Structural properties of bounded languages with respect to multiplication by a constant

Emilie Charlier, Michel Rigo

Institute of Mathematics, University of Liège, Grande Traverse 12 (B 37),
B-4000 Liège, Belgium. {echarlier,M.Rigo}@ulg.ac.be

Abstract. We consider the preservation of recognizability of a set of integers after multiplication by a constant for numeration systems built over a bounded language. As a corollary we show that any nonnegative integer can be written as a sum of binomial coefficients with some prescribed properties.

1 Introduction

Let us denote by $\mathcal{B}_\ell = a_1^* \cdots a_\ell^*$ the bounded language over the alphabet $\Sigma_\ell = \{a_1, \ldots, a_\ell\}$ of size $\ell \geq 1$ (for more on bounded languages, see for instance [4]). We always assume that $(\Sigma_\ell, <)$ is totally ordered by $a_1 < \cdots < a_\ell$. Therefore we can enumerate the words of $\mathcal{B}_\ell$ using the increasing genealogical ordering induced by the ordering $<$ of Σ_ℓ. Let $n \geq 0$. The $(n+1)$-st word of $\mathcal{B}_\ell$ is said to be the *$\mathcal{B}_\ell$-representation* of n and is denoted by $\mathrm{rep}_\ell(n)$. The reciprocal map $\mathrm{rep}_\ell^{-1} =: \mathrm{val}_\ell$ maps the n-th word of $\mathcal{B}_\ell$ onto its *numerical value* $n-1$.

Definition 1. *A set $X \subseteq \mathbb{N}$ is said to be $\mathcal{B}_\ell$-*recognizable *if $\mathrm{rep}_\ell(X)$ is a regular language over the alphabet Σ_ℓ.*

In the framework of positional numeration systems, recognizable sets of integers have been extensively studied since the seminal work of A. Cobham in the late sixties (see for instance [3, Chap. V]). Since then the notion of recognizability has been studied from various points of view (logical characterization, automatic sequences, ...). In particular, recognizability for generalized number systems like the Fibonacci system has been considered [2, 9]. Here we shall consider recognizable sets of integers in the general setting of *abstract numeration systems.*

Remark 1. Indeed, the one-to-one correspondence between the words of $\mathcal{B}_\ell$ and the integers can be extended to any infinite regular language L over a totally ordered alphabet $(\Sigma, <)$. This leads to the notion of *abstract numeration system* $S = (L, \Sigma, <)$ where $\mathrm{rep}_S(n)$ is the $(n+1)$-st word in the genealogically ordered language L and *S-recognizable sets* of integers are defined accordingly [6]. Thus $\mathcal{B}_\ell$-recognizability is a special case of S-recognizability.

If w is a word over Σ_ℓ, $|w|$ denotes its length and $|w|_{a_j}$ counts the number of letters a_j's appearing in w. The *Parikh mapping* Ψ maps a word $w \in \Sigma_\ell^*$ onto the vector $\Psi(w) := (|w|_{a_1}, \ldots, |w|_{a_\ell})$.

Remark 2. In this setting of bounded languages, rep_ℓ and Ψ are both one-to-one correspondences. Therefore, in what follows we shall make no distinction between an integer n, its $\mathcal{B}_\ell$-representation $\mathrm{rep}_\ell(n) = a_1^{i_1} \cdots a_\ell^{i_\ell} \in \mathcal{B}_\ell$ and the corresponding Parikh vector $\Psi(\mathrm{rep}_\ell(n)) = (i_1, \ldots, i_\ell) \in \mathbb{N}^\ell$. In examples, when considering cases $\ell = 2$ or 3, we shall use alphabets like $\{a < b\}$ or $\{a < b < c\}$.

The question addressed in the present paper deals with the preservation of the recognizability with respect to the operation of multiplication by a constant. Namely, *if $S = (L, \Sigma, <)$ is an abstract numeration system, can we find some necessary and sufficient condition on $\lambda \in \mathbb{N}$ such that for any S-recognizable set X, the set λX is still S-recognizable*? This question is a first step before handling more complex operations like addition of two arbitrary recognizable sets.

This question is difficult and we shall restrict ourselves with abstract numeration systems built over a bounded language. Since rep_ℓ is a one-to-one correspondence between $\mathbb{N}$ and $\mathcal{B}_\ell$, multiplication by a constant $\lambda \in \mathbb{N}$ can be view as a transformation $f_\lambda : \mathcal{B}_\ell \to \mathcal{B}_\ell$ acting on the language $\mathcal{B}_\ell$, the question being then to *determine some necessary and sufficient condition under which this transformation preserves regular subsets of $\mathcal{B}_\ell$* ?

Example 1. Let $\ell = 2$, $\Sigma_2 = \{a, b\}$ and $\lambda = 25$. We have the following diagram.

$$\begin{array}{ccc} 8 & \xrightarrow{\times 25} & 200 \\ \mathrm{rep}_2 \downarrow & & \downarrow \mathrm{rep}_2 \\ a\, b^2 & \xrightarrow{\times 25} & a^9\, b^{10} \end{array} \qquad\qquad \begin{array}{ccc} \mathbb{N} & \xrightarrow{\times \lambda} & \mathbb{N} \\ \mathrm{rep}_2 \downarrow & & \downarrow \mathrm{rep}_2 \\ \mathcal{B}_\ell & \xrightarrow{f_\lambda} & \mathcal{B}_\ell \end{array}$$

Thus multiplication by $\lambda = 25$ induces a mapping f_λ onto $\mathcal{B}_2$ such that for $w, w' \in \mathcal{B}_2$, $f_\lambda(w) = w'$ if and only if $\mathrm{val}_2(w') = 25\,\mathrm{val}_2(w)$.

This paper is organized as follows. In Section 2, we recall a few results related to our main question. In Section 3, we compute $\mathrm{val}_\ell(a_1^{n_1} \cdots a_\ell^{n_\ell})$ and derive an easy bijective proof of the fact that any nonnegative integer can be written in a unique way as

$$n = \binom{z_\ell}{\ell} + \binom{z_{\ell-1}}{\ell-1} + \cdots + \binom{z_1}{1}$$

with $z_\ell > z_{\ell-1} > \cdots > z_1 \geq 0$. In Section 4, we formulate the conjecture that the integers λ preserving recognizability over $\mathcal{B}_\ell$ are exactly those of the form $(\prod_{i=1}^k p_i^{\theta_i})^\ell$ where $p_1, \ldots, p_k > \ell$ are prime. We give partial results in that direction. In the next section, we make explicit the regular subsets of $\mathcal{B}_\ell$ and give an application to the $\mathcal{B}_\ell$-recognizability of arithmetic progressions.

