A Poisson $*$ negative binomial convolution law for random polynomials over finite fields*

Hsien-Kuei Hwang
Institute of Statistical Science
Academia Sinica
Taipei 11529
Taiwan

January 15, 1998

Abstract

Let $\mathbf{F}_q[X]$ denote a polynomial ring over a finite field $\mathbf{F}_q$ with q elements. Let $\mathcal{P}_n$ be the set of monic polynomials over $\mathbf{F}_q$ of degree n. Assuming that each of the q^n possible monic polynomials in $\mathcal{P}_n$ is equally likely, we give a complete characterization of the limiting behavior of $\mathrm{P}(\Omega_n = m)$ as $n \to \infty$ by a uniform asymptotic formula valid for $m \geq 1$ and $n - m \to \infty$, where Ω_n represents the number (multiplicities counted) of irreducible factors in the factorization of a random polynomial in $\mathcal{P}_n$. The distribution of Ω_n is essentially the convolution of a Poisson distribution with mean $\log n$ and a negative binomial distribution with parameters q and q^{-1}. Such a convolution law exhibits three modes of asymptotic behaviors: when m is small, it behaves like a Poisson distribution; when m becomes large, its behavior is dominated by a negative binomial distribution, the transitional behavior being essentially a parabolic cylinder function (or some linear combinations of the standard normal law and its iterated integrals). As applications of this uniform asymptotic formula, we derive most known results concerning $\mathrm{P}(\Omega_n = m)$ and present many new ones like the unimodality of the distribution. The methods used are widely applicable to other problems on multiset constructions. An extension to Rényi's problem, concerning the distribution of the difference of the (total) number of irreducibles and the number of distinct irreducibles, is also presented.

AMS 1991 Mathematics subject classification: Primary 11T06; secondary 60C05.

Key words: Convolution laws, singularity analysis, approximation theorems, irreducible polynomials, parabolic cylinder function, uniform asymptotics.

1 Introduction and main results

Because of many applications in diverse areas (which may be exemplified by the huge number of items referenced in Lidl and Niederreiter's and Shparlinski's books [32, 36]), finite fields have received increasing interest in the literature. Finite fields are known to be very useful in finite geometries, combinatorics, algebraic coding theory, cryptology, combinatorial design theory, symbolic computations, pseudorandom number generation, and shift register sequences; cf. [32, 36, 28].

Let $\mathbf{F}_q$ be a finite field with q elements and $\mathcal{P}_n$ the set of monic polynomials over $\mathbf{F}_q$ of degree n. Assuming that each of the q^n polynomials in $\mathcal{P}_n$ is equally likely, we are interested in the random variable Ω_n, counting the total number (i.e., counted with multiplicities) of irreducible factors of a random polynomial in $\mathcal{P}_n$. The purpose of this paper is to give a complete asymptotic characterization of the distribution of Ω_n, namely, we will give a uniform asymptotic formula for the probability

*This work was supported by National Science Council under the Grant NSC-85-2121-M-001-007.

$\mathrm{P}(\Omega_n = m)$ as $n \to \infty$ and for all possible forms of variation of m. Analytically, the problem is equivalent to the asymptotic evaluation of the coefficient[1]

$$N(n,m) := q^n \mathrm{P}(\Omega_n = m) = [u^m z^n] P(z,u), \quad P(z,u) = \prod_{j\geq 1} \left(1 - uz^j\right)^{-I_j},$$

where

$$\begin{aligned} I(z) &= \sum_{j\geq 1} I_j z^j = \sum_{k\geq 1} \frac{\mu(k)}{k} \log \frac{1}{1-qz^k} \\ &= qz + \frac{q(q-1)}{2} z^2 + \frac{q(q^2-1)}{3} z^3 + \frac{q^2(q^2-1)}{4} z^4 + \frac{q(q^4-1)}{5} z^5 + \cdots \end{aligned} \tag{1}$$

is the generating function for monic irreducible polynomials over $\mathbf{F}_q$, $\mu(k)$ being the Möbius function; cf. [30, 31, 32, 14].

Let us first summarize known results in the literature concerning N.

– Obviously,

$$N(n,1) = I_n = \frac{1}{n} \sum_{d\,|\,n} \mu(n/d) q^d = \frac{q^n}{n} \left(1 + O\left(q^{-n/2}\right)\right),$$

a result first proved by Gauss [16]. This is the "prime number theorem" on finite fields.

– Cohen [10] showed, by arguments parallel to the proof for asymptotic estimate of the number of integers $\leq x$ with m prime factors (cf. [20, Theorem 437]), that

$$\mathrm{P}(\Omega_n = m) = \frac{(\log n)^{m-1}}{n(m-1)!} \left(1 + O\left(\frac{1}{\log n}\right)\right),$$

whenever[2] $m \ll 1$.

– Car [9] extended Cohen's result by showing that

$$\mathrm{P}(\Omega_n = m) = \frac{(\log n)^{m-1}}{n(m-1)!} \left(g\left(\frac{m-1}{\log n}\right) + O\left(\frac{m-1}{(\log n)^2}\right)\right), \tag{2}$$

uniformly for $1 \leq m \leq A \log n$, where $0 < A < q$ and

$$g(u) = \frac{1}{\Gamma(1+u)} \prod_{j\geq 1} \frac{(1-1/q^j)^{I_j u}}{(1-u/q^j)^{I_j}} = \frac{e^{\kappa u}}{\Gamma(1+u)} \prod_{j\geq 1} \left(\frac{e^{-u/q^j}}{1-u/q^j}\right)^{I_j}, \qquad (|u| < q) \tag{3}$$

with

$$\kappa = \sum_{k\geq 2} \frac{\mu(k)}{k} \log \frac{1}{1-q^{1-k}}.$$

Her method parallels Selberg's classical one [35, 39] in analytic number theory. An extension of Car's result to additive arithmetical semigroups satisfying certain conditions can be found in Warlimont [40]. Note that $g(0) = g(1) = 1$.

– Flajolet and Soria [14] showed, as a special case of more general results, that the distribution of Ω_n is asymptotically normal.

[1] We use the notation $[z^n]f(z)$ to denote the coefficient of z^n in the Taylor expansion of f. The notation $[u^b z^a]f(z,u)$ is then defined as $[u^b]\left([z^a]f(z,u)\right)$.

[2] The Vinogradov symbol $\ll$ is used as a synonym for Landau's $O(.)$ symbol.

– Gao and Richmond [15] established, also as a special case of their general results, a local limit theorem for Ω_n.

– Hwang [26] studied a general exp(log) analytic scheme of which (2) is a special case. Many limit and approximation theorems for Ω_n were also derived. For example, if $m = \log n + x\sqrt{\log n}$, where $x = o(\sqrt{\log n})$, then

$$\mathrm{P}(\Omega_n = m) = \frac{e^{-\frac{1}{2}x^2 - \log n \cdot V(x/\sqrt{\log n})}}{\sqrt{2\pi \log n}} \left(1 + O\left(\frac{1+|x|}{\sqrt{\log n}}\right)\right), \tag{4}$$

uniformly in x, where

$$V(t) = (1+t)\log(1+t) - t - t^2/2 = \sum_{j\geq 3} \frac{(-1)^j}{j(j-1)}\, t^j \qquad (-1 < t \leq 1).$$

– Define the total variation distance $d_{TV}(\mathcal{L}(X), \mathcal{L}(Y))$ of the distributions of two random variables X, Y on a finite or countable space S by

$$\begin{aligned} d_{TV}(\mathcal{L}(X), \mathcal{L}(Y)) &= \max_{\sigma \in S} \left(P(X \in \sigma) - P(Y \in \sigma)\right) \\ &= \tfrac{1}{2} \sum_{\sigma \in S} \left|\mathrm{P}(X = \sigma) - P(Y = \sigma)\right|. \end{aligned}$$

Arratia, Barbour and Tavaré [1] showed that

$$d_{TV}\left(\mathcal{L}(\Omega_n), \mathrm{Po}(H_n)\right) \ll \frac{1}{\sqrt{\log n}}, \tag{5}$$

where $\mathrm{Po}(H_n)$ is the Poisson distribution with mean $H_n = \sum_{1\leq j\leq n} j^{-1}$, the harmonic numbers. For further limit theorems concerning the factor structures of random polynomials, see [17, 18, 1, 2, 11]. Note that from (4) we can show that

$$d_{TV}\left(\mathcal{L}(\Omega_n), \mathrm{Po}(\log n)\right) \ll \frac{1}{\sqrt{\log n}}.$$

Furthermore, by more precise expansions of (4), we can show that (cf. [23])

$$d_{TV}\left(\mathcal{L}(\Omega_n), \mathrm{Po}_1(\log n + g'(1))\right) = \frac{|g'(1)^2 - g''(1)|}{\sqrt{2\pi e}\, \log n} \left(1 + O\left((\log n)^{-1}\right)\right),$$

where $\mathrm{Po}_1(\lambda)$ denotes a Poisson random variable Y with

$$\mathrm{P}(Y = m) = \frac{\lambda^{m-1}}{(m-1)!}\, e^{-\lambda} \qquad (m = 1, 2, \ldots).$$

For a study on asymptotics of many probability distances of Poisson approximation to a class of discrete distributions, see [23].

The result (5) states that the distribution of Ω_n is well approximated by a Poisson distribution with mean H_n. Since $H_n \to \infty$, we have from (5) a central limit theorem for Ω_n with a Berry-Esseen error of order $(\log n)^{-1/2}$ (cf. [26]). Our purpose of this paper is to show that if instead of a Poisson approximation (5) we choose a Poisson $*$ negative binomial convolution approximation to the distribution of Ω_n, then for almost all values of Ω_n of interest, $m \geq 1$ and $n - m \to \infty$, we have an asymptotic expression with an error term essentially of order $(\log n)^{-1}$. We complete the study by giving another asymptotic formula valid for $(n-q)/2 < m \leq n$. Both these two results are based on a "fundamental (integral) formula", which explicitly isolates the contribution of factors of degree 1, and

the singularity analysis of Flajolet and Odlyzko [13]. Other analytic tools used are Selberg's method (cf. [35, 39, 26]), the uniform asymptotic methods by Bleistein [6, 7] and Temme [38], and some new techniques.

