Publ. Math. Debrecen
83/1-2 (2013), 161–178
DOI: 10.5486/PMD.2013.5568

On expanding real polynomials with a given factor

By HORST BRUNOTTE (Düsseldorf)

Abstract. Let f be a monic polynomial with real coefficients all of whose roots lie outside the closed unit disk and are non-positive. It is proved that f is a factor of a polynomial all of whose coefficients are non-negative and satisfy a rather strong boundedness condition. This result is applied to polynomials f with integer coefficients. It is shown that f is a factor of a so-called CNS polynomial provided f has at most one pair of complex-conjugate roots.

1. Introduction

Let f be a monic polynomial with real coefficients such that no root of f is non-negative. E. Meissner [23] and A. Durand [9, Théorème 2] showed that f is a factor of a polynomial F with only non-negative coefficients. Moreover, such a polynomial F of minimal degree can effectively be computed [12].

Here we further restrict to polynomials f all of whose roots lie outside the closed unit disk. In the first part of this note we show that there exists a real polynomial g such that the coefficients of the product fg are all non-negative and satisfy a rather strong boundedness condition (see Theorem 9). However, our proof of the existence of the polynomial g is nonconstructive because we use uniform distribution of irrationals modulo one.

In the second part we apply this result to polynomials f with integer coefficients and give a condition which guarantees that f is a factor of a so-called CNS polynomial. Let us briefly explain this notion. CNS polynomials[1] were introduced by A. Pethő [25] and are defined as follows. The monic nonconstant polynomial

Mathematics Subject Classification: 11C08, 11B83, 12E05, 11R04.
Key words and phrases: real polynomials, expanding polynomials, CNS polynomials.
[1]CNS polynomials are named complete base polynomials in [13].

$f \in \mathbb{Z}[X]$ with non-vanishing constant term is called a CNS polynomial if for all $A \in \mathbb{Z}[X]$ there exists a $B \in \{0, \ldots, |f(0)| - 1\}[X]$ such that $A \equiv B \pmod{f}$. Among other things it is known that the roots of CNS polynomials lie outside the closed unit disk and are non-positive. Moreover, there is an algorithm to decide the CNS property of a given polynomial [29], [8], [13]. On the other hand, the characterization of CNS polynomials has remained an open problem. G. Barat et al. [7] provided 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.

Recently, A. Pethő [26] put forward the following 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? Here we show that the answer to this question is affirmative if f has at most one pair of complex-conjugate roots (see Theorem 12). Furthermore, we associate to f a non-negative quantity $\gamma(f)$ which might be interpreted as a distance from f to the class of CNS polynomials. We discuss several examples and show that for f without complex roots a CNS polynomial which admits f as a factor can effectively be computed (see Theorem 14). For a quadratic polynomial f we construct an upper bound for $\gamma(f)$; an analogous bound for cubic f will be reported elsewhere. Finally, we list some properties of the quantity $\gamma(f)$.

2. Real polynomials with expanding roots and a given factor

Let us fix some notation. For $f \in \mathbb{R}[X]$ we denote by Ω_f the multiset of roots of f and by $L(f)$ the length of f, i.e., the sum of the absolute values of the coefficients of f. Our main interest lies in the set $\mathcal{E}$ of real monic polynomials f of positive degree such that every root α of f is expanding, i.e., all conjugates of α (including α itself) lie outside the closed unit circle (this notion was coined in [4, Introduction]).

The main tool of our approach are polynomials of the form (1) below. We prepare their application by a series of simple observations. The statements of the first lemma follow directly from the definitions.

Lemma 1. (i) *$\mathcal{E}$ is closed under multiplication.*

(ii) *If $f \in \mathcal{E}$ and $g \in \mathbb{R}[X]$ is a nonconstant monic divisor of f then $g \in \mathcal{E}$.*

We will make use of the following property of the length function (see [22]).

Lemma 2. *For $f, g \in \mathbb{R}[X]$ we have*

$$L(fg) \le L(f)L(g).$$

A central role in our consideration is played by the polynomials

$$G_n(f) = \prod_{\alpha \in \Omega_f} \left(X^n - \alpha^n\right) \qquad (n \in \mathbb{N}) \tag{1}$$

whose properties are collected now.

Lemma 3. *Let $f \in \mathbb{R}[X]$ be monic and $n \in \mathbb{N}_{>0}$.*

(i) *The polynomial $G_n(f)$ has real coefficients, f divides $G_n(f)$, and we have*

$$\deg(G_n(f)) = n \deg(f) \quad \text{and} \quad G_n(f)(0) = f(0)^n.$$

Moreover, if $f \in \mathbb{Z}[X]$ then both $G_n(f)$ and $G_n(f)/f$ have integer coefficients.

(ii) *If $g \in \mathbb{R}[X]$ is monic then*

$$G_n(fg) = G_n(f)G_n(g).$$

(iii) *If $f \in \mathcal{E}$ then we have $G_n(f) \in \mathcal{E}$.*

Proof. (i) This is well known (cf. [4, proof of Lemma 8]).
(ii), (iii) Trivial. □

For $\rho \in \mathbb{R}_{>0}$ we let

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

and

$$\mathcal{D}_\rho^+ = \mathcal{D}_\rho \cap \mathbb{R}_{\ge 0}[X].$$

Plainly, we have $1 \in \mathcal{D}_\rho^+$.

