Acta Mathematica Academiae Paedagogicae Nyíregyháziensis
33 (2017), 15–21
www.emis.de/journals
ISSN 1786-0091

SOME COMMENTS ON FACTORS OF CNS POLYNOMIALS

HORST BRUNOTTE

Abstract. It is proved that certain monic integer Hurwitz polynomials are factors of CNS polynomial.

1. Introduction

A monic integer polynomial f is a CNS polynomial if for every $p \in \mathbb{Z}[X]$ there exists a polynomial $q \in \{0, \ldots, |f(0)| - 1\} [X]$ such that $p \equiv q \pmod f$. The concept of a CNS polynomial[1]) and the general notion of a canonical number system (CNS) were introduced by Pethő [19] and extended in the sequel (see for example [2, 5, 22]). Detailed background information on the historical development and relations of CNS polynomials to other areas such as shift radix systems, finite automata or fractal tilings can be found in the survey by Kirschenhofer and Thuswaldner [15] and the literature cited there.

The CNS property of a given polynomial can be decided algorithmically [6, 10, 23], and it is known that CNS polynomials are expansive and do not have positive real roots ([1, Theorem 2.1] or [13, Section 2]). Some characterization results on these polynomials are known (for instance, see [11, 14] for quadratic polynomials, [3, 4, 7, 16] for some other classes of polynomials and [13, 17] for more general results). However, the complete description of these polynomials has remained an open problem even for small degrees.

The set $\mathcal{C}$ of CNS polynomials seems to have poor algebraic properties: For instance, $\mathcal{C}$ is not closed under multiplication (e.g., $(X + 2)^2 \in \mathcal{C}$, but $(X+2)^4 \notin \mathcal{C}$), and there exist CNS polynomials none of whose factors belongs to $\mathcal{C}$ (see [9, Example 13]). On the other hand, it is known that the product of up to five pairwise different linear CNS polynomials is a CNS polynomial; this was proved independently in [20, Theorem 5] and [13, Theorem 10] for at most four factors and in [10, Theorem 8] for five factors. Moreover, in [13,

2010 *Mathematics Subject Classification.* 12D99,11A63.
Key words and phrases. Canonical number system, radix representation.
[1]CNS polynomials are named complete base polynomials in [10].

Section 5] an example of a non-CNS polynomial is given which is the product of nine linear CNS polynomials with strictly increasing constant terms.

Some years ago, Pethő [18] put forward the following interesting question: If $f \in \mathbb{Z}[X]$ is a monic polynomial all of whose roots lie outside the closed unit disk and are non-positive is it true that f is a factor of a CNS polynomial? To the best knowledge of the author, the answer to this question is still open, but it is affirmative if f has at most one pair of complex conjugate roots [9, Theorem 12]. The aim of this note is to prove that every monic integer expansive Hurwitz polynomial is a factor of a CNS polynomial.

2. Expansive integer Hurwitz polynomials as factors of CNS polynomials

Recall that a Hurwitz polynomial is a non-constant real polynomial all of whose roots have a negative real part. We show that every monic expansive integer Hurwitz polynomial is a factor of a CNS polynomial. In other words, for certain Hurwitz polynomials we give an affirmative answer to the above mentioned question raised by Pethő. To achieve this aim for such a polynomial f we show the existence of a multiple of f which satisfies a sufficient condition for a CNS polynomial.

Let us start with several auxiliary results and fix some notation. Here our main interest lies in the set $\mathcal{E}$ of real monic expansive polynomials of positive degree which do not have a real positive root.

Let $f \in \mathcal{E}$. We observe that $f(0) > 1$ and denote by $\mathrm{Z}(f)$ the multiset of zeros of f. Further, we let

$$\mathrm{Z}_-(f) := \mathrm{Z}(f) \cap \mathbb{R} \text{ and } \mathrm{Z}_\mathrm{c}(f) := \{\alpha \in \mathrm{Z}(f) \ : \ \Im\alpha > 0\}.$$

Thus we have the factorization

$$f = \prod_{\alpha \in \mathrm{Z}_-(f) \cup \mathrm{Z}_\mathrm{c}(f)} f_\alpha$$

with

$$f_\alpha := \begin{cases} X - \alpha & (\alpha \in \mathrm{Z}_-(f)), \\ (X-\alpha)(X-\bar{\alpha}) & (\alpha \in \mathrm{Z}_\mathrm{c}(f)). \end{cases}$$

As usual, we denote by $\mathbb{N}$ the set of positive rational integers.

