# A limit theorem for the six-length of random functional graphs with a fixed degree sequence

Kevin Leckey* and Nicholas Wormald†

School of Mathematical Sciences
Monash University
VIC 3800, Australia

kevin.leckey@tu-dortmund.de, nicholas.wormald@monash.edu

Submitted: Mar 7, 2018; Accepted: Sep 9, 2019; Published: Nov 22, 2019


**Abstract**

We obtain results on the limiting distribution of the six-length of a random functional graph, also called a functional digraph or random mapping, with given in-degree sequence. The six-length of a vertex $v \in V$ is defined from the associated mapping, $f : V \to V$, to be the maximum integer $i$ such that the elements $v, f(v), \ldots, f^{i-1}(v)$ are all distinct. This has relevance to the study of algorithms for integer factorisation.

**Mathematics Subject Classifications:** 05C80, 12Y05, 05C05, 60C05

## 1 Introduction

We consider random directed graphs with all out-degrees equal to 1, which we call *functional graphs* (see Section 2 for further notation) or random mappings. The motivation in most of the related literature is a better understanding of Pollard's $\rho$-algorithm [9] for integer factorisation, or the improved version by Brent and Pollard [3]. The runtime depends on the six-length (also called $\rho$-length) of a polynomial in $\mathbb{F}_p[x]$. (Pollard's first version used $x^2 - 1$.) Under the assumption that a polynomial mod $p$ 'behaves like' a random mapping (supported by some research listed below), we are interested in the six-length of random mappings. Martins and Panario [8] studied polynomials in $\mathbb{F}_p[x]$, in particular the six-length in several random models. They found significance in the six-length of random polynomials with given in-degree sequence, and gave numerical results for several random models. Our main aim is to derive results on the six-length of random

*Current address: Fakultät Statistik, Technische Universität Dortmund, Germany.
†Supported by an ARC Australian Laureate Fellowship.

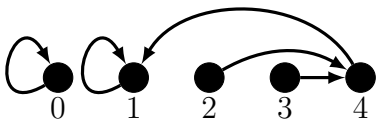
functional graphs with given in-degree sequence, to give a baseline for comparison with random polynomial models.

For standard models of random mappings, much is already known about random variables such as the ones mentioned above. An early paper by Harris [6] studies four basic models. Results pertinent to our study (i.e. with restrictions on the in-degree sequence) were obtained by Arney and Bender [1], who were motivated by the study of random shift registers. For a fixed set $\mathcal{D}$, they considered a functional graph chosen uniformly at random among those with in-degrees in $\mathcal{D}$. They studied various properties such as the in-degrees of vertices, tree size, tail length and six-length. They also obtained some information on the number of origins (vertices of in-degree 0), stopping short of being able to specify the number of origins. More recently, Hansen and Jaworski [4, 5] considered a two-stage experiment: (1) choose random in-degrees $D_1, \ldots, D_n$ from an exchangeable probability distribution, (2) choose a functional graph at random among graphs with in-degrees $D_1, \ldots, D_n$. They studied the number of cyclic vertices (vertices lying on a cycle) and of components, and component sizes, and predecessors and successors. Our model with specific in-degree frequencies can be cast into their general framework, however specific asymptotic distributions are only obtained in [4, 5] for two special distributions, relating to preferential and anti-preferential attachment.

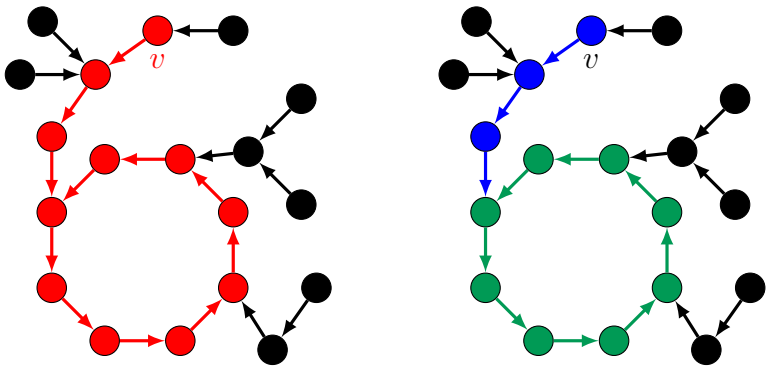
Our main results are stated in Section 2 after some basic definitions. In particular we give the limiting distribution of the six-length for functional graphs with given in-degree sequence, and also asymptotics for the moments of the distribution, as well as the joint distribution of the tail- and six-lengths. Proofs for the case that the second moment of the in-degree sequence is "large" are given in Section 3, and for the remaining case (except for some almost trivial cases) in Section 4. See also Konyagin, Luca, Mans, Mathieson, Sha and Shparlinski [7] for a study of polynomials over finite fields considering similar aspects, such as largest component and tree size of the associated functional digraphs. Similar to [8], they observe, in [7, Section 4], that the in-degree sequence of these random digraphs is distributed rather differently from that of uniformly random functional digraphs.

## 2 Definitions, model and results

**Functional Graphs.** The functional graph of a function $f : V \to V$ is a directed graph $\mathcal{G}_f$ with vertex set $V$ and edge set $\{(v, f(v)) : v \in V\}$. Consider, for example, the vertex set $V = \{0, \ldots, 4\}$ and the function $f(x) = x^2 \pmod 5$. Then $\mathcal{G}_f$ is given by




The six-length of a vertex in a functional graph is defined as follows: Let $f : V \to V$ be a function and let $id$ denote the identity function on $V$. Let $f^k$ denote the $k$-times




(a) $\mathfrak{s}(v) = 11$ (b) $\mathfrak{t}(v) = 3$, $\mathfrak{c}(v) = 8$

Figure 1: An illustration of the six-, tail-, and cycle-length.

composition of $f$, that is $f^0 = id$ and $f^k = f^{k-1} \circ f$ for $k \geqslant 1$. The *six-length* of $v \in V$ is defined as

$$\mathfrak{s}_f(v) = \min\left\{k \in \mathbb{N} : f^k(v) \in \{f^j(v) : 0 \leqslant j \leqslant k-1\}\right\}.$$

This counts all successors of $v$, together with $v$. An example for the six-length in a functional graph is given in Fig. 1(a). Note that $\mathfrak{s}_f(v)$ can be decomposed into the tail-length $\mathfrak{t}_f(v)$ and the cycle-length $\mathfrak{c}_f(v)$ as indicated in Fig. 1(b). More formally, the tail-length is the unique integer that satisfies

$$\mathfrak{t}_f(v) < \mathfrak{s}_f(v) \quad \text{and} \quad f^{\mathfrak{s}_f(v)}(v) = f^{\mathfrak{t}_f(v)}(v),$$

(and is also known as the height of $v$) and the cycle-length is given by $\mathfrak{c}_f(v) := \mathfrak{s}_f(v) - \mathfrak{t}_f(v)$, i.e. the length of the cycle in the component of the graph containing $v$.

