ON THE NUMBER OF MULTI-BASE REPRESENTATIONS OF AN INTEGER

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 is usually redundant, which means that each integer can have multiple different digit expansions. 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 and the Hamming weight of a random representation.

1. Introduction

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. Beside 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, and thus making 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 [19] 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 [24]. Generalizations in that direction can be found in [3,9,18,25].

A different way to get a better running time is to use double-base and multi-base numeral systems, which usually leads to redundancy as well. In a *multi-base representation of* n (or *multi-base expansion*), a positive integer n is expressed as a finite sum

$$n = \sum_{i=1}^{I} a_i B_i, \tag{1}$$

such that the following holds.

- The a_i (called *digits*) are taken from a fixed finite *digit set* (here, we will be using the canonical digit set $\{0, 1, \dots, d-1\}$ for some fixed integer $d \geq 2$).
- The B_i are in increasing order (i.e., $B_1 < B_2 < \cdots < B_I$) and taken from the set

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

Date: August 29, 2014.

2010 *Mathematics Subject Classification.* ???

Key words and phrases. multi-base representations, asymptotic formula, partitions.

Daniel Krenn is supported by the Austrian Science Fund (FWF): P24644 and by the Austrian Science Fund (FWF): W1230, Doctoral Program "Discrete Mathematics".

This material is based upon work supported by the National Research Foundation of South Africa under grant number 70560.

[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.

The $p_1, \ldots, p_m$ are called the *bases* (in our setting, these are fixed coprime positive integers).

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 digits at least 0 and 1), each positive integer has a double-base representation, cf. Berthé and Imbert [2]. When using general bases, less is known on the existence, cf. Krenn, Thuswaldner and Ziegler [15] 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 next question to ask is: How many representations does each integer have?

This question has also already been studied for redundant single-base representations; see Protasov [22, 23] for recent results involving non-negative digits. 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 a 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, 24]).

In the following, we will study 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).

Let us start with the double-base system with 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 p, i.e., representations of the form

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

with non-negative integers n_i. 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 [16]. By studying Mordell's functional equation, he obtained

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

The much more precise result

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

was derived by Pennington [21]. The error term in the previous asymptotic formula exhibits a periodic fluctuation.

For further reference, see A005704 in the On-Line Encyclopedia of Integer Sequences [20] for more information and see also [5, 17] for the connection to double-base systems.

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 $(p_i, p_j) = 1$ for $i \neq j$. As our first main theorem, we prove an asymptotic formula for the number of representations of n of the form (1). It will be convenient to use the abbreviation

$$\kappa = \frac{\log d}{m!}\prod_{i=1}^{m}\frac{1}{\log p_i}.$$

Theorem 1. *If $m \geq 3$, then the number $P(n)$ of distinct multi-base representations of n of the form (1) 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

$$\begin{aligned} C_0 &= \kappa, \\ C_1 &= -m(m-1)\kappa, \\ C_2 &= \kappa m\Big(1 + \tfrac{1}{2}\sum_{i=1}^{m} \log p_i - \tfrac{1}{2}\log d - \log(\kappa m)\Big). \end{aligned}$$

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

Theorem 2. *If $m = 2$, then the number $P(n)$ of distinct multi-base representations of n of the form (1) 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 numbers, and

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

Moreover, we study the distribution of two natural parameters in random multi-base representations, namely the sum of digits, i.e. $a_1 + a_2 + \cdots + a_I$ in the notation of (1), and the Hamming weight (the number of non-zero coefficients a_i):

Theorem 3. *The sum of digits in a random multi-base representation of n of the form (1) 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 4. *The Hamming weight of a random multi-base representation of n of the form (1) 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.

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 3 and the appendix for details). For the asymptotic analysis of the various harmonic sums that occur, we apply the classical Mellin transform technique, see [7]. We remark that our approach would also allow us to prove central limit theorems for other parameters as, for instance, the number of occurrences of a fixed digit.

