sciendo

uniform distribution theory

DOI: 10.2478/UDT-2023-0002
Unif. Distrib. Theory **18** (2023), no.1, 9–30

NOTES ON THE DISTRIBUTION OF ROOTS MODULO PRIMES OF A POLYNOMIAL IV

Yoshiyuki Kitaoka*

Asahi, JAPAN

ABSTRACT. For polynomials $f(x), g_1(x), g_2(x)$ over $\mathbb{Z}$, we report several observations about the density of primes p for which $f(x)$ is fully splitting at p and $\left\{\frac{g_1(r)}{p}\right\} < \left\{\frac{g_2(r)}{p}\right\}$ for some root r of $f(x) \equiv 0 \bmod p$.

Communicated by Shigeki Akiyama

1. Introduction

Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

be an integral polynomial, i.e., $a_i \in \mathbb{Z}$ for $i = 0, \ldots, n-1$ of degree n with complex roots $\alpha_1, \ldots, \alpha_n$. We fix the numbering of roots once and for all, and define the vector spaces LR, LR_0 over the rational number field $\mathbb{Q}$ by

$$LR := \left\{(l_1, \ldots, l_{n+1}) \in \mathbb{Q}^{n+1} \,\middle|\, \sum_{i=1}^{n} l_i\alpha_i = l_{n+1}\right\},$$

$$LR_0 := \left\{(l_1, \ldots, l_n) \in \mathbb{Q}^{n} \,\middle|\, \sum_{i=1}^{n} l_i\alpha_i \in \mathbb{Q}\right\},$$

and we take and fix a $\mathbb{Z}$-basis of $LR \cap \mathbb{Z}^{n+1}$

$$(m_{j,1}, \ldots, m_{j,n}, m_j) \ \big(j = 1, \ldots, t\,(:= \dim_{\mathbb{Q}} LR \geq 1)\big),$$

since the non-zero integral vector $(1, \ldots, 1, -a_{n-1})$ is in $LR \cap \mathbb{Z}^{n+1}$.

2020 Mathematics Subject Classification: 11K.
Keywords: equidistribution, polynomial, roots modulo a prime.

* The author is retired.

Next, we write, for a positive number X

$$\mathrm{Spl}_X(f) := \{p \le X \mid f(x) \text{ is fully splitting modulo } p\},$$

where the letter p denotes a prime number, and $\mathrm{Spl}(f) := \mathrm{Spl}_\infty(f)$.

We assume the following conditions on the local roots $r_1, \ldots, r_n\, (\in \mathbb{Z})$ of $f(x) \equiv 0 \bmod p$ for a prime $p \in \mathrm{Spl}(f)$:

$$f(x) \equiv \prod_{i=1}^{n}(x - r_i) \bmod p,$$
$$0 \le r_1 \le r_2 \le \cdots \le r_n < p.$$

These conditions determine the ith-root r_i of $f(x) \equiv 0 \bmod p$ uniquely.

We write, for a permutation $\sigma \in S_n$

$$\mathrm{Spl}_X(f, \sigma) := \left\{ p \in \mathrm{Spl}_X(f) \,\middle|\, \sum_{i=1}^{n} m_{j,i} r_{\sigma(i)} \equiv m_j \bmod p \, (1 \le {}^\forall j \le t) \right\},$$

and we define the density by

$$Pr(f, \sigma) := \lim_{X \to \infty} \frac{\#\mathrm{Spl}_X(f, \sigma)}{\#\mathrm{Spl}_X(f)},$$

where *we suppose that the limit exists*. The existence of the limit is supported by computer experiment. It is easy to see $\mathrm{Spl}(f) = \cup_{\sigma \in S_n} \mathrm{Spl}(f, \sigma)$.

Next, we introduce the following geometric objects

$$\Delta := \{\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n \mid 0 \le x_1 \le \cdots \le x_n \le 1\},$$

$$\hat{\mathfrak{D}}_n := \left\{ (x_1 \ldots, x_n) \in \Delta \,\middle|\, \sum_{i=1}^{n} x_i \in \mathbb{Z} \right\},$$

$$\mathfrak{D}(f, \sigma) := \left\{ (x_1 \ldots, x_n) \in \Delta \,\middle|\, \sum_{i=1}^{n} m_{j,i}\, x_{\sigma(i)} \in \mathbb{Z} \ (1 \le {}^\forall j \le t) \right\} (\subset \hat{\mathfrak{D}}_n).$$

Here, the dimension of $\mathfrak{D}(f, \sigma)$ is less than or equal to $n - t$ and we consider its volume as an $n - t$-dimensional set. In case of $t = 1$, we have $\mathfrak{D}(f, \sigma) = \hat{\mathfrak{D}}_n$.

Moreover, we introduce two groups :

$$\hat{\boldsymbol{G}} := \{\sigma \in S_n \mid \sigma(LR) \subset LR\},$$

$$\boldsymbol{G} := \{\sigma \in S_n \mid \sigma(LR_0) \subset LR_0\},$$

where we let, for $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$, $x \in \mathbb{R}$ and a permutation $\sigma \in S_n$

$$\sigma(\boldsymbol{x}) := \big(x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)}\big), \qquad \sigma((\boldsymbol{x}, x)) := \big(\sigma(\boldsymbol{x}), x\big).$$

The group $\hat{\boldsymbol{G}}$ is a subgroup of $\boldsymbol{G}$, and in case that $f(x)$ is irreducible, they are identical.

We proposed the following two conjectures in the previous papers.

Conjecture 1.1 ([K1]). *For a permutation σ with $Pr(f,\sigma)>0$, the ratio*

$$c=\frac{\mathrm{vol}(\mathfrak{D}(f,\sigma))}{Pr(f,\sigma)}$$

is independent of σ. If $\boldsymbol{G}=\hat{\boldsymbol{G}}$ holds, then two conditions $Pr(f,\sigma)>0$ and $\mathrm{vol}\big(\mathfrak{D}(f,\sigma)\big)>0$ are equivalent.

Conjecture 1.2 ([K3]). *Suppose that $Pr(f,\sigma)>0$ and $\mathrm{vol}\big(\mathfrak{D}(f,\sigma)\big)>0$ for a permutation σ; then for a set $D(\subset\mathbb{R}^n)$ satisfying that $D=\overline{D^\circ}$ and $D\cap\mathfrak{D}(f,\sigma)$ is the closure of the intersection of D° and the interior of $\mathfrak{D}(f,\sigma)$, we have*

$$Pr_D(f,\sigma):=\lim_{X\to\infty}\frac{\#\{p\in\mathrm{Spl}_X(f,\sigma)\mid(\frac{r_1}{p},\dots,\frac{r_n}{p})\in D\}}{\#\mathrm{Spl}_X(f,\sigma)}$$

$$=\frac{\mathrm{vol}(D\cap\mathfrak{D}(f,\sigma))}{\mathrm{vol}(\mathfrak{D}(f,\sigma))}. \tag{1}$$

To study the property of $Pr(f,\sigma)$, we introduce more notations:

$$\boldsymbol{G}_0:=\{\mu\in S_n\mid\alpha_{\mu(i)}=\tilde{\mu}(\alpha_i)\ \big(1\le{}^\forall i\le n\big)\text{ for }{}^\exists\tilde{\mu}\in\mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q})\},$$

$$M(f,\mu):=\{p\in\mathrm{Spl}(f)\mid\alpha_i\equiv r_{\mu(i)}\bmod\mathfrak{p}\ \big(1\le{}^\forall i\le n\big)\text{ for }{}^\exists\mathfrak{p}\,|\,p\},$$

where $\mathfrak{p}$ denotes a prime ideal of $\mathbb{Q}(f):=\mathbb{Q}(\alpha_1,\dots,\alpha_n)$ over p. The following proposition is fundamental ([K2]).

Proposition 1.1. *Suppose $\#M(f,\sigma)=\infty$; then for $\eta\in S_n$ the following three conditions are equivalent :*

(i) $M(f,\eta)=M(f,\sigma)$,

(ii) $\sigma^{-1}\eta\in\boldsymbol{G}_0$,

(iii) $\#\big(M(f,\eta)\cap M(f,\sigma)\big)=\infty$,

and we have

$$\mathrm{Spl}(f,\sigma)=\big(\cup_\mu M(f,\mu)\big)\cup T_\sigma, \tag{2}$$

where μ runs over the set of permutations satisfying $\mu\in\sigma\hat{\boldsymbol{G}}$ with $\#M(f,\mu)=\infty$, and T_σ is a finite set. Suppose $\#\,\mathrm{Spl}(f,\sigma)=\infty$, then for $\nu\in S_n$ we see that $\mathrm{Spl}(f,\sigma)\cap\mathrm{Spl}(f,\nu)$ is an infinite set if and only if $\sigma\hat{\boldsymbol{G}}=\nu\hat{\boldsymbol{G}}$, and then the difference between $\mathrm{Spl}(f,\sigma)$ and $\mathrm{Spl}(f,\nu)$ is a finite set.

The notion $M(f,\mu)$ here is better than M_μ in [K2], where the prime ideal $\mathfrak{p}$ is previously chosen arbitrarily.

Let us report three observations related to the property of $M(f,\mu)$.