Lemma 2.1. *If $\sigma \in \mathbb{R}_{>0}$ then there exists $N \in \mathbb{N}$ such that for all $n \geq N$ we have*

(1) $\sigma \left|\alpha\right|^n > 1$, *if* $\alpha \in \mathrm{Z}_-(f))$,
(2) $\left(\sigma \left|\alpha\right|^{2n} - 1\right)/\left(2\left|\alpha\right|^n\right) > 1$, *if* $\alpha \in \mathrm{Z}_\mathrm{c}(f))$.

Proof. Since $|\alpha| > 1$ for every $\alpha \in \mathrm{Z}(f)$, the existence of N with property (i) is trivial. Now, the proof can be concluded by Lemma 2.2 below. □

Lemma 2.2. *Let $a, b, \rho \in \mathbb{R}_{>0}$ such that $a, b > 1$. Then there exists $N \in \mathbb{N}$ such that*

$$\frac{\rho a^{2n} - 1}{2a^n} \geq b$$

for all $n \geq N$.

Proof. This is a straightforward exercise in calculus and left to the reader. □

For convenience, given $\rho \in \mathbb{R}_{>0}$ we abbreviate by $\mathrm{N}_\rho(f)$ the minimal integer which satisfies the properties of Lemma 2.1 for

$$\sigma := (1+\rho)^{1/(r+s)} - 1, \tag{1}$$

where we set $r := \operatorname{Card} \mathrm{Z}_-(f)$ and $s := \operatorname{Card} \mathrm{Z}_\mathrm{c}(f)$. Our next statements suggest that it is easy to find a multiple of f with small coefficients compared to $f(0)$, but that it might be not so easy to construct such a multiple with nonnegative coefficients. To this end, we put

$$G_n(f) := \prod_{\alpha \in \mathrm{Z}(f)} \Big(X^n - \alpha^n \Big) \quad (n \in \mathbb{N}).$$

Finally, we denote by $\mathrm{L}(f)$ the length of f, i.e., the sum of the absolute values of the coefficients of f, and we let

$$\mathcal{D}_\rho := \{ f \in \mathbb{R}[X] \ : \ f \text{ monic and } \mathrm{L}(f) < (1+\rho)\, |f(0)| \} .$$

Lemma 2.3. *For $\rho \in \mathbb{R}_{>0}$ and $n \geq \mathrm{N}_\rho(f)$ the following statements hold.*

(1) $G_n(f) \in \mathcal{D}_\rho$.
(2) *If $\Re(\alpha^n) \leq 0$ for all $\alpha \in \mathrm{Z}_\mathrm{c}(f)$, then $\prod_{\alpha \in \mathrm{Z}_\mathrm{c}(f)} G_n(f_\alpha) \in \mathbb{R}_{\geq 0}[X]$.*

Proof. (i) Define σ as in (1). For $\alpha \in \mathrm{Z}_-(f)$ Lemma 2.1 yields

$$\mathrm{L}(G_n(f_\alpha)) = 1 + |\alpha|^n < (1+\sigma)\, |\alpha|^n = (1+\sigma)\, |G_n(f_\alpha)(0)| ,$$

and analogously for $\alpha \in \mathrm{Z}_\mathrm{c}(f)$:

$$\mathrm{L}(G_n(f_\alpha)) \leq 1 + 2\,|\alpha|^n + |\alpha|^{2n} < 1 + \sigma\, |\alpha|^{2n} - 1 + |\alpha|^{2n} = (1+\sigma)\, |G_n(f_\alpha)(0)| \ .$$