2. The Generating Function

We start with a generating function for our problem. Consider the set

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

which is exactly the monoid that is freely generated by p_1, p_2, …, 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

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

Likewise, we have the following generating function where the second variable marks the Hamming weight (number of non-zero digits, or equivalently number of distinct parts in a partition):

$$G(z,u) = \prod_{h\in\mathcal{S}} \left(1 + uz^h + uz^{2h} + \cdots + uz^{(d-1)h}\right) = \prod_{h\in\mathcal{S}} \left(1 + uz^h \frac{1-z^{(d-1)h}}{1-z^h}\right). \tag{3}$$

Obviously, $F(z,1) = G(z,1)$. 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 following section. We will also need an asymptotic expansion in the central region. To this end, we define the two functions

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

and

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

Lemma 5. *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 $a_1(u)$, $a_2(u)$, …, $a_m(u)$ with*

$$a_m(u) = \log(1 + u + \cdots + u^{d-1}) \prod_{k=1}^{m} \frac{1}{\log p_k},$$

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

$$f(t,u) = \frac{a_m(u)}{m!}(\log 1/t)^m + \frac{a_{m-1}(u)}{(m-1)!}(\log 1/t)^{m-1} + \cdots + a_1(u)(\log 1/t) + \mathcal{O}(1).$$

Moreover,

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

and

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

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

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

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

(2) *Likewise, there exist (real-)analytic functions $b_1(u), b_2(u), \ldots, b_m(u)$ with*

$$b_m(u) = \log(1 + (d-1)u) \prod_{k=1}^{m} \frac{1}{\log p_k},$$

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

$$g(t,u) = b_m(u)(\log 1/t)^m + b_{m-1}(u)(\log 1/t)^{m-1} + \cdots + b_1(u)(\log 1/t) + \mathcal{O}(1).$$

Moreover,

$$\frac{\partial}{\partial t} g(t,u) = -\frac{m b_m(u)}{t}(\log 1/t)^{m-1} + \mathcal{O}\big(t^{-1}(\log 1/t)^{m-2}\big)$$

and

$$\frac{\partial^2}{\partial t^2} g(t,u) = \frac{m b_m(u)}{t^2}(\log 1/t)^{m-1} + \mathcal{O}\big(t^{-2}(\log 1/t)^{m-2}\big).$$

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

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

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

Proof. See Appendix A. ∎

3. 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 (2) and (3), which is done in the following sequence of lemmas. First of all, let us introduce some notation: for $x > 0$, we write $\mathcal{S}(x)$ for $\mathcal{S} \cap [1, 1/x] = \{h \in \mathcal{S}, hx \le 1\}$. It is straightforward to prove that

$$|\mathcal{S}(x)| = \frac{(\log 1/x)^m}{m! \prod_{j=1}^m \log p_j} + \mathcal{O}\big((\log 1/x)^{m-1}\big). \tag{4}$$

as $x \to 0^+$.

Lemma 6. *Let u be in the interval $[\frac{1}{2}, 2]$, and let $z = e^{-x+2\pi i y}$ with $x > 0$ and $y \in [-\frac{1}{2}, \frac{1}{2}]$. There exists an absolute constant C such that*

$$\frac{F(z,u)}{F(|z|,u)} \le \exp\Big(-C \sum_{h \in \mathcal{S}(x)} \|hy\|^2\Big)$$

and

$$\frac{G(z,u)}{G(|z|,u)} \le \exp\Big(-C \sum_{h \in \mathcal{S}(x)} \|hy\|^2\Big),$$

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

Proof. See Appendix B. ∎

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

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

For sufficiently small x, we have the following estimates for Σ:

(a) *If $|y| \le x/2$, then $\Sigma \ge A_1 (y/x)^2 (\log(1/x))^{m-1}$ for some constant A_1 (that only depends on m and the set of bases $\{p_1, p_2, \ldots, p_m\}$),*
(b) *If $|y| \ge x/2$, then $\Sigma \ge A_2 (\log(1/x))^{m-1}$ for some 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 x:

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

Proof. See Appendix C. ∎

4. 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 $F(z,u)$ and $G(z,u)$. 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 8. *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*

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

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*

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

uniformly in u.