2 First results about S-recognizability

In this section we collect a few results directly connected with our problem.

Theorem 1. *[6] Let $S = (L, \Sigma, <)$ be an abstract numeration system. Any arithmetic progression is S-recognizable.*

Let us denote by $\mathbf{u}_L(n)$ the number of words of length n belonging to L. The following result states that only some constants λ are good candidates for the multiplication within $\mathcal{B}_\ell$.

Theorem 2. *[8] Let $L \subseteq \Sigma^*$ be a regular language such that $\mathbf{u}_L(n) \in \Theta(n^k)$, $k \in \mathbb{N}$ and $S = (L, \Sigma, <)$. Preservation of the S-recognizability after multiplication by λ holds only if $\lambda = \beta^{k+1}$ for some $\beta \in \mathbb{N}$.*

As we shall see in the next section, $\mathbf{u}_{\mathcal{B}_\ell}(n) \in \Theta(n^{\ell-1})$ so we have to focus only on multiplicators of the kind β^ℓ. The particular case of $\mathbf{u}_L(n) \in \mathcal{O}(1)$ (i.e., L is *slender*) is interesting in itself and is settled as follows.

Theorem 3. *Let $L \subset \Sigma^*$ be a slender regular language and $S = (L, \Sigma, <)$. A set $X \subseteq \mathbb{N}$ is S-recognizable if and only if X is a finite union of arithmetic progressions.*

Proof. The proof is given in the appendix.

Corollary 1. *Let S be a numeration system built on a slender language. If $X \subseteq \mathbb{N}$ is S-recognizable then λX is S-recognizable for all $\lambda \in \mathbb{N}$.*

Finally, for a bounded language over a binary alphabet, the case is completely settled too, the aim of this paper being primarily to extend the following result.

Theorem 4. *[6] Let $\beta > 0$. For the abstract numeration system $S = (a^*b^*, \{a < b\})$, the multiplication by β^2 preserves S-recognizability if and only if β is an odd integer.*

3 $\mathcal{B}_\ell$-representation of an integer

In this section we determine the number of words of a given length in $\mathcal{B}_\ell$ and we obtain an algorithm for computing $\mathrm{rep}_\ell(n)$. Interestingly, this algorithm is related to the decomposition of n as a sum of binomial coefficients of a specified form. We give a few notation.

Definition 2. *Since we shall be mainly interested by the language $\mathcal{B}_\ell$, we set*

$$\mathbf{u}_\ell(n) := \mathbf{u}_{\mathcal{B}_\ell}(n) = \#(\mathcal{B}_\ell \cap \Sigma_\ell^n) \quad \textit{and} \quad \mathbf{v}_\ell(n) := \#(\mathcal{B}_\ell \cap \Sigma_\ell^{\le n}) = \sum_{i=0}^{n} \mathbf{u}_\ell(i).$$

The trim minimal automaton $\mathcal{A}_\ell$ of $\mathcal{B}_\ell$ has $\{q_1, \ldots, q_\ell\}$ as set of states. Each state is final, q_1 is initial and for $1 \le i \le j \le n$ we have a transition $q_i \xrightarrow{a_j} q_j$. For $i \in \{1, \ldots, \ell\}$, $\mathbf{u}_{q_i}(n)$ (resp. $\mathbf{v}_{q_i}(n)$) denotes the number of words of length n (resp. at most n) accepted from state q_i in $\mathcal{A}_\ell$. In particular, $\mathbf{u}_\ell(n) = \mathbf{u}_{q_1}(n)$.

Let us also recall that the binomial coefficient $\binom{i}{j}$ vanishes if $i < j$.

Lemma 1. *For all $\ell \geq 1$ and $n \geq 0$, we have*

$$\mathbf{u}_{\ell+1}(n) = \mathbf{v}_\ell(n) \tag{1}$$

and

$$\mathbf{u}_\ell(n) = \binom{n+\ell-1}{\ell-1}. \tag{2}$$

Proof. The proof is given in the appendix.

Lemma 2. *Let $S = (a_1^* \cdots a_\ell^*, \{a_1 < \cdots < a_\ell\})$. We have*

$$\mathrm{val}_\ell(a_1^{n_1} \cdots a_\ell^{n_\ell}) = \sum_{i=1}^{\ell} \binom{n_i + \cdots + n_\ell + \ell - i}{\ell - i + 1}.$$

Consequently, for any $n \in \mathbb{N}$,

$$|\mathrm{rep}_\ell(n)| = k \Leftrightarrow \underbrace{\binom{k+\ell-1}{\ell}}_{\mathrm{val}_\ell(a_1^k)} \leq n \leq \underbrace{\sum_{i=1}^{\ell} \binom{k+i-1}{i}}_{\mathrm{val}_\ell(a_\ell^k)}.$$

Proof. From the structure of the ordered language $\mathcal{B}_\ell$, one can show that

$$\mathrm{val}_\ell(a_1^{n_1} \cdots a_\ell^{n_\ell}) = \mathrm{val}_\ell(a_1^{n_1+\cdots+n_\ell}) + \mathrm{val}_{\{a_2,\ldots,a_n\}}(a_2^{n_2} \cdots a_\ell^{n_\ell})$$

where notation like $\mathrm{val}_{\{a_2,\ldots,a_n\}}(w)$ specifies not only the size but the alphabet of the bounded language on which the numeration system is built. (To understand this formula, an example is given below in the case $\ell = 3$.) Iterating the latter decomposition, we obtain

$$\mathrm{val}_\ell(a_1^{n_1} \cdots a_\ell^{n_\ell}) = \sum_{i=1}^{\ell} \mathrm{val}_{\ell-i+1}(a_1^{n_i+\cdots+n_\ell}).$$

Moreover, it is well known that $\mathrm{val}_\ell(a_1^n) = \mathbf{v}_\ell(n-1)$. Hence the conclusion follows using relations (1) and (2).

Example 2. Consider the words of length 3 in the language $a^*b^*c^*$,

$$aaa < aab < aac < abb < abc < acc < bbb < bbc < bcc < ccc.$$

We have $\mathrm{val}_3(aaa) = \binom{5}{3} = 10$ and $\mathrm{val}_3(acc) = 15$. If we apply the erasing morphism $\varphi : \{a, b, c\} \to \{a, b, c\}^*$ defined by $\varphi(a) = \varepsilon$, $\varphi(b) = b$ and $\varphi(c) = c$ on the words of length 3, we get

$$\varepsilon < b < c < bb < bc < cc < bbb < bbc < bcc < ccc.$$

So the ordered list of words of length 3 in $a^*b^*c^*$ contains an ordered copy of the words of length at most 2 in the language b^*c^* and to obtain $\mathrm{val}_3(acc)$, we just add to $\mathrm{val}_3(aaa)$ the position of the word cc in the ordered language b^*c^*. In other words, $\mathrm{val}_3(acc) = \mathrm{val}_3(aaa) + \mathrm{val}_2(cc)$ where val_2 is considered as a map defined on the language b^*c^*.