The interest of considering convolution approximations to random discrete distributions is threefold. First, for probabilists, such a consideration suggests further discrete approximations (besides Poisson, binomial, etc) for combinatorial distributions, the general intuition being that discrete approximations (as opposed to continuous ones) to discrete structures would usually provide better error estimates. Next, this line of study introduces many intriguing problems for uniform asymptotic analysis (cf. [7, 43]) and would be of special interest to analysts. Third, for combinatorialists and number-theorists, the quantitative results demand further structural interpretations and characterizations. Problems like "why it is Poisson for small m and negative binomial for large m" will shed further light on the usefulness and uniformity of a result like (7); cf. § 2.3.

Notation. Throughout this paper, q is a fixed prime power[3]. All limits, unless otherwise specified, are taken to be $n \to \infty$. To avoid excessive references, notation and symbols will be used as consistently as possible so that they will always stand for the same meanings. The symbols K and ε always denote sufficiently large and small, respectively, quantities independent of other parameters (except q), the value of each occurrence being, however, not necessarily the same.

1.1 Statement of results

To state our results, let us introduce some notation. Let

$$\Pi_m(\tau;\lambda) = e^{-\lambda}(1-\tau)^q \sum_{0\le j\le m} \binom{q+j-1}{j} \tau^j \frac{\lambda^{m-j}}{(m-j)!}$$

be the convolution of a Poisson variate with mean λ and a negative binomial random variable with parameters q and τ, $0<\tau<1$ (see the next section for details). Let $\Lambda = q\log(n-m)$,

$$\pi_m(\Lambda) = [u^m]\frac{e^{\Lambda u}}{(1-u)^q} = \sum_{0\le j\le m} \binom{q+j-1}{j} \frac{\Lambda^{m-j}}{(m-j)!}$$

and define a meromorphic function (cf. (3))

$$G(u) = q(1-u)^q g(qu) = \frac{qe^{(\kappa q-1)u}}{\Gamma(1+qu)} \prod_{j\ge 2} \left(\frac{e^{-u/q^{j-1}}}{1-u/q^{j-1}}\right)^{I_j}, \tag{6}$$

for $|u|<q$. Obviously, $\Pi_m(\tau;\lambda) = e^{-\lambda}(1-\tau)^{-q}\tau^m\pi_m(\lambda/\tau)$.

Theorem 1 *If $m\ge 1$ and $n-m\to\infty$, then*

$$\mathrm{P}(\Omega_n = m) = G(r)\left(1-q^{-1}\right)^{-q}\Pi_{m-1}\left(q^{-1};\log(n-m)\right)\left(1+O(\Lambda^{-1})\right), \tag{7}$$

uniformly in m, where $r=0$ if $m=1$; $r=\pi_{m-2}(\Lambda)/\pi_{m-1}(\Lambda)$ if $m\ge 2$. The quantity r satisfies

$$r = \begin{cases} \dfrac{m-1}{\Lambda}\left(1+O\left(\dfrac{1}{\Lambda-m+1}\right)\right), & \text{if } 1\le m\le \Lambda - K\sqrt{\Lambda};\\ 1-O\left(\dfrac{1+|\mu|^3}{\sqrt{\Lambda}}\right), & \text{if } \mu = \dfrac{m-1-\Lambda}{\sqrt{\Lambda}} = o(\Lambda^{1/6});\\ 1-\dfrac{q-1}{m-1-\Lambda}+O\left(\dfrac{\Lambda}{(m-1-\Lambda)^2}\right), & \text{if } m\ge \Lambda+K\sqrt{\Lambda}, \end{cases} \tag{8}$$

K being a sufficiently large number.

[3] All our results actually hold for any integer $q\ge 2$, an interpretation of such structures can be found in [1]. Moreover, most of our formulae subsist even in the case when q is a positive real number >1.

Note that

$$r \sim \min\left\{\frac{m-1}{\Lambda}, 1\right\} \qquad (m \geq 1).$$

The proof of this theorem is, besides some peculiarities of different inversion formulae, more involved than the one by Balazard, Delange, and Nicolas [5] for the number of integers $\leq x$ with m prime factors. In their context, the integral in question has a simple pole and a saddle point; while in our case, a pole of order q and a saddle point is encountered in the integrand; cf. also [25].

The theorem is useful only if the asymptotic behaviors of Π_m as $\lambda \to \infty$ can be explicitly described, a problem of some independent and intrinsic interest. To this aim, we split the range into three overlapping intervals:

$$\begin{array}{ll} (I) & 0 \leq m \leq \frac{\lambda}{\tau} - K\sqrt{\lambda}; \\ (II) & \left|\frac{m-\lambda/\tau}{\sqrt{\lambda/\tau}}\right| = o(\lambda^{1/6}); \quad \text{and} \\ (III) & m \geq \frac{\lambda}{\tau} + K\sqrt{\lambda}, \end{array} \tag{9}$$

where K is a sufficiently large number.

The following results state roughly that when m is small (m in (I)) the distribution is Poisson; and when m is large (m in (III)), it is negative binomial; the transitional behavior (m in (II)) is described a parabolic cylinder function $D_{-q}(-x)$ defined by (cf. [12, 41])

$$D_{-\nu}(x) = \frac{e^{-x^2/4}}{\Gamma(\nu)} \int_0^\infty t^{\nu-1} e^{-xt-t^2/2} \mathrm{d}t \qquad (\nu > 0). \tag{10}$$

Theorem 2 *As $\lambda \to \infty$, the probability distribution $\Pi_m(\tau, \lambda)$ satisfies the estimates: (i) for m in (I)*

$$\Pi_m(\tau;\lambda) = e^{-\lambda} \frac{(1-\tau)^q}{(1-\tau m/\lambda)^q} \frac{\lambda^m}{m!} \left(1 + O_K\left(\frac{m}{(\lambda-\tau m)^2}\right)\right); \tag{11}$$

(ii) for m in (II), $m = (\lambda/\tau) + \mu\sqrt{\lambda/\tau}$,

$$\Pi_{m-1}(\tau;\lambda) = e^{-\lambda}(1-\tau)^q \frac{e^m m^{-m}}{\sqrt{2\pi m}} \lambda^{m-1} m^{q/2} e^{\mu^2/4} D_{-q}(-\mu) \left(1 + O\left(\frac{1+|\mu|^3}{\sqrt{\lambda}}\right)\right); \tag{12}$$

(iii) for m in (III)

$$\Pi_m(\tau;\lambda) = e^{-\lambda(1-1/\tau)}(1-\tau)^q \tau^m \frac{(m-\lambda/\tau)^{q-1}}{(q-1)!} \left(1 + O_K\left(\frac{\lambda}{(m-\lambda/\tau)^2}\right)\right), \tag{13}$$

uniformly for m in each range.

Note that since $D_{-1}(-x) = \sqrt{2\pi} e^{x^2/2} \Phi(x)$, Φ being the standard normal distribution, our estimates reduce to those for the Poisson $*$ geometric distribution when $q = 1$; cf. [4, 25].

From the above two theorems, we can obtain precise local behaviors of N in almost all ranges of interest except for the case when $n - m \ll 1$. This gap is completed by the following result.

Theorem 3 *If $(n-q)/2 < m \leq n$ then*

$$N(n,m) = \frac{m^{q-1}}{(q-1)!} \beta_{n,m} \left(1 + O\left(\frac{\log(n-m+e)}{n}\right)\right), \tag{14}$$

uniformly in m, where

$$\beta_{n,m} = [z^{n-m}] \prod_{j \geq 2} \left(1 - z^{j-1}\right)^{-I_j}.$$

If furthermore $n - m \to \infty$, then

$$\beta_{n,m} = G(1)(n-m)^{q-1} q^{n+1-m} \left(1 + O\left(\frac{\log(n-m)}{n-m}\right)\right).$$

Actually, the relation (14) holds in an even wider range (cf. § 4.3), provided that the error term is suitably modified. The theorem is stated in its current form for two reasons: first, it completes the gap of Theorem 1; and second, the method of proof is of independent interest.

The first few terms of $\beta_{n,n-i}$, $i = 0, \ldots, 3$, are listed as follows.

$$\beta_{n,n} = 1, \quad \beta_{n,n-1} = \frac{q(q-1)}{2}, \quad \beta_{n,n-2} = \frac{q(q-1)(3q^2+5q+14)}{24},$$
$$\beta_{n,n-3} = \frac{q(q-1)(q^4+6q^3+19q^2-2q+8)}{48}.$$

The paper is organized as follows. In the next section, we state properties of the Poisson $*$ negative binomial distribution and prove its trichotomous limiting behaviors. A probabilistic interpretation of (7) is also given. Then we prove our main theorems in §3. Many consequences of the uniform asymptotic formula (7) together with other global properties are discussed in §§4 and 5. Finally, we conclude with some possible extensions and related materials.

For simplicity of presentation, we content ourselves with an asymptotic main term together with an O-estimate for the remainders of all our results, leaving aside the derivations of more refined asymptotic expansions, which may be done with more computations in almost all cases.

We note that many problems in branching processes and in random graphs also involve interesting trichotomous behaviors; see [21, 33] and the references therein.

2 The Poisson $*$ negative binomial convolution law

In this section we first discuss basic properties of the Poisson $*$ negative binomial law and then prove Theorem 2. A probabilistic interpretation of (7) is given at the end of this section.