(Sketch). Cauchy's integral formula gives us

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

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 this becomes

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

Now we choose r to be the saddle point, as in the statement of the lemma, so that the Taylor expansion in the central region becomes

$$nr + f(r+i\tau,u) + in\tau = nr + f(r,u) - f_{tt}(r,u)\frac{\tau^2}{2} + \mathcal{O}\Big(|\tau|^3 \sup_{|y|\leq\tau} |f_{ttt}(r+iy,u)|\Big). \tag{5}$$

Lemma 5 shows that r is of order $(\log n)^{m-1}/n$. Now we split the integral into the central part, where $|\tau| \leq r(\log 1/r)^{-2(m-1)/5}$, and the rest. In the central region, the error term in (5) is $\mathcal{O}(\log(1/r)^{-(m-1)/5})$ by Lemma 5, and we can complete the tails to get a Gaussian integral. The remaining parts of the integral are estimated by means of Lemmas 6 and 7. If $m > 2$, parts (a) and (b) of Lemma 7 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.

Putting everything together, one arrives at

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

and the proof for $G(z,u)$ is analogous. ∎

5. The Number of Representations

It is straightforward now to prove Theorem 1 and Theorem 2 by specialising $u = 1$ in Lemma 8, which gives us

$$P(n) = [z^n]F(z,1) \sim \frac{1}{\sqrt{2\pi f_{tt}(r,1)}} e^{nr+f(r,1)},$$

where r is given by the saddle point equation $n = -f_t(r,1)$. Making use of Lemma 5, we get

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

which readily gives us

$$\log 1/r = \log n - (m-1)\log\log n - \log\frac{a_m(1)}{(m-1)!} + \mathcal{O}\left(\frac{\log\log n}{\log n}\right)$$

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

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

and Lemma 5 also yields

$$\begin{aligned} f(r,1) &= \frac{a_m(1)}{m!}(\log 1/r)^m + \frac{a_{m-1}(1)}{(m-1)!}(\log 1/r)^{m-1} + \mathcal{O}\left((\log n)^{m-2}\right) \\ &= \frac{a_m(1)}{m!}(\log n)^m\left(1 - \frac{m(m-1)}{\log n}\log\log n - \frac{m}{\log n}\log\frac{a_m(1)}{(m-1)!} + \mathcal{O}\left(\frac{\log\log n}{(\log n)^2}\right)\right) \\ &\quad + \frac{a_{m-1}(1)}{(m-1)!}(\log n)^{m-1} + \mathcal{O}\left((\log n)^{m-2}\log\log n\right). \end{aligned}$$

Since $a_m(1)/m! = \kappa$ and $a_{m-1}(1)/(m-1)! = \kappa m(\sum_{i=1}^m \log p_i - \log d)/2$, this readily proves Theorem 1 (note that the factor $f_{tt}(r,1)$ only contributes $\mathcal{O}(\log n)$ to $\log P(n)$). To get the more precise formula (Theorem 2) in the case $m = 2$, we only need to expand a little further. In principle, it would be possible to obtain similar, more precise asymptotic formulas (in terms of $\log n$ and $\log\log n$) for all $m \geq 2$, but the expressions become very lengthy.

