#A17 INTEGERS 12 (2012)

A UNIFIED PROOF OF TWO CLASSICAL THEOREMS ON CNS POLYNOMIALS

Horst Brunotte
Haus-Endt-Strasse 88, D-40593 Düsseldorf, Germany
brunoth@web.de

Received: 8/18/11, Accepted: 2/16/12, Published: 3/1/12

Abstract
A sufficient condition for a monic integer polynomial to be a semi-CNS polynomial is presented. This result infers a unified proof of two well-known theorems on irreducible CNS polynomials thereby extending them to reducible polynomials.

1. Introduction

Canonical number systems (usually abbreviated by CNS) can be regarded as generalizations of the decimal or binary numeration systems. They have first been introduced by the Hungarian school some decades ago (see [19, 17, 18, 21] and [15,20] for the first special cases). We recommend the work [7] as a profound survey on this subject in a broader context.

The concept of CNS polynomials was introduced by A. Pethő and extended to semi-CNS polynomials by P. Burcsi and A. Kovács (the reader is referred to Section 2 for all necessary definitions). Some characterization results on these polynomials are known (see e.g., [17, 14] for quadratic polynomials, [3, 8, 4, 26, 10] for some other classes of polynomials and [22, 16] for general results). However, until now the complete description of these polynomials remains an open problem even for small degrees. On the other hand, there are a few results stating sufficient conditions for a polynomial to be a CNS polynomial (see e.g., [14, 22, 3, 12]) or a semi-CNS polynomial (see e.g., [11]).

Exploiting known methods we present a new sufficient condition for a monic integer polynomial P to be a semi-CNS polynomial (see Theorem 4). Based on this result we derive proofs of two apparently different theorems of W. J. Gilbert and B. Kovács – A. Pethő (see Corollaries 5 and 8) on irreducible CNS polynomials thereby extending them to reducible polynomials. Our result requires the knowledge of the canonical representation of the absolute value of the constant term of the polynomial P. Therefore we present an algorithm for the calculation of canonical representatives in the last part of this note.

The author is indebted to an anonymous referee for very carefully reading the first version of the manuscript.

2. A Necessary Condition for Semi-CNS Polynomials

Throughout this note we let $P \in \mathbb{Z}[X]$ be a monic integer polynomial of positive degree with $P(0) \neq 0$ and $\mathcal{D} = [0, |P(0)| - 1] \cap \mathbb{N}$ where we denote by $\mathbb{N}$ the set of nonnegative rational integers. We say that the polynomial $A \in \mathbb{Z}[X]$ is canonically representable (with respect to P) if A is congruent modulo P to a polynomial $B \in \mathcal{D}[X]$. In this case we say that B canonically represents A, and we call the coefficients of B the digits of the canonical representation of A. We denote by R_P the set of all canonically representable integer polynomials. It is easy to see that each $A \in R_P$ has a unique representative $B \in \mathcal{D}[X]$.

CNS polynomials were introduced by A. Pethő and generalized in the sequel (see e.g., [1, 5, 29]). Recently, this notion was extended to semi-CNS polynomials by P. Burcsi and A. Kovács. For convenience we recall their definitions in a form slightly adapted to our purposes here.

Definition 1.

(i) P is called a CNS polynomial if $\mathbb{Z}[X] = R_P$ [24].

(ii) P is called a semi-CNS polynomial if R_P is an additive semigroup [11, Definition 3.2].

It is known that all semi-CNS polynomial P with $|P(0)| \geq 2$ are expanding (see [10, Theorem 11]). Moreover, we shall make use of the following properties of semi-CNS polynomials.

Proposition 2.*Let $P \in \mathbb{Z}[X]$ be a monic integer polynomial.*

(i) *P be a semi-CNS polynomial with $|P(0)| \geq 2$ if and only if $\mathbb{N}[X] \subseteq R_P$.*

(ii) *P is a CNS polynomial if and only if P is a semi-CNS polynomial with $|P(0)| \geq 2$ and does not have a real positive root.*

Proof. (i) This follows directly from the definitions.

(ii) If P is a CNS polynomial then P has the required properties [14, 24]. Conversely, let P be a semi-CNS polynomial which does not have a real positive root and satisfies $|P(0)| \geq 2$. Clearly, we have $P(0) \geq 2$. We infer from [9, Theorem 21] that there is a polynomial $G \in \mathbb{Z}[X]$ such that $GP \in \mathbb{N}_{>0}[X]$. Let $A \in \mathbb{Z}[X]$.

