ON THE MAXIMAL WEIGHT OF (P, Q)-ARY CHAIN PARTITIONS WITH BOUNDED PARTS

Filippo Disanto[1]
Dept. of Biology, Stanford University, Stanford, California
fdisanto@stanford.edu

Laurent Imbert[2]
LIRMM, CNRS, University of Montpellier, France
Laurent.Imbert@lirmm.fr

Fabrice Philippe
LIRMM, CNRS, University of Montpellier, France
Fabrice.Philippe@lirmm.fr

Received: 10/24/12, Revised: 10/16/13, Accepted: 5/16/14, Published: 8/5/14

Abstract

A (p, q)-ary chain is a special type of chain partition of integers with parts of the form $p^a q^b$ for some fixed integers p and q. In this note we are interested in the maximal weight of such partitions when their parts are distinct and cannot exceed a given bound m. Characterizing the cases where the greedy choice fails, we prove that this maximal weight is, as a function of m, asymptotically independent of $\max(p, q)$, and we provide an efficient algorithm to compute it.

1. Introduction

Let p, q be two fixed integers, and let $E = \{p^a q^b : (a, b) \in \mathbb{N}^2\}$ be endowed with the divisibility order, i.e., $x \succeq y$ if, and only if, $y \mid x$. A (p, q)-ary chain is a finite non-increasing sequence in E. For example $(72, 12, 4, 4, 1)$ is a $(2, 3)$-ary chain, whereas $(72, 12, 4, 3, 1)$ is not since $4 \not\succeq 3$. We define the *weight* of a (p, q)-ary chain as the sum of its terms:

$$w = \sum_{i \geq 1} p^{a_i} q^{b_i}, \quad \text{where } p^{a_i} q^{b_i} \succeq p^{a_{i+1}} q^{b_{i+1}} \text{ for } i \geq 1. \tag{1}$$

[1]This work was done during the first author' postdoctoral stay at the university of Montpellier. He wish to thank the french Agence Nationale de la Recherche for funding this research through the contract ANR-08-NANO-052 "BASTET".

[2]The second author was partly funded by the French Agence Nationale de la Recherche through the contract ANR-12-BS02 001 "CATREL".

Expansions of this type have been proposed and successfully used by Dimitrov et al. in the context of digital signal processing and cryptography under the name *double-base number system*. (For more details see [5, 4] and the references therein.)

From a different point of view, a (p, q)-ary chain can be seen as a partition of its weight, where the parts are restricted to the set E and constrained by a divisibility condition. Surprisingly, works on integer partitions with divisibility constraints on the parts are very scarce. Erdős and Loxton considered two types of such unconventional partitions, called chain and umbrella partitions [6], and obtained "*some rather weak estimates for various partition functions*." More recently, motivated by some theoretical questions behind Dimitrov's number system, the second and third authors refined some of Erdős and Loxton's earlier results in a paper entitled *strictly chained (p, q)-ary partitions* [7]. A strictly chained (p, q)-ary partition, or (p, q)-SCP for short, is a decreasing (p, q)-ary chain, i.e., it has distinct parts. The original motivation for the present work was to extend the results from [7] to the unconventional situation where the parts of a (p, q)-SCP can be either positive or negative. The results of such a study are expected to provide significant improvements for some cryptographic primitives, e.g., the computation of the multiple of a point on an elliptic curve. In this context the first, natural question that we tackle in the present paper is: "What is the maximal weight of a (p, q)-SCP whose parts are bounded by some given integer m?" Although the problem may seem elementary at first glance, we show that the answer is not so trivial. In particular, assuming $p < q$, we prove that this maximal weight asymptotically grows as $mp/(p - 1)$, independently of q.

If the first part is given, the heaviest (p, q)-SCP may be computed using a greedy strategy by successively taking the next greatest part satisfying the divisibility condition. Nevertheless, given a bound $m > 0$ on the parts, determining how to best select the first part is not immediate and the greedy approach fails in general. Indeed, we shall see that choosing the largest part less than or equal to m does not always provide a partition of maximal weight. These facts are established in Sections 2 and 3 among other preliminary definitions, examples, and results. The cases where the greedy choice fails are fully characterized in Section 4. Section 5 is devoted to the asymptotic behavior of the maximal weight as a function of m. Finally, in Section 6 we show how to compute a best choice for the first part, thus the maximal weight, in $O(\log \log m)$ steps.

2. Preliminaries

Let m be a positive integer, and let $G(m)$ denote the maximal weight of a (p, q)-SCP whose greatest part does not exceed m. For example, with $p = 2$ and $q = 3$, the first values of G are: 1, 3, 4, 7, 7, 10, 10, 15, 15, 15, 15, 22, 22, 22, 22, 31, 31, ...

In the following, we shall assume w.l.o.g. that $p < q$. Notice that the case $p = 1$ is irrelevant since $G(m)$ is simply the sum of all the powers of q less than or equal to m. More generally, and for the same reason, we shall consider that p and q are not powers of the same integer, or equivalently *multiplicatively independent*. As a direct consequence $\log_p q$ is irrational (see, e.g., [1, Theorem 2.5.7]). Under this assumption, the first values of $G(m)$ may be quickly computed with the help of the following formula.

Proposition 1. *For $m \in \mathbb{N}^*$, let $G(m)$ denote the largest integer that can be expressed as a strictly chained (p, q)-ary partition with all parts less than or equal to m. Assume that $G(m) = 0$ if $m \notin \mathbb{N}$. Then, we have $G(1) = 1$, and for $m > 1$*

$$G(m) = \max\left(G(m-1), 1 + pG(m/p), 1 + qG(m/q)\right). \tag{2}$$

Proof. Let λ be a partition of weight $G(m)$ whose parts are all less than or equal to m. First, notice that λ must contain part 1 by definition of $G(m)$. If $m \notin E$, then $G(m) = G(m-1)$. Otherwise, it suffices to observe that removing part 1 from λ produces a partition whose parts are all divisible by either p or q. $\square$

Computing $G(m)$ with relation (2) requires $O(\log m)$ steps in the worst case: Simply note that, for all m, in at most $p-1$ baby-steps, i.e., $G(m) = G(m-1)$, one gets an integer that is divisible by p. Formula (2) may also be adapted to compute both $G(m)$ and a (p, q)-SCP of such weight. Nevertheless, it does not give any idea about the asymptotic behavior of G. Moreover, we shall see in Section 6 how to compute $G(m)$ and a (p, q)-SCP of weight $G(m)$ in $O(\log \log m)$ steps.

A natural graphic representation for (p, q)-SCPs is obtained by mapping each part $p^a q^b \in E$ to the pair $(a, b) \in \mathbb{N}^2$. Indeed, with the above assumptions on p and q, the mapping $(a, b) \mapsto p^a q^b$ is one-to-one. Since the parts of a (p, q)-SCP are pairwise distinct by definition, this graphic representation takes the form of an increasing path in $\mathbb{N}^2$ endowed with the usual product order. This is illustrated in Figure 1 with the ten $(2, 3)$-SCPs containing exactly six parts and whose greatest part equals $72 = 2^3 3^2$. Note that a (p, q)-SCP with largest part $p^a q^b$ possesses at most $a + b + 1$ parts, and that there are exactly $\binom{a+b}{b}$ of them with a maximum number of parts.

With this representation in mind, one is easily convinced that the heaviest (p, q)-SCP with first part $p^a q^b$ looks like the top left (p, q)-SCP in Figure 1. This is formalized in the following lemma.

Lemma 1. *Given $a, b \in \mathbb{N}$, the heaviest (p, q)-SCP with first part $p^a q^b$ is the one whose parts are the elements of the set $\{q^i : 0 \le i < b\} \cup \{q^b p^i : 0 \le i \le a\}$.*

Proof. Consider a (p, q)-SCP $\lambda = (\lambda_i)_{i=1}^k$ with greatest part $\lambda_1 = p^a q^b$. Let $\lambda_i = p^{a_i} q^{b_i}$. If $a_i + b_i > b$ then define $\lambda'_i = p^{a_i+b_i-b} q^b$, otherwise let $\lambda'_i = q^{a_i+b_i}$. Note that $\lambda'_1 = p^a q^b$ again. Since sequence $(a_i + b_i)_{i=1}^k$ is decreasing, $(\lambda'_i)_{i=1}^k$ is also a

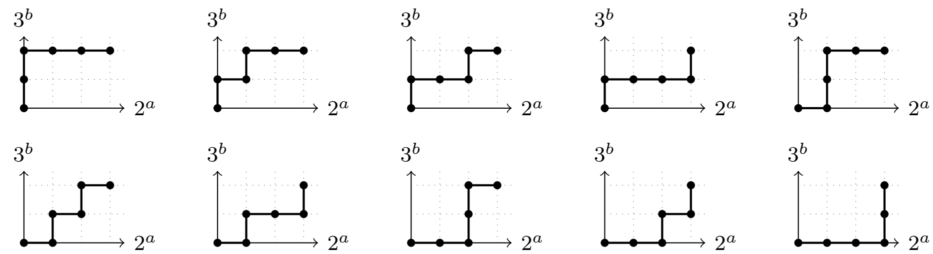

Figure 1: The set of $(2,3)$-SCPs with 6 parts and whose largest part equals $2^3 3^2 = 72$.

