International Electronic Journal of Algebra
Volume 23 (2018) 167-175
DOI: 10.24330/ieja.373660

SOME COMMENTS ON AKIYAMA'S CONJECTURE ON CNS POLYNOMIALS

Horst Brunotte

Received: 23 May 2017; Revised: 16 October 2017; Accepted: 25 October 2017
Communicated by Abdullah Harmancı

Abstract. It is well-known that in general polynomials lose their CNS property by addition of small positive integers. We comment on a conjecture of S. Akiyama on addition of sufficiently large positive constants to CNS polynomials.

Mathematics Subject Classification (2010): 12D99, 11A63
Keywords: Canonical number system, radix representation

1. Introduction

Canonical number systems (usually abbreviated by CNS) can be regarded as generalizations of the classical decimal or binary numeration systems. They have first been introduced by the Hungarian school some decades ago (see [23,24,25, 27]); special cases had already been studied in [20,21,26]. The works [7,8] are recommended as profound surveys on this subject in a broader context.

The concept of CNS polynomials (see Section 2 for the definition) was introduced by A. Pethő [32] and generalized in the sequel (see for example [2,6,34]). Some results on these polynomials are known (e.g., see [4,5,11,12,22,29]), however, until now the characterization of CNS polynomials for degrees at least 3 has remained an open problem and seems to be difficult. Moreover, the set of CNS polynomials seems to have poor algebraic properties. For instance, polynomials can lose their CNS property by addition of small positive integers.

In view of this situation, S. Akiyama [1] put forward the following interesting conjecture: For every CNS polynomial P there exists a positive integer N such that $P + n$ is a CNS polynomial for all $n \geq N$.

In this short note we collect several examples in support of Akiyama's Conjecture. Further, aiming at a quantitative version of this conjecture we propose a mapping on a certain subset of integer polynomials which contains the CNS polynomials, but which is very easy to describe. Finally, we speculate on other aspects which are related to Akiyama's Conjecture.

2. Some comments on Akiyama's Conjecture

Let us first recall the definition of a CNS polynomial[1]. The monic integer polynomial P with nonzero constant term is called a CNS polynomial if every element in $\mathbb{Z}[X]/P$ has a polynomial representative with coefficients in the set $\{0, 1, \ldots, |P(0)| - 1\}$. The CNS property of a given polynomial can be decided algorithmically [9,17,35], and we tacitly use this fact in the sequel.

It is well-known that the set $\mathcal{C}$ of all CNS polynomials is not closed under addition of positive integers. K. Scheicher and J. Thuswaldner [33, Section 7] published the first example of a CNS polynomial P such that $P + 1$ is not a CNS polynomial; more examples can be found in the sequel. Clearly, Akiyama's Conjecture means that the CNS property is preserved provided that the added integer is large enough. We observe that the truth of this conjecture would imply necessary conditions for CNS polynomials provided that these conditions have been established for CNS polynomials with a strictly dominant constant term. Recall that a polynomial is said to have a strictly dominant (dominant, resp.) constant term if the modulus of its constant term is strictly larger than (greater than or equal to, resp.) the sum of the moduli of its remaining coefficients (cf. [18]).

Akiyama's Conjecture is supported by several straightforward consequences of well-known results collected in Proposition 2.2 below. In its proof we exploit the following obvious, but useful fact.

Lemma 2.1. *Let P be a monic integer polynomial of positive degree with a positive strictly dominant constant term. Then $P \in \mathcal{C}$ if and only if $P + 1 \in \mathcal{C}$.*

Proof. Let $d = \deg(P)$ and $e \in \{0, 1\}^d$. Then the orbits of e under the iterates of τ_P and τ_{P+1} coincide (the reader is referred to [2] for the definition and the necessary background). This means in particular that they have the same set of periodic elements, and in view of [15, Lemma 3.1] this fact implies our assertion. □

Proposition 2.2. *Let $P = \sum_{i=0}^{d} p_i X^i$ be a CNS polynomial of degree d. Then Akiyama's Conjecture holds for P provided that one of the following conditions holds.*

(i) $p_2, \ldots, p_{d-1} \geq 0$,

(ii) $p_k < 0$ *for exactly one* $k \in \{1, \ldots, d-1\}$ *and*

$$\sum_{1 \leq ki \leq d} p_{ki} \geq 0. \tag{2.1}$$

[1] CNS polynomials are named complete base polynomials in [17].

