國立交通大學

應用數學系

碩士論文

以解析組合的方法討論有限體下多項式的性質

Random Polynomials over Finite Fields via Analytic Combinatorics

研 究 生：江紀葳

指導教授：符麥克 教授

中華民國一〇一年十一月

以解析組合的方法討論有限體下多項式的性質

Random Polynomials over Finite Fields via Analytic Combinatorics

研究生：江紀葳　　Student: Chi-Wei Chiang

指導教授：符麥克　　Advisor: Michael Fuchs

國立交通大學

應用數學系

碩士論文

A Thesis
Submitted to Department of Applied Mathematics
National Chiao Tung University
in Partial Fulfillment of the Requirements
for the Degree of
Master
in

Applied Mathematics

November 2012

Hsinchu, Taiwan, Republic of China

中華民國一〇一年十一月

Random Polynomials over Finite Fields via Analytic Combinatorics

Chi-Wei Chiang

Department of Applied Mathematics,
National Chiao Tung University

This thesis was supervised by Dr. Michael Fuchs

November 12, 2012

Preface

Properties of irreducible factors of random polynomials over finite fields (similar to properties of irreducible factors of random integers) have been intensively studied in the mathematical literature. Such properties have applications in computer science, cryptography, coding theory, etc.

The purpose of this thesis is three-fold. First, we want to give a survey of results which have been obtained in the literature on properties of irreducible factors of random polynomials over finite fields. Secondly, we want to demonstrate the usefulness of analytic combinatorics to prove such results. Finally, we want to discuss some applications of these properties to polynomial factorization over finite fields. We will provide detailed proofs of all the results (some of the proofs have been only sketched in the literature).

We give a brief outline of the thesis. In Chapter 1, we will give a short outlook and summarize the results we are going to prove. In Chapter 2, we will recall some tools from analytic combinatorics with detailed proofs. In Chapter 3, we will use the results from Chapter 2 to prove our results on random polynomials. Finally, in Chapter 4, we will discuss applications of the results from Chapter 3.

中文摘要

數學領域經常研究有限體下隨機多項式質因式的性質（如整係數質因式的性質）。而這些性質常常應用在資訊工程、密碼學、編碼理論...等方面上。

這篇論文有三個研究動機：第一個動機是想整理參考文獻中有關有限體下隨機多項式質因式分解的性質。第二個動機是想展現如何用解析組合來證明這些質因式分解性質的結果。第三個動機是想將質因式分解性質的結果應用在質因式分解的演算法中。這些性質大多在文獻上只有粗淺的說明，而這篇論文將提供這些性質的詳細的證明及結果。

而這篇論文主要的概述：第一章，我們將給個簡短的概況並整理後面即將證明的結果。第二章，我們會給解析組合中常用的定理及詳細的證明。第三章，我們會用第二章中的結果來證明有限體下隨機多項式質因式的性質。最後，第四章，我們將討論第三章結果的應用。

誌謝辭

首先，我要感謝我的指導教授符麥克老師。在這段時間，不論在課業上或生活中，都從老師身上學到好多好多東西。

而接下來，感謝我的好同學、好夥伴們豐富了這兩年的生活。講到這裡，就開始懷念以前一起出去玩、一起吃飯、打球、串門子、玩桌遊的日子。都是因爲有你們，害我撐到現在...哈！開玩笑的啦～謝謝你們讓我能有動力撐到現在。而現在，遊學的遊學、工作的工作、實習的實習、當兵的當兵，約大家有空的時間好好聚聚似乎很不容易。相信這兩年這些甜美的回憶將會永遠保存在大家的心中！

最後，感謝受我身體髮膚（還有零用錢、生活費、電腦），同時也持續支持我的父母，讓我能很順利在求學的過程中學習，不必擔心生活方面的問題。很開心能完成碩士學位，這在我人生中是一個很重要的里程碑。希望大家之後能一起在各自的未來打拼！

Contents

Chapter 1

Introduction

Factorizing polynomials over the finite field $\mathbb{F}_q$, where q is a prime power, may make a lot of effort in many fields such as cryptography [7, 15, 17], coding theory [4], number theory [6] and polynomial factorization over the integers [8, 13, 14, 19]. Consequently, algorithms for factorizing polynomials have been studied by many authors, e.g., see Bach and Shoup [2], Berlekamp [3], and Rónyai[18].

In the analysis of these algorithms properties of random polynomials over a finite field have played an important role. The main purpose of this thesis is to survey these properties and to show how to use generating functions and analytic combinatorics to prove these results.

Generating functions are very helpful in this context, for instance take the problem of counting monic polynomials over a finite field $\mathbb{F}_q$ as an example. Let $P(z)$ denote the corresponding generating function, i.e., the n-th coefficient of $P(z)$ is the number of monic polynomials over $\mathbb{F}_q$ of degree n. Then, monic polynomials can be counted by the irreducible factors in their unique prime factorization. This yields

$$P(z) = \prod_{k\geq 1} \left(1 + z^k + z^{2k} + z^{3k} + \cdots\right)^{I_k} = \prod_{k\geq 1} \left(\frac{1}{1-z^k}\right)^{I_k},$$

where I_k is the number of monic irreducible polynomials of degree k. Of course, monic polynomials can also be counted directly which gives

$$P(z) = 1 + qz + q^2z^2 + q^3z^3 + \cdots = \frac{1}{1-qz}.$$

Now, this simple example lends itself to many generalizations. For instance, consider the question of counting monic polynomials excluding irreducible factors of degree k_1, k_2, k_3, ... , k_r in their prime factorization. Similar as above, we get

$$\prod_{\substack{k=1 \\ k \neq k_1, \cdots, k_r}}^{\infty} \left(1 + z^k + z^{2k} + z^{3k} + \cdots\right)^{I_k} = \frac{1}{1-qz} \cdot \prod_{j=1}^{r} \left(1 - z^{k_j}\right)^{I_{k_j}}.$$

Observe that the right hand side is a meromorphic function with a simple pole at $z = 1/q$. Moreover, for $z \to 1/q$,

$$\frac{1}{1-qz} \cdot \prod_{j=1}^{r} \left(1 - z^{k_j}\right)^{I_{k_j}} \sim \frac{1}{1-qz} \cdot \prod_{j=1}^{r} \left(1 - q^{-k_j}\right)^{I_{k_j}}.$$

Using a method called singularity analysis, which will be introduced in Section 2, the latter asymptotic relation remains true on the coefficient level. This yields that the number of monic polynomials excluding irreducible factors of degree k_1, k_2, k_3, ... , k_r in their prime factorization is asymptotically equal to

$$q^n \prod_{j=1}^{r} (1 - q^{-k_j})^{I_j}.$$

(Alternatively, this result can be obtained by the Inclusion-Exclusion principle.)

Sometimes, however, generating functions in one variable are not enough. For instance, suppose we want to count the number of monic polynomials with a fixed number of irreducible factors in their prime factorization. Then, we need bivariate generating functions. More precisely, consider a second variable u which counts the number of the irreducible factors in the prime factorization of a polynomial. Then, we have for the bivariate generating function.

$$P(z,u) = \prod_{k\geq 1}\left(1 + uz^k + u^2z^{2k} + u^3z^{3k} + \cdots\right)^{I_k} = \prod_{k\geq 1}\left(\frac{1}{1-uz^k}\right)^{I_k}.$$

By taking partial derivative with respect to u and letting $u = 1$, we obtain as coefficient of z^n the cumulative number of irreducible factors in the prime factorization of all polynomials of degree n. We will see later that again an asymptotic expansion can be easily derived by singularity analysis. From this, one obtains then the expected value of the number of irreducible factors in the prime factorization of a random polynomial. Moreover, by taking higher derivatives, higher moments can be derived as well.

We conclude by giving a sketch of the thesis. First, in Chapter 2, we will introduce singularity analysis and some other analytic methods we need for deriving our results, such as Darboux's method and the Hybrid method. Then, in Chapter 3, there will be four different topics. The first topic is mainly concerned with the number of irreducible factors of random polynomials. For instance, we will derive the probability of a polynomial of degree n being irreducible. The second topic will be about k-free polynomials. There are two cases in this section, the first case is when $k = 2$ and the second case will be the more general case. The third topic is discussing the degree of the irreducible factors of the polynomial, such as the maximal degree of the irreducible factors not greater than m, the maximal degree of the irreducible factors equals m and the maximal degree $D_n^{[1]}$ of the irreducible factors equals m_1 and the second largest degree $D_n^{[2]}$ of the irreducible factors equals m_2. The fourth topic is about the degree of the irreducible factors being distinct and related questions. Finally, in Chapter 4, we are going to apply the results from Chaper 3 to polynomial factorization.

The results, we are going to present in Section 3 are summarized in the following table. (X_n is the number of irreducible factors in a random polynomial of degree n and ρ denotes the Dickman function.)

Properties		Results
Section 3.1	$\text{Prob}(X_n = 1) = I_n/q^n$	$\frac{1}{n} + O(q^{-n/2})$
	$\mathbb{E}\left(X_n\right)$	$\log n + O(1)$
	$\text{Var}(X_n)$	$\log n + O(1)$
Section 3.2	Prob($x \in$ squarefree) (for $n = 0, 1$)	1
	Prob($x \in$ squarefree) (for $n \geq 2$)	$1 - 1/q$
	$\mathbb{E}$(degree of remaining part)	$\sum_{k \geq 1} \frac{kI_k}{q^{2k} - q^k}$
	Prob($x \in k$-free) (for $n = 0, 1$)	1
	Prob($x \in k$-free) (for $n \geq 2$)	$1 - 1/q^{k-1}$
	$\mathbb{E}$(degree of remaining part)	$\sum_{j \geq 1} \frac{jI_j}{q^{kj} - q^{(k-1)j}}$
Section 3.3	Prob(m-smooth)	$\rho\left(\frac{n}{m}\right) + O(\frac{\log n}{m})$
	$\text{Prob}(D_n^{[1]} = m)$	$\frac{1}{m}\rho\left(\frac{n}{m} - 1\right) + O\left(\frac{\log n}{m^2}\right)$
	$\text{Prob}(D_n^{[1]} = m, D_n^{[2]} \leq m/2)$	$\frac{1}{m}\rho\left(\frac{2n}{m} - 2\right) + O\left(\frac{\log n}{m^2}\right)$
	$\text{Prob}(D_n^{[1]} = m_1, D_n^{[2]} = m_2 < m_1)$	$\frac{1}{m_1 m_2}\rho\left(\frac{n}{m_2} - \frac{m_1}{m_2} - 1\right) + O\left(\frac{\log n}{m_1 m_2^2}\right)$
Section 3.4	$\text{Prob}(D_n^{[1]} > D_n^{[2]} > \cdots)$	$\prod_{k \geq 1}(1 + \frac{I_k}{q^k})(1 - \frac{1}{q^k})^{I_k}$
	$\text{Prob}(D_n^{[1]} > D_n^{[2]} > \cdots)$	$\prod_{k \geq 1}(1 + \frac{I_{2k}}{q^{2k}})(1 - \frac{1}{q^{2k}})^{I_{2k}}$

Chapter 2

Some Tools from Analytic Combinatorics

We first recall Landau's *O* notation.

Definition 2.1. *Let $f(n)$ and $g(n)$ be two complex-valued functions.*

1. *If there exist constants c, $n_0 \in \mathbb{N}$ such that*

$$|f(n)| \leq c \cdot |g(n)|, \quad \forall n \geq n_0,$$

then we say that $f(n)$ is a big-O *of $g(n)$, which is denoted by $f(n) = O(g(n))$.*

2. *If for all constants $\epsilon > 0$, there exists a $n_0 = n_0(\epsilon) \in \mathbb{N}$ such that*

$$|f(n)| \leq \epsilon \cdot |g(n)|, \quad \forall n \geq n_0,$$

then we say that $f(n)$ is a small-o *of $g(n)$, which is denoted by $f(n) = o(g(n))$.*

3. *If $f(n)/g(n) \to 1$ as $n \to \infty$, then we say that $f(n)$ is asymptotic to $g(n)$, which is denoted by $f(n) \sim g(n)$.*

As already mentioned in Chapter 1, in this thesis, generating functions will play an important role. We will frequently need their n-th coefficients. Therefore, we will recall the following standard notation from combinatorics.

Definition 2.2. *Given a generating function $f(z)$, $f_n = [z^n]f(z)$ denotes the coefficient of z^n in $f(z)$.*

2.1 Singularity Analysis

In this section, we treat generating functions as analytic functions. In the sequel, we will often encounter generating functions with a singularity at ζ and (local) behavior

$$f(z) = \left(1 - \frac{z}{\zeta}\right)^{-\alpha} \left(\log \frac{1}{1 - \frac{z}{\zeta}}\right)^{\beta},$$

where α and β are arbitrary complex numbers.

For convenience, we use a transformation to let the singularity $z = \zeta$ be on the unit circle $|z| = 1$. More precisely, note that by the scaling rule, we have

$$\begin{aligned} g(z) \equiv f(z\zeta) &= \left(1 - \frac{z\zeta}{\zeta}\right)^{-\alpha} \left(\log \frac{1}{1 - \frac{z\zeta}{\zeta}}\right)^{\beta} \\ &= (1 - z)^{-\alpha} \left(\log \frac{1}{1 - z}\right)^{\beta}. \end{aligned}$$

So, $g(z)$ has a singularity at $z = 1$, and in this way, we can get $f_n = [z^n]f(z)$ as follows,

$$f_n = [z^n]f(z) = \zeta^{-n}[z^n]f(z\zeta) = \zeta^{-n}[z^n]g(z) = \zeta^{-n}\, g_n,$$

where $g_n = [z^n]g(z)$. Since all generating functions can be brought in this form, we only need to discuss generating functions with a singularity at $z = 1$ and (local) behavior

$$(1 - z)^{-\alpha} \left(\log \frac{1}{1 - z}\right)^{\beta},$$

where α and β are arbitrary complex numbers.

First, we consider the special case $(1-z)^{-r}$, where $r \in \mathbb{Z}_{\geq 1}$. Then,

$$(1-z)^{-r} = \sum_{n=0}^{\infty} \binom{n+r-1}{n} z^n.$$

Consequently, the coefficients are given by

$$\begin{aligned}[z^n](1-z)^{-r} &= \binom{n+r-1}{n} = \frac{(n+r-1)(n+r-2)\cdots(n+1)}{(r-1)!} \\ &= \frac{n^{r-1}}{(r-1)!}\left(1 + O\left(\frac{1}{n}\right)\right).\end{aligned}$$

Now, for $(1-z)^{-\alpha}$, where $\alpha \in \mathbb{C}$, we expect a similar result:

$$[z^n](1-z)^{-\alpha} = \binom{n+\alpha-1}{\alpha-1} = cn^{\alpha-1}\left(1 + O\left(\frac{1}{n}\right)\right), \tag{2.1}$$

where c is a constant which will turn out to be related to the *Gamma function* $\Gamma(\alpha)$ which is defined as follows

$$\Gamma(\alpha) := \int_0^{\infty} e^{-t} t^{\alpha-1} dt$$

for $\Re(\alpha) > 0$. Moreover, we recall the following integral representation

$$\frac{1}{\Gamma(\alpha)} = \frac{1}{2\pi i} \oint_{\mathcal{C}} (-t)^{-\alpha} e^{-t} dt, \tag{2.2}$$

where the contour $\mathcal{C}$ comes from $\infty + i$, goes around 0 in counterclockwise direction, and then goes back to $\infty - i$ (see [12, p. 745]).

The formula (2.1) is made precise in the following theorem.

Theorem 2.3. *Given a function $f(z) = (1-z)^{-\alpha}$ with $\alpha \in \mathbb{C} \setminus \mathbb{Z}_{\leq 0}$, we have for the n-th coefficient*

$$f_n = [z^n]f(z) \sim \frac{n^{\alpha-1}}{\Gamma(\alpha)}\left(1 + \sum_{k \geq 1} \frac{e_k}{n^k}\right),$$

where e_k is a polynomial in α of degree $2k$.

Proof. We first prove the case where $k = 1$. By Cauchy's coefficient formula, we have

$$f_n = \frac{1}{2\pi i} \int_{\mathcal{C}} (1-z)^{-\alpha} \frac{dz}{z^{n+1}} \, ,$$

where we choose the contour $\mathcal{C}$ as follows:

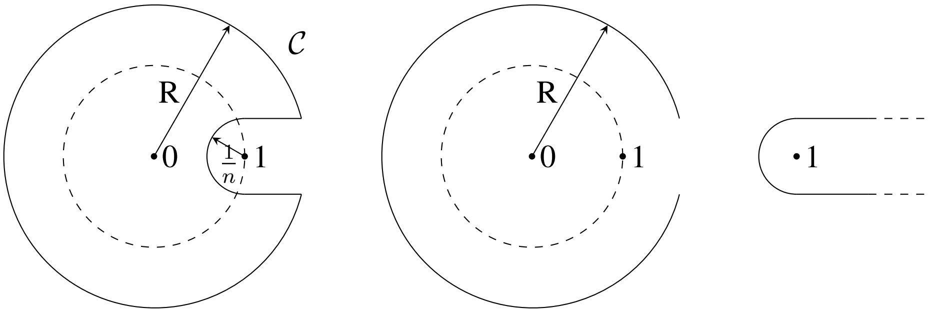


Figure 2.1: Our contour $\mathcal{C}$ is the curve on the left and we separate it into two parts, the center one and the right one.

Next, we break $\mathcal{C}$ into two parts $\widetilde{\mathcal{C}}$ and $\mathcal{H}$, where

$$\widetilde{\mathcal{C}} = \left\{ z \,\middle|\, z = Re^{i\theta},\ R > 1,\ \arcsin(1/nR) \le \theta \le 2\pi - \arcsin(1/nR) \right\} \text{ and}$$

$$\mathcal{H} = \left\{ z \,\middle|\, z = 1 + \frac{e^{i\theta}}{n},\ \pi/2 \le \theta \le 3\pi/2 \right\}$$
$$\cup \left\{ z \,\middle|\, 1 \le \Re(z) \le \sqrt{R^2 - \frac{1}{n^2}},\ \Im(z) = \pm\frac{1}{n} \right\}.$$

Then, we consider the integral over $\widetilde{\mathcal{C}}$ and $\mathcal{H}$ separately.

$\widetilde{\mathcal{C}}$: Since $|z| = R$, z^{-n} is bounded by R^{-n}. Thus, the integral over $\widetilde{\mathcal{C}}$ is exponentially small. More precisely,

$$\left| \frac{1}{2\pi i} \int_{\widetilde{\mathcal{C}}} (1-z)^{-\alpha} \frac{dz}{z^{n+1}} \right| \quad \le cR \cdot \frac{1}{R^{n+1}} \quad = O\left(\frac{1}{R^n}\right),$$

where $c = \sup_{|z|=R} |(1-z)^{-\alpha}|$.

