Mathematica Pannonica
26/2 (2017–2018), 87–106

On Akiyama's Conjecture for quartic CNS polynomials

Horst **Brunotte**

Haus-Endt-Straße 88
D-40593 Düsseldorf, GERMANY

Received: 2018. July 15

MSC 2010: 12 D 99,11 A 63

Keywords: canonical number system, radix representation

Abstract: Quartic CNS polynomials whose second highest coefficient is at least -1 preserve their CNS property under addition of sufficiently large positive integers.

1. Introduction

Canonical number systems (customarily abbreviated by CNS) can be regarded as generalizations of the classical decimal or binary numeration systems. Preceded by the study of some special cases [13, 18, 12] they have first been developed by the Hungarian school some decades ago [16, 14, 15, 20].

CNS polynomials (see Section 2 for the definition) have been introduced by A. Pethő [23] and generalized in the sequel (e.g., see [17, 24]). Several results on these polynomials are known, however, until now the characterization of CNS polynomials for degrees at least 3 has remained an open problem. Moreover, the set of CNS polynomials apparently has poor algebraic properties. For instance, polynomials can lose their CNS property by addition of positive integers (e.g., see [8]). For more details and background the reader is referred to the recent work of A. Pethő and J. Thuswaldner [24] where some light is shed on the speculation that canonical number systems seem to be quite exceptional among number systems.

In view of this situation, S. Akiyama [1] put forward the following

E-mail address: brunoth@web.de

interesting conjecture: For every CNS polynomial P there exists a natural number N such that $P+n$ is a CNS polynomial for all $n \geq N$. It is known that this conjecture holds true for many classes of CNS polynomials [9]. Among others, the truth of this conjecture implies $p_m \geq -1$ for every CNS polynomial of the form $X^d + \sum_{i=0}^{m} p_i X^i$ [9, Section 2].

In this note we establish Akiyama's Conjecture for quartic polynomials whose second highest coefficient is at least -1.

2. Definitions and statement of results

Let us briefly recall the definition of a CNS polynomial. We say that the monic polynomial $P \in \mathbb{Z}[X]$ is a CNS polynomial if for every $A \in \mathbb{Z}[X]$ there exists a polynomial $B \in \{0, \ldots, |P(0)| - 1\}[X]$ such that $A \equiv B \pmod{P}$; here we denote by $\mathbb{Z}$ ($\mathbb{N}$, $\mathbb{N}_0$, $\mathcal{C}$, respectively) the set of rational integers (the set of natural numbers, nonnegative rational integers, CNS polynomials, respectively).

Let us illustrate Akiyama's Conjecture by a simple example.

Example 2.1. The cubic polynomial $P := X^3+50X^2+73X+53$ satisfies $P+n \in \mathcal{C}$ for every nonnegative integer $n \neq 3$. For $n \geq 20$ this is clear by the Kovács – Pethő Theorem [21, Theorem 6] (see also [7, Corollary 5]), and for $n < 20$ this can be checked algorithmically (e.g., see [10]).

Now we state our main result and postpone its proof to the next section. Following Dubickas [11] we say that the real polynomial $\sum_{i=0}^{d} r_i X^i$ has a strictly dominant constant term provided

$$|r_0| > \sum_{i=1}^{d} |r_i| \, .$$

Theorem 2.2. Let $P = X^4 + p_3X^3 + p_2X^2 + p_1X + p_0$ be a CNS polynomial with $p_3 \geq -1$. If n is a natural number such that $P + n$ has a strictly dominant constant term then $P + n$ is a CNS polynomial.

Gilbert's Theorem (see [3, Theorem 3.1]) gives necessary conditions for cubic CNS polynomials. Theorem 2.2 immediately yields the analogue of this result for quartic polynomials whose second highest coefficient is at least -1. It is known that the second highest coefficient of a CNS polynomial P is at least $-P(0)$ (see Theorem 3.1 below), and the author conjectures that it is at least -1 for all CNS polynomials [9, Conjecture 2.3].

Corollary 2.3. The coefficients of the CNS polynomial $X^4 + p_3X^3 + p_2X^2 + p_1X + p_0$ with $p_3 \geq -1$ fulfill the following four conditions:

1. $p_3 + p_2 + p_1 \geq -1$
2. $p_3 + p_2 \geq -1$
3. $p_2 \geq -1$
4. $p_3 = -1$ implies $p_1 < -1$.

