Publ. Math. Debrecen
92/1-2 (2018), 223–242
DOI: 10.5486/PMD.2018.7958

On hyperbolic small-span CNS polynomials

By HORST BRUNOTTE (Düsseldorf)

Abstract. We characterize hyperbolic small-span CNS polynomials of degree up to 4.

1. Introduction

For a long time various generalizations of our ordinary decimal number system have been known and thoroughly been studied. Here we deal with canonical number systems (commonly abbreviated by CNS) special cases of which were already investigated by Grünwald [19], Knuth [25], Penney [29] and Gilbert [18]. The systematic study of canonical number systems has been initiated by the Hungarian school some decades ago (see [23], [21], [22], [26]). Detailed background information and relations to other areas such as shift radix systems, finite automata or fractal tilings can be found in the surveys by Barat *et al.* [6] and by Kirschenhofer–Thuswaldner [24].

The general notion of canonical number systems and the concept of CNS polynomials were introduced by Pethő [31]. The CNS property of a given polynomial can algorithmically be decided [36], [7], [15], and some characterization results on these polynomials are known. For instance, see [21], [18] for quadratic polynomials, [26], [4], [8], [5] for some other classes of polynomials, and [27], [20] for more general results. However, the complete description of these polynomials has remained an open problem even for small degrees (e.g., see [2, Problem 2.2] in a more general context).

Mathematics Subject Classification: 11A63, 11C08, 12E10, 11R09, 12Y05.
Key words and phrases: hyperbolic polynomial, canonical number system.

In view of this situation, several studies have been undertaken to describe particular classes of CNS polynomials (e.g., see PETHŐ [32], KANE [20], CHEN [15], MADRITSCH–ZIEGLER [28]). In this vein, we give a necessary condition for hyperbolic CNS polynomials and provide a characterization of hyperbolic small-span CNS polynomials of degree up to 4. Our approach exploits the list of irreducible hyperbolic small-span polynomials elaborated by ROBINSON [34], well-known sufficient conditions for CNS polynomials and the algorithm mentioned above.

2. On hyperbolic CNS polynomials

Let us briefly recall the definition and basic properties of CNS polynomials. The monic polynomial $f \in \mathbb{Z}[X]$ with non-vanishing constant term is called a CNS polynomial if for all $A \in \mathbb{Z}[X]$ there exists a polynomial $B \in \{0, \dots, |f(0)| - 1\}[X]$ such that $A \equiv B \pmod{f}$. Among other things, it is known (see [30] and [4, Section 1]) that the roots of CNS polynomials lie outside the closed unit disk and are non-positive. CNS polynomials of degree at most 2 are known: A monic linear integer polynomial is a CNS polynomial if and only if its constant term is at least 2 ([19], [1, Remark 4.5]), and $X^2 + bX + c \in \mathbb{Z}[X]$ is a CNS polynomial if and only if $-1 \le b \le c$ and $c \ge 2$ ([21], [22], [18], [8], [37], [5]). Furthermore, the CNS property of a given polynomial can algorithmically be decided [36], [7], [15]. The reader is referred to [1] for more background information. Throughout, we denote by $\mathcal{C}$ the set of all CNS polynomials.

A polynomial with real coefficients is called hyperbolic if it has only real roots (for a comprehensive survey see [33, Chapter 6]). Its span is the maximal difference between a pair of its roots. The span is small if it is strictly less than 4.

Here we are interested in monic hyperbolic integer polynomials with all roots less than -1. Our main result is the complete description of the hyperbolic small-span CNS polynomials of degree up to 4.

Theorem 1.

(i) *Every monic hyperbolic small-span integer polynomial of degree at most* 3 *all of whose roots are less than* -1 *is a CNS polynomial.*

(ii) *Let* p *be a monic hyperbolic small-span integer polynomial of degree* 4 *all of whose roots are less than* -1. *Then* p *is a CNS polynomial if and only if one of the following five conditions holds:*

(a) p *is irreducible.*

(b) $p = (X^2 + bX + c)(X^2 + mX + n)$ *with two irreducible quadratic integer factors and*

$$b < c \quad \text{or} \quad m < n.$$

(c) p *has exactly one monic linear integer factor.*

(d) $p = (X+i)(X+k)q$ *with* $i \geq k \geq 2$ *and* $q \in \mathbb{Z}[X]$ *irreducible such that either* $i > 2$ *or* $i = 2$, *and* $q \neq X^2 + 5X + 5$, $X^2 + 6X + 6$.

(e) $p = (X+r)(X+s)(X+t)(X+u)$ *with* $2 \leq r \leq s \leq t \leq u \leq r+3$ *and* $u \geq 3$.

Corollary 2. *Let p be a monic hyperbolic small-span integer polynomial of degree at most 4 all of whose roots are less than -1. Then every monic non-trivial divisor of p is a CNS polynomial.*

Remark 3. (i) An extension of Theorem 1 to larger degrees does not seem to be obvious. First, the product of the two hyperbolic CNS polynomials

$$X^2 + 6X + 6 \quad \text{and} \quad (X^2 + 6X + 6)(X + 5)$$

is a quintic small-span non-CNS polynomial, however, it can also be written as the product of $(X^2 + 6X + 6)^2 \notin \mathcal{C}$ and $X + 5 \in \mathcal{C}$. Second, analogously as in Section 3, below we see that the polynomials

$$f_s(X) := g(X + s) \qquad (s \geq 3)$$

are hyperbolic small-span polynomials with all roots less than -1, where

$$g := X^5 - X^4 - 4X^3 + 3X^2 + 3X - 1$$

is the (irreducible) polynomial no. 5a in [34]. We algorithmically check

$$f_3 = X^5 + 14X^4 + 74X^3 + 183X^2 + 210X + 89 \notin \mathcal{C},$$

but

$$f_4 = X^5 + 19X^4 + 140X^3 + 499X^2 + 859X + 571 \in \mathcal{C}.$$

(ii) It is well-known that Corollary 2 does not hold for arbitrary CNS polynomials. Indeed,

$$(X^2 - 2X + 3)(X + 2) \in \mathcal{C},$$

but $X^2 - 2X + 3 \notin \mathcal{C}$ ([11, Proposition 15]). Moreover, there exists a reducible CNS polynomial without CNS factors, e.g., see [11, Example 13]. A related

phenomenon in our surroundings is the following: The hyperbolic small-span polynomial

$$(X+2)^2(X+3)(X^2+5X+5)$$

is not a CNS polynomial, and it can be written as the product of the polynomials

$$X+3 \in \mathcal{C} \quad \text{and} \quad (X+2)^2(X^2+5X+5) \notin \mathcal{C},$$

or

$$X+2 \in \mathcal{C} \quad \text{and} \quad (X+2)(X+3)(X^2+5X+5) \in \mathcal{C}.$$