**Random Model.** Throughout the paper, a (finite) sequence $\mathbf{d}_n = (d_{n,1}, \ldots, d_{n,n})$ is called degree sequence if

$$\sum_{j=1}^{n} d_{n,j} = n \quad \text{and} \quad \mathbf{d}_n \in \mathbb{N}_0^n. \tag{A0}$$

A random functional graph with degree sequence $\mathbf{d}_n$ is a graph $\mathcal{G}_F$ where $F$ is drawn uniformly at random from the set

$$\mathfrak{F}(\mathbf{d}_n) := \left\{f : [n] \to [n] : |f^{-1}(\{i\})| = d_{n,i} \text{ for all } i \in [n]\right\}. \tag{1}$$

Here and elsewhere, we use $[n] := \{1, \ldots, n\}$. Note that technically what we call the degree sequence is the in-degree sequence of the directed graph. This simplification is sensible because all outdegrees are 1.

Now let $\{\mathbf{d}_n : n \in \mathbb{N}\}$ be a family of degree sequences. Let $\mathfrak{s}_n(v)$ and $\mathfrak{t}_n(v)$ be six- and tail-length of a vertex $v \in [n]$ in a random functional graph with degree sequence $\mathbf{d}_n$. The aim of this paper is to investigate the asymptotic behaviour of $(\mathfrak{s}_n(v), \mathfrak{t}_n(v))$.

We use the usual asymptotic notation such as $\mathrm{O}, \Omega, \Theta, o, \omega, \sim$; in particular $a_n = \omega(b_n)$ if $b_n = o(a_n)$. Also, for any positive integers $n, k \in \mathbb{N}$ with $k \leqslant n$ let

$$\langle n \rangle_k := n!/(n-k)!\,.$$

**Degree sequences.** For a degree sequence $\mathbf{d}_n = (d_{n,1}, \ldots, d_{n,n})$ let

$$\Delta(\mathbf{d}_n) := \max_j d_{n,j}, \quad m_k(\mathbf{d}_n) := \sum_{j=1}^{n} d_{n,j}^k, \quad \sigma^2(\mathbf{d}_n) := \frac{m_2(\mathbf{d}_n)}{n} - 1. \tag{2}$$

The parameter $\sigma^2(\mathbf{d}_n)$ is sometimes called the *coalescence*.

Throughout this section, let $\{\mathbf{d}_n : n \in \mathbb{N}\}$ be a family of degree sequences and let $\{v_n : n \in \mathbb{N}\}$ be a family of vertices with $v_n \in [n]$. For the upcoming limit theorem for $\mathfrak{s}_n(v_n)$ we assume the following:

$$\sigma^2(\mathbf{d}_n) = o(n) \quad \text{and} \quad \sigma^2(\mathbf{d}_n) = \omega\left(n^{-1}\right), \tag{A1}$$

$$\Delta(\mathbf{d}_n) = o\left(\sqrt{n\sigma^2(\mathbf{d}_n)}\right), \tag{A2}$$

**Theorem 1.** *Assume* (A0), (A1) *and* (A2). *Then* $\left(\mathfrak{s}_n(v_n)/\sqrt{n/\sigma^2(\boldsymbol{d}_n)}\right)_{n\geqslant 1}$ *converges weakly to the standard Rayleigh distribution, that is*

$$\lim_{n\to\infty} \mathbb{P}\left(\mathfrak{s}_n(v_n) > x\sqrt{n/\sigma^2(\boldsymbol{d}_n)}\right) = \mathrm{e}^{-x^2/2}, \quad x > 0.$$

In fact the methods used to prove Theorem 1 also yield the convergence of all moments for a wide range of degree sequences. More precisely, let

$$\sigma^2(\mathbf{d}_n) = o\left(\frac{n}{(\log n)^3}\right) \quad \text{and} \quad \sigma^2(\mathbf{d}_n) = \omega\left(n^{-1}\right), \tag{B1}$$

$$\Delta(\mathbf{d}_n) = o\left(\sqrt{\frac{n\sigma^2(\mathbf{d}_n)}{(\log n)^3}}\right). \tag{B2}$$

Then the convergence in Theorem (1) also holds with respect to all moments, that is:

**Theorem 2.** *Assume* (A0), (B1) *and* (B2). *Let $X$ be standard Rayleigh distributed. Then*

$$\lim_{n\to\infty} \mathbb{E}\left[\left(\frac{\mathfrak{s}_n(v_n)}{\sqrt{n/\sigma^2(\boldsymbol{d}_n)}}\right)^p\right] = \mathbb{E}[X^p], \quad p \geqslant 1.$$

*In particular,* $\mathbb{E}[\mathfrak{s}_n(v_n)] \sim \sqrt{\frac{\pi n}{2\sigma^2(\boldsymbol{d}_n)}}$ *and* $\mathrm{Var}(\mathfrak{s}_n(v_n)) \sim \frac{4-\pi}{2\sigma^2(\boldsymbol{d}_n)} n$.

Moreover, these assumptions also imply that the ratio between tail-length and six-length is asymptotically uniformly distributed. More precisely:

**Theorem 3.** *Let $X$ and $U$ be independent, $U$ be uniformly distributed on $[0,1]$, and $X$ be Rayleigh distributed. Assume* (A0), (B1) *and* (B2). *Then*

$$\left(\frac{\mathfrak{s}_n(v_n)}{\sqrt{n/\sigma^2(\boldsymbol{d}_n)}}, \frac{\mathfrak{t}_n(v_n)}{\sqrt{n/\sigma^2(\boldsymbol{d}_n)}}\right) \xrightarrow{d} (X, UX).$$

*Remark* 4. A combination of Theorem 2 and Theorem 3 yields

$$\mathbb{E}[\mathfrak{t}_n(v_n)] \sim \sqrt{\frac{\pi n}{8\sigma^2(\mathbf{d}_n)}} \quad \text{and} \quad \mathbb{E}[\mathfrak{c}_n(v_n)] \sim \sqrt{\frac{\pi n}{8\sigma^2(\mathbf{d}_n)}}.$$

These results support a conjecture by Brent and Pollard [3, Section 3] on the typical tail- and cycle-length of polynomials mod $p$.

## 3 Proofs for sequences with large coalescence

We first prove all Theorems under the additional assumption

$$\sigma^2(\mathbf{d}_n) = \omega\left(\frac{\log n}{n^{1/3}}\right). \tag{A+}$$

Cases with $\sigma^2(\mathbf{d}_n) = \mathrm{O}\left(\log n/n^{1/3}\right)$ will be discussed in Section 4.

Throughout this section we omit the dependence on $\mathbf{d}_n$ in the notation. In particular

$$\Delta := \Delta(\mathbf{d}_n), \quad m_j := m_j(\mathbf{d}_n), \quad \sigma^2 := \sigma^2(\mathbf{d}_n).$$

Moreover, we also omit the dependence on $n$ in the notation of the degrees, that is

$$(d_1, \dots, d_n) := (d_{n,1}, \dots, d_{n,n}).$$

Unless stated otherwise, $n$ is a positive integer and asymptotic results are as $n \to \infty$. Condition (A0) is the only condition assumed throughout the section. All other assumptions are stated in the lemmas separately.