6. Sum of Digits and Hamming Weight

The central limit theorems for the sum of digits and the Hamming weight (Theorems 3 and 4) now follow from a general version of the quasi-power theorem (see [8, Theorem IX.13]); we only explain how the asymptotic formulas for mean and variance are obtained. We restrict ourselves to the case of the sum of digits, since the situation for the Hamming weight is similar. Recall the bivariate generating function

$$F(z,u) = \prod_{h\in\mathcal{S}} \frac{1-(uz^h)^d}{1-uz^h}.$$

In order to obtain the average sum of digits in a random representation of n, we differentiate with respect to u and set $u = 1$ as usual: This yields

$$\mu_n = \frac{1}{P(n)}[z^n]\frac{\partial}{\partial u}F(z,u)\Big|_{u=1} = \frac{1}{P(n)}[z^n]F(z,1)\sum_{h\in S}\left(\frac{z^h}{1-z^h} - \frac{dz^{dh}}{1-z^{dh}}\right),$$

which gives us the integral representation

$$\mu_n = \frac{1}{2\pi i P(n)}\oint_{\mathcal{C}} F(z,1)\sum_{h\in S}\left(\frac{z^h}{1-z^h} - \frac{dz^{dh}}{1-z^{dh}}\right)\frac{dz}{z^{n+1}}.$$

Again it is convenient to define a function

$$J(t) = \sum_{h\in S}\left(\frac{e^{-ht}}{1-e^{-ht}} - \frac{de^{-dht}}{1-e^{-dht}}\right).$$

We use the saddle point method as in Section 4 to estimate $P(n)\Big(\mu_n - J(r)\Big)$, where r is defined as in the statement of Lemma 8 for $u = 1$. We have

$$P(n)\Big(\mu_n - J(r)\Big) = \frac{1}{2\pi}\int_{-\pi}^{\pi} \exp\Big(nr + f(r+i\tau,1) + in\tau\Big)\Big(J(r+i\tau) - J(r)\Big)d\tau.$$

As in Section 4, we can approximate this integral by an integral over a small interval around zero, with an error term that is smaller than any power of $\log 1/r$. Making use of the same Mellin transform approach as in the proof of Lemma 5, one verifies easily that the term $J(r+i\tau) - J(r)$ is of order at most $(\log 1/r)^m$, and this estimate holds uniformly for $|\tau| \le \pi$.

Let now $c > 0$ be a constant satisfying the inequalities $3(m-1)/7 < c < (m-1)/2$. For $|\tau| \le r(\log 1/r)^{-c}$, by using more terms in the Taylor approximation of $f(r+i\tau,1)$ we get

$$e^{f(r+i\tau,1)-f(r,1)+in\tau} = e^{-f_{tt}(r,1)\frac{\tau^2}{2}}\left(1 - if_{ttt}(r,1)\frac{\tau^3}{6} + \mathcal{O}\Big((\log 1/r)^{2(m-1)-6c}\Big)\right).$$

Similarly,

$$J(r+i\tau) = J(r) + iJ_t(r)\tau - J_{tt}(r)\frac{t^2}{2} + \mathcal{O}\Big((\log 1/r)^{m-1-3c}\Big).$$

We multiply the two expansions and complete the tails of the integral as we did in the proof of Lemma 8. Evaluating the resulting integrals yields

$$P(n)\Big(\mu_n - J(r)\Big) = P(n)\left(\frac{f_{ttt}(r,1)J_t(r) - f_{tt}(r,1)J_{tt}(r)}{2(f_{tt}(r,1))^2} + \mathcal{O}\Big((\log 1/r)^{3(m-1)-7c}\Big)\right),$$

which in turn implies

$$\mu_n = J(r) + \frac{f_{ttt}(r,1)J_t(r) - f_{tt}(r,1)J_{tt}(r)}{2(f_{tt}(r,1))^2} + \mathcal{O}\Big((\log 1/r)^{3(m-1)-7c}\Big). \tag{6}$$

Here, we are also using the asymptotic formula for $P(n)$ from Lemma 8. Similarly, we also have

$$P(n)\sigma_n^2 = [z^n]\frac{\partial^2}{\partial u^2}F(z,u)\Big|_{u=1} + P(n)\mu_n(1-\mu_n).$$

If we set

$$L(t) = \sum_{h\in S}\left(\frac{e^{-ht}}{(1-e^{-ht})^2} - \frac{d^2e^{-dht}}{(1-e^{-dht})^2}\right),$$

then, using the estimate (6), we get the asymptotic formula

$$\sigma_n^2 = L(r) + \mathcal{O}\Big((\log 1/r)^{m-1} + (\log 1/r)^{4m-7c-3}\Big) \tag{7}$$

for the variance.

