International Electronic Journal of Algebra
Published Online: July 20, 2026
DOI: 10.24330/ieja.1999594

DIGITAL SEMIGROUPS OF MONIC INTEGER POLYNOMIALS

Horst Brunotte

Received: 4 October 2025; Revised: 11 March 2026; Accepted: 22 May 2026
Communicated by Burkhard Külshammer

Abstract. The well-known expansion of rational integers in an arbitrary integer base is generalized to so-called P-canonically representable integers for a suitable polynomial P with rational integer coefficients. In this surroundings certain additive and multiplicative subsemigroups of rational integers are studied.

Mathematics Subject Classification (2020): 11D85, 20M14, 20M07
Keywords: Digital representation, digital semigroup, numerical monoid, Frobenius number

1. Introduction

In 2015, J. C. Rosales, M. B. Branco and D. Torrão [17] investigated sets of positive integers and their relations to the number of decimal digits. Later these relations were generalized to arbitrary integer bases [4]. This concept is extended here to so-called P-canonical representations of integers where P is a monic integer polynomial of positive degree with non-vanishing constant term. Specifically, we say that the rational integer z is P-canonically representable if there exists a polynomial U with all coefficients in[1]

$$\mathcal{N}_P := [0,\, |P(0)| - 1] \cap \mathbb{N}_0$$

such that

$$z \equiv U \pmod{P},$$

where we here and in the following mean the congruence taken in the quotient ring $\mathbb{Z}[X]/(P)$. Thus there exist a minimal $n \in \mathbb{N}_0$ and $u_0, \ldots, u_n \in \mathcal{N}_P$ with[2]

$$z \equiv u_n X^n + \cdots + u_0 \pmod{P}. \tag{1}$$

We shortly write (see [7, Section 3])

$$z = (u_n \cdots u_0)_P$$

[1]We denote by $\mathbb{N}$ ($\mathbb{N}_0$, respectively) the set of positive (non-negative, respectively) rational integers.
[2]See [12,13].

and define the P-length of z by

$$\ell_P(z) := |z|_P := n + 1\,.$$

M. Madritsch and A. Pethő [15] showed among others that the distribution properties of patterns in the sequence of digits depend neither on the polynomial P nor on the quotient ring $\mathbb{Z}[X]/(P)$; they are intimate properties of the backward division algorithm defined in [16]. Recall that this algorithm also determines the P-length[3] of a P-canonically representable integer.

Here we study properties of certain additive subsemigroups of $\mathbb{N}_0$ consisting of P-lengths of P-canonically representable integers. Our main result includes an analogue of [4, Corollary 2.4] for a family of quadratic polynomials P. Further we show that the existence of such a particular subsemigroup of $\mathbb{N}_0$ yields strong properties on the set of P-lengths of the P-canonically representable integers.

2. Basic properties of the P-length of integers

Throughout, we let P be a monic integer polynomial of degree d, $|P(0)| > 1$, $b := -P(0)$ and Z_P the set of non-zero P-canonically representable integers[4]. There is an algorithm to decide $z \in Z_P$ for a given integer z and to compute its canonical P-representative if possible (e.g., see [5,12,16,22]). From now on we require

$$\mathbb{N} \subseteq Z_P\,.$$

Lemma 2.1. (i) *Every element of Z_P has a unique P-canonical representative, and we have*

$$\mathcal{N}_P \subseteq Z_P \cup \{0\}.$$

(ii) *Let $f \in \mathcal{N}_P[X]$ be the P-canonical representative of $z \in Z_P$. Then $z = f(\rho)$ for each root ρ of P. Further, $P(0)$ divides z if and only if $f(0) = 0$.*

(iii) *For every root ρ of P, we have*

$$|\rho| > 1 + \frac{1}{2^{\binom{d}{2}}|b|^{d-1} + 1}.$$

Moreover, there is an effectively computable constant C such that

$$|\ell_P(z) - \frac{\log|z|}{\min\{|\rho| \;:\; P(\rho) = 0\}}| \le C \qquad\qquad (z \in Z_P).$$

[3]For the definition see Section 2.

[4]Note that we have $Z_{X-b} = Z_b$ in the notation of [4, Section 2].

Proof. (i) This is well-known (e.g., see [12,13]).
(ii) Using (1) there is some $t \in \mathbb{Z}[X]$ with

$$z - f = tP$$

yielding

$$z - f(\rho) = 0$$

and the second claim.
(iii) Aiming at showing the first claim an obvious modification of [14, Lemma 3] shows that the absolute value of each conjugate of every root ρ of P is at least 1. Then a review of the respective part of the proof of [14, Theorem 3] yields

$$|\rho| > 1$$

and then [2, Lemma 3.1] yields our first claim.

The second claim is a particular case of [15, Lemma 1.1]. □

Our main interest here lies in additive subsemigroups contained in the set $\ell_P(\mathbb{N})$. If there is no fear of confusion, we often omit the subscript P.

Proposition 2.2. (i) *For $z \in Z_P \cup \{0\}$, we have*

$$\ell_P(z) = 1 \iff z \in \mathcal{N}_P\,,$$

and for $z \in Z_P \setminus \mathcal{N}_P$, there are $q \in \mathbb{Z}$ and $r \in \mathcal{N}_P$ such that

$$z = q|b| + r, \quad \operatorname{sgn}(q) = \operatorname{sgn}(z) \ \text{ and } \ \ell_P(z) = \ell_P(q|b|)\,.$$

(ii) *Let $\deg(P) > 1$. Then*

$$[2, \deg(P)] \cap \ell_P(Z_P) = \emptyset\,.$$

In particular, $\ell_P(Z_P)$ is not additively closed.

Proof. (i) The straightforward proof is left to the reader.
(ii) First, let $\ell \in [2, \deg(P)]$ and assume that there exist $z \in Z$ and $u_0, \ldots, u_{\ell-1} \in \mathcal{N}$ such that

$$z \equiv \sum_{j=0}^{\ell-1} u_j X^j \pmod{P}\,.$$

Then $u_{\ell-1} \neq 0$ and there is some $T \in \mathbb{Z}[X]$ such that

$$PT = \sum_{i=0}^{\ell-1} u_i X^i - z\,.$$

Clearly, $T \neq 0$, thus $\deg(T) \geq 0$ and therefore

$$\ell - 1 = \deg(PT) = \deg(P) + \deg(T) \geq \deg(P)\,,$$

which is excluded. Second, an application of (i) terminates the proof. □

Let us briefly glance at polynomials with a very easy relation to a polynomial of smaller degree.