Proof. Using Theorem 2.2 we add a suitable integer to the given polynomial such that the resulting polynomial is a CNS polynomial with strictly dominant constant term. Then [6, Theorem 5.4] yields our claim. $\diamondsuit$

Finally, we exhibit a further example in support of our conjecture that the second highest nonzero coefficient of a CNS polynomial must be at least -1. The polynomial

$$X^d - aX^2 + bX + c \qquad (d \geq 4,\ 2 \leq a \leq c,\ a-2 \leq b \leq c-2)$$

admits the nonzero periodic element

$$(10\cdots10) \mapsto (01\cdots01) \mapsto (10\cdots10)$$

if d is even, and

$$(01\cdots010) \mapsto (10\cdots101) \mapsto (01\cdots010)$$

if d is odd.

3. Proof of Theorem 2.2

In this section we let

$$P = p_dX^d + p_{d-1}X^{d-1} + \cdots + p_1X + p_0 \in \mathbb{Z}[X] \qquad (3.1)$$

be a monic integer polynomial of positive degree d with non-vanishing constant term.

3.1. Some important properties of CNS polynomials

In this subsection we collect some useful properties of CNS polynomials.

Theorem 3.1. Let P be a CNS polynomial .

1. P is expansive, i.e., every root of P lies outside the closed unit disc.
2. If r is a real root of P then $r < -1$.
3. $p_0 \geq \max\{2,\ 1 + (-1)^{d-1} + \sum_{i=1}^{d-1} (-1)^{i-1} p_i\}$
4. $\sum_{i=1}^{d} p_i \geq 0$.

Proof. (i) [22, Theorem 6.1].
(ii) This was shown by Gilbert [12, Proposition 6] under the (unused) assumption of the irreducibility of P.
(iii) From (i) and (ii) we infer $p_0 \geq 2$ and $P(-1) \geq 1$.
(iv) See [5, Lemma 2]. ♢

To P we associate the mapping $\tau_P\colon\ \mathbb{Z}^d \to \mathbb{Z}^d$ by[1]

$$\tau_P(a_1, \ldots, a_d) := (a_2, \ldots, a_d, -\lfloor s_P(a_1, \ldots, a_d)/\, |p_0| \rfloor)$$

with

$$s_P(a_1, \ldots, a_d) := \sum_{j=0}^{d-1} p_{d-j}\, a_{j+1}$$

and the set[2]

$$\mathcal{N}_P := \{z \in \mathbb{Z}^d\ :\ \tau_P^k(z) = 0 \text{ for some } k \in \mathbb{N}\}.$$

If there is no fear of confusion we occasionally symbolize the action of τ_P by an arrow and omit the subscript P.

We tacitly exploit the following fundamental fact [2, Section 3].

Lemma 3.2. If there exists a nonzero τ_P-periodic element in $\mathbb{Z}^d$ then P is not a CNS polynomial.

[1] We denote by $\lfloor \ldots \rfloor$ the usual floor function.

[2] For a map $f\colon X \to X$ we let $f^0 = id$ and $f^{k+1} = f^k \circ f$.

The next two observations play an important role in the proof of Theorem 2.2.

Lemma 3.3. Let the coefficients of P satisfy $\sum_{i=1}^{d} p_i \geq 0$ and $p_0 > 1$. If $e \in \{0,1\}^d$ and $\tau_P(e) = e$ then we have $e = 0$.

Proof. We have[3]

$$e = (e_1, \ldots, e_d) = (e_2, \ldots, e_d, (\tau_P(e))_d),$$

hence

$$e_{i+1} = e_i \qquad (i = 1, \ldots, d-1) \qquad \text{and} \qquad (\tau_P(e))_d = e_d\,.$$

This implies

$$e_i = e_1 \qquad (i = 2, \ldots, d).$$

The assumption $e \neq 0$ would yield $e = (1, \ldots, 1)$, in particular, $(\tau_P(e))_d = 1$, and subsequently the contradiction

$$\sum_{i=1}^{d} p_i < 0\,.$$

$\diamondsuit$

Lemma 3.4. Let $P \in \mathcal{C}$ and $n \in \mathbb{N}$ such that $Q := P + n$ has a strictly dominant constant term. If $Q \notin \mathcal{C}$ then there exists some $e \in \{0,1\}^d \backslash \{0\}$ with the following properties:

(i) e is purely τ_Q-periodic.

(ii) The period length k of e is minimal among all non-vanishing purely τ_Q-periodic elements in $\{0,1\}^d$, and we have $k > 1$.

(iii) There exists $m_0 \in \mathbb{N}$ such that

$$\tau_P^m(e)_d \neq \tau_Q^i(e)_d \qquad (m \in \{0, \ldots, m_0\},\ i \in \{1, \ldots, k-1\}).$$

[3] For $i \in I$ we write x_i for the i-th component of the element $x \in X^I$.