### 3.1 Limit theorem for the six-length

This section contains the proof of Theorem 1 for degree sequences that additionally satisfy (A+), that is we prove the following statement:

**Proposition 5.** *Assume* (A0), (A1), (A2) *and* (A+). *Then*

$$\lim_{n\to\infty} \mathbb{P}\left(\mathfrak{s}_n(v_n) > x\sqrt{n/\sigma^2(\boldsymbol{d}_n)}\right) = \mathrm{e}^{-x^2/2}, \quad x > 0.$$

The proof of is based on the following explicit formula for the probabilities. In fact, the formula below remains valid even without making any assumptions on the degree sequence other than (A0). Note that our method for deriving these basic explicit results on probabilitesis standard in random graph theory and similar to what was used for the foundation results in similar studies such as [4, 5].

**Lemma 6.** *For every $n \geqslant 2$ and $v \in [n]$*

$$\mathbb{P}(\mathfrak{s}_n(v) > k) = \frac{1}{\langle n \rangle_k} \sum_{(i_1,\dots,i_k) \in J_{n,k}(v)} \prod_{j=1}^{k} d_{i_j}, \quad 1 \leqslant k \leqslant n-1,$$

*with $\langle n \rangle_k = \prod_{j=0}^{k-1}(n-j)$ and $J_{n,k}(v) = \{(j_1,\dots,j_k) \in ([n] \setminus \{v\})^k : j_\ell \neq j_m \text{ for } \ell \neq m\}$.*

*Proof.* Recall that $F$ denotes a function drawn uniformly at random from the set $\mathfrak{F}(\mathbf{d}_n)$ defined in (1). Note that $J_{n,k}(v)$ corresponds to the set of all possible non-self-intersecting $k$-paths starting at $v$. Thus, we have

$$\mathbb{P}(\mathfrak{s}_n(v) > k) = \sum_{J \in J_{n,k}(v)} \mathbb{P}\left(\left(F(v),\dots,F^{(k)}(v)\right) = J\right).$$

The probability on the right hand side can be derived by counting the functions in $\mathfrak{F}(\mathbf{d}_n)$ that lead to the path $J$. Since $J$ determines the images of exactly $k$ elements to be $i_1,\dots,i_k$, there are

$$\frac{(n-k)!}{\prod_{\ell \notin \{i_1,\dots,i_k\}} d_\ell! \prod_{j=1}^{k}(d_{i_j}-1)!}$$

possible ways to choose the remaining images. The assertion follows after dividing by the total number $n!/\prod_{\ell=1}^{n} d_\ell!$ of elements in $\mathfrak{F}(\mathbf{d}_n)$. □

**Lemma 7.** *Let $g_n : [n] \to [0,\infty)$ be defined as*

$$g_n(k) = \frac{k!}{\langle n \rangle_k} \sum_{i_1 < \cdots < i_k} \prod_{j=1}^{k} d_{i_j}$$

*where the summation is taken over all $(i_1,\dots,i_k) \in [n]^k$ with $i_1 < \cdots < i_k$. Then*

$$\mathbb{P}(\mathfrak{s}_n(v) > k) = g_n(k) - \frac{k d_v}{n-k+1} \mathbb{P}(\mathfrak{s}_n(v) > k-1), \quad k \geqslant 2,\ v \in [n].$$

*Proof.* Let $\widetilde{J}_k = \{(j_1,\dots,j_k) \in [n]^k : j_\ell \neq j_m \text{ for } \ell \neq m\}$. Lemma 6 implies

$$\mathbb{P}(\mathfrak{s}_n(v) > k) = \frac{1}{\langle n \rangle_k} \sum_{(i_1,\dots,i_k) \in \widetilde{J}_k} \prod_{j=1}^{k} d_{i_j} - \frac{1}{\langle n \rangle_k} \sum_{(i_1,\dots,i_k) \in \widetilde{J}_k \setminus J_{n,k}(v)} \prod_{j=1}^{k} d_{i_j}. \tag{3}$$

The first term equals $g_n(k)$ by matching vectors with equal order statistics. For the second sum note that

$$\widetilde{J}_k \setminus J_{n,k}(v) = \bigcup_{j=1}^{k} \left\{(i_1,\dots,i_k) \in [n]^k : i_j = v, (i_1,\dots,i_{j-1},i_{j+1},\dots,i_k) \in J_{n,k-1}(v)\right\}.$$

Hence,

$$\sum_{(i_1,\dots,i_k)\in\widetilde{J}_k\setminus J_{n,k}(v)}\prod_{j=1}^{k}d_{i_j}=kd_v\sum_{(i_1,\dots,i_{k-1})\in J_{n,k-1}(v)}\prod_{j=1}^{k-1}d_{i_j}$$

and the assertion follows from Lemma 6. □

Note that the previous Lemma in particular yields the following bounds:

$$\frac{n-k}{n-k+(k+1)d_v}g_n(k+1)\leqslant\mathbb{P}(\mathfrak{s}_n(v)>k)\leqslant\frac{n-k+1}{n-k+1+kd_v}g_n(k). \tag{4}$$

Thus we can focus on the asymptotic behaviour of $g_n(k)$ for $k=\Theta(\sqrt{n/\sigma^2})$ instead. However, since we need some large deviation bounds in later proofs, we formulate the following lemmas so as to cover a wider range for $k$ than necessary for Theorem 5.

The first step is to transform the sum in $g_n(k)$ into a probability that is covered by Poission approximation. To this end let

$$\alpha=\alpha(n,k)=\frac{k}{n}.$$

Then $g_n(k)$ can be rewritten as follows:

$$g_n(k)=\frac{k!}{\langle n\rangle_k\alpha^k}\prod_{j=1}^{n}(\alpha d_j+1)\sum_{i_1<\dots<i_k}\prod_{j=1}^{k}\frac{\alpha d_{i_j}}{\alpha d_{i_j}+1}\prod_{\ell\in[n]\setminus\{i_1,\dots,i_k\}}\frac{1}{\alpha d_\ell+1}. \tag{5}$$

Now let $B_n$ be binomially $B(n,\alpha)$ distributed. Moreover, let $X_1,\dots,X_n$ be independent, Bernoulli distributed random variables with $\mathbb{P}(X_i=1)=\alpha d_{i_j}/(\alpha d_{i_j}+1)$ and let $S_n=X_1+\cdots+X_n$. Then (5) yields

$$g_n(k)=(1-\alpha)^{n-k}\prod_{j=1}^{n}(\alpha d_j+1)\frac{\mathbb{P}(S_n=k)}{\mathbb{P}(B_n=k)}. \tag{6}$$