(p,q)-SCP. Since $p < q$ we have $\lambda'_i \geq \lambda_i$ for all i, with equality if, and only if, the parts in λ form a subset of $\{q^i : 0 \leq i < b\} \cup \{p^i q^b : 0 \leq i \leq a\}$. Therefore, the maximal weight is reached when taking the whole set, and only in this case. □

As a consequence, a (p,q)-SCP of weight $G(m)$ and whose parts do not exceed m is characterized by its greatest part only. Moreover, denoting by $p^a q^b$ this greatest part, we have $G(m) = h(a,b)$, where h is the mapping defined on $\mathbb{N}^2$ by

$$h(a,b) = \frac{q^b - 1}{q - 1} + \frac{p^{a+1} - 1}{p - 1} q^b. \tag{3}$$

Accordingly, the definition of G may be rewritten as

$$G(m) = \max_{P_m} h, \quad \text{where } P_m = \{(a,b) \in \mathbb{N}^2 : p^a q^b \leq m\}. \tag{4}$$

Finally observe that the greatest part of a (p,q)-SCP of weight $G(m)$ and whose parts do not exceed m must be a maximal element of $E \cap [0,m]$ for the divisibility order. Otherwise, the partition could be augmented by a part, resulting in a partition of larger weight. The next section is devoted to the set of these maximal elements.

3. On the Set Z_m

For convenience, let us denote by ρ the logarithmic ratio of q and p,

$$\rho = \frac{\log q}{\log p} > 1.$$

Since p and q are multiplicatively independent, ρ is irrational.

Let us further denote by Z_m the set of all maximal elements in $E \cap [0,m]$ for the divisibility order. Recall that $E = \{p^a q^b : (a,b) \in \mathbb{N}^2\}$, so that any element of E may also be written as $p^{a+b\rho}$. There are exactly $\lfloor \log_q m \rfloor + 1$ elements in Z_m, described in the following Lemma.

Lemma 2. *Let m be a positive integer. The following characterization holds:*

$$p^a q^b \in Z_m \ \textit{ if, and only if, } \ 0 \le b \le \lfloor \log_q m \rfloor \ \textit{ and } a = \lfloor \log_p m - b\rho \rfloor.$$

Proof. An element $p^a q^b$ of E is in Z_m if, and only if, a and b are non-negative, $p^a q^b \le m < p^{a+1} q^b$, and $p^a q^b \le m < p^a q^{b+1}$. Since $p < q$, the latter condition is superfluous. Checking that the former inequalities are equivalent to the Lemma's claim is immediate. $\square$

As a consequence, let us note for further use that

$$Z_{qm} = qZ_m \cup \{p^{\lfloor \rho + \log_p m \rfloor}\}, \tag{5}$$

$$Z_{pm} = \begin{cases} pZ_m & \text{if } \lfloor 1/\rho + \log_q m \rfloor = \lfloor \log_q m \rfloor, \\ pZ_m \cup \{q^{\lfloor \log_q m \rfloor + 1}\} & \text{otherwise.} \end{cases} \tag{6}$$

The elements of Z_m correspond exactly to the maximal integer points below or on the line of equation $a \log p + b \log q - \log m = 0$. An example is given in Figure 2. The corresponding values $p^a q^b$ and $h(a, b)$ are reported in Table 1.

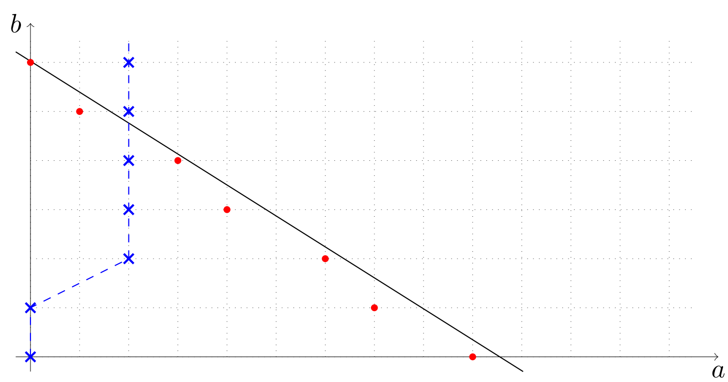

Figure 2: The set Z_{750} for $(p, q) = (2, 3)$, represented as all maximal integer points below the line of equation $x \log 2 + y \log 3 - \log 750 = 0$. The points along the dashed line correspond to the first values of the sequence ℓ defined in Theorem 1.

(a, b)	(0, 6)	(1, 5)	(3, 4)	(4, 3)	(6, 2)	(7, 1)	(9, 0)
$p^a q^b$	729	486	648	432	576	384	512
$h(a, b)$	1093	850	1255	850	1147	766	1023

Table 1: The elements of Z_{750} for $(p, q) = (2, 3)$, together with the corresponding values $p^a q^b$ and $h(a, b)$. Note that $G(750) = h(3, 4) = 1255$.

Further define z_m as the greatest integer of the form $p^a q^b$ less than or equal to m, that is,

$$z_m = \max Z_m.$$

Since $q^{\lfloor \log_q m \rfloor} \in Z_m$, we have $z_m \to \infty$ when $m \to \infty$. The next proposition goes one step further.

Proposition 2. *We have the following: $z_m \sim m$ when $m \to \infty$.*

Proof. Let $\hat{z}_m$ be the smallest integer of the form $p^a q^b$ greater than or equal to m. Thus we have $z_m \leq m \leq \hat{z}_m$. By a theorem of Tijdeman [13] we know that, for m large enough, there exists a constant $C > 0$ such that

$$\hat{z}_m - z_m < \frac{z_m}{(\log z_m)^C},$$

so that $0 \leq m - z_m < z_m/(\log z_m)^C$. □

From a greedy point of view, one might think that choosing z_m for the largest part of the (p,q)-SCP formed as in Lemma 1 yields a (p,q)-SCP of weight $G(m)$; in which case our asymptotics problem would be solved using the above proposition. Unfortunately, this is not true. In Table 1, we see for instance that $z_{750} = 729$, obtained for $(a,b) = (0,6)$, does not give a (p,q)-SCP of maximal weight. Instead, the maximal weight $G(750) = 1255$ is obtained for $(a,b) = (3,4)$. Hence, even if m is of the form $p^a q^b$, the first part of a (p,q)-SCP of maximal weight may be different from m. For instance $G(729) = 1255$ comes from a unique (p,q)-SCP whose first part is 648. In the next Section, we study the subset Y_m of Z_m, which yields the (p,q)-SCPs of maximal weight $G(m)$.

4. On the Set Y_m

According to (4), $G(m)$ is equal to $h(a,b)$ for some values a, b. First, notice that these values are not necessarily unique with respect to this property, because h is not necessarily one-to-one. For example, with $(p,q) = (2,3)$, observe from Table 1 that $h(1,5) = h(4,3) = 850$. Similarly, with $(p,q) = (2,5)$ one has $h(0,2) = h(4,0) = 31$.

Let Y_m be the set of all elements $p^a q^b$ in $E \cap [0,m]$ such that $h(a,b) = G(m)$. As already noticed, Y_m is a subset of Z_m. Next recall that $z_m = \max Z_m$ needs not be in Y_m. A particular relation between Y_m and z_m does however exist as proved in the next proposition.