Then we can find some $H \in \mathbb{N}[X]$ with $A + GHP \in \mathbb{N}[X]$. As P is a semi-CNS polynomial there is some $E \in \mathcal{D}[X]$ with

$$A + GHP \equiv E \pmod{P} ,$$

hence we conclude $A \in R_P$. □

Corollary 3. *Let P be a semi-CNS polynomial with only nonnegative coefficients and $P(0) \geq 2$. Then P is a CNS polynomial.*

Our main result exhibits a necessary condition for P to be a semi-CNS polynomial under the condition that the modulus of its constant term has a particularly nice canonical representative modulo P. The idea is taken from W. J. Gilbert [14, Proposition 7], and the essence of the proof is modeled on [25, proof of Theorem 4].

Theorem 4. *Let $P \in \mathbb{Z}[X]$ be a monic polynomial of positive degree with $P(0) \neq 0$ and assume that no root of P is a root of unity. Further, let $B \in \mathcal{D}[X]$ canonically represent $|P(0)|$ and suppose $B(1) = |P(0)|$. Then P is a semi-CNS polynomial with $|P(0)| \geq 2$.*

Proof. Let $M \in \mathbb{Z}[X]$ with $B - |P(0)| = MP$. Then

$$P(0)\bigl(M(0) + \operatorname{sign} P(0)\bigr) = (MP)(0) + |P(0)| = B(0) \in \mathcal{D},$$

hence $M(0) = -\operatorname{sign} P(0)$ in view of $P(0) \neq 0$. Further, we have $M(1) = 0$ because

$$M(1)P(1) = B(1) - |P(0)| = 0$$

and $P(1) \neq 0$. Clearly, the polynomial $MP + |P(0)|$ has only nonnegative coefficients.

It suffices to show that $\mathbb{N}[X] \subseteq R_P$ since then Proposition 2 (i) implies that P is a semi-CNS polynomial with the required property.

We closely follow [25, proof of Theorem 4]. Let $A \in \mathbb{N}[X]$ and define integers a_k and polynomials D_k by

$$D_0 = A, \qquad D_k + \left\lfloor \frac{D_k(0)}{|P(0)|} \right\rfloor PM = XD_{k+1} + a_k \qquad (k \in \mathbb{N}).$$

Obviously, the integers a_k belong to $\mathcal{D}$. Using induction we check that the polynomials D_k belong to $\mathbb{N}[X]$. Observing

$$D_k(1) = D_{k+1}(1) + a_k \tag{1}$$

we see that the sequence $(D_k(1))_{k\in\mathbb{N}}$ is monotonously decreasing, hence ultimately constant. Therefore we find some $s, \ell \in \mathbb{N}$ such that $D_k(1) = s$ for all $k \geq \ell > 0$.

Denoting by $\overline{y}$ the image of $y \in \mathbb{Z}[X]$ under the canonical epimorphism $\mathbb{Z}[X] \longrightarrow \mathbb{Z}[X]/P\mathbb{Z}[X]$ it suffices to show $\overline{D_\ell} = 0$ because then

$$\overline{A} = \overline{D_0} = \sum_{k=0}^{\ell-1} (\overline{D_k} - \overline{X}\,\overline{D_{k+1}})\overline{X}^k = \sum_{k=0}^{\ell-1} \overline{a_k}\,\overline{X}^k.$$

By (1) for $k \geq \ell$ we have $a_k = 0$, hence $\overline{D_k} = \overline{X}\,\overline{D_{k+1}}$, and therefore

$$\overline{D_\ell} = \overline{X}^k\,\overline{D_{k+\ell}} \quad \text{for all } k \in \mathbb{N}. \tag{2}$$