Finally, asymptotics for $J(r)$ and $L(r)$ in (6) and (7) are obtained by the same Mellin transform approach as in Lemma 5 again to obtain the formulas for mean and variance in Theorem 3.

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), no. 1-2, 3–58, Special volume on mathematical analysis of algorithms.

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, 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.
16. Kurt Mahler, *On a special functional equation*, J. London Math. Soc. **15** (1940), 115–123.
17. 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.
18. 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.
19. F. Morain and J. Olivos, *Speeding up the computations on an elliptic curve using addition-subtraction chains*, RAIRO Inform. Théor. Appl. **24** (1990), 531–543.
20. *The On-Line Encyclopedia of Integer Sequences*, `http://oeis.org`, 2014.
21. W. B. Pennington, *On Mahler's partition problem*, Ann. of Math. (2) **57** (1953), 531–546.
22. Vladimir Yu. Protasov, *Asymptotics of the partition function*, Mat. Sb. **191** (2000), no. 3, 65–98.
23. ———, *On the problem of the asymptotics of the partition function*, Mat. Zametki **76** (2004), no. 1, 151–156.
24. George W. Reitwiesner, *Binary arithmetic*, Advances in Computers, vol. 1, Academic Press, New York, 1960, pp. 231–308.
25. Jerome A. Solinas, *Efficient arithmetic on Koblitz curves*, Des. Codes Cryptogr. **19** (2000), 195–249.

Appendix A. Proof of Lemma 5

We only prove the first part, the second being analogous. 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

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

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

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

which exhibits the pole at 0 with residue $\log(1+u+u^2+\cdots+u^{d-1})$, and 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

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

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 negative values of σ (after suitable integration by parts) as well as negative τ (by symmetry). Therefore, we have

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

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

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

$$D(s) = \prod_{i=1}^m \frac{1}{1 - p_i^{-s}}.$$

Therefore, the Mellin transform of $f(t,u)$, which is given by $Y(s,u)D(s)$, has a pole of order $m+1$ at $s = 0$. Since $Y(s,u) \sim s^{-1}\log(1 + u + \cdots + u^{d-1})$ and $(1 - p_i^{-s}) \sim 1/(s\log p_i)$ as $s \to 0$, the Laurent series of $Y(s,u)D(u)$ has the form

$$\frac{a_m(u)}{s^{m+1}} + \frac{a_{m-1}(u)}{s^m} + \cdots + \frac{a_1(u)}{s^2} + \frac{a_0(u)}{s} + \cdots,$$

with $a_m(u)$ 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], we shift the line of integration, picking 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

$$\frac{a_m(u)}{m!}(\log 1/t)^m + \frac{a_{m-1}(u)}{(m-1)!}(\log 1/t)^{m-1} + \cdots + a_1(u)(\log 1/t) + a_0(u).$$

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 $\log p_j$ $(1 \le j \le m)$. 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

$$\prod_{\substack{r=1\\ r\neq j}}^{m} \frac{1}{|1-p_r^{2\pi ik/\log p_j}|}$$

is bounded above by a power of k. 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 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.

Appendix B. Proof of Lemma 6

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

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

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

$$\frac{|1+aw|^2}{(1+a|w|)^2} \le 1-\frac{1}{25}(|w|-\operatorname{Re} w) \le \exp\left(-\frac{1}{25}(|w|-\operatorname{Re} w)\right) \tag{8}$$

and

$$\frac{|1+aw+aw^2|^2}{(1+a|w|+a|w|^2)^2} \le 1-\frac{1}{169}(|w|-\operatorname{Re} w) \le \exp\left(-\frac{1}{169}(|w|-\operatorname{Re} w)\right). \tag{9}$$

Now let d be even, set $a=u$ and $w=z^h$, so that (8), together with the triangle inequality, yields