The proof of Theorem 1, which we delay to the next section, essentially consists of checking finitely many cases. To this end, we need the following result on hyperbolic CNS polynomials.

Theorem 4. *Let $f \in \mathbb{Z}[X]$ be a monic hyperbolic polynomial of positive degree d, and set*

$$\rho_d := \mathrm{e}^{-\log(2^{1/d}-1)}.$$

If all roots of f are less than $-\rho_d$, then f is a CNS polynomial.

Proof. Since $\rho_d > 1$, all roots of f are less than -1. For a maximal root β of f, we have

$$1 > -\frac{\log(2^{1/d}-1)}{\log(-\beta)},$$

and our result drops out from [11, Theorem 14]. □

Remark 5. The first few interesting values of the constant ρ_d are

$$\rho_3 = 3.847322\ldots, \quad \rho_4 = 5.285213\ldots, \quad \rho_5 = 6.725023\ldots.$$

Certainly, ρ_d is not optimal. Indeed, for $d = 3$ it can be replaced by $5/4$ (see [9, Corollary 5.3]). Moreover, for polynomials with only integer roots, a sharper result was established by Pethő [32, Theorem 4].

We conclude by speculating on the size of the coefficients of CNS polynomials. For expansive polynomials, Burcsi–Kovács [13, Statement 2.1] gave bounds for the moduli of the coefficients relative to their constant term. Many examples of CNS polynomials suggest the following:

Conjecture 6. *If $\sum_{i=0}^{d} p_i X^i \in \mathcal{C}$, then we have*

$$|p_i| < 2p_0 \qquad (i = 1, \ldots, d-1).$$

3. Proof of Theorem 1

Let $f \in \mathbb{Z}[X]$ be a monic non-constant hyperbolic polynomial, and let α_f (β_f, resp.) be a minimal (maximal, resp.) root of f. Thus the span of f (written $\mathrm{span}(f)$) is the difference $\beta_f - \alpha_f$.

For $\sigma \in \{-1, 1\}$ and any integer s, the polynomials $f(X)$ and $\sigma^{\deg(f)} f(\sigma X + s)$ are called equivalent. Obviously, equivalent polynomials have the same span.

For fixed degree, the number of equivalence classes of small-span polynomials is finite, and Robinson [34] computed a list of representatives of equivalence classes of irreducible hyperbolic small-span integer polynomials for degree up to 6, and conjectured lists for degrees 7 and 8. Capparelli, Del Fra and Sciò [14] presented a (possibly not exhaustive) list of small-span polynomials of degree up to 17. Flamming, Rhin and Wu [17] verified the completeness of these lists up to degree 15. Recently, El Otmani *et al.* [16] developed an alternative approach for this problem based on Linear Programming methods.

For brevity, we let $\mathcal{H}_d$ be the set of monic hyperbolic small-span integer polynomials of degree d, all of whose roots are less than -1. After some generalities, exploiting Robinson's results cited above we simply list all irreducible polynomials in $\mathcal{H}_d$ for $d = 2, 3, 4$. Then we describe the reducible CNS polynomials in $\mathcal{H}_4$, and we conclude by a proof of Theorem 1 and Corollary 2.

Lemma 7. *Let $f, g \in \mathbb{R}[X]$ be hyperbolic polynomials of positive degree with*

$$\mathrm{span}(f),\ \mathrm{span}(g) < \eta.$$

If $\beta_f \geq \beta_g$, then we have

$$\mathrm{span}(fg) < \eta \iff \beta_f - \alpha_g < \eta.$$

Proof. This can easily be checked by the definitions. □

The next two lemmas are trivial, but useful.

Lemma 8. *Let $f \in \mathcal{H}_d$ and $g \in \mathbb{Z}[X]$ be a monic divisor of f with $0 < \deg(g) < d$. Then $g \in \mathcal{H}_{\deg(g)}$.*

Lemma 9. *Let $g \in \mathbb{Z}[X]$ be a monic hyperbolic integer polynomial of positive degree d and $f \in \mathbb{Z}[X]$ equivalent to g, i.e.,*

$$f(X) = \sigma^{\deg(g)} g(\sigma X + s),$$

for some $s \in \mathbb{Z}$ and $\sigma \in \{-1, 1\}$.

