MULTI-BASE REPRESENTATIONS OF INTEGERS: ASYMPTOTIC ENUMERATION AND CENTRAL LIMIT THEOREMS

DANIEL KRENN, DIMBINAINA RALAIVAOSAONA, AND STEPHAN WAGNER

ABSTRACT. In a multi-base representation of an integer (in contrast to, for example, the binary or decimal representation) the base (or radix) is replaced by products of powers of single bases. The resulting numeral system has desirable properties for fast arithmetic. It is usually redundant, which means that each integer can have multiple different digit expansions, so the natural question for the number of representations arises. In this paper, we provide a general asymptotic formula for the number of such multi-base representations of a positive integer n. Moreover, we prove central limit theorems for the sum of digits, the Hamming weight (number of non-zero digits, which is a measure of efficiency) and the occurrences of a fixed digits in a random representation.

1. INTRODUCTION AND BACKGROUND

A *numeral system*[1] (also called *system of numeration*) is a way to represent numbers. The most common examples are, of course, the ordinary decimal and binary systems, which represent numbers in base 10 and 2, respectively. Besides those "standard" systems, there is an immense number of other numeral systems.

For fast arithmetic, the right choice of numeral system is an important aspect. The algorithms we have in mind here are, for example, exponentiation in a finite group and the scalar multiplication on elliptic curves. Both are used in cryptography, and clearly we want to improve on the running time of those algorithms (which are often based on a Horner scheme, cf. Knuth [14]).

Starting with the binary system, one can improve the performance of the aforementioned algorithms by adding more digits than needed. Thus, we make the numeral system *redundant*, which means that each element can have a lot of different representations. For instance, using digits 0, 1 and -1 can lead to a speed-up, cf. Morain and Olivos [20] for such a scalar multiplication algorithm on elliptic curves. To gain back the uniqueness, additional syntax can complement the redundant system. In the example using digits 0, 1 and -1, this can be the non-adjacent form, see Reitwiesner's seminal paper [25]. Generalizations in that direction can be found in [3, 9, 19, 27].

A different way to get redundancy, and thereby a better running time of the algorithms mentioned above, is to use double-base and multi-base numeral systems. For example, we can represent a number by a finite sum of terms $a_\ell 3^{\alpha_\ell} 7^{\beta_\ell} 11^{\gamma_\ell}$ for some digits a_ℓ, which leads to a multi-base system with three bases. A formal definition is given in the next section. Note that multiplication by one of the bases (in the example: 3, 7 or 11) is extremely simple for such representations, just like doubling is easy for binary representations. This is a very desirable property for fast arithmetic.

Double-base numeral systems are used for cryptographic applications, see for example [1, 5, 6]. The typical bases are 2 and 3. With these bases (and a digit set containing at least 0 and 1), each positive integer has a double-base representation, cf. Berthé and Imbert [2]. When using

[1]We use the term *numeral system* rather than *number system* as it is also called sometimes, since that name is ambiguous. For example, the system of p-adic numbers or the system of real numbers are called number systems.

general bases, less is known on the existence, cf. Krenn, Thuswaldner and Ziegler [16] for some
results using small symmetric digit sets. However, choosing the digit set large enough (so that the
numeral system with only one of the bases can already represent all positive integers), existence
can always be guaranteed. Thus, when each positive integer has a multi-base representation, a
natural further question arises— and this is also the main question studied in this article: how
many representations does each integer have? Our Theorem I provides an (asymptotic) answer to
this question.

The question is also motivated by the cryptoanalysis of evaluation schemes (e.g. elliptic curve
scalar multiplication): One can avoid side channel attacks if the corresponding numeral system is
very redundant, i.e., if each element has many different representations. In addition to the number
of representations, other parameters, such as the (Hamming) weight or the sum of digits, are of
importance in this context and therefore studied here as well. The Hamming weight in particular
is a measure for the efficiency of a digit representation for fast arithmetic. We show here that the
sum of digits and the Hamming weight (as well as the number of occurrences of any fixed digit) of
a typical representation of n is of order $(\log n)^m$, where m is the number of bases.

Our paper is structured as follows. The following section provides more precise definitions and
reviews existing results on the number of representations (which are available in very special cases).
This is followed (in Section 3) by the precise statements of our main results. These results also
include, apart from the asymptotic enumeration of multi-base representations, the analysis of the
sum of digits, the (Hamming) weight and the number of occurrences of a fixed digit. The remaining
parts of this article (Sections 4 to 8) are devoted to the proofs of all these results, which are based
on generating functions and the saddle-point method. Section 9 concludes the paper.

An extended abstract of this paper was presented at the AofA 2014 conference in Paris, see [15].

2. Terminology and Existing Results

In a *multi-base representation of n* (or *multi-base expansion*), a positive integer n is expressed
as a finite sum

$$n = \sum_{\ell=1}^{L} a_\ell B_\ell, \qquad\qquad (\divideontimes)$$

such that the following holds.

- The a_ℓ (called *digits*) are taken from a fixed finite *digit set* $\mathcal{D}$. Here, we will be using
  the canonical digit set $\{0, 1, \ldots, d-1\}$ for some fixed integer $d \geq 2$, but in principle our
  methods work for other sets as well.
- The B_ℓ are in increasing order (i.e., $B_1 < B_2 < \cdots < B_L$) and taken from the set

  $$\mathcal{S} = \{p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_m^{\alpha_m} : \alpha_i \in \mathbb{N} \cup \{0\}\}.$$

  The numbers p_1, ..., p_m are called the *bases* (in our setting, these are fixed coprime
  integers greater than 1). The sequence of all elements of $\mathcal{S}$ in increasing order is sometimes
  called a *Hardy–Littlewood–Pólya-sequence*.

In the following, we will discuss the number of representations of n in a given multi-base system,
which we denote by $P(n)$ (we suppress the dependence on $p_1, p_2, \ldots, p_m$ and d). Note that this
number is finite, since our digit set does not contain negative integers.

For redundant single-base representations a lot is known. Reznick [26] presents results on
certain partition functions, which correspond to representations with non-negative digits; see also
Protasov [23, 24] for more recent results on the number of representations $P(n)$. When negative
digits are used as well (for example in elliptic curve cryptography), there are usually infinitely
many representations of a number, so counting these does not make sense. In this case, expansions
with minimum number of non-zero digits are of interest, since they lead to fast evaluation schemes.
See Grabner and Heuberger [10] for a result counting minimal representations (one minimal
representation is the non-adjacent form mentioned above, cf. also [11, 12, 25]).

Let us consider double-base systems in particular, and let us take bases 2 and p, where $p > 1$
is an odd integer, and digits 0 and 1. We can group terms involving the same powers of p and

use the uniqueness of the binary expansion to show that double-base representations with bases 2 and p are in bijection with partitions into powers of p, i.e., representations of the form

$$n = n_0 + n_1 p + n_2 p^2 + n_3 p^3 + \cdots$$

with (arbitrary) non-negative integers n_ℓ. More generally, the same is true for double-base representations with bases q and p and digit set $\{0, 1, \ldots, q-1\}$. It seems that the first non-trivial approximation of $P(n)$ in this special case is due to Mahler [17]. By studying Mordell's functional equation, he obtained

$$\log P(pn) \sim (\log n)^2 / (2 \log p).$$

The much more precise result

$$\log P(pn) = \frac{1}{2 \log p} \left(\log \frac{n}{\log n} \right)^2 + \left(\frac{1}{2} + \frac{1}{\log p} + \frac{\log \log p}{\log p} \right) \log n$$
$$- \left(1 + \frac{\log \log p}{\log p} \right) \log \log n + \mathcal{O}(1)$$

was derived by Pennington [22]. The error term in the previous asymptotic formula exhibits a periodic fluctuation. Note that for bases 2 and p, the function $P(n)$ fulfils the recurrence relation

$$P(n) = \begin{cases} P(n-1) + P(n/p) & \text{if } p \mid n, \\ P(n-1) & \text{otherwise,} \end{cases}$$

which has been known for a long time in conjunction with partitions of integers.

For further reference and more information see A005704 in the On-Line Encyclopedia of Integer Sequences [21] and see also [5, 18] for the connection to double-base systems.

3. Main Results

We present our main results now. The aim of this work is to give an asymptotic formula in a more general set-up. Throughout this paper, $d \geq 2$ and $m \geq 2$ are fixed integers, and $p_1, p_2, \ldots, p_m$ are integers such that $1 < p_1 < p_2 < \cdots < p_m$ and $\gcd(p_i, p_j) = 1$ for $i \neq j$. As our first main theorem, we prove an asymptotic formula for the number of representations of n of the form (✽). It will be convenient to use the abbreviation

$$\kappa = \frac{\log d}{m!} \prod_{j=1}^{m} \frac{1}{\log p_j}.$$

Theorem I. *If $m \geq 3$, then the number $P(n)$ of distinct multi-base representations of n of the form (✽) satisfies the asymptotic formula*

$$\log P(n) = C_0 (\log n)^m + C_1 (\log n)^{m-1} \log \log n + C_2 (\log n)^{m-1} + \mathcal{O}\big((\log n)^{m-2} \log \log n\big)$$

for $n \to \infty$, where

$$C_0 = \kappa,$$
$$C_1 = -m(m-1)\kappa,$$
$$C_2 = \kappa m \Big(1 + \tfrac{1}{2} \sum_{j=1}^{m} \log p_j - \tfrac{1}{2} \log d - \log(\kappa m) \Big).$$

In the case that there are precisely two bases, we have the following more precise asymptotic result.