Using [9, Lemma 2 and Lemma 3] we conclude

$$\begin{aligned} \mathrm{L}(G_n(f)) &\leq \prod_{\alpha \in \mathrm{Z}_-(f) \cup \mathrm{Z}_\mathrm{c}(f)} \mathrm{L}(G_n(f_\alpha)) \\ &< (1+\sigma)^r \big(\prod_{\alpha \in \mathrm{Z}_-(f)} |G_n(f_\alpha)(0)| \big) (1+\sigma)^s \big(\prod_{\alpha \in \mathrm{Z}_\mathrm{c}(f)} |G_n(f_\alpha)(0)| \big) \\ &= (1+\sigma)^{r+s} \prod_{\alpha \in \mathrm{Z}_-(f) \cup \mathrm{Z}_\mathrm{c}(f)} |G_n(f_\alpha)(0)| \\ &= (1+\rho)\, |G_n(f(0))| . \end{aligned}$$

(ii) This is clear by the definitions. □

In the following we need the set $\mathcal{A} := \mathcal{E} \cap \mathbb{Z}[X]$ of integer polynomials in $\mathcal{E}$. Certainly, we know that $\mathcal{C}$ is contained in $\mathcal{A}$.

Remark 2.4. Note that for every positive ρ and every $d \geq 2$ there is a polynomial $f \in \mathcal{A} \setminus \mathcal{C}$ of degree d such that $\mathrm{L}(f) < (1+\rho)f(0)$. Indeed, pick an integer $c > \max\{3,\, 3/\rho\}$ and put $f := X^d - 2X + c$. Then f does not have a root inside the closed unit disk because otherwise $f(z) = 0$ and $|z| \leq 1$ imply the contradiction

$$|z|^d \geq c - 2\,|z| > 1.$$

Further, we immediately check that f does not have a real positive root. Thus $f \in \mathcal{A}$, and by [3, Lemma 2] or [7, Theorem 3] the polynomial f is not a CNS polynomial. Clearly, we have

$$\mathrm{L}(f) = 1 + 2 + c < (1+\rho)c = (1+\rho)\, f(0)\,.$$

An application of Dirichlet's approximation theorem yields a real multiple of f with relatively small nonnegative coefficients.

Lemma 2.5. *Let f be a monic Hurwitz polynomial, $\rho \in \mathbb{R}_{>0}$ and $N \in \mathbb{N}$. Then there exists an $n > N$ such that $G_n(f) \in \mathcal{D}_\rho \cap \mathbb{R}_{\geq 0}[X]$.*

Proof. By [21, Lemma 3] there exists some $n > \max\{N, \mathrm{N}_\rho(f)\}$ such that for all $\alpha \in \mathrm{Z}(f)$ we have

$$\Re(\alpha^n) \leq \frac{1}{2}\,|\alpha|^{n-1}\,\Re\alpha < 0,$$

thus

$$G_n(f_\alpha) \in \mathbb{R}_{\geq 0}[X],$$

and therefore by Lemma 2.3

$$G_n(f) \in \mathcal{D}_\rho \cap \mathbb{R}_{\geq 0}[X]. \qquad \square$$

By [9, Theorem 12] we know that $f \in \mathcal{A}$ is a factor of a CNS polynomial provided that every integer factor of f has at most one pair of complex conjugate roots. Now we are in a position to extend this statement.

Theorem 2.6. *Let $f_1, \ldots, f_m \in \mathcal{A}$ and assume that for each $i = 1\ldots, m$ one of the following two statements holds:*

(1) *f_i has at most one pair of complex conjugate roots,*
(2) *f_i is a Hurwitz polynomial.*

Then the product $f_1 \cdots f_m$ is a factor of a CNS polynomial.

Proof. Let

$$\sigma := 2^{1/m} - 1$$

and $i \in \{1, \ldots, m\}$.

First, let f_i have at most one pair of complex conjugate roots. Then we infer from [9, Theorem 9 and Lemma 3] that there is some $n_i \in \mathbb{N}$ such that

$$G_{n_i}(f_i) \in \mathcal{D}_\sigma \cap \mathbb{R}_{\geq 0}[X]\,. \tag{2}$$

Second, let f_i be a Hurwitz polynomial. Then Lemma 2.5 yields some $n_i \in \mathbb{N}$ such that (2) holds.