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

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

$$\begin{aligned}
F(z,u) &\le F(|z|,u)\exp\left(-\frac{1}{50}\sum_{h\in\mathcal{S}}\left(|z|^h-\operatorname{Re}(z^h)\right)\right) = F(|z|,u)\exp\left(-\frac{1}{50}\sum_{h\in\mathcal{S}} e^{-hx}\left(1-\cos(2\pi hy)\right)\right) \\
&\le F(|z|,u)\exp\left(-\frac{1}{50e}\sum_{h\in\mathcal{S}(x)}(1-\cos(2\pi hy))\right) \le F(|z|,u)\exp\left(-\frac{8}{50e}\sum_{h\in\mathcal{S}(x)}\|hy\|^2\right),
\end{aligned}$$

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 (9) (with $a = 1$ and $w = uz^h$) and use the triangle inequality in the following way:

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

For the generating function $G(z, u)$, the reasoning is fully analogous, but we also have to use (9) with $a = u$ and $w = z^h$.

Appendix C. Proof of Lemma 7

We start with the case that $|y| \leq x/2$, which implies $|hy| \leq \frac{1}{2}$ for all $h \in \mathcal{S}(x)$. Then we have

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

for any $\rho > 0$. If we take ρ sufficiently small and apply the asymptotic formula in (4), we obtain estimate (a).

Now assume that $|y| \geq x/2$. If $|y| \leq x^{2/3}$, then we have $\log|1/y| \geq \frac{2}{3}\log(1/x)$, and essentially the same idea works again:

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

and formula (4) can be applied again to obtain (a).

We are left with the case that $|y| > x^{2/3}$. By Dirichlet's approximation theorem, there exists a rational number a/q (a, q coprime) such that $q \leq x^{-2/3}$ and

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

In view of the assumption that $x^{2/3} < |y| \leq \frac{1}{2}$, we know that $q \neq 1$. Let us now distinguish two cases:

- If $q \in \mathcal{S}$, then write $q = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_m^{\alpha_m}$. We have
$$A = \max(\alpha_1, \alpha_2, \ldots, \alpha_m) \geq \frac{\log q}{\log(p_1p_2\cdots p_m)}.$$
Suppose that $\alpha_i = A$. Then for any $h_1 = p_1^{\beta_1}p_2^{\beta_2}\cdots p_m^{\beta_m} \in \mathcal{S}$ with $0 \leq \beta_i < \alpha_i = A$, ah_1/q is not an integer and thus $\|ah_1/q\| \geq 1/q$. Using (4) (applied to the bases $p_1, p_2, \ldots, p_m$ excluding p_i), we find that for some constant c_1, there exist at least $c_1(\log q)(\log 1/x)^{m-1}$ elements $h_1 \in \mathcal{S}$ with $h_1 \leq x^{-1/3}$ and $\|ah_1/q\| \geq 1/q$.
- If $q \notin \mathcal{S}$, then we clearly have $\|h_1a/q\| \geq 1/q$ for all $h_1 \in \mathcal{S}$, so the same statement as in the first case holds again.

Now 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 the pigeonhole principle, we can choose one of these intervals (I_j, say) such that for at least $c_1/c_2(\log 1/x)^{m-1}$ distinct numbers $h_1 \in \mathcal{S}$ with $h_1 \leq x^{-1/3}$, $\|h_1a/q\|$ lies in this interval, i.e., $1/(2p_1^{j+1}) \leq \|h_1a/q\| \leq 1/(2p_1^j)$. Now we have

$$\left\|\frac{h_1p_1^ja}{q}\right\| = p_1^j\left\|\frac{h_1a}{q}\right\| \geq \frac{1}{2p_1},$$

which means that we have at least $c_1/c_2(\log 1/x)^{m-1}$ elements $h = h_1p_1^j \in \mathcal{S}$ such that

- $h = h_1p_1^j \leq h_1q \leq x^{-1/3}x^{-2/3} = \frac{1}{x}$, so that $h \in \mathcal{S}(x)$,

- $\|hy\| \geq \|\frac{ha}{q}\| - \frac{x^{2/3}h}{q} \geq \frac{1}{2p_1} - \frac{x^{2/3}h_1 q}{q} \geq \frac{1}{2p_1} - x^{1/3} \geq \frac{1}{3p_1}$ (for sufficiently small x).