Proposition 2.3. *Let $k > 1$ and $Q := P(X^k)$.*

(i) $\mathcal{N}_Q = \mathcal{N}_P$.

(ii) *If $E(X) \in \mathcal{N}_P[X]$ canonically represents $A(X) \in \mathbb{Z}[X]$ modulo P, then $E(X^k)$ canonically represents $A(X^k)$ modulo Q. In particular, we have $Z_P \subseteq Z_Q$ and for $z \in Z_P$, we have*

$$\ell_Q(z) = k(\ell_P(z) - 1) + 1\,,$$

thus

$$\ell_Q(z) \equiv 1 \pmod{k}\,.$$

Explicitly, writing $\ell := \ell_{\mathrm{Q}}$ and $z = (u_{l-1}u_{l-2}\cdots u_0)_Q$ we have

$$z = (u_{l-1}wu_{l-2}w\cdots wu_0)_P$$

with

$$w := \underbrace{0\cdots 0}_{k-1}\,.$$

Proof. (i) Clear by $Q(0) = P(0)$.
(ii) Let $T \in \mathbb{Z}[X]$ with

$$PT = \sum_{i=0}^{n} e_i X^i - A\,,$$

hence we obtain[5]

$$Q(X)T(X^k) = P(X^k)T(X^k) = (PT)(X^k) = \sum_{i=0}^{n} e_i X^{ki} - A(X^k),$$

and this implies the first statement. Clearly, for $z \neq 0$, we have

$$\ell_P(z) = n + 1 \qquad \text{and} \qquad \ell_Q(z) = kn + 1,$$

and this implies our second assertion. □

We denote by $\mathcal{C}_-$ the set of all semi-CNS polynomials with negative constant term[6]. Due to results of S. Akiyama and W. Steiner (see [21], [3, Theorem 5]) $\mathcal{C}_-$

[5]We use the compatibility of composition and multiplication $(fg) \circ h = (f \circ h)(g \circ h)$.

[6]The reader is referred to [12] for background information on these polynomials which we tacitly use in the sequel.

consists of all polynomials $P \in \mathbb{Z}[X]$ with the following three properties.

P is monic, $P(1) < 0$ and apart from the constant term all coefficients of P are non-negative.

Proposition 2.4. *Let $P \in \mathcal{C}_-$ and $d > 1$.*

(i) $Z_P = \mathbb{N}$ *and* $b = (1p_{d-1} \cdots p_1 0)_P$.
(ii) $\ell_P(x) \le \ell_P(x+1)$ $(x \in \mathbb{N}_0)$.
(iii) $\ell_P(xy) \ge \ell_P(x) + \ell_P(y) - 1$ $(x, y \in \mathbb{N})$.

Proof. (i) Since Z_P is additively closed, we have $\mathbb{N} \subseteq Z_P$, and the P-canonical representation of b is clear in view of $p_1, \ldots, p_{d-1} \in \mathcal{N}$.
(ii) Write

$$n = qb + r$$

with $q \in \mathbb{N}_0$ and $r \in \mathcal{N}$. If $r < b - 1$, we have

$$\ell(n+1) = \ell(qb + r + 1) = \ell(n)$$

by Proposition 2.2. For $r = b - 1$, an elementary inspection of the addition of the P-canonical representatives of qb and b yields

$$\ell(n+1) = \ell(qb + b) \ge \ell(n)\,.$$

(iii) We may assume $x \ge y$ and we set $\ell := \ell_P(x)$ and $m := \ell_P(y)$.

Case 1 $x < b$

Then the right hand side of our claim equals 1, and we are done.

Case 2 $x \ge b$

By (i) and (ii), we have

$$\ell > d\,.$$

Case 2.1 $m = 1$

Then we have

$$\ell_P(xy) \ge \ell > d$$

by the above. The right hand side of our claim equals

$$\ell_P(x) = \ell\,,$$

thus we are done.

Case 2.2 $m > 1$

Then we have

$$m > d$$

by the above. There exist $r, s \in \mathcal{N}_P \setminus \{0\}$ and $u, v \in \mathcal{N}_P[X]$ with the properties

$$\deg(u) < \ell - 1 \qquad \text{and} \qquad \deg(v) < m - 1$$

and

$$x \equiv rX^{\ell-1} + u \pmod{P} \qquad \text{and} \qquad y \equiv sX^{m-1} + v \pmod{P}.$$

Thus we find

$$xy \equiv rsX^{\ell+m-2} + rvX^{\ell-1} + suX^{m-1} + uv \pmod{P}.$$

Clearly, there is some $w \in \mathcal{N}_P[X]$ with

$$w \equiv rvX^{\ell-1} + suX^{m-1} + uv \pmod{P},$$

thus

$$xy \equiv rsX^{\ell+m-2} + w \pmod{P},$$

and then (ii) implies

$$\ell_P(xy) = \deg(rsX^{\ell+m-2} + w) + 1 \geq \ell + m - 2 + 1 = \ell + m - 1. \qquad \square$$

Remark 2.5. Note that the length function is not always increasing on $\mathbb{N}$. For instance, for $P = X^2 - X + 2$, we have

$$\ell_P(23) = |101100110011|_P = 12 > 11 = |10011001001|_P = \ell_P(24).$$

Let us remark in passing that by Proposition 2.2, our length function is closely related to a similar function which is used for instance in semi-ring theory (e.g. [6,9,10]).

Corollary 2.6. *For $P \in \mathcal{C}_-$, the function*

$$z \mapsto \ell_P(z) - 1 \qquad (z \in \mathbb{N}_0)$$

is a length function in the sense of [9] *on the bounded factorization monoid* $(\mathbb{N}, \cdot)$.

3. P-sequences

Now we deal with equivalence classes in the set $\mathbb{N}$ defined by the length function (see [17]), namely

$$x \sim_P y :\iff \ell_P(x) = \ell_P(y) \qquad (x, y \in Z_P).$$

Definition 3.1. The P-sequence $(q_k)_{k\in\mathbb{N}}$ is defined by $q_1 = 1$ and for $k \in \mathbb{N}$ we set[7]

$$q_{k+1} = \min\{q \in \mathbb{N} \,:\, \ell_P(q|P(0)|) > \ell_P(q_k|P(0)|)\}$$

and

$$\Delta_{P,k} = \{z \in \mathbb{N} \,:\, \ell_P(z) = \ell_P(q_k|P(0)|)\}.$$

We start with an easy, but useful observation on the growth of the P-sequence.

