Acta Mathematica Academiae Paedagogicae Nyíregyháziensis
30 (2014), 1–15
www.emis.de/journals
ISSN 1786-0091

ON CANONICAL REPRESENTATIVES OF SMALL INTEGERS

HORST BRUNOTTE

Abstract. Some elementary facts on canonical representations of small rational integers are listed and a reformulation of a characterization of a certain class of CNS polynomials is presented. Furthermore, several examples in support of a conjecture of S. Akiyama on the canonical representative of -1 are provided.

1. Introduction

Let $P \in \mathbb{Z}[X]$ be a monic integer polynomial of positive degree d with nonvanishing constant term and

$$D_P = [0, |P(0)| - 1] \cap \mathbb{N}$$

where $\mathbb{N}$ denotes the set of nonnegative rational integers. We say that the polynomial $A \in \mathbb{Z}[X]$ is canonically representable w.r.t. P if there exists some polynomial $B \in D_P[X]$ such that

$$A \equiv B \pmod{P}.$$

In this case we say that B canonically represents A. If all integer polynomials are canonically representable w.r.t. P the pair (P, D_P) is called a canonical numeration system. This notion can be seen as a natural generalization of the classical decimal representation of the rational integers to algebraic integers. It has been introduced by the Hungarian school some decades ago (I. Kátai – J. Szabó [20], I. Kátai – B. Kovács [18], B. Kovács [23], A. Pethő [26]); a first example was studied by D. E. Knuth [21]. For a broader framework of this concept the reader is referred to [8, 7], and for a related notion in Galois rings see [25] where digit systems of prime cardinality are investigated.

In this short note we list some elementary facts on canonical representations of small rational integers and reformulate a characterization of certain CNS polynomials (see Definition 3.1 below) given by W. J. Gilbert [15]. Finally, we

2010 *Mathematics Subject Classification.* 11A63, 12D99, 03D45.
Key words and phrases. canonical numeration system, radix representation.

give several examples to support a conjecture of S. Akiyama on the canonical representative of -1 w.r.t. a CNS polynomial.

2. Canonically representable integer polynomials

Unless mentioned otherwise we always let $P = \sum_{i=0}^{d} p_i X^i \in \mathbb{Z}[X]$ be a monic integer polynomial of positive degree d with $p_0 \neq 0$ and $D = D_P$. We denote by R_P the set of all canonically representable integer polynomials[1]; trivially, $D[X] \subseteq R_P$. It is easy to see that each $A \in R_P$ which is not a multiple of P has a unique representative $B \in D[X]$; in this case we call

$$\mathrm{L}(A) := \mathrm{L}_P(A) := \deg(B)$$

the length of the canonical representation of A (see [24]). It is known that the canonical representative is effectively computable if it exists; the reader is referred to [16, 22, 11] for more details.

In this section we collect some examples and elementary facts on canonical representatives of integer polynomials.

Example 2.1. If $p_1, \dots, p_{d-1} \in D$ then $P - p_0$ canonically represents $-p_0$ because we have

$$(P - p_0) - (-p_0) = P.$$

We denote by $\mathrm{lc}\,(f)$ the leading coefficient and by Ω_f the set of roots of the univariate polynomial f.

Proposition 2.2. *Let $A \in R_P \setminus D[X]$ such that $\deg(A) < d$.*

(i) *We have $\mathrm{L}(A) \geq d$. Moreover, $\mathrm{L}(A) = d$ if and only if $A = B - \mathrm{lc}\,(B) \cdot P$ where $B \in D[X]$ is the canonical representative of A.*

(ii) *Assume that P is expanding, i.e., all roots of P lie outside the closed unit disk. If $\Omega_P \setminus \Omega_A \neq \emptyset$ then we have*

$$\mathrm{L}(A) > \max\left\{ \frac{\log|A(\alpha)| + \log(|\alpha| - 1) - \log(|p_0| - 1)}{\log|\alpha|} : \alpha \in \Omega_P \setminus \Omega_A \right\} - 1.$$

Proof. (i) Let $B \in D[X]$ and $T \in \mathbb{Z}[X]$ with

$$PT = A - B. \tag{1}$$

Clearly, P does not divide A, hence $B, T \neq 0$ and thus

$$\begin{aligned} d \leq \deg(PT) &= \deg(A - B) \leq \max\{\deg(A), \deg(B)\} \\ &= \max\{\deg(A), \mathrm{L}(A)\} = \mathrm{L}(A). \end{aligned}$$

Let $\mathrm{L}(A) = d$. Then $T \in \mathbb{Z}$, and comparing coefficients yields $T = -\mathrm{lc}\,(B)$ and then

$$A = B - \mathrm{lc}\,(B) \cdot P. \tag{2}$$

[1] W. J. Gilbert [15] coined the notion P-cleared for slightly more specialized polynomials P.

Conversely, equation (2) implies $B \neq 0$, (1) gives $PT = -\mathrm{lc}\,(B) \cdot P$ and therefore $T = -\mathrm{lc}\,(B) \in \mathbb{Z}$ and then $\deg(B) = d$.