Lemma 4. (i) *For $\sigma_1, \dots, \sigma_m \in \mathbb{R}_{>0}$ we have*

$$\mathcal{D}_{\sigma_1} \cdots \mathcal{D}_{\sigma_m} \subseteq \mathcal{D}_\rho$$

where we set

$$\rho = (1+\sigma_1)\cdots(1+\sigma_m) - 1.$$

(ii) *For $0 < \sigma \le \rho$ we have $\mathcal{D}_\sigma \subseteq \mathcal{D}_\rho$.*

PROOF. (i) Applying Lemma 2 to $f_i \in \mathcal{D}_{\sigma_i}$ we find

$$L(f_1 \cdots f_m) \le L(f_1) \cdots L(f_m) < (1+\sigma_1)\,|f_1(0)| \cdots (1+\sigma_m)\,|f_m(0)| \\ = (1+\rho)\,|(f_1 \cdots f_m)(0)|\,.$$

(ii) Obvious. □

Our goal is to find a multiple of $f \in \mathcal{E}$ with non-negative coefficients and bounded length. The main ingredients are Lemmas 5 and 8 below.

Lemma 5. *If $f \in \mathcal{E}$ and $\rho \in \mathbb{R}_{>0}$ then $G_n(f) \in \mathcal{D}_\rho$ for all $n \in \mathbb{N}$ such that*

$$n > -\frac{\log\bigl((1+\rho)^{1/\deg(f)} - 1\bigr)}{\log|\mu|}$$

where $\mu \in \mathbb{C}$ is a root of minimal modulus of f.

PROOF. For the sake of completeness we include a slightly adapted copy of [4, proof of Lemma 8]. Let $d = \deg(f)$, $\Omega_f = \{\alpha_1, \dots, \alpha_d\}$ and define

$$G := \sum_{i=0}^{d} g_i X^i := \prod_{i=1}^{d} \bigl(X - \alpha_i^n\bigr).$$

Then we have

$$\frac{1}{|g_0|} + \frac{|g_{d-1}|}{|g_0|} + \cdots + \frac{|g_1|}{|g_0|} + 1 \\ = 1 + \left|\sum_{1\le i\le d} \alpha_i^{-n}\right| + \left|\sum_{1\le i<j\le d} \alpha_i^{-n}\alpha_j^{-n}\right| + \cdots + \left|\prod_{1\le i\le d} \alpha_i^{-n}\right| \\ \le \prod_{1\le i\le d} \Bigl(1 + \bigl|\alpha_i^{-n}\bigr|\Bigr) \le \Bigl(1 + \bigl|\mu^{-n}\bigr|\Bigr)^d < 1 + \rho,$$

hence

$$L(G_n(f)) = L(G(X^n)) = L(G(X)) < (1+\rho)\,|g_0| \\ = (1+\rho)\,|G(0)| = (1+\rho)\,|G_n(f)(0)|$$

and therefore $G_n(f) \in \mathcal{D}_\rho$. □

We prepare the proof of Lemma 8 below and start with some auxiliary results. For $x \in \mathbb{R}$ we denote by $\|x\|$ the distance from x to the nearest integer.

Lemma 6. *Let $u, v, N \in \mathbb{N}$ and assume $(u, v) = 1$ and $v > 1$. Then there is some $n \geq N$ such that*

$$\left\| n \cdot \frac{u}{v} \right\| \geq c$$

where we set $c = 1/3$. Furthermore, if $v \neq 3$ we can choose $c = 2/5$.

Proof. First, let v be even. Choose an odd t with $t \geq 2N/v$ and set $n = (tv)/2$. Then $n \geq N$ and $tu = 2k + 1$ with some $k \in \mathbb{N}$. Therefore we have

$$n \cdot \frac{u}{v} = \frac{tuv}{2v} = \frac{2k+1}{2} = k + \frac{1}{2}$$

which implies

$$\left\| n \cdot \frac{u}{v} \right\| = \frac{1}{2} > c.$$

Second, let $v = 2w + 1$ be odd. By an obvious modification of [28, Lemma A.3] there exist $n \geq N$ and $z \in \mathbb{Z}$ such that

$$w = nu + zv.$$

We verify

$$n \cdot \frac{u}{v} = \frac{w - zv}{v} = \frac{w}{v} - z = \frac{v-1}{2v} - z = -z + \frac{1}{2} - \frac{1}{2v}$$

which implies

$$\left\| n \cdot \frac{u}{v} \right\| = \frac{1}{2} - \frac{1}{2v} \geq c. \qquad \square$$

Lemma 7. *Let $\theta \in (0, \pi)$ and $N \in \mathbb{N}$. Then there is some $n \geq N$ such that*

$$\left\| n \cdot \frac{\theta}{2\pi} \right\| \geq \begin{cases} 2/5, & \text{if } \theta < 2\pi/3, \\ 1/3, & \text{otherwise.} \end{cases}$$