**Lemma 8.** *Let $\lambda=\mathbb{E}[S_n]$, that is*

$$\lambda=\sum_{j=1}^{n}\frac{\alpha d_j}{\alpha d_j+1}$$

*with $\alpha=k/n$. Moreover, let $x\wedge y=\min\{x,y\}$. Then*

$$\lambda=k-\frac{k^2m_2}{n^2}+\mathrm{O}\left(\frac{k^3m_3}{n^3}\wedge\frac{k^2m_2}{n^2}\right).$$

*In particular, $\lambda-k=\mathrm{O}\left(k^2m_2/n^2\right)$.*

*Proof.* Note that for $x \geqslant 0$

$$\frac{x}{x+1} = x - x^2 + \frac{x^3}{x+1} = x - x^2 + \mathrm{O}(x^3 \wedge x^2).$$

Using this bound in the definition of $\lambda$ yields the assertion. □

Next we apply Chen-Stein Poisson approximation to obtain the following result:

**Lemma 9.** *Let $\lambda$ be as in the previous lemma. Then, for $k = o\left((n^2/m_2)^{2/3}\right)$,*

$$g_n(k) = (1-\alpha)^{n-k} \left( \prod_{j=1}^{n} (\alpha d_j + 1) \right) \mathrm{e}^{k-\lambda} \left( \frac{\lambda}{k} \right)^k \left( 1 + \mathrm{O}\left( \frac{k^{3/2} m_2}{n^2} \right) \right).$$

*Proof.* A standard Chen-Stein bound for Poisson approximation, such as in Barbour, Holst and Janson [2, Equation (1.23)], implies

$$\left| \mathbb{P}(S_n = k) - \mathrm{e}^{-\lambda} \frac{\lambda^k}{k!} \right| \leqslant \frac{1}{\lambda} \sum_{j=1}^{n} \left( \frac{\alpha d_j}{\alpha d_j + 1} \right)^2 \leqslant \frac{\alpha^2 m_2}{\lambda} = \frac{k^2 m_2}{\lambda n^2},$$

$$\left| \mathbb{P}(B_n = k) - \mathrm{e}^{-k} \frac{k^k}{k!} \right| \leqslant \frac{n}{k} \alpha^2 = \frac{k}{n}.$$

It only remains to transform these into relative error bounds. Note that Stirling's approximation yields

$$\mathrm{e}^{-k} \frac{k^k}{k!} = \Theta\left( \frac{1}{\sqrt{k}} \right), \qquad \mathrm{e}^{-\lambda} \frac{\lambda^k}{k!} = \Theta\left( \frac{\mathrm{e}^{k-\lambda}}{\sqrt{k}} \left( \frac{\lambda}{k} \right)^k \right).$$

As formally shown in Lemma 10 below, $\mathrm{e}^{k-\lambda}(\lambda/k)^k = 1 + o(1)$. Hence, since Lemma 8 implies $\lambda \sim k$,

$$\mathbb{P}(S_n = k) = \mathrm{e}^{-\lambda} \frac{\lambda^k}{k!} \left( 1 + \mathrm{O}\left( \frac{k^{3/2} m_2}{n^2} \right) \right),$$

$$\mathbb{P}(B_n = k) = \mathrm{e}^{-k} \frac{k^k}{k!} \left( 1 + \mathrm{O}\left( \frac{k^{3/2}}{n} \right) \right).$$

Therefore (6) implies the assertion. □

**Lemma 10.** *Let $k = o\left((n^2/m_2)^{2/3}\right)$. Then $\mathrm{e}^{k-\lambda} (\lambda/k)^k = 1 + \mathrm{O}\left(k^3 m_2^2 / n^4\right)$.*

*Proof.* First note that $k - \lambda = \mathrm{O}(k^2 m_2 / n^2)$ by Lemma 8. In particular $k - \lambda = o(\sqrt{k})$ by assumption on $k$. Hence, since $\log(1-x) = -x + \mathrm{O}(x^2)$ as $x \to 0$,

$$\frac{\lambda}{k} = \exp\left( -\frac{k-\lambda}{k} + \mathrm{O}\left( \frac{(k-\lambda)^2}{k^2} \right) \right).$$

Thus

$$\mathrm{e}^{k-\lambda}\left(\frac{\lambda}{k}\right)^k = \exp\left(\mathrm{O}\left(\frac{(k-\lambda)^2}{k}\right)\right)$$

and the assertion follows using the above bound on $k-\lambda$. □

**Lemma 11.** *Assume* $k = o\left((n^2/m_2)^{2/3} \wedge (n^3/m_3)^{1/3}\right)$. *Then*

$$g_n(k) = \exp\left(-\frac{k^2\sigma^2}{2n}\right)\left(1 + \mathrm{O}\left(\frac{k^{3/2}m_2}{n^2} + \frac{k^3 m_3}{n^3}\right)\right).$$

*Proof.* First note that Lemmas 9 and 10 yield

$$g_n(k) = (1-\alpha)^{n-k}\left(\prod_{j=1}^{n}(\alpha d_j + 1)\right)\left(1 + \mathrm{O}\left(\frac{k^{3/2}m_2}{n^2}\right)\right). \tag{7}$$

By expanding $\log(1+x)$ and using $\alpha = k/n$ we find

$$(1-\alpha)^{n-k} = \exp\left(-\alpha(n-k) - \frac{\alpha^2(n-k)}{2} + \mathrm{O}\left(\alpha^3 n\right)\right) = \exp\left(-k + \frac{k^2}{2n} + \mathrm{O}\left(\frac{k^3}{n^2}\right)\right)$$

and

$$\prod_{j=1}^{n}(\alpha d_j + 1) = \exp\left(k - \frac{k^2 m_2}{2n^2} + \mathrm{O}\left(\frac{k^3 m_3}{n^3}\right)\right).$$

Hence the assertion follows from (7) and $\sigma^2 = m_2/n - 1$, noting that the error term tends to 0. □

As a last step before proving Proposition 5, note the following:

**Lemma 12.** *Assumptions* (A2) *and* (A+) *imply* $m_3(\boldsymbol{d}_n) = o\left((n\sigma^2(\boldsymbol{d}_n))^{3/2}\right)$.

*Proof.* First note that

$$\Delta n\sigma^2 \geqslant \sum_{v\in[n]} d_v(d_v-1)^2 = m_3 - 2m_2 + n = m_3 - 2n\sigma^2 - n. \tag{8}$$

Now (A2) yields $(\Delta+2)n\sigma^2 = o\left((n\sigma^2)^{3/2}\right)$, whereas (A+) ensures $n = o\left((n\sigma^2)^{3/2}\right)$. Therefore, (8) implies the assertion. □

*Proof of Theorem 5.* Let $x > 0$ and let $k = \lfloor x\sqrt{n/\sigma^2}\rfloor$. Note that Assumption (A2) combined with (4) yields

$$\mathbb{P}(\mathfrak{s}_n(v_n) > x\sqrt{n/\sigma^2}) = g_n(k) + o(1).$$

Moreover, note that Theorem 12 implies $k = o\left((n^3/m_3)^{1/3}\right)$, whereas (A1) and (A+) imply $k = o\left((n^2/m_2)^{2/3}\right)$. Therefore Theorem 11 yields the assertion. □

### 3.2 Moment convergence.

Next up is the proof of Theorem 2 under assumption (A+), that is:

**Proposition 13.** *Assume* (A0), (B1), (B2) *and* (A+). *Let* $X$ *be standard Rayleigh distributed. Then*

$$\lim_{n\to\infty} \mathbb{E}\left[\left(\frac{\mathfrak{s}_n(v_n)}{\sqrt{n/\sigma^2(\boldsymbol{d}_n)}}\right)^p\right] = \mathbb{E}[X^p], \quad p \geqslant 1.$$

*In particular,* $\mathbb{E}[\mathfrak{s}_n(v_n)] \sim \sqrt{\frac{\pi n}{2\sigma^2(\boldsymbol{d}_n)}}$ *and* $\operatorname{Var}(\mathfrak{s}_n(v_n)) \sim \frac{4-\pi}{2\sigma^2(\boldsymbol{d}_n)} n$.

