gives a completely different, self-contained, proof of (1.5).

## 2. Erdős and Mirsky over $\mathbb{F}_q[T]$

### 2.1. *Background on polynomial arithmetic*

For a polynomial $f \in \mathbb{F}_q[T]$ of positive degree $n = \deg f$, the cycle structure is $\lambda(f) = (\lambda_1, \ldots, \lambda_n)$ if in the decomposition of $f$ into primes (monic irreducibles) $f = c\prod_j P_j$, $c \in \mathbb{F}_q^\times$, there are exactly $\lambda_i$ primes of degree $i$. A simple extension of the Prime Polynomial Theorem states that given a partition $\lambda \vdash n$ (so that $\sum_i i\lambda_i = n$), the number of monic polynomials $f \in M_n$ with cycle structure equal to $\lambda$ is

$$\#\{f \in M_n\colon \lambda(f) = \lambda\} = p(\lambda)q^n + O_n(q^{n-1}), \tag{2.1}$$

where $p(\lambda)$ is the probability that a random permutation on $n$ letters has cycle structure $\lambda$, which by Cauchy's formula is given by

$$p(\lambda) = \prod_{j=1}^{n} \frac{1}{j^{\lambda_j} \cdot \lambda_j!}.$$

The number of squarefree $f \in M_n$ is $q^n(1 - \frac{1}{q})$ for $n \geq 2$, and hence if $a_1, \ldots, a_r \in \mathbb{F}_q[T]$ all have degree less than $n$, then as $q \to \infty$, for all but $O(q^{n-1})$ polynomials $f \in M_n$, all of $f + a_1, \ldots, f + a_r$ are squarefree.

For $f \in \mathbb{F}_q[T]$ of positive degree, let $\omega(f)$ be the number of distinct prime divisors of $f$. Let $\alpha$ be an arithmetic function such that $\alpha(f)$ depends only on $\omega(f)$ if $f$ is squarefree, and that the dependence is 1-to-1, that is for squarefree $f$ and $g$, we have $\alpha(f) = \alpha(g)$ if and only if $\omega(f) = \omega(g)$. Examples are $\Omega(f)$, the number of all prime divisors, $d(f)$, the number of all (monic) divisors, and more generally $d_k(f)$, the number of all ways of writing $f$ (assumed monic) as a product of $k$ monic polynomials (so $d = d_2$):

$$d_k(f) = \#\{(a_1, \ldots, a_k) \quad \text{monic}\colon f = a_1 \cdot \ldots \cdot a_k\}$$

which for squarefree $f$ is given by $d_k(f) = k^{\omega(f)}$.

For such $\alpha$, if all of $f + a_1, \ldots f + a_r$ are squarefree (which happens for all but $O_r(q^{n-1})$ of the $f \in M_n$), then

$$\alpha(f + a_1) = \cdots = \alpha(f + a_r) \quad \Leftrightarrow \quad \omega(f + a_1) = \cdots = \omega(f + a_r).$$

Thus, for such $\alpha$,

$$S_\alpha(\overrightarrow{a}, n, q) = S_\omega(\overrightarrow{a}, n, q) + O(q^{n-1}) \tag{2.2}$$

and so in the sequel we may take $\alpha = \omega$.

Our fundamental tool going beyond (2.1) is the independence of cycle structure for shifted polynomials [1, Theorem 1.4]:

THEOREM 2.1 *For fixed positive integers $n, r$ and partitions $\lambda^{(1)} \vdash n, \ldots, \lambda^{(r)} \vdash n$,*

$$\frac{1}{q^n}\#\{f \in M_n\colon \lambda(f+a_1) = \lambda^{(1)}, \cdots, \lambda(f+a_s) = \lambda^{(r)}\} = p(\lambda^{(1)})\cdots p(\lambda^{(r)}) + O_{n,r}\left(q^{-\frac{1}{2}}\right),$$

*uniformly for all distinct polynomials* $a_1, \ldots, a_r \in \mathbb{F}_q[t]$ *of degrees* $\deg(a_i) < n$, *as* $q \to \infty$.

## 2.2. *Proof of Theorem* 1.2

For a permutation $\sigma \in S_n$ on $n$ letters, let $\omega_n$ be the number of cycles of $\sigma$, and $G_k(n)$ be the probability that a permutation on $n$ letters has $k$ cycles:

$$G_k(n) = \text{Prob}(\omega_n(\sigma) = k) = \frac{1}{n!}\#\{\sigma \in S_n\colon \omega_n(\sigma) = k\}.$$

Then

$$E_r(n) = \sum_{k=1}^{n} G_k(n)^r.$$

Note that $\omega(f)$ may be written in terms of the cycle structure $\lambda(f) = (\lambda_1, \ldots, \lambda_n)$ of $f$ as $\omega(f) = \omega_n(\lambda(f)) = \sum_{j=1}^{n}\lambda_j$, the number of parts of $\lambda(f)$ (we had earlier used $\omega_n(\sigma)$ for the number of cycles in a permutation $\sigma$). Thus,

$$\begin{aligned}
&\text{Prob}\{f \in M_n\colon \omega(f+a_1) = \cdots = \omega(f+a_r)\} \\
&\quad = \sum_{k=1}^{n} \text{Prob}\{f \in M_n\colon \omega(f+a_1) = \cdots = \omega(f+a_r) = k\} \\
&\quad = \sum_{k=1}^{n} \sum_{\substack{\lambda^{(1)}, \ldots, \lambda^{(r)} \vdash n \\ \omega_n(\lambda^{(i)}) = k}} \text{Prob}\{f \in M_n\colon \lambda(f+a_1) = \lambda^{(1)}, \ldots \lambda(f+a_r) = \lambda^{(r)}\},
\end{aligned}$$

where the inner sum is over all $r$-tuples of partitions of $n$ with the same number of parts: $\omega_n(\lambda^{(j)}) = k$.