Lemma 3.2. (i) *The P-sequence exists and is strictly increasing, and we have*

$$\frac{q_{k+1}}{q_k} \geq 1 + \frac{1}{q_k}$$

and

$$z \in \mathbb{N},\ \ell(z) \geq \ell(q_k|b|) \implies z \geq q_k|b|\,.$$

(ii) *For $b > 1$, the $(X - b)$-sequence is given by*

$$q_k = b^{k-1} \qquad (k \in \mathbb{N}).$$

(iii) $x < q_{k+1}|b| \implies \ell(x) \leq \ell(q_k|b|) \qquad (x, k \in \mathbb{N}).$

(iv) *If ℓ is increasing on the interval*

$$I := [q_k|b|, q_{k+1}|b| - 1] \cap \mathbb{N},$$

we have

$$\ell(x) = \ell(q_k|b|) \qquad (x \in I,\ k \in \mathbb{N}).$$

(v) $\#\Delta_{P,k} \leq \max \Delta_{P,k} - q_k|b| \qquad (k \in \mathbb{N}).$

(vi) *For $P \in \mathcal{C}_-$, we have*

$$\Delta_{P,k} = [q_k b, q_{k+1}b - 1] \qquad (k \in \mathbb{N}).$$

Proof. (i) The first claims are trivial. To show the last claim we assume

$$z < q_k|b|,$$

hence by definition

$$\ell(z) = \ell(q_m|b|)$$

for some $m < k$. But then we have

$$\ell(q_k|b|) \leq \ell(z) = \ell(q_m|b|)$$

[7]This definition coincides with its analogue introduced in [17], but not with the respective definition in [4].

implying the contradiction $k \leq m$.
(iii) By definition, we have

$$\ell(x) = \ell(q_t|b|)$$

for some $t \in \mathbb{N}$ with $t < k+1$. Thus we have $t \leq k$ and then

$$\ell(x) = \ell(q_t|b|) \leq \ell(q_k|b|).$$

(ii), (iv), (v) Obvious.
(vi) By Proposition 2.4, the length function grows monotonously on the non-negative integers. □

The following description of the structure of the set of the positive P-representable integers is useful for our subsequent results. Recall that a multiplicative subsemigroup D of $\mathbb{Z}$ is called lacunary if there exists a single integer z such that every element of $D \cap \mathbb{N}$ is a power of z (see [8, Definition IV.1]). For a subset $\mathcal{K}$ of $\mathbb{N}$, we write

$$D_{P,\mathcal{K}} := \bigcup_{k \in \mathcal{K}} \Delta_{P,k}.$$

Theorem 3.3. (i) *The set $D_{P,\mathbb{N}}$ is a preprime*[8] *of $\mathbb{Z}$ with minimal element $|b|$.*
(ii) *$D_{P,\mathbb{N}}$ is a non-lacunary subsemigroup of $(\mathbb{N}, \cdot)$, and we have*

$$\lim_{k \to \infty} \frac{q_{k+1}}{q_k} = 1\,.$$

(iii) *Let $\mathcal{K}$ be a non-empty subset of $\mathbb{N}$ such that $D_{P,\mathcal{K}}$ is multiplicatively closed. Then for every $\epsilon > 0$ there exists some $K \in \mathcal{K}$ such that*

$$\frac{q_{k+1}}{q_k} < 1 + \epsilon \qquad\qquad (k \geq K).$$

Proof. For simplicity we write

$$D_{\mathcal{K}} := D_{P,\mathcal{K}}\,.$$

(i) We have

$$\min D_{\mathbb{N}} = q_1|b| = |b|\,,$$

hence in particular

$$-1 \notin D_{\mathbb{N}}\,.$$

Let $x, y \in D_{\mathbb{N}}$, thus

$$x, y \in \mathbb{N} \qquad \text{and} \qquad x + y > |b|\,.$$

[8]By a preprime S of a (not necessarily commutative) ring R we mean a non-empty subset S of R such that $S + S \subseteq S, S \cdot S \subseteq S$ and $-1 \notin S$ (see [11]).

Hence there exists $k \in \mathbb{N}$ with

$$\ell(q_k|b|) = \ell(x+y)\,,$$

and this means

$$x + y \in \Delta_k \subset D_{\mathbb{N}}\,.$$

Thus, in view of $\Delta_{P,n} \subseteq \mathbb{N}$ for all positive integers n, we also have

$$xy = \underbrace{x + \cdots + x}_{y} \in D_{\mathbb{N}}.$$

(ii) By (i), the set $D_{\mathbb{N}}$ is multiplicatively closed. Now we suppose that there is an element $c \in D_{\mathbb{N}}$ such that every element of $D_{\mathbb{N}}$ is a power of c. Clearly, we have $c > 1$. Let $k \in \mathbb{N}$. Proposition 2.2 yields

$$q_k|b|,\, q_k|b| + 1 \in D_{\mathbb{N}}\,.$$

By our assumption, there are $s, t \in \mathbb{N}$ such that

$$q_k|b| = c^s \qquad \text{and} \qquad q_k|b| + 1 = c^t\,.$$

Clearly, we have $s < t$ and the impossibility

$$1 = c^t - c^s = c^s(c^{t-s} - 1).$$

Thus $D_{\mathbb{N}}$ is non-lacunary, and the limit above is calculated by a straightforward application of [8, Lemma IV.1] analogously as in the proof of (iii) below.