Theorem II. *If $m = 2$, then the number $P(n)$ of distinct multi-base representations of n of the form (✽) satisfies the asymptotic formula*

$$P(n) = K(n)(\log n)^{K_0} n^{K_1} \exp\left(\kappa \log^2 \left(\frac{n}{\log n} \right) \right)$$

for $n \to \infty$, where $K(n)$ is a fluctuating function of n, that is, bounded above and below by positive constants, and

$$K_0 = \tfrac{1}{2} + 2\kappa\big(\log(2\kappa) - \tfrac{1}{2}(\log p_1 + \log p_2 - \log d)\big),$$
$$K_1 = 2\kappa\big(1 - \log(2\kappa) + \tfrac{1}{2}(\log p_1 + \log p_2 - \log d)\big) - 1.$$

Note that the first two terms of the asymptotic formula in Theorem I coincide with those in Theorem II.

Moreover, we study the distribution of three natural parameters in random multi-base representations, namely the sum of digits, i.e. $a_1 + a_2 + \cdots + a_L$ in the notation of $(\divideontimes)$, the Hamming weight (the number of non-zero coefficients a_ℓ) and the number of occurrences of a fixed digit b. We get the following theorems.

Theorem III. *The sum of digits in a random multi-base representation of n of the form $(\divideontimes)$ asymptotically follows a Gaussian distribution with mean and variance equal to*

$$\mu_n = \frac{\kappa(d-1)}{2\log d}(\log n)^m + \mathcal{O}\big((\log n)^{m-1}\log\log n\big)$$

and

$$\sigma_n^2 = \frac{\kappa(d-1)(d+1)}{12\log d}(\log n)^m + \mathcal{O}\big((\log n)^{m-1}\log\log n\big)$$

respectively.

Theorem IV. *The Hamming weight of a random multi-base representation of n of the form $(\divideontimes)$ asymptotically follows a Gaussian distribution with mean and variance equal to*

$$\mu_n = \frac{\kappa(d-1)}{d\log d}(\log n)^m + \mathcal{O}\big((\log n)^{m-1}\log\log n\big)$$

and

$$\sigma_n^2 = \frac{\kappa(d-1)}{d^2\log d}(\log n)^m + \mathcal{O}\big((\log n)^{m-1}\log\log n\big)$$

respectively.

Theorem V. *Let $b \in \{0, 1, \ldots, d-1\}$. The number of occurrences of the digit b in a random multi-base representation of n of the form $(\divideontimes)$ asymptotically follows a Gaussian distribution with mean and variance equal to*

$$\mu_n = \frac{\kappa}{d\log d}(\log n)^m + \mathcal{O}\big((\log n)^{m-1}\log\log n\big)$$

and

$$\sigma_n^2 = \frac{\kappa(d-1)}{d^2\log d}(\log n)^m + \mathcal{O}\big((\log n)^{m-1}\log\log n\big)$$

respectively.

The proofs of all these theorems are based on a saddle-point analysis of the associated generating functions. As it turns out, the tail estimates are most challenging, especially in the case $m = 2$ (see Section 5 for details). For the asymptotic analysis of the various harmonic sums that occur, we apply the classical Mellin transform technique, see [7].

4. The Generating Function

We start with a generating function for our problem. As mentioned earlier, we define the set

$$\mathcal{S} = \{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} : \alpha_j \in \mathbb{N} \cup \{0\}\},$$

which is exactly the monoid that is freely generated by $p_1, p_2, \ldots, p_m$. Note that the representations of n correspond exactly to partitions of n into elements of $\mathcal{S}$ where each term has multiplicity at

most $d - 1$. The generating function for such partitions, where the first variable z marks the size n and the second variable u marks the sum of digits, can be written as

$$F(z, u) = \prod_{h \in \mathcal{S}} \left(1 + uz^h + u^2 z^{2h} + \cdots + u^{d-1} z^{(d-1)h}\right) = \prod_{h \in \mathcal{S}} \frac{1 - (uz^h)^d}{1 - uz^h}. \tag{4.1}$$

Likewise, we have the generating function

$$G(z, u) = \prod_{h \in \mathcal{S}} \left(1 + uz^h + uz^{2h} + \cdots + uz^{(d-1)h}\right) = \prod_{h \in \mathcal{S}} \left(1 + uz^h \frac{1 - z^{(d-1)h}}{1 - z^h}\right), \tag{4.2}$$

where the second variable marks the Hamming weight (number of non-zero digits, or equivalently number of distinct parts in a partition). For a digit $b \in \{0, 1, \ldots, d-1\}$, whose occurrences will be marked by u, we use the generating function

$$H_b(z, u) = \prod_{h \in \mathcal{S}} \left(1 + z^h + \cdots + uz^{bh} + \cdots + z^{(d-1)h}\right) = \prod_{h \in \mathcal{S}} \left(\frac{1 - z^{dh}}{1 - z^h} + (u - 1)z^{bh}\right). \tag{4.3}$$

Obviously, $F(z, 1) = G(z, 1) = H_b(z, 1)$. We would like to apply the saddle-point method to these generating functions. The trickiest part in this regard are the rather technical tail estimates, especially when $m = 2$, which will be discussed in the next section. We will also need an asymptotic expansion in the central region. To this end, we define the three functions

$$f(t, u) = \log F(e^{-t}, u) = \sum_{h \in \mathcal{S}} \log\left(1 + ue^{-ht} + u^2 e^{-2ht} + \cdots + u^{d-1} e^{-(d-1)ht}\right),$$

$$g(t, u) = \log G(e^{-t}, u) = \sum_{h \in \mathcal{S}} \log\left(1 + ue^{-ht} + ue^{-2ht} + \cdots + ue^{-(d-1)ht}\right)$$

and

$$h_b(t, u) = \log H_b(e^{-t}, u) = \sum_{h \in \mathcal{S}} \log\left(1 + e^{-ht} + \cdots + ue^{-bht} + \cdots + e^{-(d-1)ht}\right).$$

Lemma 1. *Suppose that u lies in a fixed bounded positive interval around 1, e.g. $u \in [1/2, 2]$.*

(1) *For certain (real-)analytic functions $f_1(u)$, $f_2(u)$, $\ldots$, $f_m(u)$ with*

$$f_m(u) = \log(1 + u + \cdots + u^{d-1}) \prod_{j=1}^{m} \frac{1}{\log p_j},$$

we have the following asymptotic formula as $t \to 0^+$ (t positive and real), uniformly in u:

$$f(t, u) = \frac{f_m(u)}{m!}(\log 1/t)^m + \frac{f_{m-1}(u)}{(m-1)!}(\log 1/t)^{m-1} + \cdots + f_1(u)(\log 1/t) + \mathcal{O}(1).$$

Moreover,

$$\frac{\partial}{\partial t} f(t, u) = -\frac{f_m(u)}{(m-1)! \, t}(\log 1/t)^{m-1} + \mathcal{O}\left(t^{-1}(\log 1/t)^{m-2}\right)$$

and

$$\frac{\partial^2}{\partial t^2} f(t, u) = \frac{f_m(u)}{(m-1)! \, t^2}(\log 1/t)^{m-1} + \mathcal{O}\left(t^{-2}(\log 1/t)^{m-2}\right).$$

Finally, there exists an $\eta > 0$ such that for complex t with $|\mathrm{Im}\, t| \leq \eta$, we have

$$\frac{\partial^3}{\partial t^3} f(t, u) = \mathcal{O}\left((\mathrm{Re}\, t)^{-3}(\log 1/(\mathrm{Re}\, t))^{m-1}\right)$$

as $\mathrm{Re}\, t \to 0^+$, again uniformly in u.

(2) *Likewise, there exist functions $g_1(u)$, $g_2(u)$, ..., $g_m(u)$ such that*

$$g(t, u) = \frac{g_m(u)}{m!}(\log 1/t)^m + \frac{g_{m-1}(u)}{(m-1)!}(\log 1/t)^{m-1} + \cdots + g_1(u)(\log 1/t) + \mathcal{O}(1),$$

and the same conditions as in (1) hold with

$$g_m(u) = \log(1 + (d-1)u)\prod_{j=1}^{m}\frac{1}{\log p_j}.$$

(3) *Moreover, for each digit $b \in \{0, 1, \ldots, d-1\}$, there exist functions $h_{b,1}(u)$, $h_{b,2}(u)$, ..., $h_{b,m}(u)$ such that*

$$h_b(t, u) = \frac{h_{b,m}(u)}{m!}(\log 1/t)^m + \frac{h_{b,m-1}(u)}{(m-1)!}(\log 1/t)^{m-1} + \cdots + h_{b,1}(u)(\log 1/t) + \mathcal{O}(1),$$

and the same conditions as in (1) hold with

$$h_{b,m}(u) = \log(d - 1 + u)\prod_{j=1}^{m}\frac{1}{\log p_j}.$$

Proof. To prove the first part, we apply the classical Mellin transform technique to deal with the harmonic sums, see the paper of Flajolet, Gourdon and Dumas [7]. Consider first the Mellin transform

$$Y(s, u) = \int_0^\infty \log\big(1 + ue^{-t} + u^2 e^{-2t} + \cdots + u^{d-1}e^{-(d-1)t}\big)t^{s-1}\, dt.$$

Integration by parts allows us to provide a meromorphic continuation (cf. Hwang [13]). We have

$$Y(s, u) = \frac{1}{s}\int_0^\infty t^s \frac{ue^{-t} + 2u^2 e^{-2t} + \cdots + (d-1)u^{d-1}e^{-(d-1)t}}{1 + ue^{-t} + \cdots + u^{d-1}e^{-(d-1)t}}\, dt,$$

which exhibits the pole at 0 with residue $\log\big(1 + u + u^2 + \cdots + u^{d-1}\big)$, i.e., we have

$$Y(s, u) \sim s^{-1}\log(1 + u + \cdots + u^{d-1})$$

as $s \to 0$. By repeating this process one obtains a meromorphic continuation with further poles at $-1, -2, \ldots$.