Using independence of cycle structures of $f + a_1, \ldots, f + a_r$ (Theorem 2.1), we obtain

$$\begin{aligned}
&\text{Prob}\{f \in M_n\colon \lambda(f+a_1) = \lambda^{(1)}, \ldots \lambda(f+a_r) = \lambda^{(r)}\} \\
&\quad = \prod_{i=1}^{r} \text{Prob}\{f \in M_n\colon \lambda(f) = \lambda^{(i)}\} + O_{n,r}(q^{-1/2})
\end{aligned}$$

and hence

$$\begin{aligned}
&\mathrm{Prob}\{f \in M_n\colon \omega(f+a_1) = \cdots = \omega(f+a_r)\} \\
&= \sum_{k=1}^{n} \sum_{\substack{\lambda^{(1)},\ldots,\lambda^{(r)} \vdash n \\ \omega_n(\lambda^{(i)})=k}} \prod_{i=1}^{r} \mathrm{Prob}\{f \in M_n\colon \lambda(f) = \lambda^{(i)}\} + O_{n,r}(q^{-1/2}) \\
&= \sum_{k=1}^{n} \left( \sum_{\substack{\lambda \vdash n \\ \omega_n(\lambda)=k}} \mathrm{Prob}\{f \in M_n\colon \lambda(f) = \lambda\} \right)^r + O_{n,r}(q^{-1/2}) \\
&= \sum_{k=1}^{n} (\mathrm{Prob}\{f \in M_n\colon \omega(f) = k\})^r + O_{n,r}(q^{-1/2})
\end{aligned}$$

as $q \to \infty$.

We know that the cycle structure of polynomials of degree $n$ in $\mathbb{F}_q[T]$ is modeled by that of random permutations on $n$ letters (2.1):

$$\mathrm{Prob}\{f \in M_n\colon \lambda(f) = \lambda\} = \mathrm{Prob}(\omega_n(\sigma) = k) + O_n(q^{-1})$$

and plugging that in will give

$$\begin{aligned}
&\mathrm{Prob}\{f \in M_n\colon \omega(f+a_1) = \cdots = \omega(f+a_r)\} \\
&\quad = \sum_{k=1}^{n} G_k(n)^r + O_{n,r}(q^{-1/2}) = E_r(n) + O_{n,r}(q^{-1/2})
\end{aligned}$$

which proves Theorem 1.2. □

## 3. Coincidences of shifted values of $\varphi$ over $\mathbb{F}_q[T]$

### 3.1. *Proof of Theorem* 1.4

We notice that if $f$ is squarefree, then $\varphi(f)$ only depends on $q$ and on the cycle type of $f$: if $f = \prod P_i$ is a product of distinct primes, with cycle type $\lambda(f) = (\lambda_1, \ldots, \lambda_n)$, meaning that it is divisible by exactly $\lambda_j$ primes of degree $j$, so that $\sum_{j=1}^{n} j\lambda_j = n = \deg f$, then since $\varphi(f) = |f| \prod_i \left(1 - \frac{1}{|P_i|}\right)$, it follows that

$$\varphi(f) = q^n \prod_{j=1}^{n} \left(1 - \frac{1}{q^j}\right)^{\lambda_j}.$$

We define a function $\Phi(\lambda; z)$ on partitions $\lambda \vdash n$ by the above recipe, namely

$$\Phi(\lambda; z) = \prod_{j=1}^{n} (1 - z^j)^{\lambda_j}$$

so that

$$\varphi(f) = |f| \Phi(\lambda(f); 1/q).$$

Likewise, for the sum-of-divisors function $\sigma(f) = \sum_{d|f}|d|$, if $f = \prod P_i$ is a product of distinct primes, with cycle type $\lambda(f) = (\lambda_1, \ldots, \lambda_n)$, then

$$\sigma(f) = \prod_{P|f} (|P|+1) = |f|\prod_{i=1}^{n} \left(1 + \frac{1}{q^i}\right)^{\lambda_i} = |f|\Sigma(\lambda(f); 1/q),$$

where for a partition $\lambda \vdash n$, we set

$$\Sigma(\lambda; z) := \prod_{i=1}^{n} (1 + z^i)^{\lambda_i}.$$

Both $\Phi(\lambda; z)$ and $\Sigma(\lambda; z)$ are polynomials with integer coefficients, with constant term 1, with all zeros being roots of unity.

LEMMA 3.1 *If $\lambda \neq \lambda'$ are distinct partitions of $n$, then*

(i) *The polynomials $\Phi(\lambda; z)$ and $\Phi(\lambda'; z)$ are distinct.*
(ii) *There is some $\epsilon_n > 0$ so that for all $0 < |z| < \epsilon_n$,*

$$\Phi(\lambda; z) \neq \Phi(\lambda'; z).$$

*The same conclusions hold for $\Sigma(\lambda; z)$.*

*Proof.* (i) If $A(z) = \prod_{j=1}^{n} (1 - z^j)^{a_j}$ and $B(z) = \prod_{j=1}^{n} (1 - z^j)^{b_j}$ with non-negative integers $a_j$, $b_j$ and $A(z) = B(z)$ as polynomials, we want to show that $a_j = b_j$ for all $j$. We compare logarithmic derivatives (we set $a_i = 0 = b_i$ if $i > n$):

$$-z\frac{A'}{A}(z) = \sum_{m\geq 1} z^m \sum_{i|m} i a_i$$

and likewise for $B$. Therefore, for all $m \geq 1$:

$$\sum_{i|m} i a_i = \sum_{i|m} i b_i. \tag{3.1}$$

In particular, taking $m = 1$ gives $a_1 = b_1$. Now we assume by induction that $a_i = b_i$ for $i < I$, then (3.1) for $m = I$ gives

$$I a_I + \sum_{\substack{i|I \\ i<I}} = I b_I + \sum_{\substack{i|I \\ i<I}} i b_i$$

and the inductive hypothesis gives $a_I = b_I$. The proof for $S(\lambda; z)$ is similar.