(iii) We immediately convince ourselves that $D_{\mathcal{K}}$ is non-lacunary. Let $k \in \mathbb{N}$ and $J_k \in \mathbb{N}_0$ such that

$$\Delta_k = \bigcup_{j=0}^{J_k} I_{k,j}$$

with

$$I_{k,j} := [q_k|b| + i_{j-1},\, q_k|b| + i_j] \cap \mathbb{N}$$

and

$$0 = i_{-1} \le i_{j-1} < i_j \qquad\qquad (j = 0, \ldots, J_k).$$

By [8, Lemma IV.1], we know that the quotients of consecutive elements of $D_{\mathcal{K}}$ converge to 1, thus in particular

$$\lim_{k\to\infty} \frac{q_k|b| + i_{j-1} + \nu + 1}{q_k|b| + i_{j-1} + \nu} = 1 \qquad\qquad (j = 0, \ldots, J_k,\ \nu = 0, \ldots, i_j - i_{j-1} - 1)$$

and then for the intervals $I_{k,0}$

$$1 = \lim_{k\to\infty} \prod_{\nu=0}^{i_{j-1}-1} \frac{q_k|b| + i_{j-1} + \nu + 1}{q_k|b| + i_{j-1} + \nu} = \lim_{k\to\infty} \frac{\max I_{k,0}}{\min I_{k,0}}.$$

Analogously, for $J_k > 0$, we have

$$\lim_{k\to\infty} \frac{\max I_{k,j}}{\min I_{k,j}} = 1 \qquad\qquad (j = 0, \dots, J_k)\,,$$

and then by considering the products of these quotients, we see

$$\lim_{k\to\infty} \frac{\max \Delta_k}{\min \Delta_k} = 1\,,$$

because $\max I_{k,j}$ and $\min I_{k,j+1}$ are consecutive subsets of $D_{\mathcal{K}}$. Observing that $\max \Delta_k$ and $\min \Delta_{k+1}$ are consecutive elements of $D_{\mathcal{K}}$, we see

$$\lim_{k\to\infty} \frac{\min \Delta_{k+1}}{\max \Delta_k} = 1\,,$$

and this yields

$$1 = \lim_{k\to\infty} \Big(\frac{\max \Delta_k}{\min \Delta_k} \cdot \frac{\min \Delta_{k+1}}{\max \Delta_k}\Big) = \lim_{k\to\infty} \frac{\min \Delta_{k+1}}{\min \Delta_k} = \lim_{k\to\infty} \frac{q_{k+1}|b|}{q_k|b|} = \lim_{k\to\infty} \frac{q_{k+1}}{q_k}\,. \quad \square$$

4. The function g_P

We aim at describing the P-length of squares of certain integers by means of the P-sequence. By what we have seen in the previous section for a given $k \in \mathbb{N}$, there is a unique $m \in \mathbb{N}$ such that

$$\ell_P(q_m|b|) = \ell_P((q_k b)^2)\,.$$

Thus we can define the map

$$g_P : \mathbb{N} \to \mathbb{N}$$

by

$$g_P(k) := m\,.$$

First we collect some properties of the function g_P.

Lemma 4.1. *Let $k \in \mathbb{N}$ and $g := g_P$.*

(i) $\ell(q_{g(k)}|b|) = \ell((q_k b)^2)$.

(ii) $q_{g(k)} \le q_k^2|b| \le q_{g(k)+1} - 1$ *and*

$$q_{g(k)} < q_k^2|b| \implies q_{g(k)} \le q_{g(k)+1} - 2\,.$$

(iii) *We have*

$$g(k) \ge k$$

and

$$g(k) = k \implies \big((q_{k+1}|b| - 1)^2 > q_{g(k)+1}|b| \qquad \text{and} \qquad q_k \le \sqrt{(q_{k+1} - 1)/|b|}\big). \quad (2)$$

(iv) *We have*

$$g(k) \le g(k+1)$$

and

$$g(k+1) = g(k) \implies \big(q_{g(k+1)} \le q_{g(k)+1} - 2 \text{ and } q_{g(k+1)+1} - q_{g(k+1)} \ge (2q_k+1)|b| + 1\big).$$

(v) *If*

$$(q_{k+1}|b| - 1)^2 < q_{g(k)+1}|b|,$$

then we have

$$q_{g(k)+1} - q_{g(k)} \ge (|b|-1)(2q_k+1) \qquad \text{and} \qquad \frac{q_{g(k)+1}}{q_{g(k)}} > 1 + \frac{\Theta}{\sqrt{q_{g(k)}}}$$

with $\Theta = \sqrt{2}$ *for* $|b| = 2$ *and* $\Theta = 2$ *otherwise.*

(vi) *Suppose*

$$\lim_{k\to\infty} \frac{q_{k+1}}{q_k} = 1\,.$$

Then there is some $K \in \mathbb{N}$ *such that*

$$g(k) > k \qquad\qquad (k \ge K).$$

Further, there are infinitely $k \in \mathbb{N}$ *such that*

$$g(k) < g(k+1).$$

Proof. Set $m := g(k)$.

(i), (ii) Clear by the definitions (for (i) see also Lemma 3.2).

(iii) The inequality

$$k > m$$

would imply

$$q_{m+1} \le q_k < q_k^2|b|$$

thereby contradicting the definition of g.

Now let $g(k) = k$. Then (2) is clear because the assumption

$$(q_{k+1}|b| - 1)^2 \le q_{g(k)+1}|b|$$

implies

$$(q_{k+1}|b| - 1)^2 \le q_{k+1}|b|$$

and then the impossibility

$$4 \le q_{k+1}|b| \le \frac{1}{2}(3+\sqrt{5}) < 3\,.$$

Further, we have

$$q_k^2|b| \le q_{m+1} - 1$$

and then our last assertion is clear.

(iv) The assumption

$$g(k) > g(k+1)$$

yields

$$q_{k+1}^2|b| < q_{g(k+1)+1} \le q_{g(k)} \le q_k^2|b|$$

and then the impossibility

$$q_{k+1} < q_k\,.$$

Now, the assumption

$$m = g(k) = g(k+1)$$

yields

$$q_{g(k+1)} = q_{g(k)} \le q_k^2|b| < (q_k+1)^2|b| \le q_{k+1}^2|b| \le q_{g(k)+1} - 1\,,$$

thus our first inequality

$$q_m \le q_{m+1} - 2\,.$$

To prove the second inequality, we first note

$$q_{k+1}^2 - q_k^2 - 2q_k \ge (q_k+1)^2 - q_k^2 - 2q_k = 1$$

and then using (i), we verify

$$q_{g(k+1)+1} - q_{g(k+1)} \ge q_{k+1}^2|b| + 1 - q_{g(k)} \ge q_{k+1}^2|b| - q_k^2|b| + 1\,,$$

thus

$$q_{g(k+1)+1} - q_{g(k+1)} \ge (q_{k+1}^2 - q_k^2)|b| + 1 \ge (2q_k+1)|b| + 1\,.$$