Moreover, since the integrand in the definition of $Y(s, u)$ decays exponentially as $\operatorname{Re} t \to \infty$, we can change the path of integration to the ray consisting of all complex numbers t with $\operatorname{Arg} t = \epsilon > 0$, where ϵ is chosen small enough so that there is no t with $\operatorname{Arg} t \le \epsilon$ for which the expression inside the logarithm vanishes (this is possible since u was assumed to be positive, so there are no real values of t for which this happens). Set $\beta = e^{i\epsilon}$, and perform the change of variables $t = \beta v$ to obtain

$$Y(s, u) = \beta^s \int_0^\infty \log\big(1 + ue^{-\beta v} + u^2 e^{-2\beta v} + \cdots + u^{d-1}e^{-(d-1)\beta v}\big)v^{s-1}\, dv.$$

If now $s = \sigma + i\tau$ with $\sigma > 0$, then the integral is uniformly bounded in τ for fixed σ, while the factor $\beta^s = e^{i\epsilon\sigma - \epsilon\tau}$ decays exponentially as $\tau \to \infty$. The same can be done for $\sigma = 0$ and for negative values of σ (after suitable integration by parts) as well as negative τ (by symmetry). Therefore, we have

$$Y(\sigma + i\tau, u) = \mathcal{O}\big(e^{-\epsilon|\tau|}\big)$$

as $\tau \to \infty$, uniformly in u.

Second, let us consider the Dirichlet series associated with the set $\mathcal{S}$, i.e., $D(s) = \sum_{h \in \mathcal{S}} h^{-s}$. It can be written as a product of elementary functions

$$D(s) = \sum_{h \in \mathcal{S}} h^{-s} = \prod_{j=1}^{m}\frac{1}{1 - p_j^{-s}}. \tag{4.4}$$

Each factor $1/(1 - p_j^{-s})$ has a simple pole at 0 and its singular expansion there is given by $1/(1 - p_j^{-s}) \sim 1/(s\log p_j)$ as $s \to 0$.

Next we consider the Mellin transform of $f(t, u)$, which is given by $Y(s, u) D(s)$. This function has a pole of order $m + 1$ at $s = 0$, so the Laurent series of $Y(s, u)D(s)$ has the form

$$\frac{f_m(u)}{s^{m+1}} + \frac{f_{m-1}(u)}{s^m} + \cdots + \frac{f_1(u)}{s^2} + \frac{f_0(u)}{s} + \cdots,$$

with $f_m(u)$ as indicated in the statement of our lemma. The other coefficients can be expressed in terms of certain improper integrals. Applying the Mellin inversion formula, we get

$$f(t, u) = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} Y(s, u)D(s)t^{-s}\, ds$$

for any $c > 0$. Following Flajolet, Gourdon and Dumas [7, Theorem 4], we shift the line of integration to the left and pick up residues at the poles. This is possible because of the aforementioned growth properties of $Y(s, u)$. The main contribution comes from the pole at $s = 0$, where the residue is indeed

$$\frac{f_m(u)}{m!}(\log 1/t)^m + \frac{f_{m-1}(u)}{(m-1)!}(\log 1/t)^{m-1} + \cdots + f_1(u)(\log 1/t) + f_0(u).$$

There are further poles at all multiples of $2\pi i/\log p_j$ $(1 \le j \le m)$, which are all simple poles (no two of them coincide) in view of the fact that the p_j were assumed to be pairwise coprime, hence they only contribute $\mathcal{O}(1)$. In fact, the $\mathcal{O}(1)$ term can be replaced by a sum of m Fourier series with periods $\log p_j$ $(1 \le j \le m)$ that are given by

$$\Psi_j(t) = \sum_{k \in \mathbb{Z} \setminus \{0\}} \operatorname*{Res}_{s = 2\pi i k/\log p_j} Y(s, u)D(s)t^{-s}$$

$$= \sum_{k \in \mathbb{Z} \setminus \{0\}} Y\left(\frac{2\pi i k}{\log p_j}, u\right) \cdot \frac{1}{\log p_j} \prod_{\substack{r=1 \\ r \ne j}}^{m} \frac{1}{1 - p_r^{-2\pi i k/\log p_j}} \exp\left(-\frac{2\pi i k \log t}{\log p_j}\right).$$

We remark that these Fourier series have exponentially decaying coefficients, since $Y(s, u)$ decays exponentially in imaginary direction, while Baker's theorem on linear forms in logarithms (see Chapter 12 of [4]) guarantees that

$$\prod_{\substack{r=1 \\ r \ne j}}^{m} \frac{1}{\left|1 - p_r^{-2\pi i k/\log p_j}\right|}$$

is bounded above by a power of k: indeed, there exist constants A_Λ, B_Λ (depending on the bases $p_1, p_2, \ldots, p_m$) such that

$$\Lambda = |k \log p_r - \ell \log p_j| \ge A_\Lambda k^{-B_\Lambda}$$

for all $r \ne j$ and integers k and ℓ not equal to 0. Thus, if $\|\cdot\|$ denotes the distance to the nearest integer,

$$\left\|k \frac{\log p_r}{\log p_j}\right\| \ge \frac{A_\Lambda}{\log p_j} k^{-B_\Lambda}$$

and consequently

$$\left|1 - p_r^{-2\pi i k/\log p_j}\right| = \left|1 - \exp\left(-\frac{2\pi i k \log p_r}{\log p_j}\right)\right| \ge 4\left\|\frac{k \log p_r}{\log p_j}\right\| \ge \frac{4A_\Lambda}{\log p_j} k^{-B_\Lambda}.$$

It follows that

$$\prod_{\substack{r=1 \\ r \ne j}}^{m} \frac{1}{\left|1 - p_r^{-2\pi i k/\log p_j}\right|} = \mathcal{O}\left(k^{(m-1)B_\Lambda}\right),$$

which in turn means that

$$\operatorname*{Res}_{s = 2\pi i k/\log p_j} Y(s, u)D(s)t^{-s} = \mathcal{O}\left(|k|^{(m-1)B_\Lambda} e^{-2\pi\epsilon|k|/\log p_j}\right).$$

Thus each of the Fourier series Ψ_j is convergent and indeed represents a smooth function. This proves the asymptotic formula for $f(t, u)$. The derivatives $\frac{\partial}{\partial t} f(t, u)$ and $\frac{\partial^2}{\partial t^2} f(t, u)$ have Mellin

transforms $(1-s)Y(s-1,u)D(s-1)$ and $(s-1)(s-2)Y(s-2,u)D(s-2)$ respectively, so essentially the same arguments apply, now with the main terms coming from the poles at 1 and 2 respectively.

It remains to prove the estimate for the third derivative. Note that it can be written as

$$\frac{\partial^3}{\partial t^3}f(t,u) = \sum_{h\in\mathcal{S}} h^3 e^{-ht}\frac{Q(e^{-ht},u)}{(1+ue^{-ht}+\cdots+u^{d-1}e^{-(d-1)ht})^3},$$

where Q is some polynomial. If we choose η (recall that our result will be valid for $|\operatorname{Im} t| \leq \eta$) small enough so that the denominator stays away from 0 (compare the analysis of $Y(s,u)$ above), the last factor is uniformly bounded by a constant. The Mellin transform of

$$\sum_{h\in\mathcal{S}} h^3 e^{-ht}$$

is given by $\Gamma(s)D(s-3)$, to which we can apply the same arguments as for the harmonic sums encountered before. The dominant singularity is clearly a pole of order m at $s=3$ in this case, so that the desired estimate follows immediately.

The proofs of the second and the third part of Lemma 1 are analogous. $\square$

5. Estimating the Tails

For our application of the saddle-point method, we need to estimate the tails (i.e., the parts where z is away from the positive real axis) of the generating functions given in (4.1), (4.2) and (4.3). This is done in the following sequence of lemmas. First of all, let us introduce some notation. For $r > 0$, we set

$$\mathcal{S}(r) = \mathcal{S} \cap [1, 1/r] = \{h \in \mathcal{S} : hr \leq 1\}.$$

It is straightforward to prove that

$$|\mathcal{S}(r)| = \frac{(\log 1/r)^m}{m! \prod_{j=1}^m \log p_j} + \mathcal{O}\big((\log 1/r)^{m-1}\big) \tag{5.1}$$

as $r \to 0^+$. Note that later (starting with the next section), r will be determined by the saddle point equation.