$\mathcal{H}$: We are going to break $\mathcal{H}$ into 3 parts:

$$\begin{cases} \mathcal{H}^+(n) = \left\{ z \middle| z = \omega + \frac{i}{n},\, 1 \le \omega \le \sqrt{R^2 - \frac{1}{n^2}} \right\}; \\ \mathcal{H}^-(n) = \left\{ z \middle| z = \omega - \frac{i}{n},\, 1 \le \omega \le \sqrt{R^2 - \frac{1}{n^2}} \right\}; \\ \mathcal{H}^o(n) = \left\{ z \middle| z = 1 + \frac{e^{i\theta}}{n},\, \theta \in [\frac{\pi}{2}, \frac{3\pi}{2}] \right\}. \end{cases}$$

By the change of variable $z = 1 + \frac{t}{n}$, the integral over $\mathcal{H}$ becomes

$$\begin{aligned} \frac{1}{2\pi i} \int_{\mathcal{H}} (1-z)^{-\alpha} \frac{dz}{z^{n+1}} &= \frac{1}{2\pi i} \int_{\bar{\mathcal{H}}} \left(-\frac{t}{n} \right)^{-\alpha} \frac{1/n\, dt}{(1+t/n)^{n+1}} \\ &= \frac{n^{\alpha-1}}{2\pi i} \int_{\bar{\mathcal{H}}} (-t)^{-\alpha} \left(1 + \frac{t}{n} \right)^{-n-1} dt \end{aligned}$$

with $\bar{\mathcal{H}} = \bar{\mathcal{H}}^o \cup \bar{\mathcal{H}}^+ \cup \bar{\mathcal{H}}^-$, where

$$\begin{aligned} \bar{\mathcal{H}}^+ &= \left\{ t \middle| t = \omega + i,\, 0 \le \omega \le \sqrt{n^2R^2 - 1} - n \right\}; \\ \bar{\mathcal{H}}^- &= \left\{ t \middle| t = \omega - i,\, 0 \le \omega \le \sqrt{n^2R^2 - 1} - n \right\}; \\ \bar{\mathcal{H}}^o &= \left\{ t \middle| t = e^{i\theta},\, \theta \in [\frac{\pi}{2}, \frac{3\pi}{2}] \right\}. \end{aligned}$$

Let $t = \omega + i = \sqrt{\omega^2+1}\, e^{i\theta}$ where $\theta = \arg(t)$. The absolute value of $|(-t)^{-\alpha}|$ is

$$\begin{aligned} \left|(-t)^{-\alpha}\right| &= \left| \left(\sqrt{\omega^2+1}\, e^{i(\theta+\pi)} \right)^{-\Re(\alpha) - i\Im(\alpha)} \right| \\ &= \left| \sqrt{\omega^2+1}^{\,-\Re(\alpha)-i\Im(\alpha)} \right| \left| e^{-i(\theta+\pi)(\Re(\alpha)+i\Im(\alpha))} \right| \\ &= \sqrt{\omega^2+1}^{\,-\Re(\alpha)} e^{\Im(\alpha)\theta + \Im(\alpha)\pi}. \end{aligned} \tag{2.3}$$

We will break $\bar{\mathcal{H}}^+$ (and $\bar{\mathcal{H}}^-$) into two parts according to whether $\Re(t) \le \log^2 n$ or not. Then, the integral of the part with $\Re(t) > \log^2 n$ is at most

$$\left| \int_{\log^2 n + i}^{\infty + i} (-t)^{-\alpha} \left(1 + \frac{t}{n}\right)^{-n-1} dt \right| = \int_{\log^2 n}^{\infty} \left|(-\omega - i)^{-\alpha}\right| \left| 1 + \frac{\omega + i}{n} \right|^{-n-1} d\omega$$

$$
\begin{aligned}
&= O\left(\int_{\log^2 n}^{\infty} \sqrt{\omega^2+1}^{\,-\Re(\alpha)} \left|1+\frac{\omega}{n}\right|^{-n-1} d\omega\right) \\
&= O\left(\int_{\log^2 n}^{\infty} \sqrt{\omega^2+1}^{\,-\Re(\alpha)} e^{-\omega-\frac{\omega}{n}} \, d\omega\right) \quad = O\left(\int_{\log^2 n}^{\infty} \omega^{-\Re(\alpha)} e^{-\omega} \, d\omega\right).
\end{aligned}
$$

Now, if $\Re(\alpha) \geq 0$, it is easy to see that both $\omega^{-\Re(\alpha)}$ and $e^{-\omega}$ will make the integral exponentially small; on the other hand, if $\Re(\alpha) < 0$, by integration by parts

$$
\begin{aligned}
\int_{\log^2 n}^{\infty} \omega^{-\Re(\alpha)} e^{-\omega} \, d\omega &= -\omega^{-\Re(\alpha)} e^{-\omega}\Big|_{\log^2 n}^{\infty} - \Re(\alpha) \int_{\log^2 n}^{\infty} \omega^{-\Re(\alpha)-1} e^{-\omega} \, d\omega \\
&= \cdots = O\left((\log^2 n)^{-\Re(\alpha)} e^{-\log^2 n}\right) = O\left((\log n)^{-2\Re(\alpha)} n^{-\log n}\right), \quad (2.4)
\end{aligned}
$$

which is exponentially small, too. The same estimate holds for the corresponding part of $\bar{\mathcal{H}}^{-}$.

Next, for t with $\Re(t) \leq \log^2 n$, we use the following asymptotic expansion for $(1+\frac{t}{n})^{-n-1}$:

$$
\begin{aligned}
\left(1+\frac{t}{n}\right)^{-n-1} &= e^{-(n+1)\log(1+t/n)} \\
&= \exp\left(-(n+1)\left[-\frac{\left(-\frac{t}{n}\right)}{1} - \frac{\left(-\frac{t}{n}\right)^2}{2} - \frac{\left(-\frac{t}{n}\right)^3}{3} - \cdots\right]\right) \\
&= \exp\left(-t + \frac{t^2}{2n} - \frac{t^3}{3n^2} + \cdots\right) \exp\left(-\frac{t}{n} + \frac{t^2}{2n^2} - \frac{t^3}{3n^3} + \cdots\right) \\
&= e^{-t} \cdot \exp\left(\frac{t^2-2t}{2n} - \frac{2t^3-3t^2}{6n^2} + \frac{3t^4-4t^3}{12n^3} - \cdots\right) \\
&= e^{-t}\left[1 + \frac{t^2-2t}{2n} + \frac{t^4-4t^3+4t^2}{8n^2} - \frac{2t^3-3t^2}{6n^2} + \cdots\right] \\
&= e^{-t}\left[1 + \frac{t^2-2t}{2n} + \frac{3t^4-20t^3+24t^2}{24n^2} + \cdots\right]. \qquad (2.5)
\end{aligned}
$$

For $k=1$, we only need $(1+t/n)^{-n-1} = e^{-t}\left(1+O\left(\frac{\log^4 n}{n}\right)\right)$. After plugging this in, we can add the part with $\Re(t) > \log^2 n$ since this part is again exponentially small. Overall, we can let the contour become $\widetilde{\mathcal{H}} = \widetilde{\mathcal{H}}^o \cup \widetilde{\mathcal{H}}^+ \cup \widetilde{\mathcal{H}}^-$, where

$$\begin{aligned}
\widetilde{\mathcal{H}}^+ &= \left\{t \middle| t = \omega + i,\, \omega \geq 0\right\};\\
\widetilde{\mathcal{H}}^- &= \left\{t \middle| t = \omega - i,\, \omega \geq 0\right\};\\
\widetilde{\mathcal{H}}^o &= \left\{t \middle| t = e^{i\theta},\, \theta \in [\frac{\pi}{2}, \frac{3\pi}{2}]\right\}.
\end{aligned}$$

Then,

$$\int_{\widetilde{\mathcal{H}}} (-t)^{-\alpha} e^{-t} dt \left(1 + O\left(\frac{\log^4 n}{n}\right)\right) = \frac{1}{\Gamma(\alpha)}\left(1 + O\left(\frac{\log^4 n}{n}\right)\right),$$

where the last line follows from (2.2).

Finally, by putting every thing together, we obtain

$$f_n = \frac{n^{\alpha-1}}{\Gamma(\alpha)}\left(1 + O\left(\frac{\log^4 n}{n}\right)\right).$$

This concludes the proof of $k = 1$. For the general case, one only needs to use more terms in (2.5). This then gives

$$f_n \sim \frac{n^{\alpha-1}}{\Gamma(\alpha)}\left(1 + \sum_{k\geq 1}\frac{e_k}{n^k}\right). \quad ∎$$

Theorem 2.4. *Given a function* $f(z) = (1-z)^{-\alpha}\left(\frac{1}{z}\log\frac{1}{1-z}\right)^{\beta}$ *with* $\alpha \in \mathbb{C} \setminus \mathbb{Z}_{\leq 0}$, $\beta \in \mathbb{C}$, *we have for the* n*-th coefficient*

$$f_n = [z^n]f(z) \sim \frac{n^{\alpha-1}}{\Gamma(\alpha)}(\log n)^{\beta}\left(1 + \sum_{k\geq 1}\frac{d_k}{\log^k n}\right),$$

where d_k *is a polynomial in* α *of degree 2k.*

Proof. Again by Cauchy's coefficient formula,

$$f_n = \frac{1}{2\pi i}\int_{\mathcal{C}}(1-z)^{-\alpha}\left(\frac{1}{z}\log\frac{1}{1-z}\right)^{\beta}\frac{dz}{z^{n+1}},$$

where the contour $\mathcal{C} = \widetilde{\mathcal{C}} \cup \mathcal{H}$ is as in Theorem 2.3:

$$\widetilde{\mathcal{C}} = \left\{ z \,\middle|\, z = Re^{i\theta},\ R > 1,\ \arcsin(1/nR) \leq \theta \leq 2\pi - \arcsin(1/nR) \right\}, \quad \text{and}$$

$$\mathcal{H} = \left\{ z \,\middle|\, z = 1 + \frac{e^{i\theta}}{n},\ \pi/2 \leq \theta \leq 3\pi/2 \right\}$$
$$\cup \left\{ z \,\middle|\, 1 \leq \Re(z) \leq \sqrt{R^2 - \frac{1}{n^2}},\ \Im(z) = \pm\frac{1}{n} \right\}.$$

As in the proof of Theorem 2.3, we consider the integral over $\widetilde{\mathcal{C}}$ and $\mathcal{H}$ separately.

$\widetilde{\mathcal{C}}$: Since $|z| = R$, z^{-n} is bounded by R^{-n}. Thus, the integral over $\widetilde{\mathcal{C}}$ is exponentially small

$$\left| \frac{1}{2\pi i} \int_{\widetilde{\mathcal{C}}} (1-z)^{-\alpha} \left(\frac{1}{z} \log \frac{1}{1-z} \right)^{\beta} \frac{dz}{z^{n+1}} \right| \leq cR \cdot \frac{1}{R^{n+1}} = O\left(\frac{1}{R^n} \right),$$

where $c = \sup_{|z|=R} \left| (1-z)^{-\alpha} \left(\frac{1}{z} \log \frac{1}{1-z} \right)^{\beta} \right|$.

$\mathcal{H}$: We are going to break $\mathcal{H}$ into 3 parts:

$$\begin{cases} \mathcal{H}^{+}(n) = \left\{ z \middle| z = \omega + \frac{i}{n},\ 1 \leq \omega \leq \sqrt{R^2 - \frac{1}{n^2}} \right\}; \\ \mathcal{H}^{-}(n) = \left\{ z \middle| z = \omega - \frac{i}{n},\ 1 \leq \omega \leq \sqrt{R^2 - \frac{1}{n^2}} \right\}; \\ \mathcal{H}^{o}(n) = \left\{ z \middle| z = 1 + \frac{e^{i\theta}}{n},\ \theta \in [\frac{\pi}{2}, \frac{3\pi}{2}] \right\}. \end{cases}$$

By the change of variable $z = 1 + \frac{t}{n}$,

$$\begin{aligned} &\frac{1}{2\pi i} \int_{\mathcal{H}} (1-z)^{-\alpha} \left(\frac{1}{z} \log \frac{1}{1-z} \right)^{\beta} \frac{dz}{z^{n+1}} \qquad (2.6) \\ &= \frac{1}{2\pi i} \int_{\overline{\mathcal{H}}} \left(-\frac{t}{n} \right)^{-\alpha} \left(\frac{1}{1+t/n} \log \frac{1}{-t/n} \right)^{\beta} \frac{1/n\, dt}{(1+t/n)^{n+1}} \\ &= \frac{n^{\alpha-1}}{2\pi i} (\log n)^{\beta} \int_{\bar{\mathcal{H}}} (-t)^{-\alpha} \left(1 - \frac{\log(-t)}{\log n} \right)^{\beta} \left(1 + \frac{t}{n} \right)^{-n-1-\beta} dt \end{aligned}$$

with $\bar{\mathcal{H}} = \bar{\mathcal{H}}^o \cup \bar{\mathcal{H}}^+ \cup \bar{\mathcal{H}}^-$, where

$$\begin{aligned}
\bar{\mathcal{H}}^+ &= \left\{ t \middle| t = \omega + i,\, 0 \le \omega \le \sqrt{n^2R^2 - 1} - n \right\};\\
\bar{\mathcal{H}}^- &= \left\{ t \middle| t = \omega - i,\, 0 \le \omega \le \sqrt{n^2R^2 - 1} - n \right\};\\
\bar{\mathcal{H}}^o &= \left\{ t \middle| t = e^{i\theta},\, \theta \in [\frac{\pi}{2}, \frac{3\pi}{2}] \right\}.
\end{aligned}$$

By (2.3), we have $|(-t)^{-\alpha}| = \sqrt{\omega^2+1}^{\,-\Re(\alpha)} e^{\Im(\alpha)\theta}$. As before, we break $\bar{\mathcal{H}}^+$ (and $\bar{\mathcal{H}}^-$) into two parts according to whether $\Re(t) \le \log^2 n$ or not. The part with $\Re(t) > \log^2 n$ is at most

$$\begin{aligned}
&\left| \int_{\log^2 n + i}^{\infty + i} (-t)^{-\alpha} \left(1 - \frac{\log(-t)}{\log n}\right)^{\beta} \left(1 + \frac{t}{n}\right)^{-n-1-\beta} dt \right| \\
&= O\left(\int_{\log^2 n}^{\infty} |-\omega - i|^{-\Re(\alpha)} \left| 1 - \frac{\log(-\omega - i)}{\log n} \right|^{\Re(\beta)} \left| 1 + \frac{\omega + i}{n} \right|^{-n-1-\Re(\beta)} d\omega \right) \\
&= O\Bigg(\int_{\log^2 n}^{\infty} (\omega^2+1)^{-\frac{\Re(\alpha)}{2}} \left| 1 - \frac{\log(\sqrt{\omega^2+1}) + i\theta}{\log n} \right|^{\Re(\beta)} \\
&\qquad\qquad \cdot \left| 1 + \frac{\omega + i}{n} \right|^{-n-1-\Re(\beta)} d\omega \Bigg) \\
&= O\Bigg(\int_{\log^2 n}^{\infty} |\omega^2+1|^{-\frac{\Re(\alpha)}{2}} \left[\left(1 - \frac{\log(\sqrt{\omega^2+1})}{\log n} \right)^2 + \left(\frac{\theta}{\log n} \right)^2 \right]^{\frac{\Re(\beta)}{2}} \\
&\qquad\qquad \cdot \left| 1 + \frac{\omega + i}{n} \right|^{-n-1-\Re(\beta)} d\omega \Bigg) \\
&= O\left(\int_{\log^2 n}^{\infty} \omega^c \left| 1 + \frac{\omega}{n} \right|^{-n-1} d\omega \right),
\end{aligned}$$

where c is a suitable constant.

Since this integral is exponentially small, we only need to consider the part where $\Re(t) \le \log^2 n$.

For this part, we use the following asymptotic expansion for $\left(1+\frac{t}{n}\right)^{-n-1-\beta}$:

$$\begin{aligned}
\left(1+\frac{t}{n}\right)^{-n-1-\beta} &= e^{-(n+1+\beta)\log(1+t/n)}\\
&= \exp\left(-(n+1+\beta)\left[-\frac{\left(-\frac{t}{n}\right)}{1}-\frac{\left(-\frac{t}{n}\right)^2}{2}-\frac{\left(-\frac{t}{n}\right)^3}{3}-\cdots\right]\right)\\
&= \exp\left(-t+\frac{t^2}{2n}-\frac{t^3}{3n^2}+\cdots-\frac{t(1+\beta)}{n}+\frac{t^2(1+\beta)}{2n^2}-\frac{t^3(1+\beta)}{3n^3}+\cdots\right)\\
&= e^{-t}\left(1+O\left(\frac{\log^4 n}{n}\right)\right).
\end{aligned}$$

Moreover, we have (again for $\Re(t)\le\log^2 n$)

$$\left(1-\frac{\log(-t)}{n}\right)^{\beta}\sim\sum_{k\ge0}\binom{\beta}{k}(-1)^k\left(\frac{\log(-t)}{n}\right)^k.$$

Now, as in the proof of Theorem 2.3, plugging this in and adding the tail $\Re(t)>\log^2 n$ which is exponentially small, shows that the integral (2.6) is asymptotic to

$$\begin{aligned}
&\frac{n^{\alpha-1}}{2\pi i}(\log n)^{\beta}\int_{\widetilde{\mathcal{H}}}(-t)^{-\alpha}\left(\sum_{k\ge0}\binom{\beta}{k}\left(-\frac{\log(-t)}{\log n}\right)^k\right)e^{-t}dt\\
&=\sum_{k\ge0}\frac{n^{\alpha-1}}{2\pi i}(\log n)^{\beta-k}(-1)^k\binom{\beta}{k}\int_{\widetilde{\mathcal{H}}}(-t)^{-\alpha}\log^k(-t)e^{-t}dt\\
&=\sum_{k\ge0}\frac{n^{\alpha-1}}{2\pi i}(\log n)^{\beta-k}\binom{\beta}{k}\frac{d^k}{d\alpha^k}\left[\int_{\widetilde{\mathcal{H}}}(-t)^{-\alpha}e^{-t}dt\right]\\
&=\sum_{k\ge0}\frac{d^k}{d\alpha^k}\frac{n^{\alpha-1}}{\Gamma(\alpha)}(\log n)^{\beta-k}\binom{\beta}{k}
\end{aligned}$$

with $\widetilde{\mathcal{H}}=\widetilde{\mathcal{H}}^o\cup\widetilde{\mathcal{H}}^+\cup\widetilde{\mathcal{H}}^-$, where

$$\begin{aligned}
\widetilde{\mathcal{H}}^+ &= \left\{t\middle|t=\omega+i,\ \omega\ge0\right\};\\
\widetilde{\mathcal{H}}^- &= \left\{t\middle|t=\omega-i,\ \omega\ge0\right\};
\end{aligned}$$

$$\widetilde{\mathcal{H}}^o = \left\{ t \middle| t = e^{i\theta},\, \theta \in [\frac{\pi}{2}, \frac{3\pi}{2}] \right\}.$$

This proves the claimed result. ▮

Definition 2.5. *A domain is a Δ-domain at 1 if it can be written as*

$$\Delta(R, \phi) = \{z \mid \ |z| < R,\ z \neq 1,\ |\arg(z-1)| > \phi\},$$

where $R > 1$ and $0 < \phi < \pi/2$. Moreover, if a function is analytic in some Δ-domain, the function is called a Δ-analytic function.

Theorem 2.6. *Let $\alpha\,, \beta \in \mathbb{R}$ and $f(z)$ be a function that is analytic in $\Delta := \Delta\,(R, \phi)$. If*

$$f(z) = O\left((1-z)^{-\alpha} \left(\log \frac{1}{1-z} \right)^{\beta} \right),$$

where $z \in \Delta$ and approaching 1, then

$$f_n = [z^n]f(z) = O\left(n^{\alpha-1} (\log n)^{\beta} \right).$$

Similarly, if

$$f(z) = o\left((1-z)^{-\alpha} \left(\log \frac{1}{1-z} \right)^{\beta} \right),$$

where $z \in \Delta$-domain and approaching 1, then

$$f_n = [z^n]f(z) = o(n^{\alpha-1} (\log n)^{\beta}).$$

Proof. By Cauchy's coefficient formula, we have

$$f_n = \frac{1}{2\pi i} \int_C f(z) \frac{dz}{z^{n+1}},$$

and C is a closed contour in the unit disc. Since $f(z)$ is not analytic at $z = 1$, we change the contour C into a union of following 4 parts:

$$\begin{cases} \gamma_1 = \{z \,|\, |z-1| = \frac{1}{n},\ |\arg(z-1)| \geq \theta\} & \text{(inner circle)} \\ \gamma_2 = \{z \,|\, |z-1| \geq \frac{1}{n},\ |z| \leq r,\ \arg(z-1) = \theta\} & \text{(top line segment)} \\ \gamma_3 = \{z \,|\, |z| = r,\ |\arg(z-1)| \geq \theta\} & \text{(outer circle)} \\ \gamma_4 = \{z \,|\, |z-1| \geq \frac{1}{n},\ |z| \leq r,\ \arg(z-1) = -\theta\} & \text{(bottom line segment),} \end{cases}$$

where $1 < r < R$, and $\phi < \theta < \frac{\pi}{2}$, so that our contour C lies entirely inside our Δ-domain. We let $f_n^{[1]}$, $f_n^{[2]}$, $f_n^{[3]}$, $f_n^{[4]}$ be the integral along γ_1, γ_2, γ_3, γ_4, i.e.,

$$f_n^{[i]} = \frac{1}{2\pi i}\int_{\gamma_i} f(z)\frac{dz}{z^{n+1}}.$$

Then, we have

$$f_n = \frac{1}{2\pi i}\int_C f(z)\frac{dz}{z^{n+1}} = \frac{1}{2\pi i}\left[f_n^{[1]} + f_n^{[2]} + f_n^{[3]} + f_n^{[4]}\right].$$

So now, we will discuss the integrals separately.