Therefore,

$$\Sigma \geq \frac{c_1}{c_2}\left(\log\frac{1}{x}\right)^{m-1} \cdot \left(\frac{1}{3p_1}\right)^2 = A_2\left(\log\frac{1}{x}\right)^{m-1}$$

for $A_2 = c_1/(9c_2p_1^2)$ if x is sufficiently small.

It remains to prove statement (c) in the case $m = 2$. Choose some $\epsilon \in (0, \delta)$, set $L = \lfloor(1-\epsilon)\log_{p_1} 1/x\rfloor$ and define, for a positive integer M, the set

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

Note that $\|p_1^j v\| \geq p_1^{-2}$ unless the $(j+1)$-th and the $(j+2)$-th digit after the decimal point in the p_1-adic expansion of v are either both 0 or both $p_1 - 1$. This means that for an element of $D(M)$, at least $L - M$ of the first $L+2$ digits have to be equal to the previous digit, from which it follows that the Lebesgue measure of $D(M)$ is at most

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

Here, $\binom{L+1}{j}$ is the number of ways to choose the "exceptional" digits; each digit that has to be equal to the previous one reduces the Lebesgue measure by a factor of p_1. Now for every $k \leq R = \lfloor\epsilon\log_{p_2} 1/x\rfloor$, we have $p_1^j p_2^k \leq x^{-1+\epsilon}\cdot x^{-\epsilon} = x^{-1}$ and $\|p_1^j p_2^k y\| \geq p_1^{-2}$ for at least M choices of $j \leq L$, unless $p_2^k y \bmod 1 \in D(M)$. It follows that

$$\Sigma = \sum_{h\in\mathcal{S}(x)}\|hy\|^2 \geq \sum_{j\leq L}\sum_{k\leq R}\|p_1^j p_2^k y\|^2 \geq (R+1)Mp_1^{-2} \geq \epsilon p_1^{-2} M\log 1/x,$$

except for y in the following set:

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

The map Φ_k defined by $\Phi_k(v) = p_2^k v \bmod 1$ is measure-preserving (with respect to the Lebesgue measure λ), i.e.,

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

where the implied constant only depends on p_1, p_2, M and ϵ. If we choose $M = Kp_1^2/\epsilon$, statement (c) follows with exceptional set $E = E(K, x)$.

Appendix D. Proof of Lemma 8

Here we give a more detailed account of our application of the saddle point method. 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 $z = e^{-t} = e^{-(r+i\tau)}$ to obtain

$$[z^n]F(z,u) = \frac{1}{2\pi}\int_{-\pi}^{\pi}\exp\Big(nr + f(r+it,u) + int\Big)dt. \tag{10}$$

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

$$n = -f_t(r,u). \tag{11}$$

Applying Lemma 5 to the right hand side of (11) we obtain

$$n = \frac{a_m(u)}{(m-1)!}\frac{(\log 1/r)^{m-1}}{r} + \mathcal{O}\Big((\log 1/r)^{m-2}\Big).$$

Hence, r admits the estimate

$$r(n,u) = \frac{a_m(u)}{(m-1)!}\frac{(\log n)^{m-1}}{n} + \mathcal{O}\Big((\log n)^{m-2}\log\log n\Big).$$