Proof. For simplicity we write $\tau := \tau_P$ and $\sigma := \tau_Q$, and for $a \in \mathbb{Z}^d$ put

$$t(a) := \min\{\ell \in \mathbb{N}_0 \ : \ \tau^\ell(a) = 0\}.$$

Then clearly

$$t(\tau^m(a)) = \max\{0,\ t(a) - m\} \qquad (m \in \mathbb{N}_0).$$

Since $Q \notin \mathcal{C}$ we have $\{0,1\}^d \not\subset \mathcal{N}_Q$ by [6, Corollary 4.4]. Thus we can choose a purely σ-periodic element $e \in \{0,1\}^d \setminus \{0\}$ of minimal period length k. More explicitly, we have

$$\sigma^k(e) = e \qquad \text{and} \qquad \sigma^i(e) \neq e \qquad (i = 1, \ldots, k-1)$$

with $k > 1$: Indeed, in view of Theorem 3.1 the assumption $k = 1$ yields $e = 0$ by Lemma 3.4.

Furthermore, we may assume

$$t(e) = \min\{t(\sigma^i(e)) \ : \ i = 1, \ldots, k-1\}.$$

Thus we have

$$m_0 := t(e) > 0\,,$$

and we deduce

$$\tau^m(e) \neq \sigma^i(e) \qquad (m \in \{0, \ldots, m_0\},\ i \in \{1, \ldots, k-1\})\,.$$

Indeed, set

$$m_i := t(\sigma^i(e)) \qquad (i = 1, \ldots, k-1)$$

and assume $\tau^m(e) = \sigma^i(e)$ for some $m \in \{0, \ldots, m_0\}$ and $i \in \{1, \ldots, k-1\}$. Then we see

$$m_i = t(\sigma^i(e)) = t(\tau^m(e)) = t(e) - m = m_0 - m,$$

which implies

$$m_i + m = m_0 \leq m_i,$$

hence $m = 0$ and $e = \sigma^i(e)$: Contradiction. ◊

We find it convenient to mention the following observation.

Lemma 3.5. Let P have a positive strictly dominant constant term and $d \geq 3$. If

$$e = (e_1, e_2, 0, \ldots, 0) \in \{0,1\}^d \setminus \mathcal{N}_P$$

then we have

$$p_{d-1} < -e_1, \quad e_2 = 1 \qquad \text{and} \qquad \tau_P(e) = (1, 0, \ldots, 0, 1)\,.$$

Proof. The assumption $e_2 = 0$ implies the impossibility

$$\tau(e_1, e_2, 0, \ldots, 0) = 0.$$

Thus we have $e_2 = 1$ and there exists $\delta \in \{0, 1\}$ such that

$$\tau(e_1, 1, 0, \ldots, 0) = (1, 0, \ldots, 0, \delta).$$

Clearly, we must have $\delta = 1$ and therefore $p_{d-1} < -e_1$. ♢

3.2. Auxiliary results on quartic CNS polynomials

Now we collect some facts on quartic expansive polynomials which will play an important role in our further considerations. Throughout we let

$$P = X^4 + p_3X^3 + p_2X^2 + p_1X + p_0$$

be a monic integer polynomial.

Lemma 3.6. If P is expansive and p_0 is positive then the following statements hold.

(i) $p_0 \geq 2, \quad |p_1 - p_0p_3| \leq p_0^2 - 2, \quad |p_1 + p_3| \leq p_0 + p_2 \quad$ and

$$\Delta(P) := p_0^3 - (p_0 - 1)^2 p_2 + (p_0 + 1)p_1p_3 - p_0p_3^2 - p_1^2 - p_0^2 - p_0 \geq 0.$$

(ii) If $p_2 \geq p_0 - ap_1 - bp_3 - c$ then we have

$$f(p_1, p_3) \leq (c + 1)p_0(p_0 - 2) + c,$$

where we set

$$f(x, y) := x^2 - a(p_0 - 1)^2 x - (b(p_0 - 1)^2 + (p_0 + 1)x - p_0y)y\,.$$

(iii) If $p_1 \geq 0$ and $p_3 \leq 0$ then we have $p_2 \leq p_0$.

Proof. (i) [4, Lemma 3.2].
(ii) From (i) we deduce

$$\begin{aligned} 0 &\leq p_0^3 - (p_0-1)^2(p_0 - ap_1 - bp_3 - c) + (p_0+1)p_1p_3 - p_0p_3^2 - p_1^2 - p_0^2 - p_0 \\ &= p_0^3 - (p_0-1)^2p_0 - p_0^2 - p_0 + c(p_0-1)^2 - p_1^2 + a(p_0-1)^2p_1 + \\ &\quad +(b(p_0-1)^2 + (p_0+1)p_1 - p_0p_3)p_3 \\ &= p_0^2 - 2p_0 + c(p_0^2 - 2p_0 + 1) - f(p_1, p_3), \end{aligned}$$

which implies our assertion.
(iii) Assume $p_2 > p_0$. Then an application of (ii) with $a = b = 0, c = -1$ yields the absurdity

$$0 \geq p_1^2 + (p_0+1)(-p_3)p_1 + p_0p_3^2 + 1 \geq 1\,.$$

◊

We now list some particular instances of non-CNS polynomials.