2.1 Basic properties

Let X be a Poisson random variable with mean $\lambda > 0$:

$$\varpi_j = \mathrm{P}(X = j) = e^{-\lambda}\frac{\lambda^j}{j!} \qquad (j = 0, 1, 2, \ldots),$$

and Y a negative binomial random variable with parameters q and τ, $0 < \tau < 1$:

$$\nu_j = \mathrm{P}(Y = j) = \binom{q+j-1}{j}\tau^j(1-\tau)^q \qquad (j = 0, 1, 2, \ldots).$$

The convolution U of the distribution of X and Y with X, Y independent is $U = X + Y$:

$$\begin{aligned}\Pi_m(\tau;\lambda) &= \mathrm{P}(U = m) = \sum_{0\le j\le m}\nu_j\varpi_{m-j}\\ &= e^{-\lambda}(1-\tau)^q\tau^m\sum_{0\le j\le m}\binom{q+j-1}{j}\frac{(\lambda/\tau)^{m-j}}{(m-j)!}\end{aligned}$$

for $m = 0, 1, 2, \ldots$ This convolution law is known in the actuarial literature as the Delaporte distribution (cf. [27]). In terms of probability generating functions, we have

$$\mathrm{E}(z^U) = \left(\frac{1-\tau}{1-\tau z}\right)^q e^{\lambda(z-1)},$$

where E(.) denotes the expectation of its parameter. From this expression, we can easily obtain many limit theorems, like for example, the distribution of U is asymptotically Gaussian as $\lambda \to \infty$, the convergence rate being of order $\lambda^{-1/2}$; cf. [26].

2.2 Proof of Theorem 2

In each of the ranges (9) a different analytic method will be used starting from Cauchy's integral formula. *Throughout this section,* $\rho = \tau m/\lambda$.

Case 1 *m in (I).*

We use Selberg's method [35]; see [39, 26] for details. We have

$$\begin{aligned}\Pi_m(\tau;\lambda) &= \frac{1}{2\pi i}\oint_{|z|=\rho/\tau} z^{-m-1}\left(\frac{1-\tau}{1-\tau z}\right)^q e^{\lambda(z-1)}\mathrm{d}z \\ &= e^{-\lambda}(1-\tau)^q\tau^m\frac{1}{2\pi i}\oint_{|z|=\rho} z^{-m-1}(1-z)^{-q}e^{\lambda z/\tau}\mathrm{d}z. \qquad (15)\end{aligned}$$

Expand $(1-z)^{-q}$ at $z=\rho<1$:

$$\frac{1}{(1-z)^q} = \frac{1}{(1-\rho)^q} + \frac{q}{(1-\rho)^{q+1}}(z-\rho) + \frac{q(q+1)}{(1-\rho)^{q+2}}(z-\rho)^2\int_0^1 \frac{1-t}{\left(1-t\frac{z-\rho}{1-\rho}\right)^{q+2}}\,\mathrm{d}t.$$

Substituting this formula into (15) and estimating the integral

$$\frac{1}{2\pi i}\oint_{|z|=\rho}(z-\rho)^2 z^{-m-1}e^{\lambda z/\tau}\int_0^1 \frac{1-t}{\left(1-t\frac{z-\rho}{1-\rho}\right)^{q+2}}\,\mathrm{d}t\,\mathrm{d}z$$

by Laplace's method, we obtain (11). ∎

Case 2 *m in (III).*

Before proving (13), we note that

$$\binom{m-\frac{\lambda}{\tau}+q-1}{q-1}\tau^{m-\lambda/\tau} \sim \frac{(m-\lambda/\tau)^{q-1}}{(q-1)!}\tau^{m-\lambda/\tau} \qquad (m\gg\lambda/\tau),$$

so that the behavior of (13) is essentially negative binomial. Since q is a positive integer, we have by Cauchy's formula

$$\begin{aligned}\Pi_m(\tau;\lambda) &= -e^{-\lambda}(1-\tau)^q\tau^m\mathrm{Res}_{z=1}\left(z^{-m-1}(1-z)^{-q}e^{\lambda z/\tau}\right) \\ &\quad + e^{-\lambda}(1-\tau)^q\tau^m\frac{(-1)^q}{2\pi i}\oint_{|z|=\rho} z^{-m-1}(z-1)^{-q}e^{\lambda z/\tau}\mathrm{d}z,\end{aligned}$$

where $\rho>1$ in this case. The integral on the right-hand side is evaluated as in case 1:

$$\frac{(-1)^q}{2\pi i}\oint_{|z|=\rho} z^{-m-1}(z-1)^{-q}e^{\lambda z/\tau}\mathrm{d}z = \frac{(-1)^q(\lambda/\tau)^m}{(\rho-1)^q m!}\left(1+O\left(\frac{m}{(m-\lambda/\tau)^2}\right)\right),$$

and the residue is given by

$$\begin{aligned}R_{m,q}(\tau;\lambda) &:= -\mathrm{Res}_{z=1}\left(z^{-m-1}(1-z)^{-q}e^{\lambda z/\tau}\right) \\ &= e^{\lambda/\tau}\sum_{0\le j<q}\binom{m+j}{j}\frac{(-\lambda/\tau)^{q-1-j}}{(q-1-j)!}.\end{aligned}$$

By the elementary formula

$$\binom{m+j}{j} = \frac{m^j}{j!}\left(1+\frac{j(j+1)}{2m}+O\left(\frac{j^3}{m^2}\right)\right) \qquad (m\to\infty)$$

and some straightforward computations, we derive (13).

Alternatively, we can use techniques similar to the singularity analysis of Flajolet and Odlyzko [13] by first choosing a Hankel type contour around 1 in which the radius of the larger circle equals ρ (> 1). Formula (12) is then derived using $m - \lambda/\tau$ as the asymptotic scale. The advantage of this approach is that q may be any positive number, provided that $(q-1)!$ in (13) is replaced by $\Gamma(q)$. ∎

Remarks. 1. Set $S_{m,q} = e^{-\lambda/\tau} R_{m,q}(\tau;\lambda)$. Then by integration by parts, we have available the recurrence

$$S_{m,q} = \frac{1}{q-1}\left(mS_{m+1,q-1} - \frac{\lambda}{\tau}S_{m,q-1}\right) \qquad (q \geq 2),$$

with $S_{m,q} = 1$. Thus

$$S_{m,2} = m - \frac{\lambda}{\tau}, \quad S_{m,3} = \tfrac{1}{2}\left(m - \frac{\lambda}{\tau}\right)^2 + \tfrac{1}{2}m.$$

2. $R_{m,q}(\tau,\lambda) = (-1)^m L_m^{(-m-q)}(\lambda/\tau)$, where $L_n^{(\alpha)}$ are Laguerre polynomials defined by

$$L_n^{(\alpha)}(x) = [z^n](1-z)^{-\alpha-1}\exp\left(-\frac{xz}{1-z}\right) \qquad (\alpha \in \mathbf{R}).$$

For the intermediate range (*II*), we need some standard notation in the theory of special functions. Let $D_\nu(z)$ denote the parabolic cylinder functions (cf. [12, 41]): D_ν satisfies the differential equation

$$D_\nu''(z) + \left(\nu - \tfrac{1}{2} - \frac{z^2}{4}\right) D_\nu(z) = 0,$$

and the integral representation[4]

$$D_\nu(z) = \frac{\Gamma(\nu+1)}{2\pi i}\, e^{-z^2/4} \int_{-\infty}^{(0+)} e^{zs - s^2/2} s^{-\nu-1}\mathrm{d}s \qquad (-\pi < \arg s < \pi),$$

which represents an entire function in the z-plane. Besides the special form (10), two special cases are worthy of mention:

$$D_0(z) = e^{-z^2/4}, \quad D_{-1}(z) = \sqrt{2\pi}\, e^{z^2/2}\Phi(-z).$$

We also need the following properties:

$$D_{-\nu}(x) = e^{-x^2/4}x^{-q}\left(1 - \frac{q(q+1)}{2x^2} + O\left(x^{-4}\right)\right) \qquad (x \to \infty), \tag{16}$$

$$\begin{aligned} D_{-\nu}(-x) &= \frac{\sqrt{2\pi}}{(q-1)!}\, e^{x^2/4}x^{q-1}\left(1 + \frac{(q-1)(q-2)}{2x^2} + O\left(x^{-4}\right)\right) \\ &\quad + (-1)^{q-1}e^{-x^2/4}x^{-q}\left(1 - \frac{q(q-1)}{2x^2} + O\left(x^{-4}\right)\right) \qquad (x \to \infty), \end{aligned} \tag{17}$$

$$D_{-\nu-1}(x) = \frac{-1}{\nu}\left(D'_{-\nu}(x) + \frac{x}{2}D_{-\nu}(x)\right). \tag{18}$$

From the last relation, we obtain the expression

$$D_{-\nu}(x) = A_\nu(x)e^{-x^2/4} + \sqrt{2\pi}\, B_\nu(x)e^{x^2/4}\Phi(-x) \qquad (\nu \geq 2),$$

where A_ν abd B_ν are polynomials of degree $\nu - 2$ and $\nu - 1$, respectively. They satisfy $A_1(x) = 1$, $B_1(x) = 1$, and

$$\begin{cases} A_{\nu+1}(x) = -\frac{1}{\nu}\left(A'_\nu(x) - B_\nu(x)\right) \\ B_{\nu+1}(x) = -\frac{1}{\nu}\left(B'_\nu(x) + xB_\nu(x)\right) \end{cases} \qquad (\nu = 1, 2, \ldots),$$

[4]The path of integration $\int_{-\infty}^{(0+)}$ starts at $\infty e^{-\pi i}$, encircles the origin once counter-clockwise and returns to $\infty e^{\pi i}$.

From these recurrences, the first few terms of A_ν and B_ν are computed as follows.

$$A_2(x)=1,\quad A_3(x)=-\frac{x}{2},\quad A_4(x)=\frac{x^2+2}{6},$$
$$B_2(x)=-x,\quad B_3(x)=\frac{x^2+1}{2},\quad B_4(x)=-\frac{x^3+3x}{6}.$$

We now describe the transitional behavior of Π_m in a more extended region.