(i) *Let $\sigma = 1$. Then we have*

$$f \in \mathcal{H}_d \iff s > \beta_g + 1.$$

In this case, we have

$$\alpha_f = \alpha_g - s \quad \text{and} \quad \beta_f = \beta_g - s.$$

(ii) *Let $\sigma = -1$. Then we have*

$$f \in \mathcal{H}_d \iff s < \alpha_g - 1.$$

In this case, we have

$$\alpha_f = s - \beta_g \quad \text{and} \quad \beta_f = s - \alpha_g.$$

Denoting by $\mathcal{I}_d$ the set of irreducible polynomials in $\mathcal{H}_d$, we obviously have

$$\mathcal{H}_d = \mathcal{I}_d \cup \bigcup_{\ell=0}^{d} \mathcal{R}_{d,\ell} \qquad (1 \le d \le 4),$$

where we introduce the (possibly empty) sets

$$\mathcal{R}_{d,\ell} := \{f \in \mathcal{H}_d \ : \ f \text{ reducible and } f \text{ has exactly } \ell \text{ monic linear factors}\}.$$

In the following tables, we list all elements of $\mathcal{I}_d$ for $2 \le d \le 4$ based on the tables by ROBINSON [34]. For a degree d polynomial g whose number from [34, Section 3] we give in the first column, we denote by $f(X) = \sigma^{\deg(g)} g(\sigma X + s)$ an equivalent polynomial in $\mathcal{H}_d$ parametrized by an integer parameter $t := \sigma s$. In the fourth column, the region of t is specified. In view of later use, we list the discriminant of f in case $d = 2$. Let us clarify our procedure by an easy example. Take the polynomial no. 2a

$$g := X^2 - X - 1$$

and $\sigma := -1$, hence

$$f(X) = (-1)^2 g(-X + s) = X^2 - (2s - 1)X + s^2 - s - 1$$

with $s \le -2$, because $\alpha_g = -0.6180\ldots$ and

$$s < \alpha_g - 1$$

by Lemma 9. Thus we conclude $f = X^2 + (2t + 1)X + t^2 + t - 1$, $t \ge 2$, and

$$\operatorname{discr}(f) = (2t + 1)^2 - 4(t^2 + t - 1) = 5.$$

no.	σ	$f - X^2$	t	$\operatorname{discr}(f)$
2a	1	$(2t-1)X + t^2 - t - 1$	≥ 3	5
	-1	$(2t+1)X + t^2 + t - 1$	≥ 2	5
2b	± 1	$2tX + t^2 - 2$	≥ 3	8
2c	± 1	$2tX + t^2 - 3$	≥ 3	12
2d	1	$(2t-1)X + t^2 - t - 3$	≥ 4	13
	-1	$(2t+1)X + t^2 + t - 3$	≥ 3	13

Table 1. Irreducible elements in $\mathcal{H}_2$.

no.	σ	$f - X^3$	t
3a	1	$(3t-1)X^2 + (3t^2-2t-2)X + t^3 - t^2 - t + 1$	≥ 3
	-1	$(3t+1)X^2 + (3t^2+2t-2)X + t^3 + t^2 - 2t - 1$	≥ 3
3b	1	$3tX^2 + 3(t^2-1)X + t^3 - 3t - 1$	≥ 3
	-1	$3tX^2 + 3(t^2-1)X + t^3 - 3t + 1$	≥ 3
3c	1	$(3t-1)X^2 + (3t^2-2t-3)X + t^3 - t^2 - 3t + 1$	≥ 4
	-1	$(3t+1)X^2 + (3t^2+2t-3)X + t^3 + t^2 - 3t - 1$	≥ 3
3d	1	$3tX^2 + (3t^2-4)X + t^3 - 4t - 2$	≥ 4
	-1	$3tX^2 + (3t^2-4)X + t^3 - 4t + 2$	≥ 3
3e	1	$3tX^2 + (3t^2-4)X + t^3 - 4t - 1$	≥ 4
	-1	$3tX^2 + (3t^2-4)X + t^3 - 4t + 1$	≥ 3

Table 2. Irreducible elements in $\mathcal{H}_3$.

no.	σ	$f - X^4$	t
4a	1	$(4t-2)X^3 + (6t^2-6t-2)X^2 + (4t^3-6t^2-4t+3)X + t^4 - 2t^3 - 2t^2 + 3t + 1$	≥ 4
	-1	$(4t+2)X^3 + (6t^2+6t-2)X^2 + (4t^3+6t^2-4t-3)X + t^4 + 2t^3 - 2t^2 - 3t + 1$	≥ 3
4b	1	$(4t-1)X^3 + (6t^2-3t-3)X^2 + (4t^3-3t^2-6t+1)X + t^4 - t^3 - 3t^2 + t + 1$	≥ 4
	-1	$(4t+1)X^3 + (6t^2+3t-3)X^2 + (4t^3+3t^2-6t-1)X + t^4 + t^3 - 3t^2 - t + 1$	≥ 3
4c	± 1	$4tX^3 + (6t^2-4)X^2 + (4t^3-8t)X + t^4 - 4t^2 + 2$	≥ 3
4d	1	$(4t-1)X^3 + (6t^2-3t-4)X^2 + (4t^3-3t^2-8t+2)X + t^4 - t^3 - 4t^2 + 2t + 3$	≥ 4
	-1	$(4t+1)X^3 + (6t^2+3t-4)X^2 + (4t^3+3t^2-8t-2)X + t^4 + t^3 - 4t^2 - 2t + 3$	≥ 3
4e	1	$(4t-1)X^3 + (6t^2-3t-4)X^2 + (4t^3-3t^2-8t+4)X + t^4 - t^3 - 4t^2 + 4t + 1$	≥ 3
	-1	$(4t+1)X^3 + (6t^2+3t-4)X^2 + (4t^3+3t^2-8t-4)X + t^4 + t^3 - 4t^2 - 4t + 1$	≥ 3
4f	± 1	$4tX^3 + (6t^2-5)X^2 + (4t^3-10t)X + t^4 - 5t^2 + 5$	≥ 3
4g	1	$4tX^3 + (6t^2-4)X^2 + (4t^3-8t-1)X + t^4 - 4t^2 - t + 1$	≥ 4
	-1	$4tX^3 + (6t^2-4)X^2 + (4t^3-8t+1)X + t^4 - 4t^2 + t + 1$	≥ 3
4h	1	$(4t-2)X^3 + (6t^2-6t-3)X^2 + (4t^3-6t^2-6t+5)X + t^4 - 2t^3 - 3t^2 + 5t + 1$	≥ 4
	-1	$(4t+2)X^3 + (6t^2+6t-3)X^2 + (4t^3+6t^2-6t-5)X + t^4 + 2t^3 - 3t^2 - 5t + 1$	≥ 3
4i	± 1	$4tX^3 + (6t^2-4)X^2 + (4t^3-8t)X + t^4 - 4t^2 + 1$	≥ 3
4j	1	$(4t-1)X^3 + (6t^2-3t-4)X^2 + (4t^3-3t^2-8t+1)X + t^4 - t^3 - 4t^2 + t + 2$	≥ 4
	-1	$(4t+1)X^3 + (6t^2+3t-4)X^2 + (4t^3+3t^2-8t-1)X + t^4 + t^3 - 4t^2 - t + 2$	≥ 3
4k	1	$4tX^3 + (6t^2-5)X^2 + (4t^3-10t-1)X + t^4 - t^3 - 5t^2 - t + 4$	≥ 4
	-1	$4tX^3 + (6t^2-5)X^2 + (4t^3-10t+1)X + t^4 - t^3 - 5t^2 + t + 4$	≥ 3
4l	1	$(4t-2)X^3 + (6t^2-6t-4)X^2 + (4t^3-6t^2-8t+5)X + t^4 - 2t^3 - 4t^2 + 5t + 5$	≥ 4
	-1	$(4t+2)X^3 + (6t^2+6t-4)X^2 + (4t^3+6t^2-8t-5)X + t^4 + 2t^3 - 4t^2 - 5t + 5$	≥ 3
4m	1	$(4t-1)X^3 + (6t^2-3t-4)X^2 + (4t^3-3t^2-8t)X + t^4 - t^3 - 4t^2 + 1$	≥ 4
	-1	$(4t+1)X^3 + (6t^2+3t-4)X^2 + (4t^3+3t^2-8t)X + t^4 + t^3 - 4t^2 + 1$	≥ 3
4n	1	$(4t-2)X^3 + (6t^2-6t-3)X^2 + (4t^3-6t^2-6t+4)X + t^4 - 2t^3 - 3t^2 + 4t + 1$	≥ 4
	-1	$(4t+2)X^3 + (6t^2+6t-3)X^2 + (4t^3+6t^2-6t-4)X + t^4 + 2t^3 - 3t^2 - 4t + 1$	≥ 3