First, it is likely that the density of $M(f,\mu)$ in $\mathrm{Spl}(f,\sigma)$ $\big(= \mathrm{Spl}(f,\mu)\big)$ at (2) equal to $1/[\hat{\boldsymbol{G}} : \boldsymbol{G}_0]$. We note that the condition $\hat{\boldsymbol{G}} = \boldsymbol{G}_0$ implies $\mathrm{Spl}(f,\sigma) = M(f,\sigma)$ except a finite set by Proposition 1.1.

Secondly, let us introduce the equivalence relation $\sim$ among monic integral polynomials as follows. For monic integral polynomials $f(x), g(x)$ of degree n, $f(x) \sim g(x)$ if and only if $g(x) = \delta^n f(\delta x + m)$ with $\delta = \pm 1$ and $m \in \mathbb{Z}$ holds. Denote the roots of $f(x)$ by α_i $(i = 1, \ldots, n)$ and assume that any root α_i is not a rational integer. Then $\beta_i := \delta(\alpha_i - m)$ are roots of $g(x)$, and for local roots r_i of $f(x)$ at $p \in \mathrm{Spl}(f) = \mathrm{Spl}(g)$, integers $r_i' := \delta(r_i - m)$ are roots of $g(x) \equiv 0 \bmod p$, and $0 < r_1 - m \le \cdots \le r_n - m < p$ if p is sufficiently large. Hence writing $R_i := r_i'$ in the cse of $\delta = 1$, otherwise, $R_i := p + r_{n-i+1}'$, we see that R_i $(i = 1, \ldots, n)$ are local roots of $g(x)$ if p is sufficiently large. Then we see that neglecting small primes

$$\begin{aligned} M(g,\mu) &= \big\{p \in \mathrm{Spl}(g) \mid \beta_i \equiv R_{\mu(i)} \bmod \mathfrak{p}\ (1 \le {}^\forall i \le n) \text{ for } {}^\exists \mathfrak{p} \mid p\big\} \\ &= \begin{cases} M(f,\mu) & \text{if} \quad \delta = 1, \\ M(f,\mu') & \text{if} \quad \delta = -1, \end{cases} \end{aligned}$$

where the permutation μ' is defined by $\mu'(i) := n + 1 - \mu(i)$. So, the equivalence class of $f(x)$ gives the same division $M(f,\mu)$ $(\mu \in S_n)$ of the set $\mathrm{Spl}(f)$ of primes. It is likely, conversely that the division $M(f,\mu)$ $(\mu \in S_n)$ of $\mathrm{Spl}(f)$ characterizes the above equivalence class among polynomials $g(x)$ under assumptions that $\mathbb{Q}(g) = \mathbb{Q}(f)$, $\deg g = \deg f$ and f, g have the same linear relations among roots. In case of

$$\begin{aligned} f(x) = x^3 - 3x + 1, x^4 + 2x^3 + 3x^2 - 3x + 1, x^4 + 3x^2 - 2x + 2, \\ x^4 - x^3 + 2x^2 + x + 1, x^4 + x^3 + x^2 + x + 1, (x^2)^2 + x^2 - 1, \\ (x^2)^2 + 1, x^4 + 4x^3 + 2x^2 - 4x - 1 = (x^2 + 2x)^2 - 2(x^2 + 2x) - 1, \end{aligned}$$

which exhaust all types (with respect to $\mathrm{Gal}\big(\mathbb{Q}(f)/\mathbb{Q}\big)$ and the existence of non-trivial linear relations among roots) of polynomials of degree $3, 4$ with $[\hat{\boldsymbol{G}} : \boldsymbol{G}_0] > 1$, it is true as far as we checked.

The third observation is related to the distribution of the decimal part $\{\frac{g(r)}{p}\}$ of $\frac{g(r)}{p}$ for an integral polynomial $g(x)$, where r runs over local roots of a polynomial $F(x)\big(p \in \mathrm{Spl}(F)\big)$. Let $f(x)$ be a monic irreducible integral polynomial with roots α_i as before and suppose $\mathbb{Q}(f) = \mathbb{Q}(\alpha)$ for an algebraic integer α with the monic minimal polynomial $F(x)$ and write $\alpha_i = g_i(\alpha)$ $(i = 1, \ldots, n)$

by a polynomial $g_i(x) \in \mathbb{Q}[x]$. Then we see that except finitely many primes p

$$\begin{aligned} M(f,\mu) &= \{\, p \in \mathrm{Spl}(f) \mid g_i(\alpha) \equiv r_{\mu(i)} \bmod \mathfrak{p} \ \ (1 \le {}^{\forall} i \le n) \text{ for } {}^{\exists}\mathfrak{p} \,|\, p\} \\ &= \left\{ p \in \mathrm{Spl}(f) \;\middle|\; \begin{array}{l} \text{there is an integer } r \text{ such that } F(r) \equiv 0 \bmod p \\ \text{and } g_i(r) \equiv r_{\mu(i)} \bmod p \ \ (1 \le {}^{\forall} i \le n) \end{array} \right\} \\ &= \left\{ p \in \mathrm{Spl}(f) \;\middle|\; \begin{array}{l} \left\{\frac{g_{\mu^{-1}(1)}(r)}{p}\right\} \le \cdots \le \left\{\frac{g_{\mu^{-1}(n)}(r)}{p}\right\} \ \text{ for} \\ \text{some integer root } r \text{ of } F(x) \equiv 0 \bmod p \end{array} \right\}, \end{aligned}$$

where $\{x\}$ denotes the decimal part of x, i.e., $0 \le \{x\} < 1$ and $x - \{x\} \in \mathbb{Z}$. Here we note that $\mathfrak{p} = (\alpha - r, p)$ is a prime ideal of $\mathbb{Q}(\alpha)$ for p in $\mathrm{Spl}(f)$ except finitely many primes, and the ideal $\mathfrak{p}$ and $r \bmod p$ above are unique if the prime p is sufficiently large. As stated, the density of the above set in $\mathrm{Spl}(f,\mu)$ seems to be equal to $1/[\hat{\boldsymbol{G}} : \boldsymbol{G}_0]$. If, moreover $\mathbb{Q}(\alpha_1)$ is a Galois extension over $\mathbb{Q}$, then letting $\alpha = \alpha_1, g_1(x) = x, F(x) = f(x)$, we see that the difference between sets $M(f,\mu)$ and

$$\begin{aligned} &\{p \in \mathrm{Spl}(f) \mid g_i(r_{\mu(1)}) \equiv r_{\mu(i)} \bmod p \ (1 \le {}^{\forall} i \le n)\} \\ &= \left\{ p \in \mathrm{Spl}(f) \;\middle|\; \left\{\frac{g_{\mu^{-1}(1)}(r_{\mu(1)})}{p}\right\} \le \cdots \le \left\{\frac{g_{\mu^{-1}(n)}(r_{\mu(1)})}{p}\right\} \right\} \end{aligned} \tag{3}$$

is finite. For which kind of polynomials $g_i(x)$, does the density of the above set of primes in (3) exist? If polynomials $g_i(x_1,\dots,x_n) \in \mathbb{Q}[x_1,\dots,x_n]$ are linear, then the density

$$\left\{ p \in \mathrm{Spl}(f) \;\middle|\; \left\{\frac{g_1(r_1,\dots,r_n)}{p}\right\} \le \cdots \le \left\{\frac{g_n(r_1,\dots,r_n)}{p}\right\} \right\}$$

may be described by the volume of the domain defined by linear inequalities for polynomials $g_i(x_1,\dots,x_n)$ by Conjecture 1.2.

For a monic irreducible integral polynomial $F(x)$ and integral polynomials $g_1(x),\dots,g_n(x)$ in general, there seems to be the limit

$$\lim_{X\to\infty} \frac{\#\left\{ p \in \mathrm{Spl}_X(F) \;\middle|\; \begin{array}{l} \{\frac{g_1(r)}{p}\} \le \cdots \le \{\frac{g_n(r)}{p}\} \text{ for some integer} \\ \text{root } r \text{ of } F(x) \equiv 0 \bmod p \end{array} \right\}}{\#\mathrm{Spl}_X(F)}.$$

The rest of the paper is devoted to observations related to this question.

2. Case of a polynomial without non-trivial linear relations among roots

In this section, for a monic integral polynomial $f(x)$ of degree $\tilde{n} > 1$ without non-trivial linear relations among roots, i.e., $t := \dim LR = 1$ and (not necessarily monic) integral polynomials $g_1(x), g_2(x)$, we study the density

$$\lim_{X\to\infty} \frac{\#\{p \in \mathrm{Spl}_X(f) \mid \{\frac{g_1(r)}{p}\} < \{\frac{g_2(r)}{p}\} \text{ for } {}^{\exists}r \text{ s.t. } f(r) \equiv 0 \bmod p\}}{\#\mathrm{Spl}_X(f)},$$

where $\{\frac{g_i(r)}{p}\}$ denotes the decimal part of $\frac{g_i(r)}{p}$ as before. Although we get several interesting observations, they seem not to be easy to prove.