(iii) *P is a trinomial,*

(iv) $d \leq 3$,

(v) *P has a dominant constant term and $d \leq 5$,*

(vi) *P has a strictly dominant constant term.*

(vii) *P is weakly Hurwitz stable.*

(viii) *$d \geq 4$ and P has exactly one non-real root ρ which satisfies*

$$0 < \Re(\rho) \leq -\frac{1}{2}\sum_{i=1}^{d-2} r_i$$

and

$$a_{i-1} \leq \frac{|\rho|^2}{2\Re(\rho)} a_i \qquad (i = 2, \ldots, d-2),$$

where we set

$$\sum_{i=0}^{d-2} a_i X^i := \prod_{i=1}^{d-2} (X - r_i)\,,$$

and $r_1, \ldots, r_{d-2}$ are the real roots of P.

Proof. (i) In view of [4, Lemma 2] clear by [5, Theorem 3.2] or [33, Theorem 5.8].
(ii) Clear by [5, Theorem 3.5].
(iii) Obvious by [11, Theorem 3].
(iv) This is immediate by the well-known characterization of linear (e.g., see [20]) and quadratic (e.g., see [20,23]) CNS polynomials and Gilbert's conditions for cubic CNS polynomials ([3, Theorem 3.1]).
(v) Clear by [5] and [15].
(vi) This is an immediate consequence of Lemma 2.1.
(vii) Recall that we have $\Re(\rho) \leq 0$ for every root ρ of P (e.g., see [10]). Thus all coefficients of P are non-negative and our claim is clear by (i).
(viii) Observing

$$P = X^d + (a_{d-3} - 2\Re(\rho))X^{d-1} + \sum_{i=1}^{d-2}(|\rho|^2 a_i - 2\Re(\rho)a_{i-1})X^i + |\rho|^2 a_0$$

and

$$a_{d-3} = -\sum_{i=1}^{d-2} r_i$$

our claim follows from (i). □

Let us give an example how Akiyama's Conjecture can be exploited to derive a necessary condition on CNS polynomials. Consider $P = \sum_{i=0}^{d} p_i X^i \in \mathcal{C}$ such that $p_k < 0$ for exactly one $k \in \{1, \ldots, d-1\}$. If Akiyama's Conjecture holds true then

(2.1) must be satisfied: Indeed, then there exists some[2] $n \in \mathbb{N}$ such that $P + n \in \mathcal{C}$ with strictly dominant constant term, and [5, Theorem 3.5] settles our claim.

Proposition 2.2, results of [5] and further numerical examples suggest the following.

Conjecture 2.3. Let $P = \sum_{i=0}^{d} p_i X^i \in \mathcal{C}$ with $d \geq 2$ and $(p_1, \dots, p_{d-1}) \neq (0, \dots, 0)$. If $m := \max\{i \in \{1, \dots, d-1\} \ : \ p_i \neq 0\}$ then $p_m \geq -1$.

By [4, Theorem 3] Conjecture 2.3 holds under the dominant condition, and the truth of Akiyama's Conjecture would imply this conjecture for every CNS polynomial.

In view of [4, Lemma 2] Akiyama's Conjecture is equivalent to the statement that the constant

$$\alpha(f) := \inf\{N \in \mathbb{N} \ : \ f + n \in \mathcal{C} \text{ for all } n \geq N\} \qquad (f \in \mathcal{M})$$

is finite for every CNS polynomial f; here we put

$$\mathcal{M} := \{f \in \mathbb{Z}[X] \ : \ f \text{ monic, } f(1) \geq f(0) \geq 2 \text{ and } f(-1) \geq 1\}.$$

Trivially, the set $\mathcal{M}$ is closed under multiplication. Further, $\mathcal{M}$ is obviously closed under addition of positive integers, and we recall that $\mathcal{C}$ is contained in $\mathcal{M}$. Indeed, let $f \in \mathcal{C}$. Then f is expansive by [30, Theorem 6.1][3], therefore we have $f(0) \geq 2$ by [20, Proposition 6][4], finally we have $f(1) \geq f(0)$ by [4, Lemma 2] and we conclude $f(-1) \geq 1$.