(ii) See [11, Proposition 11]. □

Corollary 2.3. *Let $p_0 > 0$ and $m \in R_P \cap \mathbb{Z}$. Then we have $\mathrm{L}(m) > d$ if one of the following conditions is satisfied:*

(i) $m \geq p_0$,
(ii) $-p_0 \leq m < 0$ *and* $p_i \notin D$ *for some* $i \in \{1, \dots, d-1\}$.

Proof. Assume that the degree of the canonical representative B of m equals d. Then Proposition 2.2 yields

$$B = bP + m \tag{3}$$

with $b := \mathrm{lc}\,(B) > 0$. The inequality

$$bp_0 + m = B(0) < p_0$$

leads to

$$m < p_0(1-b) \leq 0 \tag{4}$$

and this settles (i).

(ii) By (4) we have $b = 1$ and then (3) shows $p_i \in D$ for all $i = 1, \dots, d-1$. □

Remark 2.4. The lower bound given by Corollary 2.3 may be rather weak as the following example shows. The canonical representative of 8 w.r.t. $(X+2)^3$ is the polynomial

$$4X + 2X^2 + 3X^3 + 6X^4 + 6X^5 + X^7 + 7X^8 + 5X^9 + X^{10},$$

thus $\mathrm{L}(8) = 10$, whereas we only find $\mathrm{L}(8) \geq 4$ by Corollary 2.3. However, in general this bound cannot be strengthened as Example 2.6 (ii) below shows.

Lemma 2.5. *Let $E \in D[X]$ canonically represent $m \in \mathbb{Z} \backslash D$. Then $L(m) \geq d$, and for every $k \in \mathbb{Z}$ such that $P(k) \neq 0$ we have*

$$E(k) \equiv m \pmod{P(k)}.$$

In particular, we have

$$E(0) \equiv m \pmod{P(0)}.$$

Proof. The lower bound for the length of m is clear by Proposition 2.2. Let $T \in \mathbb{Z}[X]$ with $PT = E - m$. Then $P(k)T(k) = E(k) - m$. □

Example 2.6. In this example we write x for the image of X under the canonical epimorphism $\mathbb{Z}[X] \to \mathbb{Z}[X]/P$. Here we always assume $p_0 > 0$.

(i) For $P = X + p_0$ we find the following canonical representations:

$$p_0 = x^2 + (p_0 - 1)x, \quad -p_0 = x.$$

(ii) To find the canonical representative of a polynomial A it is often convenient to construct a polynomial M such that

$$A + MP \in D[X].$$

We illustrate some simple cases with a quadratic polynomial P.

– For $1 \leq p_1 \leq p_0$ we observe

$$(X-1)\cdot P = X^3 + (p_1 - 1)X^2 + (p_0 - p_1)X - p_0$$

which yields the canonical representation

$$p_0 = x(x^2 + (p_1 - 1)x + (p_0 - p_1)).$$

– For $p_1 = 0$ we consider

$$(X^2 - 1)\cdot P = X^4 + (p_0 - 1)X^2 - p_0$$

and find

$$p_0 = x^2(x^2 + (p_0 - 1)).$$

– For $p_1 = -1$ we exploit

$$(X^3 + X^2 - 1)\cdot P = X^5 + (p_0 - 1)X^3 + (p_0 - 1)X^2 + X - p_0$$

and receive (cf. [11, Remark 10])

$$p_0 = x(x^4 + (p_0 - 1)x^2 + (p_0 - 1)x + 1).$$

A particular instance of the following lemma is needed below.

Lemma 2.7. *Let $k \in \mathbb{N}_{>0}$. If $m \in \mathbb{Z}$ is canonically represented by the polynomial $\sum_{i=0}^{\ell} e_i X^i$ w.r.t. P, then $\sum_{i=0}^{\ell} e_i X^{ki}$ canonically represents m w.r.t. the polynomial $P(X^k)$.*

Proof. Set $F(X) := P(X^k)$ and note that $F(0) = P(0)$, hence $D_F = D_P$. Let $T \in \mathbb{Z}[X]$ with $PT = \sum_{i=0}^{\ell} e_i X^i - m$, hence

$$F(X)T(X^k) = P(X^k)T(X^k) = \sum_{i=0}^{\ell} e_i X^{ki} - m,$$

which implies the assertion. □

3. Canonical representation of $P(0)$

Now we turn our attention to certain expanding integer polynomials which have found some interest in the past few decades (see [7, 10], for instance). To keep this note self-contained we recall the necessary definitions in a form which is slightly adapted to our purposes here (cf. [11]).

Definition 3.1. (i) [26] P is called a CNS polynomial[2] if $\mathbb{Z}[X] \subseteq R_P$.
(ii) [13] P is called a semi-CNS polynomial if R_P is an additive semigroup.

[2]CNS polynomials are named complete base polynomials in [14].

For the sake of completeness we reformulate a well-known relation between these two concepts.