Proof. If $\rho := \theta/(2\pi)$ is irrational then our assertion is a consequence of the uniform distribution modulo one of the sequence $(n\rho)_{n \in \mathbb{N}}$ (e.g., see [14, Theorem 1.59]). Otherwise, let $u, v \in \mathbb{N}_{>0}$ such that $(u, v) = 1$ and $\rho = u/v$. Clearly, $v > 1$ and we can apply Lemma 6. $\square$

Lemma 8. *Let $\theta \in (0, \pi)$ and $N \in \mathbb{N}$. Then there exists an odd $n \geq N$ such that $\cos(n\theta) \leq 0$.*

PROOF. We first let $\theta \leq \pi/2$. From Lemma 7 we infer the existence of $k, \ell \in \mathbb{N}$ such that $k \geq N+1$ and

$$\left(2\ell + \frac{4}{5}\right)\pi \leq k\theta \leq \left(2\ell + \frac{6}{5}\right)\pi. \tag{2}$$

If k is odd we are done because

$$2\ell\pi + \frac{\pi}{2} < k\theta < 2\ell\pi + \frac{3\pi}{2}.$$

Otherwise we distinguish several subcases.

Case 1. $(k-1)\theta \geq (2\ell + 1/2)\pi$

Set $n = k-1$ and observe $n\theta < (2\ell + 3/2)\pi$.

Case 2. $(k-1)\theta < (2\ell + 1/2)\pi$

As $(k-1)\theta > (2(\ell-1) + 1/2)\pi$ we are done if $(k-1)\theta \leq (2(\ell-1) + 3/2)\pi$. Otherwise, we take $n = k+1$ because then by (2) and our prerequisites

$$\left(2\ell + \frac{1}{2}\right)\pi < \left(2\ell + \frac{4}{5}\right)\pi \leq n\theta \leq \left(2\ell + \frac{1}{2} + 1\right)\pi = \left(2\ell + \frac{3}{2}\right)\pi.$$

Now, we let $\theta > \pi/2$ and pick an even L such that

$$\theta \leq \frac{L}{L+1} \cdot \pi.$$

Again using Lemma 7 we find $k, \ell \in \mathbb{N}$ such that

$$k \geq N + L + 2 \tag{3}$$

and

$$\left(2\ell + \frac{2}{3}\right)\pi \leq k\theta \leq \left(2\ell + \frac{4}{3}\right)\pi.$$

If k is odd we are done. Otherwise, we set

$$\theta_\nu = (k + L - (2\nu+1))\theta, \qquad b_\nu = \left(2\left(\ell + \frac{L}{2} - (\nu+1)\right) + \frac{1}{2}\right)\pi,$$

$$B_\nu = \left(2\left(\ell + \frac{L}{2} - (\nu+1)\right) + \frac{3}{2}\right)\pi \quad (\nu \in \mathbb{Z}).$$

Similarly as above, we deal with several subcases.

Case 1. $\theta_{-1} \geq b_{-1}$

Set $n = k + L + 1$ and observe

$$n\theta \le \left(2\ell + \frac{4}{3} + L\right)\pi < B_{-1}.$$

Case 2. $\theta_{-1} < b_{-1}$

Set $c = 2\ell + 2/3$ and assume $\nu \ge -1$ and $\theta_\nu < b_\nu$. Then we have

$$c(k + L - 2\nu - 1) = \frac{cB_\nu}{\theta} < \frac{cb_\nu}{\theta} \le k\left(2\ell + L - 2\nu - \frac{3}{2}\right),$$

hence

$$2\nu(k - c) < k\left(L + 2\ell - \frac{3}{2} - c\right) - c(L - 1) < k(L - 2) - c(L - 1)$$

which yields

$$2\nu < \frac{k(L-2) - c(L-1)}{k - c}. \tag{4}$$

Moreover we find

$$\theta_{\nu+1} = \theta_\nu - 2\theta < B_\nu - 2\theta = B_{\nu+1}.$$

Thus there is a maximal $\nu \in \mathbb{N}$ such that $\theta_\nu < b_\nu$, and we choose

$$n = k + L - \big(2(\nu + 1) + 1\big).$$

By this choice we have

$$b_{\nu+1} \le n\theta = \theta_{\nu+1} < B_{\nu+1}$$

and $n \ge N$ because

$$k > c \cdot \frac{L+1}{L+2},$$

hence

$$\frac{k(L-2) - c(L-1)}{k - c} < 2L$$

and finally

$$n > k + L - \frac{k(L-2) - c(L-1)}{k - c} - 3 > k - L - 3 \ge N - 1$$

by (4) and (3). □

It was shown by E. Meissner [23] and A. Durand (see [9, Théorème 2]) that every real polynomial f without non-negative roots is a factor of a polynomial F with only non-negative coefficients. We are now in a position to show that F can be chosen in $\mathcal{D}_\rho^+$ for a given positive ρ provided that every root of f is expanding. For convenience we denote by c_f the number of pairs of complex-conjugate roots of f. Further, we use the notation

$$\mathcal{E}_- = \{f \in \mathcal{E} : \Omega_f \cap \mathbb{R}_{>0} = \emptyset\},$$

i.e., we are dealing with the set of nonconstant monic real polynomials all of whose roots are expanding and non-positive.