In preparation for the proof of Theorem 13, we note the following.

**Lemma 14.** *Assumptions* (B2) *and* (A+) *imply* $m_3(\boldsymbol{d}_n) = o\left((n\sigma^2(\boldsymbol{d}_n)/\log n)^{3/2}\right)$.

*Proof.* Same as for Theorem 12 up to some obvious changes. □

*Proof of Theorem 13.* Let $X_n = \mathfrak{s}_n(v_n)/\sqrt{n/\sigma^2}$ and let $X$ be standard Rayleigh distributed. First note that if $X_n$ converges in distribution to $X$ and

$$\sup_{n\in\mathbb{N}} \mathbb{E}[X_n^p] < \infty \quad \text{for all } p \geqslant 1 \tag{9}$$

then $\mathbb{E}[X_n^p] \to \mathbb{E}[X]$, since (9) and Markov's inequality imply that $(X_n^p)_{n\geqslant 0}$ is uniformly integrable. Hence, by Theorem 5 it is sufficient to show (9).

To this end, note that (4) and Lemma 11 imply for every $C > 0$

$$\mathbb{P}\left(X_n > x\right) \leqslant C' \exp\left(-\frac{x^2}{2}\right), \quad x \in \left[0, C\sqrt{\log n}\right], \tag{10}$$

for some constant $C'$ which only depends on $C$. In particular, since $X_n \leqslant n$,

$$\mathbb{E}\left[X_n^p \mathbf{1}_{\{X_n > C_p\sqrt{\log n}\}}\right] \leqslant n^p \mathbb{P}\left(X_n > C_p\sqrt{\log n}\right) = \mathrm{O}(1)$$

for $C_p = \sqrt{2p}$. Therefore

$$\mathbb{E}\left[X_n^p\right] = \int_0^{C_p\sqrt{\log n}} \mathbb{P}\left(X_n^p > x\right) \mathrm{d}x + \mathrm{O}(1),$$

which yields the assertion by (10). □

### 3.3 Joint limit for tail- and six-length

In this section we prove Theorem 3 under the additional assumption (A+), that is:

**Proposition 15.** *Let $X$ and $U$ be independent, $U$ be uniformly distributed on $[0,1]$, and $X$ be Rayleigh distributed. Assume* (A0), (B1), (B2) *and* (A+). *Then*

$$\left(\frac{\mathfrak{s}_n(v_n)}{\sqrt{n/\sigma^2(\boldsymbol{d}_n)}}, \frac{\mathfrak{t}_n(v_n)}{\sqrt{n/\sigma^2(\boldsymbol{d}_n)}}\right) \xrightarrow{d} (X, UX).$$

The joint limit of tail- and six-length will be established in two steps:

- Show that, conditioned on $\mathfrak{t}_n(v) > 0$ and $\mathfrak{s}_n(v) = k$, $\mathfrak{t}_n(v)$ is uniformly distributed on $[k-1]$.
- Show $\mathbb{P}(\mathfrak{t}_n(v) > 0) \to 1$ as $n \to \infty$.

The first observation is true for every degree sequence:

**Lemma 16.** *Let $\boldsymbol{d}_n$ be any degree sequence with* (A0). *Let $v$ be such that $\mathbb{P}(\mathfrak{t}_n(v) > 0) > 0$ (i.e. $d_w > 1$ for some $w \neq v$). Then, for every $k \geqslant 2$,*

$$\mathbb{P}(\mathfrak{t}_n(v) = j | \mathfrak{s}_n(v) = k, \mathfrak{t}_n(v) > 0) = \frac{1}{k-1}, \quad j \in [k-1].$$

*Proof.* The assertion is obviously true for $k = 2$, since $\mathfrak{t}_n(v) \leqslant \mathfrak{s}_n(v) - 1$ and thus $\mathfrak{t}_n(v) \in \{0,1\}$ if $\mathfrak{s}_n(v) = 2$.

Now let $k \geqslant 3$. It is sufficient to prove

$$\mathbb{P}(\mathfrak{t}_n(v) = i, \mathfrak{s}_n(v) = k) = \mathbb{P}(\mathfrak{t}_n(v) = i+1, \mathfrak{s}_n(v) = k), \quad i \in [k-2], \tag{11}$$

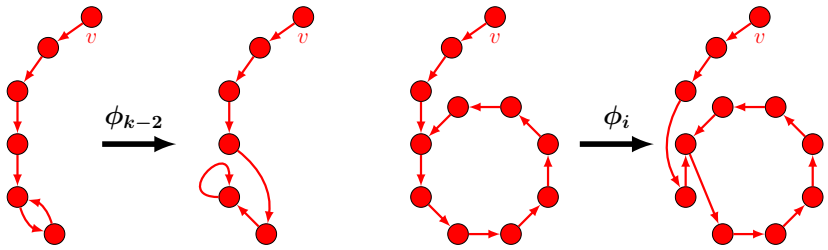
since this implies $\mathbb{P}(\mathfrak{t}_n(v) = x | \mathfrak{s}_n(v) = k, \mathfrak{t}_n(v) > 0) = \mathbb{P}(\mathfrak{t}_n(v) = y | \mathfrak{s}_n(v) = k, \mathfrak{t}_n(v) > 0)$ for all $x, y \leqslant k-1$, yielding an uniform distribution on $[k-1]$.

In order to prove (11), let $\mathfrak{F}_{k,i} := \{f \in \mathfrak{F}(\mathbf{d}_n) : \mathfrak{s}_f(v) = k, \mathfrak{t}_f(v) = i\}$. Then (11) is equivalent to

$$|\mathfrak{F}_{k,i}| = |\mathfrak{F}_{k,i+1}|, \quad i \in [k-2],$$

since the underlying random function $F$ is drawn uniformly at random from $\mathfrak{F}(\mathbf{d}_n)$. We prove the equality above by finding bijections $\phi_i : \mathfrak{F}_{k,i} \to \mathfrak{F}_{k,i+1}$. First consider the case $i = k-2$: For $f \in \mathfrak{F}_{k,k-2}$ let $\phi_{k-2}(f) = g$ where $g$ is the function given by

$$g(x) = \begin{cases} f^{(k-1)}(v), & \text{if } x = f^{(k-3)}(v), \\ f^{(k-2)}(v), & \text{if } x = f^{(k-2)}(v), \\ f(x), & \text{otherwise.} \end{cases}$$




(a) Bijection $\phi_{k-2}$ (b) Bijection $\phi_i$ for $i < k-2$

Figure 2: Bijections between $\mathfrak{F}_{k,i}$ and $\mathfrak{F}_{k,i+1}$.