Lemma 2. *Let u be in the interval $[\frac{1}{2}, 2]$, and let $z = e^{-r+2\pi iy}$ with $r > 0$ and $y \in [-\frac{1}{2}, \frac{1}{2}]$. There exists an absolute constant C such that*

$$\frac{|F(z,u)|}{F(|z|,u)} \leq \exp\bigg(-C\sum_{h\in\mathcal{S}(r)} \|hy\|^2\bigg),$$

$$\frac{|G(z,u)|}{G(|z|,u)} \leq \exp\bigg(-C\sum_{h\in\mathcal{S}(r)} \|hy\|^2\bigg)$$

and

$$\frac{|H_b(z,u)|}{H_b(|z|,u)} \leq \exp\bigg(-C\sum_{h\in\mathcal{S}(r)} \|hy\|^2\bigg),$$

where $\|\cdot\|$ denotes the distance to the nearest integer.

Proof. For positive real a and complex w, we have the two identities

$$\frac{|1+aw|^2}{(1+a|w|)^2} = 1 - \frac{2a(|w|-\operatorname{Re} w)}{(1+a|w|)^2}$$

and

$$\frac{\left|1+aw+aw^2\right|^2}{(1+a|w|+a|w|^2)^2} = 1 - \frac{2a(|w|-\operatorname{Re} w)(1+2|w|+a|w|^2+2\operatorname{Re} w)}{(1+a|w|+a|w|^2)^2}.$$

Assuming that $a \in [\frac{1}{2}, 2]$ and $|w| \leq 2$, we get

$$\frac{|1+aw|^2}{(1+a|w|)^2} \leq 1 - \frac{1}{25}(|w|-\operatorname{Re} w) \leq \exp\Big(-\frac{1}{25}(|w|-\operatorname{Re} w)\Big) \tag{5.2}$$

and

$$\frac{\left|1 + aw + aw^2\right|^2}{(1 + a\left|w\right| + a\left|w\right|^2)^2} \leq 1 - \frac{1}{169}(\left|w\right| - \operatorname{Re} w) \leq \exp\left(-\frac{1}{169}(\left|w\right| - \operatorname{Re} w)\right). \tag{5.3}$$

Now let d be even, set $a = u$ and $w = z^h$, so that (5.2), together with the triangle inequality, yields

$$\left|1 + uz^h + u^2 z^{2h} + \cdots + u^{d-1} z^{(d-1)h}\right|$$
$$\leq \left|1 + uz^h\right| + u^2 \left|z\right|^{2h} \left|1 + uz^h\right| + \cdots + u^{d-2} \left|z\right|^{(d-2)h} \left|1 + uz^h\right|$$
$$\leq \left(1 + u\left|z\right|^h + u^2 \left|z\right|^{2h} + \cdots + u^{d-1} \left|z\right|^{(d-1)h}\right) \exp\left(-\frac{1}{50}\left(\left|z\right|^h - \operatorname{Re}(z^h)\right)\right).$$

Taking the product over all $h \in \mathcal{S}$ gives

$$|F(z, u)| \leq F(|z|, u) \exp\left(-\frac{1}{50} \sum_{h \in \mathcal{S}} \left(\left|z\right|^h - \operatorname{Re}(z^h)\right)\right)$$
$$= F(|z|, u) \exp\left(-\frac{1}{50} \sum_{h \in \mathcal{S}} e^{-hr}\left(1 - \cos(2\pi h y)\right)\right)$$
$$\leq F(|z|, u) \exp\left(-\frac{1}{50e} \sum_{h \in \mathcal{S}(r)} \left(1 - \cos(2\pi h y)\right)\right)$$
$$\leq F(|z|, u) \exp\left(-\frac{8}{50e} \sum_{h \in \mathcal{S}(r)} \|hy\|^2\right),$$

which proves the first statement of the lemma with $C = 4/(25e)$. For odd d, we can argue in a similar fashion, but we also apply (5.3) (with $a = 1$ and $w = uz^h$) and use the triangle inequality in the following way:

$$\left|1 + uz^h + u^2 w^2 + \cdots + u^{d-1} z^{(d-1)h}\right|$$
$$\leq \left|1 + uz^h + u^2 z^{2h}\right| + u^3 \left|z\right|^{3h} \left|1 + uz^h\right| + \cdots + u^{d-2} \left|z\right|^{(d-2)h} \left|1 + uz^h\right|.$$

For the generating function $G(z, u)$, the reasoning is fully analogous, but we also have to use (5.3) with $a = u$ and $w = z^h$. A similar situation occurs for $H_b(z, u)$. $\qquad \square$

Next we estimate the sum that occurs in the previous lemma. When $m > 2$, relatively simple estimates suffice for our purposes, while we need an additional auxiliary result in the case that $m = 2$. The following lemma provides the necessary estimates.

Lemma 3. *Let $r > 0$ and $y \in [-\frac{1}{2}, \frac{1}{2}]$, and set*

$$\Sigma = \Sigma(r, y) = \sum_{h \in \mathcal{S}(r)} \|hy\|^2,$$

where again $\|\cdot\|$ denotes the distance to the nearest integer. For sufficiently small r, we have the following estimates for Σ.

(a) *If $|y| \leq r/2$, then $\Sigma \geq A_1 (y/r)^2 (\log(1/r))^{m-1}$ for some positive constant A_1 (that only depends on m and the set of bases $\{p_1, p_2, \ldots, p_m\}$).*

(b) *If $|y| \geq r/2$, then $\Sigma \geq A_2 (\log(1/r))^{m-1}$ for some positive constant A_2 (that also only depends on m and the set of bases $\{p_1, p_2, \ldots, p_m\}$).*

Now let $m = 2$. For any constant $K > 0$ and any $\delta > 0$, there exists a constant $B > 0$ depending on p_1, p_2, K and δ such that the following holds for sufficiently small r.

(c) *We have $\Sigma \geq K \log(1/r)$, except when y lies in a certain set $E(K, r)$ of Lebesgue measure at most $Br^{1-\delta}$.*

Proof. For better readability, the proof is split into several claims.

A. *Statement (a) is correct.*

Proof of $\boldsymbol{A}$. Let $|y| \leq r/2$, which implies $|hy| \leq \frac{1}{2}$ for all $h \in \mathcal{S}(r)$. Then we have

$$\Sigma = \sum_{h \in \mathcal{S}(r)} \|hy\|^2 = \sum_{h \in \mathcal{S}(r)} h^2 y^2 \geq \sum_{\substack{h \in \mathcal{S}(r) \\ h \notin \mathcal{S}(r/\rho)}} h^2 y^2 \geq \rho^2 (y/r)^2 \left(|\mathcal{S}(r)| - |\mathcal{S}(r/\rho)| \right)$$

for any $\rho > 0$. If we take ρ sufficiently small and apply the asymptotic formula in (5.1), we obtain estimate (a). $\qquad\square$

B. *A_2 can be chosen in such a way that statement (b) holds for $|y| \leq r^{2/3}$.*

Proof of $\boldsymbol{B}$. Let us assume that $r/2 \leq |y| \leq r^{2/3}$. Then we have $\log |1/y| \geq \frac{2}{3} \log(1/r)$, and essentially the same idea as above works again. We obtain

$$\Sigma = \sum_{h \in \mathcal{S}(r)} \|hy\|^2 \geq \sum_{h \in \mathcal{S}(2|y|)} h^2 y^2 \geq \sum_{\substack{h \in \mathcal{S}(2|y|) \\ h \notin \mathcal{S}(|y|/\rho)}} h^2 y^2 \geq \rho^2 \left(|\mathcal{S}(2|y|)| - |\mathcal{S}(|y|/\rho)| \right),$$

and formula (5.1) can be applied again to obtain (b). $\qquad\square$

We are left with the case that $|y| > r^{2/3}$, so we will assume this from now on. By Dirichlet's approximation theorem, there exists a rational number a/q (with coprime a and q) such that $q \leq r^{-2/3}$ and

$$\left| y - \frac{a}{q} \right| \leq \frac{r^{2/3}}{q}.$$

C. *There exists a positive constant c_1 that only depends on m and the set of bases $\{p_1, p_2, \ldots, p_m\}$ such that for small enough r and any coprime integers a, q with $q \leq r^{-2/3}$, there are at least*

$$c_1 (\log q)(\log 1/r)^{m-1}$$

many elements $h_1 \in \mathcal{S}(r^{1/3})$ with $\|ah_1/q\| \geq 1/q$.

Proof of $\boldsymbol{C}$. For $q = 1$, the statement is trivial, so we assume that $q \neq 1$. Let us now distinguish whether q is in the set $\mathcal{S}$ or not.