Proposition 3.2. *The polynomial P is a CNS polynomial if and only if it satisfies the following three conditions:*

(i) $P(0) > 1$,
(ii) $-1 \in R_P$,
(iii) R_P *is additively closed.*

Proof. This is clear by [10, Lemma 3]. □

Corollary 3.3. *Let $|P(0)| \geq 2$. Then P is a CNS polynomial if and only if R_P is a group.*

Proof. Since $1 \in D \subset R_P$ we have $-1 \in R_P$ if R_P is a group. Thus the assertion is clear by Proposition 3.2. □

The characterization of the class of CNS polynomials has still remained an open problem, however, there is an algorithm for the decision of the CNS property of a given polynomial (see [12, 27]). Many attempts to describe CNS polynomials aim at providing a list of properties of the coefficients (e.g., see [15, 6]). Clearly, if it exists the coefficient description is by far the most transparent and easily applicable way to check whether or not a given polynomial is a CNS polynomial. Here we restrict our attention to canonical representability of certain integers, namely p_0 and $-p_0$. While the canonical representative of p_0 and $-p_0$ do not seem to be related, the respective canonical representatives of $-p_0$ and -1 are intimately connected.

Lemma 3.4. *Let $E \in D[X]$. Then E canonically represents $-p_0$ if and only if $E + p_0 - 1$ canonically represents -1.*

Proof. If $E \in D[X]$ canonically represents $-p_0$ then we have $E(0) = 0$ by Lemma 2.5. Therefore, we have

$$-1 = -p_0 + (p_0 - 1) \equiv E + p_0 - 1 \pmod{P},$$

i.e., $E + p_0 - 1$ canonically represents -1.

Similarly, if $E + p_0 - 1$ canonically represents -1 then we have $E(0) = p_0 - 1$ and thus

$$-p_0 = -1 - (p_0 - 1) \equiv E \pmod{P},$$

i.e., E canonically represents $-p_0$. □

This easy observation allows us to reformulate a well-known sufficient CNS condition.

Proposition 3.5. [10, Lemma 3 (3)] *Let P be expanding. If $-p_0 \in R_P$ and R_P is additively closed then P is a CNS polynomial.*

Proof. This is clear by Lemma 3.4 and [10, Lemma 3] since $|p_0| > 1$. □

We now describe a seemingly rare type of the canonical representative of the constant term of P for which we introduce the following name.

Definition 3.6. The polynomial $P \in \mathbb{Z}[X]$ is called super-special if it enjoys the following properties.

(i) P is monic of positive degree and $|P(0)| > 1$.
(ii) There exists a polynomial $E \in D[X]$ which canonically represents $|P(0)|$, and we have $E(1) = |P(0)|$.

Example 3.7. Linear CNS polynomials (see [17], [4, Remark 4.5]) and quadratic CNS polynomials (see [18, 19, 15, 9, 28, 6]) with non-negative linear coefficient are super-special, but $X^2 - X + p_0$ is not super-special (see Example 2.6 (ii)).

In view of this example the next result shows that there are super-special CNS polynomials of arbitrary degree.

Proposition 3.8. *Let P be super-special and $k \in \mathbb{N}_{>0}$. Then $P(X^k)$ is super-special. Furthermore, if $E \in \mathcal{D}[X]$ is the canonical representative of $P(0)$ w.r.t. P, then $E(X^k)$ is the canonical representative of $P(0)$ w.r.t. $P(X^k)$.*

Proof. This is an immediate consequence of Lemma 2.7. □

Super-special semi-CNS polynomials must have positive constant terms as we shall see now.

Proposition 3.9. *If P is a super-special semi-CNS polynomial then we have $p_0 \geq 2$.*

Proof. Let us assume $p_0 < 2$. Then our prerequisites imply $p_0 \leq -2$, and [10, Theorem 5] yields $p_1, \ldots, p_{d-1} \geq 0$ and $P(1) < 0$. Thus

$$\sum_{i=1}^{d} p_i < -p_0 = |p_0|,$$

hence $p_1, \ldots, p_{d-1} \in D$. From Example 2.1 we infer that $E := P - p_0$ canonically represents $-p_0$, and the fact

$$E(1) = |P(0)| = -p_0$$

leads to $P(1) = 0$: Contradiction. □

The canonical representative of the modulus of the constant term of the given polynomial P seems to be interesting because of its connection to canonical numeration systems: W. J. Gilbert [15] who was among the first authors who systematically studied CNS polynomials established a sufficient condition for a polynomial to be a CNS polynomial which directly involved the canonical representation of the constant term. Here we exploit a slightly different aspect of this characterization result (see Theorem 3.12 below).

Lemma 3.10. (i) *The following statements are equivalent:*

(a) *There exists some* $C \in \mathbb{Z}[X]$ *with* $C(0) = -1$ *and* $C(1) = 0$ *such that all coefficients of the polynomial* $PC + P(0)$ *are nonnegative.*

(b) *There exists some* $M \in \mathbb{Z}[X]$ *such that the coefficients of the polynomial*

$$\sum_{k=0}^{n} q_k X^k := MP \tag{5}$$

satisfy

$$1 \leq q_n \leq q_{n-1} \leq \cdots \leq q_0 = P(0), \tag{6}$$

where we set $n = d + \deg(M)$.

