Acta Mathematica Academiae Paedagogicae Nyíregyháziensis
28 (2012), 91–94
www.emis.de/journals
ISSN 1786-0091

CHARACTERIZATION OF SEMI-CNS POLYNOMIALS

HORST BRUNOTTE

Abstract. Semi-CNS polynomials are monic polynomials with integer coefficients which are related to natural generalizations of the classical decimal representation of the rational integers to algebraic integers. We characterize semi-CNS polynomials of arbitrary degrees thereby extending known results on cubic and irreducible semi-CNS polynomials.

1. Introduction

Canonical number systems (abbreviated by CNS) can be seem as natural generalizations of the classical decimal representation of the rational integers to algebraic integers. The main ingredient of a canonical number system is a so-called CNS polynomial (see Definition 1 below) which was introduced by A. Pethő [11][1]. The characterization of this class of polynomials has remained an open problem until now, however, there is an algorithm to decide the CNS property of a given polynomial [17, 8]. The work [4] provides a detailed account on the historical development and the connections of the concept of canonical number systems to other theories, e.g. shift radix systems, finite automata or fractal tilings.

During the recent decades various generalizations of the concept of a CNS polynomial have been studied (see for instance [9], [14], [2], [16], [13]). Here we are concerned with one of them, namely with semi-CNS polynomials which were defined by P. Burcsi and A. Kovács [7]. W. Steiner [15] pointed out that this notion is intimately connected with positive finiteness as introduced by S. Akiyama and that an easy adaption of [1] to reducible polynomials shows that [7, Theorem 3.4] in fact describes all semi-CNS polynomials with negative constant terms; in particular, there are exactly $\binom{d+k-3}{k-2}$ semi-CNS polynomials of degree d and constant term $-k \quad (k \geq 2)$.

In this short note we give the details of the aforementioned adaption of the proof of S. Akiyama [1]. Thereby we extend the characterization of

2010 *Mathematics Subject Classification.* 11A63,11R04,11R21,12D99.
Key words and phrases. canonical number system, CNS polynomial, positive finiteness.
[1]CNS polynomials are named complete base polynomials in [8].

cubic semi-CNS polynomials given by A. Pethő and P. Varga [12] and the characterization of irreducible semi-CNS polynomials [5, Theorem 11].

2. Characterizations of semi-CNS polynomials

Throughout this section we let $P \in \mathbb{Z}[X]$ be a monic integer polynomial of positive degree with $P(0) \neq 0$ and $\mathcal{D}_P = [0, |P(0)| - 1] \cap \mathbb{N}$ 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 (w.r.t. P) if

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

with some polynomial $B \in \mathcal{D}_P[X]$. In this case we say that B canonically represents A. We denote by R_P the set of all canonically representable integer polynomials. It is easy to see that each $A \in R_P$ which is not a multiple of P has a unique representative $B \in \mathcal{D}_P[X]$.

We now give the definitions of (semi-) CNS polynomials in a slightly modified form.

Definition 1. (1) P is called a CNS polynomial if $\mathbb{Z}[X] \subseteq R_P$ ([10]).
(2) P is called a semi-CNS polynomial if R_P is an additive semigroup ([7, Definition 3.2]).

Our main result is the characterization of semi-CNS polynomials thereby extending results of A. Pethő and P. Varga [12] for cubic polynomials and [5, Theorem 11] for irreducible polynomials. The ingredients of our proof are the works of P. Burcsi and A. Kovács [7] and in particular of S. Akiyama [1] where the essence of our Theorem 5 is shown, but formulated in a different terminology. The reader is referred to [5, Theorem 11 (ii)] and to [1, Section 3] for details.

We start with some preparations.

Lemma 2. *If $E \in \mathcal{D}_P[X]$ canonically represents $m \in \mathbb{Z}$ then*

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

Proof. Let $T \in \mathbb{Z}[X]$ with $PT = E - m$. Then $P(0)T(0) = E(0) - m$. □

Only one implication of the second statement of the following lemma is needed for our main result, however, the other statements are mentioned here for the sake of completeness.