(v) We verify

$$\begin{aligned} q_{g(k)+1}|b| &\ge ((q_k+1)|b|-1)^2 + 1 = (q_k b)^2 + 2q_k|b|(|b|-1) + (|b|-1)^2 + 1 \\ &\ge q_{g(k)}|b| + 2(|b|-1)q_k|b| + b^2 - 2|b| + 2\,, \end{aligned}$$

hence

$$(q_{g(k)+1} - q_{g(k)})|b| \ge 2(|b|-1)q_k|b| + |b|(|b|-2) + 2$$

and then

$$q_{g(k)+1} - q_{g(k)} > 2(|b|-1)q_k + |b| - 2$$

yielding

$$q_{g(k)+1} - q_{g(k)} \ge 2(|b|-1)q_k + |b| - 1 = (|b|-1)(2q_k+1).$$

Further, we can write

$$q_{g(k)+1}|b| \quad > q_{g(k)}|b| + 2(|b|-1)\sqrt{q_{g(k)}|b|} + (|b|-1)^2\,,$$

hence

$$\frac{q_{g(k)+1}}{q_{g(k)}} > 1 + \frac{2(|b|-1)\sqrt{q_{g(k)}|b|}}{q_{g(k)}|b|} = 1 + \frac{2(|b|-1)}{\sqrt{|b|}} \cdot \frac{1}{\sqrt{q_{g(k)}}} \geq 1 + \frac{\Theta}{\sqrt{q_{g(k)}}}\,.$$

(vi) Pick $\epsilon \in (0,1]$. Then there is some $K \in \mathbb{N}$ such that

$$\frac{q_{k+1}}{q_k} < 1 + \epsilon \qquad\qquad (k \geq K)\,.$$

Consider $k \geq K$. The assumption $g(k) = k$ implies

$$q_k^2|b| \leq q_{g(k)+1} - 1 = q_{k+1} - 1 < (1+\epsilon)q_k - 1 \leq 2q_k - 1$$

and then the absurdity

$$0 \leq q_k(q_k|b| - 2) < 0\,.$$

Thus we have shown

$$g(k) > k \qquad\qquad (k \geq K)\,.$$

Now we show that for all $K \in \mathbb{N}$, there exists some $k \geq K$ such that

$$g(k+1) > g(k)\,.$$

Assume to the contrary that there exists $K \in \mathbb{N}$ such that

$$g(k+1) \leq g(k) \qquad\qquad (k \geq K),$$

hence by (v),

$$g(k) = g(K) \qquad\qquad (k \geq K).$$

Thus there exists $L \in \mathbb{N}$ with

$$\ell((q_k b)^2) \leq L \qquad\qquad (k \in \mathbb{N})$$

which is impossible. □

The following observation will play a decisive role later.

Lemma 4.2. *Let $\mathcal{K}$ be an infinite subset of $\mathbb{N}$ with the following properties.*

(i) $q_k \geq 2|b| + 1 \qquad (k \in \mathcal{K})$.
(ii) $g_P(\mathcal{K}) \subseteq \mathcal{K}$.
(iii) $\lim_{k\to\infty, k\in\mathcal{K}}(q_{k+1}/q_k) = 1$.

Then there exists $k \in \mathcal{K}$ such that

$$(q_{k+1}|b| - 1)^2 > q_{g_P(k)+1}|b|\,. \tag{3}$$

Proof. By our prerequisites there is some minimal $K \in \mathcal{K}$ with the property

$$|b|q_{k+1} < (|b|+1)q_k \qquad (k \in \mathcal{K},\, k \geq K). \tag{4}$$

The assumption

$$K \leq m := \min(\mathcal{K})$$

implies $K = m$, which contradicts our prerequisites. Thus we have $K > m$, and we set

$$k := \max([m, K-1] \cap \mathcal{K})\,.$$

In view of

$$|b|q_{k+1} \geq (|b|+1)q_k,$$

we have

$$(q_{k+1}|b|-1)^2 \geq \big(q_k|b|+q_k-1\big)^2 > (q_kb)^2 + \big(2|b|+1\big)q_k^2 - 2\big(|b|+1\big)q_k\,. \tag{5}$$

If $g(k) = k$, then our claim is clear by Lemma 4.1, thus from now on we suppose $g(k) > k$. In view of $g(k) \in \mathcal{K}$ and our choice of k, we have

$$g(k) \geq K\,,$$

and then by (4),

$$q_{g(k)+1}|b| < \big(|b|+1\big)q_{g(k)}\,. \tag{6}$$

Now we assume

$$(q_{k+1}|b|-1)^2 \leq q_{g(k)+1}|b|\,. \tag{7}$$

Then (6), (7), (5) and the definition of g yield

$$\big(|b|+1\big)q_{g(k)} > q_{g(k)+1}|b| \geq (q_{k+1}|b|-1)^2 > q_{g(k)}|b| + \big(2|b|+1\big)q_k^2 - 2\big(|b|+1\big)q_k\,,$$

thus

$$q_{g(k)} > (2|b|+1)q_k^2 - 2(|b|+1)q_k \geq 2q_{g(k)} + q_k^2 - 2(|b|+1)q_k\,,$$

and then the absurdity

$$\begin{aligned} 0 \;&>\; q_{g(k)} + q_k^2 - 2(|b|+1)q_k \geq (q_k+1) + q_k^2 - 2(|b|+1)q_k \\ &>\; q_k\big(q_k + 1 - 2(|b|+1)\big) \geq q_m\big(q_m - (2|b|+1)\big) \geq 0\,. \end{aligned}$$

□

5. Certain subsemigroups of Z_P and $\ell_P(Z_P)$

We now extend the fundamental notions introduced in [17].

Definition 5.1. (i) A P-digital semigroup D is a subsemigroup of $(Z_P, \cdot)$ such that

$$\{z \in Z_P \ : \ \ell_P(z) = \ell_P(x)\} \subseteq D$$

for all $x \in D$.

(ii) Let S be a submonoid of $(\mathbb{N}_0, +)$. We call S a P-LD-semigroup if there exists a P-digital semigroup D such that

$$S = \ell_P(D) \cup \{0\}. \tag{8}$$

Lemma 5.2. *Let S be a P-LD-semigroup and D a P-digital semigroup satisfying* (8).