1. Inner circle (γ_1):

   The line integral of $f_n^{[1]}$ will be at most the length of γ_1 times the maximum of $|f(z)|$,

   $$f_n^{[1]} \leq |\gamma_1| \cdot \max\left\{|f(z)|\,\middle|\,z \in \gamma_1\right\}.$$

   Since $f(z)$ is $O\left((1-z)^{-\alpha}\left(\log\frac{1}{1-z}\right)^{\beta}\right)$, there is a constant $c > 0$ such that $|f(z)| \leq c \cdot |1-z|^{-\alpha}\left|\log\frac{1}{1-z}\right|^{\beta}$. Hence, for the contour γ_1 where $|z-1| = 1/n$ and $|\arg(z-1)| \geq \theta$,

   $$\begin{aligned} \left|f_n^{[1]}\right| &\leq |\gamma_1| \cdot \max\left\{|f(z)|\,\middle|\,z \in \gamma_1\right\} \\ &\leq 2\pi\frac{1}{n} \cdot c\big|1-z\big|^{-\alpha}\left|\log 1 - z\right|^{\beta} \\ &= O\left(\frac{1}{n}\right) \cdot n^{\alpha}\left|\log|1-z| + i\phi\right|^{\beta} \\ &= O\left(\frac{1}{n}\right) \cdot n^{\alpha}\left(\log^2|1-z| + \phi^2\right)^{\beta/2} \\ &= O\left(n^{\alpha-1}\right) \cdot \left(\log^2 n + \phi^2\right)^{\beta/2}, \end{aligned}$$

where $\phi \in [0, 2\pi)$. Next, observe for large n

$$\begin{cases} \left(\log^2 n + \phi^2\right)^{\beta/2} \leq \left(\log^2 n + \log^2 n\right)^{\beta/2} = O\left(\log^\beta n\right), & \text{if } \beta \geq 0, \\ \left(\log^2 n + \phi^2\right)^{\beta/2} \leq \left(\log^2 n\right)^{\beta/2} = \log^\beta n = O\left(\log^\beta n\right), & \text{if } \beta < 0. \end{cases}$$

Consequently, $f_n^{[1]} = O\left(n^{\alpha-1}\log^\beta n\right)$.

2. Rectilinear parts (γ_2,γ_4):

   Again, there is a constant $c > 0$ such that $|f(z)| \leq c \cdot |1-z|^{-\alpha} \left|\log \frac{1}{1-z}\right|^\beta$. Then, by the change of variable $z = 1 + \frac{t}{n}e^{i\theta}$, our integral is

$$\begin{aligned}
\left|f_n^{[2]}\right| &= \left| \frac{1}{2\pi i} \int_{t=1}^{r'} f\left(1 + \frac{t}{n}e^{i\theta}\right) \frac{\frac{e^{i\theta}}{n}dt}{\left(1 + \frac{t}{n}e^{i\theta}\right)^{n+1}} \right| \\
&\leq \frac{c}{2\pi} \int_1^{r'} \left| \left(\frac{t}{n}\right)^{-\alpha} \left(\log \frac{1}{\frac{-t}{n}e^{i\theta}}\right)^\beta \right| \cdot \left|1 + \frac{t}{n}e^{i\theta}\right|^{-n-1} \left|\frac{e^{i\theta}}{n}\right| dt \\
&= \frac{c}{2\pi} n^{\alpha-1} \int_1^{r'} t^{-\alpha} \left|\log \frac{-te^{i\theta}}{n}\right|^\beta \cdot \left|1 + \frac{t}{n}e^{i\theta}\right|^{-n-1} dt \\
&= \frac{c}{2\pi} n^{\alpha-1} \int_1^{r'} t^{-\alpha} \left|\log(-t) + \log e^{i\theta} - \log n\right|^\beta \cdot \left|1 + \frac{t}{n}e^{i\theta}\right|^{-n-1} dt \\
&= \frac{c}{2\pi} n^{\alpha-1} \log^\beta n \int_1^{r'} t^{-\alpha} \left|1 - \frac{\log(-t) + i\theta}{\log n}\right|^\beta \cdot \left|1 + \frac{t}{n}e^{i\theta}\right|^{-n-1} dt \\
&= \frac{c}{2\pi} n^{\alpha-1} \log^\beta n \int_1^{r'} t^{-\alpha} \left|1 - \frac{\log t + i(\theta + \pi)}{\log n}\right|^\beta \cdot \left|1 + \frac{t}{n}e^{i\theta}\right|^{-n-1} dt \\
&= \frac{c}{2\pi} n^{\alpha-1} \log^\beta n \int_1^{r'} t^{-\alpha} \left[\left(1 - \frac{\log t}{\log n}\right)^2 + \left(\frac{\theta + \pi}{\log n}\right)^2\right]^{\beta/2} \\
&\qquad \cdot \left|1 + \frac{t}{n}e^{i\theta}\right|^{-n-1} dt,
\end{aligned}$$

   where r' is a constant satisfying $z = 1 + r'e^{i\theta}$ with $|z| = r$. But since as in the proof of Theorem 2.3, the integral over $t \in \left[\log^2 n, \infty\right]$ is exponentially small, so we can change the range to $1 \leq t \leq \log^2 n$. Then, obviously

$$\left[\left(1 - \frac{\log t}{\log n}\right)^2 + \left(\frac{\theta + \pi}{\log n}\right)^2\right]^{\beta/2} = O(1).$$

Consequently,

$$f_n^{[2]} = O\left(n^{\alpha-1}(\log n)^\beta \int_1^{\log^2 n} t^{-\alpha} \cdot \left|1 + \frac{t}{n}e^{i\theta}\right|^{-n-1} dt\right).$$

Since $\left|1 + \frac{t}{n}e^{i\theta}\right| \geq 1 + \Re\left(\frac{t}{n}e^{i\theta}\right) = 1 + \frac{t}{n}\cos\theta$, we have

$$\begin{aligned}
\int_1^{\log^2 n} t^{-\alpha}\left|1 + \frac{t}{n}e^{i\theta}\right|^{-n-1} dt \quad &\leq \int_1^\infty t^{-\alpha}\left(1 + \frac{t\cos\theta}{n}\right)^{-n-1} dt \\
&\leq \int_1^\infty t^{-\alpha}e^{-(n+1)\log\left(1+\frac{t\cos\theta}{n}\right)}dt \quad \leq \int_1^\infty t^{-\alpha}e^{-(n+1)\frac{t\cos\theta}{n}}dt \\
&\leq \int_1^\infty t^{-\alpha}e^{-t\cos\theta}dt,
\end{aligned}$$

where this integral is finite since $0 < \theta < \frac{\pi}{2}$.

This yields,

$$f_n^{[2]} = O\left(n^{\alpha-1}(\log n)^\beta\right).$$

3. Outer circle (γ_3):

   Since $|z| = r$, z^{-n} is bounded by r^{-n}. Thus, the integral $f_n^{[3]}$ is exponentially small.

Since $f_n^{[1]}, f_n^{[2]}, f_n^{[3]}, f_n^{[4]}$ are all $O\left(n^{\alpha-1}(\log n)^\beta\right)$, so that gives $f_n = O\left(n^{\alpha-1}(\log n)^\beta\right)$. The proof of the small-o part is similarly. ▮

Definition 2.7. *A log-power function at 1 is a finite sum of the form*

$$\sigma(z) = \sum_{k=1}^{r} c_k \left(\log\left(\frac{1}{1-z}\right)\right)(1-z)^{\alpha_k},$$

where $\alpha_1 < \cdots < \alpha_r$ and each $c_k(z)$ is a polynomial. A log-power function at a finite set of points $Z = \{\zeta_1, \cdots, \zeta_m\}$, is a finite sum

$$\Sigma(z) = \sum_{j=1}^{m} \sigma_j \left(\frac{z}{\zeta_j} \right),$$

where each σ_j is a log-power function at 1.

Theorem 2.8. *If a function $f(z)$ is analytic on a $\zeta \cdot \Delta$ domain and there exist log-power functions σ and τ such that*

$$f(z) = \sigma(z/\zeta) + O\left(\tau(z/\zeta)\right) \qquad \text{as } z \to \zeta \ \text{ in } \ \zeta \cdot \Delta,$$

then $f_n = [z^n]f(z)$ will be asymptotic to

$$f_n = \zeta^{-n}\sigma_n + O\left(\zeta^{-n}\,\tau_n\right),$$

where $\sigma_n = [z^n]\sigma(z)$ and $\tau_n = [z^n]\tau(z)$.

Proof. Let $g(z) = f(\zeta z)$. Then, $g(z)$ is Δ-analytic, with a singularity at 1 and $g(z) = \sigma(z) + O(\tau(z))$ as $z \to 1$. Now, since $\tau(z)$ is a log-power function, so

$$\begin{aligned} g_n = [z^n]g(z) &= [z^n]\sigma(z) + [z^n]O\left(\tau(z)\right) \\ &= [z^n]\sigma(z) + O\left([z^n]\tau(z)\right) \\ &= \sigma_n + O(\tau_n). \end{aligned}$$

Finally, since $f_n = \zeta^{-n}g_n$, we get

$$f_n = \zeta^{-n}g_n = \zeta^{-n}\left(\sigma_n + O(\tau_n)\right) = \zeta^{-n}\sigma_n + O\left(\zeta^{-n}\,\tau_n\right). \quad \blacksquare$$

According to the latter result, we know how to find f_n when $f(z)$ has one singularity at ζ. Similarly, f_n can be found if $f(z)$ has finitely many singularities (see [12, p. 398] for a proof).

Theorem 2.9. *Let $f(z)$ be analytic in $|z| < \rho$ with a finite number of singularities $\zeta_1, \cdots, \zeta_k$ on the circle $|z| = \rho$. Suppose there exists a Δ-domain such that $f(z)$ is analytic in the domain*

$$\mathbf{D} = \bigcap_{i=1}^{k} (\zeta_i \cdot \Delta) \ ,$$

Moreover, we have k log-power functions $\sigma_1, \cdots, \sigma_k$, and a log-power function $\tau(z) = (1-z)^{-\alpha} (\log \frac{1}{1-z})^{\beta}$ such that

$$f(z) = \sigma_i(z/\zeta_i) + O\left(\tau(z/\zeta_i)\right) \qquad as \ \ z \to \zeta_i \ \ in \ \ \mathbf{D}.$$

Then, the coefficients $f_n = [z^n]f(z)$ satisfies

$$f_n = \sum_{i=1}^{k} \zeta_i^{-n} \left(\sigma_i\right)_n + O\left(\rho^{-n} n^{\alpha-1} (\log n)^{\beta}\right) ,$$

where $(\sigma_i)_n = [z^n]\sigma_i$.

The last result is quite powerful and has many applications (for some of them see Chapter 3). However, it can be only applied if $f(z)$ is analytic in a domain which is larger than $|z| < \rho$. Sometimes, however, we only know that a function is analytic on $|z| < \rho$ and analytic extension is either hard to prove or not possible (some examples for this will be given in Section 3.4). Then, singularity analysis cannot be applied and we need other methods. We are going to introduce two such methods in the next section.

2.2 Darboux's and Hybrid Method

First, we introduce a method called Darboux's method. In contrast to singularity analysis, this method does not need that the function is analytically continuable beyond the disc of convergence. However, we will need some smoothness on the disc.

Definition 2.10. *Let $h(z)$ be a function which is analytic in $|z| < 1$ and $s \in \mathbb{N} \cup \{0\}$. If $h^{(k)}(z)$ is defined for $|z| < 1$ and has a continuous extension on $|z| \leq 1$ for all integers from 0 to s, then we call $h(z)$ $\mathcal{C}^s$-smooth on the unit disc.*

Remark 2.11. (Riemann-Lebesgue Lemma) If $f(z)$ is $\mathbf{L}^1$ integrable and supported on $(0, \infty)$, then

$$\int_0^\infty f(z)e^{-tz}dz \to 0,$$

as $|z| \to \infty$ within the half-plane $\Im(z) \geq 0$.

Theorem 2.12. *(Darboux's Method) Assume that $h(z)$ is $\mathcal{C}^s$-smooth. Then,*

$$h_n = [z^n]h(z) = o\left(\frac{1}{n^s}\right).$$

Proof. By Cauchy's coefficient formula, we have

$$h_n = \frac{1}{2\pi i}\int_{\mathcal{C}} h(z)\frac{dz}{z^{n+1}},$$

where $\mathcal{C}$ is the unit circle. Now, let $z = e^{i\theta}$, so that

$$h_n = \frac{1}{2\pi i}\int_0^{2\pi} h\left(e^{i\theta}\right)\frac{ie^{i\theta}d\theta}{\left(e^{i\theta}\right)^{n+1}} = \frac{1}{2\pi}\int_0^{2\pi} h\left(e^{i\theta}\right)e^{-ni\theta}d\theta.$$

When $s = 0$, we get $\int_0^{2\pi} h\left(e^{i\theta}\right)e^{-ni\theta}d\theta \to 0$ as $n \to \infty$ by the Riemann-Lebesgue Lemma. When $s > 0$, we use integration by parts s times and obtain

$$\begin{aligned}
h_n &= \frac{1}{2\pi}\int_0^{2\pi} h\left(e^{i\theta}\right)e^{-ni\theta}d\theta \\
&= \frac{1}{2\pi}\int_0^{2\pi} \frac{1}{ni}h'\left(e^{i\theta}\right)ie^{i\theta}e^{-ni\theta}d\theta \\
&= \frac{1}{2\pi}\frac{1}{n}\int_0^{2\pi} h'\left(e^{i\theta}\right)e^{-i(n-1)\theta}d\theta \\
&= \frac{1}{2\pi}\frac{1}{n(n-1)}\int_0^{2\pi} h''\left(e^{i\theta}\right)e^{-(n-2)i\theta}d\theta \\
&= \cdots = \frac{1}{2\pi}\frac{1}{n\cdots(n-s+1)}\int_0^{2\pi} h^{(s)}\left(e^{i\theta}\right)e^{-(n-s)i\theta}d\theta.
\end{aligned}$$

Then, again by the Riemann-Lebesgue Lemma,

$$\int_0^{2\pi} h^{(s)}\left(e^{i\theta}\right) e^{-(n-s)i\theta} d\theta \to 0.$$

Consequently, $h_n = o(n^{-s})$ as claimed. ∎

Definition 2.13. *A function $f(z)$ which is analytic in the open unit disc is said to be of global order $a \leq 0$ if there exists a constant c such that $|f(z)| \leq c\,(1-|z|)^a$ for all z satisfying $|z| < 1$. In other words, for all $|z| < 1$, we have*

$$f(z) = O\left((1-|z|)^a\right).$$

Theorem 2.14. *(Hybrid Method) Let $f(z)$ be a function that has a finite number of singularities $Z = \{\zeta_1, \ldots, \zeta_m\}$ with $|z| = 1$ and let $U(z)$, $V(z)$ be analytic functions on $|z| < 1$ satisfying $f = U \cdot V$. Assume that $V(z)$ is $\mathcal{C}^s$-smooth on the unit disc. Moreover, assume that $U(z)$ is of global order $a \leq 0$ and that there exists a log-power function $\widetilde{U}$ at Z such that $U = \widetilde{U} + R$ with R a $\mathcal{C}^t$-smooth function on the unit disc. Finally, suppose $t \geq \frac{s+a}{2} \geq 0$. Then, we have*

$$f_n = [z^n]f(z) = [z^n]\widetilde{U}(z) \cdot \overline{V}(z) + o(n^{-\frac{s+a}{2}}),$$

where $\overline{V}$ is a polynomial.

Proof. First, fix a constant $c \in \mathbb{N}$ with $c \leq s$. Next, let $V = \overline{V} + S$, where $\overline{V}$ is a polynomial of degree c that satisfies

$$\left.\frac{\partial^i}{\partial z^i}\overline{V}(z)\right|_{z=\zeta_j} = \left.\frac{\partial^i}{\partial z^i}V(z)\right|_{z=\zeta_j},$$

where $0 \leq i < c$ and $1 \leq j \leq m$. Then, since $U = \widetilde{U} + R$, we have

$$\begin{aligned} f = U \cdot V &= \left(\widetilde{U} + R\right) \cdot V = \widetilde{U} \cdot V + R \cdot V \\ &= \widetilde{U} \cdot \overline{V} + \widetilde{U} \cdot S + R \cdot V. \end{aligned}$$

Now, we are going to consider $\widetilde{U} \cdot \overline{V}$, $\widetilde{U} \cdot S$ and $R \cdot V$ separately.

$\widetilde{U} \cdot \overline{V}$:

Since $\widetilde{U}$ is a log-power function, and $\overline{V}$ is a polynomial, we can calculate the coefficient of $\widetilde{U} \cdot \overline{V}$ by singularity analysis.

$\widetilde{U} \cdot S$:

Since $S = V - \overline{V}$ and derivatives of order from 0 to $c-1$ are the same at ζ_i for V and $\overline{V}$, we have that derivatives of S of order from 0 to $c-1$ disappears at ζ_i. Consequently, we can factorize $S(z)$ into

$$S(z) = \kappa(z) \prod_{j=1}^{m} (z - \zeta_j)^c ,$$

where $\kappa(z)$ is a $\mathcal{C}^{s-c}$-smooth function. Then,

$$\widetilde{U} \cdot S = \left(\widetilde{U} \cdot \prod_{j=1}^{m} (z - \zeta_j)^c \right) \cdot \kappa(z).$$

Since U has a global order a, so $\widetilde{U}$ is $O\left((z - \zeta_j)^a\right)$ near ζ_j. Thus, $\widetilde{U} \cdot \prod_{j=1}^{m} (z - \zeta_j)^c$ is at least a $\mathcal{C}^{(a+c)}$-smooth. Since a $\mathcal{C}^{\alpha}$-smooth function times a $\mathcal{C}^{\beta}$-smooth function is at least a $\mathcal{C}^{\min(\alpha,\beta)}$-smooth function, so $\widetilde{U} \cdot S$ is a $\mathcal{C}^{\min\{a+c,s-c\}}$-smooth function. From this and Theorem 2.12, we get

$$[z^n]\, \widetilde{U} \cdot S = o\left(\frac{1}{n^u}\right),$$

where $u = \min\{a + c, s - c\}$.

$R \cdot V$:

Since R is $\mathcal{C}^t$-smooth and V is $\mathcal{C}^s$-smooth, $R \cdot V$ is $\mathcal{C}^{\min\{s,t\}}$-smooth. Set $v = \min\{s, t\}$. Then, again by Theorem 2.12,

$$[z^n]\, R \cdot V = o\left(\frac{1}{n^v}\right).$$

Summing up the three part yields

$$\begin{aligned} f_n &= [z^n]\,\widetilde{U}\cdot\overline{V} + [z^n]\,\widetilde{U}\cdot S + [z^n]\,R\cdot V \quad = [z^n]\,\widetilde{U}\cdot\overline{V} + o(n^{-u}) + o(n^{-v}) \\ &= [z^n]\,\widetilde{U}\cdot\overline{V} + o(n^{-\min\{v,u\}}) \quad = [z^n]\,\widetilde{U}\cdot\overline{V} + o(n^{-\min\{a+c,s-c,t\}}). \end{aligned}$$

We want the minimum to be as large as possible, so we choose $a + c = s - c$ which gives $c = \frac{s-a}{2}$. Then, we have

$$f_n = [z^n]\,\widetilde{P}\cdot\overline{Q} + o\left(n^{-\left(a+\frac{s-a}{2}\right)}\right) = [z^n]\,\widetilde{P}\cdot\overline{Q} + o\left(n^{-\frac{s+a}{2}}\right). \quad ∎$$

Note that $[z^n]\widetilde{U}\cdot\overline{V}$ can be obtained with singularity analysis (as already mentioned in the proof). Hence, the hybrid method combines Darboux's method with singularity analysis. We will use this method in Section 3.4.

2.3 Useful Functions

Here, we collect some useful functions. The first is the following one.

Definition 2.15. *The exponential integral $E(a)$ is defined as*

$$E\,(a) = \int_a^\infty \frac{e^{-s}}{s}\,ds,$$

where $0 \leq |\arg(a)| < \pi$, $a \neq 0$.

Remark 2.16. One important property of the exponential integral is that $e^{-E(z)}$ is bounded for all z with $\Re(z) \geq 0$ (see [1] for a proof).

Next, we use the exponential integral to find a representation of the remainder of the logarithmic series.

Lemma 2.17. *The remainders of the logarithm series*

$$r_m(z) = \sum_{k>m} \frac{z^k}{k},$$

where $|z| < 1$, *satisfies* $r_m\left(e^{-h}\right) = E\,(mh) + O\left(\frac{1}{m}\right)$ *for all* $h > 0$.