Table 3. Irreducible elements in $\mathcal{H}_4$.

We now characterize the polynomials in $\mathcal{H}_2 \cup \mathcal{H}_3$ with relatively large roots. From now on, we write $\rho := \rho_4$ for shortness.

Lemma 10. *Let $q = X^2 + bX + c \in \mathbb{Z}[X]$. Then q belongs to $\mathcal{H}_2$ if and only if $c \geq 4$ and*

$$\max\left\{4, 2\sqrt{c}\right\} \leq b \leq \min\left\{c, \sqrt{4c+15}\right\}.$$

In this case, we have

$$\alpha_q = \frac{1}{2}(-b - \sqrt{\Delta}), \quad \beta_q = \frac{1}{2}(-b + \sqrt{\Delta}), \quad \operatorname{span}(q) = \sqrt{\Delta},$$

where $\Delta := b^2 - 4c$ is the discriminant of q.

Proof. Recall that by [3, Lemma 11] all roots of q lie outside the unit disk if and only if $|b| \leq |c|$. The proof can now easily be completed. □

Lemma 11. *Let $q \in \mathcal{H}_2$ with $\beta_q \geq -\rho$.*

(i) *If q is reducible, then there exist $k \in \{2, \ldots, 5\}$ and $m \in \{0, \ldots, 3\}$ such that*

$$q = X^2 + (2k+m)X + k(k+m).$$

Further, we have $\beta_q = -k$.

(ii) *If q is irreducible, then q is one of the following polynomials:*

$$\begin{aligned}
&X^2 + (2t-1)X + t^2 - t - 1 && (3 \leq t \leq 6),\\
&X^2 + (2t+1)X + t^2 + t - 1 && (2 \leq t \leq 5),\\
&X^2 + 2tX + t^2 - 2 && (3 \leq t \leq 6),\\
&X^2 + 2tX + t^2 - 3 && (3 \leq t \leq 7),\\
&X^2 + (2t-1)X + t^2 - t - 3 && (4 \leq t \leq 7),\\
&X^2 + (2t+1)X + t^2 + t - 3 && (3 \leq t \leq 6).
\end{aligned}$$

Proof. (i) This can be checked straightforwardly.
(ii) q is equivalent to one of the polynomials f listed in Table 1, and we observe

$$t \leq \begin{cases} \beta_f + \rho & (\sigma = 1),\\ -\alpha_f + \rho & (\sigma = -1). \end{cases}$$

□

Now we turn to quartic polynomials. Here we often use the following result.

Lemma 12. *Let $p = X^4 + p_3X^3 + p_2X^2 + p_1X + p_0 \in \mathbb{Z}[X]$ enjoy the following properties:*

(i) *p is not divisible by a cyclotomic polynomial;*

(ii) $p_0 > 3$;
(iii) $p_3 > 1$;
(iv) $p_1 > 2p_2$;
(v) $2p_1 - p_2 + 2p_3 < 2p_0$;
(vi) $p_1 \le p_0 \implies p_3 \le p_2$.
Then we have $p \in \mathcal{C}$.

PROOF. If $p_1 > p_0$, then our assertion is clear by [12, Lemma 5.1]. Now, let $p_1 \le p_0$. Then we have

$$1 < p_3 \le p_2 < p_1,$$

and our assertion is clear by [27, Theorem 6]. □

We are now in a position to describe the reducible polynomials in $\mathcal{H}_4$. Our method of proof always aims at reducing as far as possible the number of polynomials which have to be checked by an algorithm. Let us begin with the product of two irreducible quadratic polynomials, i.e., the set $\mathcal{R}_{4,0}$.