Lemma 3. *Let $|P(0)| \geq 2$. Then the following statements hold.*
(1) *If P is a semi-CNS polynomial and f a nonconstant factor of P with $|P(0)| \geq 2$ then f is expanding, i.e., all roots of f lie outside the closed unit disc.*
(2) *P is a semi-CNS polynomial if and only if $\mathbb{N}[X] \subseteq R_P$.*

(3) *P is a CNS polynomial if and only if P is a semi-CNS polynomial and $-1 \in R_P$.*

Proof. (i), (ii) Clear by [5, Theorem 11 (i)].
(iii) See [5, Theorem 11 (iii)]. Note that $-1 \in R_P$ implies that P does not have a real nonnegative root, hence $P(0) > 1$. □

Further we recall the following well-known (and easy to prove (see e.g., [3, Lemma 1])) fact.

Lemma 4. *Let $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{C}[X]$ be a nonconstant polynomial with $|a_0| > \sum_{i=1}^{n} |a_i|$. Then f is expanding.*

Let us now state our main result.

Theorem 5. *Let $P \in \mathbb{Z}[X]$ be a monic integer polynomial with $|P(0)| \geq 2$. Then P is a semi-CNS polynomial if and only if one of the following two conditions holds.*

(1) *P is a CNS polynomial.*
(2) *$P(1) < 0$, and apart from the constant term all coefficients of P are nonnegative.*

Proof. We first show that semi-CNS polynomials can be characterized by either of the two conditions stated above. Trivially, every CNS polynomial is a semi-CNS polynomial. Now, let $P = \sum_{i=0}^{d} p_i X^i$ with $P(1) < 0$ and $p_1, \dots, p_{d-1} \geq 0$. Then $p_0 < 0$, and P is expanding by Lemma 4. Now we infer from [7, Theorem 3.4] that P is a semi-CNS polynomial.

Conversely, let P be a semi-CNS polynomial. If $P(0) > 0$ then P is a CNS polynomial by [6, Section 3.4.2]. Let $P(0) < 0$, hence P has a real positive root r. In view of Lemma 3 (ii) we find $E \in \mathcal{D}_P[X]$ with

$$E \equiv -p_0 \pmod{P},$$

and we can write

$$E = \sum_{i=1}^{n} e_i X^i$$

by Lemma 2. Pick $T \in \mathbb{Z}[X]$ with $PT = E + p_0 =: Q$, thus $Q(r) = 0$. As the sequence of coefficients of Q admits exactly one variation in sign Q has exactly one positive root by Descartes' rule of signs, and this root is r. We know from [5, Theorem 11 (i)] that $r > 1$, therefore

$$Q(1) < 0\,. \tag{1}$$

Trivially $T(0) = 1$. If T were nonconstant then Q would have a root inside the closed unit disk which in view of (1) contradicts Lemma 4. Hence, $T = 1$ and therefore $P = Q$. The proof is complete. □

References

[1] S. Akiyama. Positive finiteness of number systems. In *Number theory*, volume 15 of *Dev. Math.*, pages 1–10. Springer, New York, 2006.

[2] S. Akiyama, C. Frougny, and J. Sakarovitch. Powers of rationals modulo 1 and rational base number systems. *Israel J. Math.*, 168:53–91, 2008.

[3] S. Akiyama and A. Pethő. On canonical number systems. *Theoret. Comput. Sci.*, 270(1-2):921–933, 2002.

[4] 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.

[5] H. Brunotte. On the roots of expanding integer polynomials. *Acta Math. Acad. Paedagog. Nyházi. (N.S.)*, 27(2):161–171, 2011.

[6] P. Burcsi. Algorithmic aspects of generalized number systems. PhD Thesis, 2008.

[7] P. Burcsi and A. Kovács. Exhaustive search methods for CNS polynomials. *Monatsh. Math.*, 155(3-4):421–430, 2008.

[8] A. Chen. On the reducible quintic complete base polynomials. *J. Number Theory*, 129(1):220–230, 2009.

[9] B. Kovács. CNS rings. In *Topics in classical number theory, Vol. I, II (Budapest, 1981)*, volume 34 of *Colloq. Math. Soc. János Bolyai*, pages 961–971. North-Holland, Amsterdam, 1984.

[10] A. Pethö. 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.

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

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

[13] K. Scheicher, P. Surer, J. M. Thuswaldner, and C. van de Woestijne. Digits systems in commutative rings. to appear.

[14] K. Scheicher and J. M. Thuswaldner. Digit systems in polynomial rings over finite fields. *Finite Fields Appl.*, 9(3):322–333, 2003.

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

[16] P. Surer. ε-shift radix systems and radix representations with shifted digit sets. *Publ. Math. Debrecen*, 74(1-2):19–43, 2009.

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

Received November 2, 2011.

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