Proof. First note

$$r_m(z) = \int_0^z r_m'(t)\,dt = \int_0^z \sum_{k>m} t^{k-1} dt.$$

Then, by the plugging in $z = e^{-h}$ and using the change of variable $t = e^{-u}$, we have

$$\begin{aligned}
r_m\left(e^{-h}\right) &= \int_0^{e^{-h}} \sum_{k>m} t^{k-1} dt \quad = \int_\infty^h \left(\sum_{k>m} e^{-u(k-1)} \right) \left(-e^{-u}\right) du \\
&= \int_h^\infty \sum_{k>m} e^{-ku} du \quad = \int_h^\infty \frac{e^{-u(m+1)}}{1-e^{-u}} du \quad = \int_h^\infty \frac{e^{-mu}}{e^u - 1}\, du \\
&= \int_h^\infty \left[\frac{e^{-mu}}{u} + \frac{e^{-mu}}{e^u-1} - \frac{e^{-mu}}{u} \right] du \\
&= \int_h^\infty \left[m\frac{e^{-mu}}{mu} + e^{-mu}\left(\frac{1}{e^u-1} - \frac{1}{u} \right) \right] du \\
&= \int_{mh}^\infty \left[m\frac{e^{-s}}{s} + e^{-s}\left(\frac{1}{e^{s/m}-1} - \frac{1}{s/m} \right) \right] \frac{1}{m} ds \\
&= \int_{mh}^\infty \left[\frac{e^{-s}}{s} + \frac{e^{-s}}{m}\left(\frac{1}{e^{s/m}-1} - \frac{1}{s/m} \right) \right] ds \\
&= \int_{mh}^\infty \frac{e^{-s}}{s} ds + \frac{1}{m}\int_{mh}^\infty e^{-s}\left(\frac{1}{e^{s/m}-1} - \frac{1}{s/m} \right) ds \\
&= E\left(mh\right) + \frac{1}{m}\int_{mh}^\infty e^{-s}\phi\left(\frac{s}{m}\right) ds,
\end{aligned}$$

where $\phi(z) = \frac{1}{e^z-1} - \frac{1}{z}$. Now, if the function $\phi(z)$ is bounded, then $\frac{1}{m}\int_{mh}^\infty e^{-s}\phi\left(\frac{s}{m}\right) ds$ will be $O(1/m)$. In order to show that $\phi(z)$ is bounded, note that

$$\phi(z) \to 0 \quad \text{as } z \to \infty, \qquad \text{and} \qquad \phi(z) \to -1 \quad \text{as } z \to -\infty.$$

Moreover, when z is approaching 0, we have

$$\begin{aligned}
\lim_{z\to 0} \frac{1}{e^z-1} - \frac{1}{z} = \lim_{z\to 0} \frac{z - e^z + 1}{z\left(e^z - 1\right)} \quad &= \lim_{z\to 0} \frac{1-e^z}{\left(e^z-1\right) + ze^z} \\
= \lim_{z\to 0} \frac{-e^z}{e^z + \left(e^z + ze^z\right)} \quad &= \lim_{z\to 0} \frac{-e^z}{2e^z + ze^z} \\
= \lim_{z\to 0} \frac{-1}{2+z} \quad &= -\frac{1}{2}.
\end{aligned}$$

So, $\phi(z)$ is bounded and our claim is proved. ▮

In Section 3, we will need another function which is very similar to ϕ.

Lemma 2.18. *Let $\psi(z)$ be defined as*

$$\psi(z) = \frac{1}{1-e^{-z}} - \frac{1}{z}.$$

Then $\psi(z)$ is also bounded.

Proof. First, observe

$$\psi(z) \to 1 \quad \text{as } z \to \infty, \qquad\qquad \text{and} \qquad\qquad \psi(z) \to 0 \quad \text{as } z \to -\infty.$$

Next, when z is approaching 0, we have

$$\begin{aligned} \lim_{z\to 0} \frac{1}{1-e^{-z}} - \frac{1}{z} &= \lim_{z\to 0} \frac{z-1+e^{-z}}{z\left(1-e^{-z}\right)} = \lim_{z\to 0} \frac{1-e^{-z}}{\left(1-e^{-z}\right)+ze^{-z}} \\ &= \lim_{z\to 0} \frac{e^{-z}}{e^{-z}+\left(e^{-z}-ze^{-z}\right)} = \lim_{z\to 0} \frac{e^{-z}}{2e^{-z}-ze^{-z}} \\ &= \lim_{z\to 0} \frac{1}{2-z} = \frac{1}{2}. \end{aligned}$$

Thus, $\psi(z)$ is bounded. ▮

Another function which will be needed later is the Dickman function.

Definition 2.19. *The Dickman function $\rho\left(u\right)$ is the unique continuous solution of the difference-differential equation*

$$\begin{cases} \rho\left(u\right) = 1 & 0 \le u \le 1, \\ u\rho'\left(u\right) = -\rho\left(u-1\right) & u > 1. \end{cases}$$

Lemma 2.20. *The Laplace transform of the Dickman function $\widehat{\rho}\left(s\right)$ satisfies $s\widehat{\rho}\left(s\right) = e^{-E(s)}$. Consequently, we have*

$$\rho\left(u\right) = \frac{1}{2\pi i}\int_{1-i\infty}^{1+i\infty} \frac{e^{-E(v)}}{v} e^{uv}\, dv.$$

As a final class of functions, we will need polylogarithms (see [16] and [12, p. 408]).

Definition 2.21. *The polylogarithm $Li_m(z)$, with $m \in \mathbb{N}$, is defined as*

$$Li_m(z) = \sum_{n\geq 1} \frac{z^n}{n^m}.$$

Remark 2.22. Note that $Li_m(z)$ is $\mathcal{C}^{m-2}$-smooth.

Lemma 2.23. *$Li_m(z)$ is analytically continuable to $\mathbb{C} \setminus [1, \infty)$. Moreover, the singularity expansion at $z = 1$ is given by*

$$Li_m(z) = \frac{(-1)^m}{(m-1)!}\tau^{m-1}(\log \tau - H_{m-1}) + \sum_{j\geq 0,\, j\neq m-1} \frac{(-1)^j}{j!}\zeta(m-j)\tau^j,$$

where τ, the harmonic numbers H_m and the Riemann zeta function $\zeta(s)$ are defined as

$$\tau = -\log z = \sum_{l\geq 1} \frac{(1-z)^l}{l}, \quad H_m = \sum_{k=1}^{m} \frac{1}{k} \quad \textit{and} \quad \zeta(s) = \sum_{k\geq 1} \frac{1}{k^s}.$$

Chapter 3

Properties of Random Polynomials over Finite Fields

In this chapter, we will show the properties of random polynomials over finite fields from the introduction. We will do this in four sections. More precisely, in Section 3.1, we will discuss the number of irreducible factors of a polynomial, in Section 3.2, we will look at squarefree and k-free polynomials, in Section 3.3, we will discuss the maximal degree of the irreducible factors, and finally in Section 3.4, we will discuss the probability that a random polynomial has all irreducible factors of distinct degrees. Throughout the section all polynomials will be considered to be monic.

3.1 The Number of Irreducible Factors

Definition 3.1. *Let I_n be the number of irreducible polynomials of degree n and denote by $I(z)$ its generating function. Moreover, let X_n be the number of irreducible factors in a random polynomial of degree n (counted with multiplicities).*

Theorem 3.2. *The number of irreducible polynomials of degree n is*

$$I_n = \frac{q^n}{n} + O\left(q^{n/2}\right).$$

Proof. As already explained in the introduction, from the uniqueness of the prime factorization, we obtain

$$\begin{aligned} P(z) &= \prod_{k\geq 1}\left(\frac{1}{1-z^k}\right)^{I_k} = \exp\left(\sum_{k\geq 1} I_k \log\frac{1}{1-z^k}\right) = \exp\left(\sum_{k\geq 1}\sum_{j\geq 1} I_k \frac{z^{kj}}{j}\right) \\ &= \exp\left(I(z) + \frac{1}{2}I(z^2) + \frac{1}{3}I(z^3) + \cdots\right) = \frac{1}{1-qz}. \end{aligned}$$

Taking logarithms on both sides of the equality in the second line gives

$$\log\frac{1}{1-qz} = \sum_{k\geq 1}\frac{I(z^k)}{k}.$$

Next, the right hand side can be written as

$$\sum_{k\geq 1}\frac{I(z^k)}{k} = \sum_{k\geq 1}\sum_{l\geq 1}\frac{1}{k}I_l z^{kl} = \sum_{n\geq 1}\sum_{k|n}\frac{1}{k}I_{n/k}z^n.$$

Consequently, by Möbius inversion formula

$$I(z) = \log\frac{1}{1-qz} + \sum_{j\geq 2}\frac{\mu(j)}{j}\log\frac{1}{1-qz^j}.$$

Note that the second term is an analytic function on $|z| < q^{-1/2}$. Hence, applying singularity analysis gives

$$I_k = \frac{q^k}{k} + O(q^{k/2}). \quad \blacksquare$$

Example 3.3. The distribution of X_n.

1. The expected value $\mathbb{E}(X_n)$:

   We have $P(z) = (1-qz)^{-1}$. Now, let $P(z,u)$ be a bivariate generating function with the exponent of u counting the numbers of irreducible factors. Then,

$$P(z,u) = \prod_{k\geq 1} \frac{1}{(1-uz^k)^{I_k}}.$$

Next, differentiating with respect to u and letting $u=1$ yields

$$\begin{aligned}
\frac{\partial}{\partial u} P(z,u)\bigg|_{u=1} &= \prod_{k\geq 1} \frac{1}{(1-z^k)^{I_k}} \cdot \sum_{k\geq 1} \frac{I_k z^k}{1-z^k} \quad = P(z) \cdot \sum_{k\geq 1} \frac{I_k z^k}{1-z^k} \\
&= \frac{1}{1-qz} \cdot \sum_{k\geq 1} \frac{z^k}{1-z^k} \left(\frac{q^k}{k} + O\left(q^{k/2}\right) \right) \\
&= \frac{1}{1-qz} \cdot \left(\sum_{k\geq 1} \frac{q^k}{k} \frac{z^k}{1-z^k} + \sum_{k\geq 1} \frac{z^k}{1-z^k} O(q^{k/2}) \right) \\
&= \frac{1}{1-qz} \cdot \left(\sum_{k\geq 1} \frac{q^k}{k} \frac{z^k}{1-z^k} + \sum_{k\geq 1} O\left(\frac{q^{\frac{k}{2}} z^k}{1-z^k} \right) \right) \\
&= \frac{1}{1-qz} \cdot \left(\sum_{j\geq 1} \sum_{k\geq 1} \frac{q^k}{k} z^{jk} + \sum_{k\geq 1} O\left(\frac{q^{\frac{k}{2}} z^k}{1-z^k} \right) \right) \\
&= \frac{1}{1-qz} \cdot \left(\log \frac{1}{1-qz} + \sum_{j\geq 2} \log \frac{1}{1-qz^j} + \sum_{k\geq 1} O\left(\frac{q^{\frac{k}{2}} z^k}{1-z^k} \right) \right) \qquad (3.1) \\
&= \frac{1}{1-qz} \log \frac{1}{1-qz} + \frac{1}{1-qz} \cdot \left(\sum_{j\geq 2} \log \frac{1}{1-qz^j} + S(z) \right),
\end{aligned}$$

where $S(z) = \sum_{k\geq 1} O\left(\frac{q^{\frac{k}{2}} z^k}{1-z^k} \right)$. Note that the two terms in the bracket are analytic on $|z| < q^{-1/2}$. Hence, by singularity analysis, we have

$$\mathbb{E}(X_n) = \frac{1}{q^n} [z^n] \frac{\partial}{\partial u} P(z,u)\bigg|_{u=1} = \log n + \gamma + c + O(n^{-1}),$$

where γ is Euler's constant and $c = \sum_{j\geq 2} \log(1-q^{1-j})^{-1} + S(1/q)$.

2. The variance of X_n:

Again, we start from

$$P(z,u)=\prod_{k\geq 1}\frac{1}{(1-uz^k)^{I_k}}.$$

Now, we take the second derivative with respect to u and again set $u=1$ (the additional factor u after taking the first derivative is needed because we want to compute the second moment).

$$\begin{aligned}
\frac{\partial}{\partial u}\left(u\cdot\frac{\partial}{\partial u}P(z,u)\right)\Big|_{u=1} &= \frac{\partial}{\partial u}\left(u\cdot\prod_{k\geq 1}(1-uz^k)^{-I_k}\cdot\sum_{k\geq 1}\frac{I_kz^k}{1-uz^k}\right)\Big|_{u=1}\\
&=\prod_{k\geq 1}(1-uz^k)^{-I_k}\sum_{k\geq 1}\frac{I_kz^k}{1-uz^k}\Big|_{u=1}+u\prod_{k\geq 1}(1-uz^k)^{-I_k}\left(\sum_{k\geq 1}\frac{I_kz^k}{1-uz^k}\right)^2\Big|_{u=1}\\
&\qquad +u\cdot\prod_{k\geq 1}(1-uz^k)^{-I_k}\cdot\sum_{k\geq 1}\frac{I_kz^{2k}}{(1-uz^k)^2}\Big|_{u=1}\\
&=\prod_{k\geq 1}(1-z^k)^{-I_k}\cdot\left[\sum_{k\geq 1}\frac{I_kz^k}{1-z^k}+\left(\sum_{k\geq 1}\frac{I_kz^k}{1-z^k}\right)^2+\sum_{k\geq 1}\frac{I_kz^{2k}}{(1-z^k)^2}\right]\\
&=\frac{1}{1-qz}\cdot\left[\sum_{k\geq 1}\frac{I_kz^k}{1-z^k}+\left(\sum_{k\geq 1}\frac{I_kz^k}{1-z^k}\right)^2+\sum_{k\geq 1}\frac{I_kz^{2k}}{(1-z^k)^2}\right].
\end{aligned}$$

Note that the last term in the bracket is analytic on $|z|<q^{-1/2}$. As for the first two terms, we use what we already obtained in the analysis of the mean,

$$\sum_{k\geq 1}\frac{I_kz^k}{1-z^k}=\log\frac{1}{1-qz}+\sum_{j\geq 2}\log\frac{1}{1-qz^j}+S(z),$$

Plugging this in and applying singularity analysis gives

$$\begin{aligned}
\mathbb{E}(X_n^2)=&\frac{1}{q^n}[z^n]\frac{1}{1-qz}\cdot\left[\log\frac{1}{1-qz}+S(z)\right]+\frac{1}{q^n}[z^n]\frac{1}{1-qz}\cdot\log^2\frac{1}{1-qz}\\
&+\frac{1}{q^n}[z^n]\frac{1}{1-qz}\cdot 2\log\frac{1}{1-qz}\left[\sum_{j\geq 2}\log\frac{1}{1-qz^j}+S(z)\right]
\end{aligned}$$

$$
\begin{aligned}
&+\frac{1}{q^n}[z^n]\frac{1}{1-qz}\cdot\left(\sum_{j\geq 2}\log\frac{1}{1-qz^j}+S(z)\right)^2\\
&+\frac{1}{q^n}[z^n]\frac{1}{1-qz}\cdot\sum_{k\geq 1}\frac{I_k z^{2k}}{(1-z^k)^2}\\
=&\log n+O(1)+\log^2 n+2\gamma\log n+O(1)+2c\log n+O(1)\\
=&\log^2 n+(2\gamma+2c+1)\log n+O(1).
\end{aligned}
$$

Consequently, $\mathrm{Var}(X_n)=\mathbb{E}(X_n^2)-\mathbb{E}(X_n)^2$

$$
\begin{aligned}
&=\log^2 n+(2\gamma+2c+1)\log n+O(1)-\big(\log^2 n+2(\gamma+c)\log n+O(1)\big)\\
&=\log n+O(1).
\end{aligned}
$$

3. The probability of $X_n=1$, which is the same as the probability that a random polynomial of degree n is irreducible, is given by

$$
Prob\,(X_n=1)=\frac{1}{q^n}\cdot I_n=\frac{1}{q^n}\left(\frac{q^n}{n}+O\left(q^{n/2}\right)\right)=\frac{1}{n}+O\left(q^{-n/2}\right).
$$

4. The probability of $X_n=2$, which is the probability of a random polynomial of degree n to be a product of two irreducible factors, is obtained from the generating function

$$
\begin{aligned}
I^{[2]}(z)=\frac{I(z)\cdot I(z)}{2!}+\frac{I(z^2)}{2}=&\frac{1}{2}\left(\log\frac{1}{1-qz}+\sum_{j\geq 2}\frac{\mu(j)}{j}\log\frac{1}{1-qz^j}\right)^2\\
&+\frac{1}{2}\left(\log\frac{1}{1-qz^2}+\sum_{j\geq 2}\frac{\mu(j)}{j}\log\frac{1}{1-qz^{2j}}\right).
\end{aligned}
$$

Since the latter term is analytic on $|z|<q^{-1/2}$, singularity analysis yields

$$
Prob\,(X_n=2)=\frac{1}{q^n}\cdot[z^n]I^{[2]}(z)=\frac{\log n}{n}+O\left(\frac{1}{n}\right).
$$

3.2 Squarefree Polynomials and K-free Polynomials

Definition 3.4. *A polynomial is called squarefree if each of its irreducible factors appears only once.*

Remark 3.5. If a polynomial $f\,(x)$ is not squarefree, we can sort the irreducible factors of the polynomial into a squarefree part $g\,(x)$ and a remaining part $h\,(x)$. The squarefree part $g\,(x)$ gathers all of the irreducible factors only once, and the remaining part $h\,(x)$ takes the rest.

Remark 3.6. The remaining part $h = f/g$ is not necessarily not squarefree, e.g., if $f(x) = (x+1)^2(x+2)(x^2+x+1)^3$, then $g(x) = (x+1)(x+2)(x^2+x+1)$ and consequently $h(x) = (x+1)(x^2+x+1)^2$.

Example 3.7. Here, we want to find the probability of a random polynomial being squarefree and the expected value of the degree of the remaining part.

1. The probability of a random polynomial being squarefree:

   The generating functions of squarefree polynomials (denoted by $Q(z)$) and all polynomials are

$$\begin{aligned} Q(z) &= \prod_{k=1}^{\infty}(1+z^k)^{I_k}, \\ P(z) &= \prod_{k=1}^{\infty}(1-z^k)^{-I_k} = \frac{1}{1-qz}. \end{aligned}$$

   Now, a relation between squarefree polynomials and all polynomials is as follows: every polynomial can be factorized into a square part and a remaining part, which is squarefree, e.g.,

$$\begin{aligned} f(x) &= x(x+1)(x+3)^7(x^2+1)^2(x^2+5)^6 \\ &= (x+3)^6(x^2+1)^2(x^2+5)^6 \cdot x(x+1)(x+3) \end{aligned}$$

$$= \underbrace{\left[(x+3)^3(x^2+1)^1(x^2+5)^3\right]^2}_{\text{square part}} \cdot \underbrace{x(x+1)(x+3)}_{\text{remaining part}}.$$

This yields,

$$\begin{aligned} P(z) &= P(z^2)\cdot Q(z). \\ Q(z) &= \frac{P(z)}{P(z^2)} = \frac{1-q(z^2)}{1-qz} = (1-qz^2)\cdot(1+qz+q^2z^2+q^3z^3+\cdots) \\ &= \sum_{k\geq 0} q^k z^k - \sum_{k\geq 2} q^{k-1}z^k. \end{aligned}$$

Hence, the coefficient Q_n of z^n in $Q(z)$ is easily obtained as

$$Q_n = \begin{cases} q^n, & \text{if } n = 0, 1; \\ q^n - q^{n-1}, & \text{if } n \geq 2. \end{cases}$$

So, the probability of a random polynomial with degree n being squarefree is

$$\begin{cases} 1, & \text{when } n = 0, 1; \\ 1 - \frac{1}{q}, & \text{when } n \geq 2. \end{cases}$$

2. The expected value of the degree of the remaining part:

   We again use a bivariate generating function $P(z,u)$, where the second variable counts the degree of the remaining part. Consequently,

$$P(z,u) = \prod_{k\geq 1}\left(1+z^k+u^kz^{2k}+u^{2k}z^{3k}+\cdots\right)^{I_k} = \prod_{k\geq 1}\left(1+\frac{z^k}{1-u^kz^k}\right)^{I_k}.$$

   Now, differentiating with respect to u and setting $u=1$ yields

$$
\begin{aligned}
&\frac{\partial}{\partial u} P(z,u)\bigg|_{u=1} \\
&= \prod_{k\geq 1}\left(1+\frac{z^k}{1-z^k}\right)^{I_k} \cdot \sum_{k\geq 1} \frac{I_k\left(1+\frac{z^k}{1-z^k}\right)^{I_k-1}\left(-z^k\right)\left(1-z^k\right)^{-2}\left(-kz^k\right)}{\left(1+\frac{z^k}{1-z^k}\right)^{I_k}} \\
&= \prod_{k\geq 1}\left(\frac{1}{1-z^k}\right)^{I_k} \cdot \sum_{k\geq 1} kI_k \frac{z^{2k}\left(1-z^k\right)^{-2}}{\left(1-z^k\right)^{-1}} \\
&= P(z)\cdot \sum_{k\geq 1} kI_k \cdot \frac{z^{2k}}{1-z^k} = \frac{1}{1-qz}\cdot \sum_{k\geq 1} kI_k \cdot \frac{z^{2k}}{1-z^k}.
\end{aligned}
$$

Note that the second term is analytic on $|z| < q^{-1/2}$. Consequently, by singularity analysis

$$
[z^n]\frac{\partial}{\partial u} P(z,u)\bigg|_{u=1} \sim q^n \sum_{k\geq 1} kI_k \frac{q^{-2k}}{1-q^{-k}} = q^n \sum_{k\geq 1} \frac{kI_k}{q^{2k}-q^k}.
$$

Hence, the expected value of the degree of the remaining part is asymptotically equal to

$$
\sum_{k\geq 1} \frac{kI_k}{q^{2k}-q^k}.
$$

A natural extension of squarefree polynomials are k-free polynomials. We will consider them next.