Proposition 3. *For $m \in \mathbb{N}^*$, let $z_m = p^a q^b$. Then*

$$Y_m \subset \{p^i q^j \in Z_m : j \leq b\}. \qquad (7)$$

Proof. Using (3), we have

$$\begin{aligned}\frac{p-1}{p}\,h(a,b) &= \frac{p-1}{p}\,\frac{q^b-1}{q-1}+\frac{q^b}{p}(p^{a+1}-1)\\ &= p^aq^b - q^b\,\frac{q-p}{pq-p}-\frac{p-1}{p(q-1)},\end{aligned}$$

so that

$$h(a,b)=\frac{p}{p-1}\left(p^aq^b-rq^b\right)-\frac{1}{q-1},\quad \text{where } r=\frac{q-p}{pq-p}\in(0,1/p). \tag{8}$$

Note that $0<r<1/p$, because $pq-p>p(q-p)$. As a consequence, we have

$$h(a,b)>h(a',b') \quad \text{if, and only if,} \quad p^aq^b-p^{a'}q^{b'}>r(q^b-q^{b'}). \tag{9}$$

If $p^{a'}q^{b'}\in Z_m$ we have $z_m=p^aq^b>p^{a'}q^{b'}$. Hence $b'>b$ implies $h(a,b)>h(a',b')$, which concludes the proof. □

Geometrically, Proposition 3 tells us that the points $(a,b)\in\mathbb{N}^2$ such that $h(a,b)=G(m)$ cannot be located "above" or equivalently "left" of z_m. In particular, when $z_m=p^a$, we have $G(m)=h(a,0)=(p^{a+1}-1)/(p-1)$.

In Proposition 4, we will see that the set Y_m has at most two elements. Let us first focus on those elements of E that provide the heaviest (p,q)-SCP in a unique way, i.e., those for which $Y_{p^aq^b}=\{p^aq^b\}$. The following theorem shows that the corresponding points in $\mathbb{N}^2$ form an infinite area whose boundary is a particular sequence as illustrated in Figure 2.

Theorem 1. *There exists a sequence $\ell=(\ell_b)_{b\in\mathbb{N}}$ in $\mathbb{N}$ such that*

$$Y_{p^aq^b}=\{p^aq^b\} \quad \textit{if, and only if,} \quad a\geq \ell_b. \tag{10}$$

Moreover, the sequence ℓ is non-decreasing, unbounded, and satisfies $\ell_0=0$.

Proof. Let us first establish the following statements:

(i) For all $b\geq 0$, there exists $a\geq 0$ such that $p^aq^b\in Y_{p^aq^b}$.

(ii) If $p^aq^b\in Y_{p^aq^b}$ then, for all $k\geq 1$, $Y_{p^{a+k}q^b}=\{p^{a+k}q^b\}$.

Let $b\in\mathbb{N}$. As already seen, the mapping $(i,j)\mapsto p^iq^j$ is one-to-one. Therefore, we have $q^b-p^iq^j\geq 1$ for all $p^iq^j\in Z_{q^b}\setminus\{q^b\}$. Choose a such that

$$p^a\geq r(q^b-1),\quad \text{where } r=\frac{q-p}{pq-p} \text{ as in (8).}$$

Then, for all $p^i q^j \in Z_{q^b}$ with $j < b$, we have

$$p^a q^b - p^{a+i} q^j \geq p^a \geq r(q^b - 1) \geq r(q^b - q^j). \tag{11}$$

Using (9), it follows that $h(a, b) \geq h(a+i, j)$; in other words $p^a q^b \in p^a Z_{q^b}$. According to Proposition 3, we also have $Y_{p^a q^b} \subset \{p^i q^j \in Z_{p^a q^b} : j \leq b\}$. Using Lemma 2, it is immediate to check that the latter set is identical to $p^a Z_{q^b}$; thus $p^a q^b \in Y_{p^a q^b}$ and (i) is proved. Now, if $p^a q^b \in Y_{p^a q^b}$ then replacing a by $a + k$ for any $k \geq 1$ turns (11) into a strict inequality. Therefore, $Y_{p^{a+k} q^b} = \{p^{a+k} q^b\}$, and (ii) is proved too. Accordingly, letting

$$\ell_b = \min \left\{ a \in \mathbb{N} : Y_{p^a q^b} = \{p^a q^b\} \right\} \tag{12}$$

provides the claimed sequence ℓ. Since $Y_1 = \{1\}$ and $1 = p^0 q^0$, we get $\ell_0 = 0$.

Let us now prove that ℓ is non-decreasing. Given $b \in \mathbb{N}$, either $\ell_b = 0$ thus $\ell_{b+1} \geq \ell_b$, or $\ell_b \geq 1$. In the latter, there exists $p^i q^j \in Z_{p^{\ell_b - 1} q^b}$ such that $j \neq b$ and $h(i, j) \geq h(\ell_b - 1, b)$. From (3), it is not difficult to see that $h(i, j+1) = qh(i, j) + 1$, and thus $h(i, j+1) - h(\ell_b - 1, b+1) = q\left(h(i, j) - h(\ell_b - 1, b)\right)$. Therefore $h(i, j+1) \geq h(\ell_b - 1, b + 1)$, so that $\ell_{b+1} > \ell_b - 1$.

Finally suppose that ℓ is bounded. This would imply that there exists an integer a such that, for all $b \in \mathbb{N}$, $Y_{p^a q^b} = \{p^a q^b\}$. The following statement shows that this is impossible.

(iii) For all $a \in \mathbb{N}$ there exists $b \in \mathbb{N}$ such that $h(a + \lfloor b\rho \rfloor, 0) > h(a, b)$.

Indeed, by Lemma 2 we know that $p^{a+\lfloor b\rho \rfloor} \in Z_{p^a q^b}$. Fix $a \in \mathbb{N}$, choose $b \in \mathbb{N}^*$, and set $a' = a + \lfloor b\rho \rfloor$. According to (9), and denoting by $\{b\rho\} = b\rho - \lfloor b\rho \rfloor$ the fractional part of $b\rho$, we have

$$\begin{aligned} h(a, b) < h(a', 0) &\Leftrightarrow p^a q^b - p^{a'} < r(q^b - 1) \\ &\Leftrightarrow p^{\lfloor b\rho \rfloor} > q^b \left(1 - r/p^a \left(1 - 1/q^b\right)\right) \\ &\Leftrightarrow \{b\rho\} < -\log_p \left(1 - r/p^a \left(1 - 1/q^b\right)\right). \end{aligned} \tag{13}$$

Now observe that the sequence $(\phi_{a,b})_{b \in \mathbb{N}}$ defined by

$$\phi_{a,b} = -\log_p \left(1 - \frac{r}{p^a} \left(1 - \frac{1}{q^b}\right)\right), \tag{14}$$

where $r = (q - p)/(pq - p)$, is increasing, with $\phi_{a,0} = 0$. Since ρ is irrational, we know that $(b\rho)_{b \in \mathbb{N}}$ is equidistributed modulo 1. Thus there exists $b > 0$ such that $\{b\rho\} < \phi_{a,1}$; hence $\{b\rho\} < \phi_{a,b}$, which, using (13), concludes the proof. $\square$

Let us anticipate a result of the next section, implying that the sequence ℓ is completely known as soon as we can compute its *jump indices*, that is, the values

$b > 0$ for which $\ell_b > \ell_{b-1}$. Indeed, we shall establish with statement (25) that if b is a jump index of ℓ then $\ell_b = \lfloor \alpha(b) \rfloor$, where

$$\alpha(b) = \log_p \frac{q^b - 1}{q^b - p^{\lfloor b\rho \rfloor}} + \log_p \frac{q-p}{q-1}. \tag{15}$$

Computing the jump indices of ℓ may be done recursively as shown in the next corollary. Referring to the sequence ϕ defined in (14), let the mapping β be defined on $\mathbb{N}$ by

$$\beta(a) = \min \{ j \in \mathbb{N}^* : \ \{j\rho\} < \phi_{a,j} \}. \tag{16}$$

Corollary 1. *The increasing sequence $(j_k)_{k \in \mathbb{N}}$ of the jump indices of ℓ satisfies*

$$j_0 = \beta(0), \quad j_{k+1} = \beta(\ell_{j_k}).$$

Proof. Given any $a \in \mathbb{N}$, we know that $Y_{p^a} = \{p^a\}$ by Proposition 3. Moreover, letting b be incremented by 1 from 0 iteratively, it follows from (5) and (9) that $Y_{p^a q^b} = \{p^a q^b\}$ as long as $h(a, b) > h(a + \lfloor b\rho \rfloor, 0)$. As it is shown in part (iii) of the proof of Theorem 1, the latter inequality is equivalent to $\{b\rho\} < \phi_{a,b}$. Accordingly, $Y_{p^a q^b} = \{p^a q^b\}$ if $b < \beta(a)$. Hence $\ell_{\beta(a)-1} \leq a < \ell_{\beta(a)}$, so that $\beta(a)$ is a jump index for ℓ. The result follows immediately since ℓ is non-decreasing. □

As claimed before, we next show that Y_m has at most 2 elements. This might be established by directly using (9) and studying the diophantine equation

$$p^a q^b - p^c = r(q^b - 1), \quad \text{where } r = \frac{q-p}{pq-p}.$$

Unfortunately, the latter is seemingly not easy to cope with, whereas Theorem 1 proves handy.