Let us consider the simplest case, that is let $f(x)$ be as before and $g_1(x) = mx, g_2(x) = nx$ for distinct non-zero integers m, n. We see that

$$\#\left\{p \in \mathrm{Spl}_X(f) \mid \left\{\frac{mr}{p}\right\} < \left\{\frac{nr}{p}\right\} \text{ for } {}^{\exists}r \in \mathbb{Z} \text{ s.t. } f(r) \equiv 0 \bmod p\right\}$$

$$= \#\mathrm{Spl}_X(f) - \#\left\{p \in \mathrm{Spl}_X(f) \mid \left\{\frac{nr}{p}\right\} \le \left\{\frac{mr}{p}\right\} \text{ for } {}^{\forall}r \text{ s.t. } f(r) \equiv 0 \bmod p\right\},$$

hence

$$\begin{aligned} d_{m,n} &:= \lim_{X\to\infty} \frac{\#\{p \in \mathrm{Spl}_X(f) \mid \{\frac{mr}{p}\} < \{\frac{nr}{p}\} \text{ for } {}^{\exists}r \text{ s.t. } f(r) \equiv 0 \bmod p\}}{\#\mathrm{Spl}_X(f)} \\ &= 1 - \lim_{X\to\infty} \frac{\#\{p \in \mathrm{Spl}_X(f) \mid \{\frac{nr}{p}\} < \{\frac{mr}{p}\} \text{ for } {}^{\forall}r \text{ s.t. } f(r) \equiv 0 \bmod p\}}{\#\mathrm{Spl}_X(f)} \\ &= 1 - \frac{\mathrm{vol}(I_{n,m}^{\tilde{n}} \cap \hat{\mathfrak{D}}_{\tilde{n}})}{\mathrm{vol}(\hat{\mathfrak{D}}_{\tilde{n}})} \quad \text{(under Conjecture 1.2)}, \end{aligned}$$

since the number of the prime p satisfying $\left\{\frac{nr}{p}\right\} = \left\{\frac{mr}{p}\right\}$ is finite and we write

$$I_{n,m} := \big\{x \in (0,1) \mid \{nx\} < \{mx\}\big\}.$$

Let us evaluate the ratio of volumes. Note that the dimension $\dim I_{n,m}^{\tilde{n}} \cap \hat{\mathfrak{D}}_{\tilde{n}}$ is less than or equal to $\tilde{n}-1$ and the volume is considered as the $(\tilde{n}-1)$-dimensional set under the assumption $\dim LR = 1$. We know

$$\mathrm{vol}(\hat{\mathfrak{D}}_{\tilde{n}}) = \frac{\sqrt{\tilde{n}}}{\tilde{n}!}.$$

On the other hand, we see that

$$\Big\{(x_1,\dots,x_{\tilde n}) \mid 0 \le x_i \le 1, x_i \in I_{n,m}\,({}^\forall i), \sum x_i \in \mathbb{Z}\Big\} = \bigcup_{\sigma\in S_{\tilde n}} \Big\{(x_1,\dots,x_{\tilde n}) \mid 0 \le x_{\sigma(1)} \le \dots \cdots \le x_{\sigma(\tilde n)} \le 1, x_i \in I_{n,m}\,({}^\forall i), \sum x_i \in \mathbb{Z}\Big\},$$

and the permutation induces the orthogonal transformation on $\mathbb{R}^{\tilde n}$, and the dimension of the intersection of the subsets corresponding to distinct permutation is less than $\tilde n - 1$, hence we see

$$\mathrm{vol}(I_{n,m}^{\tilde n} \cap \hat{\mathfrak{D}}_{\tilde n}) = \frac{1}{\tilde n!}\,\mathrm{vol}\left(\Big\{(x_1,\dots,x_{\tilde n}) \in (0,1)^{\tilde n} \mid x_i \in I_{n,m}, \sum x_i \in \mathbb{Z}\Big\}\right),$$

hence

$$\frac{\mathrm{vol}(I_{n,m}^{\tilde n} \cap \hat{\mathfrak{D}}_{\tilde n})}{\mathrm{vol}(\hat{\mathfrak{D}}_{\tilde n})} = \frac{1}{\sqrt{\tilde n}}\,\mathrm{vol}\left(\Big\{(x_1,\dots,x_{\tilde n}) \in (0,1)^{\tilde n} \mid x_i \in I_{n,m}, \sum x_i \in \mathbb{Z}\Big\}\right). \quad (4)$$

In the rest of this section we will show the following :

Theorem 2.1. *For integers M, N satisfying*

$$0 < N < M \quad \text{and} \quad (M,N) = 1,$$

we have

$$\frac{\mathrm{vol}(I_{N,M}^{\tilde n} \cap \hat{\mathfrak{D}}_{\tilde n})}{\mathrm{vol}(\hat{\mathfrak{D}}_{\tilde n})} = \frac{1}{2^{\tilde n}} - \frac{B_{\tilde n}(0)}{\tilde n!(MN(M-N))^{\tilde n}} \times \big\{3\big(MN(M-N)\big)^{\tilde n} + M^{2\tilde n} + N^{2\tilde n} + (M-N)^{2\tilde n} - 2\big((M-N)N\big)^{\tilde n} - 2M^{\tilde n}\big((M-N)^{\tilde n} + N^{\tilde n}\big)\big\},$$

where $B_{\tilde n}(x)$ is the Bernoulli polynomial.

The above matches computer experiment. We note that

(i) the ratio of volumes is independent of M, N for odd $\tilde n > 1$, since $B_{\tilde n}(0) = 0$ for odd $\tilde n > 1$.

(ii) Let $f(x)$ be quadratic; then the above shows $\frac{\mathrm{vol}(I_{N,M}^2 \cap \hat{\mathfrak{D}}_2)}{\mathrm{vol}(\hat{\mathfrak{D}}_2)} = 0$. As a matter of fact, we can show that sets $I_{N,M}^2 \cap \hat{\mathfrak{D}}_2$ and

$$\left\{p \in \mathrm{Spl}_X(f) \mid \left\{\frac{nr}{p}\right\} < \left\{\frac{mr}{p}\right\} \text{ for } {}^\forall r \text{ s.t. } f(r) \equiv 0 \bmod p\right\}$$

are finite sets, that is $d_{m,n} = 1$ for an irreducible quadratic polynomial $f(x)$.

2.1. Bernoulli polynomial

In this subsection, let us recall several facts on Bernoulli polynomials. For non-negative integer m, we write

$$\Delta_m\big(f(x)\big) := \left.\frac{d^m f(x)}{dx^m}\right|_{x=0},$$

for example,

$$\Delta_m(e^{rx}) = r^m.$$

We define Bernoulli polynomials $B_n(t)$ by

$$\sum_{n=0}^{\infty} B_n(t)\frac{x^n}{n!} := \frac{xe^{tx}}{e^x-1} = \left(\sum_{k=0}^{\infty}\frac{B_k(0)}{k!}x^k\right)\left(\sum_{m=0}^{\infty}\frac{(tx)^m}{m!}\right),$$

that is

$$\Delta_n\left(\frac{xe^{tx}}{e^x-1}\right) = B_n(t) = \sum_{i=0}^{n}\binom{n}{i}B_{n-i}(0)t^i,$$

$$B_m(0) = \Delta_m\left(\frac{x}{e^x-1}\right).$$

In this paper, the notation B_n denotes the Bernoulli polynomial, and so we use the notation $B_n(0)$ for the Bernoulli number.

We see that, for a real number a and a non-negative integer m

$$\begin{aligned}
&\frac{1}{m+1}\big(B_{m+1}(a+1) - B_{m+1}(a)\big)\\
&= \frac{1}{m+1}\left(\Delta_{m+1}\left(\frac{xe^{(a+1)x}}{e^x-1}\right) - \Delta_{m+1}\left(\frac{xe^{ax}}{e^x-1}\right)\right)\\
&= \frac{\Delta_{m+1}(xe^{ax})}{m+1} = a^m,
\end{aligned}$$

hence for integers $n, m \geq 0$,

$$\sum_{l=0}^{n}(a+l)^m = \frac{1}{m+1}\big(B_{m+1}(a+n+1) - B_{m+1}(a)\big).$$

Therefore, for a positive real number a and a positive integer $n > 1$, we see that

$$\begin{aligned}
\sum_{l\geq 0}\max(0, a-l)^{n-1} &= \sum_{0\leq l\leq \lfloor a\rfloor}(a-l)^{n-1} = \sum_{0\leq l\leq \lfloor a\rfloor}(\{a\} + \lfloor a\rfloor - l)^{n-1}\\
&= \frac{1}{n}\big(B_n(\{a\} + \lfloor a\rfloor + 1) - B_n(\{a\})\big)\\
&= \frac{1}{n}\big(B_n(a+1) - B_n(\{a\})\big), \qquad (5)
\end{aligned}$$

which we need to prove the theorem.

2.2. Proof of Theorem 2.1

It is convenient to introduce the notation $\risingdotseq$: For sets S, T, we write $S \risingdotseq T$ if and only if $\#(S \setminus T) + \#(T \setminus S) < \infty$.