Definition 3.8. *A polynomial is called k-free if the multiplicity of each irreducible factor is less than k.*

Remark 3.9. If a polynomial $f(x)$ is not k-free, we can sort the irreducible factors of the polynomial into a k-free part $g(x)$ and a remaining part $h(x)$. The k-free part $g(x)$ gathers all of the irreducible factors at most $k-1$ times and the remaining part $h(x)$ takes the rest.

Example 3.10. Let us find the probability of a random polynomial being k-free and the expected value of the degree of the remaining part. The analysis is similar to the one from Example 3.7.

1. The probability of a random polynomial being k-free:

   The generating function of k-free polynomials $Q^{[k]}(z)$ is

   $$Q^{[k]}(z) = \prod_{j\geq 1} \left(1 + z^j + z^{2j} + z^{3j} + \cdots + z^{(k-1)j}\right)^{I_k}.$$

   Then, we again can find a relation between $Q^{[k]}(z)$ and $P(z)$. More precisely, since every polynomial can be composed into a k-free polynomial times a polynomial of power k, so

   $$\begin{aligned} P(z) &= Q^{[k]}(z) \cdot P(z^k). \\ Q^{[k]}(z) &= \frac{P(z)}{P(z^k)} = \frac{1 - qz^k}{1 - qz} = (1 - qz^k) \cdot (1 + qz + q^2z^2 + q^3z^3 + \cdots) \\ &= \sum_{j\geq 0} q^j z^j - \sum_{j\geq 0} q^{j+1} z^{k+j}. \end{aligned}$$

   Since a polynomial with degree $n < k$ must be k-free, so the probability of a polynomial of degree $n < k$ being k-free is 1. Next, we consider on polynomial of degree $n \geq k$. From the above, we get for the number of k-free polynomials (denoted by $Q_n^{[k]}$):

   $$Q_n^{[k]} = q^n - q^{n-k+1}.$$

   So, the probability that a random polynomial of degree $n \geq k$ is k-free is $1 - \frac{1}{q^{k-1}}$.

2. The expected value of the degree of the remaining part:

   Similar as in Example 3.7, we find the bivariate generating function with u counting the degree of the remaining part.

Then,

$$\begin{aligned}P(z,u) &= \prod_{j\geq 1}\left(1+z^j+z^{2j}+\cdots+z^{(k-1)j}+u^j z^{kj}+u^{2j}z^{(k+1)j}+\cdots\right)^{I_j}\\ &= \prod_{j\geq 1}\left(\frac{1-z^{(k-1)j}}{1-z^j}+\frac{z^{(k-1)j}}{1-u^j z^j}\right)^{I_j}.\end{aligned}$$

Next, we differentiate with respect to u and let $u=1$. This yields

$$\begin{aligned}&\frac{\partial}{\partial u}P(z,u)\bigg|_{u=1}\\ &= \prod_{j\geq 1}\left(\frac{1}{1-z^j}\right)^{I_j}\cdot\sum_{j\geq 1}\frac{I_j\left(\frac{1}{1-z^j}\right)^{I_j-1}\left(-z^{(k-1)j}\right)\left(1-z^j\right)^{-2}\left(-jz^j\right)}{\left(\frac{1}{1-z^j}\right)^{I_j}}\\ &= \prod_{j\geq 1}\left(\frac{1}{1-z^j}\right)^{I_j}\cdot\sum_{j\geq 1}\left(\frac{jI_j z^{kj}\left(1-z^j\right)^{-2}}{\left(1-z^j\right)^{-1}}\right)\\ &= P(z)\cdot\sum_{j\geq 1}\left(jI_j\cdot\frac{z^{kj}}{1-z^j}\right)=\frac{1}{1-qz}\cdot\sum_{j\geq 1}\left(jI_j\cdot\frac{z^{kj}}{1-z^j}\right).\end{aligned}$$

Applying singularity analysis yields

$$[z^n]\frac{\partial}{\partial u}P(z,u)\Big|_{u=1}\sim q^n\sum_{j\geq 1}jI_j\frac{q^{-kj}}{1-q^{-j}}=q^n\sum_{j\geq 1}\frac{jI_j}{q^{kj}-q^{(k-1)j}}.$$

Hence, the expected value of the remaining part is asymptotic to

$$\sum_{j\geq 1}\frac{jI_j}{q^{kj}-q^{(k-1)j}}.$$

3.3 The Degree of the Irreducible Factors

Definition 3.11. *A polynomial is called m-smooth polynomial if there is no irreducible factor whose degree is greater than m.*

Example 3.12. First, we discuss the number of m-smooth polynomial of degree n. Therefore, let $S_m(z)$ be the generating function of m-smooth polynomials. Then, for $|z| < 1$

$$\begin{aligned} S_m(z) = \prod_{k=1}^{m} \left(1 - z^k\right)^{-I_k} \quad &= P(z) \cdot \prod_{k>m} \left(1 - z^k\right)^{I_k} \\ &= \frac{1}{1-qz} \cdot \exp\left(\sum_{k>m} I_k \log\left(1 - z^k\right)\right) \\ &= \frac{1}{1-qz} \cdot \exp\left(\sum_{k>m} I_k \cdot \left(-z^k - \frac{z^{2k}}{2} - \frac{z^{3k}}{3} - \cdots\right)\right) \\ &= \frac{1}{1-qz} \cdot \exp\left(-\sum_{k>m}\sum_{j\geq 1} I_k \cdot \frac{z^{kj}}{j}\right) \\ &= \frac{1}{1-qz} \cdot \exp\left(-\sum_{j\geq 1}\frac{1}{j}\sum_{k>m} I_k z^{kj}\right) \\ &= \frac{1}{1-qz} \cdot \exp\left(-\sum_{j\geq 1}\frac{r_m^{[j]}(z)}{j}\right), \end{aligned}$$

where $r_m^{[j]}(z) = \sum_{k>m} I_k z^{kj}$. Next, we need suitable estimates for $r_m^{[j]}$. First, we estimate $r_m^{[1]}(z)$ for $|z| < 1$:

$$r_m^{[1]}\left(\frac{z}{q}\right) = \sum_{k>m} I_k \left(\frac{z}{q}\right)^k = \sum_{k>m} \frac{z^k}{k} + O\left(q^{-m/2}\right).$$

Moreover, for $r_m^{[j]}(z)$ with $j \geq 2$, we have

$$r_m^{[j]}\left(\frac{z}{q}\right) = \sum_{k>m} O\left(q^k \frac{z^{kj}}{q^{kj}}\right) = \sum_{k>m} O\left(\frac{z^{kj}}{q^{k(j-1)}}\right) = O\left(\frac{1}{q^{m(j-1)}}\right),$$

for $|z| < 1$. Overall, we have found that the sum of the error terms of $r_m^{[j]}(z)$ with $j \geq 2$ are bounded by the error term of $r_m^{[1]}(z)$ which is $O\left(q^{-m/2}\right)$.

So, the number of m-smooth polynomial of degree n (denoted by $N_q(n,m)$) is

$$
\begin{aligned}
N_q(n,m) &= \frac{1}{2\pi i}\int_{\mathcal{C}} S_m(z)\frac{dz}{z^{n+1}} = \frac{q^n}{2\pi i}\int_{\widetilde{\mathcal{C}}} S_m\left(\frac{z}{q}\right)\frac{dz}{z^{n+1}} \\
&= \frac{q^n}{2\pi i}\int_{\widetilde{\mathcal{C}}} \frac{1}{1-q(z/q)}\cdot\exp\left(-r_m^{[1]}\left(\frac{z}{q}\right) - \frac{r_m^{[2]}(z/q)}{2} - \frac{r_m^{[3]}(z/q)}{3} - \cdots\right)\frac{dz}{z^{n+1}} \\
&= \frac{q^n}{2\pi i}\int_{\widetilde{\mathcal{C}}} \frac{1}{1-z}\cdot\exp\left(-\sum_{k>m}\frac{z^k}{k} + O\left(q^{-m/2}\right)\right)\frac{dz}{z^{n+1}} \\
&= \frac{q^n}{2\pi i}\int_{\widetilde{\mathcal{C}}} \frac{1}{1-z}\cdot\exp\left(-r_m(z) + O\left(q^{-m/2}\right)\right)\frac{dz}{z^{n+1}},
\end{aligned}
$$

where the contour $\widetilde{\mathcal{C}}$ is $z = e^{i\theta - 1/n}$ with $-\pi \leq \theta \leq \pi$. Next, we use the change of variable $z = e^{-h/n}$. Note that, by Lemma 2.17, we have

$$
r_m(z) = r_m\left(e^{-h/n}\right) = E\left(\mu h\right) + O\left(1/m\right),
$$

where $\mu = m/n$. Moreover, note that since $O\left(q^{-m/2}\right)$ is exponentially small, so it will be eliminated by $O\left(1/m\right)$ in $r_m(z)$. Consequently,

$$
\begin{aligned}
N_q\left(n,m\right) &= \frac{q^n}{2\pi i}\int_{\widetilde{\mathcal{C}}} \frac{1}{1-z}\cdot\exp\left(-r_m(z) + O\left(q^{-m/2}\right)\right)\frac{dz}{z^{n+1}} \\
&= \frac{q^n}{2\pi i}\int_{1+in\pi}^{1-in\pi} \frac{1}{1-e^{-h/n}}\cdot\exp\left(-r_m\left(e^{-h/n}\right) + O\left(q^{-m/2}\right)\right)\frac{-\frac{1}{n}e^{-h/n}dh}{e^{-h(1+1/n)}} \\
&= \frac{q^n}{2\pi i}\int_{1-in\pi}^{1+in\pi} \frac{\exp\left(-E\left(\mu h\right) + O\left(1/m\right)\right)}{n\left(1-e^{-h/n}\right)}e^h dh \\
&= \frac{q^n}{2\pi i}\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h)}\frac{e^{O(1/m)}}{n\left(1-e^{-h/n}\right)}e^h dh. \qquad (3.2)
\end{aligned}
$$

Now, set $\psi(z) = \frac{1}{1-e^{-z}} - \frac{1}{z}$ which is analytic in $|z| < 2\pi$. We can rewrite parts of the integrand of (3.2) into an expression of ψ.

$$
\frac{1}{n\left(1-e^{-h/n}\right)} = \frac{1}{n}\left(\frac{1}{h/n} + \psi\left(\frac{h}{n}\right)\right) = \frac{1}{h} + \frac{1}{n}\psi\left(\frac{h}{n}\right)
$$

$$\begin{aligned}\frac{e^{O(1/m)}}{n\left(1-e^{-h/n}\right)} &= \left(\frac{1}{h}+\frac{1}{n}\psi\left(\frac{h}{n}\right)\right)\cdot\left(1+O\left(\frac{1}{m}\right)\right)\\ &= \frac{1}{h}+\frac{1}{n}\psi\left(\frac{h}{n}\right)+O\left(\frac{1}{hm}\right).\end{aligned} \tag{3.3}$$

Next, substitute (3.3) into (3.2) and separate the integral into three parts

$$\begin{aligned}N_q(n,m) &= \frac{q^n}{2\pi i}\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h)}\frac{e^{O(1/m)}}{n\left(1-e^{-h/n}\right)}e^h dh\\ &= \frac{q^n}{2\pi i}\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h)}\left(\frac{1}{h}+\frac{1}{n}\psi\left(\frac{h}{n}\right)+O\left(\frac{1}{hm}\right)\right)e^h dh\\ &= \frac{q^n}{2\pi i}\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h)}\frac{1}{n}\psi\left(\frac{h}{n}\right)e^h dh+\frac{q^n}{2\pi i}\int_{1-in\pi}^{1+in\pi}\frac{e^{-E(\mu h)}}{h}e^h dh\\ &\quad+\frac{q^n}{2\pi i}\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h)}O\left(\frac{1}{hm}\right)e^h dh\,.\end{aligned}$$

Now, we will discuss the 3 integrals separately:

1. The main term:

$$\begin{aligned}&\frac{1}{2\pi i}\int_{1-in\pi}^{1+in\pi}\frac{e^{-E(\mu h)}}{h}e^h dh\\ &\quad=\frac{1}{2\pi i}\int_{1-i\infty}^{1+i\infty}\frac{e^{-E(\mu h)}}{h}e^h dh-\frac{1}{2\pi i}\int_{\mathcal{L}}\frac{e^{-E(\mu h)}}{h}e^h dh,\end{aligned}$$

where $\mathcal{L}$ is the union of the two semi-vertical lines $(1+in\pi, 1+i\infty)$ and $(1-i\infty, 1-in\pi)$. Then, by partial integration, we obtain for the $\mathcal{L}$ part the bound $O\left(\frac{1}{n}\right)$. Since the proofs of the positive and negative semi-vertical line are the same, we only consider the positive part.

$$\begin{aligned}&\int_{1+in\pi}^{1+i\infty}\frac{e^{-E(\mu h)}}{h}e^h dh\\ &\quad=\frac{e^{-E(\mu h)}}{h}e^h\Bigg|_{1+in\pi}^{1+i\infty}-\int_{1+in\pi}^{1+i\infty}\left(\frac{e^{-E(\mu h)}}{h}\frac{e^{-\mu h}}{h}-\frac{e^{-E(\mu h)}}{h^2}\right)e^h dh\\ &\quad=\frac{e^{-E(\mu h)}}{h}e^h\Bigg|_{1+in\pi}^{1+i\infty}+\int_{1+in\pi}^{1+i\infty}\frac{e^{-E(\mu h)}}{h^2}\left(1-e^{-\mu h}\right)e^h dh.\end{aligned}$$

In order to go on, note that since $e^{-E(z)}$ is bounded for $\Re(z) > 0$, there exists a constant $c > 0$ such that $|e^{-E(z)}| \le c$. So the absolute value of the first term is

$$\begin{aligned}\left|\frac{e^{-E(\mu h)}}{h}e^{h}\Big|_{1+in\pi}^{1+i\infty}\right| &\le c\left(\lim_{x\to\infty}\frac{|e^{1+ix}|}{|1+ix|}+\frac{|e^{1+in\pi}|}{|1+in\pi|}\right)\\ &= ce\left(\lim_{x\to\infty}\frac{1}{\sqrt{x^2+1}}+\frac{1}{\sqrt{n^2\pi^2+1}}\right) \quad = O\left(\frac{1}{n}\right).\end{aligned}$$

Moreover, the absolute value of the second term is bounded by

$$\begin{aligned}&\left|\int_{1+in\pi}^{1+i\infty}\frac{e^{-E(\mu h)}}{h^2}\left(1-e^{-\mu h}\right)e^{h}dh\right|\\ &\le \int_{n\pi}^{\infty}\left|\frac{e^{-E(\mu+i\mu x)}}{(1+ix)^2}\left(1-e^{-\mu-i\mu x}\right)e^{1+ix}\right|dx \le ce\int_{n\pi}^{\infty}\left|\frac{1-e^{-\mu-i\mu x}}{(1+ix)^2}\right|dx\\ &\le ce\int_{n\pi}^{\infty}\frac{1}{|1+ix|^2}dx+ce\int_{n\pi}^{\infty}\frac{|e^{-\mu-i\mu x}|}{|1+ix|^2}dx\\ &= ce\int_{n\pi}^{\infty}\frac{1}{1+x^2}dx+ce^{1-\mu}\int_{n\pi}^{\infty}\frac{1}{1+x^2}dx\\ &= \left(ce+ce^{1-\mu}\right)\int_{n\pi}^{\infty}\frac{1}{1+x^2}dx\\ &\le \left(ce+ce^{1-\mu}\right)\int_{n\pi}^{\infty}\frac{1}{x^2}dx=\frac{ce+ce^{1-\mu}}{n\pi}=O\left(\frac{1}{n}\right).\end{aligned}$$

So, the main term becomes

$$\begin{aligned}&\frac{1}{2\pi i}\int_{1-i\infty}^{1+i\infty}\frac{e^{-E(\mu h)}}{h}e^{h}dh+O\left(\frac{1}{n}\right)\\ &\qquad=\frac{1}{2\pi i}\int_{1-i\infty}^{1+i\infty}\frac{e^{-E(\mu h)}}{\mu h}(e^{\mu h})^{\frac{1}{\mu}}\mu dh+O\left(\frac{1}{n}\right)\\ &\qquad=\frac{1}{2\pi i}\int_{1-i\infty}^{1+i\infty}\frac{e^{-E(\mu h)}}{\mu h}(e^{\mu h})^{\frac{1}{\mu}}d(\mu h)+O\left(\frac{1}{n}\right).\end{aligned}$$

Then, by Lemma 2.20, $\rho\left(u\right)=\frac{1}{2\pi i}\int_{1-i\infty}^{1+i\infty}\frac{e^{-E(v)}}{v}e^{uv}dv$. So, our main term is

$$\begin{aligned}&\frac{1}{2\pi i}\int_{1-i\infty}^{1+i\infty}\frac{e^{-E(\mu h)}}{\mu h}\left(e^{\mu h}\right)^{\frac{1}{\mu}}d\left(\mu h\right)+O\left(\frac{1}{n}\right)\\ &\qquad=\rho\left(\frac{1}{\mu}\right)+O\left(\frac{1}{n}\right)=\rho\left(\frac{n}{m}\right)+O\left(\frac{1}{n}\right).\end{aligned}$$

2. The part containing $\frac{1}{n}\psi\left(\frac{h}{n}\right)$:

Integration by part gives

$$\frac{1}{2\pi i}\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h)}\,\frac{1}{n}\psi\left(\frac{h}{n}\right)e^{h}dh=\frac{1}{2n\pi i}\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h)}\,\psi\left(\frac{h}{n}\right)e^{h}dh$$

$$=\frac{1}{2n\pi i}\left(e^{-E(\mu h)}\,\psi\left(\frac{h}{n}\right)e^{h}\Big|_{1-in\pi}^{1+in\pi}-\int_{1-in\pi}^{1+in\pi}\left(e^{-E(\mu h)}\,\psi\left(\frac{h}{n}\right)\right)'e^{h}dh\right)$$

$$=\frac{1}{2n\pi i}\left(e^{-E(\mu h)}\,\psi\left(\frac{h}{n}\right)e^{h}\Big|_{1-in\pi}^{1+in\pi}\right.$$
$$\left.-\int_{1-in\pi}^{1+in\pi}\left(\frac{e^{-\mu h}}{h}e^{-E(\mu h)}\,\psi\left(\frac{h}{n}\right)+e^{-E(\mu h)}\,\frac{1}{n}\psi'\left(\frac{h}{n}\right)\right)e^{h}dh\right)$$

$$=\frac{1}{2n\pi i}\left(e^{-E(\mu h)}\,\psi\left(\frac{h}{n}\right)e^{h}\Big|_{1-in\pi}^{1+in\pi}\right.$$
$$\left.-\int_{1-in\pi}^{1+in\pi}e^{-E(\mu h)}\left(\frac{e^{-\mu h}}{h}\psi\left(\frac{h}{n}\right)+\frac{1}{n}\psi'\left(\frac{h}{n}\right)\right)e^{h}dh\right).$$

We will bound this expression in three steps. In every step we will use that $e^{-E(z)}$ and $\psi(z)$ are bounded:

(a) $\left|\frac{1}{2n\pi i}e^{-E(\mu h)}\psi\left(\frac{h}{n}\right)e^{h}\Big|_{1-in\pi}^{1+in\pi}\right|$:

Here, we have

$$\frac{1}{2n\pi}\left|e^{-E(\mu h)}\psi\left(\frac{h}{n}\right)e^{h}\Big|_{1-in\pi}^{1+in\pi}\right|=\frac{1}{2n\pi}\left|e^{-E(\mu(1+in\pi))}\psi\left(\frac{1+in\pi}{n}\right)e^{1+in\pi}\right.$$
$$\left.-\,e^{-E(\mu(1-in\pi))}\psi\left(\frac{1-in\pi}{n}\right)e^{1-in\pi}\right|$$
$$\leq\frac{1}{2n\pi}\left(\left|e^{-E(\mu(1+in\pi))}\psi\left(\frac{1+in\pi}{n}\right)e^{1+in\pi}\right|\right.$$
$$\left.+\left|e^{-E(\mu(1-in\pi))}\psi\left(\frac{1-in\pi}{n}\right)e^{1-in\pi}\right|\right)$$
$$\leq\frac{c}{2n\pi}\left(\left|e^{1+in\pi}\right|+\left|e^{1-in\pi}\right|\right)=\frac{ce}{2n\pi}\left(\left|e^{in\pi}\right|+\left|e^{-in\pi}\right|\right)=O\left(\frac{1}{n}\right).$$

So, $\left|\frac{1}{2n\pi i}e^{-E(\mu h)}\psi\left(\frac{h}{n}\right)e^{h}\Big|_{1-in\pi}^{1+in\pi}\right| = O\left(\frac{1}{n}\right)$.