Proposition 4. *For all $m \in \mathbb{N}$, the set Y_m has either one or two elements.*

Proof. Assume $|Y_m| \geq 2$ and denote by $p^a q^b$ its greatest element. Since $Y_m = Y_{p^a q^b}$, we have $a < \ell_b$ by definition of sequence ℓ in Theorem 1. To be more precise, statement (ii) in the proof of this theorem even tells us that $a = \ell_b - 1$. Now let $p^c q^d$ be the second greatest element in Y_m. According to Proposition 3 we must have $d < b$, and thus $c > a$ by Lemma 2. Since ℓ is non-decreasing, it follows that $\ell_d \leq \ell_b$. Since $a = \ell_b - 1$ we get $c \geq \ell_d$, which means that $Y_{p^c q^d} = \{p^c q^d\}$ from Theorem 1. Therefore, there cannot exist a third element in Y_m as it would also be in $Y_{p^c q^d}$. □

5. Asymptotic Behavior of G

In this section, our goal is to prove that $G(m)$ is equivalent to $mp/(p-1)$ as m tends to infinity, independently of q. As a simple first step, let us exhibit a sharp upper bound for G.

Lemma 3. *For all $m \in \mathbb{N}$ and all $n \in Y_m$, we have $G(m) < np/(p-1)$. In particular,*

$$\limsup_{m\to\infty} \frac{G(m)}{m} = \frac{p}{p-1}.$$

Proof. Let $n = p^a q^b \in Y_m$. According to (8) we have

$$h(a,b) - \frac{np}{p-1} = -\left(\frac{rpq^b}{p-1} + \frac{1}{q-1}\right) < 0, \quad \text{where } r \in (0, 1/p). \tag{17}$$

Hence $G(m) = h(a,b) < np/(p-1)$. Since $n \leq m$, it follows that $G(m)/m \leq p/(p-1)$. To conclude, observe that for $m = p^a$ we have $G(p^a) = (p^{a+1}-1)/(p-1)$ from Prop 3. Therefore, $\lim_{a\to\infty} G(p^a)/p^a = p/(p-1)$. □

Let us now define a mapping y as follows: For all m, let y_m denote the smallest integer of the form $p^a q^b$ such that $G(m) = h(a,b)$, that is,

$$y_m = \min Y_m. \tag{18}$$

According to Proposition 3, y_m is also the element of Y_m with the smallest exponent in q. We shall next give a characterization of y_m using the sequence ℓ defined in Theorem 1. Recall that this sequence is defined by $\ell_b = \min\{a \in \mathbb{N} : Y_{p^a q^b} = \{p^a q^b\}\}$ and satisfies (10). Since ℓ is non-decreasing, the sequence $(p^{\ell_b} q^b)_{b\in\mathbb{N}}$ is increasing. We may thus define, for all $m \in \mathbb{N}$,

$$m_\ell = \max\{b \in \mathbb{N} : p^{\ell_b} q^b \leq m\}. \tag{19}$$

Theorem 2. *For all $m \in \mathbb{N}$, we have*

$$y_m = \max\{p^a q^b \in Z_m : b \leq m_\ell\}. \tag{20}$$

Moreover, let $\bar{a} = \lfloor \log_p m - m_\ell \rho \rfloor$ and $\bar{m} = \lfloor m/p^{\bar{a}} \rfloor$. Then $y_m = p^{\bar{a}} z_{\bar{m}}$.

Proof. Let $y_m = p^i q^j$. Since $y_m = \min Y_m$, we have $Y_{y_m} = \{y_m\}$ thus $i \geq \ell_j$ using (10). Suppose $j > m_\ell$, then $p^i q^j \geq p^{\ell_j} q^j$, and thus $p^i q^j > m$ from (19), which contradicts the fact that $y_m \leq m$. Therefore, $j \leq m_\ell$.

Now consider any $p^a q^b \in Z_m$ such that $b \leq m_\ell$. Since ℓ is non-decreasing we have $\ell_{m_\ell} \geq \ell_b$. By Lemma 2, there exists $k \in \mathbb{N}$ such that $p^k q^{m_\ell} \in Z_m$, and we have $k \geq \ell_{m_\ell}$ because $p^{\ell_{m_\ell}} q^{m_\ell} \leq m$. Since $p^a q^b \in Z_m$, condition $b \leq m_\ell$ implies that $a \geq k$ by Lemma 2 again, so that $a \geq \ell_{m_\ell} \geq \ell_b$. Therefore, $Y_{p^a q^b} = \{p^a q^b\}$. Supposing $p^a q^b > p^i q^j$ would then imply that $h(i,j) < h(a,b)$, contradicting the definition of y_m. Thus $p^a q^b \leq p^i q^j$, and (20) is established.

Accordingly, $j = \lfloor \log_p m - i\rho \rfloor \leq \bar{a}$, so that $y_m/p^{\bar{a}}$ is an element of E. Therefore, $y_m/p^{\bar{a}} \leq m/p^{\bar{a}}$ implies $y_m/p^{\bar{a}} \leq \lfloor m/p^{\bar{a}} \rfloor = \bar{m}$, which in turn implies $\lfloor m/p^{\bar{a}} \rfloor \leq z_{\bar{m}}$. We thus get

$$y_m \leq p^{\bar{a}} z_{\bar{m}} \leq p^{\bar{a}} \bar{m} \leq m.$$

Let $z_{\bar{m}} = p^a q^b$. To conclude the proof by using (20) again, it suffices to show that $b \leq m_\ell$. Since $p^{\bar{a}} q^{m_\ell} \in Z_m$, we have $p^{\bar{a}} q^{m_\ell} \leq m < p^{\bar{a}} q^{m_\ell+1}$, so that $q^{m_\ell} \leq \bar{m} < q^{m_\ell+1}$. Thus $\lfloor \log_q \bar{m} \rfloor = m_\ell$, and hence $b \leq m_\ell$ by Lemma 2. □

Comparing with Proposition 3, characterization (20) of y_m no more depends on z_m. Moreover, it provides a first improvement of Lemma 3.

Corollary 2. *For all $m \in \mathbb{N}$, we have*

$$\frac{G(m)}{y_m} \sim \frac{p}{p-1} \quad \textit{as } m \to \infty. \tag{21}$$

Proof. For $m \in \mathbb{N}$, let $y_m = p^{a_m} q^{b_m}$. According to (17) we have

$$\frac{G(m)}{y_m} - \frac{p}{p-1} = -\frac{t_m}{p^{a_m}}, \quad \text{where } t_m = \frac{q-p}{(p-1)(q-1)} + \frac{1}{q^{b_m}(q-1)}.$$

Observe that $t_m \in \left(\frac{q-p}{(p-1)(q-1)}, \frac{1}{p-1}\right]$ is uniformly bounded. To conclude the proof, we need to show that a_m tends to infinity as m tends to infinity. According to Theorem 2, we have $b_m \leq m_\ell$, and thus $a_m \geq \ell_{m_\ell}$. Since m_ℓ goes to infinity with m, and since ℓ is non-decreasing and unbounded by Theorem 1, a_m goes to infinity with m too. Hence the claim. □

According to the latter result and Proposition 2, the final task consists in showing that $y_m \sim z_m$. This is done next, so that our main claim is established.

Theorem 3. *For all $m \in \mathbb{N}$, we have*

$$\frac{G(m)}{m} \sim \frac{p}{p-1} \quad \textit{as } m \to \infty.$$

Proof. Assume $y_m \neq z_m$. According to Theorem 2, the elements in Z_m that exceed y_m are of the form $p^i q^j$ with $m_\ell < j \leq \lfloor \log_q m \rfloor$. Let us sort these elements together with y_m in an increasing sequence $(n_0 = y_m, n_1, \ldots, n_N = z_m)$, so that $n_0 = y_m$ and $n_N = z_m$. Observe that the elements of this sequence are consecutive elements of E for the usual order. As soon as m is large enough, we know by Tijdeman's result already mentioned [13] that $n_{i+1} - n_i \leq n_i/(\log n_i)^C$ for an explicitly computable constant $C > 0$. Therefore,

$$z_m - y_m \leq \sum_{i=0}^{N-1} \frac{n_i}{(\log n_i)^C} \leq \sum_{i=0}^{N-1} \frac{p y_m}{(\log \frac{m}{p})^C}.$$

Accordingly, for all $m \in \mathbb{N}$,

$$0 \leq z_m - y_m \leq \left(\lfloor \log_q m \rfloor - m_\ell\right) \frac{p y_m}{(\log \frac{m}{p})^C}. \tag{22}$$