The following result is given in [5]. Here we obtain a bijective proof relying only on the use of abstract numeration systems on a bounded language.

Corollary 2. *Let $\ell \in \mathbb{N} \setminus \{0\}$. Any integer n can be uniquely written as*

$$n = \binom{z_\ell}{\ell} + \binom{z_{\ell-1}}{\ell-1} + \cdots + \binom{z_1}{1} \tag{3}$$

with $z_\ell > z_{\ell-1} > \cdots > z_1 \geq 0$.

Proof. The mapping $\mathrm{rep}_\ell : \mathbb{N} \to a_1^* \cdots a_\ell^*$ is a one-to-one correspondence. So any integer n has a unique representation of the form $a_1^{n_1} \cdots a_\ell^{n_\ell}$ and the conclusion follows from Lemma 2.

The general method given in [6, Algorithm 1] has a special form in the case of the language $\mathcal{B}_\ell$. We derive an algorithm computing the decomposition (3) or equivalently the $\mathcal{B}_\ell$-representation of any integer.

Algorithm 1 *Let* `n` *be an integer and* `l` *be a positive integer. The following algorithm produces integers* `z(l)`,...,`z(1)` *corresponding to the z_i's appearing in the decomposition* (3) *of* `n` *given in Corollary 2.*

```
For i=l,l-1,...,1 do
   if n>0,
      find t such that (t choose i) ≤ n < (t+1 choose i)
      z(i)←t
      n←n-(t choose i)
   otherwise, z(i)←i-1
```

Consider now the triangular system having $\alpha_1, \ldots, \alpha_\ell$ as unknowns

$$\alpha_i + \cdots + \alpha_\ell = \mathtt{z}(\ell - i + 1) - \ell + i, \quad i = 1, \ldots, \ell.$$

One has $\mathrm{rep}_\ell(\mathtt{n}) = a_1^{\alpha_1} \cdots a_\ell^{\alpha_\ell}$.

Remark 3. To speed up the computation of `t` in the above algorithm, one can benefit from numerical analysis methods. Indeed, for given `i` and `n`, $\binom{\mathtt{t}}{\mathtt{i}} - \mathtt{n}$ is a polynomial in `t` of degree `i` and we are looking for the largest root z of this polynomial. Therefore, $\mathtt{t} = \lfloor z \rfloor$.

Example 3. For $\ell = 3$, one gets for instance

$$12345678901234567890 = \binom{4199737}{3} + \binom{3803913}{2} + \binom{1580642}{1}$$

and solving the system

$$\left.\begin{aligned} n_1 + n_2 + n_3 &= 4199737 - 2 \\ n_2 + n_3 &= 3803913 - 1 \\ n_3 &= 1580642 \end{aligned}\right\} \Leftrightarrow (n_1, n_2, n_3) = (395823, 2223270, 1580642),$$

we have $\mathrm{rep}_3(12345678901234567890) = a^{395823} b^{2223270} c^{1580642}$.

4 Multiplication by $\lambda = \beta^\ell$

In the case of a bounded language on three letters, if multiplication by some constant preserves recognizability, then, by Theorem 2 and Lemma 1, this constant must be a cube. On two letters, only odd squares have the expected property, on three letters, one can also exclude whole classes of cubes which do not preserve recognizability.

Theorem 5. *For the abstract numeration system $S = (a^*b^*c^*, \{a < b < c\})$, if $\beta \in \mathbb{N} \setminus \{0,1\}$ is such that $\beta \not\equiv \pm 1 \pmod 6$ then the multiplication by β^3 does not preserve the S-recognizability.*

Proof. The proof is given in the appendix.

Thanks to computer experiments, we conjecture the following result.

Conjecture 1 *Multiplication by β^ℓ preserves S-recognizability for the abstract numeration system $S = (a_1^* \cdots a_\ell^*, \{a_1 < \cdots < a_\ell\})$ built on the bounded language $\mathcal{B}_\ell$ over ℓ letters if and only if*

$$\beta = \prod_{i=1}^{k} p_i^{\theta_i}$$

where $p_1, \ldots, p_k$ are prime numbers strictly greater than ℓ. Otherwise stated, multiplication by β^ℓ does <u>not</u> preserve S-recognizability if and only if

$$\exists M \in \{2, \ldots, \ell\} : \beta \equiv 0 \pmod M.$$

In what follows, we assume that $\ell \geq 2$ and $\beta \in 2\mathbb{N} + 3$ are given once and for all. The next result relates the length of the $\mathcal{B}_\ell$-representations of n and $\beta^\ell n$, roughly by a factor β.

Lemma 3. *For $n \in \mathbb{N}$ large enough, we have*

$$|\mathrm{rep}_\ell(\beta^\ell n)| = \beta\, |\mathrm{rep}_\ell(n)| + \frac{(\beta-1)(\ell-1)}{2} + i$$

with $i \in \{-1, 0, \ldots, \beta - 1\}$.

Proof. The proof is given in the appendix.

Using this latter lemma, we are able to define a partition of $\mathbb{N}$.

Definition 3. *For all $i \in \{-1, 0, \ldots, \beta - 1\}$ and $k \in \mathbb{N}$ large enough, we define*

$$\mathcal{R}_{i,k} := \left\{ n \in \mathbb{N} : |\mathrm{rep}_\ell(n)| = k \text{ and } |\mathrm{rep}_\ell(\beta^\ell n)| = \beta\, k + \frac{(\beta-1)(\ell-1)}{2} + i \right\}.$$

The following result is technical but it is interesting to note that its hypothesis is exactly the condition introduced in our conjecture.

Lemma 4. *If β satisfies the condition given in Conjecture 1, then for any $u \geq \ell$, we have*
$$\binom{u}{\ell} \equiv \binom{u+\beta^\ell}{\ell} \pmod{\beta^\ell}.$$

Proof. The proof is given in the appendix.

From now on, we assume that β satisfies the condition of Conjecture 1. A deep inspection of the multiplication by β^ℓ using the partition induced by Lemma 3 provides us with the following observation.