Observe that the nonempty set $\{D_{k+\ell} : k \in \mathbb{N}\}$ is finite because $D_{k+\ell}$ has only nonnegative coefficients and $D_{k+\ell}(1)$ is bounded. Thus there exist $k, m \in \mathbb{N},\ k < m$ with $D_{k+\ell} = D_{m+\ell}$. Using (2) we find

$$(\overline{X}^{m+\ell} - \overline{X}^{k+\ell})\overline{D_{k+\ell}} = \overline{X}^{m+\ell}\,\overline{D_{m+\ell}} - \overline{X}^\ell\,\overline{D_\ell} = \overline{X}^\ell\,\overline{D_\ell} - \overline{X}^\ell\,\overline{D_\ell} = 0,$$

i.e., P divides $X^{k+\ell}(X^{m-k} - 1)D_{k+\ell}$, and we conclude that P is a divisor of $X^{k+\ell}D_{k+\ell}$ by our assumptions on P. Thus we find some $G \in \mathbb{Z}[X]$ with $PG = X^{k+\ell}D_{k+\ell}$ which by (2) yields our desired relation. □

The following result was established by B. Kovács and A. Pethő for irreducible polynomials and generalized in [2].

Corollary 5 (Kovács – Pethő [22, Theorem 6]). *Let $P = p_d X^d + p_{d-1}X^{d-1} + \cdots + p_0 \in \mathbb{Z}[X],\ d \geq 1$ and $1 = p_d \leq p_{d-1} \leq \ldots \leq p_1 \leq p_0$. If P is not divisible by a cyclotomic polynomial then P is a CNS polynomial.*

Proof. Set $B = (X - 1) \cdot P$ and apply the Theorem and Proposition 2 (ii). □

We mention two easily applicable consequences of Corollary 5.

Corollary 6. *Let $P = p_d X^d + p_{d-1}X^{d-1} + \cdots + p_0 \in \mathbb{Z}[X],\ d \geq 2$ and $1 = p_d \leq p_{d-1} \leq \ldots \leq p_1 \leq p_0$. If either P is irreducible and $p_0 \geq 2$ or*

$$\gcd\big\{j \in \{1, \ldots, d+1\} : p_j < p_{j-1}\big\} = 1 \qquad (p_{d+1} := 0) \tag{3}$$

then P is a CNS polynomial.

Proof. If P is irreducible then the assertion is clear by Corollary 5. Now assume (3) and set

$$\mu = \min\Big\{\frac{p_j}{p_{j+1}} : j = 0, \ldots, d-1\Big\},$$

hence $\mu \geq 1$. By Corollary 5 it suffices to show that P is not divisible by a cyclotomic polynomial. Assume on the contrary that P has a root on the boundary of the unit circle. Then $\mu = 1$ by the theorem of Eneström-Kakeya [6]. But then [6, Theorem 1] yields a contradiction to our prerequisites. □

Corollary 7. *Let* $P = X^d + p_{d-1}X^{d-1} + \cdots + p_0,\ d \geq 2$ *and* $1 \leq p_{d-1} \leq p_{d-2} \leq \cdots \leq p_1 < p_0$. *Then* P *is a CNS polynomial.*

Proof. The set defined in (3) contains 1, hence its greatest common divisor is 1 and the assertion follows from Corollary 6. □

The following statement was proved by W. J. Gilbert for irreducible polynomials.

Corollary 8 (Gilbert [14, Proposition 7]). *Let* P *be a monic integral polynomial with the following properties:*

(i) *All coefficients of* P *are nonnegative.*

(ii) $p_0 = P(0) > 1$

(iii) P *is not divisible by a cyclotomic polynomial.*

(iv) *There exist* $q_1, \ldots, q_m \in \{0, \ldots, p_0 - 1\}$ *with* $m \geq$ *deg* (P) *and* $p_0 = \sum_{i=1}^m q_i$ *such that* P *divides the polynomial* $\sum_{i=1}^m q_i X^i - p_0$.

Then P *is a CNS polynomial.*

Proof. Choose $M \in \mathbb{Z}[X]$ such that $PM = \sum_{i=1}^m q_i X^i - p_0$, and set $B = \sum_{i=1}^m q_i X^i$. Then all prerequisites of the Theorem above are satisfied, and an application of Proposition 2 (ii) completes the proof. □

Example 9. Assume that no cyclotomic polynomial divides $P = X^d + p_{d-1}X^{d-1} + \cdots + p_1 - p_0 \in \mathbb{Z}[X]$ with $p_i \geq 0$ $(i = 1, \ldots, d-1)$ and $p_0 = 1 + p_1 + \cdots + p_{d-1} \geq 2$. Obviously, p_0 is canonically representable, and its canonical representation meets the requirements of Theorem 4. Hence P is a semi-CNS polynomial.