If $q \in \mathcal{S}$, then write $q = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$. We have

$$A = \max(\alpha_1, \alpha_2, \ldots, \alpha_m) \geq \frac{\log q}{\log(p_1 p_2 \ldots p_m)}.$$

Suppose that $\alpha_i = A$. Consider the elements $h_1 = p_1^{\beta_1} p_2^{\beta_2} \cdots p_m^{\beta_m} \in \mathcal{S}$ with $0 \leq \beta_i < \alpha_i = A$. For any of these h_1, the number ah_1/q is not an integer and thus $\|ah_1/q\| \geq 1/q$. Let us now find a lower bound for the number of such elements h_1. Using (5.1) (applied to the set $\mathcal{S}_i = \{s \in \mathcal{S} : p_i \nmid s\}$), we find that for some positive constants $\hat{c}_1$ and c_1, there exist at least

$$\hat{c}_1 A |\mathcal{S}_i(r^{1/3})| \geq c_1 (\log q)(\log 1/r)^{m-1}$$

elements $h_1 \in \mathcal{S}$ with $h_1 \leq r^{-1/3}$.

If $q \notin \mathcal{S}$, then we clearly have $\|h_1 a/q\| \geq 1/q$ for all $h_1 \in \mathcal{S}$, so the same statement as in the first case holds again. $\qquad\square$

D. *There exists a positive constant c that only depends on m and the set of bases $\{p_1, p_2, \ldots, p_m\}$ such that for sufficiently small r and $r^{2/3} < |y| \leq \frac{1}{2}$, there are at least*

$$c(\log 1/r)^{m-1}$$

many elements $h \in \mathcal{S}(r)$ with $\|hy\| \geq 1/(3p_1)$.

Proof of $\boldsymbol{D}$. Let us divide the interval $[1/q, 1/2]$ into subintervals

$$I_0 = [1/(2p_1), 1/2], \ I_1 = [1/(2p_1^2), 1/(2p_1)], \ \ldots$$

whose ends have a ratio of p_1 (except possibly for the last one). There are at most

$$\log(q/2)/\log(p_1) \leq c_2 \log q$$

such intervals.

By **C** and the pigeonhole principle, we can choose one of these intervals (I_j, say) such that for at least $c_1/c_2 (\log 1/r)^{m-1}$ distinct numbers $h_1 \in \mathcal{S}$ with $h_1 \leq r^{-1/3}$, the number $\|h_1 a/q\|$ lies in this interval I_j, i.e., we have $1/(2p_1^{j+1}) \leq \|h_1 a/q\| \leq 1/(2p_1^j)$.

Now we have

$$\left\| \frac{h_1 p_1^j a}{q} \right\| = p_1^j \left\| \frac{h_1 a}{q} \right\| \geq \frac{1}{2p_1},$$

which means that we have at least $c_1/c_2 (\log 1/r)^{m-1}$ elements $h = h_1 p_1^j \in \mathcal{S}$ with $\|ah/q\| \geq 1/(2p_1)$ and

$$h = h_1 p_1^j \leq h_1 q \leq r^{-1/3} r^{-2/3} = \frac{1}{r}.$$

All of these numbers h are therefore in the set $\mathcal{S}(r)$. For sufficiently small r, it follows that

$$\|hy\| \geq \left\| \frac{ha}{q} \right\| - \frac{r^{2/3}h}{q} \geq \frac{1}{2p_1} - \frac{r^{2/3}h_1 q}{q} \geq \frac{1}{2p_1} - r^{1/3} \geq \frac{1}{3p_1},$$

which proves the claim. □

E. *A_2 can be chosen in such a way that statement (b) holds for $|y| \geq r^{2/3}$.*

*Proof of **E**.* The result follows from **D** since

$$\Sigma \geq c \left(\log \frac{1}{r} \right)^{m-1} \cdot \left(\frac{1}{3p_1} \right)^2 = A_2 \left(\log \frac{1}{r} \right)^{m-1}$$

for $A_2 = c/(9p_1^2)$ if r is sufficiently small. □

So (b) is now proven in both cases, and it remains to prove statement (c) of the lemma, so assume that $m = 2$. Choose some $\epsilon \in (0, \delta)$, set

$$L = \lfloor (1 - \epsilon) \log_{p_1} 1/r \rfloor$$

and define, for a positive integer M, the set

$$D(M) = \left\{ v \in [0, 1] : \|p_1^\ell v\| < p_1^{-2} \text{ for } 0 \leq \ell \leq L \text{ with at most } M \text{ exceptions} \right\}.$$

The constant M will be chosen appropriately at the end of the proof.

We get the following result, which almost proves (c).

F. *Set $R = \lfloor \epsilon \log_{p_2} 1/r \rfloor$. If y is not contained in the set*

$$E = \bigcup_{k \leq R} \{ y \in [-\tfrac{1}{2}, \tfrac{1}{2}] : p_2^k y \bmod 1 \in D(M) \},$$

then

$$\Sigma \geq \epsilon p_1^{-2} M \log_{p_2} 1/r.$$

*Proof of **F**.* By our assumptions, there is no $k \leq R$ such that $p_2^k y \bmod 1 \in D(M)$. Therefore, for a fixed k the inequality $\|p_1^\ell p_2^k y\| \geq p_1^{-2}$ holds for more than M choices of $\ell \leq L$. Moreover, we have $p_1^\ell p_2^k \leq r^{-1+\epsilon} \cdot r^{-\epsilon} = r^{-1}$ for all such k and ℓ.

It follows that

$$\Sigma = \sum_{h \in \mathcal{S}(r)} \|hy\|^2 \geq \sum_{\ell \leq L} \sum_{k \leq R} \|p_1^\ell p_2^k y\|^2 \geq (R+1)M p_1^{-2} \geq \epsilon p_1^{-2} M \log_{p_2} 1/r,$$

which is what we wanted to show. □

It remains to show that the set E is small. This is done in the following two claims.

G. *The Lebesgue measure of the set $D(M)$ is at most $\mathcal{O}\left(L^M p_1^{M-L} \right)$.*

*Proof of **G**.* First, note that $\|p_1^\ell v\| \geq p_1^{-2}$ unless the $(\ell + 1)$-th and the $(\ell + 2)$-th digit after the decimal[2] point in the p_1-adic expansion of v are either both 0 or both $p_1 - 1$. For an upper bound, we relax this condition to both digits being equal.

Therefore, for an element of $D(M)$, at least $L - M + 1$ of the first $L + 2$ digits have to be equal to the previous digit. Allowing exactly $j \leq M$ exceptions, there are $\binom{L+1}{j}$ number of ways to choose the "exceptional" digits. Moreover, each digit that has to be equal to the previous one reduces the Lebesgue measure by a factor of p_1.

Putting everything together, we end up finding that the Lebesgue measure of $D(M)$ is at most

$$\sum_{j=0}^{M} \binom{L+1}{j} p_1^{-(L+1)+j} = \mathcal{O}\left(L^M p_1^{M-L}\right),$$

which proves the claim. □

We need one more claim, which concerns the size of the exceptional set E.

H. *The set E has Lebesgue measure $\mathcal{O}\left(r^{1-\epsilon}(\log 1/r)^{M+1}\right)$.*

*Proof of **H**.* Since $y \in [-\frac{1}{2}, \frac{1}{2}]$ (an interval of length 1) and p_2^k is an integer, the Lebesgue measure λ is preserved under taking the pre-image of $v \mapsto p_2^k v \bmod 1$. Therefore, we have

$$\lambda\left(\{y \,:\, p_2^k y \bmod 1 \in D(M)\}\right) = \lambda(D(M))$$

and obtain

$$\lambda(E) \leq \sum_{k \leq R} \lambda(D(M)) = \mathcal{O}\left(RL^M p_1^{M-L}\right) = \mathcal{O}\left(r^{1-\epsilon}(\log 1/r)^{M+1}\right).$$

Note that the implied constant only depends on p_1, p_2, M and ϵ. □

If we choose $M = \lceil K\epsilon^{-1} p_1^2 \log p_2 \rceil$, then statement (c) follows from the claims above (in particular, **F** and **H**) with exceptional set $E = E(K, r)$. Note that $\lambda(E) = \mathcal{O}\left(r^{1-\epsilon}(\log 1/r)^{M+1}\right) = \mathcal{O}\left(r^{1-\delta}\right)$. This completes the proof. □

6. Application of the Saddle-Point Method

We are now ready to apply the saddle-point method (see Chapter VIII of [8] for an excellent introduction), which gives us asymptotic formulas for the coefficients of the generating functions $F(z, u)$, $G(z, u)$ and $H_b(z, u)$. In the following, we use the notations $f_t(t, u)$, $f_{tt}(t, u)$, ... for the derivatives of f with respect to the first coordinate.