Theorem 9. *Let $f \in \mathcal{E}_-$ and $\rho \in \mathbb{R}_{>0}$.*

(i) *If $c_f = 0$ then there exists $N \in \mathbb{N}$ such that for all odd $n \geq N$ we have $G_n(f) \in \mathcal{D}_\rho^+$.*

(ii) *Let $c_f = 1$ and $N \in \mathbb{N}$. Then there is an odd $n \geq N$ such that $G_n(f) \in \mathcal{D}_\rho^+$.*

(iii) *There exists a polynomial $g \in \mathcal{E}_- \cup \{1\}$ such that $gf \in \mathcal{D}_\rho^+$.*

Proof. (i) Lemma 5 yields $G_n(f) \in \mathcal{D}_\rho$. As n is odd $G_n(f)$ can be written as a product of polynomials with non-negative coefficients and our assertion follows.

(ii) We use induction on $\deg(f)$ and first let $\deg(f) = 2$, hence $f = (X - \alpha)(X - \bar{\alpha})$ with $\alpha \in \mathbb{C}$ and $\Im(\alpha) \neq 0$. We may assume $\alpha = |\alpha| \, \mathrm{e}^{\mathrm{i}\theta}$ with $0 < \theta < \pi$. Lemma 8 yields an odd

$$n \geq \max\left\{N, \ \frac{\log 3 - \log \rho}{\log |\alpha|}\right\}$$

such that $\cos(n\theta) \leq 0$. Then

$$G_n(f) = X^{2n} - 2\Re(\alpha^n)X^n + |\alpha|^{2n}$$

has non-negative coefficients, and by our choice of n we have

$$L(G_n(f)) < (1 + \rho)\,|\alpha|^{2n},$$

i.e., $G_n(f) \in \mathcal{D}_\rho^+$. Now, let $\deg(f) > 2$. Using Lemma 1 (ii) we write

$$f = qg \qquad (q, g \in \mathcal{E}_-, \ \deg(q) = 2, \ c_q = 1) \tag{5}$$

and pick a real σ with

$$0 < \sigma \leq \sqrt{1 + \rho} - 1. \tag{6}$$

Clearly, $c_g = 0$. By (i) there is some N such that for all odd $n \geq N$ we have

$G_n(g) \in \mathcal{D}_\sigma^+$, and by what we have just seen there is an odd $n \geq N$ such that $G_n(q) \in \mathcal{D}_\sigma^+$. By Lemma 3 (ii) and Lemma 4 (i) we find

$$G_n(f) = G_n(q)G_n(g) \in \mathcal{D}_\sigma^+\mathcal{D}_\sigma^+ \subseteq \mathcal{D}_\rho^+.$$

(iii) We proceed by induction on c_f and observe that the case $c_f < 2$ is settled by (i), (ii), Lemma 3 (i) and (iii) because the quotient $G_n(f)/f$ belongs to $\mathcal{E} \cap \mathbb{R}_{\geq 0}[X]$ and thus does not have a non-negative root. Therefore, let $c_f \geq 2$ now. Let us pick a σ with (6) and again factorize f as in (5), thus in particular $c_g < c_f$. By (ii) there is some n such that $G_n(q) \in \mathcal{D}_\sigma^+$, and by induction hypothesis we find $h \in \mathcal{E}_- \cup \{1\}$ such that $hg \in \mathcal{D}_\sigma^+$. In view of Lemma 3 (i) we deduce

$$h \cdot \frac{G_n(q)}{q} \cdot f = h \cdot \frac{G_n(q)}{q} \cdot q \cdot g = (hg)\, G_n(q) \in \mathcal{D}_\sigma^+\mathcal{D}_\sigma^+ \subseteq \mathcal{D}_\rho^+. \qquad \square$$

We point out that in general the product gf in Theorem 9 (iii) cannot be replaced by $G_n(f)$ for some positive n: For instance, let ζ be a primitive fifth root of unity and set $\alpha = (4+\sqrt{5})\zeta$ and $\beta = (4-\sqrt{5})\zeta^2$. The polynomial

$$f = (X-\alpha)(X-\bar{\alpha})(X-\beta)(X-\bar{\beta}) \tag{7}$$

belongs to $\mathcal{E}_-$, and we have $c_f = 2$ and

$$\Re(\alpha^n)\Re(\beta^n) < 0 \qquad (n \in \mathbb{N}_{>0}).$$

If we assume $G_n(f) \in \mathbb{R}_{\geq 0}[X]$ for some positive n then Lemma 10 below would imply

$$0.3 < \left(\frac{4-\sqrt{5}}{4+\sqrt{5}}\right)^n \cdot 0.81 \leq \frac{4-\sqrt{5}}{4+\sqrt{5}} \cdot 0.81$$

which is absurd.