The effect of $\phi_{k-2}$ on a functional graph is illustrated in Fig. 2(a). It is not hard to check that $\phi_{k-2}(\mathfrak{F}_{k,k-2}) \subseteq \mathfrak{F}_{k,k-1}$ Note that $\phi_{k-2}$ is invertible by choosing $\phi_{k-2}^{-1}(g) := h$,

$$h(x) = \begin{cases} g^{(k-1)}(v), & \text{if } x = g^{(k-3)}(v), \\ g^{(k-2)}(v), & \text{if } x = g^{(k-1)}(v), \\ g(x), & \text{otherwise.} \end{cases}$$

Thus $\phi_{k-2}$ is a bijection and (11) follows for $i = k-2$. A similar bijection works for $i < k-2$, as schematically shown in Fig. 2(b). Details are left to the reader. □

In order to obtain $\mathbb{P}(\mathfrak{t}_n(v) > 0) \to 1$, we first establish the following bound:

**Lemma 17.** *For every $v \in [n]$, as $n \to \infty$,*

$$\mathbb{P}(\mathfrak{t}_n(v) = 0) = \mathrm{O}\left(d_v \mathbb{E}\left[\mathfrak{s}_n(v)/n\right] + d_v n \mathbb{P}(\mathfrak{s}_n(v) > n/2)\right).$$

*Proof.* Note that $\mathbb{P}(\mathfrak{t}_n(v) = 0) = \sum_{k=0}^{n-1} \mathbb{P}(\mathfrak{t}_n(v) = 0, \mathfrak{s}_n(v) = k+1)$ where

$$\begin{aligned} \mathbb{P}(\mathfrak{t}_n(v) = 0, \mathfrak{s}_n(v) = k+1) &= \sum_{(v_1,\dots,v_k) \in J_{n,k}(v)} \left( \prod_{j=1}^{k} \frac{d_{v_j}}{n-j+1} \right) \frac{d_v}{n-k} \\ &= \frac{d_v}{n-k} \mathbb{P}(\mathfrak{s}_n(v) > k). \end{aligned}$$

For $k \leqslant n/2$ we get, uniformly in $k$, $\mathbb{P}(\mathfrak{t}_n(v) = 0, \mathfrak{s}_n(v) = k+1) = \mathrm{O}(d_v/n)\mathbb{P}(\mathfrak{s}_n(v) > k)$. For $k > n/2$ use $\frac{d_v}{n-k}\mathbb{P}(\mathfrak{s}_n(v) > k) \leqslant d_v \mathbb{P}(\mathfrak{s}_n(v) > n/2)$. Combining these bounds with $\sum_k \mathbb{P}(\mathfrak{s}_n(v) > k) = \mathbb{E}[\mathfrak{s}_n(v)]$ yields the assertion. □

**Corollary 18.** *Assume* (A0), (B1), (B2) *and* (A+). *Then* $\lim_{n\to\infty} \mathbb{P}(\mathfrak{t}_n(v_n) = 0) = 0$.

*Proof.* Theorem 13 and assumption (B2) imply $d_v \mathbb{E}[\mathfrak{s}_n(v)/n] \to 0$. Moreover, by Theorem 13 and Markov's inequality

$$\mathbb{P}(\mathfrak{s}_n(v) > n/2) = \mathrm{O}\left((n\sigma^2)^{-p/2}\right), \qquad p \geqslant 1.$$

Thus condition (A+) implies $d_v n \mathbb{P}(\mathfrak{s}_n(v) > n/2) \to 0$. Therefore Theorem 17 yields the assertion. □

*Proof of Theorem 15.* Let $U$ be a uniformly on $[0,1]$ distributed random variable that is independent of $(\mathfrak{s}_n(v))_{n\geqslant 1}$. Moreover, let $\gamma_n = \sqrt{n/\sigma^2(\mathbf{d}_n)}$. Then, by Lemma 16,

$$\begin{aligned}&\mathbb{P}(\mathfrak{s}_n(v) > x\gamma_n, \mathfrak{t}_n(v) > y\gamma_n | \mathfrak{t}_n(v) > 0)\\ &= \mathbb{P}(\mathfrak{s}_n(v) > x\gamma_n, \lceil U(\mathfrak{s}_n(v)-1)\rceil > y\gamma_n | \mathfrak{t}_n(v) > 0).\end{aligned}$$

Moreover, by Lemma 18 and since $\gamma_n \to \infty$,

$$\begin{aligned}&\mathbb{P}(\mathfrak{s}_n(v) > x\gamma_n, \lceil U(\mathfrak{s}_n(v)-1)\rceil > y\gamma_n | \mathfrak{t}_n(v) > 0)\\ &= \mathbb{P}(\mathfrak{s}_n(v) > x\gamma_n, U\mathfrak{s}_n(v) > y\gamma_n) + o(1).\end{aligned}$$

Finally, Theorem 1 and the independent choice of $U$ yield

$$\mathbb{P}(\mathfrak{s}_n(v) > x\gamma_n, U\mathfrak{s}_n(v) > y\gamma_n) \to \mathbb{P}(X > x, UX > y),$$

which implies the joint convergence as claimed. □

## 4 An extension to cases with small coalescence

In this section we discuss how to extend Theorem 1 to degree sequences with small coalescence, that is sequences with $\sigma^2(\mathbf{d}_n) = \mathrm{O}(n^{-1/3}\log n)$ and $n\sigma^2(\mathbf{d}_n) \to \infty$. The key idea is to contract edges incident to vertices with degree 1 until we obtain a reduced graph that satisfies (A+). The six-length of this reduced graph converges to a standard Rayleigh distribution by Theorem 5. Finally, a concentration argument will allow us to deduce a limit theorem for the original graph.

**Definition 19.** Let $\mathbf{d}_n$ be a degree sequence and let $\hat{n} = \lfloor (n\sigma^2(\mathbf{d}_n))^{4/3}\rfloor$. Let $w$ be a vertex. The *$w$-reduction* of a functional graph $\mathcal{G}$ is the graph $\mathcal{G}_w$ obtained as follows: If $\hat{n} \geqslant n$ let $\mathcal{G}_w = \mathcal{G}$. Otherwise, $\mathcal{G}_w$ is obtained as follows: Let $k = n - \hat{n}$. Let $v_1, \dots, v_k$ be $k$ of the degree 1 vertices in $[n]\setminus\{w\}$, chosen using any canonical method. (Note that there are more than $k$ vertices with degree 1 by the choice of $k$ and the fact that $n\sigma^2 = \sum_j (d_j - 1)^2 \geqslant n - \#\{j : d_j = 1\}$.) Then do the following for $i = 1, \dots, k$:

(i) If $v_iv_i$ is an edge in the graph, then delete $v_iv_i$. Otherwise, replace the two edges $xv_i$ and $v_iy$ incident to $v_i$ by a single edge $xy$;

(ii) Delete the vertex $v_i$ from the graph.