At this point, what remains to be proved is that $\lfloor \log_q m \rfloor - m_\ell$ grows asymptotically slower than $(\log \frac{m}{p})^C$ so that $z_m \sim y_m$, and to conclude using (21) and Lemma 2. Recall that m_ℓ is defined as the largest value b such that $p^{\ell_b} q^b \leq m$. Therefore, we have

$$p^{\ell_{m_\ell}} q^{m_\ell} \leq m < p^{\ell_{m_\ell+1}} q^{m_\ell+1}.$$

Equivalently, using $\rho = \log q / \log p$, we have

$$\frac{\ell_{m_\ell}}{\rho} + m_\ell \leq \log_q m < \frac{\ell_{m_\ell+1}}{\rho} + m_\ell + 1, \tag{23}$$

so that

$$\lfloor \log_q m \rfloor - m_\ell < \frac{\ell_{m_\ell+1}}{\rho} + 1. \tag{24}$$

It thus remains to evaluate the terms in sequence ℓ. For that purpose, we first give an explicit formula for ℓ, valid at the jumps of ℓ. We claim that, for all $b \in \mathbb{N}^*$,

$$\text{if} \quad \ell_b > \ell_{b-1} \quad \text{then} \quad \ell_b = \left\lfloor \log_p \frac{(q-p)(q^b-1)}{(q-1)(q^b - p^{\lfloor b\rho \rfloor})} \right\rfloor. \tag{25}$$

Indeed, assume that $\ell_b > \ell_{b-1}$. Then, for all $p^i q^j \in Z_{p^{\ell_{b-1}} q^{b-1}}$, we know from (9) that

$$p^{\ell_{b-1}} q^{b-1} - p^i q^j > r(q^{b-1} - q^j).$$

Multiplying both sides by q yields, for all $p^i q^j \in q Z_{p^{\ell_{b-1}} q^{b-1}}$,

$$p^{\ell_{b-1}} q^b - p^i q^j > r(q^b - q^j).$$

Now, $\ell_b > \ell_{b-1}$ implies that there exists an element $p^i q^j \in Z_{p^{\ell_{b-1}} q^b}$ for which the latter inequality does not hold. By Lemma 2 and the definition of Z_{qm} in (5), this element must be $p^{\ell_{b-1} + \lfloor b\rho \rfloor}$, so that

$$p^{\ell_{b-1}}(q^b - p^{\lfloor b\rho \rfloor}) \leq r(q^b - 1).$$

In fact, note that this inequality does not only hold for $p^{\ell_{b-1}}$; by definition of ℓ, it remains valid for $p^{\ell_{b-1}+1}, \ldots, p^{\ell_b - 1}$. Accordingly, we get

$$p^{\ell_b - 1}(q^b - p^{\lfloor b\rho \rfloor}) \leq r(q^b - 1) < p^{\ell_b}(q^b - p^{\lfloor b\rho \rfloor}),$$

which proves claim (25).

It follows from (25) that, for any b such that $\ell_b > \ell_{b-1}$,

$$\ell_b < \log_p \frac{q^b}{q^b - p^{\lfloor b\rho \rfloor}}. \tag{26}$$

A further result of Tijdeman (see [12, Theorem 1]) states that, as soon as $p^{\lfloor b\rho \rfloor} > 3$, there exists another explicit constant $C' > 1$ such that

$$q^b - p^{\lfloor b\rho \rfloor} \geq \frac{p^{\lfloor b\rho \rfloor}}{\left(\log p^{\lfloor b\rho \rfloor}\right)^{C'}}. \tag{27}$$

Therefore, since $q^b = p^{b\rho}$, (26) and (27) imply that

$$\ell_b < \log_p \frac{q^b (\log p^{\lfloor b\rho \rfloor})^{C'}}{p^{\lfloor b\rho \rfloor}} = \{b\rho\} + \frac{C'}{\log p} \log p^{\lfloor b\rho \rfloor} < 1 + \frac{C'}{\log p} \log\log q^b. \tag{28}$$

Putting all this together, we get the claimed result. Indeed, let b be the smallest index such that $\ell_{m_\ell+1} = \ell_b$. Since $\ell_b > \ell_{b-1}$, we have

$$\ell_{m_\ell+1} = \ell_b < 1 + \frac{C'}{\log p} \log\log q^b \leq 1 + \frac{C'}{\log p} \log\log q^{m_\ell+1} \leq 1 + \frac{C'}{\log p} \log\log qm. \tag{29}$$

Using (24) we get

$$\lfloor \log_q m \rfloor - m_\ell < 1 + \frac{1}{\rho} + \frac{C'}{\log q} \log\log qm = o\left((\log m/p)^C\right), \tag{30}$$

which implies, using (22), that $y_m \sim z_m$ and concludes the proof. □

Note that the above proof mainly relies on the fact that the sequence ℓ is non-decreasing and that, due to the lower bound in (27) essentially, it grows very slowly. The theorem of Tijdeman that provides this lower bound hinges on a result of Fel'dman about linear forms in logarithms. More recent results of Laurent et alii [9] about such forms in two logarithms allow one to make precise the value of the effective constant C' in (27). Nevertheless, this value remains large and does not seem convenient to compute m_ℓ using (30), in particular when m is not very large. The algorithm presented in the next section provides one with an alternative method.

6. Computing y_m and $G(m)$

Using the mapping h, computing $G(m)$ is straightforward as soon as an element of Y_m is known, in particular y_m. In Theorem 2, we proved that $y_m = p^{\bar{a}} z_{\bar{m}}$, where $\bar{a}$ and $z_{\bar{m}}$ both depend on m_ℓ. Once m_ℓ is known, computing $z_{\bar{m}}$ (the greatest element in $Z_{\bar{m}}$) can be done efficiently with an algorithm explained in [3]. We shall establish a slightly different and simpler version of that algorithm at the end of this section.

Computing m_ℓ requires to compute the values of ℓ (see (19)). Theorem 4 given below asserts that the jump indices of ℓ are denominators of convergents of ρ. Furthermore, the relation $\ell_b = \lfloor \alpha(b) \rfloor$, see (15), also holds for *all* denominators of both convergents of ρ of even index and their mediants. This provides an explicit method for computing any term of ℓ, stated in Corollary 3.

Let us recall some known facts about the convergents of an irrational number (see, e.g., [8] or [1] for more details). Let $[a_0, a_1, ...]$ be the regular continued fraction expansion of ρ, and for $i \geq 0$, denote by h_i/k_i the i^{th} principal convergent of ρ. It is well known that the sequence $(h_i/k_i)_{i\geq 0}$ converges to ρ and satisfies

$$|k_i\rho - h_i| = (-1)^i(k_i\rho - h_i),$$

and

$$\frac{1}{k_i + k_{i+1}} < |k_i\rho - h_i| < \frac{1}{k_{i+1}}.$$

Given $i \geq 0$, the intermediate convergents of h_i/k_i, sometimes referred to as mediants, are the rational numbers $h_{i,j}/k_{i,j}$ given by

$$h_{i,j} = h_i + jh_{i+1}, \quad k_{i,j} = k_i + jk_{i+1}, \quad \text{for } 0 < j < a_{i+2}. \tag{31}$$

If $0 < j \leq j' < a_{i+2}$ we thus have $h_i/k_i < h_{i,j}/k_{i,j} \leq h_{i,j'}/k_{i,j'} < h_{i+2}/k_{i+2}$. Let us denote by $(H_n/K_n)_{n\in\mathbb{N}}$ the increasing sequence of all principal convergents of ρ of even index, h_{2i}/k_{2i}, together with their intermediate convergents. It is known (see [11, Theorem 2]) that $(H_n/K_n)_{n\in\mathbb{N}}$ is the best approximating sequence of ρ from below, that is, its terms are characterized by the following property: For each $n \in \mathbb{N}$, and for integers h and k,

$$\text{if} \quad \frac{H_n}{K_n} < \frac{h}{k} < \rho \quad \text{then} \quad k > K_n. \tag{32}$$

We shall need two immediate consequences of (32). The first one is that, while the sequence $(K_n)_{n\in\mathbb{N}}$ increases to infinity, the sequence $(\{K_n\rho\})_{n\in\mathbb{N}}$ decreases to 0. Indeed, property (32) implies that $H_n = \lfloor K_n\rho\rfloor$, so that (31) implies, for $0 \leq j < a_{i+2}$,

$$\{k_{2i,j+1}\rho\} - \{k_{2i,j}\rho\} = k_{2i+1}\rho - h_{2i+1} \in (-1/k_{2i+2}, 0). \tag{33}$$

The second one rephrases the sufficient condition in (32): If $\{b\rho\} \leq \{j\rho\}$ holds for all integers $0 < j \leq b$, then b is a term of $(K_n)_{n\in\mathbb{N}}$. Indeed, let h, k be such that

$$\frac{\lfloor b\rho\rfloor}{b} < \frac{h}{k} < \rho.$$

Then, since $h < k\rho$, the above inequalities still hold for $h = \lfloor k\rho\rfloor$. This implies $\{k\rho\} < \frac{k}{b}\{b\rho\}$. Supposing $k \leq b$ yields $\{k\rho\} < \{b\rho\}$, which contradicts our hypothesis. Hence $\lfloor b\rho\rfloor/b$ satisfies (32).