Case 3 *Let $b=\operatorname{sign}(\rho-1)\sqrt{2(\rho^{-1}+\log\rho-1)}$. If $m\to\infty$ and $\tau m/\lambda\le B$, for any $B>1$, then Π_m satisfies*

$$\begin{aligned}\Pi_{m-1}(\tau;\lambda) &= e^{-\lambda}(1-\tau)^q\tau^{m-1}\frac{e^m\rho^{1-m}}{\sqrt{2\pi m}}\,m^{q/2}e^{mb^2/4}\Big\{\eta_0 D_{-q}(-b\sqrt{m})\left(1+O\left(m^{-1}\right)\right)\\ &\quad-\frac{\eta_1}{\sqrt{m}}D_{1-q}(-b\sqrt{m})\left(1+O\left(m^{-1}\right)\right)\Big\},\end{aligned}\tag{19}$$

uniformly in m, where

$$\eta_0=\left(\frac{\rho-1}{\rho b}\right)^{q-1},\qquad \eta_1=\frac{1}{b}\left(\left(\frac{\rho-1}{\rho b}\right)^{q-1}-\left(\frac{b}{\rho-1}\right)^q\right),$$

are bounded coefficients.

We first show how to derive (12) from (19). By definition, we have

$$\begin{aligned}\eta_0 &= 1-\frac{\sqrt{\tau}}{3\sqrt{\lambda}}\,q\mu+O\left(\frac{\mu^2}{\lambda}\right),\\ \eta_1 &= \frac{q+1}{3}+\frac{\sqrt{\tau}\mu}{12\sqrt{\lambda}}(1-2q^2)+O\left(\frac{\mu^3}{\lambda}\right),\end{aligned}$$

for m in (II). Next, from (18), it follows that

$$b\sqrt{m}=\mu-\frac{\sqrt{\tau}\mu^2}{6\sqrt{\lambda}}+O\left(\frac{\mu^2}{\lambda}\right),$$

and thus

$$D_{-q}(-b\sqrt{m})=D_{-q}(-\mu)\left(1+O\left(\frac{1+|\mu|^3}{\sqrt{\lambda}}\right)\right).$$

This completes the proof. ∎

We now prove (19) using the methods of Temme [38] and Bleistein [6, 7]. Assume for the moment that $\rho<1$. Let

$$I_q=I_q(m-1)=\frac{1}{2\pi i}\oint_{|z|=\rho}z^{-m}(1-z)^{-q}e^{\lambda z/\tau}\mathrm{d}z.$$

By Cauchy's theorem we may straighten the integration path so that we have

$$\begin{aligned}I_q &= \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}z^{-m}e^{\lambda z/\tau}(1-z)^{-q}\,\mathrm{d}z &(20)\\ &= \frac{e^m\rho^{1-m}}{2\pi i}\int_{c-i\infty}^{c+i\infty}e^{m\phi(s)}\,(1-\rho s)^{-q}\,\mathrm{d}s\qquad(0<c<1), &(21)\end{aligned}$$

where $\phi(s)=s-1-\log s$. The steepest descent curve is described by

$$\mathcal{C}:\ \ \Im\,\phi(s)=\Im\,\phi(\sigma+it)=0,\quad\text{or}\quad \sigma=t\cot t,\quad -\pi<t<\pi;$$

and the function ϕ is real and negative on $\mathcal{C}$. Now we define a mapping of the s-plane into the w-plane by the equation

$$-\tfrac{1}{2}w^2 = \phi(s),$$

with the condition that $s \in \mathcal{C}$ corresponds to $w \in \mathbf{R}$, and $w > 0$ if $t > 0$; $w < 0$ if $t < 0$. It follows that

$$w = i(1-s)\left(\frac{2(s-1-\log s)}{(1-s)^2}\right)^{1/2},$$

where the square root is positive for positive values of its argument. Deforming the integration path of the integral in (21) into $\mathcal{C}$, we obtain

$$I_q = \frac{e^m \rho^{1-m}}{2\pi i}\int_{-\infty}^{\infty} e^{-mw^2/2}\,\frac{f(w)}{(ib-w)^q}\,\mathrm{d}w,$$

where

$$w = ib := i\,\mathrm{sign}(\rho-1)\sqrt{2(\rho^{-1}+\log\rho-1)}$$

is the corresponding point of $s = \rho^{-1}$ in the w-plane and

$$f(w) = \left(\frac{ib-w}{1-\rho s}\right)^q \frac{\mathrm{d}s}{\mathrm{d}w}.$$

Since $b \sim (\rho-1) \to 0$ as $\rho \sim 1$, we can get rid of the restriction that $\rho < 1$ by suitably deforming the integration path, if necessary, to avoid the polar singularity.

The integral can now be evaluated by the method of Bleistein (cf. [6, 7, 38]):

$$\begin{aligned} I_q \;=\; & \frac{e^m\rho^{1-m}}{\sqrt{2\pi}}\,m^{(q-1)/2}e^{mb^2/4}\left(i^q D_{-q}(-b\sqrt{m})\left(\sum_{0\le j\le \nu}\frac{\gamma_{2j}}{m^j}+O\left(m^{-\nu-1}\right)\right)\right. \\ & \left. -\,\frac{i^{q-1}}{\sqrt{m}}D_{1-q}(-b\sqrt{m})\left(\sum_{0\le j\le \nu}\frac{\gamma_{2j+1}}{m^j}+O\left(m^{-\nu-1}\right)\right)\right), \end{aligned}$$

for any $\nu = 0, 1, 2, \ldots$, where the γ_j's are bounded coefficients depending on m and λ. The result holds for $m \to \infty$ and $\rho \le B$, $B > 1$.

In particular, by l'Hôpital's rule,

$$\gamma_0 = \left(\frac{1}{i}\right)^q\left(\frac{\rho-1}{\rho b}\right)^{q-1}, \qquad \gamma_1 = \left(\frac{1}{i}\right)^{q-1}\frac{1}{b}\left(\left(\frac{\rho-1}{\rho b}\right)^{q-1}-\left(\frac{b}{\rho-1}\right)^q\right),$$

from which (19) follows. ∎

Recall that $\Lambda = q\log(n-m)$ and $r = \pi_{m-2}(\Lambda)/\pi_{m-1}(\Lambda)$. From Theorem 2 and the relation

$$\Pi_m(\tau;\lambda) = e^{-\lambda}(1-\tau)^{-q}\tau^m\pi_m(\lambda/\tau),$$

we obtain the estimates (8) for r.

Furthermore, by replacing q by $q-1$ in (12), we obtain the following results for the difference

$$\delta_m := \pi_m(\Lambda) - \pi_{m-1}(\Lambda) = [u^m]\frac{e^{\Lambda u}}{(1-u)^{q-1}},$$

which will be required for the proof of Theorem 1.

Lemma 1 *The difference of $\pi_m(\Lambda)$ and $\pi_{m-1}(\Lambda)$ satisfies*

$$\delta_m = \begin{cases} \dfrac{\Lambda^m}{m!(1-m/\Lambda)^{q-1}}\left(1+O\left(\dfrac{m}{(\Lambda-m)^2}\right)\right), & \text{if } 1\le m\le \Lambda - K\sqrt{\Lambda}; \\ \dfrac{e^m\rho^{-m}}{\sqrt{2\pi}}\, m^{(q-2)/2}e^{\mu^2/4}D_{1-q}(-\mu)\left(1+O\left(\dfrac{1+|\mu|^3}{\sqrt{\Lambda}}\right)\right), & \text{if } \mu=\dfrac{m-\Lambda}{\sqrt{\Lambda}}=o(\Lambda^{1/6}); \\ e^{\Lambda}\dfrac{(m-\Lambda)^{q-2}}{(q-2)!}\left(1+O\left(\dfrac{1}{m-\Lambda}\right)\right), & \text{if } m\ge \Lambda+K\sqrt{\Lambda}. \end{cases}$$

Note that the asymptotic estimates (16)–(18) can be used to check the formulae (11) and (13) in the overlapping range (*II*) with (12).

2.3 Probabilistic interpretation

The composite limiting behaviors of Ω_n can be explained by writing

$$\Omega_n = \Omega'_n + \Upsilon_n,$$

where Ω'_n and Υ_n denote the number of monic irreducible factors of degree ≥ 2 and $= 1$, respectively, in the factorization of a random polynomial in $\mathcal{P}_n$. Roughly, the Poisson behavior of Ω_n originates from Ω'_n and the negative binomial behavior from Υ_n. More precisely, we have for $n \ge 1$

$$\begin{aligned} \mathrm{P}(\Upsilon_n = m) &= q^{-n}[u^m z^n]\frac{1}{(1-uz)^q}\prod_{j\ge 2}(1-z^j)^{-I_j} \\ &= \binom{q+m-1}{m} q^{-m} \times \begin{cases} (1-q^{-1})^{-q}, & \text{if } 0\le m\le n-q; \\ \sum_{0\le k\le n-m}\binom{q}{k}(-1/q)^k, & \text{if } 0\le n-m<q, \end{cases} \end{aligned}$$

and

$$\mathrm{P}(\Omega'_n = m) = \frac{(\log n)^{m-1}}{n(m-1)!}\left(g_0\left(\frac{m-1}{\log n}\right)+O\left(\frac{m}{(q^2\log n - m)^2}\right)\right),$$

uniformly for $1 \le m \le q^2\log n - K\sqrt{\log n}$, where (cf. (3))

$$g_0(u) = (1-u/q)^q g(u).$$

In particular, the distribution of Υ converges to a negative binomial with parameters q and $1/q$. The formula for Ω'_n follows from (using essentially the singularity analysis [13], cf. [26])

$$q^{-n}[z^n]\prod_{j\ge 1}(1-uz^j)^{-I_j} = ug_0(u)n^{u-1}\left(1+O_\varepsilon(n^{-1})\right),$$

uniformly for $|u| \le q^2 - \varepsilon$; and from Selberg's method. Details are omitted here.