Proposition 1. *Let $i \in \{0,\ldots,\beta-1\}$. There exists a constant $\mathbf{L} \geq 0$ (depending only on ℓ and β) such that for all $k \geq \mathbf{L}$, if $m = \min \mathcal{R}_{i,k}$ and $n = \min \mathcal{R}_{i,k+\beta^{\ell-1}}$ then*
$$\forall t \in \{2,\ldots,\ell\} : |\mathrm{rep}_\ell(\beta^\ell m)|_{a_t} = |\mathrm{rep}_\ell(\beta^\ell n)|_{a_t}.$$
Furthermore, $|\mathrm{rep}_\ell(\beta^\ell m)|_{a_1} + \beta^\ell = |\mathrm{rep}_\ell(\beta^\ell n)|_{a_1}$

Proof. The proof is given in the appendix.

Corollary 3. *Let $i \in \{0,\ldots,\beta-1\}$ and $k \geq \mathbf{L}$. Set*
$$A_i(k) := \binom{\beta\, k + \frac{(\beta-1)(\ell-1)}{2} + i + \ell - 1}{\ell}.$$
The first element belonging to $\mathcal{R}_{i,k}$ is given by $\left\lceil \frac{A_i(k)}{\beta^\ell} \right\rceil$.

Proof. It is a direct consequence of the proof of Proposition 1.

Remark 4. Proposition 1 says nothing about the smallest element in $\mathcal{R}_{-1,k}$. For k large enough, it can be shown that there exists $C > 0$ such that
$$\underbrace{\binom{\beta k + \frac{(\beta-1)(\ell-1)}{2} + \ell - 1}{\ell}}_{\mathrm{val}_\ell(a_1^{\beta k + (\beta-1)(\ell-1)/2})} - \beta^\ell \underbrace{\binom{k+\ell-1}{\ell}}_{\mathrm{val}_\ell(a_1^k)} = C\, k^{\ell-2} + o(k^{\ell-2}) > 0$$
which implies that a_1^k is the first word of length k whose image under val_ℓ belongs to $\mathcal{R}_{-1,k}$.

Definition 4. *Let $i \in \{0,\ldots,\beta-1\}$. In view of Proposition 1, if m_k is the first word in $\mathcal{R}_{i,k}$ ($k \geq \mathbf{L}$) then for $t = 2,\ldots,\ell$, $|\mathrm{rep}_\ell(\beta^\ell m_k)|_{a_t}$ depends only on k $\pmod{\beta^{\ell-1}}$ and is therefore denoted $\alpha_t^{(j)}$ if $0 \leq j < \beta^{\ell-1}$ and $j \equiv k \pmod{\beta^{\ell-1}}$.*

For $i \in \{0,\ldots,\beta-1\}$ and $j \in \{0,\ldots,\beta^{\ell-1}-1\}$, it is thus convenient to set
$$M_{i,j} := a_2^{\alpha_t^{(j)}} \cdots a_\ell^{\alpha_\ell^{(j)}} \quad \text{and} \quad \mu_{i,j} := \mathrm{val}_{\{a_2,\ldots,a_\ell\}}(M_{i,j}).$$
From the proof of Proposition 1, it can be shown that
$$\mu_{i,j} = -A_i(j + n\,\beta^{\ell-1}) \pmod{\beta^\ell}$$
for any n such that $j + n\,\beta^{\ell-1} \geq \mathbf{L}$.

Example 4. Let $\ell = 3$ and $\beta = 5$. The number 171717 (resp. 172739) is the first element belonging to $\mathcal{R}_{0,100}$ (resp. $\mathcal{R}_{1,100}$). We have

$$\mathrm{rep}_3(171717) = a^{95}b^3c^2 \text{ and } \mathrm{rep}_3(5^3\, 171717) = a^{490}\mathbf{b^{14}c^0},$$

$$\mathrm{rep}_3(172739) = a^{55}b^{41}c^4 \text{ and } \mathrm{rep}_3(5^3\, 172739) = a^{493}\mathbf{b^{0}c^{12}}.$$

So $M_{0,0} = b^{14}$ (resp. $M_{1,0} = c^{12}$) and $\mu_{0,0} = \mathrm{val}_{\{b,c\}}(b^{14}) = 105$ (resp. $\mu_{1,0} = \mathrm{val}_{\{b,c\}}(c^{12}) = 90$). The number 333396 (resp. 334986) is the first element belonging to $\mathcal{R}_{0,125}$ (resp. $\mathcal{R}_{1,125}$)and

$$\mathrm{rep}_3(333396) = a^{119}b^6c^0 \text{ and } \mathrm{rep}_3(5^3\, 333396) = a^{615}\mathbf{b^{14}c^0},$$

$$\mathrm{rep}_3(333396) = a^{69}b^{41}c^{15} \text{ and } \mathrm{rep}_3(5^3\, 333396) = a^{618}\mathbf{b^{0}c^{12}}.$$

The following result describes precisely how multiplication by β^ℓ affects representations inside a region $\mathcal{R}_{i,k}$.

Proposition 2. *Let $k \geq \mathbf{L}$ be such that $k \equiv j \pmod{\beta^{\ell-1}}$ and m be the first element of $\mathcal{R}_{i,k}$, $0 \leq i \leq \beta - 1$. If $m + t$ belongs to $\mathcal{R}_{i,k}$ then*

$$\mathrm{rep}_\ell(\beta^\ell(m+t)) = a_1^{s(t)}\, \mathrm{rep}_{\{a_2,\dots,a_\ell\}}(\mu_{i,j} + t\ \beta^\ell)$$

where $s(t)$ is such that $|\mathrm{rep}_\ell(\beta^\ell(m+t))| = \beta\, k + \frac{(\beta-1)(\ell-1)}{2} + i$.

Proof. Trivial.

Corollary 4. *Let $i \in \{0,\dots,\beta-1\}$ and $j \in \{0,\dots,\beta^{\ell-1}-1\}$. We have*

$$\bigcup_{n:j+n\beta^{\ell-1}\geq \mathbf{L}} \{\mathrm{rep}_\ell(\beta^\ell\, m) \mid m \in \mathcal{R}_{i,j+n\beta^{\ell-1}}\}$$

$$= \left[a_1^*\, \mathrm{rep}_{\{a_2,\dots,a_\ell\}}(\mu_{i,j} + \mathbb{N}\ \beta^\ell)\right] \bigcap \Sigma_\ell^C (\Sigma_\ell^{\beta^\ell})^*$$

where $C = \beta j + \frac{(\beta-1)(\ell-1)}{2} + i + n_0\beta^\ell$ and $n_0 = \min\{n \mid j + n\beta^{\ell-1} \geq \mathbf{L}\}$.