Proposition 2.2. *Let n, m be non-zero distinct integers, and write $n = dN$, $m = dM$ for $d := (n, m)$. Then we see that*

$$I_{n,m} \risingdotseq \cup_{k=0}^{d-1} \left\{ \frac{k+\epsilon}{d} \,\middle|\, \epsilon \in I_{N,M} \right\}, \tag{6}$$

and under the assumptions $M > N > 0$ and $(M, N) = 1$

$$I_{N,M} \risingdotseq \cup_{K=1}^{M-1} \begin{cases} \left(\frac{1}{M}(K - \frac{L-M}{N}), \frac{K}{M}\right) & \text{if } L > M, \\ \left(\frac{1}{M}(K - \frac{M-L}{M-N}), \frac{K}{M}\right) & \text{if } L < M, \end{cases} \tag{7}$$

where the integer L is defined by

$$L \equiv NK \bmod M, N \le L \le M + N - 1.$$

Proof. The condition $x \in I_{n,m}$ means $\{nx\} < \{mx\}$, i.e., $\{dNx\} < \{dMx\}$, hence $\{dx\} \in I_{N,M}$. We have only to write $dx = k + \{dx\}$ for an integer k for the proof of (6). Let us show the equation (7). Take a number $x \in I_{N,M}$, which implies $Mx \notin \mathbb{Z}$ and write $x = \frac{K-\epsilon}{M}$ $(1 \le K \le M, K \in \mathbb{Z}, 0 < \epsilon < 1)$. We note that the condition $K = M$ is equivalent to $L = M$ by the definition of L and the assumption $M > N, (M, N) = 1$. Then it is easy to see that

$$\{Mx\} = 1 - \epsilon \quad \text{and} \quad \{Nx\} = \left\{\frac{NK - N\epsilon}{M}\right\} = \left\{\frac{L - N\epsilon}{M}\right\}.$$

The inequalities $0 < L - N\epsilon < 2M$ show that $\{Nx\} = \frac{L-N\epsilon}{M}$ or $\frac{L-N\epsilon}{M} - 1$ according to $L - N\epsilon < M$ or $L - N\epsilon \ge M$. Let us note that

(i) the inequality $\frac{L-M}{N} < \frac{2M-L}{M-N}$ follows from the assumption $L < M + N$,

(ii) $\frac{L-N\epsilon}{M} - 1 < 1 - \epsilon \Leftrightarrow \epsilon < \frac{2M-L}{M-N}$, and

(iii) $\frac{L-N\epsilon}{M} < 1 - \epsilon \Leftrightarrow \epsilon < \frac{M-L}{M-N}$.

First, suppose $L < M$: By $0 < L - N\epsilon < M$, we have $\{Nx\} = \frac{L-N\epsilon}{M}$, hence $\{Nx\} < \{Mx\} \Leftrightarrow \frac{L-N\epsilon}{M} < 1 - \epsilon \Leftrightarrow 0 < \epsilon < \frac{M-L}{M-N}$ by (iii). Next, suppose $L \ge M$: Under the supposition $\{Nx\} < \{Mx\}$, the condition $L - N\epsilon < M$ implies $\{Mx\} = 1 - \epsilon > \{Nx\} = \frac{L-N\epsilon}{M}$, which is equivalent to $(0 <)\, \epsilon < \frac{M-L}{M-N}$, which contradicts the assumption $L \ge M$. Hence the condition $\{Nx\} < \{Mx\}$ implies $L - N\epsilon \ge M$, i.e., $\epsilon \le \frac{L-M}{N}$. Conversely, suppose $\epsilon \le \frac{L-M}{N}$, which is equivalent to $L - N\epsilon \ge M$ and implies $\epsilon < \frac{2M-L}{M-N}$ by (i) , hence $\{Nx\} = \frac{L-N\epsilon}{M} - 1$, and the property (ii) imply $\{Nx\} < \{Mx\}$. If $K = M$ happens, then we have $L = M$ and the contradiction

$$\{Nx\} = \{\frac{M - N\epsilon}{M}\} = 1 - \frac{N}{M}\epsilon > 1 - \epsilon = \{Mx\}. \quad \square$$

Hereafter, we assume that integers M, N satisfy $M > N > 0$ and $(M, N) = 1$ as in Theorem 2.1.

We write, for an integer K

$$\tau(K) := \begin{cases} \frac{L-M}{N} & \text{if } L \geq M, \\ \frac{M-L}{M-N} & \text{if } L < M, \end{cases}$$

where L is the integer defined by $L \equiv NK \bmod M$, and $N \leq L \leq M + N - 1$. It is easy to see $\tau(0) = 0, \tau(1) = 1$ By Proposition 2.2, we have

$$I_{N,M} \doteq \cup_{K=1}^{M-1} S_{\tau(K)} \quad \text{with } S_{\tau(K)} := \left(\frac{K - \tau(K)}{M}, \frac{K}{M} \right). \tag{8}$$

Proposition 2.3. *The mapping τ is the bijection from $\{1, 2, \ldots, M-1\}$ to $\Sigma := \Sigma_1 \cup \Sigma_2$, where $\Sigma_1 := \left\{\frac{1}{N}, \ldots, \frac{N-1}{N}\right\}$, $\Sigma_2 := \left\{\frac{1}{M-N}, \ldots, \frac{M-N}{M-N}\right\}$ and $\tau(K) = K$ holds in the ring $\mathbb{Z}/M\mathbb{Z}$. The set Σ_1 is empty if $N = 1$. Moreover, we have*

$$K - \tau(K) = \begin{cases} \frac{MA_1}{N} & (1 \leq {}^\exists A_1 \leq N - 1) \quad \text{if } \tau(K) \in \Sigma_1, \\ \frac{MA_2}{M-N} & (0 \leq {}^\exists A_2 \leq M - N - 1) \quad \text{if } \tau(K) \in \Sigma_2, \end{cases}$$

and $K - \tau(K)$ $(K = 1, \ldots, M - 1)$ are distinct.

Proof. It is clear that the value $\tau(K)$ is in the set Σ and $\#\Sigma = M - 1$. Since $(M, M - N) = (M, N) = 1$, we see that $\tau(K) = \frac{L}{N} = K$ in $\mathbb{Z}/M\mathbb{Z}$, which implies the injectivity of τ. Write $NK = L + aM$ $(a \in \mathbb{Z})$. Suppose that $L > M$; it implies $K - \tau(K) = \frac{M}{N}(a + 1)$, and from inequalities $N \leq L \leq M + N - 1$ follows

$$\frac{N(K-1)}{M} - 1 + \frac{1}{M} \leq a \leq \frac{K-1}{M} N,$$

hence $-1 < a < N$. If $a = N - 1$ occurs, then $L = NK - (N - 1)M$ holds and then the assumption $L > M$ implies $NK > NM$, which contradicts $K \leq M - 1$. Next, suppose that $L < M$; then we see $K - \tau(K) = \frac{M}{M-N}(K - 1 - a)$ and inequalities $N \leq L \leq M + N - 1$ imply

$$K - \frac{N}{M}(K-1) - 1 \leq K - 1 - a \leq \left(1 - \frac{N}{M}\right) K + \frac{N-1}{M},$$

hence

$$\begin{aligned}0 \le K-1-a &\le \left(1-\frac{N}{M}\right)(M-1)+\frac{N-1}{M}\\ &< M-N-1+2\frac{N}{M}-\frac{1}{M} < M-N+1.\end{aligned}$$

If $K-1-a=M-N$ occurs, then the assumption $L<M$ implies $NK-aM<M$, hence

$$K-M+N=a+1>\frac{NK}{M},$$

i.e., $(M-N)K>(M-N)M$, which is the contradiction. Next, assume that

$$K_1-\tau(K_1)=K_2-\tau(K_2) \quad \text{for } 1\le K_1<K_2\le M-1;$$

it implies the contradiction $1 \le K_2-K_1=\tau(K_2)-\tau(K_1)<1$. □

When we change the domain of the mapping τ from $\{1,\dots,M-1\}$ to $\{0,1,\dots,M-1\}$, the set $\{0,1,\dots,M-1\}$ corresponds, through $K\to K-\tau(K)$ to $\Sigma' := \Sigma'_1 \sqcup \Sigma'_2$ for

$$\Sigma'_1:=\left\{\frac{MA_1}{N} \mid 0\le A_1\le N-1\right\}, \quad \Sigma'_2:=\left\{\frac{MA_2}{M-N} \mid 0\le A_2\le M-N-1\right\},$$

where $K=0,1$ are supposed to correspond to $0\in\Sigma'_1, 0\in\Sigma'_2$, respectively. Now we see that

$$\begin{aligned}&\mathrm{vol}\left(\left\{(x_1,\dots,x_{\tilde n})\in(0,1)^{\tilde n} \mid x_i\in I_{N,M}, \sum x_i\in\mathbb{Z}\right\}\right)\\ &=\sum_{K_1,\dots,K_{\tilde n}=1}^{M-1}\mathrm{vol}\left(\left\{(x_1,\dots,x_{\tilde n})\in(0,1)^{\tilde n} \mid x_i\in S_{\tau(K_i)}, \sum x_i\in\mathbb{Z}\right\}\right)\end{aligned}$$

writing $x_i=\frac{K_i-\epsilon_i}{M}$ $\big(0<\epsilon_i<\tau(K_i)\big)$

$$=\frac{1}{M^{\tilde n-1}}\sum_{\substack{K_i=1\\(1\le i\le\tilde n)}}^{M-1}\mathrm{vol}\left(\left\{(\epsilon_1,\dots,\epsilon_{\tilde n})\in(0,1)^{\tilde n}\;\middle|\;\begin{array}{l}0<\epsilon_i<\tau(K_i),\sum\epsilon_i\in\mathbb{Z},\\ \sum\epsilon_i\equiv\sum K_i \bmod M\end{array}\right\}\right). \tag{9}$$

Let us begin the evaluation of the volume. Write $\tilde M(x):=\max(0,x)$ for simplicity.