3 Proof of Theorems 1 and 3

In this section, we first give a fundamental formula on which the proof of Theorems 1 and 3 will be based. Then we prove Theorems 1 and 3 in the remaining subsections.

Throughout this section, we write consistently

$$P(z,u) = \frac{Q(z,u)}{(1-uz)^q}, \qquad Q(z,u) = 1+\sum_{n,m} N'(n,m)u^m z^n = \prod_{j\ge 2}(1-uz^j)^{-I_j}$$

and $\rho = (m-1)/\Lambda$. Thus $N'(n,m)$ represents the number of polynomials of degree n without factors of unit degree and with exactly m irreducible factors (multiplicities counted).

3.1 The fundamental formula

The following decomposition formula will be used to prove both Theorems 1 and 3. Intuitively, it separates the contribution of factors of degree 1 from all others and it is these factors which will make the negative binomial behavior more significant when m becomes large.

Lemma 2 *For $0 < \upsilon < 1$ and $0 < \zeta < q^{-1}$,*

$$N(n,m) = \frac{1}{(2\pi i)^2} \oint_{|u|=\upsilon} \oint_{|z|=\zeta} \frac{u^{-m-1}}{(1-u)^q} z^{-n+m-1} Q(u/z, z)\, \mathrm{d}z\, \mathrm{d}u. \tag{22}$$

Proof. It is easily verified that

$$\begin{aligned} N(n,m) &= [u^m z^n] P(z,u) = [u^m z^n] \frac{Q(z,u)}{(1-uz)^q} \\ &= [u^m z^{n-m}] \frac{Q(u/z,z)}{(1-u)^q}, \end{aligned}$$

from which (22) follows by Cauchy's formula. ∎

Note that from the above decomposition, we have for $n/2 < m \le n$

$$\begin{aligned} N(n,m) &= \sum_{0\le j\le m} \binom{q+j-1}{j} N'(n-j, m-j) \\ &= \sum_{0\le j\le n-m} \binom{q+m-j-1}{m-j} N'(n-m+j, j), \end{aligned} \tag{23}$$

since $N'(a,b) = 0$ for $b > a/2$. Although this last expression can also be used to prove (14), we prefer a more unified proof by (22) and the singularity analysis.

The next lemma will be very useful.

Lemma 3 *If $n - m \to \infty$ then*

$$[z^{n-m}] Q(u/z, z) = uG(u) q^{n-m+1} (n-m)^{qu-1} \left(1 + T(u)\right), \tag{24}$$

where G is defined in (6) and

$$T(u) \ll_\varepsilon \frac{\log(n-m)}{n-m} \ll_\varepsilon \Lambda e^{-\Lambda/q} \qquad (|u| \le q - \varepsilon,\ \varepsilon > 0).$$

Proof. We have

$$Q(u/z, z) = e^{-qu + uI(z)/z} S(z,u), \qquad S(z,u) = \prod_{j\ge 2} \left(\frac{e^{-uz^{j-1}}}{1 - uz^{j-1}} \right)^{I_j}.$$

From (1), we deduce the local expansion

$$Q(u/z, z) = uG(u)\Gamma(qu)(1-qz)^{-qu} \left(1 + O\left((z - q^{-1}) \log \frac{1}{1-qz}\right)\right) \qquad (z \sim q^{-1}),$$

uniformly for z in any compact region in the cut-disk:

$$\{z : |z| < q^{-1/2} - \varepsilon,\ z \notin [q^{-1}, q^{-1/2}]\}.$$

By choosing a suitable Hankel type contour in the style of [13] and using the singularity analysis (cf. [26] for details), we obtain (24). ∎

3.2 Proof of Theorem 3

For the proof of Theorem 3, we first evaluate the integrals in (22) with respect to u.

We have, for $|z| < q^{-1}$ and u in a small neighborhood of 1,

$$\begin{aligned} Q(u/z, z) &= Q(1/z, z) \exp\left(\sum_{\ell \geq 1} \frac{(-1)^\ell}{\ell} h_\ell(z)(1-u)^\ell \right) \\ &= Q(1/z, z) \left(1 + \sum_{\ell \geq 1} H_\ell(z)(1-u)^\ell \right), \end{aligned}$$

where

$$h_\ell(z) = \sum_{j \geq 2} I_j \left(\frac{z^{j-1}}{1 - z^{j-1}} \right)^\ell = \frac{q(q-1)}{2} z^\ell + \cdots,$$

and the H_ℓ's are linear combinations of h_ℓ. Thus

$$\begin{aligned} &[z^{n-m}][u^m] \frac{Q(u/z, z)}{(1-u)^q} \\ &\quad = [z^{n-m}] Q(1/z, z) \binom{q+m-1}{m} + [z^{n-m}] \sum_{1 \leq \ell \leq q-1} H_\ell(z) Q(1/z, z) \binom{q-\ell+m-1}{m} \\ &\qquad + (-1)^m \sum_{\ell \geq m} [z^{n-m}] H_{\ell+q}(z) \binom{\ell}{m}. \end{aligned}$$

But the last sum is identically zero when $m > (n-q)/2$ since $H_\ell(z) = c_\ell z^\ell + \cdots$ for some coefficient c_ℓ. On the other hand, since

$$h_\ell(z) = \frac{1}{z^\ell} \left(\log \frac{1}{1 - q z^\ell} - q z^\ell \right) + \widetilde{h}_\ell(z),$$

where $\widetilde{h}_\ell$ is analytic for $|z| < q^{-1/2}$, we have

$$[z^{n-m}] Q(1/z, z) H_\ell(z) \ll q^{n-m} (n-m)^{q-1} \left(\log(n-m) \right)^\ell \qquad (\ell = 1, 2, \ldots, q-1),$$

by Lemma 3 and the singularity analysis. Therefore

$$N(n, m) = \binom{q+m-1}{m} \beta_{n,m} + E,$$

where E is $\ll m^{q-2}$ when $n - m \ll 1$; and

$$E \ll q^{-m} (n-m)^{q-1} \sum_{1 \leq \ell \leq q-1} \binom{q-\ell+m-1}{m} \left(\log(n-m) \right)^\ell \ll q^{-m} (n-m)^{q-1} \frac{\log(n-m)}{m},$$

when $n - m \to \infty$. Thus we obtain (14) in any case. The asymptotic estimate of $\beta_{n,m}$ follows from Lemma 3. ∎

3.3 Proof of Theorem 1

We use again (22) but in the opposite order, namely, first with respect to z and then with respect to u.

With (22) and (24), we can write

$$N(n, m) = \frac{q^{n-m}}{n-m} \left(N_1 + N_2 \right),$$

where

$$N_1 = [u^{m-1}]G(u)\frac{(n-m)^{qu}}{(1-u)^q}, \qquad N_2 = [u^{m-1}]G(u)T(u)\frac{(n-m)^{qu}}{(1-u)^q}.$$

Recall that $r = \pi_{m-2}(\Lambda)/\pi_{m-1}(\Lambda)$.

Lemma 4 *If $m \geq 1$ and $n - m \to \infty$ then*

$$N_1 = G(r)\pi_{m-1}(\Lambda)\left(1 + O(\Lambda^{-1})\right).$$

Proof. We use again Selberg's method. The choice of r implies that

$$N_1 = \frac{1}{2\pi i}\oint_{|u|=r} u^{-m}G(u)\frac{e^{\Lambda u}}{(1-u)^q}\,\mathrm{d}u = G(r)\pi_{m-1}(\Lambda) + 0 + J,$$

where

$$J = \frac{1}{2\pi i}\oint_{|u|=r}\frac{(u-r)^2}{(1-u)^q}G_2(u,r)u^{-m}e^{\Lambda u}\,\mathrm{d}u,$$

with $G_2(u,r) = \int_0^1(1-t)G''(r+t(u-r))\,\mathrm{d}t$. We now show that

$$J \ll \pi_{m-1}(\Lambda)\Lambda^{-1}, \tag{25}$$

The method of proof will be different from those in Balazard [3] and in Hwang [25]. We divide the proof of (25) into three cases.

Case 1 $1 \leq m \leq \Lambda - K\sqrt{\Lambda}$.

By Laplace's method and the first formula of Lemma 1, we have

$$\begin{aligned} J &\ll \frac{r^{1-m}}{(1-r)^q}\,e^{r\Lambda}r^2\int_{-\pi}^{\pi} t^2 e^{-r\Lambda(1-\cos t)}\,\mathrm{d}t \ll \frac{r^{1/2}\Lambda^{-3/2}}{(1-r)^q}\,r^{1-m}e^{r\Lambda} \\ &= \frac{\pi_{m-1}(\Lambda)}{\pi_{m-1}(\Lambda)-\pi_{m-2}(\Lambda)}\cdot\frac{r^{1/2}\Lambda^{-3/2}}{(1-r)^{q-1}}\,r^{1-m}e^{r\Lambda} \\ &\ll \pi_{m-1}(\Lambda)\left(\frac{1-\rho}{1-r}\right)^{q-1}\frac{(m-1)!}{\Lambda^{m-1}}\,L(r)r^{1/2}\Lambda^{-3/2}, \end{aligned}$$

where $L(t) := t^{1-m}e^{t\Lambda}$. We now show that L satisfies

$$L(r) \ll L(\rho), \tag{26}$$

for $1 \leq m \leq \Lambda - K\sqrt{\Lambda}$. To see this, observe that $L'(t) = L(t)(\Lambda - (m-1)/t)$ for $t > 0$. By the first mean value theorem, we have

$$\begin{aligned} L(t) &= L(\rho)\left(1 - \frac{\rho - t}{L(\rho)}L'(\rho - \theta(\rho - t))\right) \qquad (0 < \theta < 1,\, 0 < t \leq 1) \\ &= L(\rho)\left(1 - \frac{L(\rho-\theta(\rho-t))}{L(\rho)}(\rho - t)\left(\Lambda - \frac{m-1}{t}\right)\right) \\ &\leq L(\rho)\left(1 - (\rho - t)\left(\Lambda - \frac{m-1}{t}\right)\right), \end{aligned}$$

since L attains the minimum at $\rho = (m-1)/\Lambda$. This inequality together with (8) yield

$$\begin{aligned} L(r) &\leq L(\rho)\left(1 + \frac{\Lambda}{r}(\rho - r)^2\right) \ll L(\rho)\left(1 + \frac{\Lambda\rho}{(\Lambda - m + 1)^2}\right) \\ &\ll L(\rho)\left(1 + \frac{m-1}{(\Lambda-m+1)^2}\right) \ll L(\rho)\left(1 + \frac{1}{A^2}\right) \\ &\ll L(\rho). \end{aligned}$$

Thus (26) follows.