Lemma 13. *Let* $q = X^2 + bX + c$, $r = X^2 + mX + n \in \mathbb{Z}[X]$ *be irreducible, and assume* $qr \in \mathcal{H}_4$. *Then we have*

$$qr \in \mathcal{C} \quad \iff \quad b < c \quad \text{or} \quad m < n.$$

PROOF. Corollary 15 below tells us that

$$p := X^4 + p_3X^3 + p_2X^2 + p_1X + p_0 := qr \tag{3.1}$$

is not a CNS polynomial if $b = c$ and $m = n$. To prove the converse, we may restrict to $\beta_p \ge -\rho$ in view of Theorem 4. Without loss of generality, we assume $\beta_p = \beta_q$, hence

$$b \le 2\rho + \sqrt{b^2 - 4c}, \tag{3.2}$$

and

$$\sqrt{m^2 - 4n} - \sqrt{b^2 - 4c} \le m - b < \sqrt{m^2 - 4n} - \sqrt{b^2 - 4c} + 8. \tag{3.3}$$

We frequently use $b, m \ge 5$ (see Table 1), $p_0 = cn > 3$ and

$$1 < p_3 = b + m \ < \ p_2 = bm + n + c \ < \ p_1 = cm + bn. \tag{3.4}$$

If $p_1 \le p_0$, we are done by the Kovács–Pethő theorem [27, Theorem 6] (see also [10, Corollary 5]), because p is not divisible by a cyclotomic polynomial. Therefore, in the following we impose the condition $p_1 > p_0$, hence

$$(c-b)n < cm. \tag{3.5}$$

Furthermore, we only need to consider the case

$$(2(c-b)+1)n \le (2c-b+2)m - c + 2b. \tag{3.6}$$

Indeed, the opposite inequality means

$$2p_1 - p_2 + 2p_3 < 2p_0,$$

and then Lemma 12 yields $p \in \mathcal{C}$, because we convince ourselves that then also the inequality

$$p_1 > 2p_2$$

holds. Simply observe

$$n > \frac{(2c-b+2)m - c + 2b}{2(c-b)+1},$$

and verify

$$(b-2)((2c-b+2)m - c + 2b) + (2c-2b+1)((c-2b)m - 2c) > 0.$$

The remainder of the proof consists of checking several cases. Specifically, we let q run through the (irreducible) polynomials described in Lemma 11, and r through the polynomials listed in Table 1. Let q be the first polynomial, hence we let

$$3 \le t \le 6, \qquad b = 2t-1, \qquad c = t^2 - t - 1.$$

For convenience, we collect the following values:

t	b	c	p_3	p_2	p_1	p_0	(3.5)	(3.6)
3	5	5	$m+5$	$5m+n+5$	$5(m+n)$	$5n$	–	$n \le 7m+5$
4	7	11	$m+7$	$7m+n+11$	$11m+7n$	$11n$	$4n < 11m$	$9n \le 17m+3$
5	9	19	$m+9$	$9m+n+19$	$19m+9n$	$19n$	$10n < 19m$	$21n \le 31m-1$
6	11	29	$m+11$	$11m+n+29$	$29m+11n$	$29n$	$18n < 29m$	$37n \le 49m-7$

Now, we let r run through the polynomials listed in Table 1, and start with

$$m = 2s-1, \quad n = s^2 - s - 1 \qquad (s \ge 3).$$

Our prerequisites and (3.3) yield that

$$t+1 \le s \le t+3.$$

For $t=3$, we check

$$X^4+12X^3+51X^2+90X+55, \quad X^4+14X^3+69X^2+140X+95,$$

$$X^4+16X^3+89X^2+200X+145 \in \mathcal{C}$$

by an algorithm. Now, $t=4$ is excluded by (3.6), and $t=5,6$ by (3.5).

The remaining polynomials are dealt with analogously and left to the reader. □

Lemma 14. *If $2<b<c$, then*

$$X^4+bX^3+(b+c)X^2+2cX+c \notin \mathcal{C}.$$

Proof. We refer the reader to [1] for some basic facts on CNS polynomials, and observe that our polynomial admits the following periodic sequence:

$$\begin{aligned}(1,-1,1,-1) \to (-1,1,-1,1) \to (1,-1,1,0) \to (-1,1,0,-1) \to (1,0,-1,2) \to \\ \to (0,-1,2,-2) \to (-1,2,-2,2) \to (2,-2,2,-1) \to (-2,2,-1,0) \to \\ \to (2,-1,0,1) \to (-1,0,1,-1) \to (0,1,-1,1) \to (1,-1,1,-1).\end{aligned}$$ □

Corollary 15. *If $n,m \in \mathbb{N}$, then*

$$(X^2+nX+n)(X^2+mX+m) \notin \mathcal{C}.$$

Proof. If $n+m<nm$, we are done by Lemma 14. Otherwise, we have either

$$nm = n+m-1 \quad \text{or} \quad nm = n+m.$$

In the first case, we have $n=1$ or $m=1$, hence one of the factors is a cyclotomic polynomial and the product cannot be a CNS polynomial. In the second case, we have $n=m=2$, and we check

$$(X^2+2X+2)^2 = X^4+4X^3+8X^2+8X+4 \notin \mathcal{C}.$$ □

Now, we convince ourselves that all polynomials in $\mathcal{H}_4$ which admit exactly one linear factor are in fact CNS polynomials.

Lemma 16. *We have* $\mathcal{R}_{4,1} \subset \mathcal{C}$.

PROOF. Let $p \in \mathcal{R}_{4,1}$. If $\beta_p < -\rho$, then we are done by Theorem 4. Therefore, we assume $\beta_p \geq -\rho$, and write

$$p = (X + v) \cdot f =: X^4 + p_3X^3 + p_2X^2 + p_1X + p_0,$$

where

$$f = X^3 + aX^2 + bX + c$$

is one of the polynomials in Table 2, and

$$\max\{1, t - 4 - \alpha_g\} < v < t + 4 - \beta_g \qquad (\sigma = 1),$$

or

$$\max\{1, t - 4 - \beta_g\} < v < t + 4 + \alpha_g \qquad (\sigma = -1);$$

here we use Lemma 9 and denote by g the polynomial in [34] which is equivalent to f. We verify

$$p_0 = cv, \quad p_1 = bv + c, \quad p_2 = av + b, \quad p_3 = v + a.$$

Here we only give the proof for the first polynomial (no. 3a in [34]) in some detail; the remaining polynomials are treated analogously.