Lemma 2.4. *Let a,b,m be real numbers and suppose $a\le b$ and $m\ne -1$. Then we have*

$$\int_a^b \tilde M(t-w)^m dw=\frac{1}{m+1}\left(\tilde M(t-a)^{m+1}-\tilde M(t-b)^{m+1}\right). \tag{10}$$

P r o o f. By writing $t-w=W$, the left hand is equal to

$$\begin{aligned}\int_{t-a}^{t-b}\tilde{M}(W)^m(-dW) &= -\left(\int_{-\infty}^{t-b}\tilde{M}(W)^m dW - \int_{-\infty}^{t-a}\tilde{M}(W)^m dW\right)\\ &= \int_0^{t-a}\tilde{M}(W)^m dW - \int_0^{t-b}\tilde{M}(W)^m dW\\ &= \frac{1}{m+1}\left(\tilde{M}(t-a)^{m+1} - \tilde{M}(t-b)^{m+1}\right). \qquad \square\end{aligned}$$

Here we introduce the notation, for $x, \tau_1, \ldots, \tau_n \in \mathbb{R}$

$$\begin{aligned}W_l(x;\tau_1,\ldots,\tau_n) &:= \sum_{0\le k\le n}\ \sum_{1\le i_1<\cdots<i_k\le n}(-1)^k\tilde{M}(x-\tau_{i_1}-\cdots-\tau_{i_k})^l\\ &= \sum_S(-1)^{|S|}\tilde{M}\left(x-\sum_{i\in S}\tau_i\right)^l,\end{aligned}$$

where S runs over all 2^n subsets of $\{1,\ldots,n\}$ and $|S|=\#S$. It is obvious that

$$W_l(x;\tau_1,\ldots,\tau_n) = W_l(x;\tau_{\sigma(1)},\ldots,\tau_{\sigma(n)})$$

for any permutation σ. Moreover, we see

$$W_l(x;\tau_1,\ldots,\tau_n) = W_l(x;\tau_1,\ldots,\tau_{n-1}) - W_l(x-\tau_n;\tau_1,\ldots,\tau_{n-1}). \tag{11}$$

In particular, the equation (11) says that

$$W_l(x;\tau_1,\ldots,\tau_n) = 0 \quad \text{if } {}^\exists\tau_i = 0. \tag{12}$$

Proposition 2.5. *For positive numbers $\tau_1,\ldots,\tau_n$, the volume of the set*

$$V_n(x;\tau_1,\ldots,\tau_n) := \left\{(x_1,\ldots,x_n) \mid 0\le x_i\le\tau_i, \sum_{i=1}^n x_i\le x\right\}$$

is

$$\frac{1}{n!}W_n(x;\tau_1,\ldots,\tau_n). \tag{13}$$

P r o o f. We use the induction on n. Write

$$U_n(x) = \mathrm{vol}\big(V_n(x;\tau_1,\ldots,\tau_n)\big)$$

simply. For $n=1$, it is easy to see that

$$U_1(x) = \tilde{M}(x) - \tilde{M}(x-\tau_1) = \frac{1}{1!}W_1(x;\tau_1).$$

Supposing (13), we see that $U_{n+1}(x)$ is

$$\int_{x_{n+1}=0}^{\tau_{n+1}} \cdots \int_{\substack{x_1=0,\\ \sum x_i \le x}}^{\tau_1} 1\, dx_1 \ldots dx_{n+1} = \int_{x_{n+1}=0}^{\tau_{n+1}} U_n(x - x_{n+1}) dx_{n+1}$$

$$= \int_{x_{n+1}=0}^{\tau_{n+1}} \frac{1}{n!} \sum_{k=0}^{n} (-1)^k \left\{ \sum_{1 \le i_1 < \cdots < i_k \le n} \tilde{M}(x - x_{n+1} - \tau_{i_1} - \cdots - \tau_{i_k})^n \right\} dx_{n+1}$$

$$= \frac{1}{(n+1)!} \sum_{k=0}^{n} (-1)^k \sum_{1 \le i_1 < \cdots < i_k \le n} \Big\{ \tilde{M}(x - \tau_{i_1} - \cdots - \tau_{i_k})^{n+1}$$
$$- \tilde{M}(x - \tau_{i_1} - \cdots - \tau_{i_k} - \tau_{n+1})^{n+1} \Big\}$$

$$= \frac{1}{(n+1)!} \sum_{k=0}^{n} (-1)^k \left\{ \sum_{1 \le i_1 < \cdots < i_k \le n} \tilde{M}(x - \tau_{i_1} - \cdots - \tau_{i_k})^{n+1} \right\}$$
$$+ \frac{1}{(n+1)!} \sum_{j=1}^{n+1} (-1)^j \left\{ \sum_{1 \le i_1 < \cdots < i_j = n+1} \tilde{M}(x - \tau_{i_1} - \cdots - \tau_{i_j})^{n+1} \right\} = U_{n+1}(x).$$

□

Example. It is easy to check, by drawing the figure

$$\mathrm{vol}\big(V_2(x; \tau_1, \tau_2)\big)$$
$$= \frac{1}{2} \big\{ \tilde{M}(x)^2 - \tilde{M}(x - \tau_1)^2 - \tilde{M}(x - \tau_2)^2 + \tilde{M}(x - \tau_1 - \tau_2)^2 \big\}.$$

We note that the proposition implies the following equation :

$$\sum_{S} (-1)^{|S|} (c - \sum_{i \in S} \tau_i)^l = \begin{cases} 0 & \text{if} \quad 0 \le l \le n-1, \\ n! \prod_i \tau_i & \text{if} \quad l = n, \end{cases}$$

where $\tau_1, \ldots, \tau_n$ and c are variables and S runs over all 2^n subsets of $\{1, \ldots, n\}$.

Proposition 2.6. *For positive numbers $\tau_1, \ldots, \tau_n$, the $n-1$-dimensional volume of the set*

$$S_n(x; \tau_1, \ldots, \tau_n) := \left\{ (x_1, \ldots, x_n) \mid 0 \le x_i \le \tau_i, \sum_{i=1}^{n} x_i = x \right\} \tag{14}$$

is

$$\frac{\sqrt{n}}{(n-1)!} W_{n-1}(x; \tau_1, \ldots, \tau_n). \tag{15}$$

P r o o f. Using orthnormal basis

$$\begin{aligned}
\boldsymbol{f}_1 &:= \frac{1}{\sqrt{1+1^2}}(1,-1,0,\dots,0),\\
&\ \vdots\\
\boldsymbol{f}_k &:= \frac{1}{\sqrt{k+k^2}}\bigl(1,\dots,1,-k,0,\dots,0\bigr),\\
&\ \vdots\\
\boldsymbol{f}_{n-1} &:= \frac{1}{\sqrt{(n-1)+(n-1)^2}}\bigl(1,\dots,1,-(n-1)\bigr),\\
\boldsymbol{f}_n &:= \frac{1}{\sqrt{n}}(1,\dots,1),
\end{aligned}$$

and the transformation

$$(y_1,\dots,y_n) = (x_1,\dots,x_n)({}^t\boldsymbol{f}_1,\dots,{}^t\boldsymbol{f}_n),$$

that is,

$$\sqrt{n}y_n = x_1+\cdots+x_n,$$

we see, denoting $S_n(x;\tau_1,\dots,\tau_n)$ by $S_n(x)$ simply

$$\operatorname{vol}\bigl(V_n(x;\tau_1,\dots,\tau_n)\bigr) = \int_{\boldsymbol{x}\in V_n(x)} 1\,d\boldsymbol{x} = \int_{\sqrt{n}y_n\le x} \operatorname{vol}\bigl(S_n(\sqrt{n}y_n)\bigr)dy_n,$$

hence $U_n'(x) = \sqrt{n}^{-1}\operatorname{vol}\bigl(S_n(x)\bigr)$, i.e., $\operatorname{vol}\bigl(S_n(x)\bigr) = \sqrt{n}\,U_n'(x)$. □

EXAMPLE. The length of $S_2(x;\tau_1,\tau_2)$ is easily checked to be

$$\sqrt{2}\{\tilde{M}(x) - \tilde{M}(x-\tau_1) - \tilde{M}(x-\tau_2) + \tilde{M}(x-\tau_1-\tau_2)\} = \sqrt{2}U_2'(x).$$

We note that the volume of $S_n(x;\tau_1,\dots,\tau_n)$ is positive if and only if $0 < x < \sum\tau_i$ holds, and that $\operatorname{vol}\bigl(S_n(x;\tau_1,\dots,\tau_n)\bigr) = \operatorname{vol}\bigl(S_n(x;\tau_{\sigma(1)},\dots,\tau_{\sigma(n)})\bigr)$ for every permutation $\sigma\in S_n$, since a permutation induces the orthogonal transformation. In particular, for positive numbers $\tau_1,\dots,\tau_n$ and a real number x, $W_{n-1}(x;\tau_1,\dots,\tau_n) > 0$ if and only if $0 < x < \sum\tau_i$ holds.