Lemma 4. *Let $u \in [\frac{1}{2}, 2]$, and define $r > 0$ implicitly by the saddle-point equation*

$$n = -f_t(r, u).$$

The coefficients of $F(z, u)$ satisfy the asymptotic formula

$$[z^n]F(z, u) = \frac{1}{\sqrt{2\pi f_{tt}(r, u)}} e^{nr + f(r, u)}\left(1 + \mathcal{O}\left((\log n)^{-(m-1)/5}\right)\right),$$

uniformly in u. Likewise, if we define $r > 0$ by

$$n = -g_t(r, u),$$

then the coefficients of $G(z, u)$ satisfy the asymptotic formula

$$[z^n]G(z, u) = \frac{1}{\sqrt{2\pi g_{tt}(r, u)}} e^{nr + g(r, u)}\left(1 + \mathcal{O}\left((\log n)^{-(m-1)/5}\right)\right),$$

uniformly in u, and if we define $r > 0$ by

$$n = -h_{a,t}(r, u),$$

---

[2] We should rather correctly say "p_1-point" instead of "decimal point" since p_1 is the base of our numeral system, but this may lead to even more confusion.

then the coefficients of $H_b(z, u)$ satisfy the asymptotic formula

$$[z^n]H_b(z, u) = \frac{1}{\sqrt{2\pi h_{b,tt}(r, u)}} e^{nr + h_b(r,u)} \left(1 + \mathcal{O}\left((\log n)^{-(m-1)/5}\right)\right).$$

Let us first give a short outline on the proof, which we only present for F, since the other two cases are analogous. We start by using Cauchy's integral formula to extract the coefficient of z^n from $F(z, u)$. After the subsequent change to polar coordinates ($z = e^{-(r+it)}$), we choose r to satisfy the saddle point equation. Thus the Taylor expansion in the central region simplifies (the first order term vanishes). Lemma 1 shows that r is of order $(\log n)^{m-1}/n$. In the central region (to be defined later), the error term is $\mathcal{O}\left(\log(1/r)^{-(m-1)/5}\right)$ by Lemma 1, and we can complete the tails to get a Gaussian integral. The remaining parts of the integral are estimated by means of Lemmas 2 and 3. If $m > 2$, parts (a) and (b) of Lemma 3 already give sufficiently strong bounds. In the case that $m = 2$, we have to divide the tails further into a small "exceptional part", where we apply (b), and the rest, where the stronger bound from (c) holds.

So much for the overview; let us start with the actual proof now.

Proof. By Cauchy's integral formula, we have

$$[z^n]F(z, u) = \frac{1}{2\pi i} \oint_{\mathcal{C}} F(z, u) \frac{dz}{z^{n+1}},$$

where $\mathcal{C}$ is a circle around 0 with radius less than 1. Let $r > 0$ and perform the change of variables $z = e^{-t} = e^{-(r+i\tau)}$, so that the integral becomes

$$[z^n]F(z, u) = \frac{1}{2\pi} \int_{-\pi}^{\pi} \exp(nr + f(r + i\tau, u) + in\tau) \, d\tau. \tag{6.1}$$

Now we choose $r = r(n, u) > 0$ to be the unique positive solution of the saddle-point equation

$$n = -f_t(r, u). \tag{6.2}$$

Let c be a constant such that $(m-1)/3 < c < (m-1)/2$, we choose specifically $c = 2(m-1)/5$. Consider first the integral

$$I_0 = \frac{1}{2\pi} \int_{-r(\log 1/r)^{-c}}^{r(\log 1/r)^{-c}} \exp(nr + f(r + i\tau, u) + in\tau) \, d\tau.$$

For $|\tau| \le r(\log 1/r)^{-c}$, using Taylor expansion and Lemma 1, we have

$$f(r + i\tau, u) = f(r, u) + if_t(r, u)\tau - f_{tt}(r, u)\frac{\tau^2}{2} + \mathcal{O}\left(|\tau|^3 \sup_{|y| \le \tau} |f_{ttt}(r + iy, u)|\right)$$

$$= f(r, u) + if_t(r, u)\tau - f_{tt}(r, u)\frac{\tau^2}{2} + \mathcal{O}\left((\log 1/r)^{m-1-3c}\right).$$

Therefore, by the definition of r in (6.2), we have

$$I_0 = \frac{e^{nr + f(r,u)}}{2\pi} \int_{-r(\log 1/r)^{-c}}^{r(\log 1/r)^{-c}} \exp\left(-f_{tt}(r, u)\frac{\tau^2}{2}\right) d\tau \left(1 + \mathcal{O}\left((\log 1/r)^{m-1-3c}\right)\right).$$

Furthermore,

$$\int_{-r(\log 1/r)^{-c}}^{r(\log 1/r)^{-c}} \exp\left(-f_{tt}(r, u)\frac{\tau^2}{2}\right) d\tau$$

$$= \int_{-\infty}^{\infty} \exp\left(-f_{tt}(r, u)\frac{\tau^2}{2}\right) d\tau - 2 \int_{r(\log 1/r)^{-c}}^{\infty} \exp\left(-f_{tt}(r, u)\frac{\tau^2}{2}\right) d\tau$$

$$= \sqrt{\frac{2\pi}{f_{tt}(r, u)}} - 2 \int_{r(\log 1/r)^{-c}}^{\infty} \exp\left(-f_{tt}(r, u)\frac{\tau^2}{2}\right) d\tau,$$

and

$$0 \leq \int_{r(\log 1/r)^{-c}}^{\infty} \exp\left(-f_{tt}(r,u)\frac{\tau^2}{2}\right) d\tau \leq \int_{r(\log 1/r)^{-c}}^{\infty} \exp\left(-\frac{\tau}{2} f_{tt}(r,u) r(\log 1/r)^{-c}\right) d\tau$$

$$= \frac{2\exp\left(-f_{tt}(r,u) r^2 (\log 1/r)^{-2c}/2\right)}{f_{tt}(r,u) r(\log 1/r)^{-c}}$$

$$= \mathcal{O}\left(r(\log 1/r)^{-(m-1-c)} e^{-\gamma(\log 1/r)^{m-1-2c}}\right)$$

for a constant $\gamma > 0$. Since $m - 1 - 2c = (m-1)/5 > 0$, the $\mathcal{O}$-term goes to zero faster than any power of $\log 1/r$. Hence we have

$$I_0 = \frac{e^{nr+f(r,u)}}{\sqrt{2\pi f_{tt}(r,u)}}\left(1 + \mathcal{O}\left((\log 1/r)^{m-1-3c}\right)\right) = \frac{e^{nr+f(r,u)}}{\sqrt{2\pi f_{tt}(r,u)}}\left(1 + \mathcal{O}\left((\log n)^{-(m-1)/5}\right)\right). \quad (6.3)$$

It remains to show that the rest of the integral in (6.1) is small compared to I_0. To this end, note for comparison that $1/\sqrt{2\pi f_{tt}(r,u)}$ is of order $r(\log 1/r)^{-(m-1)/2}$. Now consider

$$I_1 = \int_{r(\log 1/r)^{-c}}^{\pi} \exp(nr + f(r+i\tau,u) + in\tau) \, d\tau.$$

Then

$$|I_1| \leq e^{nr+f(r,u)} \int_{r(\log 1/r)^{-c}}^{\pi} \exp(\mathrm{Re}(f(r+i\tau,u) - f(r,u))) \, d\tau$$

$$= e^{nr+f(r,u)} \int_{r(\log 1/r)^{-c}}^{\pi} \frac{\left|F(e^{-(r+i\tau)},u)\right|}{F(e^{-r},u)} \, d\tau.$$

If $m \geq 3$, then we can use Lemma 2 and parts (a) and (b) of Lemma 3 to show that the integrand $\left|F(e^{-(r+i\tau)},u)\right|/F(e^{-r},u)$ on the right hand side is $\mathcal{O}\left(\exp\left(-CA_1/(2\pi)^2 \cdot (\log 1/r)^{m-1-2c}\right)\right)$ for $|\tau| \leq \pi r$ and $\mathcal{O}\left(\exp\left(-CA_2(\log 1/r)^{m-1}\right)\right)$ otherwise, which immediately shows that

$$|I_1| = \mathcal{O}\left(e^{nr+f(r,u)}\left(r\exp\left(-CA_1/(2\pi)^2 \cdot (\log 1/r)^{m-1-2c}\right) + \exp\left(-CA_2(\log 1/r)^{m-1}\right)\right)\right).$$

For $m = 2$, we need to be more careful. Again, part (a) of Lemma 3 can be used for the interval where $|\tau| \leq \pi r$, with the same bound as above. The rest of the integral is split again: we choose a constant $K > 0$ such that $CK > 1$ (C as in Lemma 2), and $\delta > 0$ such that $\delta < CA_2$ (A_2 as in Lemma 3).

If $y = -\tau/(2\pi)$ is not in the exceptional set $E(K,r)$ as defined in Lemma 3, then we have

$$\frac{\left|F(e^{-(r+i\tau)},u)\right|}{F(e^{-r},u)} = \mathcal{O}(\exp(-CK\log 1/r)) = \mathcal{O}\left(r^{CK}\right).$$

By part (c) of Lemma 3, the set of τ-values for which this estimate does not hold has Lebesgue measure $\mathcal{O}\left(r^{1-\delta}\right)$, and we have the estimate

$$\frac{\left|F(e^{-(r+i\tau)},u)\right|}{F(e^{-r},u)} = \mathcal{O}(\exp(-CA_2\log 1/r)) = \mathcal{O}\left(r^{CA_2}\right)$$

for all those τ. Putting everything together shows that

$$|I_1| = \mathcal{O}\left(e^{nr+f(r,u)}\left(r\exp\left(-CA_1(\log 1/r)^{1/5}\right) + r^{CK} + r^{CA_2+1-\delta}\right)\right),$$

which again means that I_1 is negligible, since the exponents CK and $CA_2 + 1 - \delta$ are both > 1. The same reasoning can of course be applied to

$$I_2 = \int_{-\pi}^{-r(\log 1/r)^{-c}} \exp(nr + f(r+i\tau,u) + in\tau) \, d\tau.$$

This finishes the proof for the function $F(z,u)$. The proof for $G(z,u)$ and $H_b(z,u)$ is analogous. $\quad\square$

7. The Number of Representations

It is straightforward now to prove our main results.