Remark 10.

(i) Apparently only two types of examples for an application of Theorem 4 to CNS polynomials seem to be known, namely the polynomials described in Corollary 5 and the polynomials

$$X^n + p_0 \qquad (p_0 \geq 2), \tag{4}$$

see [14, Section 6] for special cases. Note that the CNS property of the polynomial (4) can also be seen by [8, Theorem 1].

(ii) The converse of Theorem 4 does certainly not hold if $d \geq 2$: The canonical representative of p_0 with respect to the CNS polynomial $X^2 - X + p_0$ (with $p_0 \geq 2$; see e.g., [14, Theorem 1]) is

$$X(X^4 + (p_0 - 1)X^2 + (p_0 - 1)X + 1)\ .$$

3. Computation of Canonical Representatives

In [7, p. 2021] the iteration process for the computation of canonical representatives was presented. Based on this procedure we give a formalized algorithm here. More specifically, we compute the canonical representative of $Q = \sum_{i=0}^{d-1} q_i X^i \in \mathbb{Z}[X]$ with respect to a given monic expanding polynomial $P = X^d + \sum_{i=0}^{d-1} p_i X^i \in \mathbb{Z}[X]$ if such a representative exists. Our Algorithm 1 below requires a bound for the degree of the canonical representative of Q. A suitable value for this bound may be taken from Corollary 13 provided all its prerequisites are satisfied; otherwise one can choose a large heuristic bound. For instance, if P is an irreducible CNS polynomial the algorithm yields the canonical representative of Q.

Algorithm 1 Computation of a canonical representative

Input: $d \in \mathbb{N}_{>0}$, $q_0, \dots, q_{d-1} \in \mathbb{Z}$, coefficients $p_0, \dots, p_{d-1} \in \mathbb{Z}$ of the expanding polynomial $X^d + \sum_{i=0}^{d-1} p_i X^i$, bound $\in \mathbb{N}$.

Output: Vector A of the digits of the canonical representative of $\sum_{i=0}^{d-1} q_i X^i$ or "not canonically representable" or "overflow"

$Q^{(0)} \leftarrow (q_0, \dots, q_{d-1})$
$k \leftarrow 0$
repeat
  $c \leftarrow \left\lfloor Q_0^{(k)} / |p_0| \right\rfloor$
  $A_k \leftarrow Q_0^{(k)} - c\,|p_0|$
  $Q^{(k+1)} \leftarrow (Q_1^{(k)} - (\operatorname{sign} p_0) c p_1, \dots, Q_{d-1}^{(k)} - (\operatorname{sign} p_0) c p_{d-1}, -(\operatorname{sign} p_0) c)$
  $k \leftarrow k + 1$
until $Q^{(k)} = (0, \dots, 0)$ or $Q^{(k)} = Q^{(j)}$ for some $j < k$ or $k >$ bound
if $k >$ bound **then**
  return "overflow"
else
  if $Q^{(k)} = Q^{(j)}$ for some $j < k$ **then**
    return "Not canonically representable"
  else
    return "Digits of the canonical representation:" A
  end if
end if

We conclude with some results on bounds for the degrees of representatives of elements of R_P. Here we denote by $\mathrm{L}_P(A)$ the degree of the canonical representative of $A \in \mathbb{Z}[X]$ if A is not a multiple of P; otherwise we set $\mathrm{L}_P(0) = 0$. Clearly, we have

$$\mathrm{L}_P(X^n A) = n + \mathrm{L}_P(A) \qquad (n \in \mathbb{N})$$

provided P does not divide A.

We start with an easily computable lower bound for degrees of representatives of elements of R_P and denote by Ω_f the set of roots of $f \in \mathbb{Z}[X]$.