We can now establish our main claims. According to (25), the values of ℓ are known explicitly at every jump index j of ℓ. In these cases, we have $\ell_j = \lfloor\alpha(j)\rfloor$ where, as already defined in (15),

$$\alpha(b) = \log_p \frac{q^b - 1}{q^b - p^{\lfloor b\rho\rfloor}} + \log_p \frac{q-p}{q-1}.$$

Theorem 4. *Every jump index of ℓ is a term of the sequence $(K_n)_{n\in\mathbb{N}}$. Moreover, for each $K \in (K_n)_{n\in\mathbb{N}}$, we have $\ell_K = \lfloor \alpha(K) \rfloor$.*

Proof. According to Corollary 1, the jump indices j_k of ℓ can be computed starting from $j_0 = \beta(0)$ and iterating $j_{k+1} = \beta(\ell_{j_k})$, where $\beta(a) = \min\{j \in \mathbb{N}^* : \{j\rho\} < \phi_{a,j}\}$ (see (14) and (16)). Let us fix $a \in \mathbb{N}$. Since the sequence $(\phi_{a,i})_{i\geq 0}$ increases from 0 and the sequence $(\{K_i\rho\})_{i\geq 0}$ decreases to 0, there exists a unique n such that $\{K_n\rho\} < \phi_{a,K_n}$ and $\{K_i\rho\} \geq \phi_{a,K_i}$ for all $i < n$, if any. In particular, $K_n \geq \beta(a)$. We next establish that $K_n = \beta(a)$. This is clear if $n = 0$ since $K_0 = 1$ and $\beta(a) \geq 1$. In the following, we assume $n \geq 1$.

Let $b = \beta(a)$ for short, and suppose $b < K_n$. Let $K = K_{n-1}$ for short again, and let $c = \min\{j > 0 : \{j\rho\} < \{K\rho\}\}$. For all $i < c$ we have $\{i\rho\} \geq \{K\rho\} > \{c\rho\}$, so that $c \in (K_i)$, which implies $c = K_n$ since $(\{K_i\rho\})$ decreases. Therefore, $b < K_n$ forces $\{b\rho\} \geq \{K\rho\}$, so that

$$\phi_{a,b} > \{b\rho\} \geq \{K\rho\} \geq \phi_{a,K}. \tag{34}$$

Since $\phi_{a,i}$ increases with i, we get $K < b < K_n$. Property (32) implies that $\lfloor b\rho \rfloor / b < \lfloor K_n\rho \rfloor / K_n$. Since we cannot have $\lfloor K\rho \rfloor / K < \lfloor b\rho \rfloor / b < \lfloor K_n\rho \rfloor / K_n$ ([11], (ii) of Lemma 1), it follows that $\lfloor b\rho \rfloor / b < \lfloor K\rho \rfloor / K$, that is, $\{b\rho\}/b > \{K\rho\}/K$. Thus

$$\{b\rho\} - \{K\rho\} > \frac{b-K}{K}\{K\rho\} \geq \frac{\phi_{a,K}}{K} > \frac{x(1-q^{-K})}{K\log p},$$

where $x = r/p^a$ for short. Nevertheless,

$$\phi_{a,b} - \phi_{a,K} < \phi_{a,\infty} - \phi_{a,K} = \log_p\left(1 + \frac{x}{1-x}q^{-K}\right) < \frac{x}{(1-x)q^K \log p}.$$

According to (34) we should thus have

$$\frac{(1-q^{-K})}{K} < \frac{1}{(1-x)q^K},$$

which would imply, since $x \leq r$,

$$q - 1 < \frac{q^K - 1}{K} < \frac{1}{1-x} \leq \frac{p(q-1)}{q(p-1)} < q - 1.$$

Therefore, $K_n = \beta(a)$ as claimed, which proves the first assertion of the Theorem.

Now, let $K \in (K_n)$. On one hand, $\ell_K \leq \lfloor \alpha(K) \rfloor$ holds. Indeed, there is a unique jump index K^* of ℓ such that $\ell_K = \ell_{K^*}$, and $K^* \leq K$ because ℓ is non-decreasing. According to the first assertion of the Theorem, $K^* \in (K_n)$. Since (K_n) increases and $(\{K_n\rho\})$ decreases, $(\alpha(K_n))$ is increasing, and thus $(\lfloor \alpha(K_n) \rfloor)$ is non-decreasing. Therefore, $\ell_K = \ell_{K^*} = \lfloor \alpha(K^*) \rfloor \leq \lfloor \alpha(K) \rfloor$. On the other hand, we also have $\lfloor \alpha(K) \rfloor \leq \ell_K$. Indeed, letting $a = \lfloor \alpha(K) \rfloor$ for short, we have $a \leq \alpha(K)$, that is,

$$p^a \leq \frac{(q-p)(q^K-1)}{(q-1)(q^K - p^{\lfloor K\rho \rfloor})}.$$

Recalling (9), this also reads

$$(p^{a-1}q^K - p^{a-1+\lfloor K\rho \rfloor}) \leq r(q^K - 1).$$

Since $\ell_K \geq 0$, we may assume $a \geq 1$. Letting $a' = a + \lfloor K\rho \rfloor$, the above inequality means that

$$h(a-1, K) \leq h(a'-1, 0).$$

Finally notice that $p^{a'-1} < p^{a-1}q^K$. Therefore, $Y_{p^{a-1}q^K} \neq \{p^{a-1}q^K\}$, so that $a - 1 < \ell_K$ by (10). Thus $\lfloor \alpha(K) \rfloor = a \leq \ell_K$ as claimed. $\square$

Accordingly, computing ℓ_b for an arbitrary b only requires applying α to the largest term of $(K_n)_{n\in\mathbb{N}}$ not exceeding b. More explicitly:

Corollary 3. *Given $b \in \mathbb{N}$, let s and t be the integers defined by*

$$k_{2s} \leq b < k_{2s+2}, \quad \text{and} \quad t = \left\lfloor \frac{b - k_{2s}}{k_{2s+1}} \right\rfloor.$$

Then $\ell_b = \lfloor \alpha(k_{2s,t}) \rfloor$.

Let us finally turn to the computation of $y_m = p^a q^b$ and $G(m) = h(a, b)$. Of course, writing these values requires $O(\log m)$ bits, but we show that the a and b exponents of y_m can be obtained with $O(\log \log m)$ operations involving numbers of $O(\log \log m)$ bits.

According to Lemma 2, for each integer $b \in [0, \log_m]$ there is a unique integer a such that $p^a q^b \in Z_m$, given by $a = \lfloor \log_p m - b\rho \rfloor$. Let us define, for any $b \in \mathbb{N}$,

$$\zeta(b) = p^{\lfloor \log_p m - b\rho \rfloor} q^b.$$

In particular, for each $0 \leq b \leq \lfloor \log_q m \rfloor$, $\zeta(b)$ is the element of Z_m whose exponent in q is b. In the example given in Figure 2 for $(p, q) = (2, 3)$ and $m = 750$, the terms of ζ, given for $0 \leq b \leq \lfloor \log_q m \rfloor = 6$, are $(512, 384, 576, 432, 648, 486, 729)$. Let us now define the sequence $(b_i)_{i\in\mathbb{N}}$ as follows: $b_0 = 0$ and, for $i \geq 0$,

$$b_{i+1} = \min\{b \in \mathbb{N} : b > b_i \text{ and } \zeta(b) > \zeta(b_i)\}.$$

This sequence is the basis for the algorithm in [3] that computes z_m. The following lemma tells us that the latter algorithm may also be used to compute y_m.