Lemma 10. *Let $a, b, u, v \in \mathbb{R}$, $n \in \mathbb{N}_{>0}$. If*

$$a, b \geq 1, \quad uv \leq 0, \quad \text{and} \quad (X^{2n} - 2a^n u X^n + a^{2n})(X^{2n} - 2b^n v X^n + b^{2n}) \in \mathbb{R}_{\geq 0}[X]$$

then we have

$$\max\{u, v\} \leq \left(\frac{\min\{a, b\}}{\max\{a, b\}}\right)^n |\min\{u, v\}|.$$

PROOF. By our prerequisites we have

$$a^n u + b^n v \leq 0 \quad \text{and} \quad a^n v + b^n u \leq 0.$$

Without loss of generality we may assume $u \geq 0$, hence

$$\max\{u, v\} = u \quad \text{and} \quad \min\{u, v\} = v.$$

If $a \leq b$ we have

$$a^n |v| = -a^n v \geq b^n u,$$

hence

$$u \leq (a/b)^n |v|.$$

The case $a > b$ can be treated analogously. □

3. Application to polynomials with integer coefficients

We let $\mathcal{A}$ be the set of monic integer polynomials f of positive degree such that every root α of f satisfies the following conditions:

- α is expanding.
- If α is real then α is negative.

These properties were named analytical conditions in [1]. Using the notation of the previous section we can write

$$\mathcal{A} = \mathcal{E}_- \cap \mathbb{Z}[X].$$

We aim at giving conditions which guarantee that $f \in \mathcal{A}$ is a factor of a CNS polynomial. Some background on the class $\mathcal{C}$ of CNS polynomials is required in Example 13 below, and we refer the reader to [25], [1], [7].

Let us first collect some properties of $\mathcal{A}$. The last statement Proposition 11 (v) is not needed here, we just mention it for the sake of completeness.

Proposition 11. (i) *$\mathcal{C}$ is contained in $\mathcal{A}$.*

(ii) *$\mathcal{A}$ is multiplicatively closed.*

(iii) *If $g \in \mathbb{Z}[X]$ is a non-constant monic divisor of some $f \in \mathcal{A}$ then $g \in \mathcal{A}$.*

(iv) *Let $f \in \mathcal{A}$. Then $f(0) \geq 2$, $f(-1) \geq 1$ and $f(1) \geq 1$.*

(v) *If $f \in \mathcal{A}$ then every root of f is a positively algebraic integer.*[2]

[2]For the definition see [21, Section 2].

PROOF. (i) See for instance [1, Theorem 2.1].

(ii), (iii) Clear by the definitions.

(iv) Trivial.

(v) Clear by [15]. □

In order to decide the above mentioned question it actually is enough do deal with polynomials with only positive coefficients because we have the following result: For $f \in \mathcal{A}$ there exists a non-negative integer m bounded by an effectively computable constant such that $(X+2)^m f$ has only positive coefficients (for a proof see for instance [11, Lemma 2]). However, so far we cannot exploit this fact for our purposes here. Therefore we proceed differently and give the following partial answer to the question raised above.

Theorem 12. *Let $f_1, \dots, f_m \in \mathcal{A}$ and assume that each polynomial f_i has at most one pair of complex conjugate roots $(i = 1, \dots, m)$. Then the product $f_1 \cdots f_m$ is a factor of a CNS polynomial.*

PROOF. Let

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

and $i \in \{1, \dots, m\}$. As $c_{f_i} \le 1$ we infer from Theorem 9 and Lemma 3 (i), (iii) that there is some $n_i \in \mathbb{N}$ such that

$$G_{n_i}(f_i) \in \mathcal{D}_\sigma^+ \cap \mathcal{E}, \quad g_i := G_{n_i}(f_i)/f_i \in \mathbb{Z}[X].$$

All coefficients of $G_{n_i}(f_i)$ are non-negative, hence using Lemma 4 (i)

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

by [6, Theorem 3.2]) or [18]. □

We define a function $\gamma : \mathcal{A} \to \mathbb{N} \cup \{\infty\}$ by

$$\gamma(f) = \inf \{\deg(g) : g \in \mathbb{Z}[X],\ gf \in \mathcal{C}\}.$$

Thus $\gamma(f)$ might be interpreted as a distance from f to the set of CNS polynomials. Clearly, $f \in \mathcal{C}$ is equivalent to $\gamma(f) = 0$. A polynomial $g \in \mathbb{Z}[X]$ such that $gf \in \mathcal{C}$ and $\deg(g) = \gamma(f)$ is called a CNS multiplier of f.