Example 5. Let $\ell = 3$ and $\beta = 5$. The first element belonging to $\mathcal{R}_{0,100}$ (resp. $\mathcal{R}_{0,125}$) is $m = 171717$ (resp. $n = 333396$). We have $\#\mathcal{R}_{0,100} = 1022$ and $\#\mathcal{R}_{0,100} = 1590$. We get the following table illustrating Proposition 2.

i	$\Psi(\mathrm{rep}_3(5^3\,(m+i)))$	$\Psi(\mathrm{rep}_3(5^3\,(n+i)))$	$\Psi(\mathrm{rep}_{\{b,c\}}(\mu_{0,0} + 5^3\, i))$
0	$(490, 14, 0)$	$(615, 14, 0)$	$(14, 0)$
1	$(484, 0, 20)$	$(609, 0, 20)$	$(0, 20)$
2	$(478, 22, 4)$	$(603, 22, 4)$	$(22, 4)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
1021	$(0, 34, 470)$	$(125, 34, 470)$	$(34, 470)$
1022	$\times$	$(124, 415, 90)$	$(415, 90)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
1589	$\times$	$(0, 34, 595)$	$(34, 595)$

5 Regular subsets of $\mathcal{B}_\ell$

To study preservation of recognizability after multiplication by a constant, one has to consider an arbitrary recognizable subset $X \subseteq \mathbb{N}$ and show that $\beta^\ell X$ is still recognizable. To that end, we recall the form of the regular subsets of $\mathcal{B}_\ell$.

Definition 5. *A subset X of $\mathbb{N}^k$ is* linear *if there exists $p_0, p_1, \cdots, p_t \in \mathbb{N}^k$ such that*

$$X = p_0 + \mathbb{N}\,p_1 + \cdots + \mathbb{N}\,p_t = \{p_0 + \lambda_1 p_1 + \cdots + \lambda_t p_t \mid \lambda_1, \ldots, \lambda_t \in \mathbb{N}\}.$$

The vectors $p_1, \ldots, p_t$ are said to be the periods *of X. A set is* semi-linear *if it is a finite union of linear sets. The set of periods of a semi-linear set is the union of the sets of periods of the corresponding linear sets. For $x \in \mathbb{N}^k$, $[x]_i$ denotes its i-th component.*

The following result is obvious.

Lemma 5. *A set $X \subseteq \mathbb{N}$ is $\mathcal{B}_\ell$-recognizable if and only if $\Psi(\mathrm{rep}_\ell(X))$ is a semi-linear set whose periods are integer multiple of canonical vectors $\mathbf{e}_i$'s where $[\mathbf{e}_i]_j = \delta_{i,j}$.*

With such a characterization, it is not difficult to obtain Theorem 1 in a different way.

Proposition 3. *Let $p, q \in \mathbb{N}$. The set $\Psi(\mathrm{rep}_\ell(q + \mathbb{N}\,p)) \subseteq \mathbb{N}^\ell$ is a finite union of linear sets of the form*

$$p_0 + \mathbb{N}\,\theta\,\mathbf{e}_1 + \cdots + \mathbb{N}\,\theta\,\mathbf{e}_\ell \quad \textit{for some } \theta \in \mathbb{N}.$$

Proof. The proof is given in the appendix.

Example 6. In Figure 1, the x-axis (resp. y-axis) counts the number of a_1's (resp. a_2's) in a word. The empty word corresponds to the lower-left corner. A point in $\mathbb{N}^2$ of coordinates (i, j) has its color determined by the value of $\mathrm{val}_2(a_1^i\, a_2^j)$ modulo p (with $p = 3, 5, 6$ and 8 respectively). There are therefore p possible colors. On this figure, we represent words $a_1^i\, a_2^j$ for $0 \le i, j \le 19$.

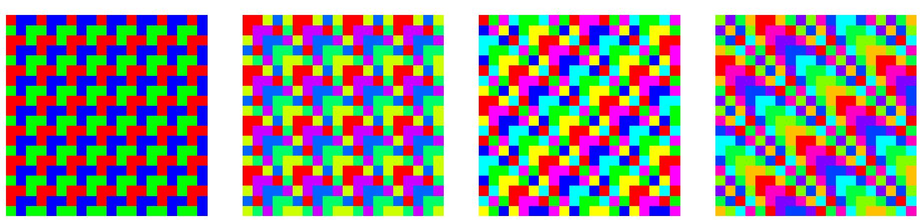

Fig. 1. $\Psi(\mathrm{rep}_2(p\mathbb{N} + k))$ for $p = 3, 5, 6, 8$.

6 Conclusions

We have obtained several structural results about the words in $\mathcal{B}_\ell$ before and after multiplication by β^ℓ. Nevertheless, a proof of Conjecture 1 is still at large.

One way to prove Conjecture 1 could be to consider an arbitrary lattice $\mathcal{L} = p_0 + \mathbb{N}\,\gamma_1\,\mathbf{e_1} + \cdots + \mathbb{N}\,\gamma_\ell\,\mathbf{e}_\ell \subseteq \mathbb{N}^\ell$ with $\gamma_i \in \mathbb{N}$ (indeed, recognizable sets correspond to finite unions of such lattices) and study separately multiplication by β^ℓ for each

$$X_{i,j} := \mathrm{val}_\ell(\Psi^{-1}(\mathcal{L})) \bigcap \left(\bigcup_{n:j+n\beta^{\ell-1}\geq \mathbf{L}} \mathcal{R}_{i,j+n\beta^{\ell-1}} \right),$$

$i \in \{-1,\ldots,\beta-1\}$, $j \in \{0,\ldots,\beta^{\ell-1}-1\}$. Unfortunately, it is not an easy task to see that $\mathrm{rep}_\ell(\beta^\ell\,X_{i,j})$ is still regular even if we take into account Lemma 3 and Propositions 1 or 2.

Up to now, such an approach seems to be fruitful only for an alphabet of size $\ell = 2$. Indeed, for a given lattice $\mathcal{L} = p_0 + \mathbb{N}\,\gamma_1\,\mathbf{e_1} + \mathbb{N}\,\gamma_2\,\mathbf{e_2}$, if we denote by $m_{i,k}$ (resp. $\tau_{i,k}$) the first element in $\mathcal{R}_{i,k}$ (resp. the first element in $\mathcal{R}_{i,k} \cap \mathrm{val}_2(\Psi^{-1}(\mathcal{L}))$), then $g_i(k) := \tau_{i,k} - m_{i,k}$ is ultimately periodic. This argument can then be used together with Proposition 2 to obtain an alternative proof of Theorem 4. But our attempts to solve the conjecture for $\ell > 2$ with the same arguments are still unsuccessful. A possible drawback is that the difference between two consecutive elements in $\mathcal{R}_{i,k} \cap \mathrm{val}_\ell(\Psi^{-1}(\mathcal{L}))$ is constant (resp. non-constant) for $\ell = 2$ (resp. for $\ell \geq 3$). Nevertheless, we hope that the reader has now a better understanding of how words are distributed with respect to the multiplication by β^ℓ. Moreover, partial results like Lemma 4 seem to plead in favor of our conjecture.