Proposition 11. *Let $P \in \mathbb{Z}[X]$ be a monic expanding polynomial and $A \in R_P$. If there is some root of P which is not a root of A we have*

$$\mathrm{L}_P(A) > \max\left\{\frac{\log|A(\alpha)| + \log(|\alpha|-1) - \log(|P(0)|-1)}{\log|\alpha|} \;:\; \alpha \in \Omega_P \setminus \Omega_A\right\} - 1\,.$$

Proof. Our proof is adapted from [23,p. 170]. Let $E = \sum_{i=0}^{k} e_i X^i \in \mathcal{D}[X]$ be the representative of A and $\alpha \in \Omega_P$. Then we have

$$\begin{aligned}|A(\alpha)| = |E(\alpha)| &\le \sum_{i=0}^{k} e_i\, |\alpha|^i \le (|P(0)|-1)\sum_{i=0}^{k} |\alpha|^i \\ &= (|P(0)|-1)\cdot\frac{|\alpha|^{k+1}-1}{|\alpha|-1} < \frac{(|P(0)|-1)\,|\alpha|^{k+1}}{|\alpha|-1}\end{aligned}$$

which implies our assertion by taking logarithms. □

Our next statements are modeled on respective results in the works [23] and [13].

Theorem 12. *Let $P \in \mathbb{Z}[X]$ be a monic, irreducible and expanding polynomial of degree ≥ 2. Then there exist constants L_P and K_P with the following properties.*

(i) *If $A \in R_P$ is not a multiple of P we have*

$$\mathrm{L}_P(A) \le L_P + \left\lceil \max\left\{\frac{\log|A(\alpha)|}{\log|\alpha|} \;:\; \alpha \in \Omega_P\right\}\right\rceil .$$

(ii) *If A, B, $A+B \in R_P$ we have*

$$\mathrm{L}_P(A+B) \le K_P + \max\{\mathrm{L}_P(A),\, \mathrm{L}_P(B)\}\,.$$

Proof. (i) Let $\mu \in \Omega_P$ have minimal modulus among all roots of P and set

$$c = 1 + \frac{|P(0)|-1}{|\mu|-1}\,.$$

It is well known that the set

$$\mathcal{B} = \left\{\gamma \in \mathbb{Z}[\mu] \setminus \{0\} \;:\; \overline{|\gamma|} < c\right\}$$

is finite; here $\overline{|\gamma|}$ denotes the maximum modulus of the conjugates of γ. In view of the uniqueness of the CNS representation the set

$$\mathcal{S} = \{E \in \mathcal{D}[X] \;:\; E(\mu) \in \mathcal{B}\}$$

is also finite. Clearly, $\mathcal{S}$ is nonvoid because $X \in \mathcal{S}$, and we can define

$$L_P = \max\{\deg(E) \ : \ E \in \mathcal{S}\}\,.$$

Set

$$k = \left\lceil \max\left\{ \frac{\log|A(\alpha)|}{\log|\alpha|} \ : \ \alpha \in \Omega_P \right\} \right\rceil,$$

and hence $|A(\alpha)| \le |\alpha|^k$ for all $\alpha \in \Omega_P$. Let $E \in \mathcal{D}[X]$ be the representative of A. Thus there exist $e_0, \ldots, e_{k-1} \in \mathcal{D}$ and $F \in \mathcal{D}[X]$ such that we can write

$$E = \sum_{i=0}^{k-1} e_i X^i + X^k F\,.$$

If $F = 0$ we have

$$\mathrm{L}_P(A) = \deg(E) \le k - 1,$$

and we are done. Otherwise $F \in \mathcal{S}$ as can be seen similarly as in the proof of [22, Lemma 4]: For every $\alpha \in \Omega_P$ we have

$$|\alpha|^k\,|F(\alpha)| \le |A(\alpha)| + \sum_{i=0}^{k-1} e_i\,|\alpha|^i\,,$$

hence

$$|F(\alpha)| \le 1 + \frac{(|P(0)|-1))(|\alpha|^k - 1)}{|\alpha|^k\,(|\alpha|-1)} < 1 + \frac{|P(0)|-1}{|\alpha|-1} \le \frac{|P(0)|-1}{|\mu|-1},$$

and we conclude

$$\mathrm{L}_P(A) = k + \deg(F) \le k + L_P\,.$$

(ii) This can be proved similarly using

$$c = \frac{2\,(|P(0)|-1)}{|\mu|-1}$$

and an analogous definition of K_P. The reader may compare the proof of [13, Proposition 2] which in turn is a modification of an argument in [28, p. 271]. □

The constant K_P introduced above plays a key role in finding a bound mentioned in Algorithm 1.

Corollary 13. *Let $P \in \mathbb{Z}[X]$ be a monic, irreducible and expanding polynomial of degree ≥ 2 and $p = |P(0)|$.*

(i) *If $p \in R_P$ then*

$$\ell := \mathrm{L}_P\,(p) \le \min\left\{ K_P,\ L_P + \left\lceil \frac{\log p}{\log|\mu|} \right\rceil \right\}$$

where K_P and L_P are the constants given by Theorem 12 and μ is a root of minimal modulus of P.