Now we see that, using (4), (9)

$$\begin{aligned}
&\frac{\mathrm{vol}(I_{N,M}^{\tilde n}\cap\hat{\mathfrak{D}}_{\tilde n})}{\mathrm{vol}(\hat{\mathfrak{D}}_{\tilde n})}\\
&=\frac{1}{\sqrt{\tilde n}}\,\mathrm{vol}\left(\left\{(x_1,\dots,x_{\tilde n})\in(0,1)^{\tilde n}\mid x_i\in I_{N,M},\sum x_i\in\mathbb{Z}\right\}\right)\\
&=\frac{1}{\sqrt{\tilde n}M^{\tilde n-1}}\sum_{1\le K_1,\dots,K_{\tilde n}<M}\sum_{l\in\mathbb{Z}}\mathrm{vol}\left(S_{\tilde n}\left(\sum K_i-Ml;\tau_1,\dots,\tau_{\tilde n}\right)\right)\\
&=\frac{1}{(\tilde n-1)!M^{\tilde n-1}}\sum_{1\le K_1,\dots,K_{\tilde n}<M}\sum_{l\in\mathbb{Z}}W_{\tilde n-1}\Big(\sum K_i-Ml;\tau_1,\dots,\tau_{\tilde n}\Big),
\end{aligned}$$

where $\tau_j=\tau(K_j)$, and note that

$$W_{\tilde n-1}\Big(\sum K_i-Ml;\tau_1,\dots,\tau_{\tilde n}\Big)>0\Leftrightarrow 0<\sum K_i-Ml<\sum\tau_i\,,$$

which implies $0\le l\le\tilde n$, and continuing the above

$$=\frac{1}{(\tilde n-1)!M^{\tilde n-1}}\sum_{0\le K_1,\dots,K_{\tilde n}<M}\sum_{l=0}^{\tilde n}W_{\tilde n-1}\left(\sum K_i-Ml;\tau_1,\dots,\tau_{\tilde n}\right)$$

by $\tau(0)=0$ and (12)

$$=\frac{1}{(\tilde n-1)!M^{\tilde n-1}}\sum_{0\le K_1,\dots,K_{\tilde n}<M}\sum_{l=0}^{\tilde n}\sum_{S}(-1)^{|S|}\tilde M\left(\sum K_i-Ml-\sum_{i\in S}\tau_i\right)^{\tilde n-1},$$

where S runs over all subsets of $\{1,\dots,\tilde n\}$. Thus we see that

$$\begin{aligned}
&(\tilde n-1)!M^{\tilde n-1}\frac{\mathrm{vol}(I_{N,M}^{\tilde n}\cap\hat{\mathfrak{D}}_{\tilde n})}{\mathrm{vol}(\hat{\mathfrak{D}}_{\tilde n})}\\
&=\sum_{S}(-1)^{|S|}\sum_{\substack{0\le K_i\le M-1\\(1\le i\le\tilde n)}}\sum_{l=0}^{\tilde n}\tilde M\left(\sum_{i\notin S}K_i+\sum_{j\in S}(K_j-\tau_j)-Ml\right)^{\tilde n-1},
\end{aligned}$$

where $K_j-\tau_j$ runs over $\Sigma':=\Sigma_1'\sqcup\Sigma_2'$ as stated after Proposition 2.3 and continuing

$$= \sum_{k=0}^{\tilde{n}} (-1)^k \binom{\tilde{n}}{k} \sum_{\substack{0 \le K_i \le M-1 (i>k), \\ \tau'_j \in \Sigma' (j \le k)}} \sum_{l=0}^{\tilde{n}} \tilde{M} \left(\sum_{i>k} K_i + \sum_{j \le k} \tau'_j - Ml \right)^{\tilde{n}-1}$$

$$= M^{\tilde{n}-1} \sum_{k=0}^{\tilde{n}} (-1)^k \binom{\tilde{n}}{k} \sum_{\substack{0 \le K_i \le M-1 (i>k), \\ \tau'_j \in \Sigma' (j \le k)}} \sum_{l=0}^{\tilde{n}} \tilde{M} \left(\frac{\sum_{i>k} K_i + \sum_{j \le k} \tau'_j}{M} - l \right)^{\tilde{n}-1}$$

$$= \frac{M^{\tilde{n}-1}}{\tilde{n}} \sum_{k=0}^{\tilde{n}} (-1)^k \binom{\tilde{n}}{k} \sum_{\substack{0 \le K_i \le M-1 (i>k), \\ \tau'_j \in \Sigma' (j \le k)}}$$

$$\left(B_{\tilde{n}} \left(\frac{\sum_{i>k} K_i + \sum_{j \le k} \tau'_j}{M} + 1 \right) - B_{\tilde{n}} \left(\left\{ \frac{\sum_{i>k} K_i + \sum_{j \le k} \tau'_j}{M} \right\} \right) \right),$$

by (5). For an integer k $(0 \le k \le \tilde{n})$, we see that

$$T_{1,k} := \sum_{\substack{0 \le K_i \le M-1 (i>k), \\ \tau'_j \in \Sigma' (j \le k)}} B_{\tilde{n}} \left(\frac{\sum_{i>k} K_i + \sum_{j \le k} \tau'_j}{M} + 1 \right)$$

$$= \sum_{\substack{0 \le K_i \le M-1 (i>k), \\ \tau'_j \in \Sigma' (j \le k)}} \Delta_{\tilde{n}} \left(\frac{x}{e^x - 1} e^{\left(\frac{\sum_{i>k} K_i + \sum_{j \le k} \tau'_j}{M} + 1 \right) x} \right)$$

$$= \Delta_{\tilde{n}} \left(\frac{xe^x}{e^x - 1} \cdot \left(\sum_{0 \le K \le M-1} e^{\frac{K}{M} x} \right)^{\tilde{n}-k} \cdot \left(\sum_{\tau' \in \Sigma'} e^{\frac{\tau'}{M} x} \right)^k \right).$$

Noting

$$\sum_{0 \le K \le M-1} e^{\frac{K}{M} x} = \frac{e^x - 1}{e^{\frac{x}{M}} - 1}$$

and

$$\sum_{\tau' \in \Sigma'} e^{\frac{\tau'}{M} x} = \sum_{A_1=0}^{N-1} e^{\frac{A_1}{N} x} + \sum_{A_2=0}^{M-N-1} e^{\frac{A_2}{M-N} x} = \frac{e^x - 1}{e^{\frac{x}{N}} - 1} + \frac{e^x - 1}{e^{\frac{x}{M-N}} - 1},$$

we see that

$$T_{1,k} = \Delta_{\tilde{n}} \left(\frac{xe^x}{e^x - 1} \cdot \left(\frac{e^x - 1}{e^{\frac{x}{M}} - 1} \right)^{\tilde{n}-k} \cdot \left(\frac{e^x - 1}{e^{\frac{x}{N}} - 1} + \frac{e^x - 1}{e^{\frac{x}{M-N}} - 1} \right)^k \right),$$

and so

$$\begin{aligned}
&\sum_{k=0}^{\tilde{n}}(-1)^k\binom{\tilde{n}}{k}T_{1,k}\\
&=\Delta_{\tilde{n}}\left(\frac{xe^x}{e^x-1}\sum_{k=0}^{\tilde{n}}(-1)^k\binom{\tilde{n}}{k}\cdot\left(\frac{e^x-1}{e^{\frac{x}{M}}-1}\right)^{\tilde{n}-k}\cdot\left(\frac{e^x-1}{e^{\frac{x}{N}}-1}+\frac{e^x-1}{e^{\frac{x}{M-N}}-1}\right)^k\right)\\
&=\Delta_{\tilde{n}}\left(\frac{xe^x}{e^x-1}\left(\frac{e^x-1}{e^{\frac{x}{M}}-1}-\frac{e^x-1}{e^{\frac{x}{N}}-1}-\frac{e^x-1}{e^{\frac{x}{M-N}}-1}\right)^{\tilde{n}}\right)=\Delta_{\tilde{n}}\left(f(x)g(x)^{\tilde{n}}\right),
\end{aligned}$$

where

$$f(x):=\frac{xe^x}{e^x-1},\qquad g(x):=\frac{e^x-1}{e^{\frac{x}{M}}-1}-\frac{e^x-1}{e^{\frac{x}{N}}-1}-\frac{e^x-1}{e^{\frac{x}{M-N}}-1}.$$

We see that

$$\Delta_0(f)=f(0)=1,\qquad \Delta_0(g)=g(0)=0,\qquad \Delta_1(g)=\frac{1}{2},$$

and

$$\begin{aligned}
\Delta_{\tilde{n}}(fg^{\tilde{n}})&=\sum_{\substack{k_1+\cdots+k_{\tilde{n}+1}=\tilde{n},\\ \forall k_i\geq 0}}\frac{\tilde{n}!}{k_1!\ldots k_{\tilde{n}+1}!}\Delta_{k_1}(f)\Delta_{k_2}(g)\ldots\Delta_{k_{\tilde{n}+1}}(g)\\
&=\tilde{n}!\,\Delta_1(g)^{\tilde{n}}=\frac{\tilde{n}!}{2^{\tilde{n}}},
\end{aligned}$$

thus

$$\sum_{k=0}^{\tilde{n}}(-1)^k\binom{\tilde{n}}{k}T_{1,k}=\frac{\tilde{n}!}{2^{\tilde{n}}}.$$

Next, for an integer k ($0\leq k\leq\tilde{n}$), let us evaluate

$$T_{2,k}:=\sum_{\substack{0\leq K_i\leq M-1\,(i>k),\\ \tau'_j\in\Sigma'(j\leq k)}}B_{\tilde{n}}\left(\left\{\frac{\sum_{i>k}K_i+\sum_{j\leq k}\tau'_j}{M}\right\}\right),$$

where $\frac{\tau'_j}{M}$ runs over the set $\Sigma'':=\Sigma''_1\sqcup\Sigma''_2$ for

$$\Sigma''_1:=\left\{\frac{A_1}{N}\mid 0\leq A_1\leq N-1\right\},\qquad \Sigma''_2:=\left\{\frac{A_2}{M-N}\mid 0\leq A_2\leq M-N-1\right\}.$$