(i) *D is non-lacunary, and there exists an infinite set of positive integers $\mathcal{K}$ such that*

$$D \cap \mathbb{N} = D_{P,\mathcal{K}}\,. \tag{9}$$

Moreover, we have

$$\lim_{k\to\infty, k\in\mathcal{K}} \frac{q_{k+1}}{q_k} = 1\,.$$

(ii) $g_P(\mathcal{K}) \subseteq \mathcal{K}$.

(iii) *Assume that there exists $k \in \mathcal{K}$ with the properties*

(a) $(q_{k+1}|b| - 1)^2 \geq q_{g_P(k)+1}|b|$

(b) $q_{g_P(k)}|b| \leq x \leq q_{g_P(k)+1}|b| \implies \ell_P(x) \leq \ell_P(x+1) \leq \ell_P(x) + 1\,.$

Then S is a numerical monoid.

(iv) *If $\deg(P) > 1$, we have*

$$D \subseteq \mathbb{Z} \setminus (\mathcal{N}_P \cup \{-1\}).$$

Proof. (i) The existence of $\mathcal{K}$ with (9) is clear by the definitions; obviously $\mathcal{K}$ cannot not be finite. Now, take an element $s \geq |b|$ in S and write

$$s = \ell_P(q_k|b|)$$

with some $k \in \mathcal{K}$. In view of

$$\ell_P(q_k|b|) = \ell_P(q_k|b| + 1) \in S$$

and the fact that D is a P-digital semigroup, we know

$$q_k|b|,\ q_k|b| + 1 \in D \cap \mathbb{N}\,,$$

thus D cannot be lacunary. The second part of our claim is clear by Theorem 3.3.
(ii) Clear by the definition of g and the properties of D.
(iii) In view of (ii) it suffices to show that there exist $x, y \in \Delta_k$ such that

$$\ell(q_{g(k)}|b|) + 1 = \ell(xy) \in S\,.$$

By our prerequisites, there exists a minimal $x \in \Delta_k$ such that there is some $y \in \Delta_k$ with the properties

$$x \le y \qquad \text{and} \qquad \ell(xy) \ge \ell(q_{g(k)+1}|b|)\,. \tag{10}$$

(Observe that the integers $x := y := q_{k+1}|b| - 1 \in \Delta_k$ have these properties.) Further we may assume that y is minimal with this property. We convince ourselves that

$$\ell(x^2) \ge \ell(q_{g(k)}|b|)\,, \quad xy \in D \quad \text{and} \quad \ell(xy) > \ell(q_{g(k)}|b|)\,.$$

Now we distinguish two cases. First, we assume $x = q_k|b|$. Then $y > x$ and

$$y - 1 \in \Delta_k\,.$$

For

$$z := x(y-1) \in \Delta_{g(k)},$$

we have

$$\ell(q_{g(k)}|b|) \le \ell(z) \le \ell(q_{g(k)}|b|)\,,$$

thus in view of (10)

$$\ell(z) = \ell(q_{g(k)}|b|) \in S \qquad \text{and} \qquad [z, xy] \cap \mathbb{N} \subseteq \Delta_{g(k)} \subseteq D\,. \tag{11}$$

Now, there exists a minimal $e \in \mathbb{N}$ with

$$\ell(z+e) > \ell(q_{g(k)}|b|).$$

Exploiting our prerequisites, we verify

$$\ell(z+e-1) = \ell(q_{g(k)}|b|) \qquad \text{and} \qquad \ell(z+e) = \ell(q_{g(k)}|b|) + 1 \le \ell(xy)\,,$$

thus

$$\ell(z+e) \in S\,.$$

We conclude

$$\ell(q_{g(k)}|b|) \in S \qquad \text{and} \qquad \ell(q_{g(k)}|b|) + 1 \in S\,.$$

Second, we assume $x > q_k|b|$. Then

$$x - 1 \in \Delta_k \qquad \text{and} \qquad \ell((x-1)y) = \ell(q_{g(k)}|b|)\,,$$

and for

$$z := (x-1)y \in \Delta_{g(k)},$$

(11) holds, and we conclude the proof analogously as above.
(iv) Clear by Proposition 2.2. □

Let us look at some basic properties of P-LD-semigroups.

Proposition 5.3. (i) *Let S be a P-LD-semigroup. Then there does not exist a $p \in \mathbb{Z}[X]$ and $n > 1$ with $P = p(X^n)$. Moreover, given an integer $m > 1$, we have*

$$\#\{\overline{\ell_P(z)} \,:\, z \in Z_P\} = m\,,$$

where $\overline{x}$ denotes the residue class of $x \in \mathbb{Z}$ modulo m.

(ii) *Let S, T be P-LD-semigroups. Then $S \cap T$ is a P-LD-semigroup. Moreover, if both S and T are numerical semigroups[9], then so is $S \cap T$.*

(iii) *Assume that there is some $N \in \mathbb{N}$ such that*

$$\ell_P(n) \le \ell_P(n+1) \le \ell_P(n) + 1 \qquad (n \ge N).$$

Then every P-LD-semigroup is a numerical monoid.

Proof. (i) First, we assume to the contrary that $P = Q(X^k)$ with $k > 1$, and pick an element x in a P-digital semigroup D with $S = \ell_P(D) \cup \{0\}$. Then $\ell := \ell_P(x) \in S$ and $2\ell \in S$, and then Propositions 2.2 and 2.3 imply

$$\ell > 1, \quad \ell \equiv 1 \pmod{k} \quad \text{and} \quad 2\ell \equiv 1 \pmod{k}\,.$$

Thus there exist $s, t \in \mathbb{N}$ such that

$$\ell - 1 = ks \qquad \text{and} \qquad 2\ell - 1 = kt$$

yielding

$$kt = 2(ks+1) - 1 = 2ks + 1\,,$$

thus the impossibility $k \mid 1$.