Case 1. $\beta_p = -v$.

Then, we have

$$v \leq \min\{5, t - \beta_g\},$$

which implies

$$\beta_g + 2 \leq t < \alpha_g + 9 \qquad (\sigma = 1),$$

or

$$\beta_g + 2 \leq t < -\beta_g + 9 \qquad (\sigma = -1).$$

Case 1.1. Polynomial 3a with $\sigma = 1$.

Then we have $4 \leq t \leq 7$. For $t = 4$, we have $v = 2$, and we check algorithmically that $X^4 + 13X^3 + 60X^2 + 121X + 90$ is a CNS polynomial. For $t = 5$, we have $v = 3$, and an application of the Kovács–Pethő theorem (see the proof of Lemma 13 above) yields our claim. Analogously, we treat the remaining two cases.

Case 1.2. Polynomial 3a with $\sigma = -1$.

Again, we have $4 \leq t \leq 7$. For $t = 4$, we have $v = 2$, and we check algorithmically that $X^4 + 15X^3 + 80X^2 + 177X + 138$ is a CNS polynomial, and for $t = 5, 6, 7$, the Kovács–Pethő theorem confirms our claim.

Case 2. $\beta_p \neq -v$.

Using $\beta_f > -v$ and $\beta_f \geq -\rho$, we deduce

$$t \leq \rho + \beta_g, \quad \max\{1, t-\beta_g, t-4-\alpha_g\} < v < t+4-\beta_g \qquad (\sigma = 1),$$

or

$$t \leq \rho - \alpha_g, \quad \max\{1, t+\alpha_g, t-4-\beta_g\} < v < t+4+\alpha_g \qquad (\sigma = -1).$$

Case 2.1. Polynomial 3a with $\sigma = 1$.

Then we have $3 \leq t \leq 7$. For $t = 3$, we have $2 \leq v \leq 5$, $p_0 = 16v$, $p_1 = 19v+16$, $p_2 = 8v+19$, $p_3 = v+8$, and we prove $p \in \mathcal{C}$ algorithmically. Similarly, we treat the remaining cases.

Case 2.2. Polynomial 3a with $\sigma = -1$.

Then we have $3 \leq t \leq 6$. For $t = 3$, we have $2 \leq v \leq 5$, and we check algorithmically that the polynomials with the coefficients

$$p_0 = 29v, \quad p_1 = 31v+29, \quad p_2 = 10v+31, \quad p_3 = v+10$$

belong to $\mathcal{C}$. Then we apply Lemma 12 in the remaining cases $t = 4, 5, 6$. □

Now, we aim at describing the CNS property of a product of a reducible and an irreducible quadratic polynomial in $\mathcal{H}_4$.

Lemma 17. *Let $q = X^2 + 4X + c$ and $r \in \mathbb{Z}[X]$ such that $qr \in \mathcal{H}_4$.*

(i) $q = (X+2)^2$.

(ii) *If r is irreducible, then we have*

$$qr \in \mathcal{C} \iff r \neq X^2+5X+5,\ X^2+6X+6.$$

Proof. (i) Clear by Lemmas 8 and 10.

(ii) From Corollary 15, we infer that the conditions on r are necessary. To prove the converse, we write $r = X^2 + mX + n$, and observe

$$-2 + \frac{1}{2}\big(m + \sqrt{\mathrm{discr}(r)}\big) = \beta_q - \alpha_r < 4,$$

hence

$$6 \leq m < 12 - \sqrt{\mathrm{discr}(r)}; \tag{3.7}$$

here we exploit the inequality $m > 5$, which is clear by Table 1 and our prerequisites.

Now, we let r run through the polynomials in Table 1 which satisfy (3.7), and check algorithmically that the resulting product polynomials are in fact CNS polynomials. The details are left to the reader. □

Lemma 18. *Let $i \geq k \geq 2$ and $q = (X+i)(X+k)$. Further, let $r \in \mathbb{Z}[X]$ be irreducible such that $qr \in \mathcal{H}_4$. Then $qr \in \mathcal{C}$ if and only if either $i > 2$ or $i = 2$ and $r \neq X^2 + 5X + 5,\ X^2 + 6X + 6$.*

Proof. If $i = 2$, our claim is clear by Lemma 17. Therefore, we let $i > 2$, write

$$r = X^2 + mX + n, \quad q = X^2 + bX + c$$

with

$$b := 2k + \ell \geq 5, \quad c := k(k+l) \qquad (\ell \in \{0, \ldots, 3\}),$$

and set $p := qr$. Now, we show $p \in \mathcal{C}$, and analogously as in the proof of Lemma 13, we assume $\beta_p \geq -\rho$ and conditions (3.5) and (3.6).

First, consider $\beta_p = \beta_q$, hence $k \leq \rho$. For $k = 2, \ldots, 5$ we let r run through the polynomials in Table 1, and we check our assertion algorithmically.

Second, let $\beta_p > \beta_q$, hence $\beta_r \geq -\rho$, and therefore

$$m - \sqrt{\operatorname{discr}(r)} \leq 2\rho.$$

Further, we have

$$4 > \beta_r - \alpha_q = \frac{1}{2}\big(-m + \sqrt{\operatorname{discr}(r)}\big) - (-(k+\ell)),$$

which implies

$$2(k+\ell) < 8 + m - \sqrt{\operatorname{discr}(r)} \leq 2\rho + 8,$$

and then

$$k \leq k + \ell \leq 9.$$

Analogously as before, the proof can now be completed by letting r run through the polynomials listed in Lemma 11. □

Finally, we inspect the set $\mathcal{R}_{4,4}$, i.e., the subset of products of four monic linear factors in $\mathcal{H}_4$. The characterization of CNS polynomials of this type is an easy consequence of a general result by Pethő [31] on CNS polynomials with only integer roots.