(b) $\left|\frac{1}{2n\pi i}\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h)}\psi\left(\frac{h}{n}\right)\frac{e^{(1-\mu)h}}{h}dh\right|$:

Here, we have

$$\begin{aligned}
&\frac{1}{2n\pi}\left|\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h)}\psi\left(\frac{h}{n}\right)\frac{e^{(1-\mu)h}}{h}dh\right| \\
&\quad\le \frac{1}{2n\pi}\int_{-n\pi}^{n\pi}\left|e^{-E(\mu+i\mu x)}\psi\left(\frac{1+ix}{n}\right)\frac{e^{(1-\mu)(1+ix)}}{1+ix}\right|dx \\
&\quad\le \frac{c}{2n\pi}\int_{-n\pi}^{n\pi}\left|\frac{e^{(1-\mu)(1+ix)}}{1+ix}\right|dx \;=\frac{ce^{1-\mu}}{2n\pi}\int_{-n\pi}^{n\pi}\frac{1}{\sqrt{1+x^2}}dx \\
&\quad= \frac{ce^{1-\mu}}{2n\pi}\int_{0}^{n\pi}\frac{2}{\sqrt{1+x^2}}dx \\
&\quad= \frac{ce^{1-\mu}}{n\pi}\left(\int_0^1\frac{1}{\sqrt{1+x^2}}dx+\int_1^{n\pi}\frac{1}{\sqrt{1+x^2}}dx\right) \\
&\quad= \frac{ce^{1-\mu}}{n\pi}\left(\log(x+\sqrt{1+x^2})\Big|_0^1+\int_1^{n\pi}\frac{1}{\sqrt{1+x^2}}dx\right) \\
&\quad= \frac{ce^{1-\mu}}{n\pi}\left(\log(1+\sqrt{2})+\int_1^{n\pi}\frac{1}{\sqrt{1+x^2}}dx\right) \quad = O\left(\frac{\log n}{n}\right).
\end{aligned}$$

Thus, $\left|\frac{1}{2n\pi i}\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h)}\psi\left(\frac{h}{n}\right)\frac{e^{(1-\mu)h}}{h}dh\right| = O\left(\frac{\log n}{n}\right)$.

(c) $\left|\frac{1}{2n^2\pi i}\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h)}\psi'\left(\frac{h}{n}\right)e^{h}dh\right|$:

Note that $\psi'(z)$ is also bounded. Hence,

$$\begin{aligned}
&\frac{1}{2n^2\pi}\left|\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h)}\psi'\left(\frac{h}{n}\right)e^{h}dh\right| \\
&\quad\le \frac{1}{2n^2\pi}\int_{-n\pi}^{n\pi}\left|e^{-E(\mu+i\mu x)}\psi'\left(\frac{1+ix}{n}\right)e^{1+ix}\right|dx \\
&\quad\le \frac{c}{2n^2\pi}\int_{-n\pi}^{n\pi}\left|e^{1+ix}\right|dx = \frac{ce}{2n^2\pi}\int_{-n\pi}^{n\pi}\left|e^{ix}\right|dx = O\left(\frac{1}{n}\right).
\end{aligned}$$

This gives $\left|\frac{1}{2n^2\pi i}\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h)}\psi'\left(\frac{h}{n}\right)e^{h}dh\right| = O\left(\frac{1}{n}\right)$.

Overall, we obtain $\frac{1}{2\pi i}\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h)}\frac{1}{n}\psi\left(\frac{h}{n}\right)e^{h}dh = O\left(\frac{\log n}{n}\right)$.

3. The part containing $O\left(\frac{1}{hm}\right)$:

   Since $e^{-E(\mu h)}$ is bounded, we easily get the error term:

$$\left|\frac{1}{2\pi i}\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h)}O\left(\frac{1}{hm}\right)e^{h}dh\right| \leq c\int_{-n\pi}^{n\pi}\left|O\left(\frac{1}{(1+ix)m}\right)e^{1+ix}\right|dx$$
$$= ce\int_{-n\pi}^{n\pi} O\left(\frac{1}{\sqrt{1+x^2}m}\right)dx = O\left(\frac{\log n}{m}\right).$$

Hence, by combining the above estimates, we have

$$N_q\left(n,m\right) = q^n\cdot\left(\rho\left(\frac{n}{m}\right)+O\left(\frac{\log n}{m}\right)\right).$$

Next, we are going to discuss the degree of the largest irreducible factor of a random polynomial of degree n (which we denote by $D_n^{[1]}$).

Example 3.13. Here, we consider the probability that a random polynomial has the degree of the largest irreducible factor $D_n^{[1]} = m$.

As before, we first find the generating function $L_m(z)$ of polynomials with the degree of the largest irreducible factor $= m$. By the previous example, we have the generating function $S_m(z)$ of m-smooth polynomials. Then, $L_m(z)$ is given by

$$\begin{aligned} L_m(z) &= S_m(z) - S_{m-1}(z) = S_m(z)\left(1-(1-z^m)^{I_m}\right) \\ &= S_m(z)\cdot\left(\sum_{k\geq 1}\binom{I_m}{k}(-1)^{k+1}z^{km}\right) \\ &= S_m(z)\cdot\left(I_m z^m + \sum_{k\geq 2}\binom{I_m}{k}(-1)^{k+1}z^{km}\right). \end{aligned}$$

Thus,

$$\begin{aligned} Pr\left(D_n^{[1]} = m\right) &= \frac{1}{q^n}[z^n]L_m(z) = [z^n]L_m\left(\frac{z}{q}\right) = \frac{1}{2\pi i}\int_{\mathcal{C}} L_m\left(\frac{z}{q}\right)\frac{dz}{z^{n+1}} \\ &= \frac{1}{2\pi i}\int_{\mathcal{C}} S_m\left(\frac{z}{q}\right)\left(I_m\frac{z^m}{q^m} + \sum_{k\geq 2}\binom{I_m}{k}(-1)^{k+1}\left(\frac{z}{q}\right)^{km}\right)\frac{dz}{z^{n+1}}. \end{aligned}$$

Since $I_m = q^m/m + O\left(q^{m/2}\right) = O(q^m/m)$, the probability becomes

$$\begin{aligned} Pr\left(D_n^{[1]} = m\right) &= \frac{1}{2\pi i}\int_{\mathcal{C}} S_m\left(\frac{z}{q}\right)\left(I_m\frac{z^m}{q^m} + O\left(\frac{1}{m^2}\right)\right)\frac{dz}{z^{n+1}} \\ &= \frac{1}{2\pi i}\int_{\mathcal{C}} S_m\left(\frac{z}{q}\right)\left(\frac{z^m}{m} + O\left(q^{-m/2}\right) + O\left(\frac{1}{m^2}\right)\right)\frac{dz}{z^{n+1}} \\ &= \frac{1}{2\pi i}\int_{\mathcal{C}} S_m\left(\frac{z}{q}\right)\frac{z^m}{m}\frac{dz}{z^{n+1}}\left(1 + O\left(\frac{1}{m}\right)\right), \end{aligned}$$

where the contour $\mathcal{C}$ is $z = e^{-1/n+i\theta}$ with $-\pi \le \theta \le \pi$. By the change of variable $z = e^{-h/n}$, we have

$$\begin{aligned} Pr\left(D_n^{[1]} = m\right) &= \frac{1}{2\pi i}\int_{\mathcal{C}} S_m\left(\frac{z}{q}\right)\frac{z^m}{m}\frac{dz}{z^{n+1}}\left(1 + O\left(\frac{1}{m}\right)\right) \\ &= \frac{1}{2\pi i}\int_{1+in\pi}^{1-in\pi} S_m\left(\frac{e^{-h/n}}{q}\right)\frac{e^{-\mu h}}{m}\frac{-\frac{1}{n}e^{-h/n}dh}{e^{-h-h/n}}\left(1 + O\left(\frac{1}{m}\right)\right) \\ &= \frac{1}{2\pi i}\int_{1-in\pi}^{1+in\pi} S_m\left(\frac{e^{-h/n}}{q}\right)\frac{e^{(1-\mu)h}}{nm}dh\left(1 + O\left(\frac{1}{m}\right)\right), \end{aligned}$$

where $\mu = m/n$. Now, as in Example 3.12,

$$\begin{aligned} Pr\left(D_n^{[1]} = m\right) &= \frac{1}{2m\pi i}\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h)}\frac{e^{O(1/m)}}{n\left(1 - e^{-h/n}\right)}e^{(1-\mu)h}dh\left(1 + O\left(\frac{1}{m}\right)\right) \\ &= \frac{1}{2m\pi i}\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h)}\left[\frac{1}{h} + \frac{1}{n}\psi\left(\frac{h}{n}\right) + O\left(\frac{1}{hm}\right)\right]e^{(1-\mu)h}dh. \end{aligned}$$

As before, we break the integral into three parts and discuss the three parts separately:

1. The main term:

   By Example 3.12, we know that the contour of the first part $[1 - in\pi, 1 + in\pi]$ can be replaced by $(1 - i\infty, 1 + i\infty)$. Then, by Lemma 2.20,

$$\begin{aligned} \frac{1}{2m\pi i}\int_{1-i\infty}^{1+i\infty} e^{-E(\mu h)}\frac{1}{h}e^{(1-\mu)h}dh &= \frac{1}{2m\pi i}\int_{1-i\infty}^{1+i\infty} e^{-E(\mu h)}\frac{1}{\mu h}e^{\mu h\left(\frac{1}{\mu}-1\right)}d\left(\mu h\right) \\ &= \frac{1}{m}\rho\left(\frac{1}{\mu} - 1\right). \end{aligned}$$

2. The term containing $\frac{1}{n}\psi\left(\frac{h}{n}\right)$:

   This term is similar as in Example 3.12. Integration by part gives

$$\begin{aligned}
&\frac{1}{2m\pi i}\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h)}\,\frac{1}{n}\psi\left(\frac{h}{n}\right)e^{(1-\mu)h}dh \\
&\quad= \frac{1}{2nm\pi i}\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h)}\,\psi\left(\frac{h}{n}\right)e^{(1-\mu)h}dh \\
&\quad= \frac{1}{2nm\left(1-\mu\right)\pi i}\left(e^{-E(\mu h)}\,\psi\left(\frac{h}{n}\right)e^{(1-\mu)h}\Big|_{1-in\pi}^{1+in\pi}\right. \\
&\qquad\qquad \left.-\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h)}\left(\frac{e^{-\mu h}}{h}\,\psi\left(\frac{h}{n}\right)+\frac{1}{n}\psi'\left(\frac{h}{n}\right)\right)e^{(1-\mu)h}dh\right).
\end{aligned}$$

   (a) $\left|\frac{1}{2nm\pi i}e^{-E(\mu h)}\psi\left(\frac{h}{n}\right)e^{(1-\mu)h}\Big|_{1-in\pi}^{1+in\pi}\right|$:

   Since $e^{-E(z)}$ and $\psi(z)$ are bounded, we have

$$\begin{aligned}
&\frac{1}{2nm\pi}\left|e^{-E(\mu h)}\psi\left(\frac{h}{n}\right)e^{(1-\mu)h}\Big|_{1-in\pi}^{1+in\pi}\right| \\
&\quad= \frac{1}{2nm\pi}\left|e^{-E(\mu(1+in\pi))}\psi\left(\frac{1+in\pi}{n}\right)e^{(1-\mu)(1+in\pi)}\right. \\
&\qquad\qquad \left.-\,e^{-E(\mu(1-in\pi))}\psi\left(\frac{1-in\pi}{n}\right)e^{(1-\mu)(1-in\pi)}\right| \\
&\quad\le \frac{1}{2nm\pi}\left(\left|e^{-E(\mu(1+in\pi))}\psi\left(\frac{1+in\pi}{n}\right)e^{(1-\mu)(1+in\pi)}\right|\right. \\
&\qquad\qquad \left.+\left|e^{-E(\mu(1-in\pi))}\psi\left(\frac{1-in\pi}{n}\right)e^{(1-\mu)(1-in\pi)}\right|\right) \\
&\quad\le \frac{c}{2nm\pi}\left(\left|e^{(1-\mu)(1+in\pi)}\right|+\left|e^{(1-\mu)(1-in\pi)}\right|\right)=\frac{ce^{1-\mu}}{nm\pi}=O\left(\frac{1}{nm}\right).
\end{aligned}$$

   So, $\left|\frac{1}{2nm\pi i}e^{-E(\mu h)}\psi\left(\frac{h}{n}\right)e^{(1-\mu)h}\Big|_{1-in\pi}^{1+in\pi}\right|=O\left(\frac{1}{nm}\right)$.

   (b) $\left|\frac{1}{2nm\pi i}\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h)}\psi\left(\frac{h}{n}\right)\frac{e^{(1-2\mu)h}}{h}dh\right|$:

   Since $e^{-E(z)}$ and $\psi(z)$ are bounded, we have

$$\begin{aligned}
&\frac{1}{2nm\pi}\left|\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h)}\psi\left(\frac{h}{n}\right)\frac{e^{(1-2\mu)h}}{h}dh\right| \\
&\quad\leq \frac{1}{2nm\pi}\int_{-n\pi}^{n\pi}\left|e^{-E(\mu+i\mu x)}\psi\left(\frac{1+ix}{n}\right)\frac{e^{(1-2\mu)(1+ix)}}{1+ix}\right|dx \\
&\quad\leq \frac{c}{2nm\pi}\int_{-n\pi}^{n\pi}\left|\frac{e^{(1-2\mu)(1+ix)}}{1+ix}\right|dx = \frac{ce^{1-2\mu}}{2nm\pi}\int_{-n\pi}^{n\pi}\frac{1}{\sqrt{1+x^2}}dx \\
&\quad= \frac{ce^{1-2\mu}}{2nm\pi}\int_{0}^{n\pi}\frac{2}{\sqrt{1+x^2}}dx \\
&\quad= \frac{ce^{1-2\mu}}{nm\pi}\left(\int_0^1\frac{1}{\sqrt{1+x^2}}dx+\int_1^{n\pi}\frac{1}{\sqrt{1+x^2}}dx\right) \\
&\quad= \frac{ce^{1-2\mu}}{nm\pi}\left(\log(x+\sqrt{1+x^2})\Big|_0^1+\int_1^{n\pi}\frac{1}{\sqrt{1+x^2}}dx\right) \\
&\quad= \frac{ce^{1-2\mu}}{nm\pi}\left(\log(1+\sqrt{2})+\int_1^{n\pi}\frac{1}{\sqrt{1+x^2}}dx\right) \quad = O\left(\frac{\log n}{nm}\right).
\end{aligned}$$

This gives $\left|\frac{1}{2nm\pi i}\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h)}\psi\left(\frac{h}{n}\right)\frac{e^{(1-2\mu)h}}{h}dh\right| = O\left(\frac{\log n}{nm}\right)$.

(c) $\left|\frac{1}{2n^2m\pi i}\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h)}\psi'\left(\frac{h}{n}\right)e^{(1-\mu)h}dh\right|$:

We know that $e^{-E(z)}$ and $\psi'(z)$ are bounded. Consequently,

$$\begin{aligned}
&\frac{1}{2n^2m\pi}\left|\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h)}\psi'\left(\frac{h}{n}\right)e^{(1-\mu)h}dh\right| \\
&\quad\leq \frac{1}{2n^2m\pi}\int_{-n\pi}^{n\pi}\left|e^{-E(\mu+i\mu x)}\psi'\left(\frac{1+ix}{n}\right)e^{(1-\mu)(1+ix)}\right|dx \\
&\quad\leq \frac{c}{2n^2m\pi}\int_{-n\pi}^{n\pi}\left|e^{(1-\mu)(1+ix)}\right|dx \\
&\quad= \frac{ce^{1-\mu}}{2n^2m\pi}\int_{-n\pi}^{n\pi}\left|e^{ix(1-\mu)}\right|dx = O\left(\frac{1}{nm}\right).
\end{aligned}$$

This gives $\left|\frac{1}{2n^2\pi i}\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h)}\psi'\left(\frac{h}{n}\right)e^{h}dh\right| = O\left(\frac{1}{nm}\right)$.

Overall, summing up these three parts gives an error term $O\left(\frac{\log n}{nm}\right)$.

3. The part containing $O\left(\frac{1}{hm}\right)$:

   Since $e^{-E(\mu h)}$ and $e^{(1-\mu)h}$ are bounded, we obtain the estimate

$$\begin{aligned}\left|\frac{1}{2m\pi i}\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h)}O\left(\frac{1}{hm}\right)e^{(1-\mu)h}dh\right|&\\ \leq \frac{c}{2m\pi}\int_{-n\pi}^{n\pi}\left|O\left(\frac{1}{m(1+ix)}\right)e^{(1-\mu)(1+ix)}\right|dx&\\ = \frac{ce^{1-\mu}}{2m\pi}\int_{-n\pi}^{n\pi}O\left(\frac{1}{m\sqrt{1+x^2}}\right)dx = O\left(\frac{\log n}{m^2}\right).&\end{aligned}$$

Overall, we get for the probability of $D_n^{[1]} = m$:

$$Pr\left(D_n^{[1]} = m\right) = \frac{1}{m}\rho\left(\frac{1}{\mu}-1\right) + O\left(\frac{\log n}{m^2}\right) = \frac{1}{m}\rho\left(\frac{n}{m}-1\right) + O\left(\frac{\log n}{m^2}\right).$$

Example 3.14. Here, we discuss the probability that a random polynomial has $D_n^{[1]} = m$ and $D_n^{[2]} \leq m/2$, where $D_n^{[2]}$ denotes the degree of the second largest irreducible factor.

The generating function $\widetilde{L}_m(z)$ of polynomials with $D_n^{[1]} = m$ and $D_n^{[2]} \leq m/2$ is given by

$$\begin{aligned}\widetilde{L}_m(z) = S_{\lfloor m/2\rfloor}(z)\cdot\frac{I_m z^m}{1-z^m} &= S_{\lfloor m/2\rfloor}(z)\cdot\frac{z^m}{1-z^m}\cdot\left(\frac{q^m}{m}+O\left(q^{m/2}\right)\right)\\ &= S_{\lfloor m/2\rfloor}(z)\cdot\frac{q^m z^m}{m(1-z^m)}\cdot\left(1+O(mq^{-m/2})\right).\end{aligned}$$

Then, the probability of $D_n^{[1]} = m$ and $D_n^{[2]} \leq m/2$ is

$$\begin{aligned}Pr\left(D_n^{[1]} = m, D_n^{[2]} \leq m/2\right) &= \frac{1}{q^n}[z^n]\widetilde{L}_m(z) = [z^n]\widetilde{L}_m\left(\frac{z}{q}\right) = \frac{1}{2\pi i}\int_{\mathcal{C}}\widetilde{L}_m\left(\frac{z}{q}\right)\frac{dz}{z^{n+1}}\\ &= \frac{1}{2\pi i}\int_{\mathcal{C}} S_{\lfloor m/2\rfloor}\left(\frac{z}{q}\right)\frac{z^m}{m\left(1-z^m/q^m\right)}\frac{dz}{z^{n+1}}(1+O(mq^{-m/2}))\end{aligned}$$

with the contour $\mathcal{C}$ equal to $z = e^{-1/n+i\theta}$ with $-\pi \leq \theta \leq \pi$. Then, by the change of variable $z = e^{-h/n}$, we have

$$
\begin{aligned}
&Pr\left(D_n^{[1]}=m, D_n^{[2]} \le m/2\right)\\
&\quad= \frac{1}{2\pi i}\int_{\mathcal{C}} S_{\lfloor m/2\rfloor}\left(\frac{z}{q}\right)\frac{z^m}{m\left(1-z^m/q^m\right)}\frac{dz}{z^{n+1}}(1+O(mq^{-m/2}))\\
&\quad= \frac{1}{2\pi i}\int_{1+in\pi}^{1-in\pi} S_{\lfloor m/2\rfloor}\left(\frac{e^{-h/n}}{q}\right)\frac{e^{-\mu h}}{m\left(1-e^{-\mu h}/q^m\right)}\frac{-\frac{1}{n}e^{-h/n}dh}{e^{-h-h/n}}(1+O(mq^{-m/2}))\\
&\quad= \frac{1}{2\pi i}\int_{1-in\pi}^{1+in\pi} S_{\lfloor m/2\rfloor}\left(\frac{e^{-h/n}}{q}\right)\frac{e^{(1-\mu)h}}{m\left(1-e^{-\mu h}/q^m\right)}\frac{1}{n}dh(1+O(mq^{-m/2}))\\
&\quad= \frac{1}{2m\pi i}\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h/2)}\frac{e^{O(1/m)}}{n\left(1-e^{-h/n}\right)}e^{(1-\mu)h}\left(1+\frac{e^{-\mu h}}{q^m}+\frac{e^{-2\mu h}}{q^{2m}}+\cdots\right)dh.
\end{aligned}
$$

Here, the error term $O(mq^{-m/2})$ is eliminated by the error term $O(1/m)$. Moreover, we can ignore $\sum_{k\ge 1}\left(e^{-\mu h}/q^m\right)^k$ since it is exponentially small. So, the probability is

$$
Pr\left(D_n^{[1]}=m, D_n^{[2]} \le m/2\right) = \frac{1}{2m\pi i}\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h/2)}\frac{e^{O(1/m)}}{n\left(1-e^{-h/n}\right)}e^{(1-\mu)h}dh.
$$

Next, by (3.3) of Example 3.12,

$$
\begin{aligned}
&Pr\left(D_n^{[1]}=m, D_n^{[2]} \le m/2\right)\\
&\quad= \frac{1}{2m\pi i}\int_{1-in\pi}^{1+in\pi} e^{-E(\mu h/2)}\left[\frac{1}{h}+\frac{1}{n}\psi\left(\frac{h}{n}\right)+O\left(\frac{1}{hm}\right)\right]e^{(1-\mu)h}dh.
\end{aligned}
$$

As before, we break the integral into three parts. For the second and third part, we again obtain $O\left(\frac{\log n}{m^2}\right)$.