Lemma 3.7. The polynomial P is not a CNS polynomial if its coefficients have one of the following three properties.

(i) $p_2 \leq -2$ and $p_1 + p_3 \geq 0$

(ii) $p_1 \geq p_0 - 1, p_2 \geq -1$ and $p_3 = -1$

(iii) $p_1 \geq 0,\ p_2 \in \{p_0 - 1, p_0\}$ and $p_3 = -1$

Proof. Assume $P \in \mathcal{C}$, hence

$$p_0 \geq p_1 - p_2 + p_3 \tag{3.2}$$

by Theorem 3.1 (iii). An inspection of [19, Section 25] reveals $p_0 \geq 3$, a fact which we tacitly use in the sequel.
(i) In view of (3.2) and our prerequisites we have

$$0 \leq p_1 + p_3 \leq p_0 + p_2 < p_0$$

and

$$-2 \geq p_2 \geq p_1 + p_3 - p_0 \geq -p_0\,,$$

and we immediately verify

$$0101 \to 1010 \to 0101,$$

which contradicts our assumption.
(ii) Note that we have

$$p_1 - p_2 \leq p_0 + 1 \tag{3.3}$$

by (3.2).

First, let $p_2 = -1$, hence

$$p_0 - 1 \leq p_1 \leq p_0\,,$$

and in both cases we find nonzero periodic elements: For $p_1 = p_0 - 1$ we have

$$1001 \to 001-1 \to 01-11 \to 1-110 \to -1100 \to 1001\,,$$

and for $p_1 = p_0$ we have

$$1001 \to 001-1 \to 01-12 \to 1-12-2 \to -12-22 \to \cdots$$

$$\cdots \to 2-22-1 \to -22-11 \to 2-110 \to -1100 \to 1001\,.$$

Now, let $p_2 \geq 0$, hence by Lemma 3.6 (iii)

$$p_2 \leq p_0 - 1\,,$$

thus by (3.3)

$$p_1 \leq p_0 + 1 + p_2 \leq 2p_0\,.$$

Observe that we have

$$p_1 - p_2 \geq 1\,,$$

since otherwise we had

$$p_1 = p_2 = p_0 - 1\,,$$

yielding the impossibility $\Delta(P) < 0$ (see Lemma 3.6 (i)). We check

$$1001 \to 001-1\,.$$

Case 1 $p_1 - p_2 \leq p_0$

We verify

$$001-1 \to 01-11 \to 1-110$$

yielding

$$p_2 \geq p_0 - 2\,,$$

since otherwise we get the contradiction

$$1-110 \to -1100 \to 1001\,.$$

Now, a straightforward application of Lemma 3.6 (i) excludes $p_2 = p_0 - 1$, thus we have

$$p_2 = p_0 - 2\,,$$

But then we must have

$$p_1 \leq \frac{7}{5}p_0 - \frac{9}{5}\,.$$

Indeed, assuming the contrary we infer from Lemma 3.6 (i)

$$0 \leq \Delta(P) < p_0^3 - (p_0-1)^2(p_0-2) - \frac{1}{5}(p_0+1)(7p_0-9) - \frac{1}{25}(7p_0-9)^2 - p_0^2 - 2p_0 \leq 0$$

which is absurd.

By direct computation we check that $(1,1,-2,2)$ is τ_P-periodic (of period length 11) in case $p_0 \leq 6$. Therefore we may now assume $p_0 \geq 7$ and verify

$$0-12-1 \to -12-10 \to 2-102 \to 2-102 \to -102-2 \to 02-21 \to \cdots$$

$$\cdots \to 2-211 \to -211-2 \to 11-22 \to 1-220 \to -220-1 \to 20-12 \to 0-12-1\,.$$

Again by Lemma 3.2 P cannot be a CNS polynomial.

Case 2 $p_1 - p_2 > p_0$

Then we have

$$p_1 - p_2 = p_0 + 1$$

and further

$$001-1 \to 01-12 \to 1-12-2 \to -12-22 \to 2-22-1 \to -22-11 \to \cdots$$

$$\cdots \to 2-110 \to -1100 \to 1001$$

yielding a contradiction.