Our examples show that in favorable cases the computation of $\gamma(f)$ or the determination of bounds for $\gamma(f)$ can be easy. We need the well known characterization of linear and quadratic CNS polynomials (for proofs see for instance [17], [2, Remark 4.5] and [19], [20], [16], [10], [30], [6], respectively):

$$X + c \in \mathcal{C} \iff c \ge 2$$

and

$$X^2 + bX + c \in \mathcal{C} \iff -1 \le b \le c \ge 2.$$

Example 13. (i) It is known [27], [24] that the cubic polynomials

$$f \in \{X^3 + 80X^2 + 117X + 89, X^3 + 97X^2 + 143X + 109,$$
$$X^3 + 173X^2 + 257X + 198, X^3 + 410X^2 + 611X + 473\}$$

have the property $f \in \mathcal{C}$, but $f+1 \notin \mathcal{C}$. Thus we expect that $\gamma(f+1)$ should be small. Indeed, in all four cases we see $\gamma(f+1) = 1$ because we easily check

$$(X + 4) \cdot (f + 1) \in \mathcal{C}.$$

(ii) Let $f = X^2 - 2X + 6$ and $g = X^3 + 2X^2 + 3$, thus $f \notin \mathcal{C}$ by the well known characterization of quadratic CNS polynomials and $g \notin \mathcal{C}$ by [10, Theorem 3]. Using an algorithm mentioned above we can check that the product

$$p := fg = X^5 + 2X^3 + 15X^2 - 6X + 18$$

is a CNS polynomial. We remark that $\gamma(f) = 1$ (e.g., by Proposition 16 below) and also $\gamma(g) = 1$ because the product

$$(X + 2) \cdot g = X^4 + 4X^3 + 4X^2 + 3X + 6$$

is a CNS polynomial as can be checked algorithmically.

We resume that f, g provide an example of non-CNS polynomials whose product is a CNS polynomial. Thereby we answer a question of Ch. van der Woestijne [31, Section 4]. It is easy to see that the degree of such a product must be at least five.

Moreover, as both f and g are irreducible we observe that p is a reducible CNS polynomial without a CNS factor of degree less than $\deg(p)$.

(iii) The roots of the polynomial $f = X^4 - X^3 + 31X^2 + 99X + 121$ given by (7) are the conjugates of $\alpha = (4 + \sqrt{5})\zeta$ and $\beta = (4 - \sqrt{5})\zeta^2$ where ζ is a primitive fifth root of unity. We easily check $f \notin \mathcal{C}$ because $(0, 0, 1, 0) \in \mathbb{Z}^4$ is periodic[3] (of period length 3), but

$$(X + 6) \cdot f = X^5 + 5X^4 + 25X^3 + 285X^2 + 715X + 726 \in \mathcal{C}$$

by Kovács' Theorem [3, Theorem 2.3]. Therefore we find $\gamma(f) = 1$.

[3]The reader is referred to [2] for the necessary background.

Now we show that for every monic integer polynomial f all of whose roots are real and less than -1 we can construct a CNS polynomial which admits f as a factor.

Theorem 14. *Let $f \in \mathcal{A}$ have degree d and assume that f has only real roots. Let n be an odd integer with*

$$n > -\frac{\log(2^{1/d} - 1)}{\log(-r)}$$

where r is a maximal root of f. Then we have

$$\gamma(f) \leq (n-1)d,$$

and we can effectively compute a polynomial $g \in \mathbb{Z}[X]$ such that gf is a CNS polynomial.

Proof. Using Lemma 5 we choose an odd integer n with

$$G_n(f) \in \mathcal{D}_1^+$$

and we set $g := G_n(f)/f$. Thus $gf \in \mathcal{C}$ by [6, Theorem 3.2]) or [18]. □

Let us take a closer look at quadratic polynomials. Firstly, we give the γ-values of some quadratic polynomials in $\mathcal{A}$. In view of the description of CNS polynomials of degree at most 2 we observe that in all cases dealt with in Proposition 15 multipliers can be found which are CNS polynomials themselves.

Proposition 15. *Let $f = X^2 + bX + c \in \mathcal{A}$.*

(i) *We have $c \geq 2$ and $-2\sqrt{c} < b \leq c$.*

(ii) *$\gamma(f) = 0$ if and only if $-1 \leq b \leq c$.*

(iii) *$\gamma(f) = 1$ if and only if $-\sqrt{c+1} \leq b \leq -2$. In this case $X - b$ is a CNS multiplier of f.*

(iv) *If $-\sqrt{2c+1} \leq b < -\sqrt{c+1}$ then $\gamma(f) = 2$ and $X^2 - bX + c$ is a CNS multiplier of f.*

(v) *If $b^2 \geq 4c$ then $b \geq 0$ and $\gamma(f) = 0$.*

Proof. (i) We have $c \geq 2$ by Proposition 17 and $|b| \leq c$ by [4, Lemma 11]. Inspecting the roots of f we check $b > -2\sqrt{c}$.

(ii) Clear by (i) and the characterization of quadratic CNS polynomials cited above.

(iii) Let $\gamma(f) = 1$ and $r \in \mathbb{Z}$ with

$$(X + r) \cdot f = X^3 + (r + b)X^2 + (c + br)X + cr \in \mathcal{C}.$$

Then $b \le -2$ by (ii), and [3, Theorem 3.1] yields $r \ge -b \ge 2$ and $c+br \ge b+r-1$, hence

$$b^2 - 1 = (-b - 1)(1 - b) \le (r - 1)(1 - b) \le c$$

and $b^2 \le c + 1$.

Conversely, let $b \ge -\sqrt{c+1}$. Then $\gamma(f) > 0$ by (i), and

$$(X - b) \cdot f = X^3 + (c - b^2)X - bc \in \mathcal{C}$$

by [3, Proposition 3.2].