References

1. M. Andraşiu, G. Păun, J. Dassow, A. Salomaa, Language-theoretic problems arising from Richelieu cryptosystems, *Theoret. Comput. Sci.* **116** (1993), 339–357.
2. V. Bruyère, G. Hansel, Bertrand numeration systems and recognizability, *Theoret. Comput. Sci.* **181** (1997) 17–43.
3. S. Eilenberg, *Automata, Languages, and Machines* vol. A, Academic Press, New York, (1974).
4. S. Ginsburg, E. H. Spanier, Bounded ALGOL-like languages, *Trans. Am. Math. Soc.* **113** (1964), 333-368.
5. G. Katona, A theorem on finite sets, Theory of Graphs, Proc. Colloquium, Tihany, Hungary (1966), 187–207.
6. P.B.A. Lecomte, M. Rigo, Numeration systems on a regular language, *Theory Comput. Syst.* **34** (2001), 27–44.
7. G. Păun, A. Salomaa, Thin and slender languages, *Discrete Appl. Math.* **61** (1995), 257–270.
8. M. Rigo, Numeration systems on a regular language: arithmetic operations, recognizability and formal power series, *Theoret. Comput. Sci.* **269** (2001), 469–498.
9. J. Shallit, Numeration systems, linear recurrences, and regular sets, *Inform. and Comput.* **113** (1994), 331–347.

7 Appendix: omitted proofs

Here, one can find the omitted proofs of Theorems 3 and 5, Lemmata 1, 3 and 4, Propositions 1 and 3.

Let us first give the definition of a slender language and recall a characterization of such languages.

Definition 6. *[1] Let d be a positive integer. The language L is said to be* d-slender *if for all $n \geq 0$, $\mathbf{u}_L(n) \leq d$. The language L is said to be* slender *if it is d-slender for some d. A regular language is slender if and only if for some $k \geq 1$ and words x_i, y_i, z_i, $1 \leq i \leq k$,*

$$L = \bigcup_{i=1}^{k} x_i\, y_i^* z_i.$$

In this case, L is said to be a union of single loops *[7, 9]. Moreover, we can assume that the sets $x_i\, y_i^* z_i$ are pairwise disjoint.*

Proof (Proof of Theorem 3). By the characterization of slender languages, we have

$$L = \bigcup_{i=1}^{k} x_i\, y_i^* z_i \cup F_0,\ \ x_i, z_i \in \Sigma^*, y_i \in \Sigma^+$$

where the sets $x_i\, y_i^* z_i$ are pairwise disjoint and F_0 is a finite set. The sequence $(\mathbf{u}_L(n))_{n\in\mathbb{N}}$ is ultimately periodic of period $C = \mathrm{lcm}_j |y_j|$. Moreover, for n large enough, if $x_i\, y_i^n\, z_i$ is the m-th word of length $|x_i\, z_i| + n\,|y_i|$ then $x_i\, y_i^{n+C/|y_i|}\, z_i$ is the m-th word of length $|x_i\, z_i| + n\,|y_i| + C$. Roughly speaking, for n sufficiently large, the structures of the ordered sets of words of length n and $n + C$ are the same.

The regular subsets of L are of the form

$$\bigcup_{j\in J} x_j\,(y_j^{\alpha_j})^* z_j \cup F_0' \tag{4}$$

where $J \subseteq \{1, \ldots, k\}$, $\alpha_j \in \mathbb{N}$ for $j \in J$ and F_0' is a finite subset of L.

We can now conclude. If X is S-recognizable, then $\mathrm{rep}_S(X)$ is a regular subset of L of the form (4). In view of the first part of the proof, it is clear that X is ultimately periodic. The converse is immediate by Theorem 1.

Example 7. Consider the language $L = ab^*c \cup b(aa)^*c$. It contains exactly two words of each positive even length: $ab^{2i}c < ba^{2i}c$ and one word for each odd length larger than 2: $ab^{2i+1}c$. The sequence $\mathbf{u}_L(n)$ is ultimately periodic of period two: $0, 0, 2, 1, 2, 1, \ldots$.

Proof (Proof of Lemma 1). Relation (1) follows from the fact that the set of words of length n belonging to $\mathcal{B}_{\ell+1}$ is partitioned into

$$\bigcup_{i=0}^{n} \left(a_1^* \cdots a_\ell^* \cap \Sigma_\ell^i\right) a_{\ell+1}^{n-i}.$$

To obtain (2), we proceed by induction on $\ell \geq 1$. Indeed, for $\ell = 1$, it is clear that $\mathbf{u}_1(n) = 1$ for all $n \geq 0$. Assume that (2) holds for ℓ and let us verify it still holds for $\ell + 1$. Thanks to (1), we have

$$\mathbf{u}_{\ell+1}(n) = \sum_{i=0}^{n} \mathbf{u}_\ell(i) = \sum_{i=0}^{n} \binom{i+\ell-1}{\ell-1} = \sum_{i=0}^{n} \binom{i+\ell-1}{i}.$$

To conclude, it is an easy exercise to show by induction on $n \geq 0$ that

$$\sum_{i=0}^{n} \binom{i+\ell-1}{i} = \binom{n+\ell}{\ell}.$$

Proof (Proof of Theorem 5). Assume first $\beta \equiv 2 \pmod 6$. For n large enough, we have

$$\mathrm{rep}_3\left[(6k+2)^3\, \mathrm{val}_3(a^n)\right] = a^r\, b^{s+(3k+1)n}\, c^{t+(3k+1)n}$$

where the constants r, s, t are given by

$$r = 4k + 6k^2, \quad s = 5k + 11k^2 + 24k^3 + 18k^4, \quad t = -3k - 17k^2 - 24k^3 - 18k^4.$$

This can be checked by applying val_3 on both sides and obtain an identity involving binomial coefficients. If $\beta \equiv 3 \pmod 6$, then for n large enough,

$$\mathrm{rep}_3\left[(6k+3)^3\, \mathrm{val}_3(a^n)\right] = a^r\, b^{s+(2k+1)n}\, c^{t+(4k+2)n}$$

where the constants r, s, t are given by

$$r = 1+6k+6k^2,\ s = 1+11k+27k^2+36k^3+18k^4,\ t = -1-11k-33k^2-36k^3-18k^4.$$

If $\beta \equiv 4 \pmod 6$, then for n large enough,

$$\mathrm{rep}_3\left[(6k+4)^3\, \mathrm{val}_3(a^n)\right] = a^r\, b^{s+(3k+2)n}\, c^{t+(3k+2)n}$$

where the constants r, s, t are given by

$$r = 2+8k+6k^2,\ s = 4+23k+47k^2+48k^3+18k^4,\ t = -4-25k-53k^2-48k^3-18k^4.$$

Finally, if $\beta \equiv 0 \pmod 6$, then for n large enough,

$$\mathrm{rep}_3\left[(6k)^3\, \mathrm{val}_3(a^n)\right] = a^r\, b^{s+5k\,n}\, c^{t+k\,n}$$

where the constants r, s, t are given by

$$r = -1 + 6k^2, \quad s = -1 + 5k - 3k^2, \quad t = k - 3k^2 - 18k^4.$$

Let $X \subset \mathbb{N}$ be such that $\mathrm{rep}_3(X) = a^*$. From the above formulas, it is obvious that X is S-recognizable but that $\mathrm{rep}_3(\beta^3 X)$ is a context-free language which is not regular.