(iii) First, let $p_2 = p_0$. The inequality

$$p_1^2 + (p_0 + 1)p_1 + p_0 - p_0^2 + 2p_0 \leq 0$$

is a consequence of Lemma 3.6 (ii) (with $a = b = c = 0$) and yields $p_1 \leq p_0 - 3$. We immediately check that $(1, 0, 0, 1)$ is a τ_P-periodic element (of period length 10): Contradiction.

Second, let $p_2 = p_0 - 1$. If

$$p_1 < p_0 - 1$$

then the period

$$1001 \to 0010 \to 0100 \to 1001$$

establishes our claim. If

$$p_1 \geq p_0 - 1$$

we deduce

$$p_1^2 + (p_0 + 1)p_1 + p_0 - p_0^2 + 2p_0 \leq 0$$

from Lemma 3.6 (ii) (with $a = b = 0, c = 1$) which is impossible. $\diamondsuit$

3.3. Proof of Theorem 2.2

After these preparations we are now in a position to prove Akiyama's Conjecture for particular quartic CNS polynomials. First recall

$$p_1 + p_2 + p_3 \geq -1 \tag{3.4}$$

and

$$p_0 \geq p_1 - p_2 + p_3 \tag{3.5}$$

by Theorem 3.1.

Let us assume $Q := P + n \notin \mathcal{C}$. From Lemma 3.4 we infer the existence of a purely σ-periodic element $f \in \{0, 1\}^4 \setminus \{0\}$ with minimal period length $k \geq 2$ and

$$s(f) < -p_0 \qquad \text{or} \qquad s(f) \geq p_0, \tag{3.6}$$

where we set $\sigma := \tau_Q$ and

$$s(e) := e_1 + e_2 p_3 + e_3 p_2 + e_4 p_1 \qquad (e \in \mathbb{Z}^4).$$

We aim at proving the impossibility of the existence of f, and if this cannot be achieved we show that P cannot be a CNS polynomial. Our proof is divided into two main parts consisting of the inspection of several cases and subcases.

In the first main part we assume that there is some $j \in \{0, \ldots, k-1\}$ such that

$$s(\sigma^j(f)) < -p_0\,.$$

Setting $e := \sigma^j(f)$ we have

$$e^{(i)} := \sigma^i(e) \in \{0,1\}^4 \setminus \{0\} \qquad (i \in \mathbb{N}_0),$$

$$e_1 + e_2 p_3 + e_3 p_2 + e_4 p_1 < -p_0 \tag{3.7}$$

and $e^{(1)} = (e_2, e_3, e_4, 1)$.

Case 1 $\qquad e_4 = 0$

Thus we deal with $e = (e_1, e_2, e_3, 0)$ and

$$e_1 + e_2 p_3 + e_3 p_2 < -p_0\,.$$

by (3.7).

We must have $e_3 = 1$. Indeed, the assumption $e_3 = 0$ yields $e_2 = 1$ by Lemma 3.5 and then

$$-1 \leq e_1 + p_3 < -p_0$$

by (3.7) which is impossible.

Then we have $e = (e_1, e_2, 1, 0)$, $e^{(1)} = (e_2, 1, 0, 1)$ and

$$e_1 + e_2 p_3 + p_2 < -p_0\,. \tag{3.8}$$

We deduce $e_2 = 1$, since otherwise (3.8) would yield

$$p_2 < -p_0$$

contradicting Lemma 3.6 (i).

Thus we have

$$p_2 + p_3 \ < -p_0,$$

by (3.7), hence

$$p_2 \le -p_0 - 1 - p_3 \le -p_0 - 1 + 1 = -p_0$$

and then

$$p_1 + p_3 = 0$$

by Lemma 3.6 (i) again, and we obtain the absurdity

$$0 = p_1 + p_3 \ge -1 - p_2 \ge -1 + p_0 > 0\,.$$

Case 2 $\qquad e_4 = 1$

We note $e = (e_1, e_2, e_3, 1)$, $e^{(1)} = (e_2, e_3, 1, 1)$ and

$$e_1 + e_2p_3 + e_3p_2 + p_1 < -p_0\,.$$

Case 2.1 $\qquad e_3 = 0$

Then $e = (e_1, e_2, 0, 1)$, $e^{(1)} = (e_2, 0, 1, 1)$ and

$$e_1 + e_2p_3 + p_1 < -p_0\,.$$

Case 2.1.1 $\qquad e_2 = 0$

Thus $e = (e_1, 0, 0, 1)$, $e^{(1)} = (0, 0, 1, 1)$, $k > 2$ and

$$p_1 \le -p_0 - e_1 - 1 \le -p_0 - 1$$

yielding

$$p_2 + p_3 \ge -1 - p_1 \ge p_0$$

by (3.4).