First of all, we note that, for positive integers d,d_1,d_2 with $(d_1,d_2)=1$

$$\sum_{j=0}^{d-1}B_{\tilde{n}}\left(\frac{j}{d}\right)=\frac{B_{\tilde{n}}(0)}{d^{\tilde{n}-1}},\qquad \sum_{\substack{0\leq j_i\leq d_i-1,\\ (i=1,2)}}B_{\tilde{n}}\left(\left\{\frac{j_1}{d_1}+\frac{j_2}{d_2}\right\}\right)=\frac{B_{\tilde{n}}(0)}{(d_1d_2)^{\tilde{n}-1}}. \tag{16}$$

Because,

$$\sum_{j=0}^{d-1} B_{\tilde{n}}\left(\frac{j}{d}\right) = \sum_{j=0}^{d-1} \Delta_{\tilde{n}}\left(\frac{xe^{\frac{jx}{d}}}{e^x-1}\right) = \Delta_{\tilde{n}}\left(\frac{x}{e^x-1}\sum_{j=0}^{d-1} e^{\frac{jx}{d}}\right)$$
$$= \Delta_{\tilde{n}}\left(\frac{x}{e^{\frac{x}{d}}-1}\right) = \Delta_{\tilde{n}}\left(d\sum_{k=0}^{\infty}\frac{B_k(0)}{k!}\left(\frac{x}{d}\right)^k\right) = \frac{B_{\tilde{n}}(0)}{d^{\tilde{n}-1}},$$

and

$$\sum_{\substack{0\le j_i\le d_i-1,\\(i=1,2)}} B_{\tilde{n}}\left(\left\{\frac{j_1}{d_1}+\frac{j_2}{d_2}\right\}\right) = \sum_{0\le j\le d_1d_2-1} B_{\tilde{n}}\left(\frac{j}{d_1d_2}\right).$$

We see that

$$T_{2,k} = \sum_{\substack{0\le K_i\le M-1\\(i>k)}} \sum_{l=0}^{k}\binom{k}{l} \sum_{\substack{\tau_i''\in\Sigma_1''(i\le l),\\ \tau_j''\in\Sigma_2''(l+1\le j\le k)}}$$
$$B_{\tilde{n}}\left(\left\{\frac{\sum_{i>k}K_i}{M} + \sum_{1\le i\le l}\tau_i'' + \sum_{l+1\le j\le k}\tau_j''\right\}\right)$$
$$= \sum_{\substack{0\le K_i\le M-1\\(i>k)}} \Bigg\{ \sum_{1\le a_2\le M-N} B_{\tilde{n}}\left(\left\{\frac{\sum_{i>k}K_i}{M} + \frac{a_2}{M-N}\right\}\right)$$
$$\times \#\Big\{(A_1,\ldots,A_k) \mid 1\le A_i\le M-N,\ \sum_i A_i \equiv a_2 \bmod M-N\Big\}$$
$$+ \sum_{l=1}^{k-1}\binom{k}{l} \sum_{\substack{1\le a_1\le N,\\ 1\le a_2\le M-N}} \Bigg\{ B_{\tilde{n}}\left(\left\{\frac{\sum_{i>k}K_i}{M} + \frac{a_1}{N} + \frac{a_2}{M-N}\right\}\right)$$
$$\times \#\Big\{(A_1,\ldots,A_l) \mid 1\le A_i\le N, \sum_i A_i \equiv a_1 \bmod N\Big\}$$
$$\times \#\Big\{(A_{l+1},\ldots,A_k) \mid 1\le A_i\le M-N, \sum A_i \equiv a_2 \bmod M-N\Big\}\Bigg\}$$
$$+ \sum_{1\le a_1\le N} B_{\tilde{n}}\left(\left\{\frac{\sum_{i>k}K_i}{M} + \frac{a_1}{N}\right\}\right)$$
$$\times \#\Big\{(A_1,\ldots,A_k) \mid 1\le A_i\le N, \sum A_i \equiv a_1 \bmod N\Big\}\Bigg\}$$

$$= \sum_{\substack{0\le K_i\le M-1\\(i>k)}} \left\{ \sum_{1\le a_2\le M-N} B_{\tilde{n}}\left(\left\{\frac{\sum_{i>k}K_i}{M}+\frac{a_2}{M-N}\right\}\right)(M-N)^{k-1} \right.$$

$$+\sum_{l=1}^{k-1}\binom{k}{l}\sum_{\substack{1\le a_1\le N,\\1\le a_2\le M-N}} B_{\tilde{n}}\left(\left\{\frac{\sum_{i>k}K_i}{M}+\frac{a_1}{N}+\frac{a_2}{M-N}\right\}\right)$$

$$\times N^{l-1}(M-N)^{k-l-1}$$

$$\left. +\sum_{1\le a_1\le N} B_{\tilde{n}}\left(\left\{\frac{\sum_{i>k}K_i}{M}+\frac{a_1}{N}\right\}\right)N^{k-1}\right\}.$$

Hence, we see that

$$T_{2,\tilde{n}} = \sum_{1\le a_2\le M-N} B_{\tilde{n}}\left(\left\{\frac{a_2}{M-N}\right\}\right)(M-N)^{\tilde{n}-1}$$

$$+\sum_{l=1}^{\tilde{n}-1}\binom{\tilde{n}}{l}\sum_{\substack{1\le a_1\le N,\\1\le a_2\le M-N}} B_{\tilde{n}}\left(\left\{\frac{a_1}{N}+\frac{a_2}{M-N}\right\}\right)N^{l-1}(M-N)^{\tilde{n}-l-1}$$

$$+\sum_{1\le a_1\le N} B_{\tilde{n}}\left(\left\{\frac{a_1}{N}\right\}\right)N^{\tilde{n}-1}$$

$$= B_{\tilde{n}}(0)+\sum_{l=1}^{\tilde{n}-1}\binom{\tilde{n}}{l}\frac{B_{\tilde{n}}(0)}{N^{\tilde{n}-l}(M-N)^l}+B_{\tilde{n}}(0)$$

$$=\left(2+\left(\frac{1}{N}+\frac{1}{M-N}\right)^{\tilde{n}}-\frac{1}{N^{\tilde{n}}}-\frac{1}{(M-N)^{\tilde{n}}}\right)B_{\tilde{n}}(0)$$

by (16) and for $1\le k<\tilde{n}$ we have

$$T_{2,k} = \frac{B_{\tilde{n}}(0)}{M^k(M-N)^{\tilde{n}-k}}+\sum_{l=1}^{k-1}\binom{k}{l}\frac{B_{\tilde{n}}(0)}{M^kN^{\tilde{n}-l}(M-N)^{\tilde{n}-k+l}}+\frac{B_{\tilde{n}}(0)}{M^kN^{\tilde{n}-k}}$$

$$=\left(\frac{1}{M^k(M-N)^{\tilde{n}-k}}+\frac{M^k-N^k-(M-N)^k}{M^k(N(M-N))^{\tilde{n}}}+\frac{1}{M^kN^{\tilde{n}-k}}\right)B_{\tilde{n}}(0)$$

and

$$T_{2,0} = \sum_{\substack{0\le K_i\le M-1,\\(i\ge1)}} B_{\tilde{n}}\left(\left\{\frac{\sum_{i\ge1}K_i}{M}\right\}\right) = B_{\tilde{n}}(0).$$

Thus we have

$$\sum_{k=0}^{\tilde{n}}(-1)^k\binom{\tilde{n}}{k}T_{2,k} = \Bigg\{1+\sum_{k=1}^{\tilde{n}-1}(-1)^k\binom{\tilde{n}}{k}$$

$$\times\left(\frac{1}{M^k(M-N)^{\tilde{n}-k}}+\frac{M^k-N^k-(M-N)^k}{M^k(N(M-N))^{\tilde{n}}}+\frac{1}{M^kN^{\tilde{n}-k}}\right)$$

$$+(-1)^{\tilde{n}}\left(2+\left(\frac{1}{N}+\frac{1}{M-N}\right)^{\tilde{n}}-\frac{1}{N^{\tilde{n}}}-\frac{1}{(M-N)^{\tilde{n}}}\right)\Bigg\}B_{\tilde{n}}(0)$$

$$=\Bigg\{1+\frac{N^{\tilde{n}}}{(M(M-N))^{\tilde{n}}}+\frac{(M-N)^{\tilde{n}}}{(MN)^{\tilde{n}}}$$

$$-\frac{1}{(MN)^{\tilde{n}}}-\frac{1}{(M(M-N))^{\tilde{n}}}-\frac{2(-1)^{\tilde{n}}}{M^{\tilde{n}}}-\frac{1}{(M-N)^{\tilde{n}}}-\frac{1}{N^{\tilde{n}}}$$

$$+\frac{(-1)^{\tilde{n}}}{(M(M-N))^{\tilde{n}}}+\frac{(-1)^{\tilde{n}}}{(MN)^{\tilde{n}}}+\frac{1-(-1)^{\tilde{n}}}{(N(M-N))^{\tilde{n}}}$$

$$+(-1)^{\tilde{n}}\left(2+\left(\frac{1}{N}+\frac{1}{M-N}\right)^{\tilde{n}}-\frac{1}{N^{\tilde{n}}}-\frac{1}{(M-N)^{\tilde{n}}}\right)\Bigg\}B_{\tilde{n}}(0)$$

$$=\frac{1}{(MN(M-N))^{\tilde{n}}}\Big\{3\big(MN(M-N)\big)^{\tilde{n}}+M^{2\tilde{n}}+N^{2\tilde{n}}+(M-N)^{2\tilde{n}}$$

$$-2\big((M-N)N\big)^{\tilde{n}}-2M^{\tilde{n}}\big((M-N)^{\tilde{n}}+N^{\tilde{n}}\big)\Big\}B_{\tilde{n}}(0),$$

where we replaced $(-1)^{\tilde{n}}$ by 1 by virtue of $B_n(0)=0$ for odd $n>1$. These complete the proof of Theorem 2.1.