(ii) By part (i), the different polynomial $F_{\lambda,\lambda''}(z) := \Phi(\lambda; z) - \Phi(\lambda'; z)$ is not the zero polynomial if $n > 1$. It is a polynomial of degree $\leq n - 1$, which vanishes at the origin, since the original polynomials have the same constant term (equal to 1). Its other zeros are bounded away from the origin, hence part (ii). □

Given distinct $a_1, \dots, a_r \in \mathbb{F}_q[T]$ with $\deg a_j < n$, we define for an $r$-tuple $\overrightarrow{\lambda} = (\lambda^{(1)}, \dots \lambda^{(r)})$ of partitions $\lambda^{(j)} \vdash n$, a function

$$R(\overrightarrow{\lambda}; n, q; \overrightarrow{a}) := \#\left\{ \begin{array}{cc} f \in M_n: & \lambda(f + a_1) = \lambda^{(1)}, \dots, \lambda(f + a_r) = \lambda^{(r)} \\ & f + a_1, \dots f + a_r \quad \text{all squarefree} \end{array} \right\}.$$

Then

$$S_\varphi(\overrightarrow{a}; n, q) = \sum_{\substack{\overrightarrow{\lambda} \\ \Phi(\lambda^{(1)}; 1/q) = \dots = \Phi(\lambda^{(r)}; 1/q)}} R(\overrightarrow{\lambda}; n, q; \overrightarrow{a}) + O(q^{n-1}), \tag{3.2}$$

where the sum is finite, as there are a finite number (depending on $n$) of partitions $\lambda \vdash n$.

By Lemma 3.1(ii), there is some $q_n \gg 1$ so that for all $q > q_n$, if $\lambda \neq \lambda' \vdash n$ then $\Phi(\lambda; 1/q) \neq \Phi(\lambda'; 1/q)$. Hence, for $q > q_n$, we have that the only contribution to the outer sum in (3.2) is the diagonal term $\lambda^{(1)} = \dots = \lambda^{(r)}$:

$$S_\varphi(\overrightarrow{a}; n, q) = \sum_{\lambda \vdash n} R((\lambda, \dots, \lambda); n, q; \overrightarrow{a}) + O(q^{n-1}).$$

Now we use independence of cycle structures (Theorem 2.1) to write

$$\begin{aligned} R((\lambda, \dots, \lambda); n, q; \overrightarrow{a}) &= \#\left\{ \begin{array}{cc} f \in M_n: & \lambda(f + a_1) = \lambda, \dots, \lambda(f + a_r) = \lambda \\ & f + a_1, \dots, f + a_r \quad \text{squarefree} \end{array} \right\} \\ &= q^n \left( \frac{\#\{f \in M_n: \lambda(f) = \lambda\}}{q^n} \right)^r + O(q^{n-1/2}) \end{aligned}$$

(uniformly in $\overrightarrow{a}$). By (2.1),

$$\#\{f \in M_n: \lambda(f) = \lambda\} = p(\lambda) q^n + O_n(q^{n-1}), \tag{2.1}$$

where $p(\lambda)$ is the probability that a random permutation on $n$ letters has cycle structure $\lambda$. Hence we find that uniformly in $\overrightarrow{a}$,

$$S_\varphi(\overrightarrow{a}; n, q) = q^n \sum_{\lambda \vdash n} p(\lambda)^r + O(q^{n-1/2}).$$

Now note that

$$\sum_{\lambda \vdash n} p(\lambda)^r = \text{Prob}((\sigma_1, \dots, \sigma_r) \in (S_n)^r: \lambda(\sigma_1) = \dots = \lambda(\sigma_r)) =: W_r(n)$$

is the probability that an $r$-tuple of random permutations in $S_n$ have the same cycle structure, that is

$$S_\varphi(\overrightarrow{a}; n, q) = W_r(n)q^n + O(q^{n-1/2})$$

(uniformly in $\overrightarrow{a}$). This proves Theorem 1.4. The case of the sum-of-divisors function is identical. □

### 3.2. *Discussion*

The crux of the argument is that we are given an arithmetic function $\alpha$ for which, there is $q_n > 1$ so that if $f, g \in M_n$ are both squarefree, then $\alpha(f) = \alpha(g)$ is equivalent to $f$ and $g$ have the same cycle structure:

$$\alpha(f) = \alpha(g) \leftrightarrow \lambda(f) = \lambda(g), \quad \forall f, g, \in M_n \quad \text{squarefree}, \quad \forall q > q_n.$$

More generally, consider an arithmetic function $\alpha$ such that for squarefree $f, g \in M_n$, satisfies: for $q > q_n$, $\alpha(f) = \alpha(g)$ if and only if $f$ and $g$ have the same cycle structure: $\lambda(f) = \lambda(g)$. Examples are $\varphi, \sigma$, and more generally $\sigma_s(f) = \sum_{d|f} |d|^s$.

For such $\alpha$, given $a_1, \ldots, a_r \in \mathbb{F}_q[T]$ all of degree less than $n$, for all $f \in M_n$ such that $f + a_1 \ldots f + a_r$ are all squarefree, we have

$$\alpha(f + a_1) = \cdots = \alpha(f + a_r) \quad \Leftrightarrow \quad \lambda(f + a_1) = \cdots = \lambda(f + a_r), \quad \forall q > q_n$$

and, therefore,

$$S_\alpha(\overrightarrow{a}; n, q) = S_\varphi(\overrightarrow{a}; n, q) + O_{n,r}(q^{n-1})$$

which makes the argument go through.

## 4. Random permutation theory

In this section, we will prove (1.4) and (1.5). For both, the case $r = 2$ is known and we verify that similar arguments work in general.

### 4.1. *Random permutations with the same number of cycles*

Proposition 4.1

$$E_r(n) \sim \frac{c_r}{(\log n)^{(r-1)/2}}, \quad n \to \infty, \qquad c_r = \frac{1}{(2\pi)^{(r-1)/2}\sqrt{r}}.$$

The case $r = 2$ can be found in the preprint [17].