With the inequality (26) and returning to J, we have

$$\begin{aligned} J &\ll \pi_{m-1}(\Lambda)\frac{(m-1)!}{\Lambda^{m-1}}L(\rho)r^{1/2}\Lambda^{-3/2} \\ &\ll \pi_{m-1}(\Lambda)\sqrt{m-1}\,r^{1/2}\Lambda^{-3/2} \\ &\ll \pi_{m-1}(\Lambda)\frac{m-1}{\Lambda^2} \\ &\ll \pi_{m-1}(\Lambda)\Lambda^{-1}, \end{aligned} \tag{27}$$

by Stirling's formula and (8).

For the remaining two cases we use the decomposition

$$\frac{(u-r)^2}{(1-u)^q} = \frac{(1-r)^2}{(1-u)^q} - 2\frac{1-r}{(1-u)^{q-1}} + \frac{1}{(1-u)^{q-2}}$$

and write $J = J_1 + J_2 + J_3$, J_i corresponding to replacing the factor $(u-r)^2/(1-u)^q$ in J by the i-th term on the right-hand side. It follows that

$$J \ll J_1 + J_2 + J_3 \ll (1-r)^{-q+2}r^{-1/2}\Lambda^{-1/2}r^{-m}e^{r\Lambda},$$

and thus

$$J \ll \frac{\pi_{m-1}(\Lambda)}{\pi_{m-1}(\Lambda)-\pi_{m-2}(\Lambda)}\frac{r^{-1/2}\Lambda^{-1/2}}{(1-r)^{q-3}}\,r^{-m}e^{r\Lambda}.$$

Case 2 $m \geq \Lambda + K\sqrt{\Lambda}$.

In this case we have by the third formula of Lemma 1 and (8)

$$\begin{aligned} J &\ll \pi_{m-1}(\Lambda)(m-1-\Lambda)^{-1}\Lambda^{-1}e^{\Lambda(r-1-\log r)-K\sqrt{\Lambda}\log r} \\ &\ll \pi_{m-1}(\Lambda)(m-1-\Lambda)^{-1}\Lambda^{-1} \ll \pi_{m-1}(\Lambda)\Lambda^{-1}, \end{aligned}$$

since

$$\Lambda(r-1-\log r) \ll \Lambda(r-1)^2 \ll A^{-2} \ll 1, \qquad \sqrt{\Lambda}\log r \ll \sqrt{\Lambda}(r-1) \ll 1.$$

Case 3 $m = \Lambda + \mu\sqrt{\Lambda}$, $|\mu| \leq K$.

Again, by the second formula of Lemma 1 and (8), we have

$$\begin{aligned} J &\ll \pi_{m-1}(\Lambda)m^{-(q-2)/2}\Lambda^{-1/2}m^{(q-3)/2}e^{\Lambda(1-r-\log r)-\mu\sqrt{\Lambda}\log r} \\ &\ll \pi_{m-1}(\Lambda)m^{-1/2}\Lambda^{-1/2} \ll \pi_{m-1}\Lambda^{-1}. \end{aligned}$$

Following exactly the same line of arguments, we can show that the contribution of N_2 is negligible.

Lemma 5 *For $m \geq 1$ and $n - m \to \infty$*

$$N_2 \ll \pi_{m-1}(\Lambda)\Lambda e^{-\Lambda/q} \ll \pi_{m-1}(\Lambda)\Lambda^{-1}.$$

Proof. Omitted. ∎

Collecting the above results, we complete the proof of Theorem 1. ∎

4 Local behaviors of Ω_n

The combination of Theorems 1 and 2 yields more precise (and elementary) local asymptotics of N. As the derivations are straightforward computations, they are omitted here.

4.1 Poisson range

Our first result is more precise than Car's (2):

Corollary 1 *If* $1 \le m \le q\log n - K\sqrt{\log n}$, *then*

$$\mathrm{P}(\Omega_n = m) = \frac{(\log n)^{m-1}}{n(m-1)!}\left(g\left(\frac{m-1}{\log n}\right) + O\left(\frac{m-1}{(q\log n - m)^2}\right)\right),$$

uniformly in m.

Proof. Apply Theorem 1 together with the better estimate (27). ∎

In particular, since $g(1) = 1$, we have for $m = \log n + \omega_n$, where $\omega_n = o(\log n)$,

$$\mathrm{P}(\Omega_n = m) = \frac{(\log n)^{m-1}}{n(m-1)!}\left(1 + O\left(\frac{1+\omega_n}{\log n}\right)\right),$$

This certainly implies that the distribution of Ω_n is asymptotically normal.

4.2 Transitional range

Corollary 2 *If* $\mu = (m - q\log n)/\sqrt{\log n} = o((\log n)^{1/6})$, *then*

$$\mathrm{P}(\Omega_n = m) = \frac{G(1)}{\sqrt{2\pi m}}\, n^{-1} e^m m^{-m} (\log n)^{m-1} m^{q/2} e^{\mu^2/4} D_{-q}(-\mu)\left(1 + O\left(\frac{1+|\mu|^3}{\sqrt{\log n}}\right)\right).$$

Note that by Stirling's formula the result can also be written as

$$\mathrm{P}(\Omega_n = m) = G(1)\frac{(\log n)^{m-1}}{n\, m!}\, m^{q/2} e^{\mu^2/4} D_{-q}(-\mu)\left(1 + O\left(\frac{1+|\mu|^3}{\sqrt{\log n}}\right)\right).$$

4.3 Negative binomial range

Corollary 3 *If* $m \ge q\log n + K\sqrt{\log n}$ *and* $n - m \to \infty$, *then*

$$\mathrm{P}(\Omega_n = m) = G(1) q^{-m+1} \frac{(n-m)^{q-1}(m - q\log n)^{q-1}}{(q-1)!}\left(1 + O\left(\frac{\log n}{(m - q\log n)^2}\right)\right).$$

A combination of Theorem 3 and the above corollary yields the following

Corollary 4 *For* $q\log n + K\sqrt{\log n} \le m \le n$, *we have*

$$\mathrm{P}(\Omega_n = m) \sim \frac{(m - q\log n)^{q-1}}{(q-1)!}\beta_{n,m}.$$

Thus when $m \ge q\log n + K\sqrt{\log n}$ there is an abundant number of factors of degree 1.

5 Global behaviors of Ω_n

Besides the uniform asymptotic formula (7), we consider in this section other properties of Ω_n.

5.1 Unimodality

As in [4] and in [25], we show that the sequence $\{N(n,m)\}_m$ first increases and then decreases. But instead of following a similar line of proof, we use again our fundamental formula to keep consistency.

Theorem 4 *For sufficiently large values of n, we have (i) if $q=2$ then $N(n,m)$ is unimodal in m for $1\le m\le n-1$, and $N(n,n-1)-N(n,n)=-2$ for $n\ge 2$; (ii) if $q\ge 3$ then $N(n,m)$ is unimodal in m for $1\le m\le n$. In both cases, the mode of the distribution is attained at the integral part of μ, where, asymptotically,*

$$\mu=\log n+g'(1)-\frac{2g'(1)^3-2g'(1)^2-3g'(1)g''(1)+2g''(1)+g'''(1)}{2\log n}+O\left((\log n)^{-2}\right),$$

g being defined in (3).

Note that

$$\begin{aligned} g'(1) &= \gamma-1+\sum_{j\ge 1} I_j\left(\log\left(1-q^{-j}\right)+\frac{1}{q^j-1}\right)\\ &= \gamma-1+\sum_{j\ge 1}\left(\frac{I_j}{q^j-1}-\frac{1}{j}\right), \end{aligned}$$

γ being Euler's constant, and that the mean of Ω_n satisfies

$$\mathrm{E}(\Omega_n)=\log n+g'(1)+1+(n^{-1}).$$

Proof. We divide the range $1\le m\le n$ into three parts:

1. $m=n-1$;
2. $1\le n-m\le K$;
3. $K\le n-m\le n-1$.

Consider first the case $m=n-1$. We have by (23)

$$\begin{aligned} N(n,n-1)-N(n) &= \binom{q+n-3}{q-1}\frac{q(q-1)}{2}-\binom{q+n-1}{q-1}\\ &= \frac{(q+n-3)!}{(q-1)!n!}\left(\frac{(q+1)(q-2)}{2}n^2-\frac{q^2+3q-6}{2}n-(q-1)(q-2)\right), \end{aligned}$$

from which we conclude that $N(n,n-1)-N(n,n)=-2$ for $q=2$ and $N(n,n-1)-N(n,n)>0$ for $q\ge 3$ and for sufficiently large n.

For the case $1\le n-m\le K$, we use Theorem 3:

$$N(n,m)-N(n,m+1)=\frac{m^{q-1}}{(q-1)!}\left(\beta_{n,m}-\beta_{n,m+1}\right)\left(1+O_K\left(\frac{1}{n}\right)\right),$$

where by definition $(0<\zeta<1/q)$

$$\begin{aligned} \beta_{n,m}-\beta_{n,m+1} &= \frac{q^{-n}}{2\pi i}\oint_{|z|=\zeta} z^{-n+m-1}(1-z)\prod_{j\ge 2}\left(1-z^{j-1}\right)^{-I_j}\mathrm{d}z\\ &= \frac{q^{-n}}{2\pi i}\oint_{|z|=\zeta} z^{-n+m-1}(1-z)^{-I_2+1}\prod_{j\ge 3}\left(1-z^{j-1}\right)^{-I_j}\mathrm{d}z\\ &\ge 0, \end{aligned}$$

since $I_2 - 1 = \frac{1}{2}q(q-1) - 1 \geq 0$.