Proof (Proof of Lemma 3). Using Lemma 2, an integer n has a $\mathcal{B}_\ell$-representation $\mathrm{rep}_\ell(n)$ of length k if and only if $\mathrm{val}_\ell(a_1^k) \le n < \mathrm{val}_\ell(a_1^{k+1})$. Therefore for such an integer n we have

$$\beta^\ell \binom{\ell+k-1}{\ell} \le \beta^\ell n < \beta^\ell \binom{\ell+k}{\ell}. \tag{5}$$

First, let us observe that

$$\mathrm{val}_\ell(a_1^{\beta k}) = \binom{\ell+\beta k-1}{\ell} \le \beta^\ell \binom{\ell+k-1}{\ell} \le \beta^\ell n.$$

This means that $k' := |\mathrm{rep}_\ell(\beta^\ell n)| \ge \beta k$ and we write can k' as $\beta k + u$ for some $u \ge 0$. What we have to show is that

$$\frac{(\beta-1)(\ell-1)}{2} - 1 \le u \le \frac{(\beta-1)(\ell-1)}{2} + \beta - 1.$$

Since $|\mathrm{rep}_\ell(\beta^\ell n)| = k'$, we have

$$\binom{\ell+k'-1}{\ell} \le \beta^\ell n < \binom{\ell+k'}{\ell}. \tag{6}$$

From (5) and (6), we deduce that

$$\binom{\ell+k'-1}{\ell} < \beta^\ell \binom{\ell+k}{\ell} \text{ and } \beta^\ell \binom{\ell+k-1}{\ell} < \binom{\ell+k'}{\ell}.$$

Substituting k' with $\beta k + u$ in the first inequality, we get

$$\prod_{v=0}^{\ell-1} (\beta k + u + v) < \beta^\ell \prod_{v=1}^{\ell} (k+v). \tag{7}$$

The expression in the l.h.s. can be written as follows

$$\sum_{i=0}^{\ell} \alpha_i (\beta k + u)^i = \sum_{j=0}^{\ell} \sum_{i=j}^{\ell} \alpha_i \binom{i}{j} (\beta k)^{i-j}\, u^j \tag{8}$$

for some positive integer coefficients α_i's with $\alpha_\ell = 1$, $\alpha_{\ell-1} = s(\ell-1)$, $\ldots$, $\alpha_1 = (\ell-1)!$ and for $\alpha_0 = 0$, where $s(n) := 1 + 2 + \cdots + n$. In the same way, the r.h.s. can be written as $\beta^\ell \sum_{i=0}^{\ell} \gamma_i\, k^i$ with $\gamma_\ell = 1$, $\gamma_{\ell-1} = s(\ell)$, $\ldots$, $\gamma_0 = \ell!$. Subtracting to both sides of (7) the term corresponding to $j = 0$ in (8), we get

$$\underbrace{u \sum_{j=1}^{\ell} \sum_{i=j}^{\ell} \alpha_i \binom{i}{j} (\beta k)^{i-j}\, u^{j-1}}_{:=T(k)} < \sum_{i=0}^{\ell-1} (\beta^{\ell-i}\gamma_i - \alpha_i)(\beta k)^i.$$

Since the length k can be arbitrarily large, we shall consider these expressions as polynomials in k of degree $\ell-1$. Let us show that u is bounded above and assume $u \geq 2$. The leading term in $T(k)$ is $\ell(\beta k)^{\ell-1}$ and since T has positive coefficients, we have

$$u\,\ell\,(\beta k)^{\ell-1} < u\,\ell\,(\beta k)^{\ell-1} + T - \ell\,(\beta k)^{\ell-1} < u\,T < \sum_{i=0}^{\ell-1}(\beta^{\ell-i}\gamma_i - \alpha_i)(\beta k)^i.$$

Thus, dividing by $\ell\,(\beta k)^{\ell-1}$

$$u + \frac{T - \ell\,(\beta k)^{\ell-1}}{\ell\,(\beta k)^{\ell-1}} < \frac{\beta s(\ell) - s(\ell-1)}{\ell} + \sum_{i=0}^{\ell-2}\frac{\beta^{\ell-i}\gamma_i - \alpha_i}{\ell}(\beta k)^{i-\ell+1}.$$

Now, letting k tend to infinity, we obtain

$$u \leq \frac{\beta s(\ell) - s(\ell-1)}{\ell} = \frac{(\beta-1)(\ell-1)}{2} + \beta.$$

To conclude, one has to obtain $u \leq \frac{(\beta-1)(\ell-1)}{2} + \beta - 1$. This can be checked by showing (in the same way as in Remark 4) that for k large enough, we have

$$\beta^\ell n < \beta^\ell \binom{\ell+k}{\ell} \leq \binom{\beta k + \frac{(\beta-1)(\ell-1)}{2} + \beta + \ell - 1}{\ell}$$

meaning that $\beta^\ell n$ is less than the numerical value of the first word of length $\beta k + \frac{(\beta-1)(\ell-1)}{2} + \beta$.

To obtain the expected lower bound for u, one can proceed in the same lines as above taking advantage that we have already shown that u is bounded.

Proof (Proof of Lemma 4). Let $u, v \geq \ell$. One has

$$\binom{v}{\ell} - \binom{u}{\ell} = \frac{v(v-1)\cdots(v-\ell+1) - u(u-1)\cdots(u-\ell+1)}{\ell!}.$$

The numerator on the r.h.s. is an integer divisible by $\ell!$. Moreover, this numerator is also clearly divisible by $v-u$ (indeed, it is of the form $P(v) - P(u)$ for some polynomial P).