Case 2.1.1.1 $\qquad p_1 + p_2 \ge 0$

Then we have $p_2 \ge p_0 + 1, e^{(2)} = (0, 1, 1, 0)$, $e^{(3)} = (1, 1, 0, 0)$, $e^{(4)} = (1, 0, 0, 0)$ and $e^{(5)} = 0$: Contradiction.

Case 2.1.1.2 $\qquad p_1 + p_2 < 0$

Now, $p_1 + p_2 + p_3 \geq 0$ is impossible, since then we would have $e^{(6)} = 0$, and similarly we exclude $p_1 + p_2 + p_3 = -1$. Thus in view of (3.4) this case cannot occur.

Case 2.1.2 $\qquad e_2 = 1$

Then $e = (e_1, 1, 0, 1)$, $e^{(1)} = (1, 0, 1, 1)$, $k > 2$,

$$p_1 + p_3 \leq -p_0 - e_1 - 1 \leq -p_0 - 1 \tag{3.9}$$

and

$$p_2 \geq -1 - (p_1 + p_3) \geq p_0 \,.$$

The assumption $p_1 + p_2 \geq -1$ yields $e^{(2)} = (0, 1, 1, 0)$, $e^{(3)} = (1, 1, 0, 0)$, $e^{(4)} = (1, 0, 0, 0)$ and $e^{(5)} = 0$: Contradiction. Therefore, we have

$$p_1 + p_2 < -1 \,,$$

thus $e^{(2)} = (0, 1, 1, 1)$, $p_3 \geq 1$ by (3.4), hence by (3.9)

$$p_1 \leq -p_0 - 1 - p_3 \leq -p_0 - 2$$

and then

$$p_1 + p_2 + p_3 \geq 0 \,, \tag{3.10}$$

because otherwise we had $e^{(3)} = (1, 1, 1, 1)$, $e^{(4)} = (1, 1, 1, 0)$, $e^{(5)} = (1, 1, 0, 0)$, $e^{(6)} = (1, 0, 0, 0)$ and $e^{(7)} = 0$: Contradiction.

An application of

$$p_2 \geq -(p_1 + p_3) \geq p_0 + 1$$

to Lemma 3.6 (ii) (with $a = b = 0, c = -1$) yields the absurdity

$$0 \geq p_1^2 - (p_0+1)p_1p_3 + p_0p_3^2 + 1 > p_1^2 - (p_0+1)p_1 + p_0 > (p_0+2)^2 + (p_0+2)(p_0+1) \,.$$

Case 2.2 $\qquad e_3 = 1$

Then $e = (e_1, e_2, 1, 1)$, $e^{(1)} = (e_2, 1, 1, 1)$ and

$$e_1 + e_2p_3 + p_2 + p_1 < -p_0 \,,$$

hence

$$p_1 + p_2 \leq -p_0 - 1 - e_2p_3 - e_1 \,.$$

The assumption $e_2 = 1$ would imply

$$p_1 + p_2 \leq -p_0 - p_3 - 1$$

contradicting (3.4).

Therefore, we have $e_2 = 0$, $e = (e_1, 0, 1, 1)$, $e^{(1)} = (0, 1, 1, 1)$, $k > 2$,

$$-p_3 - 1 \leq p_1 + p_2 \leq -p_0 - 1\,,$$

hence $p_3 \geq p_0$ and then (3.10): Indeed, the assumption

$$p_1 + p_2 + p_3 = -1$$

yields $e^{(2)} = (1, 1, 1, 1)$, $e^{(3)} = (1, 1, 1, 0)$ and then by periodicity

$$p_2 + p_3 < -1\,, \tag{3.11}$$

yielding $p_2 \leq -p_0 - 2$, $e^{(4)} = (1, 1, 0, 1)$, $e^{(5)} = (1, 0, 1, 0)$, $e^{(6)} = (0, 1, 0, 1)$, and $e^{(7)} = e^{(5)}$ which leads to the contradiction $k = 2$.

We conclude $e^{(2)} = (1, 1, 1, 0)$, deduce (3.11) and then similarly as above $e^{(3)} = (1, 1, 0, 1)$, $e^{(4)} = (1, 0, 1, 0)$, $e^{(5)} = (0, 1, 0, 1)$, and $e^{(6)} = e^{(4)}$ which again leads to the contradiction $k = 2$.