Lemma 4. *Let $I = \max\{i \in \mathbb{N} : b_i \leq \log_q m\}$ and $J = \max\{i \in \mathbb{N} : b_i \leq m_\ell\}$, then $\zeta(b_I) = z_m$ and $\zeta(b_J) = y_m$.*

Proof. Let $z_m = \zeta(b^*)$. Since $\zeta(b_I) \in Z_m$, we have $\zeta(b^*) \geq \zeta(b_I)$. Suppose $\zeta(b^*) > \zeta(b_I)$; then $b^* \geq b_{I+1}$, which contradicts the definition of I. Thus $\zeta(b^*) = \zeta(b_I)$, and hence $b^* = b_I$. Finally, it follows from Theorem 2 that $\zeta(b_J) = y_m$. $\square$

In our running example (see Figure 2), it can be read directly from Table 1 that sequence (b_i) starts with $(0, 2, 4, 6)$. We thus have $I = 3$ and, since $m_\ell = 4$ (to be read on Figure 2), $J = 2$.

To compute successive terms of $(b_i)_{i\in\mathbb{N}}$, we next state a modified version of the result in [3]. We obtain a simple bound on the number of steps required to get z_m from $(b_i)_{i\in\mathbb{N}}$ without any assumption concerning the partial quotients of ρ.

For each principal convergent h_s/k_s of ρ, let $\varepsilon_s = |k_s\rho - h_s|$. We know that $(\varepsilon_s)_{s\in\mathbb{N}}$ is strictly decreasing and converges towards 0. Besides, the convergents of even index approach ρ from below (see (32)), whereas those of odd index approach ρ from above. Hence $\varepsilon_{2s} = k_{2s}\rho - h_{2s}$ and $\varepsilon_{2s+1} = -k_{2s+1}\rho + h_{2s+1}$. Thus we have $\{k_{2s}\rho\} = \varepsilon_{2s}$ and, for all $0 \leq t \leq a_{2s+2}$,

$$\{k_{2s,t}\rho\} = \varepsilon_{2s} - t\varepsilon_{2s+1} = \varepsilon_{2s+2} + (a_{2s+2} - t)\varepsilon_{2s+1}. \tag{35}$$

Our main theorem regarding the computation of y_m and $G(m)$ can now be established.

Theorem 5. *For all $i \geq 0$, let $d_{i+1} = b_{i+1} - b_i$. The sequence $(d_i)_{i\geq 1}$ is non-decreasing ; its terms all belong to $(K_n)_{n\in\mathbb{N}}$ and satisfy the following properties:*

(i) For each $s \in \mathbb{N}$, there exists at most one value of t in $(0, a_{2s+2})$ such that $k_{2s,t}$ belongs to $(d_i)_{i\geq 1}$. If $d_{i+1} = k_{2s,t}$ with $0 < t < a_{2s+2}$, then $t = t_s$ is given by

$$t_s = \left\lceil \frac{\varepsilon_{2s} - \{\log_p m - b_i\rho\}}{\varepsilon_{2s+1}} \right\rceil. \tag{36}$$

(ii) If $d_{i+1} = k_{2s}$ with either $i = 0$ or $d_{i+1} > d_i$, then k_{2s} occurs n_s consecutive times in $(d_i)_{i\geq 1}$, where

$$n_s = \left\lfloor \frac{\{\log_p m - b_i\rho\}}{\varepsilon_{2s}} \right\rfloor. \tag{37}$$

Moreover, if either $s = 0$ or $d_i = k_{2s-2,t}$ with $0 < t < a_{2s}$, then $n_s \leq a_{2s+1}$, else $n_s \leq 1 + a_{2s+1}$.

Proof. Let $r_i = \{\log_p m - b_i\rho\}$ for short. For all integers b such that $b_i < b \leq \log_q m$, we have [3]

$$\begin{aligned} \log_p \zeta(b) - \log_p \zeta(b_i) =& \lfloor \log_p m - b\rho \rfloor + b\rho - \lfloor \log_p m - b_i\rho \rfloor - b_i\rho \\ =& \lfloor r_i - \{(b - b_i)\rho\} \rfloor + \{(b - b_i)\rho\}. \end{aligned} \tag{38}$$

[3]Observe that $0 \leq y \leq x$ implies $\lfloor x - y \rfloor + y - \lfloor x \rfloor = \lfloor \{x\} - \{y\} \rfloor + \{y\}$.

Thus $\zeta(b) > \zeta(b_i)$ if, and only if, $\{(b - b_i)\rho\} \le r_i$. For $b = b_{i+1}$, this reads $\zeta(b_{i+1}) > \zeta(b_i) \iff \{d_{i+1}\rho\} \le r_i$. Therefore, any positive integer $c < d_{i+1}$ satisfies $\{c\rho\} > r_i$, hence

$$d_{i+1} = \min\{d \in \mathbb{N}^* : \{d\rho\} \le r_i\}. \tag{39}$$

Using the second consequence of (32), d_{i+1} is thus a term of $(K_n)_{n\in\mathbb{N}}$. Similarly, we next get $\{d_{i+2}\rho\} \le r_{i+1}$. Since $r_i \ge \{d_{i+1}\rho\}$ from (39), observe that $r_{i+1} = \{\log_p m - b_i\rho - d_{i+1}\rho\} = r_i - \{d_{i+1}\rho\} < r_i$, so that $d_{i+2} \ge d_{i+1}$. The first claims regarding the terms of $(d_{i+1})_{i\in\mathbb{N}}$ are thus proved.

Let us now prove the properties in (i). Assume $d_{i+1} = k_{2s,t}$. Since $\{k_{2s,t}\rho\} = \varepsilon_{2s} - t\varepsilon_{2s+1}$, we get using (39) again

$$\varepsilon_{2s} - t\varepsilon_{2s+1} \le r_i < \varepsilon_{2s} - (t-1)\varepsilon_{2s+1};$$

thus $t \ge (\varepsilon_{2s} - r_i)/\varepsilon_{2s+1} > t - 1$, and hence we have (36). It follows that $r_{i+1} = r_i - \{k_{2s,t}\rho\} < \varepsilon_{2s+1}$, and since the minimum value of $\{k_{2s,t'}\rho\}$, reached for $t' = a_{2s+2} - 1$, is $\varepsilon_{2s+2} + \varepsilon_{2s+1}$, we must have $d_{i+2} > k_{2s,a_{2s+2}-1}$, and thus $d_{i+2} \ge k_{2s+2}$.

Turning to (ii), assume that $d_{i+1} = k_{2s}$. Hence $r_i \ge \varepsilon_{2s}$, so that n_s given in (37) is positive. If $n_s > 1$ we get $r_{i+1} = r_i - \varepsilon_{2s} \ge \varepsilon_{2s}$, thus $d_{i+2} = k_{2s}$. By iterating, it follows that $r_{i+j-1} \ge \varepsilon_{2s}$ and $d_{i+j} = k_{2s}$ for each $j \le n_s$, and that $r_{i+n_s} < \varepsilon_{2s}$. Thus $d_{i+n_s+1} > k_{2s}$.

Finally assume without loss of generality that either $i = 0$ or $d_i < d_{i+1}$. Thus $s = 0$ implies $i = 0$. Since $r_0 = \{\log_p m\} < 1$ and $\varepsilon_0 = \{\rho\}$, $n_0 \le \lfloor 1/\{\rho\}\rfloor = a_1$. If $s > 0$, since $d_{i+1} > k_{2s-2,a_{2s}-1}$ we get using (35)

$$r_i < \varepsilon_{2s} + \varepsilon_{2s-1} = (a_{2s+1} + 1)\varepsilon_{2s} + \varepsilon_{2s+1};$$

thus $n_s \le a_{2s+1} + 1$. Finally, when $d_i = k_{2s-2,t}$ with $0 < t < a_{2s}$, (36) shows that $r_i < \varepsilon_{2s-1}$, which is tighter and yields $n_s \le a_{2s+1}$ in the same way. $\square$

We now describe how Theorem 5 can be turned into an algorithm that computes sequence $(b_i)_{i\in\mathbb{N}}$. As seen in Lemma 4, the same algorithm can be used to compute either z_m or y_m. Accordingly, we use an additional input parameter, denoted by B_m, and standing for either $\lfloor \log_q m \rfloor$ or m_ℓ respectively. The algorithm works as follows. Starting from values $s = 0$, $i_0 = 0$, $b_0 = 0$, $r_0 = \{\log_p m\}$, iterate:

1. **if** $(r_{2s} \ge \varepsilon_{2s})$ **then**
   - (a) $n_s = \lfloor r_{2s}/\varepsilon_{2s} \rfloor$; $\quad r_{2s+1} = r_{2s} - n_s\varepsilon_{2s}$; $\quad i_{2s+1} = i_{2s} + n_s$;
   - (b) **for** $i_{2s} < i \le i_{2s+1}$ **do** $\quad d_i = k_{2s}$; $\quad b_i = b_{i-1} + k_{2s}$;
   - (c) **if** $(b_{i_{2s+1}} > B_m)$ **then return** $b_{i_{2s}} + \lfloor (B_m - b_{i_{2s}})/k_{2s} \rfloor k_{2s}$;

   else $r_{2s+1} = r_{2s}$; $\quad i_{2s+1} = i_{2s}$;