(ii) *Suppose that* P *has a root outside the closed unit disk and that statement (b) in (i) is satisfied. Then* P *is super-special.*

Proof. (i) If some $C \in \mathbb{Z}[X]$ with the required properties exists then C is nonconstant with positive leading coefficient, and C is divisible by $X - 1$. Let $M \in \mathbb{Z}[X]$ with $(X - 1)M = C$. Clearly, $q_n > 0$, $C(0) = -1$ yields $M(0) = 1$, and by (5) we have

$$\begin{aligned} q_n X^{n+1} + \sum_{k=1}^{n} (q_{k-1} - q_k) X^k &= q_n X^{n+1} + \sum_{k=1}^{n} (q_{k-1} - q_k) X^k - q_0 + M(0)P(0) \\ &= XMP - MP + P(0) \\ &= (X-1)MP + P(0) = CP + P(0) \in \mathbb{N}[X], \end{aligned}$$

hence (6).

Conversely, let us assume that $M \in \mathbb{Z}[X]$ exists such that (5) and (6) are satisfied. In view of

$$p_0 = q_0 = (MP)(0) = M(0)p_0$$

we have $M(0) = 1$, and the polynomial $C := (X-1)M$ fulfills our requirements.

(ii) Using the notation introduced above we know

$$q_n X^{n+1} + \sum_{k=1}^{n} (q_{k-1} - q_k) X^k \equiv P(0) \pmod{P}.$$

Observe that $q_n < p_0$: The assumption of the contrary leads to

$$q_k = p_0 \quad (k = 0, \ldots, n),$$

hence $p_0 X^{n+1} = CP + p_0$, and therefore

$$p_0(X^{n+1} - 1) = CP.$$

This implies that every root of the polynomial PC is an $(n+1)$st root of unity which contradicts our assumptions. The proof can now easily be completed. □

In view of this result we consider the following set

$$\mathcal{K} := \left\{ \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X] \ : \ n \in \mathbb{N}_{>0}, 0 < a_n < a_0, a_n \leq a_{n-1} \leq \cdots \leq a_1 \leq a_0 \right\}$$

of integer polynomials. Polynomials of this structure were introduced by B. Kovács [23] in the course of his investigations of canonical numeration systems.

Remark 3.11. Let $p_0 > 1$. We exhibit canonical representatives of p_0 w.r.t. two different polynomials thereby showing that these polynomials are in fact super-special.

(i) The polynomial $X^{2d}+(p_0-1)X^d$ canonically represents p_0 w.r.t. X^d+p_0 because we have
$$(X^d + p_0)(X^d - 1) = X^{2d} + (p_0 - 1)X^d - p_0.$$
(ii) If $\sum_{k=0}^{d} p_k X^k \in \mathcal{K}$ then $p_d X^{d+1} + \sum_{k=1}^{d}(p_{k-1} - p_k)X^k$ canonically represents p_0 because we have
$$(X-1) \cdot \sum_{k=0}^{d} p_k X^k = p_d X^{d+1} + \sum_{k=1}^{d}(p_{k-1} - p_k)X^k - p_0.$$

We can now characterize super-special polynomials which do not vanish at roots of unity.

Theorem 3.12. *Let $P \in \mathbb{Z}[X]$ be a monic polynomial of positive degree such that no root of P is a root of unity. Then P is super-special if and only if there exists some $M \in \mathbb{Z}[X]$ such that*

$$MP \in \mathcal{K}. \tag{7}$$

Proof. Let us first assume that P is super-special. We infer from Proposition 3.9 that $p_0 > 1$. Let $E \in D[X]$ canonically represent p_0, thus $E(1) = p_0$, and there is $T \in \mathbb{Z}[X]$ such that

$$PT = E - p_0.$$

Therefore $P(1)T(1) = 0$, hence $T(1) = 0$ since $P(1) \neq 0$. Let $M \in \mathbb{Z}[X]$ such that $T = (X-1)M$ and set

$$Q := \sum_{k=0}^{n} q_k X^k := (E - p_0)/(X - 1),$$

thus $MP = Q$, $q_n \neq 0$, and using Lemma 2.5 we find

$$q_0 = (E(0) - p_0)/(-1) = p_0.$$

Multiplying by $X - 1$ yields

$$q_n X^{n+1} + \sum_{k=1}^{n}(q_{k-1} - q_k)X^k - q_0 = E - p_0,$$

hence

$$q_{k-1} - q_k \in D \qquad (k = 1, \dots, n)$$

and thus

$$1 \le q_n \le q_{n-1} \le \cdots \le q_0,$$

i.e., (7) holds.

Conversely, let $M \in \mathbb{Z}[X]$ such that (7) holds. Then P is super-special by Lemma 3.10. □

Now we are in a position to slightly sharpen [11, Theorem 4].