For the remaining range, we use again our fundamental formula (22):

$$N(n,m) - N(n,m+1) = \frac{1}{(2\pi i)^2} \oint_{|u|=v} \oint_{|z|=\zeta} \frac{u^{-m-1}}{(1-u)^q} (1 - z/u) z^{-n+m-1} Q(u/z, z)\, \mathrm{d}z\, \mathrm{d}u$$

and apply *mutatis mutandis* the methods of proof of Lemmas 3–5. The resulting formula is

$$N(n,m) - N(n,m+1) = q^n \frac{1 - (qr)^{-1}}{(1-q^{-1})^q} G(r) \Pi_{m-1}(\Lambda) \left(1 + O(\Lambda^{-1})\right),$$

uniformly for $m \geq 1$ and $n - m \geq K$, where $\Lambda = q \log(n-m)$. We need only determine the sign of the factor $(1 - 1/qr)$. From (8), we deduce that there is a sufficiently large number $A > 1$ such that

$$1 - \frac{1}{qr} \begin{cases} < 0, & \text{if } 1 \leq m \leq \Lambda/q - A; \\ > 0, & \text{if } m \geq \Lambda/q + A,\ n - m \geq K. \end{cases}$$

The remaining interval $(\Lambda/q - A, \Lambda/q + A)$ is then completed either by the local limit theorem (4) or by a direct computation starting from the uniform asymptotic formula (using the singularity analysis, cf. [26])

$$[z^n] P(z,u) = u g(u) q^n n^{u-1} \left(1 + O_\varepsilon\left(n^{-1}\right)\right), \tag{28}$$

uniformly for $|u| \leq q - \varepsilon$. This last formula can also be used to determine the position of the mode to great precision by writing $m - 1 = \log n + m_0$ and by Laplace's method applying to the integral

$$N(n,m) - N(n,m+1) = \frac{q^n}{2\pi} \int_{-\pi}^{\pi} g(e^{it})(1 - e^{-it}) e^{-i(m-1)t} n^{it-1} \left(1 + O_\varepsilon\left(n^{-1}\right)\right) \mathrm{d}t. \quad \blacksquare$$

The advantage of the above arguments is that they can be easily extended to the consideration of the k-th difference:

$$\begin{aligned} \nabla_k(n,m) &:= \sum_{0 \leq j \leq k} \binom{k}{j} (-1)^j N(n, m+j) \\ &= \frac{q^{-n}}{(2\pi i)^2} \oint_{|u|=v} \oint_{|z|=\zeta} \frac{u^{-m-1}}{(1-u)^q} (1 - z/u)^k z^{-n+m-1} Q(u/z, z)\, \mathrm{d}z\, \mathrm{d}u. \end{aligned}$$

Only the range $0 \leq n - m \leq K$ requires further treatment and will not be given here. For the case $n - m \geq K$, the conclusion is $\nabla_{2k}(n,m) \geq 0$ and $\nabla_{2k+1}(n,m)$ behaves like $\nabla_1(n,m)$ as $n \to \infty$, namely, it is increasing for $1 \leq m \leq \mu$ and then decreases. Actually, we have more precise quantitative asymptotic estimates.

5.2 The distribution function of Ω_n

In this section, we briefly discuss the asymptotic behavior of the distribution function $\mathrm{P}(\Omega_n \leq m)$. While the local behavior of Ω_n is well approximated by a Poisson $*$ negative binomial convolution law, the cumulative behavior of Ω_n is essentially Poisson; thus the negative binomial part is asymptotically negligible.

Let us first consider the distribution function of U (cf. § 2):

$$\mathrm{P}(U \leq m) = \sum_{j \leq m} \Pi_j(\tau; \lambda) = \frac{1}{2\pi i} \oint_{|z|=\zeta} \frac{z^{-m-1}}{1-z} e^{\lambda(z-1)} \varphi(z)\, \mathrm{d}z,$$

where $0 < \zeta < 1$ and $\varphi(z) = (1-\tau)^q/(1-\tau z)^q$.

Since the function φ is analytic for $|z| < 1/\tau$, we obtain, by the same methods of proof of Lemma 4,

$$\mathrm{P}(U \le m) = \varphi(\varrho) \sum_{0\le j\le m} \frac{\lambda^j}{j!}\, e^{-\lambda} \left(1 + O\left(\lambda^{-1}\right)\right),$$

where $\varrho = 0$ if $m = 1$, and

$$\varrho = \varrho(\lambda; m) = \frac{\sum_{0\le j\le m-1} \lambda^j e^{-\lambda}/j!}{\sum_{0\le j\le m} \lambda^j e^{-\lambda}/j!} \sim \min\left\{1, \frac{m}{\lambda}\right\}.$$

As for $\mathrm{P}(\Omega \le m)$, we have

$$\mathrm{P}(\Omega_n \le m) = \frac{q^{-n}}{(2\pi i)^2} \oint_{|u|=\upsilon} \oint_{|z|=\zeta} \frac{u^{-m-1}}{1-u} z^{-n-1} P(z,u)\, \mathrm{d}z\, \mathrm{d}u,$$

where $0 < \upsilon < 1$ and $0 < \zeta < q^{-1}$.

Theorem 5 *For $1 \le m \le n$, we have*

$$\mathrm{P}(\Omega_n \le m) = g(r_0) n^{-1} \sum_{0\le j\le m-1} \frac{(\log n)^j}{j!} \left(1 + O\left((\log n)^{-1}\right)\right),$$

uniformly in m, where $r_0 = \varrho(\log n; m-1)$.

Proof. (Sketch) By (28) and the methods of proof of Lemmas 3–5. ∎

Corollary 5 *For $1 \le m \le n$, we have*

$$\mathrm{P}(\Omega_n \le m) \sim g\left(\min\left\{1, \frac{m-1}{\log n}\right\}\right) n^{-1} \sum_{0\le j\le m-1} \frac{(\log n)^j}{j!}.$$

5.3 Rényi's problem

In number theory, Rényi's problem is concerned with the distribution of the difference of the total number of prime factors (with multiplicity) and the number of distinct prime factors (without multiplicity) of an integer. While this problem is not yet completely characterized for all possible forms of variation of the second parameter (cf. [42, 44]), the analogous problem for finite fields can be completely solved by the methods of this paper.

Let Δ_n be the random variable representing the difference of the total number of irreducible factors and the number of distinct irreducible factors of a random polynomial in $\mathcal{P}_n$. Then by definition we have the generating function

$$1 + \sum_{n\ge 1} z^n \sum_{\pi\in\mathcal{P}_n} u^{\Delta_n(\pi)} = \prod_{j\ge 1} \left(1 + \frac{z^j}{1-uz^j}\right)^{I_j}.$$

Since

$$\prod_{j\ge 1} \left(1 + \frac{z^j}{1-uz^j}\right)^{I_j} = \frac{1}{1-qz} \prod_{j\ge 1} \left(\left(1 + \frac{z^j}{1-uz^j}\right)\left(1-z^j\right)\right)^{I_j},$$

we deduce easily that $\lim_{n\to\infty} \mathrm{P}(\Delta_n = m)$ exists for each m:

$$\lim_{n\to\infty} \mathrm{P}(\Delta_n = m) = d_m,$$

where

$$d_m = [u^m] \prod_{j\ge 1} \left(\left(1 + \frac{1}{q^j - u}\right)\left(1 - q^{-j}\right)\right)^{I_j}.$$

Thus the limiting distribution of Δ_n is discrete. Asymptotically, we have

$$d_m = \gamma_q q^{-m} \frac{m^{q-1}}{(q-1)!} \left(1 + O\left(m^{-1}\right)\right) \qquad (m \to \infty),$$

where

$$\gamma_q = q^{-q} \left(1 - q^{-1}\right)^q \prod_{j \geq 2} \left(\left(1 + \frac{1}{q^j - q}\right)\left(1 - q^{-j}\right)\right)^{I_j}.$$

The problem of interest here is a more precise description of the remainder term. By the methods of this paper, we can obtain the following results.

Theorem 6 *If $m \geq 0$ and $n - m \to \infty$, then*

$$\mathrm{P}(\Delta_n = m) = d_m + V(r_1) q^{-(n+m-1)/2} (n-m)^{-2} \pi_{m-1}\left(\sqrt{q}\log(n-m)\right)\left(1 + O\left(\frac{1}{\log(n-m)}\right)\right),$$

where

$$\begin{aligned} V(u) &= \frac{\sqrt{q}u - 1}{\Gamma(\sqrt{q}u + 1)} \left(1 + q^{-1/2} - u\right)^q \left(1 - q^{-1}\right)^{q(\sqrt{q}u-1)} \\ &\quad \times \prod_{j \geq 2} \left(\left(1 + \frac{1}{q^{j/2} - q^{-1/2}u}\right)\left(1 - q^{-j/2}\right)(1 - q^{-j})^{\sqrt{q}u-1}\right)^{I_j}, \end{aligned}$$

and $r_1 = \pi_{m-2}(\sqrt{q}\log(n-m))/\pi_{m-1}(\sqrt{q}\log(n-m))$.

6 Conclusion

We have presented a set of analytic tools which are useful for describing the global statistical behaviors of parameters in structures whose bivariate generating functions are of the form

$$\prod_{j \geq 1} (1 - uz^j)^{-c_j},$$

a standard generating function for multiset constructions. Our methods are especially useful when the radius of convergence of the power series $C(z) = \sum_{j \geq 1} c_j z^j$ lies strictly in the unit interval. For applications of the methods to integer partitions (for which the radius of convergence of C is always 1), see [24] (cf. also [34]).