(iv) Clearly, we have $\gamma(f) > 1$ by (ii) and (iii). Further, we find

$$(X^2 - bX + c) \cdot f = X^4 + (2c - b^2)X^2 + c^2 \in \mathcal{C}$$

by [10, Theorem 1].

(v) We have $b \ge 0$ by (i), and we finish the proof using (ii). □

Secondly, we establish effectively computable bounds for the γ-values of non-CNS quadratic polynomials with negative discriminants.

Proposition 16. *Let $f = X^2 - bX + c \in \mathcal{A} \setminus \mathcal{C}$ and assume $b^2 < 4c$.*

(i) *We have $2 \le b < 2\sqrt{c}$.*

(ii) *Let $b = 2$. If $c = 2$ then $\gamma(f) = 2$ and $X^2 + 2X + 2$ is a CNS multiplier of f. If $c \ge 3$ then $\gamma(f) = 1$ and $X + 2$ is a CNS multiplier of f.*

(iii) *Let $b \ge 3$ and $\theta \in (0, \pi/2)$ such that $\cos\theta = b/(2\sqrt{c}\,)$. Then*

$$\gamma(f) \le 2(2^n - 1)$$

where the integer n is determined by the inequalities

$$\frac{\pi}{2^{n+1}} \le \theta < \frac{\pi}{2^n}.$$

Proof. (i) Clear by Proposition 15 (i).

(ii) Clear by Proposition 15 (iii) and (iv).

(iii) With $\alpha := \sqrt{c}\,\mathrm{e}^{\mathrm{i}\theta}$ we easily check

$$\Re\big(\alpha^{2^n}\big) = c^{2^{n-1}} \cos(2^n\theta) \le 0$$

$$0 \le -2\,\Re\big(\alpha^{2^n}\big) \le |\alpha|^{2^{n+1}} = c^{2^n}.$$

Therefore

$$G_{2^n}(f) = X^{2^{n+1}} - 2\Re\big(\alpha^{2^n}\big)X^{2^n} + |\alpha|^{2^{n+1}} \in \mathcal{C}$$

by [10, Theorem 1], and we easily conclude the proof using Lemma 3 (i). □

We conclude by listing some simple properties of the function γ.

Proposition 17. *Let $f \in \mathcal{A}$.*

(i) *$\gamma(f) > 0$ if and only if there are polynomials $h \in \mathbb{Z}[X]$, $g \in \{0, 1, \ldots, f(0) - 1\}[X] \setminus \{0\}$ and a positive integer n such that $\deg(g) < n$ and $hf \equiv g \pmod{X^n - 1}$.*

(ii) *Let $0 < \gamma(f) < \infty$ and $g \in \mathbb{Z}[X]$ such that gf is a CNS polynomial. Then $g \in \mathcal{A}$, $\gamma(g) \le \deg(f)$ and*

$$g(1) \ge \frac{f(0)}{f(1)} \cdot g(0).$$

(iii) *Let $\gamma(f) < \infty$ and $g \in \mathbb{Z}[X]$ be a monic divisor of f of positive degree. Then $g \in \mathcal{A}$ and*

$$\gamma(g) \le \gamma(f) + \deg(f) - \deg(g).$$

(iv) *Let $f(1) = 1$. Then $\gamma(f) \ge 2$, and $f(0) \ge 3$ implies $\gamma(f) \ge 3$.*

(v) *For $g \in \mathcal{A}$ we have*

$$\gamma(fg) \ge \max\{\gamma(f) - \deg(g), \gamma(g) - \deg(f)\}.$$

(vi) *Let $p \in \mathcal{C}$ and $n, m \in \mathbb{N}_{>0}$ such that $G_n(f) = p(X^m)$. Then we have*

$$\gamma(f) \le m \deg(p) - \deg(f).$$

(vii) *If $\gamma(f) < \infty$ then each root of f has the height reducing property[4] with the set*

$$\{0, 1, \ldots, kf(0) - 1\}$$

for some positive integer k.

Proof. (i) Clear by [18, Theorem 4].

(ii) In view of Proposition 11 (i) and (ii) the first two statements are obvious. By [5, Lemma 2] we have

$$f(1)g(1) = (fg)(1) \ge (fg)(0) = f(0)g(0),$$

hence the assertion is clear by Proposition 11 (iv).

(iii) This is an obvious consequence of the definitions.

(iv) We use [5, Lemma 2] and first observe $f \notin \mathcal{C}$, hence $\gamma(f) > 0$. Then the assumption $\gamma(f) = 1$ leads to the existence of some $r \in \mathbb{N}_{\ge 2}$ such that

$$p := (X + r) \cdot f \in \mathcal{C}.$$

[4] For the definition see [4, Section 1].