Theorem 3.13. *Every super-special polynomial which does not vanish at a root of unity is a CNS polynomial.*

Proof. From [11, Theorem 4] we infer that P is a semi-CNS polynomial with $|P(0)| \ge 2$. By [10, Lemma 3] we know that P is expanding, and Proposition 3.9 yields $P(0) \ge 2$. Thus $P(1) > 0$, and an application of [10, Theorem 5] concludes the proof. □

We mention that super-special polynomials with positive constant terms need not be CNS polynomials; more precisely, super-special polynomials may vanish at a root of unity.

Example 3.14. Let $p \in \mathbb{Z}, p \ge 2$ and $P = X^3 + X^2 + pX + p$, thus $P \in \mathcal{K}$. In view of

$$(X-1) \cdot P = X^4 + (p-1)X^2 - p$$

the canonical representative of p is $X^4 + (p-1)X^2$, hence P is super-special. However, P is not a CNS polynomial since it vanishes at -1 (see [15, 26]).

4. Canonical representation of -1

The main interest of the algorithm described in [11] is the computation of the coefficients of the canonical representative of a given integer polynomial if such a representative exists. In this section we shed some more light on auxiliary quantities which are used in the course of this algorithm.

As is sometimes convenient we set the degree of the zero polynomial equal to -1. We always assume $|p_0| > 1$. For $A = \sum_{i=0}^{d-1} a_i X^i \in \mathbb{Z}[X]$ we set

$$T_P(A) = \sum_{i=1}^{d-1} (a_i - \operatorname{sign}(p_0) \lfloor a_0/|p_0| \rfloor p_i)\, X^{i-1} - \operatorname{sign}(p_0) \lfloor a_0/|p_0| \rfloor\, X^{d-1}\,.$$

Thus T_P is a mapping from the set of integer polynomials of degree less than d into itself (see [11, Section 3] for more details).

Lemma 4.1. *Let $A \in \mathbb{Z}[X]$ with $\deg(A) < d$. Further, we set $A_k = T_P^k(A)$ and $\delta_k = -\lfloor A_k(0)/|p_0| \rfloor$ for $k \in \mathbb{N}$.*

(i) *The following recurrence relation holds:*

$$XA_{k+1} = A_k - A_k(0) + \delta_k \sum_{i=1}^{d} p_i X^i \quad (k \in \mathbb{N}).$$

In particular, we have $\deg(A_k) < d$ *for all* $k \in \mathbb{N}$.

(ii) *If* $A \in R_P$ *then the coefficients of the canonical representative of* A *are given by*

$$e_k = A_k(0) + \delta_k |p_0| \quad (k \in \mathbb{N}).$$

(iii) *Let* $k \in \mathbb{N}$. *If* $\delta_k \neq 0$ *then* $\deg(A_{k+1}) = d - 1$ *and* $\mathrm{lc}\,(A_{k+1}) = \delta_k$.

Proof. (i), (ii) This is a reformulation of the algorithm described in [11].
(iii) Clear by (i). □

In the following we tacitly use the notation introduced in Lemma 4.1.

Lemma 4.2. *Let* $A \in \mathbb{Z}[X]$ *with* $\deg(A) < d$. *Then* $A \in R_P$ *if and only if there is some* $m \in \mathbb{N}$ *such that*

$$\delta_m = \delta_{m+1} = \cdots = \delta_{m+d-1} = 0.$$

Moreover, if $d \geq 2$, $A \in R_P \setminus D[X]$ *and* m *is chosen minimal with this property then the leading coefficient of the canonical representative of* A *equals* δ_{m-1}.

Proof. Let $A \in R_P$. If $A \in D[X]$ our assertion is trivial. Therefore let $A \notin D[X]$, thus $\mathrm{L}(A) \geq d$ by Proposition 2.2, and there is some minimal $K \in \mathbb{N}$ such that $A_k = 0$ for all $k \geq K$. In particular, we see

$$e_k = 0 \quad (k \geq K) \tag{8}$$

by Lemma 4.1 and therefore $K \geq d$. Observe that

$$\delta_k = 0 \quad (k \geq K - 1) \tag{9}$$

by Lemma 4.1 (iii). Therefore we can choose $m := K - 1$.

Conversely, let $\delta_m = \cdots = \delta_{m+d-1} = 0$. Then Lemma 4.1 immediately yields

$$A_{m+j+1} = 0 \text{ or } \deg(A_{m+j+1}) = \deg(A_{m+j}) - 1 \quad (j = 0, \ldots, d-1).$$

Therefore, in particular we find

$$\deg(A_{m+d-1}) \leq \deg(A_m) - (d-1) \leq 0$$

which together with $\delta_{m+d-1} = 0$ implies $A_{m+d} = 0$ and then

$$A_k = 0 \quad (k \geq m + d)$$

by Lemma 4.1. But this means $A \in R_P$.