Proof of Theorems I and II. We specialize by $u = 1$ in Lemma 4, which gives us

$$P(n) = [z^n]F(z,1) = \frac{1}{\sqrt{2\pi f_{tt}(r_0,1)}} e^{nr_0+f(r_0,1)}\big(1 + \mathcal{O}\big((\log n)^{-(m-1)/5}\big)\big),$$

where r_0 is given by the saddle-point equation $n = -f_t(r_0,1)$ (as its unique positive solution). Making use of Lemma 1, we get

$$n = \frac{f_m(1)}{(m-1)!r_0}(\log 1/r_0)^{m-1} + \mathcal{O}\big((\log 1/r_0)^{m-2}\big),$$

which readily gives us

$$\log 1/r_0 = \log n - (m-1)\log\log n - \log\frac{f_m(1)}{(m-1)!} + \mathcal{O}\left(\frac{\log\log n}{\log n}\right) \qquad (7.1)$$

for $n \to \infty$. Now it follows that

$$nr_0 = \frac{f_m(1)}{(m-1)!}(\log n)^{m-1}\left(1 + \mathcal{O}\left(\frac{\log\log n}{\log n}\right)\right),$$

and Lemma 1 also yields

$$f(r_0,1) = \frac{f_m(1)}{m!}(\log 1/r_0)^m + \frac{f_{m-1}(1)}{(m-1)!}(\log 1/r_0)^{m-1} + \mathcal{O}\big((\log n)^{m-2}\big)$$

$$= \frac{f_m(1)}{m!}(\log n)^m\left(1 - \frac{m(m-1)}{\log n}\log\log n - \frac{m}{\log n}\log\frac{f_m(1)}{(m-1)!} + \mathcal{O}\left(\frac{\log\log n}{(\log n)^2}\right)\right)$$

$$+ \frac{f_{m-1}(1)}{(m-1)!}(\log n)^{m-1}\left(1 + \mathcal{O}\left(\frac{\log\log n}{\log n}\right)\right) + \mathcal{O}\big((\log n)^{m-2}\log\log n\big).$$

Since $f_m(1)/m! = \kappa$ and $f_{m-1}(1)/(m-1)! = \kappa m(\sum_{j=1}^m \log p_j - \log d)/2$, this readily proves Theorem I (note that the factor $f_{tt}(r_0,1)$ only contributes $\mathcal{O}(\log n)$ to $\log P(n)$).

To get the more precise formula (Theorem II) in the case $m = 2$, we only need to expand a little further. $\qquad\square$

In principle, it would be possible to obtain similar (as in Theorem II), more precise asymptotic formulas (in terms of $\log n$ and $\log\log n$) for all $m \geq 2$, but the expressions become very lengthy.

8. Sum of Digits, Hamming Weight, Occurrences of a Digit

This section is devoted to the central limit theorems for the sum of digits (Theorem III), the Hamming weight (Theorem IV) and the occurrence of a fixed digit (Theorem V). We will only present the proof for the sum of digits; the other two proofs being analogous. The weak convergence to a Gaussian distribution will follow from the following general theorem (see [8, Theorem IX.13] and the comment thereafter, which states that it is sufficient to consider real values of u):

Lemma 5 (cf. [8, Theorem IX.13]). *Let $X_1, X_2, \ldots$ be a sequence of discrete random variables that only take on non-negative integer values. Assume that, for u in a fixed interval Ω around 1, the probability generating function $P_n(u)$ of X_n satisfies an asymptotic formula of the form*

$$P_n(u) = \exp(R_n(u))(1 + o(1))$$

uniformly with respect to u, where each $R_n(u)$ is analytic in Ω. Assume also that the conditions

$$R_n'(1) + R_n''(1) \to \infty \qquad and \qquad \frac{R'''(u)}{(R_n'(1) + R_n''(1))^{3/2}} \to 0$$

hold uniformly in u. Then the normalised random variables

$$X_n^* = \frac{X_n - R_n'(1)}{(R_n'(1) + R_n''(1))^{1/2}}$$

converge in distribution to a standard Gaussian distribution.

Proof of Theorem III. We use Lemma 4. Let X_n be the sum of digits of a random multi-base representation of n, and let

$$P_n(u) = \frac{[z^n]F(z,u)}{[z^n]F(z,1)}$$

be the associated probability generating function. In the following, we write $r(u)$ instead of just r to emphasize the dependence on u (of course, r depends on n as well). Moreover, we set $r_0 = r(1)$ as in the previous section. In view of Lemma 4, Lemma 5 applies with

$$R_n(u) = n(r(u) - r_0) + f(r(u), u) - f(r_0, 1) - \frac{1}{2}\log f_{tt}(r(u), u) + \frac{1}{2}\log f_{tt}(r_0, 1).$$

We only have to confirm the conditions on the asymptotic behaviour of the derivatives. It is easy to extend the argument of Lemma 1 to obtain

$$\frac{\partial^j}{\partial t^j}\frac{\partial^k}{\partial u^k}f(t,u) = \begin{cases} \frac{\partial^k}{\partial u^k}\frac{f_m(u)}{m!}(\log 1/t)^m + \mathcal{O}\big((\log 1/t)^{m-1}\big), & j = 0, \\ (-1)^j(j-1)!\frac{\partial^k}{\partial u^k}\frac{f_m(u)}{(m-1)!}\frac{(\log 1/t)^{m-1}}{t^j} + \mathcal{O}\big(t^{-j}(\log 1/t)^{m-2}\big), & j \neq 0, \end{cases} \tag{8.1}$$

as $t \to 0^+$, uniformly in u. The definition of r by the implicit equation $n = -f_t(r(u), u)$ allows us to express $r'(u)$ and all higher derivatives in terms of derivatives of f by means of implicit differentiation: we have $r'(u) = -f_{tu}(r(u), u)/f_{tt}(r(u), u)$, and so forth. Thus it is possible to express the derivatives of R_n only in terms of $f(r(u), u)$ and its partial derivatives, for which we have the aforementioned asymptotic formula (8.1). Putting everything together, one obtains

$$\frac{\partial^k}{\partial u^k}R_n(u) = \frac{1}{m!}\left(\frac{\partial^k}{\partial u^k}f_m(u)\right)\left(\log\frac{1}{r(u)}\right)^m + \mathcal{O}\left(\left(\log\frac{1}{r(u)}\right)^{m-1}\right)$$

for $k \in \{1, 2, 3\}$, so (making use of (7.1))

$$R_n'(1) \sim \frac{f_m'(1)}{m!}(\log 1/r_0)^m \sim \frac{f_m'(1)}{m!}(\log n)^m = \frac{d-1}{2m!} \cdot \prod_{j=1}^m \frac{1}{\log p_j}(\log n)^m$$

and likewise

$$R_n''(1) \sim \frac{f_m''(1)}{m!}(\log 1/r_0)^m \sim \frac{f_m''(1)}{m!}(\log n)^m = \frac{(d-1)(d-5)}{12m!} \cdot \prod_{j=1}^m \frac{1}{\log p_j}(\log n)^m$$

and $R_n'''(u) = \mathcal{O}((\log n)^m)$ uniformly in u. Thus the conditions of Lemma 5 are satisfied, which proves asymptotic normality of the distribution. However, we still need to verify the asymptotic behaviour of the moments (which is not implied by weak convergence). To this end, we apply the saddle point method once again.

The generating function of the total sum of digits is $F_u(z,1) = \frac{\partial}{\partial u}F(z,u)\big|_{u=1}$, and the mean is given by

$$\mu_n = \frac{[z^n]F_u(z,1)}{[z^n]F(z,1)},$$

so we have to determine an asymptotic formula for the coefficients of $F_u(z,1)$. Cauchy's integral formula,

$$[z^n]F_u(z,1) = \frac{1}{2\pi i}\oint_{\mathcal{C}} F_u(z,1)\frac{dz}{z^{n+1}},$$

and the change of variables $z = e^{-t} = e^{-(r_0+i\tau)}$ (where r_0 satisfies the saddle point equation as before) yields

$$[z^n]F_u(z,1) = \frac{1}{2\pi}\int_{-\pi}^{\pi}\exp(nr_0 + f(r_0 + i\tau, 1) + in\tau)\,f_u(r_0 + i\tau, 1)d\tau.$$

Thus,

$$[z^n]F_u(z,1) - f_u(r_0,1)[z^n]F(z,1)$$
$$= \frac{1}{2\pi}\int_{-\pi}^{\pi}\exp(nr_0 + f(r_0 + i\tau, 1) + in\tau)\,(f_u(r_0 + i\tau, 1) - f_u(r_0,1))dt.$$