Let $V_w = [n]\setminus\{v_1, \dots, v_k\}$. Finally, let $\mathbf{d}_{n,w}$ denote the degree sequence of $\mathcal{G}_w$, that is $\mathbf{d}_{n,w} = (d_v)_{v\in V_w}$.

*Remark* 20. Note that 4/3 in the definition of $\hat{n}$ is somewhat arbitrary; the proof works equally well for a range of similar numbers. Also note that $\hat{n} = o(n)$ for degree sequences with $\sigma^2(\mathbf{d}_n) = o\left(n^{-1/4}\right)$. Finally, note that $\hat{n} \to \infty$ as $n \to \infty$ for any degree sequence with (A1).

*Remark* 21. Suppose $\mathbf{d}_n$ is a degree sequence with (A1) and (A2) (or (B1) and (B2) respectively), which does not satisfy (A+). Note that $\mathcal{G}_w$ is a functional graph with $\hat{n}$ vertices and with

$$\hat{n}\sigma^2(\mathbf{d}_{n,w}) = \sum_{v\in[n]\setminus V_w} (d_v - 1)^2 = \sum_{v\in[n]} (d_v - 1)^2 = n\sigma^2(\mathbf{d}_n). \tag{12}$$

In particular, $\sigma^2(\mathbf{d}_{n,w}) \sim \hat{n}^{-1/4}$ by the choice of $\hat{n}$ and therefore $\mathbf{d}_{n,w}$ satisfies (A+). Moreover (12) and $\Delta(\mathbf{d}_{n,w}) = \Delta(\mathbf{d}_n)$ imply that $\mathbf{d}_{n,w}$ also satisfies (A1) and (A2) (or (B1) and (B2) respectively).

**Definition 22.** Let $V' \subset [n]$ and let $G = (V', E')$ be a functional graph. An *$n$-extension* of $G$ is a graph $H$ with vertex set $[n]$ which is generated according to the following procedure:

(1) Start with $V_0 = V'$ and $E_0 = E'$ and $i = 0$.

(2) Let $w$ be the smallest element in $[n] \setminus V_i$. Let $X_w = 1$ with probability $1/(|E_i| + 1)$ and let $X_w = 0$ otherwise. Then do the following:

   (a) If $X_w = 1$, add $w$ to the graph as an isolated vertex with a single loop, that is $V_{i+1} = V_i \cup \{w\}$ and $E_{i+1} = E_i \cup \{ww\}$.

   (b) If $X_w = 0$, choose an edge $xy \in E_i$ uniformly at random. Set $V_{i+1} = V_i \cup \{w\}$ and $E_{i+1} = (E_i \setminus \{xy\}) \cup \{xv, vw\}$.

(3) If $V_i = [n]$ set $H = (V_i, E_i)$. Otherwise, increase $i$ by one and return to step 2.

**Lemma 23.** *Let $\boldsymbol{d}_n$ be a degree sequence, $w \in [n]$, and let $\boldsymbol{d}_{n,w}$ be as in Definition 19. If $\mathcal{G}_w$ is a random functional graph with degree sequence $\boldsymbol{d}_{n,w}$, then an $n$-extension of $\mathcal{G}_w$ is a random functional graph with degree sequence $\boldsymbol{d}_n$.*

*Proof.* Let $H$ be any functional graph with degree sequence $\mathbf{d}_n$ and let $\mathcal{H}$ denote the $n$-extension of $\mathcal{G}_w$. The claim is that $\mathbb{P}(\mathcal{H} = H) = 1/|\mathfrak{F}(\mathbf{d}_n)|$.

Since $H$ can only be an $n$-extension of $\mathcal{G}_w$ if $\mathcal{G}_w = H_w$, it is sufficient to show that all possible $n$-extensions of a graph $G$ are equally likely. But since there is exactly one way of choosing edges in (2) throughout the procedure that leads to a particular graph $H$, we have

$$\mathbb{P}(\mathcal{H} = H | \mathcal{G}_w = H_w) = \prod_{j=1}^{n-n_w} \frac{1}{n_w + j}$$

and the assertion follows. □

**Definition 24.** A classical $(a, b)$-Pólya urn scheme is an urn initialized with $a$ red and $b$ blue balls which evolves in discrete time as follows: In each time step $n$ draw a ball from the urn at random and put it back together with another ball of the same colour.

Let $\mathcal{R}(n, a, b)$ denote the number of red balls after adding $n$ balls to the urn.

**Corollary 25.** *Let $\boldsymbol{d}_{n,w}$ be as in Definition 19 and let $\mathfrak{s}_{n,w}(w)$ be the six-length of $w$ in a random functional graph with degree sequence $\boldsymbol{d}_{n,w}$. Then*

$$\mathfrak{s}_n(w) \stackrel{d}{=} \mathcal{R}(n-\hat{n}, \mathfrak{s}_{n,w}(w), \hat{n}+1-\mathfrak{s}_{n,w}(w)),$$

*where $\{\mathcal{R}(n,a,b) : a,b,n \in \mathbb{N}_0\}$ is independent of $\mathfrak{s}_{n,w}(w)$ and distributed as in Definition 24.*

*Proof.* Identify edges contributing to the six-length $\mathfrak{s}_{n,w}(w)$ with red balls and all other edges (including a 'phantom' edge for step 2a in Definition 22) with blue balls in a Pólya urn. Then the dynamics described in Definition 22 is equivalent to the procedure of drawing from a Pólya urn. Therefore Lemma 23 implies the assertion. □

**Lemma 26.** *Let $\mathcal{R}(n,a,b)$ be as in Definition 24 and let $\mu(n,a,b) = a(1+n/(a+b))$. Then*

$$\mathbb{P}\left(|\mathcal{R}(n,a,b) - \mu(n,a,b)| \geqslant t\mu(n,a,b)\right) \leqslant 2\exp\left(-\frac{t^2a^2}{8(a+b)}\right).$$

*Proof.* Let

$$M_k := \frac{\mathcal{R}(k,a,b)}{k+a+b}, \quad k \geqslant 0.$$

It is not hard to check that $(M_k)_{k\geqslant 0}$ is a martingale. Since $|\mathcal{R}(k+1,a,b) - \mathcal{R}(k,a,b)| \leqslant 1$ and $\mathcal{R}(k,a,b) \leqslant a+k$, one obtains

$$|M_{k+1} - M_k| \leqslant \frac{2}{k+1+a+b}.$$

Therefore, the Azuma-Hoeffding inequality yields the assertion. □

We end the section with the missing proofs for Theorems 1, 2, and 3. Note that we may assume w.l.o.g. that

$$\sigma^2(\mathbf{d}_n) = \mathrm{O}\left(n^{-1/3}\log^2 n\right), \tag{A-}$$

since the other case is covered by the proofs in Section 3.