Finally, we turn to the last statement of our lemma. Here $m > 0$, and by the minimality of m we have $\delta_{m-1} \neq 0$. We claim

$$\delta_{K-j} = 0, \quad A_{K-j} \in D[X], \quad \deg(A_{K-j}) = j - 1 \quad (j = 1, \ldots, d) \tag{10}$$

where K is defined as above. Indeed, observe $\delta_{K-1} = 0$ by (9), hence $A_{K-1}(0) \in D$, and set $A_{K-1} = \sum_{i=0}^{n} a_i X^i$ with $a_n \neq 0$. Then Lemma 4.1 yields

$$0 = XA_K = \sum_{i=1}^{n} a_i X^i,$$

hence $n = 0$, i.e., $\deg(A_{K-1}) = 0$, and (9) implies $a_0 = A_{K-1}(0) \in D$.

Now assume $1 \leq j < d$, $A_{K-j} = \sum_{i=0}^{j-1} a_i X^i \in D[X]$ and $A_{K-(j+1)} = \sum_{i=0}^{n} b_i X^i$ with $n < d$. Using Lemma 4.1 (i) and comparing degrees yields $\delta_{K-j-1} = 0$, $b_1 = a_0, \ldots, b_j = a_{j-1} \in D$ and $b_i = 0$ for $i > j$, thus in particular $\deg(A_{K-(j+1)}) = j$. The assumption $b_0 \notin D$ would lead to $\delta_{K-(j+1)} \neq 0$ and imply the contradiction $\deg(A_{K-j}) = d-1$. Thus $A_{K-(j+1)} \in D[X]$. The proof of (10) is complete.

From the above we deduce

$$A_m = A_{K-d} \in D[X],$$

and

$$e_{K-1} = A_{K-1}(0) = \operatorname{lc}(A_{K-2}) = \cdots = \operatorname{lc}(A_{K-d}) = \operatorname{lc}(A_m) = \delta_{m-1}.$$

In view of (8) the proof is terminated. □

We now describe the first few steps of the iteration T_P applied to a small negative integer. Certainly, these considerations can be carried over to find the canonical representatives of arbitrary integer polynomials, however, we give it in this special form for reasons of simplicity.

Lemma 4.3. *Let $d \geq 3$, $p_0 \geq 2$ and $A_0 \in \{-p_0, \ldots, -1\}$.*

(i) *We have*

$$A_1 = \sum_{i=0}^{d-1} p_{i+1} X^i, \quad \delta_1 = -\lfloor p_1/p_0 \rfloor$$

and

$$A_k = \sum_{i=0}^{d-k} a_{k,i} X^i + \sum_{i=d-k+1}^{d-2} b_{k,i} X^i + \delta_{k-1} X^{d-1}$$

for $k = 2, \ldots, d$, where we put

$$a_{k,i} = \sum_{j=0}^{k-1} \delta_j p_{i+k-j}, \; b_{k,i} = \sum_{j=1}^{k-1} \delta_{k-j} p_{i+j} \quad (k, i \in \mathbb{N})$$

with

$$\delta_0 = 1, \; \delta_k = -\left\lfloor \frac{1}{p_0} \sum_{j=0}^{k-1} \delta_j p_{k-j} \right\rfloor \quad (k = 2, \ldots, d)$$

and the conventions $p_j := 0$ for $j \in \mathbb{Z} \setminus \{0, \ldots, d\}$.

(ii) *For $k \geq 1$ we have*

$$A_{d+k} = \sum_{i=0}^{d-2} b_{d+k,i} X^i + \delta_{d+k-1} X^{d-1}$$

with

$$\delta_{d+k} = -\left\lfloor \frac{1}{p_0} \sum_{j=0}^{d-1} \delta_{d+k-j-1} p_{j+1} \right\rfloor.$$

(iii) $A_0 \in R_P$ *if and only if* $e_k = 0$ *for* k *sufficiently large where we have*

$$e_k = \begin{cases} A_0 + p_0 & (k = 0), \\ \sum_{j=0}^{k} \delta_j p_{k-j} & (1 \leq k \leq d), \\ \sum_{j=1}^{k} \delta_j p_{k-j} & (k > d). \end{cases}$$

In this case, $\sum_{k=0}^{\infty} e_k X^k$ *canonically represents* A_0.

Proof. (i), (ii) Using the algorithm described in [11] this can easily be checked by induction.

(iii) Clear by an application of (i), (ii) and Lemma 4.1. □

Proposition 4.4. *Let* $P = X^3 + p_2 X^2 + p_1 X + p_0$ *be a super-special cubic polynomial which satisfies Gilbert's conditions (see* [5, Section 3]*), i.e.,*

(i) $p_0 \geq 2$,
(ii) $p_1 + p_2 \geq -1$,
(iii) $p_1 - p_2 \leq p_0 - 2$
(iv) $0 \leq p_2 \leq \begin{cases} p_0 - 2, & \text{if } p_1 \leq 0, \\ p_0 - 1, & \text{if } 1 \leq p_1 \leq p_0 - 1, \\ p_0, & \text{if } p_1 \geq p_0. \end{cases}$

Then we have $P \in \mathcal{K}$ *or* $p_1 = p_2 = 0$. *Furthermore, the canonical representative of* p_0 *(*$-p_0$*, respectively) is monic.*

Proof. Using Lemmas 4.1 and 4.3 this can straightforwardly be checked. We leave the details to the reader. □

S. Akiyama predicted the leading coefficient of the canonical representative of -1 w.r.t. CNS polynomials.

Conjecture 4.5. [1] If P is a CNS polynomial then the canonical representative of -1 w.r.t. P is monic.