(ii) *For* $n \in \mathbb{N}_{>0}$ *we have*

$$\mathrm{L}_P\,(np) \leq \ell + (n-1)K_P$$

provided $p, 2p, \ldots, np \in R_P$.

(iii) *If* $\mathbb{N} \subseteq R_P$ *we have*

$$\mathrm{L}_P\,(n) \leq \ell + \left\lfloor \frac{n}{p} \right\rfloor K_P \qquad (n \in \mathbb{N}_{\geq p}).$$

(iv) *If* P *is a semi-CNS polynomial and* $f \in \mathbb{N}[X] \setminus \{0\}$ *we have*

$$\mathrm{L}_P\,(f) \leq \ell + \deg(f) + \Big(\left\lfloor \frac{H(f)}{p} \right\rfloor + \deg(f) \Big) K_P$$

where $H(f)$ *denotes the (naive) height of* f.

(v) *Let* $n \in \mathbb{N}_{>0}$, $r \in \mathcal{D}$ *and* $-kp \in R_P$ *for* $k = 1, \ldots, n$. *Then we have*

$$\mathrm{L}_P\,(-np + r) \leq \overline{\ell} + (n-1)K_P$$

with $\overline{\ell} = \mathrm{L}_P\,(-p)$.

(vi) *Let* $n \in \mathbb{N}_{\geq p}$ *and* $-\left\lceil \frac{n}{p} \right\rceil p \in R_P$. *Then* $-n \in R_P$ *and we have*

$$\mathrm{L}_P\,(-n) \leq \overline{\ell} + \Big(\left\lceil \frac{n}{p} \right\rceil - 1 \Big) K_P\,.$$

(vii) *If* $\mathbb{Z} \subseteq R_P$ *we have*

$$\mathrm{L}_P\,(n) \leq \ell^\star + \left\lfloor \frac{|n|}{p} \right\rfloor K_P \qquad (n \in \mathbb{Z})$$

with $\ell^\star = \max\left\{\ell, \overline{\ell}\right\}$.

(viii) *If* P *is a CNS polynomial and* $f \in \mathbb{Z}[X] \setminus \{0\}$ *we have*

$$\mathrm{L}_P\,(f) \leq \ell^\star + \deg(f) + \Big(\left\lfloor \frac{H(f)}{p} \right\rfloor + \deg(f) \Big) K_P\,.$$

Proof. For simplicity we now omit the subscript P. (i) In view of $\mathcal{D} \subseteq R$ and Theorem 12 (ii) we have $\ell \leq \max\{\mathrm{L}(p-1), \mathrm{L}(1)\} + K = K$.

(ii) The statement is trivial for $n = 1$, and by induction we find

$$\mathrm{L}\,((n+1)p) \leq \max\{\mathrm{L}(np),\, \ell\} + K \leq \max\{\ell + (n-1)K,\, \ell\} + K = \ell + nK\,.$$

(iii) This is trivial for $n < p$. Otherwise we write $n = \left\lfloor \frac{n}{p} \right\rfloor p + r$ with $r \in \mathcal{D}$ and infer from (ii)

$$\mathrm{L}\,(n) = \mathrm{L}\left(\left\lfloor \frac{n}{p} \right\rfloor p \right) \leq \ell + \left\lfloor \frac{n}{p} \right\rfloor K\ .$$

(iv) We proceed by induction on $d := \deg(f)$. If $d = 0$ the statement is clear by (iii). Otherwise, we write $f = Xg + c$ with $c \in \mathbb{N},\ g \in \mathbb{N}[X],\ \deg(g) = d - 1,\ H(g) \leq H(f)$, hence with $q := \left\lfloor \frac{H(f)}{p} \right\rfloor$

$$\mathrm{L}\,(f) \leq \max\left\{1 + \mathrm{L}(g)),\, \mathrm{L}(c)\right\} + K$$

$$\leq 1 + \ell + \deg(g) + (q + \deg(g))K + K = \ell + d + (q + d)K\ .$$

Proofs of (v) through (viii) follow the same scheme and are left to the reader. □

The practical application of Theorem 12 for the determination of the constants K_P and L_P for an irreducible semi-CNS polynomial P requires the computation of sets of the form

$$\mathcal{G} = \left\{ \gamma \in \mathbb{Z}[\mu]\ :\ \overline{|\gamma|} < c \right\}\ .$$

It is well known that $\mathcal{G}$ can be computed in finitely many steps (see for instance [27, Chapter 3.3]). However, so far no bounds for the degrees of canonical representatives (if they exist) of the elements of $\mathcal{G}$ seem to be known.