*Proof.* Let $f_n(t) := \mathrm{E}(e^{it\omega_n})$ be the characteristic function of $\omega_n$, which, by definition, has Fourier expansion

$$f_n(t) = \sum_{k=0}^{\infty} \mathrm{Prob}(\omega_n = k)\, e^{ikt} = \sum G_k(n)\, e^{ikt}.$$

Now note that

$$E_r(n) = (f_n * \ldots * f_n)(0)$$

with convolution given by

$$f * g(x) = \frac{1}{2\pi} \int_{-\pi}^{\pi} f(y)\, g(x-y)\, \mathrm{d}y.$$

Indeed, the convolution has Fourier coefficients

$$\widehat{f * g}(k) = \widehat{f}(k)\, \widehat{g}(k)$$

so that the Fourier expansion of the $r$-fold convolution $f_n * \ldots * f_n$ is

$$f_n * \ldots * f_n(x) = \sum_k G_k(n)^r e^{ikx}$$

whose value at $x = 0$ is $\sum_k n)^r = E_r(n)$.

As $n \to \infty$, $f_n(t)$ is asymptotic to $\left(\text{It is known (see [2, Section 1.1]) that } f_n(t) := \mathrm{E}(e^{it\omega_n}) = \prod_{j=1}^{n} \left(1 - \frac{1}{j} + \frac{e^{it}}{j}\right).\right)$

$$f_n(t) \sim \frac{1}{\Gamma(e^{it})} e^{\log n\,(e^{it}-1)} =: g_{\log n}(t). \tag{4.1}$$

Indeed, we have

$$f_n(t) = \sum_{k=0}^{\infty} \mathrm{Prob}(\omega_n = k)\, e^{ikt} = \sum_{\lambda \vdash n} p(\lambda)\, e^{it\sum_j \lambda_j}$$

and hence the generating function $F(z, t) = \sum_{n \geq 0} f_n(t) z^n$ is given by

$$\begin{aligned} F(z,t) &= \sum_{\lambda} p(\lambda)\, e^{it\sum_j \lambda_j} z^{\sum_j j\lambda_j} = \sum_{\lambda} \prod_j \frac{z^{j\lambda_j} e^{it\lambda_j}}{j^{\lambda_j} \cdot \lambda_j!} \\ &= \prod_{j=1}^{\infty} \sum_{\lambda_j \geq 0} \frac{1}{\lambda_j!} \left(\frac{z^j e^{it}}{j}\right)^{\lambda^j} = \exp \sum_{j=1}^{\infty} \frac{z^j e^{it}}{j} \end{aligned}$$

that is

$$F(z, t) = (1 - z)^{-e^{it}}$$

so that $f_n(t)$ is the $n$th Taylor coefficient of $F(z, t) = (1 - z)^{-e^{it}}$. The $n$th Taylor coefficient of $(1 - z)^{-w}$ is asymptotic to

$$[z^n](1 - z)^{-w} = \frac{\Gamma(n + w)}{\Gamma(w)\Gamma(n + 1)} \sim \frac{n^{w-1}}{\Gamma(w)}, \quad n \to \infty$$

which gives (4.1).

Therefore

$$E_r(n) \sim (g_{\log n} * \ldots * g_{\log n})(0).$$

So we need an asymptotic evaluation, as $L \to \infty$, of the $r$-fold convolution $(g_L * \ldots * g_L)(0)$.

LEMMA 4.2 As $L \to \infty$,

$$(g_L * \ldots * g_L)(0) \sim \frac{c_r}{L^{(r-1)/2}}, \qquad c_r = \frac{1}{(2\pi)^{(r-1)/2}\sqrt{r}}.$$

This will give our claim $E_r(n) \sim \frac{c_r}{(\log n)^{(r-1)/2}}$. □

4.2. *Proof of Lemma* 4.2

We have

$$(g_L * \ldots * g_L)(0) = \frac{1}{(2\pi)^{r-1}} \int_{[-\pi,\pi]^{r-1}} \prod_{j=1}^{r} g_L(t_j)\, \mathrm{d}t_1 \ldots \mathrm{d}t_{r-1},$$

where we set

$$t_r = -(t_1 + \ldots + t_{r-1}).$$

Outside of the cube $\{(\max_j |t_j|) < L^{-0.4}\}$, we have

$$L \max_j (1 - \cos t_j) \gg L^{0.2}$$

and so

$$\left| \prod_{j=1}^{r} g_L(t_j) \right| = \prod_{j=1}^{r} \frac{\mathrm{e}^{-L(1-\cos t_j)}}{|\Gamma(e^{it_j})|} \ll \mathrm{e}^{-cL^{0.2}}$$

is very rapidly decreasing. So we have

$$(g_L * \dots * g_L)(0) \sim \frac{1}{(2\pi)^{r-1}} \int_{(\max_j |t_j|) < L^{-0.4}} \prod_{j=1}^{r} g_L(t_j)\, \mathrm{d}t_1 \dots \mathrm{d}t_{r-1}.$$

For $|t| < L^{-0.4}$ we may write

$$g_L(t) = \frac{1}{\Gamma(e^{it})} e^{L(e^{it}-1)} = e^{iLt - Lt^2/2}(1 + O(L^{-0.2})).$$

Hence, in this small cube,

$$\begin{aligned} &\int_{(\max_j |t_j|) < L^{-0.4}} \prod_{j=1}^{r} g_L(t_j)\, \mathrm{d}t_1 \dots \mathrm{d}t_{r-1} \\ &\quad \sim \int_{(\max_j |t_j|) < L^{-0.4}} e^{iL\sum_j t_j} \mathrm{e}^{-\frac{L}{2}\sum_j t_j^2} \mathrm{d}t_1 \dots \mathrm{d}t_{r-1} \\ &\quad = \int_{(\max_j |t_j|) < L^{-0.4}} \mathrm{e}^{-\frac{L}{2}\sum_j t_j^2} \mathrm{d}t_1 \dots \mathrm{d}t_{r-1} \end{aligned}$$

since $\sum_{j=1}^{r} t_j = 0$.