This terminates the proof of the first main part, and we now assume

$$s(\sigma^j(f)) \geq -p_0 \qquad\qquad (j = 0, \ldots, k-1),$$

hence by (3.6)

$$p_0 \leq s(f) \leq e_1 p_3 + e_2 p_2 + e_3 p_1 + 1\,,$$

where we set

$$e := \sigma(f) := (e_1, e_2, e_3, 0).$$

For convenience we collect the following inequalities:

$$p_0 - 1 \leq e_1 p_3 + e_2 p_2 + e_3 p_1\,, \tag{3.12}$$

$$s(e^{(j)}) \geq -p_0 \qquad\qquad (j \in \mathbb{N}_0)\,, \tag{3.13}$$

and by Lemma 3.5

$$s(e^{(i)}) < 0 \qquad \text{for some } i \in \{0,1\}\,. \tag{3.14}$$

We may assume that i is minimal with this property.

Case 1 $\qquad i = 0$

Thus $e^{(1)} = (e_2, e_3, 0, 1)$, further

$$-p_0 \le e_1 + e_2 p_3 + e_3 p_2 < 0 \tag{3.15}$$

by (3.13) and (3.14), and

$$p_1 \ge -p_0 - e_3 p_3 - e_2 \tag{3.16}$$

by (3.13) again.

Case 1.1 $\qquad e_3 = 0$

Then we infer $e_2 = 1$ from Lemma 3.5, thus $e = (e_1, 1, 0, 0)$, $e^{(1)} = (1, 0, 0, 1)$, further

$$p_3 \le -1 - e_1 \le -1$$

by (3.15) yielding $p_3 = -1$, $e_1 = 0$ and $e = (0, 1, 0, 0)$. Then we have

$$p_2 \ge p_0 - 1$$

by (3.12), and

$$p_1 \ge -p_0 - 1$$

by (3.16).

Case 1.1.1 $\qquad p_1 < -1$

Then $e^{(2)} = (0, 0, 1, 1)$ and $e^{(3)} = (0, 1, 1, 0)$ by (3.4). But this implies the contradiction $e^{(4)} = (1, 1, 0, 0)$, $e^{(5)} = (1, 0, 0, 0)$ and $e^{(6)} = 0$.

Case 1.1.2 $\qquad p_1 \ge -1$

Then $e^{(2)} = (0, 0, 1, 0)$, $e^{(3)} = (0, 1, 0, 0)$ and $e^{(4)} = e^{(1)}$, hence $k = 3$ and $e_1 = 0$. Lemma 3.6 (ii) (with $a = -1, b = c = 0$) shows $p_1 \ne -1$. Thus we have $p_1 \ge 0$ and by Lemma 3.6 (iii) $p_2 \le p_0$, thus

$$p_2 \in \{p_0, p_0 - 1\},$$

and our claim follows from Lemma 3.7 (iii).

Case 1.2 $e_3 = 1$

Then $e = (e_1, e_2, 1, 0)$, $e^{(1)} = (e_2, 1, 0, 1)$, further

$$-p_0 \le e_1 + e_2 p_3 + p_2 \le -1 \tag{3.17}$$

by (3.15),

$$-p_0 - e_2 \le p_1 + p_3$$

by (3.16), and

$$p_0 - 1 \le e_1 p_3 + e_2 p_2 + p_1$$

by (3.12).

Further we have

$$p_1 + p_3 \ge -e_2\,.$$

Indeed, the opposite inequality, (3.4) and (3.17) yield

$$-e_2 > p_1 + p_3 \ge -1 - p_2 \ge e_2 p_3\,,$$

hence $e_2 = 1$ and then the impossibility $-1 > p_3$.

Thus we have $e^{(2)} = (1, 0, 1, 0)$ and by (3.17)

$$p_2 \le -1 - e_2 p_3 - e_1\,.$$

Case 1.2.1 $e_2 = 0$

This implies

$$p_1 + p_3 \ge 0$$

and $e = (e_1, 0, 1, 0), e^{(1)} = (0, 1, 0, 1)$, further

$$-p_0 - e_1 \le p_2 \le -1 - e_1 \le -1$$

and

$$p_0 - 1 \le p_1 + e_1 p_3\,. \tag{3.18}$$

Case 1.2.1.1 $p_2 = -1$

Then we successively find $e_1 = 0$, $e = (0, 0, 1, 0), e^{(3)} = (0, 1, 0, 0)$, $p_3 = -1$ and $p_1 \ge p_0 - 1$. Lemma 3.7 (ii) shows that P is not a CNS polynomial: Contradiction.

Case 1.2.1.2 $\qquad p_2 < -1$

Then we have $e_1 = 1$: Indeed, otherwise we would have $e = (0,0,1,0), e^{(1)} = (0,1,0,1), e^{(2)} = (1,0,1,0)$ and $e^{(3)} = e^{(1)}$, which would yield $k = 2$, hence $e = e^{(2)}$: Contradiction.