As we have seen in the proof of Lemma 4, the tails (the parts of the integral where $|\tau| \geq r(\log 1/r)^{-c}$) are negligible in that they only contribute an error term that goes faster to 0 than any power of $\log 1/r$. So we may focus on the central part, where we expand into a power series

$$\exp(nr_0 + f(r_0 + i\tau, 1) + in\tau)\left(f_u(r_0 + i\tau, 1) - f_u(r_0, 1)\right) = e^{nr_0 + f(r_0,1) - f_{tt}(r_0,1)\tau^2/2}$$

$$\times \left(if_{tu}(r_0,1)\tau - \frac{f_{ttu}(r_0,1)}{2}\tau^2 - i\frac{f_{tttu}(r_0,1)}{6}\tau^3 + \frac{4f_{ttt}(r_0,1)f_{tu}(r_0,1) + f_{ttttu}(r_0,1)}{24}\tau^4 + \cdots\right).$$

We continue in the same way as in the proof of Lemma 4 to evaluate the integral over the central region asymptotically by making use of the asymptotic formula (8.1). This eventually gives us

$$\mu_n = \frac{[z^n]F_u(z, 1)}{[z^n]F(z, 1)} = f_u(r_0, 1) + \frac{f_{tu}(r_0,1)f_{ttt}(r_0,1) - f_{tt}(r_0,1)f_{ttu}(r_0,1)}{f_{tt}(r_0,1)^2} + \mathcal{O}\left((\log 1/r_0)^{-(m-1)}\right).$$

Thus in particular

$$\mu_n = f_u(r_0, 1) + \mathcal{O}(1) = \frac{f'_m(1)}{m!}(\log 1/r_0)^m + \mathcal{O}\left((\log 1/r_0)^{m-1}\right)$$

$$= \frac{\kappa(d-1)}{2\log d}(\log n)^m + \mathcal{O}\left((\log n)^{m-1}\log\log n\right).$$

We repeat the process with $F_{uu}(z, u) + F_u(z, u)$ in the place of $F_u(z, u)$ to obtain an asymptotic formula for the second moment, which in turn yields formula

$$\sigma_n^2 = \frac{[z^n](F_{uu}(z, 1) + F_u(z, 1))}{[z^n]F(z, 1)} - \mu_n^2 = f_{uu}(r_0, 1) + f_u(r_0, 1) + \mathcal{O}\left((\log 1/r_0)^{m-1}\right)$$

$$= \frac{f'_m(1) + f''_m(1)}{m!}(\log 1/r_0)^m + \mathcal{O}\left((\log 1/r_0)^{m-1}\right)$$

$$= \frac{\kappa(d-1)(d+1)}{12\log d}(\log n)^m + \mathcal{O}\left((\log n)^{m-1}\log\log n\right).$$

for the variance. This completes our proof. $\qquad\square$

9. Conclusion

We obtained an asymptotic formula for the number of representations of an integer n in a multi-base system with given bases $p_1, p_2, \ldots, p_m$, which are equivalent to partitions into elements of the set

$$\mathcal{S} = \{p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_m^{\alpha_m} : \alpha_i \in \mathbb{N}\cup\{0\}\}.$$

Moreover, we proved central limit theorems for three very natural parameters: the sum of digits (corresponding to the length of a partition), the Hamming weight (corresponding to the number of distinct parts of a partition), and the number of occurrences of a given digit. There are many more parameters that could be studied; to give one further example, the probablilty that the digit associated with a given element $s \in \mathcal{S}$ in a random multi-base representation of n is equal to b for some $b \in \{0, 1, \ldots, d-1\}$ is $1/d$ in the limit as $n \to \infty$, as one would heuristically expect. It is not difficult to adapt our saddle point approach to this problem, the generating function being

$$z^{bs}\prod_{\substack{h\in\mathcal{S}\\h\neq s}}\frac{1 - z^{hd}}{1 - z^h}$$

in this case. As it was already mentioned in Section 2, it would also be possible to extend our results to other digit sets.

References

[1] Roberto Avanzi, Vassil Dimitrov, Christophe Doche, and Francesco Sica, *Extending scalar multiplication using double bases*, Advances in Cryptology—ASIACRYPT 2006, Lecture Notes in Comput. Sci., vol. 4284, Springer, Berlin, 2006, pp. 130–144.

[2] Valérie Berthé and Laurent Imbert, *Diophantine approximation, Ostrowski numeration and the double-base number system*, Discrete Mathematics and Theoretical Computer Science **11:1** (2009), 153–172.

[3] Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart, *Elliptic curves in cryptography*, London Mathematical Society Lecture Note Series, vol. 265, Cambridge University Press, 1999.

[4] Henri Cohen, *Number theory. vol. II. analytic and modern tools*, Graduate Texts in Mathematics, vol. 240, Springer, New York, 2007.

[5] Vassil Dimitrov, Laurent Imbert, and Pradeep K. Mishra, *The double-base number system and its application to elliptic curve cryptography*, Math. Comp. **77** (2008), no. 262, 1075–1104.

[6] Vassil S. Dimitrov, Graham A. Jullien, and William C. Miller, *Theory and applications of the double-base number system*, IEEE Transactions on Computers **48** (1999), 1098–1106.

[7] Philippe Flajolet, Xavier Gourdon, and Philippe Dumas, *Mellin transforms and asymptotics: Harmonic sums*, Theoret. Comput. Sci. **144** (1995), 3–58.

[8] Philippe Flajolet and Robert Sedgewick, *Analytic combinatorics*, Cambridge University Press, Cambridge, 2009.

[9] Daniel M. Gordon, *A survey of fast exponentiation methods*, J. Algorithms **27** (1998), 129–146.

[10] Peter J. Grabner and Clemens Heuberger, *On the number of optimal base 2 representations of integers*, Des. Codes Cryptogr. **40** (2006), no. 1, 25–39.

[11] Clemens Heuberger and Daniel Krenn, *Analysis of width-w non-adjacent forms to imaginary quadratic bases*, J. Number Theory **133** (2013), no. 5, 1752–1808.

[12] _____, *Optimality of the width-w non-adjacent form: General characterisation and the case of imaginary quadratic bases*, J. Théor. Nombres Bordeaux **25** (2013), no. 2, 353–386.

[13] Hsien-Kuei Hwang, *Limit theorems for the number of summands in integer partitions*, J. Combin. Theory Ser. A **96** (2001), no. 1, 89–126.

[14] Donald E. Knuth, *Seminumerical algorithms*, third ed., The Art of Computer Programming, vol. 2, Addison-Wesley, 1998.

[15] Daniel Krenn, Dimbinaina Ralaivaosaona, and Stephan Wagner, *On the number of multi-base representations of an integer*, 25th International Conference on Probabilistic, Combinatorial, and Asymptotic Methods for the Analysis of Algorithms (AofA'14), DMTCS-HAL Proceedings, vol. BA, 2014, pp. 229–240.

[16] Daniel Krenn, Jörg Thuswaldner, and Volker Ziegler, *On linear combinations of units with bounded coefficients and double-base digit expansions*, Monatsh. Math. **171** (2013), no. 3–4, 377–394.

[17] Kurt Mahler, *On a special functional equation*, J. London Math. Soc. **15** (1940), 115–123.

[18] Pradeep Kumar Mishra and Vassil Dimitrov, *A combinatorial interpretation of double base number system and some consequences*, Adv. Math. Commun. **2** (2008), no. 2, 159–173.

[19] Atsuko Miyaji, Takatoshi Ono, and Henri Cohen, *Efficient elliptic curve exponentiation*, Information and communications security. 1st international conference, ICICS '97, Beijing, China, November 11–14, 1997. Proceedings (Yongfei Han, Tatsuaki Okamoto, and Sihan Qing, eds.), Lecture Notes in Comput. Sci., vol. 1334, Springer-Verlag, 1997, pp. 282–290.

[20] François Morain and Jorge Olivos, *Speeding up the computations on an elliptic curve using addition-subtraction chains*, RAIRO Inform. Théor. Appl. **24** (1990), 531–543.

[21] *The On-Line Encyclopedia of Integer Sequences*, http://oeis.org, 2015.

[22] William Barry Pennington, *On Mahler's partition problem*, Ann. of Math. (2) **57** (1953), 531–546.

[23] Vladimir Yu. Protasov, *Asymptotics of the partition function*, Mat. Sb. **191** (2000), no. 3, 65–98.

[24] _____, *On the problem of the asymptotics of the partition function*, Mat. Zametki **76** (2004), no. 1, 151–156.

[25] George W. Reitwiesner, *Binary arithmetic*, Advances in Computers, Vol. 1, Academic Press, New York, 1960, pp. 231–308.

[26] Bruce Reznick, *Some binary partition functions*, Analytic number theory (Allerton Park, IL, 1989), Progr. Math., vol. 85, Birkhäuser Boston, Boston, MA, 1990, pp. 451–477.

[27] Jerome A. Solinas, *Efficient arithmetic on Koblitz curves*, Des. Codes Cryptogr. **19** (2000), 195–249.

Daniel Krenn, Institute of Analysis and Computational Number Theory (Math A), Graz University of Technology, Steyrergasse 30, 8010 Graz, Austria
E-mail address: math@danielkrenn.at *or* krenn@math.tugraz.at

Dimbinaina Ralaivaosaona, Department of Mathematical Sciences, Stellenbosch University, Private Bag X1, Matieland 7602, South Africa
E-mail address: naina@sun.ac.za

Stephan Wagner, Department of Mathematical Sciences, Stellenbosch University, Private Bag X1, Matieland 7602, South Africa
E-mail address: swagner@sun.ac.za