Changing variables $u = \sqrt{\frac{L}{2}}\ t$ gives

$$\int_{(\max_j |t_j|) < L^{-0.4}} \mathrm{e}^{-\frac{L}{2}\sum_j t_j^2} \mathrm{d}t_1 \dots \mathrm{d}t_{r-1} \sim \left(\sqrt{\frac{2}{L}}\right)^{r-1} \int_{\mathbb{R}^{r-1}} \prod_{j=1}^{r} \mathrm{e}^{-u_j^2} \cdot \mathrm{d}u_1 \dots \mathrm{d}u_{r-1},$$

where $u_r = -(u_1 + \dots + u_{r-1})$. Therefore, we find

$$(g_L * \dots * g_L)(0) \sim \frac{c_r}{L^{(r-1)/2}}$$

with

$$c_r = \frac{(\sqrt{2})^{r-1}}{(2\pi)^{r-1}} \int_{\mathbb{R}^{r-1}} \prod_{j=1}^{r} \mathrm{e}^{-u_j^2}\, \mathrm{d}u_j.$$

It remains to determine the Gaussian integral. This is precisely the $r$-fold convolution of $\mathrm{e}^{-u^2}$ with itself (convolution over $\mathbb{R}$):

$$\int_{\mathbb{R}^{r-1}} \prod_{j=1}^{r} \mathrm{e}^{-u_j^2} du_j = (\mathrm{e}^{-u^2} *_{\mathbb{R}} \dots *_{\mathbb{R}} \mathrm{e}^{-u^2})(0).$$

Using Fourier inversion, this equals

$$(\mathrm{e}^{-u^2} *_{\mathbb{R}} \dots *_{\mathbb{R}} \mathrm{e}^{-u^2})(0) = \int_{-\infty}^{\infty} \widehat{(\mathrm{e}^{-u^2} *_{\mathbb{R}} \dots *_{\mathbb{R}} \mathrm{e}^{-u^2})}(x)\, \mathrm{d}x = \int_{-\infty}^{\infty} (\widehat{\mathrm{e}^{-u^2}}(x))^r\, \mathrm{d}x.$$

Now the Fourier transform of $\mathrm{e}^{-u^2}$ is

$$\widehat{\mathrm{e}^{-u^2}}(x) = \int_{-\infty}^{\infty} \mathrm{e}^{-u^2}\mathrm{e}^{-2\pi i u x}\mathrm{d}u = \sqrt{\pi}\,\mathrm{e}^{-\pi^2 x^2}.$$

Hence,

$$(\mathrm{e}^{-u^2} *_{\mathbb{R}} \ldots *_{\mathbb{R}} \mathrm{e}^{-u^2})(0) = \int_{-\infty}^{\infty} (\sqrt{\pi}\mathrm{e}^{-\pi^2 x^2})^r \,\mathrm{d}x = \pi^{r/2}\int_{-\infty}^{\infty} \mathrm{e}^{-r\pi^2 x^2}\,\mathrm{d}x = \frac{\pi^{(r-1)/2}}{\sqrt{r}}.$$

Thus

$$c_r = \frac{(\sqrt{2})^{r-1}}{(2\pi)^{r-1}}\frac{\pi^{(r-1)/2}}{\sqrt{r}} = \frac{1}{(2\pi)^{(r-1)/2}\sqrt{r}}$$

concluding the proof. □

4.3. *Random permutations with the same cycle structure: Proof of (1.5)*

Let $W_r(n)$ be the probability that $r$ random permutations on $n$ letters have the same cycle structure. Arguing as in [7, Section 4.2] (who treat the case $r = 2$, for which a completely different argument is also given in [3]) shows that

$$W_r(n) \sim \frac{A_r}{n^r}, \quad \text{as } n \to \infty, \tag{4.2}$$

where

$$A_r = \sum_{n=1}^{\infty} W_r(n) = \prod_{k=1}^{\infty} I_r\left(\frac{1}{k^r}\right)$$

with

$$I_r(y) = \sum_{j=0}^{\infty} \frac{y^j}{(j!)^r} = {}_0F_{r-1}(;\underbrace{1,\ldots,1}_{r-1};y)$$

is the generalized hypergeometric function. Thus, we evaluate

$$A_2 = 4.2634, \quad A_3 = 2.59071\ldots, \quad A_4 = 2.23647\ldots$$

Indeed, the generating function of the probability that $r$ random permutations share the same cycle structure is

$$W^{(r)}(z) := \sum_{n\geq 0} W_r(n) z^n = \sum_{n\geq 0}\sum_{\lambda\vdash n} \frac{z^{\lambda_1+2\lambda_2+\cdots}}{\prod_i i^{r\lambda_i}(\lambda_i!)^r} = \prod_{k\geq 1}\left(\sum_{\lambda_k\geq 0}\frac{z^{k\lambda_k}}{k^{r\lambda_k}(\lambda_k!)^r}\right).$$

Thus,

$$W^{(r)}(z) = \prod_{k\geq 1} I_r\left(\frac{z^k}{k^r}\right)$$

with

$$I_r(y) = \sum_{j=0}^{\infty} \frac{y^j}{(j!)^r} = {}_0F_{r-1}(;\underbrace{1,\dots,1}_{r-1}; y).$$

We have

$$H_r(y) \coloneqq \log I_r(y) = \sum_{\ell\geq 1} h_\ell^{(r)} y^\ell = y + O(y^2)$$

and so

$$W^{(r)}(z) = \exp\left(\sum_{k\geq 1} H_r\left(\frac{z^k}{k^r}\right)\right) = \exp\left(\sum_{\ell\geq 1} h_\ell^{(r)} \mathrm{Li}_{r\ell}(z^\ell)\right),$$

where

$$\mathrm{Li}_\nu(z) = \sum_{j\geq 1} \frac{z^j}{j^\nu}$$

is the polylogarithm function.