Thus, from (3.15) we infer

$$-p_0 - 1 \leq p_2 \leq -2,$$

then

$$p_1 + p_3 \geq 1$$

from (3.4) and $p_3 = -1$ from Lemma 3.7 (i). Now (3.18) yields

$$p_1 \geq p_0$$

and then (3.5) the absurdity

$$p_0 \geq p_0 + 2 - 1 > p_0\,.$$

Case 1.2.2 $\qquad e_2 = 1$

By the above we have

$$p_1 + p_3 \geq -1, \qquad p_2 + p_3 \leq -1 - e_1$$

and $e = (e_1, 1, 1, 0), e^{(1)} = (1,1,0,1), e^{(2)} = (1,0,1,0)$ and $k > 2$.

Now we have $p_2 \geq -1$. Indeed, the assumption $p_2 < -1$ yields $e^{(3)} = (0,1,0,1)$, and in view of $k > 2$ we must have

$$p_1 + p_3 = -1\,,$$

which implies the impossibility

$$p_2 \geq -1 - (p_1 + p_3) = 0\,.$$

Thus we find $e^{(3)} = (0,1,0,0)$ yielding

$$p_3 = -1, \qquad p_1 \geq 0\,,$$

and $e^{(4)} = (1,0,0,1), e^{(5)} = (0,0,1,0)$ and then $p_2 = -1$, since otherwise we would have $e^{(6)} = e^{(3)}$) yielding $k = 3$ and the absurdity $e = e^{(3)}$.

From (3.4) we infer $p_1 \geq 1$ yielding $e^{(6)} = (0,1,0,1), e^{(7)} = e^{(2)}$, hence $k = 5$ and the contradiction $e = e^{(5)}$.

Case 2 $\qquad i = 1$

Our assumptions imply

$$e_3p_2{+}e_2p_3{+}e_1 = s(e) \geq 0,\ e^{(1)} = (e_2, e_3, 0, 0) \text{ and } e_3p_3{+}e_2 = s(e^{(1)}) < 0\,,$$

and applying Lemma 3.5 we deduce

$$e_3 = 1,\ p_3 = -1, \qquad e_2 = 0,\ e = (e_1, 0, 1, 0) \qquad \text{and} \qquad p_2 \geq -e_1\,.$$

Now (3.12) implies

$$p_1 \geq p_0 - 1 + e_1 \geq p_0 - 1\,,$$

and then Lemma 3.7 (ii) leads to the contradiction

$$-e_1 \leq p_2 < -1\,.$$

The proof is now complete.

References

[1] S. AKIYAMA. Private communication (2012).

[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), pp. 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), pp. 402–415.

[4] S. AKIYAMA and N. GJINI, *Connectedness of number theoretic tilings*, Discrete Math. Theor. Comput. Sci., 7 (2005), pp. 269–312 (electronic).

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

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

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

[8] ——, *Unusual CNS polynomials*, Math. Pannon., 24 (2013), pp. 125–137.

[9] ——, *Some comments on Akiyama's conjecture on CNS polynomials.*, Int. Electron. J. Algebra, 23 (2018), pp. 167–175.

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

[11] A. DUBICKAS, *Roots of polynomials with dominant term*, Int. J. Number Theory, 7 (2011), pp. 1217–1228.

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

[13] 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), pp. 203–221, 367.

[14] I. KÁTAI and B. KOVÁCS, *Kanonische Zahlensysteme in der Theorie der quadratischen algebraischen Zahlen*, Acta Sci. Math. (Szeged), 42 (1980), pp. 99–107.

[15] ——, *Canonical number systems in imaginary quadratic fields*, Acta Math. Acad. Sci. Hungar., 37 (1981), pp. 159–164.

[16] I. KÁTAI and J. SZABÓ, *Canonical number systems for complex integers*, Acta Sci. Math. (Szeged), 37 (1975), pp. 255–260.

[17] P. KIRSCHENHOFER and J. M. THUSWALDNER, *Shift radix systems—a survey*, in Numeration and substitution 2012, RIMS Kôkyûroku Bessatsu, B46, Res. Inst. Math. Sci. (RIMS), Kyoto, 2014, pp. 1–59.

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

[19] A. KOVÁCS, *Generalized binary number systems*, Ann. Univ. Sci. Budapest. Sect. Comput., 20 (2001), pp. 195–206.

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

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

[22] 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, pp. 31–43.

[23] ——, *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", S. Katayama, C. Levesque, and T. Nakahara, eds., Saga, 2004, Saga Univ., pp. 115–125.

[24] A. PETHŐ and J. THUSWALDNER, *Number systems over orders.*, Monatsh. Math., 187 (2018), pp. 681–704.