2. **if** $(r_{2s+1} \geq \varepsilon_{2s} - \varepsilon_{2s+1})$ **then**

   (a) $t_s = \lceil(\varepsilon_{2s} - r_{2s+1})/\varepsilon_{2s+1}\rceil$;

   (b) $r_{2s+2} = r_{2s+1} - \varepsilon_{2s} + t_s\varepsilon_{2s+1}$; $\quad i_{2s+2} = i_{2s+1} + 1$;

   (c) $d_{i_{2s+2}} = k_{2s,t_s}$; $\quad b_{i_{2s+2}} = b_{i_{2s+1}} + k_{2s,t_s}$;

   (d) **if** $(b_{i_{2s+2}} > B_m)$ **then return** $b_{i_{2s+1}}$

   else $r_{2s+2} = r_{2s+1}$; $\quad i_{2s+2} = i_{2s+1}$;

Corollary 4. *The above algorithm requires at most* $2 + \lfloor \log_2 \log_q m \rfloor$ *iterations.*

Proof. Let $z_m = \zeta(b_I)$ and let $d_I = k_{2S,t}$, with $S \geq 0$ and either $t = 0$ or $t = t_S$. Then $k_{2S} \leq b_I \leq \log_q m$. But relations $k_{i+3} = (a_{i+2}a_{i+1} + 1)k_{i+1} + k_i$ and $k_0 = 1$ imply that $k_{2i} \geq 2^i$, with equality only if $i \leq 1$. Thus $S \leq \log_2 \log_q m$. Finally, checking the stopping condition requires n_{S+1} be computed in the case $t = t_S$. □

Observe that the required precision is about $\log_2 \log_q m$ bits for the floating point calculations with fractional parts. Alternatively, the computation may be carried out with integers by approximating ρ by the convergent H/K, where K is the greatest element in $(K_n)_{n\in\mathbb{N}}$ not exceeding $\log_q m$, and by performing the operations modulo K.

To output y_m, the above algorithm requires m_ℓ to be known. If N is the largest index such that $K_N + \lfloor\alpha(K_N)\rfloor/\rho \leq \log_p m$, we simply have $m_\ell = \lfloor \log_p m - \lfloor\alpha(K_N)\rfloor/\rho\rfloor$. Indeed, $\ell_b = \ell_{K_N} = \lfloor\alpha(K_N)\rfloor$ for all $b \in [K_N, K_{N+1})$. To compute K_N, it suffices to

1: compute the largest k_{2s} such that $k_{2s} + \lfloor\alpha(k_{2s})\rfloor/\rho \leq \log_p m$,

2: compute the largest $k_{2s,t}$ such that $k_{2s,t} + \lfloor\alpha(k_{2s,t})\rfloor/\rho \leq \log_p m$.

Task 1 requires at most $2 + \log_2 \log_q m$ steps, each step essentially consisting in computing next values of k_{2i} and $\alpha(k_{2i})$. Task 2 may be done by using a binary search of t in $[0, a_{2s+2})$, which requires $\log_2 a_{2s+2}$ similar steps. Whereas we are sure that $a_{2s} < \log_q m$ because $a_{2s} < k_{2s}$, a_{2s+1} or a_{2s+2} might exceed $\log_q m$. In the former case we conclude that $t = 0$, since $\log_q m < k_{2s,1} = k_{2s} + k_{2s+1}$. In the latter case, we may simply use a binary search of t in $[0, \lfloor(\log_q m - k_{2s})/k_{2s+1}\rfloor]$ because $k_{2s,t} \leq \log_q m$ must hold. We have thus established:

Proposition 5. *Computing* m_ℓ *can be done by computing* $K + \lfloor\alpha(K)\rfloor/\rho$ *for at most* $2 + 2\lfloor\log_2 \log_q m\rfloor$ *values of* K *in the sequence* (K_n).

The final remaining problem is that computing $\alpha(b)$ might be expensive. Recall that

$$\alpha(b) = \log_p \frac{q^b - 1}{q^b - p^{\lfloor b\rho\rfloor}} + \log_p \frac{q-p}{q-1}. \tag{40}$$

We next show that a fitting approximation of α is given by

$$\alpha^+(b) = \log_p \frac{q-p}{(q-1)\log p} + \log_p \frac{1}{\{b\rho\}} + \frac{1}{2}\{b\rho\}. \tag{41}$$

Proposition 6. *For all $n \in \mathbb{N}$, we have*

$$0 < \alpha^+(K_n) - \alpha(K_n) < \frac{\log p}{6}\{K_n\rho\}^2 + \frac{1}{q^{K_n}-1}.$$

Proof. Let $\delta_n = \alpha^+(K_n) - \alpha(K_n)$ and $u_n = \frac{1}{2}\{K_n\rho\}\log p$. According to (40) and (41),

$$\delta_n = \log_p \frac{\sinh u_n}{u_n} - \log_p(1 - q^{-K_n}).$$

Observe that $\delta_n > 0$ because $\sinh u_n > u_n > 0$ and $0 < q^{-K_n} < 1$. Furthermore, $-\log(1-x) < x/(1-x)$ for $0 < x < 1$; thus $-\log_p(1-q^{-K_n}) < 1/(q^{K_n}-1)$. Finally, $(1-e^{-x})/x < 1 - x/2 + x^2/6$ for $0 < x$, so that

$$\log \frac{\sinh u_n}{u_n} = u_n + \log \frac{1-e^{-2u_n}}{2u_n} < \frac{2u_n^2}{3}.$$

Hence the claimed inequalities. □

7. Concluding remark

When $m = q^N$ for some positive integer N, applying Theorem 5 to find z_m provides one with a representation of N by a finite sum of terms of $(K_n)_{n\in\mathbb{N}}$. This representation is similar in spirit to Ostrovski's number system [10, 2]. For example, consider $\rho = \log_2 3$ whose partial quotients start with $[1, 1, 1, 2, 2, 3, 1, ...]$. Sequence $(K_n)_{n\in\mathbb{N}}$ starts with $(1, 2, 7, 12, 53, ...)$ and sequence $(k_n)_{n\in\mathbb{N}}$ starts with $(1, 1, 2, 5, 12, 41, 53, ...)$. Using Theorem 5 with $m = q^6$ we get $6 = 3K_1 = 3k_2$, whereas $6 = k_1 + k_3$ in Ostrovski's representation. Studying this novel representation is beyond the scope of this paper and should be the topic of future work.

To conclude, the authors wish to thank an anonymous referee for her/his stimulating comments, which, in particular, lead them to discover and prove Theorem 5.

References

[1] J.-P. Allouche and J. Shallit, *Automatic Sequences*, Cambridge University Press, 2003.

[2] V. Berthé, *Autour du système de numération d'Ostrowski*, Bull. Belg. Math. Soc. Simon Stevin **8** (2001), 209–239.

[3] V. Berthé and L. Imbert, *Diophantine approximation, Ostrowski numeration and the double-base number system*, Discrete Math. Theor. Comput. Sci. **11** (2009), no. 1, 153–172.

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

[5] V. Dimitrov, G. A. Jullien, and W. C. Miller, *Theory and applications of the double-base number system*, IEEE Trans. Comput. **48** (1999), no. 10, 1098–1106.

[6] P. Erdős and J. H. Loxton, *Some problems in partitio numerorum*, J. Aust. Math. Soc., Series A **27** (1979), no. 3, 319–331.

[7] L. Imbert and F. Philippe, *Strictly chained* (p, q)*-ary partitions*, Contrib. Discrete Math. **5** (2010), no. 2, 119–136.

[8] S. Lang, *An Introduction to Diophantine Approximations*, Springer, 1995.

[9] M. Laurent, M. Mignotte, and Y. Nesterenko, *Formes linéaires en deux logarithmes et déterminants d'interpolation*, J. Number Theory **55** (1995), no. 2, 285–321.

[10] A. M. Ostrowski, *Bemerkungen zur theorie der diophantischen approximationen*, Abh. Math. Semin. Univ. Hambg. **1** (1922), 77–98.

[11] I. Richards, *Continued fractions without tears*, Math. Mag. **54** (1981), no. 4, 163–171.

[12] R. Tijdeman, *On integers with many small prime factors*, Compos. Math. **26** (1973), no. 3, 319–330.

[13] R. Tijdeman, *On the maximal distance between integers composed of small primes*, Compos. Math. **28** (1974), 159–162.