Now 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

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

For $|\tau| \le r|\log r|^{-c}$, using Taylor expansion and Lemma 5, we have

$$\begin{aligned} f(r+i\tau,u) &= f(r,u) + if_t(r,u)\tau - f_{tt}(r,u)\frac{\tau^2}{2} + \mathcal{O}\left(|\tau|^3 \sup_{|y|\le\tau}|f_{ttt}(r+iy,u)|\right) \\ &= f(r,u) + if_t(r,u)\tau - f_{tt}(r,u)\frac{\tau^2}{2} + \mathcal{O}\left((\log 1/r)^{m-1-3c}\right). \end{aligned}$$

Therefore, by the definition of r in (11), we have

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

Furthermore,

$$\begin{aligned} \int_{-r(\log 1/r)^{-c}}^{r(\log 1/r)^{-c}} \exp\Big(-f_{tt}(r,u)\frac{\tau^2}{2}\Big)d\tau &= \int_{-\infty}^{\infty}\exp\Big(-f_{tt}(r,u)\frac{\tau^2}{2}\Big)d\tau - 2\int_{r(\log 1/r)^{-c}}^{\infty}\exp\Big(-f_{tt}(r,u)\frac{\tau^2}{2}\Big)d\tau \\ &= \sqrt{\frac{2\pi}{f_{tt}(r,u)}} - 2\int_{r(\log 1/r)^{-c}}^{\infty}\exp\Big(-f_{tt}(r,u)\frac{\tau^2}{2}\Big)d\tau, \end{aligned}$$

and

$$\begin{aligned} \int_{r(\log 1/r)^{-c}}^{\infty}\exp\Big(-f_{tt}(r,u)\frac{\tau^2}{2}\Big)d\tau &\le \int_{r(\log 1/r)^{-c}}^{\infty}\exp\Big(-\frac{\tau}{2}f_{tt}(r,u)r(\log 1/r)^{-c}\Big)d\tau \\ &= \frac{2\exp\Big(-f_{tt}(r,u)r^2(\log 1/r)^{-2c}/2\Big)}{f_{tt}(r,u)r(\log 1/r)^{-c}} \\ &= \mathcal{O}\left(r(\log 1/r)^{m-1-c}e^{-K(\log 1/r)^{m-1-2c}}\right) \end{aligned}$$

for a constant $K > 0$. 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

$$I_0 = \frac{e^{nr+f(r,u)}}{\sqrt{2\pi f_{tt}(r,u)}}\Big(1+\mathcal{O}((\log 1/r)^{m-1-3c})\Big) = \frac{e^{nr+f(r,u)}}{\sqrt{2\pi f_{tt}(r,u)}}\Big(1+\mathcal{O}((\log n)^{-(m-1)/5})\Big). \quad (12)$$

It remains to show that the rest of the integral in (10) 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

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

Then

$$\begin{aligned} |I_1| &\le e^{nr+f(r,u)}\int_{r(\log 1/r)^{-c}}^{\pi}\exp\Big(\operatorname{Re}\Big(f(r+i\tau,u)-f(r,u)\Big)\Big)\,d\tau \\ &= e^{nr+f(r,u)}\int_{r(\log 1/r)^{-c}}^{\pi}\frac{|F(e^{-(r+i\tau)},u)|}{F(e^{-r},u)}\,d\tau. \end{aligned}$$

If $m \geq 3$ then we can use Lemma 6 and parts (a) and (b) of Lemma 7 to show that the integrand on the right hand side is $\mathcal{O}(\exp(-CA_1(\log 1/r)^{m-1-2c}))$ for $|\tau| \leq \pi r$ and $\mathcal{O}(\exp(-CA_2(\log 1/r)^{m-1}))$ otherwise, which immediately shows that

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

For $m = 2$, we need to be more careful. Again, part (a) of Lemma 7 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 6), and $\delta > 0$ such that $\delta < CA_2$ (A_2 as in Lemma 7).

If $y = -\tau/(2\pi)$ is not in the exceptional set $E(K,r)$ as defined in Lemma 7, then we have

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

By part (c) of Lemma 7, the set of τ-values for which this estimate does not hold has Lebesgue measure $\mathcal{O}(r^{1-\delta})$, and we have the estimate

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

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

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

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