*Proof of Theorem 1.* Let $X_n := \mathfrak{s}_n(v_n)/\sqrt{n/\sigma^2(\mathbf{d}_n)}$ and let $X$ be standard Rayleigh distributed. The claim is that $X_n$ converges in distribution to $X$. By Theorem 5 this holds for degree sequences with (A+) and thus, we may assume (A-).

Let $w = v_n$. Let $\mathfrak{s}_{n,w}(w)$ and $\mathcal{R}(n-\hat{n}, \mathfrak{s}_{n,w}(w), \hat{n}+1-\mathfrak{s}_{n,w}(w))$ be as in Corollary 25. Moreover, let $X_{n,w} = \mathfrak{s}_{n,w}(w)/\sqrt{\hat{n}/\sigma^2(\mathbf{d}_{n,w})}$. Note that

(a) $X_{n,w}$ converges in distribution to $X$ by Theorem 5 and Remark 21;

(b) $(\mathfrak{s}_{n,w}(w))^2/\hat{n} \to \infty$ in probability by (a) and $\sigma^2(\mathbf{d}_{n,w}) \sim \hat{n}^{-1/4}$. Hence, using the tail bound in Lemma 26 with arbitrary constant $t > 0$,

$$\frac{\mathcal{R}(n-\hat{n}, \mathfrak{s}_{n,w}(w), \hat{n}+1-\mathfrak{s}_{n,w}(w))}{\mathfrak{s}_{n,w}(w)(n+1)/(\hat{n}+1)} \xrightarrow{\mathbb{P}} 1,$$

where $\xrightarrow{\mathbb{P}}$ denotes convergence in probability.

Moreover, Corollary 25 and $n\sigma^2(\mathbf{d}_n) = \hat{n}\sigma^2(\mathbf{d}_{n,w})$ (see Remark 21) imply

$$X_n \stackrel{d}{=} \frac{\mathcal{R}(n-\hat{n}, \mathfrak{s}_{n,w}(w), \hat{n}+1-\mathfrak{s}_{n,w}(w))}{\mathfrak{s}_{n,w}(w)(n+1)/(\hat{n}+1)} X_{n,w}\,(1+o(1))\,, \tag{13}$$

where $\stackrel{d}{=}$ denotes equality in distribution. It is not hard to check, e.g. with Slutsky's Theorem, that (13), (a) and (b) imply the assertion. Details are left to the reader. □

*Proof of Theorem 2.* Let $X_n$, $X_{n,w}$ and $X$ be as in the previous proof. As in the proof of Theorem 13 it is sufficient to show that

$$\sup_{n\in\mathbb{N}} \mathbb{E}[X_n^p] < \infty, \quad p \geqslant 1, \tag{14}$$

since this bound combined with Theorem 1 implies $\mathbb{E}[X_n^p] \to \mathbb{E}[X^p]$ for all $p \geqslant 1$. Note that $\sup_n \mathbb{E}[X_{n,w}^p] < \infty$ by Theorem 13 and Remark 21.

Now let $A_n := \{\mathfrak{s}_{n,w}(w) \geqslant \sqrt{\hat{n}+1}\}$. With the coupling in Theorem 25 it is not hard to check that

$$\mathbb{E}[X_n^p | A_n^c] \leqslant \mathbb{E}[X_n^p | A_n], \quad p \geqslant 1.$$

Thus, since $\mathbb{P}(A_n) \to 1$ by Theorem 1, it is sufficient to show

$$\sup_{n\in\mathbb{N}} \mathbb{E}\left[X_n^p \mathbf{1}_{A_n}\right] < \infty, \quad p \geqslant 1.$$

Moreover, by (13) and $\sup_n \mathbb{E}[X_{n,w}^p] < \infty$ it is sufficient to show that

$$\sup_{n\in\mathbb{N}} \mathbb{E}\left[\left(\frac{\mathcal{R}(n-\hat{n}, \mathfrak{s}_{n,w}(w), \hat{n}+1-\mathfrak{s}_{n,w}(w))}{\mathfrak{s}_{n,w}(w)(n+1)/(\hat{n}+1)}\right)^p \mathbf{1}_{A_n}\right] < \infty, \quad p \geqslant 1,$$

which is a consequence of the tail bound in Theorem 26. Therefore (14) holds and the convergence of all moments follows. □

*Proof of Theorem 3.* Once again, we may assume w.l.o.g. that (A-) holds. Note that we may copy the proof of Theorem 15 provided we establish

$$\mathbb{P}(\mathfrak{t}_n(v_n) = 0) \to 0. \tag{15}$$

Now let $w = v_n$ and let $\mathfrak{t}_{n,w}(w)$ denote the tail-length of $w$ in the $w$-reduction of the functional graph. Note that $\mathfrak{t}_n(w) = 0$ if and only if $\mathfrak{t}_{n,w}(w) = 0$. Since $\mathbb{P}(\mathfrak{t}_{n,w}(w) = 0) \to 0$ by Theorem 18, we obtain (15). Therefore, the assertion follows using the same proof strategy as for Theorem 15. □

**Acknowledgements**

The authors are grateful to Igor Shparlinksi for suggesting this topic of study, and to the anonymous referee for suggesting additional references.

## References

[1] Arney, J. and Bender, E. Random mappings with constraints on coalescence and number of origins. *Pacific Journal of Mathematics* **103** (2), 269–294, 1982.

[2] Barbour, A.D., Holst, L. and Janson, S. *Poisson Approximation*, Clarendon Press, Oxford, 1992.

[3] Brent, R.P. and Pollard, J. Factorization of the eighth Fermat number. *Mathematics of Computation* **36**, 627–630, 1981.

[4] Hansen, J. C. and Jaworski, J. Random mappings with exchangeable in-degrees. *Random Structures & Algorithms* **33**, 105–126, 2008.

[5] Hansen, J. C. and Jaworski, J. Predecessors and successors in random mappings with exchangeable in-degrees. *Journal of Applied Probability* **50**, 721–740, 2013.

[6] Harris, B. Probability distributions related to random mappings, *Annals of Mathematical Statistics* **31**, 1045–1062, 1960.

[7] Konyagin, S.V., Luca, F., Mans, B., Mathieson, L., Sha, M. and Shparlinski, I.E. Functional graphs of polynomials over finite fields. *Journal of Combinatorial Theory, Series B* **116**, 87–122, 2016.

[8] Martins, R. SV. and Panario, D. On the heuristic of approximating polynomials over finite fields by random mappings. *International Journal of Number Theory* **12** (07), 1987-2016, 2016.

[9] Pollard, J. M. A Monte Carlo method for factorization. *BIT Numerical Mathematics* **15** (3), 331–334, 1975.