Lemma 19. *Let $r, s, t, u \in \mathbb{N}$ such that $2 \leq r \leq s \leq t \leq u \leq r + 3$. Then we have*

$$(X+r)(X+s)(X+t)(X+u) \in \mathcal{C} \iff u \geq 3.$$

PROOF. Assume that our polynomial belongs to $\mathcal{C}$ and $u = 2$. Then $r = s = t = 2$, but $(X+2)^4 \notin \mathcal{C}$ by Corollary 15, a contradiction.

Conversely, let $u \geq 3$. If

$$\frac{1}{r} + \frac{1}{s} + \frac{1}{t} + \frac{1}{u} \leq 1,$$

then our assertion follows from [31, Theorem 4]. Therefore, we suppose

$$\frac{1}{r} + \frac{1}{s} + \frac{1}{t} + \frac{1}{u} > 1, \tag{3.8}$$

hence $r \leq 3$. We distinguish two cases and several subcases.

Case 1. $r = 2$.

We consider the polynomial

$$X^4+(s+t+u+2)X^3+(tu+(s+2)(t+u)+2s)X^2+((s+2)tu+2s)(t+u))X+2stu.$$

Case 1.1. $s = 2$.

Thus we have to check the polynomial

$$X^4 + (t+u+4)X^3 + (tu+4(t+u)+4)X^2 + 4(tu+t+u)X + 4tu.$$

Case 1.1.1. $t = 2$.

For $u = 3, 4, 5$, we algorithmically check that the polynomials

$$X^4 + X^3 + 30X^2 + 44X + 24, \quad X^4 + 10X^3 + 36X^2 + 56X + 32,$$
$$X^4 + 11X^3 + 42X^2 + 68X + 40$$

are in fact CNS polynomials.

u	$P - X^4$
3	$9X^3 + 30X^2 + 44X + 24$
4	$10X^3 + 36X^2 + 56X + 32$
5	$11X^3 + 42X^2 + 68X + 40$

u	$P - X^4$	number of witnesses
3	$9X^3 + 30X^2 + 44X + 24$	469
4	$10X^3 + 36X^2 + 56X + 32$	405
5	$11X^3 + 42X^2 + 68X + 40$	385

Case 1.1.2. $t = 3$.

Similarly as above, we convince ourselves that the polynomials

$$X^4 + 10X^3 + 37X^2 + 60X + 36, \quad X^4 + 11X^3 + 44X^2 + 76X + 48,$$
$$X^4 + 12X^3 + 51X^2 + 92X + 60$$

are in fact CNS polynomials.

Case 1.1.3. $t = 4$.

Analogously, we see that the polynomials

$$X^4 + 12X^3 + 52X^2 + 96X + 64, \; X^4 + 13X^3 + 60X^2 + 116X + 80$$

are CNS polynomials.

Case 1.1.4. $t = 5$.

Finally, the polynomial

$$X^4 + 14X^3 + 69X^2 + 140X + 100$$

is a CNS polynomial.

Case 1.2. $s = 3$.

The following table gives a survey on the polynomials

$$p = X^4 + (t + u + 5)X^3 + (tu + 5(t + u) + 6)X^2 + (5tu + 6(t + u))X + 6tu,$$

which are algorithmically checked to be CNS polynomials.

t	u	$p - X^4$
3	3	$11X^3 + 45X^2 + 81X + 54$
	4	$12X^3 + 53X^2 + 102X + 72$
	5	$13X^3 + 61X^2 + 123X + 90$
4	4	$13X^3 + 62X^2 + 128X + 96$
	5	$14X^3 + 71X^2 + 154X + 120$
5	5	$15X^3 + 81X^2 + 185X + 150$

Case 1.3. $s = 4$.

Case 1.3.1. $t = 4$.

For $u = 4, 5$, the polynomials

$$X^4 + (u + 10)X^3 + 2(5u + 16)X^2 + 32(u + 1)X + 32u$$

are checked as above.

u	$P - X^4$
4	$14X^3 + 72X^2 + 160X + 128$
5	$15X^3 + 82X^2 + 192X + 160$

Case 1.3.2. $t = 5$.

Then we have $u = 5$, and Lemma 12 yields our assertion.

Case 1.4. $s = 5$.

We have $t = u = 5$, and $X^4 + 17X^3 + 195X^2 + 275X + 250$ is checked to be a CNS polynomial.

Case 2. $r = 3$.

Then we have $3 \le u \le 6$, (3.8) yields $t \le 5$, and we inspect the polynomials

$$X^4+(s+t+u+3)X^3+(tu+(s+3)(t+u)+3s)X^2+((s+3)tu+3s(t+u))X+3stu.$$

Case 2.1. $s = 3$.

The following table gives a survey on the polynomials

$$p = X^4 + (t + u + 6)X^3 + (tu + 6(t + u) + 9)X^2 + (6tu + 9(t + u))X + 9tu,$$

which are algorithmically checked to be CNS polynomials.

t	u	$p - X^4$
3	3	$12X^3 + 54X^2 + 108X + 81$
	4	$13X^3 + 63X^2 + 135X + 108$
	5	$14X^3 + 72X^2 + 162X + 135$
	6	$15X^3 + 81X^2 + 189X + 162$
4	4	$14X^3 + 73X^2 + 158X + 144$
	5	$15X^3 + 83X^2 + 191X + 180$
	6	$16X^3 + 93X^2 + 224X + 216$
5	5	$16X^3 + 94X^2 + 240X + 225$
	6	$17X^3 + 105X^2 + 279X + 270$

Case 2.2. $s \ge 4$.