References

[1] Akiyama, S. and Borbély, T. and Brunotte, H. and Pethő, A. and Thuswaldner, J. M., Generalized radix representations and dynamical systems. I, Acta Math. Hungar., Acta Mathematica Hungarica **108** (2005), 207–238.

[2] Akiyama, Shigeki and Borbély, Tibor and Brunotte, Horst and Pethő, Attila and Thuswaldner, Jörg M., Basic properties of shift radix systems, Acta Math. Acad. Paedagog. Nyházi. (N.S.) **22** (2006), 19–25 (electronic).

[3] Akiyama, Shigeki and Pethő, Attila, On canonical number systems., Theoret. Comput. Sci. **270** (2002), 921–933.

[4] Akiyama, Shigeki and Rao, Hui, New criteria for canonical number systems, Acta Arith. **111** (2004), 5–25.

[5] Akiyama, Shigeki and Scheicher, Klaus, Symmetric shift radix systems and finite expansions, Math. Pannon. **18** (2007), 101–124.

[6] Anderson, N. and Saff, E. B. and Varga, R. S., On the Eneström-Kakeya theorem and its sharpness, Linear Algebra Appl. **28** (1979), 5–16.

[7] Barat, Guy and Berthé, Valérie and Liardet, Pierre and Thuswaldner, Jörg, Dynamical directions in numeration, Numération, pavages, substitutions, Ann. Inst. Fourier (Grenoble) **56** (2006), 1987–2092.

[8] Brunotte, Horst, Characterization of CNS trinomials, Acta Sci. Math. (Szeged) **68** (2002), 673–679

[9] Brunotte, Horst, On some classes of polynomials with nonnegative coefficients and a given factor, to appear in Periodica Mathematica Hung.

[10] Brunotte, Horst, On the roots of expanding integer polynomials, to appear in Acta Math. Acad. Paedagog. Nyházi. (N.S.), (2011).

[11] Burcsi, Péter and Kovács, Attila, Exhaustive search methods for CNS polynomials, Monatsh. Math. **155** (2008), 421–430.

[12] Chen, Alex, On the reducible quintic complete base polynomials, J. Number Theory **129** (2009), 220–230.

[13] Frougny, Christiane and Solomyak, Boris, Finite beta-expansions, Ergodic Theory Dynam. Systems **12** (1992), 713–723.

[14] Gilbert, William J., Radix representations of quadratic fields, J. Math. Anal. Appl. **83**, (1981), 264–274.

[15] Grünwald, V., 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), Giornale di matematiche di Battaglini **23** (1885), 203-221, 367.

[16] Kane, Daniel M., Generalized base representations, J. Number Theory **120** (2006), 92–100.

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

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

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

[20] Knuth, Donald E., An imaginary number system, Comm. ACM **3** (1960), 245–247.

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

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

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

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

[25] Pethő, Attila, Connections between power integral bases and radix representations in algebraic number fields, Proceedings of the 2003 Nagoya Conference "Yokoi-Chowla Conjecture and Related Problems", 115–125, Saga Univ., Saga, 2004.

[26] Pethő, Attila and Varga, Peter, Characterization of semi-CNS polynomials, 8th Joint Conf. on Math. and Comp. Sci., Komárno, Slovakia, 2010.

[27] Pohst, M. and Zassenhaus, H., Algorithmic algebraic number theory, Encyclopedia of Mathematics and its Applications, 30, Revised reprint of the 1989 original, Cambridge University Press, Cambridge, 1997, xiv+499.

[28] Schmidt, Klaus, On periodic expansions of Pisot numbers and Salem numbers, Bull. London Math. Soc. **12** (1980), 269–278.

[29] Surer, Paul, ε-shift radix systems and radix representations with shifted digit sets, Publ. Math. Debrecen **74** (2009), 19–43.