By [2] the truth of this conjecture is equivalent to the connectedness of the SRS tile (see [3] for details). Here we can only list some examples where Conjecture 4.5 turns out to be true. To this purpose we exploit the following straightforward reformulation of the conjecture.

Lemma 4.6. *Let* P *be a CNS polynomial. Then* P *satisfies Conjecture 4.5 if and only if there exists a monic polynomial* $M \in \mathbb{Z}[X]$ *with* $M(0) = 1$ *such that apart from the constant term all coefficients of* MP *belong to* D.

Proof. Let $E \in D[X]$ be monic such that $E(0) \equiv -1 \pmod P$. Then there exists $M \in \mathbb{Z}[X]$ such that $MP = E+1$. Clearly, M is monic, and Lemma 2.5 yields $M(0) = 1$.

Conversely, $E := MP$ is monic, $E(0) = p_0$ and $E - 1 \in D[X]$. Thus $E - 1$ is the canonical representative of -1. □

Proposition 4.7. *If P be a CNS polynomial then the canonical representative of -1 is monic provided that one the following conditions hold:*

(i) $P(0) = 2$.

(ii) *P fulfills the dominant condition (see* [6]*), i.e.,*

$$\sum_{i=1}^{d-1} |p_i| < p_0. \tag{11}$$

(iii) *$P(X) = Q(X^r)$ where $r \in \mathbb{N}_{>0}$ and the polynomial Q admits a monic canonical representative of -1.*

(iv) $0 \le p_i \le p_0 - 1$ *for* $i = 1, \dots, d-1$.

(v) $d \le 3$.

(vi) *The coefficients of P enjoy the following properties:*

$$p_0 \le p_1 < 2p_0,\ 1 \le p_{d-1} < p_0,\ 0 \le p_i - p_{i-1} + p_{i-2} < p_0 \quad (i = 2, \dots, d).$$

Proof. (i) In view of $D = \{0, 1\}$ this is trivial.

(ii) By Example 2.6 the assertion is clear for $d = 1$. Therefore let $d \ge 2$. Using Lemma 4.3 and the notation introduced there we easily find $\delta_k \in \{-1, 0, 1\}$ for every $k \in \mathbb{N}$, and an application of Lemma 4.2 concludes the proof.

(iii) Clear by Lemma 2.7.

(iv) Clear by Lemma 4.6 with $M := 1$.

(v) As just mentioned above the case $d = 1$ is clear. For $d = 2$ we have $-1 \le p_1 \le p_0$ (see the references in Example 3.7). If $0 \le p_1 < p_0$ our assertion is clear by (iv). For $p_1 = -1$ Lemma 4.3 yields $\delta_1 = 1$ and $\delta_2 = \delta_3 = 0$ and we are done by Lemma 4.2. Similarly, for $p_1 = p_0$ we find $\delta_1 = \delta_2 = -1$, $\delta_3 = 1$, and $\delta_4 = \delta_5 = 0$, and we conclude as before.

Let now $d = 3$. By [5, Theorem 3.1] the coefficients p_1 and p_2 satisfy Gilbert's conditions. An application of Lemma 4.3 yields the following results (in this table only additional conditions on the coefficients p_1 and p_2 are listed):

p_1	p_2	canonical representative of -1
$0 \le p_1 < p_0$		$X^3 + p_2X^2 + p_1X + p_0 - 1$
$p_1 = p_0$	$p_2 = p_0$	$X^9 + (p_0 - 1)X^8 + X^6 + (p_0 - 1)X^4 + X^3 + p_0 - 1$
$p_1 \ge p_0$	$p_2 < p_1$	$X^5 + (p_2 - 1)X^4 + (p_1 - p_2 + 1)X^3 + (p_0 - p_1 + p_2)X^2 + (p_1 - p_0)X + p_0 - 1$
$p_1 < 0$	$p_2 = -p_1 - 1$	$X^5 + (p_2 + 1)X^4 + (p_0 - 1)X^2 + (p_0 + p_1)X + p_0 - 1$
$p_1 < 0$	$p_2 \ge -p_1$	$X^4 + (p_2 + 1)X^3 + (p_1 + p_2)X^2 + (p_0 + p_1)X + p_0 - 1$

(vi) Clear by Lemma 4.6 with $M := X^2 - X + 1$. □

Certainly, one can easily construct similar examples as the final condition of the Proposition above. Here we only give a simple illustration of this condition.

Example 4.8. The canonical representative of -1 of the CNS polynomial $X^4 + X^3 + 3X^2 + 5X + 4$ is monic by Proposition 4.7 (vi).