Remark 1. Although it seems to be true that the density referred at the beginning of this section exists for any integral polynomials $g_1(x)$, $g_2(x)$, we do not guess what the value is. For example, for polynomials $g_1(x)=x^2$, $g_2(x)=-2x$ (resp. $g_1(x)=x^2$, $g_2(x)=2x$), the density seems $\frac{7}{8}$, $\frac{7}{8}-\frac{1}{16}$, $\frac{7}{8}+\frac{1}{16}$ (resp. $\frac{7}{8}, \frac{7}{8}+\frac{1}{16}, \frac{7}{8}$) according as

$$f(x)=x^3+2, \qquad x^3+x^2-2x-1, \qquad x^3+3x^2-1.$$

Also, it is mysterious that the density seems to be $\frac{7}{8}$ for $g_1(x)=mx^2$, $g_2(x)=nx^2$ for any integers m,m with $mn\neq 0, m\neq n$ for an irreducible polynomial $f(x)$ of degree 3.

3. Case of $x^4 + 1$

In this section, set $f(x) = x^4 + 1$ whose roots are $\alpha_1 = \frac{1+\sqrt{-1}}{\sqrt{2}}$, $\alpha_2 = \frac{1-\sqrt{-1}}{\sqrt{2}}$, $\alpha_3 = -\frac{1-\sqrt{-1}}{\sqrt{2}}$, $\alpha_4 = -\frac{1+\sqrt{-1}}{\sqrt{2}}$, where linear relations among roots over rationals are spanned by $\alpha_1+\alpha_4=\alpha_2+\alpha_3=0$. It is easy to see that $\#\hat{\boldsymbol{G}}=8, \#\boldsymbol{G}_0=4$, more explicitly $\boldsymbol{G}_0 = \{id, (1,2)(3,4), (1,4)(2,3), (1,3)(2,4)\}$ and $\hat{\boldsymbol{G}} = \boldsymbol{G}_0 \cup (1,4)\boldsymbol{G}_0$, and $\mathfrak{D}(f,\sigma) = \{(x_1,\ldots,x_4) \mid 0 \le x_1 \le \cdots \le x_4 \le 1, x_1 + x_4 = x_2 + x_3 = 1\}$ ($\sigma \in \hat{\boldsymbol{G}}$) except finite points, which is identified to $\{(x_1,x_2) \mid 0 \le x_1 \le x_2 \le \frac{1}{2}\}$ and $\{(x_3,x_4) \mid \frac{1}{2} \le x_3 \le x_4 \le 1\}$.

For integral polynomials $g_1(x), g_2(x)$ of $\deg g_i \le 2$, let us consider

$$M_i(X) := \Big\{p \in \mathrm{Spl}_X(f) \mid \big\{\tfrac{g_1(r_i)}{p}\big\} < \big\{\tfrac{g_2(r_i)}{p}\big\}\Big\} \quad (i = 1,\ldots,4),$$

where r_i's are local roots of the polynomial $f(x)$ for a prime $p \in \mathrm{Spl}(f)$ and $\{a\}$ denotes the decimal part of a as usual, and write $M(X) := \big(M_1(X),\ldots,M_4(X)\big)$ and $\#M(X) := \big(\#M_1(X),\ldots,\#M_4(X)\big)$ for simplicity. For non-zero integers m,n, the set $I_{m,n}$ of $x \in (0,1)$ satisfying $\{mx\} < \{nx\}$ is a union of intervals. Hence, for linear polynomials $g_1(x) = mx, g_2(x) = nx$ we see

$$\begin{aligned} M_i(X) &= \left\{p \in \mathrm{Spl}_X(f) \,\middle|\, \left\{\frac{g_1(r_i)}{p}\right\} < \left\{\frac{g_2(r_i)}{p}\right\}\right\} \\ &= \left\{p \in \mathrm{Spl}_X(f) \,\middle|\, \frac{r_i}{p} \in I_{m,n}\right\}, \end{aligned}$$

and the density $\lim_{X\to\infty} \frac{\#M_i(X)}{\#\mathrm{Spl}_X(f)}$ is described by the domain of

$$\{\boldsymbol{x} \in (0,1)^4 \mid x_i \in I_{m,n}\}$$

by Conjecture 1.2. For example, for special polynomials $g_1(x) = nx$, $g_2(x) = 2nx$ ($n \ne 0, n \in \mathbb{Z}$), the computer experiment suggests that the density

$$\lim_{X\to\infty} \frac{\#M(X)}{\#\mathrm{Spl}_X(f)} = \begin{cases} \big(\frac{n+1}{2n}, \frac{n+1}{2n}, \frac{n-1}{2n}, \frac{n-1}{2n}\big) & \text{if } 2 \nmid n, \\ \big(\frac{n+1}{2n}, \frac{n-1}{2n}, \frac{n+1}{2n}, \frac{n-1}{2n}\big) & \text{if } 2 \mid n, \end{cases}$$

which is equal to

$$\frac{1}{\frac{1}{8}}\big(\mathrm{vol}(D_1),\ldots,\mathrm{vol}(D_4)\big),$$

where

$$D_i = \left\{(x_1,x_2) \mid 0 \le x_1 \le x_2 \le \frac{1}{2}, \{g_1(x_i)\} < \{g_2(x_i)\}\right\} \quad (i = 1,2),$$

$$D_i = \left\{(x_3,x_4) \mid \frac{1}{2} \le x_3 \le x_4 \le 1, \{g_1(x_i)\} < \{g_2(x_i)\}\right\} \quad (i = 3,4),$$

and the denominator $\frac{1}{8}$ is the volume of the whole spaces

$$\left\{(x_1, x_2) \mid 0 \le x_1 \le x_2 \le \frac{1}{2}\right\}, \qquad \left\{(x_3, x_4) \mid \frac{1}{2} \le x_3 \le x_4 \le 1\right\},$$

which are identified with $\{(x_1, \dots, x_4) \mid 0 \le x_1 \le \cdots \le x_4 \le 1, x_1 + x_4 = x_2 + x_3 = 1\}$. These match the experiment above quite well and Conjecture 1.2. We classify integral polynomials $g_i(x)$ with $\deg\bigl(g_i(x)\bigr) \le 2$ and $g_1(0) = g_2(0) = 0$ except cases $\deg\bigl(g_1(x)\bigr) = \deg\bigl(g_2(x)\bigr) = 1$ as follows :

(i) $\deg\bigl(g_1(x)\bigr) = 2$ and $g_2(x) = nx\,(n \ne 0)$,

(ii) $\deg\bigl(g_1(x)\bigr) = \deg\bigl(g_2(x)\bigr) = 2$ and $g_1(x) - g_2(x) = nx, (n \ne 0)$, or

(iii) $\deg\bigl(g_1(x)\bigr) = \deg\bigl(g_2(x)\bigr) = \deg\bigl(g_1(x) - g_2(x)\bigr) = 2$.

Then, in case of (i),(ii) the density looks like

$$\begin{cases} \left(\frac{3n-2}{6n}, \frac{3n-1}{6n}, \frac{3n+1}{6n}, \frac{3n+2}{6n}\right) & \text{if } n \equiv 1 \bmod 2, \\ \left(\frac{3n-2}{6n}, \frac{3n+2}{6n}, \frac{3n-2}{6n}, \frac{3n+2}{6n}\right) & \text{if } n \equiv 0 \bmod 2, \end{cases}$$

and in case of (iii) it looks like $\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right)$. The author does not know how to elucidate these, in particular, even the reason of

$$\lim_{X \to \infty} \frac{\#M_1(X) + \#M_4(X)}{\#\mathrm{Spl}_X(f)} = \lim_{X \to \infty} \frac{\#M_2(X) + \#M_3(X)}{\#\mathrm{Spl}_X(f)} = 1.$$

REFERENCES

[K1] KITAOKA, Y.: *Notes on the distribution of roots modulo a prime of a polynomial*, Unif. Distrib. Theory **12** (2017), no. 2, 91–116.

[K2] KITAOKA, Y.: , *Notes on the distribution of roots modulo a prime of a polynomial II*, Unif. Distrib. Theory **14** (2019), no. 1, 87–104.

[K3] KITAOKA, Y.: *Notes on the distribution of roots modulo a prime of a polynomial III*, Unif. Distrib. Theory **15** (2020), no. 1, 93–104.

Received August 16, 2022
Accepted December 12, 2022

Yoshiyuki Kitaoka
Author is retired,
Asahi
JAPAN
E-mail: y_kitaoka@tg.commufa.jp