Second, we suppose that there is an integer $m > 1$ with

$$\#\{\overline{\ell(z)} \,:\, z \in Z\} < m\,. \tag{12}$$

Let us consider

$$\mathcal{F} := \{T \,:\, T \text{ subsemigroup of } S\},$$

which clearly is an infinite family of subsemigroups of $\mathbb{N}_0$ because for every $i \in \mathbb{N}$ the set

$$\{0, s_i, s_{i+1}, \ldots\}$$

[9]For details the reader is referred to [19].

belongs to $\mathcal{F}$, where we put

$$S := \{0, s_1, s_2, \ldots\} \text{ with } 0 < s_1 < s_2 < \ldots .$$

By [1, Lemma 5], there exists some $T \in \mathcal{F}$ such that there are infinitely many $n \in \mathbb{N}$ with

$$n + \{0, \ldots, m-1\} \subseteq T \setminus \{0\}.$$

However, in view of

$$T \setminus \{0\} \subseteq S \setminus \{0\} \subseteq \ell(Z)$$

and (12), there must be $i, j \in \{0, \ldots, m-1\}$ with $i \neq j$ such that

$$n + i \equiv n + j \pmod{m},$$

which is impossible.
(ii) This can immediately be verified.
(iii) Let S be a P-LD-semigroup, D a P-digital semigroup satisfying (8), $\mathcal{K}$ an infinite set of positive integers such that (9) holds, and set

$$\mathcal{K}_0 := \{k \in \mathcal{K} \,:\, q_k \geq \max\{2|b|+1,\, N/|b|\}.$$

Note that we have

$$g(\mathcal{K}_0) \subseteq \mathcal{K}_0$$

by Lemma 5.2. By this lemma, there exists a minimal $K \in \mathcal{K}_0$ such that

$$|b|q_{k+1} < (|b|+1)q_k \qquad (k \in \mathcal{K}_0,\, k \geq K)$$

holds. Now Lemma 4.2 yields some $k \in \mathcal{K}_0$ such that (3) holds, and then Lemma 5.2 completes our proof. □

Now we present a polynomial P which does not admit a P-LD-semigroup.

Lemma 5.4. *For the polynomial $P = X^2 + 2X + 2$, we have $Z_P = \mathbb{Z} \setminus \{0\}$, but there does not exist a P-LD-semigroup.*

Proof. The first claim is well-known (e.g., see [12]), and [5] shows

$$\ell(\mathbb{Z}) = \{a(n) \,:\, n \in \mathbb{N}\} \qquad \text{and} \qquad \ell(z) \equiv 0, 1 \pmod{4} \qquad (z \in \mathbb{Z}),$$

where the sequence $a(n)_{n\in\mathbb{N}_0}$ is given by[10]

$$a(0) = 0 \qquad \text{and} \qquad a(n) = a(n-1) + (-1)^n + 2 \qquad (n \in \mathbb{N}).$$

Thus our claim is immediate by Proposition 5.3. □

[10] see [20, A042948]

6. A remark on varieties

If P is linear, then the set of P-LD-semigroups is a Frobenius variety [4, Section 2]. However, this is no longer true for higher degree polynomials P as we illustrate in Theorem 6.1 below. Recall that an $\mathcal{R}$-variety (see [18]) is a non-empty family $\mathcal{V}$ of numerical semigroups[11] with the following properties.

(i) $\mathcal{V}$ has a maximal element with respect to the inclusion order (denoted by $\Delta(\mathcal{V})$).
(ii) $S, T \in \mathcal{V}$ implies $S \cap T \in \mathcal{V}$.
(iii) $S \in \mathcal{V},\ S \neq \Delta(\mathcal{V})$ imply $S \cup \{F_{\Delta(\mathcal{V})}(S)\} \in \mathcal{V}$.

Let us present an easy example of polynomials P whose families of P-LD semigroups form $\mathcal{R}$-varieties. We conjecture that an analogue of Theorem 6.1 holds for all quadratic semi-CNS polynomials with negative constant terms.

Theorem 6.1. *Let $P = X^2 + (b-2)X - b \in \mathbb{N}[X]$ with $b > 2$. The set $\mathcal{G}_P$ of all P-LD semigroups is an $\mathcal{R}$-variety, but not a Frobenius pseudo-variety.*

Proof. By Lemma 6.2 below and Proposition 5.3, all elements of $\mathcal{G}_P$ are numerical monoids and

$$\ell_P(\mathbb{N}_0) = \begin{cases} \{1,3,5,7,9,\to\} & (b=3), \\ \{1,3,5,7,\to\} & (b=4,5), \\ \{1,3,5,\to\} & (b \geq 6). \end{cases}$$

Proposition 5.3 tells us that for $S, T \in \mathcal{G}_P$, we have $S \cap T \in \mathcal{G}_P$. We easily convince ourselves that the maximal elements of $\mathcal{G}_P$ are given by

$$M_P := \Delta(\mathcal{G}_P) = \begin{cases} \{0,5,7,9,\to\} & (b=3), \\ \{0,5,7,\to\} & (b=4,5), \\ \{0,5,\to\} & (b \geq 6). \end{cases}$$

Further, the Frobenius numbers of M_P are given by

$$F(M_P) = \begin{cases} 8 & (b=3), \\ 6 & (b=4,5), \\ 4 & (b \geq 6), \end{cases}$$

but $M_P \cup \{F(M_P)\}$ is not a P-LD semigroup since $F(M_P) \notin \ell_P(\mathbb{N})$ by what we have seen above. Therefore, $\mathcal{G}_P$ is not a Frobenius pseudo-variety, and by the above $\mathcal{G}_P$ is an $\mathcal{R}$-variety. □

[11] For numerical semigroups S, T with $S \subsetneq T$ we adapt the notation $F_T(S) := \max(T \setminus S)$ for the Frobenius number of S restricted to T.

The following elementary observations have been exploited in Theorem 6.1.

Lemma 6.2. *Let $P = X^2 + (b-2)X - b$ with $b \geq 3$.*

(i) $b = 1(b-2)0$.

(ii) *In case $b = 3$, we have*

$$9b = 120101000\,,$$

$$21b = 12021021100$$

and for $n \geq 21$, we have[12]

$$nb = 1202w0 \qquad (w \in \mathcal{N}_P^\star)$$

with $\ell_P(nb) \geq 11$.

(iii) *Let $b \geq 4$. Then we have*

$$4b = \begin{cases} 1302000 & (b = 4) \\ 1403020 & (b = 5) \\ 1503240 & (b = 6) \\ 1604260 & (b = 7) \\ 1(b-1)0(b-1)(b-4)0(b-8)0 & (b \geq 8). \end{cases}$$

(iv) *Let $N = 21$ $(b = 3)$, resp. $N = 4$ $(b \geq 4)$. For $n \geq N$, we have*

$$nb = 1(b-1)0vw0 \qquad (2 \leq v \leq b-1,\ w \in \mathcal{N}_P^\star).$$

(v) $\ell_P(n+1) \leq \ell_P(n) + 1 \qquad \big(n \in \mathbb{N}, n \geq 27\ (b = 3),\ \text{resp. } n \geq 4b\ (b \geq 4)\big)$.