The expansion converges in the unit disk $|z| < 1$, and the dominant singularity on the unit circle $|z| = 1$ is at $z = 1$, where

$$\mathrm{Li}_r(z) \sim \frac{(-1)^{r-1}}{(r-1)!}(1-z)^{r-1}\log\frac{1}{1-z}, \quad z \to 1^-$$

so that

$$W^{(r)}(z) \sim W^{(r)}(1)\left(1 + \frac{(-1)^{r-1}}{(r-1)!}(1-z)^{r-1}\log\frac{1}{1-z} + \cdots\right), \quad z \to 1^-.$$

By the argument of [7], the $n$th coefficient in the expansion of $W^{(r)}(z)/W^{(r)}(1)$ at $z = 0$ is asymptotic to that of $\frac{(-1)^{r-1}}{(r-1)!}(1-z)^{r-1}\log\frac{1}{1-z}$, which is

$$\frac{(-1)^{r-1}}{(r-1)!}[z^n](1-z)^{r-1}\log\frac{1}{1-z} \sim \frac{1}{n^r}, \quad n \to \infty$$

and hence

$$W_n^{(r)} \sim \frac{W^{(r)}(1)}{n^r}, \quad n \to \infty$$

which is the claimed result. □

## Funding

The research of Z.R. was supported by the European Research Council under the European Union's Seventh Framework Programme (FP7/2007-2013)/ERC grant agreement no. 320755, and from the Israel Science Foundation (Grant no. 925/14). Research of R.P. supported by ISF Grant 861/15 and by ERC starting Grant 678520 (Local Order).

## Acknowledgements

We thank Julio Andrade and Ofir Gorodetsky for discussions on the subject of the paper.

## References

1. J. C. Andrade, L. Bary-Soroker and Z. Rudnick, *Shifted convolution and the Titchmarsh divisor problem over* $\mathbb{F}_q[t]$, *Philos. Trans. A* **373** (2015), 20140308. 18 pp. correction in Philos. Trans. A 374 (2016), no. 2060, 20150360.
2. R. Arratia, A. D. Barbour and S. Tavare, Logarithmic combinatorial structures: a probabilistic approach, E.M.S. Monographs, 2003.
3. S. R. Blackburn, J. R. Britnell and M. Wildon, The probability that a pair of elements of a finite group are conjugate, *J. Lond. Math. Soc. (2)* **86** (2012), 755–778.
4. P. Erdős and L. Mirsky, The distribution of values of the divisor function d(n), *Proc. Lond. Math. Soc.* **3** (1952), 257–271.
5. P. Erdős, C. Pomerance and A. Sarkőzy, On locally repeated values of certain arithmetic functions. II, *Acta Math. Hungar.* **49** (1987), 251–259.
6. P. Erdős, C. Pomerance and A. Sarkőzy, On locally repeated values of certain arithmetic functions. III, *Proc. Amer. Math. Soc.* **101** (1987), 1–7.
7. P. Flajolet, E. Fusy, X. Gourdon, D. Panario and N. Pouyanne, A hybrid of Darboux's method and singularity analysis in combinatorial asymptotics, *Electr. J. Comb.* **13** (2006), 103.
8. D. A. Goldston, S. W. Graham, J. Pintz and C. Y. Yildirim, Small gaps between almost primes, the parity problem, and some conjectures of Erdős on consecutive integers, *Int. Math. Res. Not.* **7** (2011), 1439–1450.
9. S. W. Graham, J. J. Holt and C. Pomerance, On the Solutions to $\varphi(n) = \varphi(n + k)$, *Number Theory in Progress* **Vol. 2** (Eds. K. Gyory, H. Iwaniec and J. Urbanowicz), de Gruyter, Berlin and New York, 1999, 867–882.
10. D. R. Heath-Brown, The divisor function at consecutive integers, *Mathematika* **31** (1984), 141–149.
11. A. Hildebrand, The divisor function at consecutive integers, *Pac. J. Math.* **129** (1987), 307–319.

**12.** L. Moser, Mathematical notes: some equations involving Euler's totient function, *Amer. Math. Monthly* **56** (1949), 22–23.
**13.** C. G. Pinner, Repeated values of the divisor function, *Q. J. Math.* **48** (1997), 499–502.
**14.** A. Schinzel, *Sur l'équation* $\phi(x+k)=\phi(x)$, *Acta Arith.* **4** (1958), 181–184.
**15.** J.-C. Schlage-Puchta, *The equation* $\omega(n)=\omega(n+1)$, *Mathematika* **50** (2003), 99–101 (2005).
**16.** C. A. Spiro, *The frequency with which an integer-valued, prime-independent, multiplicative or additive function of n divides a polynomial function of n*, Ph.D. Diss., University of Illinois at Urbana-Champaign, 1981.
**17.** H. S. Wilf, *The variance of the Stirling cycle numbers*, 2005. Available at: http://arxiv.org/abs/math/0511428v2.

## Appendix A. Permutations with the same cycle structure by Ron Peled

For integer $n \geq 1$, a vector $\lambda = (\lambda_1, \ldots, \lambda_n)$ of non-negative integers is said to be a *partition of* $n$, denoted $\lambda \vdash n$, if $\sum_{j=1}^{n} j\lambda_j = n$. The cycle structure of a permutation on $n$ letters is the partition of $n$ given by $\lambda = (\lambda_1, \ldots, \lambda_n)$, where $\lambda_j$ is the number of cycles of length $j$.

Let $W_r(n)$ be the probability that $r$ uniformly random and independent permutations on $n$ letters have the same cycle structure. Define also $W_r(0) := 1$. In this section, we prove that

THEOREM A.1 *For* $r \geq 2$ *integer*,

$$W_r(n) \sim \frac{A_r}{n^r}, \quad n \to \infty,$$

*where*

$$A_r := \sum_{m=0}^{\infty} W_r(m).$$

Fix an integer $r \geq 2$. Cauchy's formula says the probability that a uniformly sampled permutation on $n$ letters has cycle structure $\lambda$ is

$$p(\lambda) := \prod_{j=1}^{n} \frac{1}{j^{\lambda_j}\, \lambda_j!} \tag{A.1}$$

so that

$$\sum_{\lambda \vdash n} p(\lambda) = 1 \tag{A.2}$$

and

$$W_r(n) = \sum_{\lambda \vdash n} p(\lambda)^r.$$

We denote by $\omega_n(\lambda)$ the number of cycles in $\lambda$:

$$\omega_n(\lambda) := \sum_j \lambda_j,$$

and by $T(\lambda)$ the length of the longest cycle:

$$T(\lambda) := \max(j\colon \lambda_j \neq 0).$$

For $n \geq 1$, we set

$$L = L(n) := \log_2(2n^3), \qquad a = a(n) := \frac{1}{3}n^{2/3}$$

($\log_2$ is the base 2 logarithm) and from the set of cycle structures $\lambda \vdash n$, we form three subsets:

- $\mathcal{A} = \mathcal{A}(n)$: $\omega_n(\lambda) > L$;
- $\mathcal{B} = \mathcal{B}(n)$: $\omega_n(\lambda) \leq L$ and $n/L \leq T(\lambda) < n - a$;
- $\mathcal{C} = \mathcal{C}(n)$: $n - a \leq T(\lambda) \leq n$.