Our numerical calculations suggest that Conjecture 4.5 might be extended.

Conjecture 4.9. Let P be a CNS polynomial. For every $m \in \mathbb{Z} \setminus D_P$ the canonical representative of m is monic.

5. Acknowledgement

The author wishes to express his gratitude to Professor Shigeki Akiyama for informing him on his Conjecture 4.5 and its relation to SRS tiles. The author is indebted to an anonymous referee for carefully reading the first version of this paper.

References

[1] S. Akiyama. Private communication, 2001.
[2] S. Akiyama. Private communication, 2006.
[3] S. Akiyama. Pisot number system and its dual tiling. In *Physics and theoretical computer science*, volume 7 of *NATO Secur. Sci. Ser. D Inf. Commun. Secur.*, pages 133–154. IOS, Amsterdam, 2007.
[4] S. Akiyama, T. Borbély, H. Brunotte, A. Pethő, and J. M. Thuswaldner. Generalized radix representations and dynamical systems. I. *Acta Math. Hungar.*, 108(3):207–238, 2005.
[5] S. Akiyama, H. Brunotte, and A. Pethő. Cubic CNS polynomials, notes on a conjecture of W. J. Gilbert. *J. Math. Anal. Appl.*, 281(1):402–415, 2003.
[6] S. Akiyama and H. Rao. New criteria for canonical number systems. *Acta Arith.*, 111(1):5–25, 2004.
[7] G. Barat, V. Berthé, P. Liardet, and J. Thuswaldner. Dynamical directions in numeration. *Ann. Inst. Fourier (Grenoble)*, 56(7):1987–2092, 2006. Numération, pavages, substitutions.
[8] V. Berthé. Numeration and discrete dynamical systems. *Computing*, 94(2-4):369–387, 2012.
[9] H. Brunotte. Characterization of CNS trinomials. *Acta Sci. Math. (Szeged)*, 68(3-4):673–679, 2002.
[10] H. Brunotte. Characterization of semi-CNS polynomials. *Acta Math. Acad. Paedagog. Nyházi. (N.S.)*, 28(2):91–94, 2012.
[11] H. Brunotte. A unified proof of two classical theorems on CNS polynomials. *Integers*, 12(4):709–721, 2012.
[12] P. Burcsi. *Algorithmic aspects of generalized number systems.* Phd thesis, Eötvös Loránd University, Budapest, 2008.
[13] P. Burcsi and A. Kovács. Exhaustive search methods for CNS polynomials. *Monatsh. Math.*, 155(3-4):421–430, 2008.
[14] A. Chen. On the reducible quintic complete base polynomials. *J. Number Theory*, 129(1):220–230, 2009.
[15] W. J. Gilbert. Radix representations of quadratic fields. *J. Math. Anal. Appl.*, 83(1):264–274, 1981.
[16] E. H. Grossman. Number bases in quadratic fields. *Studia Sci. Math. Hungar.*, 20(1-4):55–58, 1985.

[17] V. Grünwald. Intorno all' aritmetica dei sistemi numerici a base negativa con particolare riguardo al sistema numerico a base negativo-decimale per lo studio delle sue analogie coll' aritmetica ordinaria (decimale). *Battaglini G.*, 23:203–221, 1885.

[18] I. Kátai and B. Kovács. Kanonische Zahlensysteme in der Theorie der quadratischen algebraischen Zahlen. *Acta Sci. Math. (Szeged)*, 42(1-2):99–107, 1980.

[19] I. Kátai and B. Kovács. Canonical number systems in imaginary quadratic fields. *Acta Math. Acad. Sci. Hungar.*, 37(1-3):159–164, 1981.

[20] I. Kátai and J. Szabó. Canonical number systems for complex integers. *Acta Sci. Math. (Szeged)*, 37(3-4):255–260, 1975.

[21] D. E. Knuth. An imaginary number system. *Comm. ACM*, 3:245–247, 1960.

[22] A. Kovács. Number expansions in lattices. *Math. Comput. Modelling*, 38(7-9):909–915, 2003. Hungarian applied mathematics and computer applications.

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

[24] B. Kovács and A. Pethő. On a representation of algebraic integers. *Studia Sci. Math. Hungar.*, 27(1-2):169–172, 1992.

[25] V. L. Kurakin. The first digit carry function in a Galois ring. *Diskret. Mat.*, 24(2):21–36, 2012.

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

[27] A. Tátrai. Parallel implementations of Brunotte's algorithm. *J. Parallel Distrib. Comput.*, 71(4):565–572, 2011.

[28] J. M. Thuswardner. Elementary properties of canonical number systems in quadratic fields. In *Applications of Fibonacci numbers, Vol. 7 (Graz, 1996)*, pages 405–414. Kluwer Acad. Publ., Dordrecht, 1998.

Received September 7, 2013.

Haus-Endt-Strasse 88,
D-40593 Düsseldorf,
Germany
E-mail address: brunoth@web.de