Notice that for $v = u + \beta^\ell$, the corresponding numerator is divisible by $\ell!$ and also by β^ℓ. But since any prime factor of β is larger than ℓ, $\ell!$ and β^ℓ are relatively prime. Consequently, the corresponding numerator is divisible by $\beta^\ell \ell!$.

Proof (Proof of Proposition 1). Since $m \in \mathcal{R}_{i,k}$, by Lemma 2, we have

$$\underbrace{\binom{\beta\,k + \frac{(\beta-1)(\ell-1)}{2} + i + \ell - 1}{\ell}}_{=:A_i(k)} \leq \beta^\ell m$$

$$\leq \underbrace{\sum_{j=1}^{\ell}\binom{\beta\,k + \frac{(\beta-1)(\ell-1)}{2} + i + j - 1}{j}}_{=:B_i(k)}.$$

And since $m-1 \in \mathcal{R}_{i-1,k}$, we also obtain

$$\underbrace{\binom{\beta\, k + \frac{(\beta-1)(\ell-1)}{2} + i + \ell - 2}{\ell} + \beta^\ell}_{=:C_i(k)}$$

$$\leq \beta^\ell m \leq \underbrace{\sum_{j=1}^{\ell} \binom{\beta\, k + \frac{(\beta-1)(\ell-1)}{2} + i + j - 2}{j} + \beta^\ell}_{=:D_i(k)}.$$

It is straightforward to check that $D_i(k) = A_i(k) - 1 + \beta^\ell$,

$$A_i(k) - C_i(k) = \frac{\beta^{\ell-1}}{(\ell-1)!}\, k^{\ell-1} + o(k^{\ell-1})$$

and

$$B_i(k) - D_i(k) = \frac{\beta^{\ell-1}}{(\ell-1)!}\, k^{\ell-1} + o(k^{\ell-1}).$$

So there exists $\mathbf{L}$ such that for all $k \geq \mathbf{L}$, we have $A_i(k) > C_i(k)$, $B_i(k) > D_i(k)$ and

$$A_i(k) \leq \beta^\ell m < A_i(k) + \beta^\ell.$$

Otherwise stated, there exists a unique integer $\mu_i(k)$ such that

$$\beta^\ell m = A_i(k) + \mu_i(k) \quad \text{and} \quad 0 \leq \mu_i(k) \leq \beta^\ell - 1.$$

In the same way, there exists a unique integer $\mu_i(k+\beta^{\ell-1})$ such that

$$\beta^\ell n = A_i(k+\beta^{\ell-1}) + \mu_i(k+\beta^{\ell-1}) \quad \text{and} \quad 0 \leq \mu_i(k+\beta^{\ell-1}) \leq \beta^\ell - 1.$$

From Lemma 4, we deduce that $A_i(k) \equiv A_i(k+\beta^{\ell-1}) \pmod{\beta^\ell}$ and consequently, $\mu_i(k) = \mu_i(k+\beta^{\ell-1})$. From Lemma 2, we deduce that

$$\mathrm{rep}_\ell(\beta^\ell m) = a_1^t\, \mathrm{rep}_{\{a_2,\ldots,a_\ell\}}(\mu_i(k))$$

where t is such that $|\mathrm{rep}_\ell(\beta^\ell m)| = \beta\, k + \frac{(\beta-1)(\ell-1)}{2} + i$ and

$$\mathrm{rep}_\ell(\beta^\ell n) = a_1^{t+\beta^\ell}\, \mathrm{rep}_{\{a_2,\ldots,a_\ell\}}(\mu_i(k)).$$

Proof (Proof of Proposition 3). We use the notation from Definition 2 about the minimal automaton of $\mathcal{B}_\ell$. For any, $i_1,\ldots,i_\ell \in \mathbb{N}$, we have

$$\mathrm{val}_\ell(a_1^{i_1} \cdots a_\ell^{i_\ell}) = \sum_{j=1}^{\ell} \mathbf{v}_{q_j}(i_j + \cdots + i_\ell - 1).$$

Indeed, we have to count the words genealogically less than $a_1^{i_1} \cdots a_\ell^{i_\ell}$ in the language. First we have the words of length less than $i_1 + \cdots + i_\ell$, there are exactly $\mathbf{v}_{q_1}(i_1 + \cdots + i_\ell - 1)$ words of this kind. Then amongst the words of length $i_1 + \cdots + i_\ell$, the are $\mathbf{v}_{q_2}(i_2 + \cdots + i_\ell - 1)$ words starting with at least $i_1 + 1$ letters a_1's. After that, there are $\mathbf{v}_{q_3}(i_3 + \cdots + i_\ell - 1)$ words starting with $a_1^{i_1}$ followed by at least $i_2 + 1$ letters a_2's and so on.

For a given $j \in \{1, \ldots, \ell\}$, the sequence $(\mathbf{v}_{q_j}(n) \mod p)_{n\in\mathbb{N}}$ is ultimately periodic, say of period π_j and preperiod τ_j. (Indeed, the sequence $(\mathbf{v}_{q_j}(n))_{n\in\mathbb{N}}$ satisfies a linear recurrence relation with constant coefficients.) Let $P = \mathrm{lcm}_j\, \pi_j$ and $T = \max_j \tau_j$. Then, for all $j \in \{1, \ldots, \ell\}$, if $i_1, \ldots, i_\ell > T$,

$$\mathrm{val}_\ell(a_1^{i_1} \cdots a_j^{i_j} \cdots a_\ell^{i_\ell}) \equiv \mathrm{val}_\ell(a_1^{i_1} \cdots a_j^{i_j+P} \cdots a_\ell^{i_\ell}) \pmod p.$$

We have just shown that for every $x \in \mathbb{N}^\ell$ such that $T < \sup_i x_i \leq T + P$, x belongs to $\Psi(\mathrm{rep}_\ell(q + \mathbb{N}\, p))$ if and only if $x + n_1\, P\mathbf{e}_1 + \cdots + n_\ell\, P\mathbf{e}_\ell$ belongs to the same set, $n_1, \ldots, n_\ell \in \mathbb{N}$. The conclusion follows easily:

$$\Psi(\mathrm{rep}_\ell(q + \mathbb{N}\, p)) = F \cup \bigcup_{\substack{\mathrm{val}_\ell(a_1^{x_1} \cdots a_\ell^{x_\ell}) \in q + \mathbb{N}\, p \\ T < \sup x_i \leq T + P}} x + \mathbb{N}\, P\mathbf{e}_1 + \cdots + \mathbb{N}\, P\mathbf{e}_\ell$$

where the finite set F is $\{x \in \mathbb{N}^\ell \mid \mathrm{val}_\ell(a_1^{x_1} \cdots a_\ell^{x_\ell}) \in q + \mathbb{N}\, p \text{ and } \sup_i x_i \leq T\}$.