Further, set

$$\Sigma_{\mathcal{A}} = \Sigma_{\mathcal{A}}(n) := \sum_{\lambda \in \mathcal{A}} p(\lambda)^r$$

and likewise for $\Sigma_{\mathcal{B}}, \Sigma_{\mathcal{C}}$.

We claim that $\mathcal{A} \cup \mathcal{B} \cup \mathcal{C}$ exhausts all cycle structures $\lambda \vdash n$. Indeed, note that $\lambda \vdash n$ means $\sum_j j\lambda_j = n$, and the sum takes place only over $j \leq T(\lambda)$ by definition. Hence,

$$n = \sum_{j=1}^{T(\lambda)} j\lambda_j \leq T(\lambda) \sum_j \lambda_j = T(\lambda)\omega_n(\lambda)$$

so that $T(\lambda) \geq n/\omega_n(\lambda)$. Now if $\lambda \notin \mathcal{A}$, that is $\omega_n(\lambda) \leq L$, then

$$T(\lambda) \geq n/\omega_n(\lambda) \geq n/L$$

so that $\lambda \in \mathcal{B} \cup \mathcal{C}$. Note that we omitted the requirement that $\omega_n(\lambda) \leq L$ from $\mathcal{C}$, so we do not get a disjoint union: $\mathcal{C} \cap \mathcal{A} \neq \varnothing$. Nonetheless, we have

$$\Sigma_{\mathcal{C}} \leq W_r(n) \leq \Sigma_{\mathcal{A}} + \Sigma_{\mathcal{B}} + \Sigma_{\mathcal{C}} \tag{A.3}$$

and we will see that the dominant contribution to $W_r(n)$ for large $n$ will be from $\Sigma_{\mathcal{C}}$.

LEMMA A.1 *For $n \geq 1$,*

$$\Sigma_{\mathcal{A}} \leq \frac{1}{n^{3(r-1)}}.$$

*Proof.* We use, for $\lambda_j \geq 0$, that

$$\frac{1}{j^{\lambda_j}\ \lambda_j!} \leq \frac{2}{2^{\lambda_j}}$$

(where the factor 2 is only needed when $j = 1$ and $1 \le \lambda_1 \le 3$). Therefore,

$$p(\lambda) = \prod_{j=1}^{n} \frac{1}{j^{\lambda_j}\,\lambda_j!} \le 2 \prod_{j=1}^{n} \frac{1}{2^{\lambda_j}} = \frac{2}{2^{\omega_n(\lambda)}},$$

from which we deduce, using (A.2) and the definition of $L$, that

$$\begin{aligned}\Sigma_{\mathcal{A}} &= \sum_{\substack{\lambda \vdash n \\ \omega_n(\lambda) > L}} p(\lambda)^r \\ &\le \sum_{\substack{\lambda \vdash n \\ \omega_n(\lambda) > L}} p(\lambda) \left(\frac{2}{2^{\omega_n(\lambda)}}\right)^{r-1} \\ &\le \left(\frac{2}{2^L}\right)^{r-1} \sum_{\lambda \vdash n} p(\lambda) = \left(\frac{2}{2^L}\right)^{r-1} = \frac{1}{n^{3(r-1)}}.\end{aligned}$$

□

LEMMA A.2 *For $n \ge 1$,*

$$\Sigma_{\mathcal{C}} = \sum_{0 \le m \le a} \frac{1}{(n-m)^r} W_r(m).$$

*Proof.* Note that for $\lambda \in \mathcal{C}$, if $t = T(\lambda) \ge n - a$, then since $a < n/2$ there is a *unique* cycle of length $t$. Thus

$$\lambda = (\hat{\lambda}, \overbrace{1}^{\text{position } t}, 0, \ldots)$$

with $\hat{\lambda}$ a partition of $n - t$, and then $p(\lambda) = p(\hat{\lambda}) \cdot \frac{1}{t}$ by Cauchy's formula (A.1) (where for $t = n$, $\hat{\lambda}$ is empty and we define $p(\hat{\lambda}) := 1$). Hence,

$$\begin{aligned}\Sigma_{\mathcal{C}} &= \sum_{n-a \le t \le n} \sum_{\substack{\lambda \in \mathcal{C} \\ T(\lambda) = t}} p(\lambda)^r \\ &= \sum_{n-a \le t \le n} \frac{1}{t^r} \sum_{\hat{\lambda} \vdash n-t} p(\hat{\lambda})^r \\ &= \sum_{n-a \le t \le n} \frac{1}{t^r} W_r(n-t)\end{aligned}$$

(recalling that $W_r(0) = 1$). Changing variables to $m = n - t$ gives our statement. □

We next want to use induction to give upper bounds for $W_r(n)$ and an asymptotic bound for $\Sigma_{\mathcal{B}}$.

LEMMA A.3 *There is a constant $C_r > 0$ so that for all $n \ge 1$,*

$$W_r(n) \le \frac{C_r}{n^r}. \tag{A.4}$$

*In addition*

$$\Sigma_{\mathcal{B}} = o\left(\frac{1}{n^r}\right) \quad \text{as } n \to \infty. \tag{A.5}$$

*Proof.* Fix an integer $N_r \geq 1$ for which (recalling that $r \geq 2$)

$$\sum_{m=N_r}^{\infty} \frac{1}{m^r} \leq \frac{1}{6} \cdot \left(\frac{2}{3}\right)^r \quad \text{and} \quad \sup_{k \geq N_r} \frac{(3L(k))^r}{k^{\frac{2}{3}r-1}} \leq \frac{1}{3}. \tag{A.6}$$

Let $C_r > 0$ be a sufficiently large constant, satisfying several lower bounds imposed below. We take $C_r \geq (N_r)^r$ so that (A.4) is satisfied for $1 \leq n \leq N_r$, as $W_r(n) \leq 1$ for all $n$.