For the first part, similar as in Example 3.12 we can replace $[1-in\pi, 1+in\pi]$ by $(1-i\infty, 1+i\infty)$. Then, by the change of variable $v=\mu h/2$ and Lemma 2.20,

$$
\begin{aligned}
\frac{1}{2m\pi i}\int_{1-i\infty}^{1+i\infty} e^{-E(\mu h/2)}\frac{1}{h}e^{(1-\mu)h}dh &= \frac{1}{2m\pi i}\int_{1-i\infty}^{1+i\infty} e^{-E(v)}\frac{1}{2v/\mu}e^{(1-\mu)2v/\mu}\frac{2}{\mu}dv\\
&= \frac{1}{2m\pi i}\int_{1-i\infty}^{1+i\infty} \frac{e^{-E(v)}}{v}e^{2v\left(\frac{1}{\mu}-1\right)}dv \;=\frac{1}{m}\rho\left(\frac{2}{\mu}-2\right).
\end{aligned}
$$

Overall,

$$\begin{aligned} Pr\left(D_n^{[1]} = m,\ D_n^{[2]} \leq m/2\right) &= \frac{1}{m}\,\rho\left(\frac{2}{\mu} - 2\right) + O\left(\frac{\log n}{m^2}\right) \\ &= \frac{1}{m}\,\rho\left(\frac{2n}{m} - 2\right) + O\left(\frac{\log n}{m^2}\right). \end{aligned}$$

Example 3.15. Finally, we discuss the probability that a random polynomials has $D_n^{[1]} = m_1$ and $D_n^{[2]} = m_2$ with $m_2 < m_1$.

The generating function $L_{m_1,m_2}(z)$ of random polynomials with $D_n^{[1]} = m_1$ and $D_n^{[2]} = m_2$ is

$$\begin{aligned} L_{m_1,m_2}(z) = L_{m_2}(z) \cdot \frac{I_{m_1} z^{m_1}}{1 - z^{m_1}} &= L_{m_2}(z) \cdot \frac{z^{m_1}}{1 - z^{m_1}} \cdot \left(\frac{q^{m_1}}{m_1} + O(q^{m_1/2})\right) \\ &= L_{m_2}(z) \cdot \frac{q^{m_1} z^{m_1}}{m_1(1 - z^{m_1})} \cdot \left(1 + O(m_1 q^{-m_1/2})\right). \end{aligned}$$

Then, the probability of $D_n^{[1]} = m_1$ and $D_n^{[2]} = m_2$ is

$$\begin{aligned} &Pr\left(D_n^{[1]} = m_1, D_n^{[2]} = m_2\right) \\ &\quad= \frac{1}{q^n}[z^n]L_{m_1,m_2}(z) = [z^n]L_{m_1,m_2}\left(\frac{z}{q}\right) = \frac{1}{2\pi i}\int_{\mathcal{C}} L_{m_1,m_2}\left(\frac{z}{q}\right)\frac{dz}{z^{n+1}} \\ &\quad= \frac{1}{2\pi i}\int_{\mathcal{C}} S_{m_2}\left(\frac{z}{q}\right)\frac{z^{m_2}}{m_2}\frac{z^{m_1}}{m_1\left(1 - z^{m_1}/q^{m_1}\right)}\frac{dz}{z^{n+1}}\left(1 + O\left(\frac{1}{m_2}\right)\right) \end{aligned}$$

with the contour $\mathcal{C}$ equal to $z = e^{-1/n + i\theta}$ with $-\pi \leq \theta \leq \pi$. Then, by the change of variable $z = e^{-h/n}$, we have

$$\begin{aligned} &Pr\left(D_n^{[1]} = m_1, D_n^{[2]} = m_2\right) \\ &\quad= \frac{1}{2\pi i}\int_{\mathcal{C}} S_{m_2}\left(\frac{z}{q}\right)\frac{z^{m_1+m_2}}{m_1 m_2\left(1 - z^{m_1}/q^{m_1}\right)}\frac{dz}{z^{n+1}}\left(1 + O\left(\frac{1}{m_2}\right)\right) \\ &\quad= \frac{1}{2\pi i}\int_{1+in\pi}^{1-in\pi} S_{m_2}\left(\frac{e^{-h/n}}{q}\right)\frac{e^{-(\mu_1+\mu_2)h}}{m_1 m_2\left(1 - e^{-\mu_1 h}/q^{m_1}\right)}\frac{-\frac{1}{n}e^{-h/n}dh}{e^{-h-h/n}}\left(1 + O\left(\frac{1}{m_2}\right)\right) \\ &\quad= \frac{1}{2\pi i}\int_{1-in\pi}^{1+in\pi} e^{-E(\mu_2 h)}\frac{e^{O(1/m_2)}}{n\left(1 - e^{-h/n}\right)} \cdot \frac{e^{(1-\mu_1-\mu_2)h}}{m_1 m_2\left(1 - e^{-\mu_1 h/q^{m_1}}\right)}dh, \end{aligned}$$

where $\mu_1 = m_1/n$ and $\mu_2 = m_2/n$. Note that we can replace $\left(1 - e^{-\mu_1 h}/q^{m_1}\right)^{-1}$ by 1 since the remainder is exponentially small. Then, as in Example 3.12, the probability is

$$\begin{aligned} &Pr\left(D_n^{[1]} = m_1, D_n^{[2]} = m_2\right) \\ &\quad = \frac{1}{2m_1m_2\pi i}\int_{1-in\pi}^{1+in\pi} e^{-E(\mu_2 h)}\left[\frac{1}{h} + \frac{1}{n}\psi\left(\frac{h}{n}\right) + O\left(\frac{1}{hm_2}\right)\right] e^{(1-\mu_1-\mu_2)h}dh. \end{aligned}$$

We again break this integral into three parts, where the second and third part satisfy $O\left(\frac{\log n}{m_1m_2}\right)$.

For the first part we replace the contour by $(1 - i\infty, 1 + i\infty)$. Then, by Lemma 2.20 and change of variable $v = \mu_2 h$, the main term becomes

$$\begin{aligned} &\frac{1}{2m_1m_2\pi i}\int_{1-in\pi}^{1+in\pi} e^{-E(\mu_2 h)}\frac{1}{h}e^{(1-\mu_1-\mu_2)h}dh \\ &\qquad = \frac{1}{2m_1m_2\pi i}\int_{1-i\infty}^{1+i\infty} e^{-E(v)}\frac{1}{v/\mu_2}e^{(1-\mu_1-\mu_2)v/\mu_2}\frac{1}{\mu_2}dv \\ &\qquad = \frac{1}{2m_1m_2\pi i}\int_{1-i\infty}^{1+i\infty} \frac{e^{-E(v)}}{v}e^{v\left(\frac{1-\mu_1-\mu_2}{\mu_2}\right)}dv = \frac{1}{m_1m_2}\rho\left(\frac{1-\mu_1-\mu_2}{\mu_2}\right). \end{aligned}$$

Overall, we obtain for the probability that $D_n^{[1]} = m_1$ and $D_n^{[2]} = m_2$:

$$\begin{aligned} Pr\left(D_n^{[1]} = m_1,\ D_n^{[2]} = m_2\right) &= \frac{1}{m_1m_2}\rho\left(\frac{1}{\mu_2} - \frac{\mu_1}{\mu_2} - 1\right) + O\left(\frac{\log n}{m_1m_2^2}\right) \\ &= \frac{1}{m_1m_2}\rho\left(\frac{n}{m_2} - \frac{m_1}{m_2} - 1\right) + O\left(\frac{\log n}{m_1m_2^2}\right). \end{aligned}$$

3.4 Other Restrictions on the Degree of Irreducible Factors

Example 3.16. Here, we will discuss the probability that a random polynomial has irreducible factors of distinct degrees.

Let $D(z)$ denote the corresponding generating function. Then,

$$D(z) = \prod_{k\geq 1} \left(1 + I_k z^k\right).$$

So, the probability of a random polynomial having irreducible factors of distinct degrees equals

$$\frac{D_n}{q^n} = [z^n]D(z/q).$$

In order to find the asymptotics, we first rewrite $D(z/q)$ as follows

$$\begin{aligned}
D(z/q) = \prod_{k\geq 1}\left(1 + I_k\left(\frac{z}{q}\right)^k\right) &= \exp\left(\sum_{k\geq 1}\log\left(1 + I_k\left(\frac{z}{q}\right)^k\right)\right) \\
&= \exp\left(-\sum_{k\geq 1}\sum_{m\geq 1}\frac{1}{m}\left(-I_k\frac{z^k}{q^k}\right)^m\right) \\
&= \exp\left(\sum_{m\geq 1}\frac{(-1)^{m+1}}{m}\sum_{k\geq 1}\left(I_k\frac{z^k}{q^k}\right)^m\right).
\end{aligned}$$

Observe that for $m = 1$, $\sum_{k\geq 1} I_k z^k q^{-k}$ equals to $I(z/q)$. For convenience, set $\Lambda_m(z) := \sum_{k\geq 1}\left(I_k z^k q^{-k}\right)^m$, for $m \geq 2$. Then,

$$\begin{aligned}
D(z/q) &= e^{I(z/q)} \cdot \exp\left(\sum_{m\geq 2}\frac{(-1)^{m+1}}{m}\Lambda_m(z)\right) \\
&= \exp\left(\log\frac{1}{1-z} + \sum_{j\geq 2}\frac{\mu(j)}{j}\log\frac{1}{1 - q\cdot\frac{z^j}{q^j}}\right)\cdot\exp\left(\sum_{m\geq 2}\frac{(-1)^{m+1}}{m}\Lambda_m(z)\right) \\
&= \frac{1}{1-z}\exp\left(\sum_{j\geq 2}\frac{\mu(j)}{j}\log\frac{1}{1 - z^j q^{1-j}}\right)\cdot\exp\left(\sum_{m\geq 2}\frac{(-1)^{m+1}}{m}\Lambda_m(z)\right).
\end{aligned}$$

Let $A(z) := \sum_{j\geq 2}\frac{\mu(j)}{j}\log\frac{1}{1-z^j q^{1-j}}$ which is analytic on $|z| < q^{1/2}$. Moreover, for $\Lambda_m(z)$, we have

$$\Lambda_m(z) = \sum_{k\geq 1}\left(I_k z^k q^{-k}\right)^m = \sum_{k\geq 1}\left(\frac{z^k}{k} + O(q^{-k/2})\right)^m$$

$$= \sum_{k\geq 1} \frac{z^{km}}{k^m} + S_m(z) = Li_m(z^m) + S_m(z),$$

where $S_m(z)$ is analytic on $|z| < q^{1/2}$, too.

Next, we plug this into the expression of $D(z/q)$ and factor $D(z/q) = U(z)V(z)$, where

$$U(z) = \frac{1}{1-z} \cdot \exp\left(\sum_{m=2}^{M} \frac{(-1)^{m+1}}{m} Li_m(z^m) \right)$$

and

$$V(z) = e^{A(z)} \cdot \exp\left(\sum_{m=2}^{M} \frac{(-1)^{m+1}}{m} S_m(z) + \sum_{m\geq M+1} \frac{(-1)^{m+1}}{m} \Lambda_m(z) \right).$$

Choose $M = 2$. Then, $V(z)$ is $\mathcal{C}^1$-smooth. Moreover, $U(z)$ is of global order -1. Next, we need to write $U(z) = \widetilde{U}(z) + R(z)$, where $\widetilde{U}(z)$ is a log-power function and $R(z)$ is smooth. Therefore, observe that $U(z)$ has singularities at $z = 1$ and $z = -1$. In order to find the singularity expansions, first note that by Lemma 2.23, the singularity expansion of $Li_2(z)$ at $z = 1$ is

$$\begin{aligned} Li_2(z) &= \tau(\log\tau - 1) + \sum_{j\geq 0, j\neq 1} \frac{(-1)^j}{j!} \zeta(2-j)\tau^j \\ &= \zeta(2) + \tau\log\tau - \tau + \sum_{j\geq 2} \frac{(-1)^j}{j!} \zeta(2-j)\tau^j, \end{aligned}$$

where $\tau := -\log z = (1-z) + O\left((1-z)^2\right)$. Consequently,

$$Li_2(z) = \zeta(2) + (1-z)\log(1-z) + O(1-z).$$

Hence, the singularity expansion of $U(z)$ at $z = 1$ is

$$\begin{aligned} U(z) &= \frac{1}{1-z} \cdot \exp\left(-\frac{\zeta(2)}{2} - \frac{1-z^2}{2} \log(1-z^2) + O(1-z^2) \right) \\ &= \frac{e^{-\zeta(2)/2}}{1-z} \cdot \exp\left(-(1-z)\log(1-z) + O(1-z) \right) \\ &= \frac{e^{-\zeta(2)/2}}{1-z} \cdot \left(1 - (1-z)\log(1-z) + O(1-z) \right) \end{aligned}$$

$$= \frac{e^{-\zeta(2)/2}}{1-z} - e^{-\zeta(2)/2}\log(1-z) + O(1) \qquad \leftarrow \text{where } O(1) \text{ is } \mathcal{C}^0\text{-smooth.}$$

Moreover, the singularity expansion at $z=-1$ is

$$\begin{aligned}
U(z) &= \frac{1}{1-z}\cdot\exp\left(-\frac{\zeta(2)}{2} - \frac{1-z^2}{2}\log(1-z^2) + O(1-z^2)\right)\\
&= \frac{e^{-\zeta(2)/2}}{1-z}\cdot\exp\left(-(1+z)\log(1+z) + O(1+z)\right)\\
&= \frac{e^{-\zeta(2)/2}}{1-z}\cdot\left(1-(1+z)\log(1+z) + O(1+z)\right) = O(1) \qquad \leftarrow \mathcal{C}^0\text{-smooth.}
\end{aligned}$$

Combining this yields $U(z) = \widetilde{U}(z) + R(z)$, where $R(z)$ is $\mathcal{C}^0$-smooth and

$$\widetilde{U}(z) = \frac{e^{-\zeta(2)/2}}{1-z} - e^{-\zeta(2)/2}\log(1-z).$$

Consequently, by applying Theorem 2.14, we obtain

$$[z^n]D\left(\frac{z}{q}\right) \sim e^{-\zeta(2)/2}V(1)[z^n]\left(\frac{1}{1-z} - \log(1-z)\right) \sim e^{-\zeta(2)/2}V(1).$$

In order to make the constant explicit, note that

$$\begin{aligned}
e^{-\zeta(2)/2}V(1) &= \lim_{z\to1}(1-z)D(z/q) = \lim_{z\to1}\frac{D(z/q)}{P(z/q)}\\
&= \lim_{z\to1}\left(\prod_{k\geq1}\left(1+I_k z^k q^{-k}\right)\left(1-z^k q^{-k}\right)^{I_k}\right).
\end{aligned}$$

Next observe,

$$\begin{aligned}
&\prod_{k\geq1}\left(1+I_k z^k q^{-k}\right)\left(1-z^k q^{-k}\right)^{I_k}\\
&\qquad = \prod_{k\geq1}\left(1+\frac{1}{k}+O(q^{k/2})\right)\left(1-\frac{1}{k}+O(k^{-2})\right) = \prod_{k\geq1}\left(1+O(k^{-2})\right).
\end{aligned}$$

Since this infinite product converges, we can plug in $z=1$. Then, we obtain

$$[z^n]D\left(\frac{z}{q}\right) \sim \prod_{k\geq1}\left(1+I_k q^{-k}\right)\left(1-q^{-k}\right)^{I_k}.$$

Finally note that

$$\begin{aligned}\lim_{q\to\infty}\prod_{k\geq 1}(1+I_kq^{-k})(1-q^{-k})^{I_k} &= \lim_{q\to\infty}\prod_{k\geq 1}\left(1+\frac{1}{k}+O(q^{-k/2})\right)e^{-\frac{1}{k}+O(q^{-k/2})}\\ &= \lim_{q\to\infty}\prod_{k\geq 1}\left(1+\frac{1}{k}\right)e^{-\frac{1}{k}} = e^{-\gamma},\end{aligned}$$

where γ is Euler's constant and the last step follows from the product representation of the Gamma function.

Example 3.17. Here, we consider the probability of a random polynomials having irreducible factors of even degrees distinct.

Let $D^{[e]}(z)$ denote the generating function. Then,

$$D^{[e]}(z) = \prod_{k\geq 1}(1+I_{2k}z^{2k})\left(\frac{1}{1-z^{2k-1}}\right)^{I_{2k-1}}.$$

Consequently, the probability of a random polynomials having irreducible factors with even degrees distinct equals

$$\frac{D_n^{[e]}}{q^n} = [z^n]D^{[e]}(z/q).$$

Now, observe

$$\begin{aligned}D^{[e]}(z/q) &= \prod_{k\geq 1}\left(1+I_{2k}(z/q)^{2k}\right)\left(\frac{1}{1-(z/q)^{2k-1}}\right)^{I_{2k-1}}\\ &= \exp\left(\sum_{k\geq 1}\log\left(1+I_{2k}(z/q)^{2k}\right) - I_{2k-1}\log\left(1-(z/q)^{2k-1}\right)\right)\\ &= \exp\left(\sum_{k\geq 1}\sum_{m\geq 1}\frac{(-1)^{m-1}(I_{2k})^m(z/q)^{2km}}{m} + \sum_{k\geq 1}I_{2k-1}\sum_{m\geq 1}\frac{(z/q)^{(2k-1)m}}{m}\right)\\ &= \exp\left(\sum_{m\geq 1}\left(\frac{(-1)^{m+1}}{m}\sum_{k\geq 1}\left(I_{2k}\frac{z^{2k}}{q^{2k}}\right)^m + \frac{1}{m}\sum_{k\geq 1}I_{2k-1}(z/q)^{(2k-1)m}\right)\right).\end{aligned}$$

For convenience, set $\Lambda_m^{[e]}(z) := \sum_{k\geq 1}\left(I_{2k}z^{2k}q^{-2k}\right)^m$ and $\Theta_m(z) := \sum_{k\geq 1} I_{2k-1}\left(\frac{z^{2k-1}}{q^{2k-1}}\right)^m$. For $m=1$, note that

$$\Lambda_1^{[e]}(z) + \Theta_1(z) = \sum_{k\geq 1} I_{2k}\frac{z^{2k}}{q^{2k}} + \sum_{k\geq 1} I_{2k-1}\frac{z^{2k-1}}{q^{2k-1}} = \sum_{k\geq 1} I_k\frac{z^k}{q^k} = I\left(\frac{z}{q}\right).$$

Thus,

$$\begin{aligned}
D^{[e]}(z/q) &= e^{I(z/q)}\cdot\exp\left(\sum_{m\geq 2}\left(\frac{(-1)^{m+1}}{m}\Lambda_m^{[e]}(z) + \frac{1}{m}\Theta_m(z)\right)\right)\\
&= \exp\left(\log\frac{1}{1-z} + \sum_{j\geq 2}\frac{\mu(j)}{j}\log\frac{1}{1-q\cdot\frac{z^j}{q^j}}\right)\\
&\qquad\qquad\cdot\exp\left(\sum_{m\geq 2}\left(\frac{(-1)^{m+1}}{m}\Lambda_m^{[e]}(z) + \frac{1}{m}\Theta_m(z)\right)\right)\\
&= \frac{1}{1-z}\exp\left(\sum_{j\geq 2}\frac{\mu(j)}{j}\log\frac{1}{1-z^jq^{1-j}}\right)\\
&\qquad\qquad\cdot\exp\left(\sum_{m\geq 2}\left(\frac{(-1)^{m+1}}{m}\Lambda_m^{[e]}(z) + \frac{1}{m}\Theta_m(z)\right)\right).
\end{aligned}$$

Let $A(z) := \left(\sum_{j\geq 2}\frac{\mu(j)}{j}\log\frac{1}{1-z^jq^{1-j}}\right)$ which is analytic on $|z| < q^{1/2}$.