But this yields the contradiction

$$2r \le p(0) \le p(1) = 1 + r.$$

Now, let $f(0) \ge 3$ and assume that there are $r, s \in \mathbb{Z}$ such that

$$p := (X^2 + sX + r) \cdot f \in \mathcal{C}.$$

Having in mind that the first factor belongs to $\mathcal{A}$ and using $s \le r \ge 2$ (see Proposition 15 (i)) we similarly deduce the contradiction

$$3r \le p(0) \le p(1) = 1 + s + r \le 1 + 2r.$$

(v) In case $\gamma(fg) = \infty$ then our assertion trivially holds. Therefore, let $\gamma(fg) < \infty$ and assume

$$\gamma(fg) < \max\{\gamma(f) - \deg(g), \gamma(g) - \deg(f)\}.$$

Then there exists $h \in \mathbb{Z}[X]$ such that $h(fg) \in \mathcal{C}$ and

$$\deg(h) = \gamma(fg) < \max\{\gamma(f) - \deg(g), \gamma(g) - \deg(f)\}.$$

W.l.o.g. we may suppose $\deg(h) < \gamma(f) - \deg(g)$. As $(hg)f \in \mathcal{C}$ we have

$$\gamma(f) \le \deg(hg) = \deg(h) + \deg(g)$$

which implies the impossibility

$$\deg(h) \ge \gamma(f) - \deg(g).$$

(vi) Clear by the definitions.

(vii) By assumption there is some $g \in \mathbb{Z}[X]$ such that $p := gf$ is a CNS polynomial, hence $g = 1$ or $g \in \mathcal{A}$ by (ii), thus $k := g(0) \ge 1$ by Proposition 11 (iv). Let $\beta \in \mathbb{Z}[\alpha]$, thus we can write $\beta = h(\alpha)$ with some $h \in \mathbb{Z}[X]$. We find $r \in \{0, 1, \ldots, kf(0) - 1\}[X]$ with $h \equiv r \pmod{p}$. Let $h = r + pt$ with $t \in \mathbb{Z}[X]$, thus

$$\beta = r(\alpha) + (pt)(\alpha) = r(\alpha) + g(\alpha)f(\alpha)t(\alpha) = r(\alpha). \qquad \square$$

Acknowledgement. The author is much indebted to Professor Attila Pethő for putting forward the CNS polynomial problem mentioned in the introduction. This problem was the main motivation for the present note. Further, the author thanks the anonymous referees for very carefully reading the first version of this note.

References

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

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

[3] S. Akiyama, H. Brunotte and A. Pethő, Cubic CNS polynomials, notes on a conjecture of W. J. Gilbert, *J. Math. Anal. Appl.* **281** (2003), 402–415.

[4] S. Akiyama, P. Drugilas and J. Jankauskas, Height reducing problem on algebraic integers, *Funct. Approx. Comment. Math.* **47** (2012), 105–119.

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

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

[7] G. Barat, V. Berthé, P. Liardet and J. Thuswaldner, Dynamical directions in numeration, *Ann. Inst. Fourier (Grenoble)* **56** (2006), 1987–2092, Numération, pavages, substitutions.

[8] T. Borbély, Általánosított számrendszerek, Master Thesis, *University of Debrecen*, 2003.

[9] J.-P. Borel, Polynômes à coefficients positifs multiples d'un polynôme donné, Vol. 1415, Cinquante ans de polynômes (Paris, 1988), Lecture Notes in Math., *Springer, Berlin*, 1990, 97–115.

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

[11] B. Horst, On real polynomials without nonnegative roots, *Acta Math. Acad. Paedagog. Nyházi. (N.S.)* **26** (2010), 31–34.

[12] B. Horst, Polynomials with nonnegative coefficients and a given factor, *Period. Math. Hungar.* **66** (2013), 61–72.

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

[14] M. Drmota and R. F. Tichy, Sequences, discrepancies and applications, Vol. 1651, Lecture Notes in Mathematics, *Springer-Verlag, Berlin*, 1997.

[15] A. Dubickas, On roots of polynomials with positive coefficients, *Manuscripta Math.* **123** (2007), 353–356.

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

[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), *Giornale di matematiche di Battaglini* **23** (1885), 203–221, 367.

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

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

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

[21] G. Kuba, Several types of algebraic numbers on the unit circle, *Arch. Math. (Basel)* **85** (2005), 70–78.

[22] K. Mahler, Lectures on transcendental numbers, Vol. 546, Lecture Notes in Mathematics, *Springer-Verlag, Berlin*, 1976.

[23] E. Meissner, Über positive Darstellungen von Polynomen, *Math. Ann.* **70** (1911), 223–235.

[24] A. Pethő, Private communication, 2003.

[25] 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", *Saga Univ., Saga*, 2004, 115–125.

[26] A. Pethő, Private communication, 2011.

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

[28] E. Seneta, Non-negative matrices and Markov chains, Springer Series in Statistics, Revised reprint of the second (1981) edition [Springer-Verlag, New York; MR0719544], *Springer, New York*, 2006.

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

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

[31] C. van de Woestijne, Number systems and the Chinese Remainder Theorem, Preprint, arXiv:1106.4219v1, 2011.

HORST BRUNOTTE
HAUS-ENDT-STRASSE 88
D-40593 DÜSSELDORF
GERMANY

E-mail: brunoth@web.de

(Received June 6, 2012; revised October 6, 2012)