Now, (3.8) yields $s < 5$, thus $s = 4$, and then $t = 4$ and $u \le 5$, and the polynomials

$$X^4 + 15X^3 + 84X^2 + 208X + 192,\ X^4 + 16X^3 + 95X^2 + 248X + 240$$

are checked as above.

u	$P - X^4$
4	$15X^3 + 84X^2 + 208X + 192$
5	$16X^3 + 95X^2 + 248X + 240$

The proof is now completed. □

Remark 20. Our present tools are not sufficient to prove Lemma 14 without the restriction on the span. Indeed, for $r = s = t = 2$ and $u \geq 3$, inequality (3.8) is satisfied but Lemma 12 (iv) is not. Further, note that in [20, Section 5], an example of a non-CNS polynomial is given, which is the product of nine linear pairwise different CNS polynomials.

Proof of Theorem 1 and Corollary 2. (i) In view of the well-known characterization of CNS polynomials of degree ≤ 2 cited in the beginning of Section 2, Table 1 above, and

$$\mathcal{R}_{2,2} = \left\{X^2 + (r+s)X + rs \ : \ r, s \in \mathbb{N},\, 2 \leq r \leq s \leq r+3\right\},$$

we have

$$\mathcal{H}_1 \cup \mathcal{H}_2 \subset \mathcal{C}.$$

Inspecting the polynomials in Table 2, we see

$$\mathcal{I}_3 \subset \mathcal{C}$$

by using either the Kovács–Pethő theorem or [9, Theorem 5.1], depending on the size of the linear coefficient. From [9, Corollary 5.2] we infer

$$\mathcal{R}_{3,1} \cup \mathcal{R}_{3,3} \subset \mathcal{C}.$$

Therefore, we see

$$\mathcal{H}_3 = \mathcal{I}_3 \cup \mathcal{R}_{3,1} \cup \mathcal{R}_{3,3} \subset \mathcal{C}.$$

(ii) Similarly as above, we find

$$\mathcal{I}_4 \subset \mathcal{C} \tag{3.9}$$

by an application of the Kovács–Pethő theorem, Lemma 12 or algorithmically. Clearly, we have

$$\mathcal{H}_4 = \mathcal{I}_4 \cup \mathcal{R}_{4,0} \cup \mathcal{R}_{4,1} \cup \mathcal{R}_{4,2} \cup \mathcal{R}_{4,4},$$

and our assertion drops out from (3.9) and Lemmas 13, 16, 18 and 19. The proof of the theorem is completed and Corollary 2 is then clear by Lemma 8. □

Acknowledgements. The author is much indebted to the anonymous referee for constructive suggestions to improve the first version of this paper. Some computations of the present paper were done with SAGE [35].

References

[1] 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.

[2] S. Akiyama, H. Brunotte, A. Pethő, W. Steiner and J. M. Thuswaldner, Problems and conjectures around shift radix systems, *Open Problems Math.* **2** (2014), 1–4.

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

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

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

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

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

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

[9] H. Brunotte, On cubic CNS polynomials with three real roots, *Acta Sci. Math. (Szeged)* **70** (2004), 495–504.

[10] H. Brunotte, A unified proof of two classical theorems on CNS polynomials, *Integers* **12** (2012), 709–721.

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

[12] H. Brunotte, A. Huszti and A. Pethő, Bases of canonical number systems in quartic algebraic number fields, *J. Théor. Nombres Bordeaux* **18** (2006), 537–557.

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

[14] S. Capparelli, A. Del Fra and C. Sciò, On the span of polynomials with integer coefficients, *Math. Comp.* **79** (2010), 967–981.

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

[16] S. El Otmani, A. Maul, G. Rhin and J.-M. Sac-Épée, Integer linear programming applied to determining monic hyperbolic irreducible polynomials with integer coefficients and span less than 4, *J. Théor. Nombres Bordeaux* **25** (2013), 71–78.

[17] V. Flammang, G. Rhin and Q. Wu, The totally real algebraic integers with diameter less than 4, *Mosc. J. Comb. Number Theory* **1** (2011), 17–25.

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

[19] 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), *Giorn. Mat. Battaglini* **23** (1885), 203–221; Errata *ibid.* 367.

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

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

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

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

[24] P. Kirschenhofer and J. M. Thuswaldner, Shift radix systems – a survey, In: Numeration and Substitution, 2012, **B46**, *Res. Inst. Math. Sci. (RIMS)*, *Kyoto*, 2014, 1–59.

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

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

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

[28] M. G. Madritsch and V. Ziegler, An infinite family of multiplicatively independent bases of number systems in cyclotomic number fields, *Acta Sci. Math. (Szeged)* **81** (2015), 33–44.

[29] W. Penney, A 'binary' system for complex numbers, *J. Assoc. Comput. Mach.* **12** (1965), 247–248.

[30] A. Pethő, On a polynomial transformation and its application to the construction of a public key cryptosystem, In: Computational Number Theory, Debrecen, 1989, *de Gruyter*, *Berlin*, 1991, 31–43.

[31] 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 University*, *Saga*, 2004, 115–125.

[32] A. Pethő, Notes on CNS polynomials and integral interpolation, In: More Sets, Graphs and Numbers, Bolyai Soc. Math. Stud., Vol. **15**, *Springer*, *Berlin*, 2006, 301–315.

[33] Q. I. Rahman and G. Schmeisser, Analytic Theory of Polynomials, London Mathematical Society Monographs, New Series, Vol. **26**, *Oxford University Press*, *Oxford*, 2002.

[34] R. M. Robinson, Algebraic equations with span less than 4, *Math. Comp.* **18** (1964), 547–559.

[35] W. A. Stein *et al.*, Sage Mathematics Software (Version 5.3), *The Sage Development Team*, 2012, `http://www.sagemath.org`.

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

[37] J. M. Thuswaldner, Elementary properties of canonical number systems in quadratic fields, In: Applications of Fibonacci Numbers, Vol. **7**, Graz, 1996, *Kluwer Acad. Publ.*, *Dordrecht*, 1998, 405–414.

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

E-mail: brunoth@web.de

(Received February 27, 2017; revised April 11, 2017)