The enumerating polynomials $P_n(u) = [z^n]P(z,u)$ seem to have some intriguing qualitative properties which remain unknown. Figure 1 depicts the distribution of the zeros of two such polynomials. The figure suggests that the zeros are contained in certain small circles which tend to a certain simple contour.

On the other hand, simulations suggest that the polynomials

$$\begin{aligned} R_n(u) &= [z^n] \prod_{j \geq 1} \left(1 + \frac{uz^j}{1 - z^j}\right)^{I_j}, \\ Q_n(u) &= [z^n] \prod_{j \geq 1} \left(1 + uz^j\right)^{I_j}, \\ S_n(u) &= [z^n] \prod_{j \geq 1} \left(1 + I_j uz^j\right) \end{aligned}$$

all have their roots lying in the left half-plane $\Re u < 0$ (except for the trivial simple zero at the origin). These polynomials have natural interpretations: $R_n(u)$ and $Q_n(u)$ are the generating polynomials for

Figure 1: The distribution of the zeros of the two polynomials $P_{30}(u)$ and $P_{60}(u)$ when $q = 2$.

the number of polynomials in $\mathcal{P}_n$ having m distinct irreducible factors with and without, respectively, repetitions; $S_n(u)$ is the generating polynomials for the number of polynomials in $\mathcal{P}_n$ into m distinct degree irreducible factors. If the observed phenomenon were true then we would have local limit theorems for the underlying quantities, results that can be established by other methods (cf. [26]); moreover, other properties like unimodality would also follow.

Asymptotic behaviors of the two sequences

$$[u^m z^n] \prod_{j\geq 1} \left(1 + \frac{uz^j}{1-z^j}\right)^{I_j}, \qquad [u^m z^n] \prod_{j\geq 1} \left(1 + uz^j\right)^{I_j}$$

for $m \ll \log n$ can be treated by application of the singularity analysis and Selberg's method (cf. [9, 40, 26]). Different methods, like the two-dimensional saddle-point method (cf. [22, 43]), are, however, required when $m \gg \log n$.

The methods used in this paper can also be applied to the number of irreducible factors (multiplicities counted) in the polynomial factorization of the characteristic polynomial in a random element in $GL_n(\mathbf{F}_q)$ with bivariate generating function (cf. [37, 19])

$$\prod_{k\geq 1} \left(\prod_{j\geq 1} \frac{1}{1 - wz^k/q^{kj}}\right)^{e(k)},$$

where $e(1) = I_1 - 1 = q - 1$ and $e(k) = I_k$ for $k \geq 2$. Other problems to which our methods apply include: arithmetical semigroups under Axiom $\mathrm{A}^{\#}$ of Knopfmacher (cf. [30]), the uniform distribution

modulo k (cf. [26]), the problem of "factorisatio numerorum" in arithmetical semigroups (cf. [29, 26]), and number-theoretic functions like the number of *integer* factors of a randomly chosen integer between 1 and x (cf. [26]).

Acknowledgement

The author wishes to thank one of the referees for his (or her) careful reading and useful comments.

References

[1] R. Arratia, A. D. Barbour, and S. Tavaré, On random polynomials over finite fields, *Mathematical Proceedings of the Cambridge Philosophical Society*, 114, 347–368 (1993).

[2] R. Arratia and S. Tavaré, Independent process approximations for random combinatorial structures, *Advances in Mathematics*, 104, 90–154 (1994).

[3] M. Balazard, *Sur la répartition des valeurs de certaines fonctions arithmétiques additives*, Thèse, Université de Limoges, 1987.

[4] M. Balazard, Comportement statistique du nombre de facteurs premiers des entiers, In *Séminaire de Théorie des Nombres, Paris 1987–88*, pages 1–21, Birkäuser, 1990.

[5] M. Balazard, H. Delange, and J.-L. Nicolas, Sur le nombre de facteurs premiers des entiers, *Comptes Rendus de l'Académie des Sciences, Série I, Paris*, 306, 511–514 (1988).

[6] N. Bleistein, Uniform asymptotic expansions of integrals with stationary point near algebraic singularity, *Communications on Pure and Applied Mathematics*, 19, 353–370 (1966).

[7] N. Bleistein and R. A. Handelsman, *Asymptotic expansions of integrals*, Dover Publications, Inc., New York, 1986.

[8] E. R. Canfield. Central and local limit theorems for the coefficients of polynomials of binomial type. *Journal of Combinatorial Theory, Series A*, 23, 275–290 (1977).

[9] M. Car, Factorisation dans $\mathbf{F}_q[X]$, *Comptes Rendus de l'Académie des Sciences, Série I, Paris*, 294, 147–150 (1982).

[10] S. D. Cohen, Further arithmetical functions in finite fields, *Proceedings of the Edinburgh Mathematical Society*, 16, 349–363 (1969).

[11] P. Diaconis, M.-J. McGrath and J. Pitman, Riffle shuffles, cycles, and descents, *Combinatorica*, 15, 11–29 (1995).

[12] A. Erdélyi, *Higher transcendental functions, volume I*, Robert E. Krieger Publishing Company, Malabar, Florida, 1953.

[13] P. Flajolet and A. M. Odlyzko, Singularity analysis of generating functions, *SIAM Journal on Discrete Mathematics*, 3, 216–240 (1990).

[14] P. Flajolet and M. Soria, Gaussian limiting distributions for the number of components in combinatorial structures, *Journal of Combinatorial Theory, Series A*, 53, 165–182 (1990).

[15] Z. Gao and L. B. Richmond, Central and local limit theorems applied to asymptotic enumeration IV: multivariate generating functions, *Journal of Computational and Applied Mathematics*, 41, 177–186 (1992).

[16] C. F. Gauss, *Untersuchungen über höhere Arithmetik*, Springer, Berlin, 1889. German translation of "Disquisitiones arithmeticae", reprinted by Chelsea, N.Y., 1965.

[17] Jennie C. Hansen, Factorization in $\mathbf{F}_q[x]$ and Brownian motion, *Combinatorics, Probability and Computing*, 2, 285–299 (1993).

[18] Jennie C. Hansen, Order statistics for decomposable combinatorial structures, *Random Structures and Algorithms*, 5, 517–533 (1994).

[19] Jennie C. Hansen and E. Schmutz, How random is the characteristic polynomial of a random matrix? *Mathematical Proceedings of the Cambridge Philosophical Society*, 114, 507–515 (1993).

[20] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford science publications, Oxford, fifth edition, 1979.

[21] T. E. Harris, *The theory of braching processes*, Springer-Verlag, Berlin, 1963.

[22] A. Hildebrand and G. Tenenbaum, On the number of prime factors of an integer, *Duke Mathematical Journal*, 56, 471–501 (1988).

[23] H.-K. Hwang, Asymptotics of Poisson approximation to random discrete distributions: an analytic approach, submitted.

[24] H.-K. Hwang, Distributions of integer partitions with large number of summands, *Acta Arithmetica*, 78, 351–365 (1997).

[25] H.-K. Hwang, A Poisson $*$ geometric law for the number of components in unlabelled combinatorial structures, *Combinatorics, Probability and Computing*, to appear.

[26] H.-K. Hwang, *Théorèmes limites pour les structures combinatoires et les fonctions arithmétiques*, Thèse, Ecole polytechnique, 1994.

[27] N. L. Johnson, S. Kotz, and A. W. Kemp, *Univariate discrete distributions*, John Wiley & Sons, Inc., New York, second edition, 1992.

[28] D. Jungnickel, *Finite fields—structure and arithmetics*, Bibliographisches Institut, Mannheim, 1993.

[29] A. Knopfmacher, J. Knopfmacher, and R. Warlimont, "Factorisatio numerorum" in arithmetical semigroups, *Acta Arithmetica*, 61, 327–336 (1992).

[30] J. Knopfmacher, *Abstract analytic number theory*, North-Holland, Amsterdam, 1975.

[31] D. E. Knuth, *The art of computer programming, volume II, seminumerical algorithms*, Second edition, Addison Wesley, Reading, MA, 1981.

[32] R. Lidl and H. Niederreiter, *Finite fields*, Addison-Wesley, Reading, MA, 1983.

[33] T. Łuczak and B. Pittel, Components of random forests, *Combinatorics, Probability, and Computing*, 1, 35–52 (1992).

[34] B. Pittel, On a likely shape of the random Ferrars diagram, *Advances in Applied Mathematics*, 18, 432–488 (1997).

[35] A. Selberg, Note on a paper by L. G. Sathe, *Journal of the Indian Mathematical Society*, 18, 83–87 (1954).

[36] I. E. Shparlinski, *Computational and algorithmic problems in finite fields*, Kluwer Academic Publishers Group, Dordrecht, 1992. Mathematics and its Applications (Soviet Series), 88.

[37] R. Stong, Some asymptotic results on finite vector spaces, *Advances in Applied Mathematics*, 9, 167–199 (1988).

[38] N. M. Temme, Uniform asymptotic expansions of confluent hypergeometric functions, *Journal of the Institute of Mathematics and its Applications*, 22, 215–223 (1978).

[39] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, Institut Elie Cartan, Université de Nancy I, Nancy, France, 1990. English version by C. B. Thomas, Cambridge University Press, 1995.

[40] R. Warlimont, Arithmetical semigroups IV: Selberg's analysis, *Archiv der Mathematik*, 60, 58–72 (1993).

[41] E. T. Whittaker and G. N. Watson, *A course of modern analysis,* an introduction to the general theory of infinite processes and of analytic functions; with an account of the principal transcendental functions, Cambridge University Press, Cambridge, 4th edition, 1927.

[42] D. Wolke, On a problem of Rényi, *Monatshefte für Mathematik*, 111, 323–330 (1991).

[43] R. Wong, *Asymptotic approximations of integrals*, Academic Press, Inc., Boston, 1989.

[44] J. Wu, Sur un problème de Rényi, *Monatshefte für Mathematik*, 117, 303–322 (1994).