Now, setting

$$g_i := G_{n_i}(f_i)/f_i \in \mathbb{Z}[X] \qquad (i = 1, \ldots, m)$$

and using [9, Lemma 4] we deduce

$$(g_1 \cdots g_m)(f_1 \cdots f_m) = G_{n_1}(f_1) \cdots G_{n_m}(f_m) \in \mathcal{D}_1 \cap (\mathbb{N} \cup \{0\})[X]\,.$$

By [4, Theorem 3.2] or [13, Theorem 11] we know that every monic polynomial in $\mathcal{D}_1$ with nonnegative integer coefficients is a CNS polynomial. □

Let us briefly comment on the prerequisites and the method of proof of our theorem.

(1) Certainly, a polynomial in $\mathcal{A}$ which does not satisfy the prerequisites of our theorem may be a factor of a CNS polynomials. For instance, the irreducible polynomial

$$X^4 - X^3 + 31X^2 + 99X + 121 \in \mathcal{A}$$

has two pairs of complex conjugate roots and is not a Hurwitz polynomial, but it is a factor of a CNS polynomial of degree 5 (see [9, Example 13]).

(2) Observe that the proof of Lemma 2.5 is not constructive. Therefore, our method does not allow to exhibit a bound for the degree of the CNS polynomial involved in Theorem 2.6.

Speculating on further progress in the vein of our result above we formulate the following conjecture; obviously, it would be implied by an affirmative answer to the above mentioned question of Pethő.

Conjecture 2.7. The set $\{f \in \mathcal{A} : f \text{ factor of a CNS polynomial}\}$ is multiplicatively closed.

Remark 2.8. For an affirmative answer to Pethő's question and for a proof of the conjecture above it suffices to consider polynomials with only positive coefficients. Indeed, let $f \in \mathcal{A}$. By Handelman's theorem on real polynomials without positive real roots [12, Theorem A] there is some $n \in \mathbb{N}$ such that

$$g := (X+2)^n \cdot f \in \mathcal{A} \cap \mathbb{N}[X];$$

for the sake of completeness we mention that by [8, Lemma 3] n can be bounded by an effectively computable constant depending on f. Trivially, if g divides some CNS polynomial, then so does f.

References

[1] S. Akiyama, T. Borbély, H. Brunotte, A. Pethő, and J. M. Thuswaldner. On a generalization of the radix representation—a survey. In *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, volume 41 of *Fields Inst. Commun.*, pages 19–27. Amer. Math. Soc., Providence, RI, 2004.

[2] 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.

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

[4] S. Akiyama and H. Rao. New criteria for canonical number systems. *Acta Arith.*, 111(1):5–25, 2004.

[5] S. Akiyama and K. Scheicher. Symmetric shift radix systems and finite expansions. *Math. Pannon.*, 18(1):101–124, 2007.

[6] T. Borbély. Általánosított számrendszerek. Master thesis, University of Debrecen, 2003.

[7] H. Brunotte. Characterization of CNS trinomials. *Acta Sci. Math. (Szeged)*, 68(3-4):673–679, 2002.

[8] H. Brunotte. On real polynomials without nonnegative roots. *Acta Math. Acad. Paedagog. Nyházi. (N.S.)*, 26(1):31–34, 2010.

[9] H. Brunotte. On expanding real polynomials with a given factor. *Publ. Math. Debrecen*, 83(1-2):161–178, 2013.

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

[11] W. J. Gilbert. Radix representations of quadratic fields. *J. Math. Anal. Appl.*, 83(1):264–274, 1981.

[12] D. Handelman. Positive polynomials and product type actions of compact groups. *Mem. Amer. Math. Soc.*, 54(320):xi+79, 1985.

[13] D. M. Kane. Generalized base representations. *J. Number Theory*, 120(1):92–100, 2006.

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

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

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

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

[18] A. Pethő. Private communication.

[19] 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 Univ., Saga, 2004.

[20] A. Pethő. Notes on CNS polynomials and integral interpolation. In *More sets, graphs and numbers*, volume 15 of *Bolyai Soc. Math. Stud.*, pages 301–315. Springer, Berlin, 2006.

[21] A. Schinzel. A class of algebraic numbers. *Tatra Mt. Math. Publ.*, 11:35–42, 1997. Number theory (Liptovský Ján, 1995).

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

[23] A. Tátrai. Parallel implementations of brunotte's algorithm. *J. Parallel Distrib. Comput.*, 71:565–572, 2011.

Received July 8, 2015.

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