Let $k > N_r$ and assume by induction that (A.4) holds with $1 \leq n < k$. We proceed to establish (A.4) with $n = k$. To this end, we first give upper bounds for $\Sigma_{\mathcal{A}}(k)$, $\Sigma_{\mathcal{B}}(k)$ and $\Sigma_{\mathcal{C}}(k)$.

By Lemma A.1, using that $3(r-1) > r$ and taking $C_r \geq 3$,

$$\Sigma_{\mathcal{A}}(k) \leq \frac{1}{k^{3(r-1)}} \leq \frac{1}{3}\frac{C_r}{k^r}. \tag{A.7}$$

For $\lambda \in \mathcal{B}(k)$, such that $T(\lambda) = t$, note that since $\lambda_t \geq 1$,

$$\frac{1}{t^{\lambda_t}\,\lambda_t!} \leq \frac{1}{t} \cdot \frac{1}{t^{\lambda_t - 1}\,(\lambda_t - 1)!}$$

and then by Cauchy's formula (A.1),

$$p(\lambda) = \prod_{j=1}^{t-1} \frac{1}{j^{\lambda_j}\,\lambda_j!} \cdot \frac{1}{t^{\lambda_t}\,\lambda_t!} \leq \frac{1}{t} \cdot \left(\prod_{j=1}^{t-1} \frac{1}{j^{\lambda_j}\,\lambda_j!}\right) \cdot \frac{1}{t^{\lambda_t - 1}\,(\lambda_t - 1)!} = \frac{1}{t} p(\tilde{\lambda}),$$

where $\tilde{\lambda} = (\lambda_1, \ldots, \overbrace{\lambda_t - 1}^{t}, 0, \ldots)$ is a partition of $k - t$. Hence

$$\begin{aligned}
\Sigma_{\mathcal{B}}(k) &= \sum_{\frac{k}{L} \leq t < k-a} \sum_{\substack{\lambda \in \mathcal{B} \\ T(\lambda) = t}} p(\lambda)^r \\
&\leq \sum_{\frac{k}{L} \leq t < k-a} \frac{1}{t^r} \sum_{\tilde{\lambda} \vdash k-t} p(\tilde{\lambda})^r \\
&= \sum_{\frac{k}{L} \leq t < k-a} \frac{1}{t^r} W_r(k-t).
\end{aligned}$$

Using the induction hypothesis for $n = k - t$, we obtain

$$\begin{aligned}
\Sigma_{\mathcal{B}}(k) &\leq \sum_{\frac{k}{L(k)} \leq t < k - a(k)} \frac{1}{t^r} \frac{C_r}{(k-t)^r} \\
&\leq C_r\, k \left(\frac{L(k)}{k\, a(k)}\right)^r = \frac{C_r}{k^r} \frac{(3L(k))^r}{k^{\frac{2}{3}r-1}} \leq \frac{1}{3}\frac{C_r}{k^r},
\end{aligned} \tag{A.8}$$

where we substituted the definition of $a(k)$ and applied (A.6).

Next, using Lemma A.2,

$$\Sigma_{\mathcal{C}}(k) \le \frac{1}{(k-a)^r} \sum_{0\le m\le a} W_r(m) \le \left(\frac{3}{2k}\right)^r \left(N_r + \sum_{N_r\le m\le a} \frac{C_r}{m^r}\right),$$

where we used the fact that $W_r(m) \le 1$ for all $m$ and the induction hypothesis for $N_r \le n = m \le a$. Applying (A.6) and taking $C_r \ge 6\left(\frac{3}{2}\right)^r N_r$, we conclude that

$$\Sigma_{\mathcal{C}}(k) \le \left(\frac{3}{2k}\right)^r \left(N_r + \frac{1}{6}\left(\frac{2}{3}\right)^r C_r\right) \le \frac{1}{3}\frac{C_r}{k^r}. \tag{A.9}$$

Finally, applying (A.3) and substituting (A.7), (A.8) and (A.9), we conclude that

$$W_r(k) \le \Sigma_{\mathcal{A}}(k) + \Sigma_{\mathcal{B}}(k) + \Sigma_{\mathcal{C}}(k) \le \frac{C_r}{k^r},$$

finishing the proof by induction of (A.4).

To see (A.5), note that as the bound (A.8) is now verified for all large $k$ and as $r \ge 2$, we have

$$\Sigma_{\mathcal{B}}(k) \le \frac{C_r}{k^r}\frac{(3L(k))^r}{k^{\frac{2}{3}r-1}} = o\left(\frac{1}{k^r}\right) \quad \text{as } k \to \infty. \qquad \square$$

We are now in position to obtain the asymptotics of $\Sigma_{\mathcal{C}}$:

$$\Sigma_{\mathcal{C}} \sim \frac{A_r}{n^r}, \qquad A_r = \sum_{m=0}^{\infty} W_r(m). \tag{A.10}$$

Indeed, by Lemma A.2,

$$\Sigma_{\mathcal{C}} = \sum_{0\le m\le a} \frac{1}{(n-m)^r} W_r(m) \sim \frac{1}{n^r} \sum_{0\le m\le a} W_r(m)$$

since $(n-m)^r \sim n^r$ uniformly for $0 \le m \le a = o(n)$. We now extend the sum, using our upper bound (A.4) and the fact that $a(n) \to \infty$, and obtain (A.10).

We can now prove Theorem A.1: by (A.3),

$$W_r(n) = \Sigma_{\mathcal{C}} + O(\Sigma_{\mathcal{A}} + \Sigma_{\mathcal{B}}) \sim \frac{A_r}{n^r}$$

using (A.10), Lemma A.1 (recalling that $r \ge 2$ so that $3(r-1) > r$) and (A.5).