Next, consider $\Lambda_m^{[e]}(z)$ for which we have

$$\begin{aligned}
\Lambda_m^{[e]}(z) &= \sum_{k\geq 1}\left(I_{2k}\frac{z^{2k}}{q^{2k}}\right)^m = \sum_{k\geq 1}\left(\frac{z^{2k}}{2k} + O(q^{-k})\right)^m\\
&= \frac{1}{2^m}\sum_{k\geq 1}\frac{(z^{2m})^k}{k^m} + S_m^{[e]}(z) = \frac{1}{2^m}Li_m(z^{2m}) + S_m^{[e]}(z),
\end{aligned}$$

where $S_m^{[e]}(z)$ is analytic on $|z| < q^{1/2}$. By a similar argument, $\Theta_m(z)$ is analytic on $|z| < q^{1/2}$, too.

Now, after plugging every thing into $D(z/q)$, we can factor $D(z/q) = U(z)V(z)$ with

$$U(z) = \frac{1}{1-z}\cdot\exp\left(\sum_{m=2}^{M}\frac{(-1)^{m+1}}{m2^m}Li_2(z^{2m})\right)$$

and

$$V(z) = e^{A(z)} \cdot \exp\left(\sum_{m=2}^{M} \frac{(-1)^{m+1} S_m^{[e]}(z) + \Theta_m(z)}{m} \right.$$
$$\left. + \sum_{m \geq M+1} \frac{(-1)^{m+1} \Lambda_m^{[e]}(z) + \Theta_m(z)}{m} \right).$$

As before, choose $M = 2$. Then, $V(z)$ is $\mathcal{C}^1$-smooth. Moreover, $U(z)$ is of global order -1 with singularity at $z = \pm 1$ and $z = \pm i$.

In order to find the singularity expansions, we again use the singularity expansion of $Li_2(z)$ at $z = 1$

$$Li_2(z) = \zeta(2) + (1-z)\log(1-z) + O(1-z).$$

Then, as before, $U(z) = \widetilde{U}(z) + R(z)$ with $R(z)$ $\mathcal{C}^0$-smooth and

$$\widetilde{U}(z) = \frac{e^{-\zeta(2)/8}}{1-z} - \frac{1}{4} e^{-\zeta(2)/8} \log(1-z).$$

Consequently, by applying Theorem 2.14, we obtain

$$[z^n] D^{[e]}\left(\frac{z}{q}\right) \sim e^{-\zeta(2)/8} V(1) [z^n] \left(\frac{1}{1-z} - \frac{\log(1-z)}{4} \right) \sim e^{-\zeta(2)/8} V(1).$$

In order to make the constant explicit, note that

$$e^{-\zeta(2)/8} V(1) = \lim_{z \to 1} (1-z) D^{[e]}(z/q) = \lim_{z \to 1} \frac{D^{[e]}(z/q)}{P(z/q)}$$
$$= \lim_{z \to 1} \left(\prod_{k \geq 1} \left(1 + I_{2k} z^{2k} q^{-2k}\right) \left(1 - z^{2k} q^{-2k}\right)^{I_{2k}} \right).$$

Next observe that

$$\prod_{k \geq 1} \left(1 + I_{2k} z^{2k} q^{-2k}\right) \left(1 - z^{2k} q^{-2k}\right)^{I_{2k}}$$
$$= \prod_{k \geq 1} \left(1 + \frac{1}{2k} + O(q^{-k})\right) \left(1 - \frac{1}{2k} + O(k^{-2})\right) = \prod_{k \geq 1} \left(1 + O(k^{-2})\right),$$

which is convergent. Hence, the above limit can be evaluated by plugging in $z = 1$. This finally gives

$$[z^n]D^{[e]}\left(\frac{z}{q}\right) \sim \prod_{k\geq 1}\left(1 + I_{2k}q^{-2k}\right)\left(1 - q^{-2k}\right)^{I_{2k}}.$$

Finally, for Chapter 4, we need another example which is a slight variant of Example 3.16.

Example 3.18. The probability that a random polynomials has irreducible factors (counted without multiplicities) of distinct degrees.

Let $D^{\star}(z)$ denote the corresponding generating function. Then,

$$D^{\star}(z) = \prod_{k\geq 1}\left(1 + I_k z^k + I_k z^{2k} + \cdots\right) = \prod_{k\geq 1}\left(1 + \frac{I_k z^k}{1 - z^k}\right).$$

Using a similar analysis as before yields

$$[z^n]D^{\star}(z/q) \sim \prod_{k\geq 1}\left(1 + \frac{I_k}{q^k - 1}\right)\left(1 - q^{-k}\right)^{I_k}.$$

Note that again

$$\lim_{q\to\infty}\prod_{k\geq 1}\left(1 + \frac{I_k}{q^k - 1}\right)\left(1 - q^{-k}\right)^{I_k} = \lim_{q\to\infty}\prod_{k\geq 1}\left(1 + \frac{1}{k} + O\left(q^{-\frac{k}{2}}\right)\right)e^{-\frac{1}{k} + O(q^{-\frac{k}{2}})} = e^{-\gamma}.$$

Chapter 4

Application to Polynomial Factorization

In this chapter, we give some applications of the results of the previous chapter to factorization of polynomials. We first explain a three step procedure which is used by many factorization algorithms.

The first step is the observation that it suffices to factorize square free polynomials.

Step 1: Note that if there are repeated factors in the prime factorization of $f(x)$, then the repeated factors will also appear in the derivative of $f(x)$. Hence, we can obtain the repeated factors by computing the greatest common divisor of $f(x)$ and $f'(x)$. Next, by dividing $f(x)$ by $\gcd(f(x), f'(x))$, we can get rid of the repeated factors and turn the polynomial $f(x)$ into a squarefree polynomial. (Note that since the derivative of a irreducible factor whose multiplicity is a multiple of p is 0 in the finite field $\mathbb{F}_q$ with $q = p^n$, so this procedure does not work if $f(x)$ contains irreducible factors whose multiplicity is a multiple of p. A slight modification of the procedure, however, works. For the sake of simplicity, we will not discuss this here.) We will call the output of this step $\widetilde{f}(z)$.

The second step will factor $\widetilde{f}(z)$ into a product of $b^{[k]}(x)$, where $b^{[k]}(x)$ contains all irreducible factors of degree k. For this we will use a well-known fact from the theory of finite fields, namely, $x^{q^k} - x$ is the product of all irreducible polynomials of degree $\leq k$ in $\mathbb{F}_q$. Consequently, computing the greatest common divisor of $\widetilde{f}(z)$ and $x^{q^k} - x$ will separate the factors into two parts: one containing all irreducible factors of degree $\leq k$ and the other containing the remaining factors. Using this observation, the second step works as follows.

Step 2: We start from $k = 1$ and compute the greatest common divisor of $\widetilde{f}(z)$ and $x^{q^k} - x$. This gives $b^{[1]}(x)$. Then we replace $\widetilde{f}(z)$ by $\widetilde{f}(z)/b^{[1]}(x)$ and continue like this with $k = 2,\, 3, \cdots$ to find the other factors.

After Step 2, the problem is reduced to the factorization of $b^{[k]}(x)$. However, there is no efficient deterministic algorithm for this factorization. Consequently, we use a random procedure. Therefore note that since $b^{[k]}(x)$ is a product of irreducible factors of degree k, i.e., $b^{[k]}(x) = r_1(x) \cdot r_2(x) \cdots r_j(x)$ with $r_i(x)$ irreducible and $\deg(r_i(x)) = k$, so $\mathbb{F}_q[x]/\left(b^{[k]}(x)\right)$ is isomorphic to the product of $\mathbb{F}_q[x]/\left(r_i(x)\right)$. Next recall that in $\mathbb{F}_q[x]/\left(r_i(x)\right) \setminus \{0\}$, half of the elements are squares and the other half are not. Thus, if we pick a polynomial $h(x)$ at random, then if it is a square in $\mathbb{F}_q[x]/\left(r_i(x)\right)$, we have $h(x)^{\frac{q^k-1}{2}} \equiv 1 \mod r_i(x)$, i.e., $r_i(x)\big|h(x)^{\frac{q^k-1}{2}} - 1$. This will happen with probability $1/2$. Consequently, computing the $\gcd$ of $h(x)^{\frac{q^k-1}{2}} - 1$ and $b^{[k]}(x)$ will give the irreducible factors for which $h(x)$ is a square. The number of these factors will be binomially distributed with mean $j/2$. Using this idea, the step 3 works as follows.

Step 3: For every $b^{[k]}(x)$, if the degree of $b^{[k]}(x)$ is greater than k, we choose a random polynomial $h(x)$ with degree equal $deg(b^{[k]}(x)) - 1$. Then, let $v(x)$ be the greatest common divisor of $b^{[k]}(x)$ and $h(x)^{\frac{q^k-1}{2}} - 1$. After $v(x)$ is found, we repeat this process with $v(x)$ and $b^{[k]}(x)/v(x)$ until all irreducible factors are found.

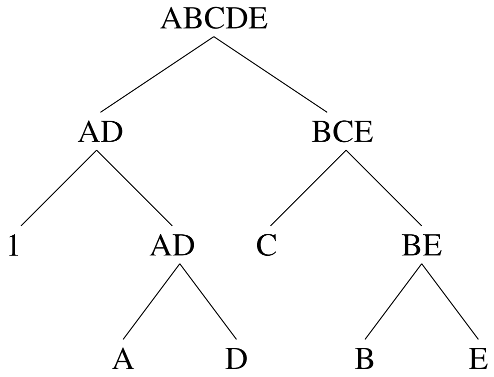


Figure: A possible outcome of Step 3 if $b^{[k]} = $ ABCDE with A, B, C, D, E irreducible factors of degree k.

Now, we are going to consider an example. For example, consider the following polynomial over $\mathbb{F}_5$:

$$f(x) = x^9 + 2x^8 + 4x^7 + 2x^6 + 2x^5 + 3x^4 + x^3 + x^2 + 3x + 1.$$

Step 1: The derivative of $f(x)$, is

$$f'(x) = 4x^8 + x^7 + 3x^6 + 2x^5 + 2x^3 + 3x^2 + 2x + 3.$$

Consequently, $\gcd(f, f') = x + 4$, which means that the factor $x + 4$ is repeated. So we divide $f(x)$ by $x + 4$ and obtain

$$f(x) = (x+4) \cdot \widetilde{f}(x) = (x+4) \cdot (x^8 + 3x^7 + 2x^6 + 4x^5 + x^4 + 4x^3 + x + 4),$$

where $\widetilde{f}(x)$ is a squarefree polynomial.

Step 2: Let $k = 1$. Then, we have

$$b^{[1]}(x) = \gcd(\widetilde{f}(x),\, x^5 - x) = x^2 + 2x + 2.$$

Next, divide $\widetilde{f}(x)$ by $x^2 + 2x + 2$ which gives $x^6 + x^5 + 3x^4 + x^3 + 3x^2 + x + 2$. Set $k = 2$. Then,

$$b^{[2]}(x) = \gcd\left(\frac{\widetilde{f}(x)}{b^{[1]}(x)},\, x^{25} - x\right) = x^6 + x^5 + 3x^4 + x^3 + 3x^2 + x + 2.$$

Thus, we have factorized $\widetilde{f}(x)$ as follows

$$\widetilde{f}(x) = b^{[1]}(x) \cdot b^{[2]}(x) = (x^2 + 2x + 2) \cdot (x^6 + x^5 + 3x^4 + x^3 + 3x^2 + x + 2).$$

Step 3: Here, we have to factorize $b^{[1]}(x)$ and $b^{[2]}(x)$:

1. For $b^{[1]}(x)$:

   Since the degree of $b^{[1]}(x)$ equals 2, we choose a random polynomial $h(x)$ of degree 1, e.g., $h(x) = x + 1$. Then, $h(x)^{\frac{q^k-1}{2}} - 1$ is

   $$(x+1)^{\frac{5^1-1}{2}} - 1 = (x+1)^2 - 1 = (x^2 + 2x + 1) - 1 = x^2 + 2x.$$

   However,

   $$v(x) = \gcd(b^{[1]}(x),\, x^2 + 2x) = 1.$$

   So, we have to repeat this step with another random polynomial. Therefore, pick $h(x) = x + 2$. Then,

   $$(x+2)^{\frac{5^1-1}{2}} - 1 = (x+2)^2 - 1 = (x^2 + 4x + 4) - 1 = x^2 + 4x + 3.$$

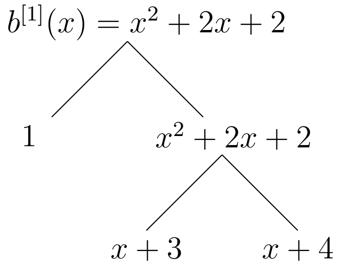
   Next,

   $$v(x) = \gcd(b^{[1]}(x),\, x^2 + 4x + 3) = x + 3.$$

   The other factor is

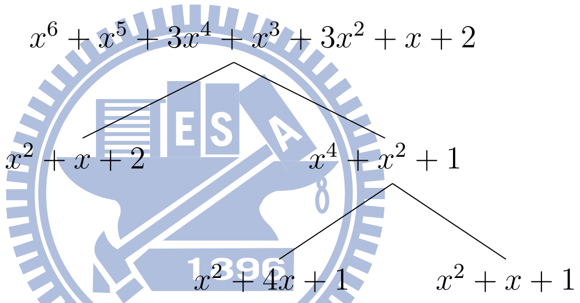
   $$b^{[1]}(x)/(x+3) = x + 4.$$

So, we finished the factorization of $b^{[1]}(x)$, having



2. For $b^{[2]}(x)$:

   Since its degree of $b^{[2]}(x)$ equals 6, so we choose a random polynomial $h(x)$ of degree 5. A similar procedure as before then yields:



Overall, we have factorized the polynomial and obtain:

$$f(x) = (x+3)(x+4)^2(x^2+x+1)(x^2+x+2)(x^2+4x+1).$$

Next, we are going to explain the usefulness of the results of the previous chapter when analyzing the algorithm.

First, Step 1's purpose was to turn the random polynomial into a squarefree polynomial. Since by Example 3.7 the probability that a random polynomial is squarefree equals $1-1/q$, this step is very fast since there is only a probability of $1/q$ that the division is needed. Moreover, if the polynomial is not squarefree, again by Example

3.7 the expected value of the degree of the remaining part is still small, so that the division is not costly on average, even in this case.

Second, recall that the purpose of Step 2 was to separate the irreducible factors according to their degrees. The most simple way to do this is by repeating this step from $k = 1$ to n (we call this *strategy 1*). However, note that if $k > n/2$, then the remaining polynomial is either irreducible or constant. Thus, a better strategy would be to consider k from 1 to $n/2$ (*strategy 2*). Finally, an even better strategy is based on the following observation: if the degree of the remaining polynomial is $< 2k$ in the k-th step, then the remaining polynomial is again either already irreducible or a constant. This leads to a third strategy (*strategy 3*) for which we repeat until

$$k > \max\left\{\lfloor D_n^{[1]}/2\rfloor, D_n^{[2]}\right\},$$

where $D_n^{[1]}$ and $D_n^{[2]}$ are as in Chapter 3. The complexity of the Step 2 for these three strategies was analyzed in 4.1. In particular, for strategy 3, the results from Section 3.3 were used. We only state the result without giving a more detailed explanation. We need the following assumptions: let $\tau_1 n^2$ be the cost of multiplying two polynomials of degree $< n$ and reducing the result module a polynomial of degree equal to n. Moreover, let $\tau_2 n^2$ be the cost of computing the greatest common divisor of two polynomials of degree at most n. Then, in [10, p. 21] the following result was proved.

Theorem 4.1. *The expected complexity of Step 2 under the three strategies mentioned above when applied to a random polynomial of degree n is as follows*

$$\begin{cases} 0.47n^3 & \textit{for strategy 1;} \\ 0.31n^3 & \textit{for strategy 2;} \\ 0.27n^3 & \textit{for strategy 3.} \end{cases}$$

Here, $\lambda(q) := \lfloor \log_2 q \rfloor + \nu(q) - 1$ and $\nu(q)$ is the number of ones in the binary representation of q.

Finally, we consider Step 3 in which the polynomials $b^{[k]}(x)$ with all irreducible factors of equal degree k are factorized. First note that nothing has to be done in this step if all the $b^{[k]}(x)$ are irreducible. According to Example 3.18, the probability for this $e^{-\gamma}$ when n is very large. Second, as for the complexity of this step, in [10, p. 39] a result was proved which used a connection to random tries. For completeness, we recall the result here.

Theorem 4.2. *The expected complexity of Step 3 is* $O(n^2 \log q)$. *More precisely, the complexity is asymptotic to*

$$\left(\frac{3}{4}\tau_1 \frac{q^2}{q^2-1}\log_2 q\right)(1+\xi_n)n^2,$$

where $-\frac{1}{3}+o(1) \leq \xi_n \leq \frac{1}{3}+o(1)$.

Bibliography

[1] ABRAMOWITZ, M., STEGUN, I. (1970). *Handbook of Mathematical Functions.* Dover, New York.

[2] BACH E., SHOUP V. (1990). Factoring Polynomials Using Fewer Random Bits, *Journal of Symbolic Computation*, **9**, 229–239.

[3] BERLEKAMP E. (1967). Factoring Polynomials over Finite Fields, *Bell Systems Technol. J.*, **46** 1853–1859.

[4] BERLEKAMP, E. (1968). *Algebraic Coding Theory.* McGraw Hill, New York NY.

[5] BOCHNER S., CHANDRASEKHARAN K. (1949). *Fourier Transforms.* Princeton University Press.

[6] BUCHMANN, J. (1990). Complexity of Algorithms in Algebraic Number Theory. In *Number Theory. Proc. First Conf. Canadian Number Theory Assoc.* Walter de Gruyter, 37–53.

[7] CHOR, B., RIVEST, R. L. (1985). A Knapsack type Public Key Cryptosystem based on Arithmetic in Finite Fields, *IEEE Trans. Inf. Theory*, **34**, 901–909.

[8] COLLINS, G. E. (1979). Factoring Univariate Integral Polynomials in Polynomial Average Time. In Proceedings of EUROSAM'79 Marseille, France, LNCS **72**, 317–329.

[9] FLAJOLET, P., FUSY E., GOURDON X., PANARIO D., POUYANNE N. (2006). A Hybrid of Darbouxs Method and Singularity Analysis in Combinatorial Asymptotics, *The Electronic Journal of Combinatorics,* **13**, 35 pages.

[10] FLAJOLET, P., GOURDON X., PANARIO D. (2001). The Complete Analysis of a Polynomial Factorization Algorithm over Finite Fields, *Journal of Algorithms,* **409**, 37–81.

[11] FLAJOLET, P., ODLYZKO, A. (1990). Singularity Analysis of Generating Functions, *SIAM Journal on Discrete Mathematics*, **3**, 216–240.

[12] FLAJOLET, P., SEDGEWICK, R. (2009). *Analytic Combinatorics*. Cambridge University Press.

[13] KNUTH, D. E. (1998). *The Art of Computer Programming, Volume 2, Seminumerical Algorithms*, 3^{rd} edn. Reading, MA, Addison-Wesley.

[14] LENSTRA A. K., LENSTRA, JR., H. W., LOVASZ, L. (1982). Factoring Polynomials with Rational Coefficients, *Math. Ann.*, **261**, 515–534.

[15] LENSTRA, JR., H. W. (1991). On the Chor-Rivest Knapsack Cryptosystem, *J. Cryptol.*, **3**, 149–155.

[16] LEWIN L. (1991). *Structural Properties of Polylogarithms.* American Mathematical Society.

[17] Odlyzko, A. (1985). Discrete Logarithms and Their Cryptographic Significance. In *Advances in Cryptology: Proceedings of EUROCRYPT 1984, Paris, France,* LNCS **209**, 224–314.

[18] Rónyai L.(1988). Factoring Polynomials over Finite Fields, *Journal of Algorithms*, **9**, 391–400.

[19] Zassenhaus, H. (1969). On Hensel Factorization, I, *J. Number Theory*, **1**, 291–311.