Proof. (i) See Proposition 2.4.

(ii) We compute the P-canonical representative of

$$jb + b \qquad (j = 1, \ldots, 6)$$

and then we proceed by induction.

(iii) This can easily be checked.

(iv)-(v) The proof is a tedious, but elementary computation whose details we leave to the reader. Here we only give hints for the case $b \geq 4$. For $q \in \mathbb{N}$ with $q \geq 4$, we have

$$\ell := \ell_P(qb) \geq 8$$

by Proposition 2.4 and there exists $h \in \mathcal{N}[X]$ with $\deg(h) = \ell - 4$ such that

$$qb \equiv X^{\ell-1} + (b-1)X^{\ell-2} + h \pmod{P}\,.$$

[12]For an alphabet A we denote by $A^\star = \bigcup_{n\in\mathbb{N}} A^n$ the set of finite words over A.

Choose $m \in \mathbb{N}$ minimal with

$$\ell_P(qb + mb) > \ell\,. \tag{13}$$

Thus for the representative $g \in \mathcal{N}[X]$ modulo P of $h + mb$, we convince ourselves that we have

$$\ell - 4 < \deg(g) \leq \ell - 2\,.$$

Since the assumption

$$\deg(g) = \ell - 3$$

contradicts (13), we must have

$$\deg(g) = \ell - 2\,,$$

and we verify

$$g = X^{\ell-2} + r \qquad\qquad (r \in \mathcal{N}[X],\ \deg(r) < \ell - 2)$$

yielding

$$\begin{aligned}(q+m)b &\equiv X^{\ell-1} + bX^{\ell-2} + r \pmod{P}\\ &\equiv X^{\ell-1} + (X^2 + (b-2)X)X^{\ell-2} + r \pmod{P}\\ &\equiv X^{\ell} + (b-1)X^{\ell-1} + r \pmod{P}\,,\end{aligned}$$

thus

$$\ell(qb + mb) = \ell + 1\,.$$

□

Acknowledgement. The author is heavily indebted to the referee for insightful comments on the first version of the manuscript.

Disclosure statement. The author reports that there are no competing interests to declare.

References

[1] P.-Y. Bienvenue, *Metric decomposability theorems on sets of integers*, Bull. Lond. Math. Soc., 55(6) (2023), 2653-2659.

[2] D. Bóka, P. Burcsi and M. J. Uray, *On the algorithmic complexity of some numeration-related problems*, Publ. Math. Debrecen, 98(1-2) (2021), 65-81.

[3] H. Brunotte, *Characterization of semi-CNS polynomials*, Acta Math. Acad. Paedagog. Nyházi. (N.S.), 28 (2012), 91-94.

[4] H. Brunotte, *Digital semigroups*, RAIRO Theor. Inform. Appl., 50(1) (2016), 67-79.

[5] H. Brunotte, *A remark on Penney's algorithm*, Publ. Math. Debrecen, 107(1-2) (2025), 237-254.

[6] S. T. Chapman, F. Gotti and M. Gotti, *Factorization invariants of Puiseux monoids generated by geometric sequences*, Comm. Algebra, 48 (2020), 380-396.

[7] C. Frougny and A. C. Lai, *Negative bases and automata*, Discrete Math. Theor. Comput. Sci., 13(1) (2011), 75-93.

[8] H. Furstenberg, *Disjointness in ergodic theory, minimal sets, and a problem in Diophantine approximation*, Math. Systems Theory, 1 (1967), 1-49.

[9] F. Gotti and H. Polo, *On the arithmetic of polynomial semidomains*, Forum Math., 35(5) (2023), 1179-1197.

[10] F. Halter-Koch, *Finiteness theorems for factorizations*, Semigroup Forum, 44(1) (1992), 112-117.

[11] D. K. Harrison, Finite and Infinite Primes for Rings and Fields, Mem. Amer. Math. Soc., 68, 1966.

[12] P. Kirschenhofer and J. M. Thuswaldner, *Shift radix systems—a survey*, Numeration and substitution 2012, RIMS Kôkyûroku Bessatsu, B46, Res. Inst. Math. Sci. (RIMS), Kyoto (2014), 1-59.

[13] B. Kovács, *Canonical number systems in algebraic number fields*, Acta Math. Acad. Sci. Hungar., 37(4) (1981), 405-407.

[14] B. Kovács and A. Pethő, *Number systems in integral domains, especially in orders of algebraic number fields*, Acta Sci. Math. (Szeged), 55(3-4) (1991), 287-299.

[15] M. G. Madritsch and A. Pethő, *Asymptotic normality of additive functions on polynomial sequences in canonical number systems*, J. Number Theory, 131(9) (2011), 1553-1574.

[16] A. Pethő, *On a polynomial transformation and its application to the construction of a public key cryptosystem*, Computational number theory (Debrecen, 1989), de Gruyter, Berlin (1991), 31-43.

[17] J. C. Rosales, M. B. Branco and D. Torrão, *Sets of positive integers closed under product and the number of decimal digits*, J. Number Theory, 147 (2015), 1-13.

[18] J. C. Rosales, M. B. Branco and M. A. Traesel, *Frobenius R-variety of the numerical semigroups contained in a given one*, Mediterr. J. Math., 19(3) (2022), 103 (13 pp).

[19] J. C. Rosales and P. A. García-Sánchez, Numerical Semigroups, Developments in Mathematics, 20, Springer, New York, NY, 2009.

[20] N. J. A. Sloane, *The on-line encyclopedia of integer sequences*, Notices Amer. Math. Soc., 65(9) (2018), 1062-1074.

[21] W. Steiner, Zbl 1191.11004, Zentralbl. Math., 2008.

[22] C. van de Woestijne, Deterministic Equation Solving over Finite Fields, Ph.D. thesis (Leiden), 2006.

Horst Brunotte
Haus-Endt-Straße 88
D-40593 Düsseldorf, Germany
e-mail: brunoth@web.de