In the following we collect some easy properties of the map $\alpha\colon \mathcal{M} \to \mathbb{N} \cup \{\infty\}$. To this end, we introduce a function $\delta\colon \mathcal{M} \to \mathbb{N}_0$ which might be regarded as the distance of a polynomial to the nearest suitable polynomial with a strictly dominant constant term. Specifically, we set

$$\delta\big(\sum_{i=0}^{d} a_i X^i\big) := \max\left\{1 - a_0 + \sum_{i=1}^{d} |a_i|\,,\ 0\right\}.$$

Proposition 2.4. *Let $f \in \mathcal{M}$.*

(i) *For $n \in \mathbb{N}_0$ we have*

$$\alpha(f) = n + \alpha(f + n).$$

[2] $\mathbb{N}$ is the set of positive rational integers and $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

[3] [20, Corollary 4] shows the every root of an irreducible CNS polynomial lies outside the open unit disk. In the respective part of the proof of [30, Theorem 6.1] the assumption "without multiple roots" is not used.

[4] Irreducibility is not used in the proof of [20, Proposition 6].

(ii) *For $n \in \mathbb{N}$ we have*

$$\alpha(f(X^n)) = \alpha(f(X)) \,.$$

In particular, $f(X^n)$ satisfies Akiyama's Conjecture if and only if $f(X)$ does.

(iii) *Let $f \in \mathcal{C}$. Then $\alpha(f) < \infty$ if and only $f + \delta(f) \in \mathcal{C}$. In this case, we have*

$$\alpha(f) \leq \delta(f) + 1 \,. \tag{2.2}$$

Proof. (i) Clear by the definition.

(ii) Clear by [11, Theorem 1].

(iii) If $\alpha(f) < \infty$ then we can find some n such that $f + n$ is a CNS polynomial with strictly dominant constant term. Since $f + \delta(f)$ also has a strictly dominant constant term our assertion is clear by Lemma 2.1.

Conversely, if $f + \delta(f) \in \mathcal{C}$ then we have $f + \delta(f) + n \in \mathcal{C}$ for all $n \in \mathbb{N}$ by Lemma 2.1, hence

$$\alpha(f + \delta(f)) = 1,$$

and therefore (2.2) by (i). □

Remark 2.5. (i) *The bound for α given in Proposition 2.4 can certainly be improved for particular classes of CNS polynomials. For instance, let $P \in \mathcal{C}$ with $P(0) = 2$ and degree at most* 11*. Then we have*

$$\alpha(P) \leq \delta(P).$$

Indeed, apply [33, Theorem 5.8] *to the lists of these CNS polynomials in* [28, Section 2.5] *and* [16, Section 4].

(ii) *Let $f \in \mathcal{M}$ be a trinomial. The well-known characterization of CNS trinomials* [11] *shows $\alpha(f) \in \{1, 2, 3, \infty\}$; in particular, $f \in \mathcal{C}$ yields $\alpha(f) = 1$.*

This remark also shows that the CNS property is sensitive for inserting zeroes into the sequence of the coefficients of polynomials. Indeed, consider the CNS trinomial $X^4 - X^2 + 3$ with $\alpha(X^4 - X^2 + 3) = 1$, but $X^5 - X^2 + 3 \in \mathcal{M} \setminus \mathcal{C}$ with $\alpha(X^5 - X^2 + 3) = \infty$.

We now present a bound for α for a polynomial in our larger set $\mathcal{M}$.

Proposition 2.6. *Let $P = \sum_{i=0}^{d} p_i X^i \in \mathcal{M}$ with degree $d \geq 2$ and assume that there is exactly one index k such that $p_k < 0$. If*

$$\sum_{1 \leq ki \leq d} p_{ki} \geq 0$$

then inequality (2.2) *holds.*

Proof. Clear by [15, Theorem 3.5]. □

To conclude, let us consider some more examples to motivate further conjectures.

Example 2.7. (i) *Exploiting the well-known characterization of linear and quadratic CNS polynomials we have*

$$\alpha(X^d + c) = \alpha(X^2 + bX + c) = 1 \qquad (d \in \mathbb{N},\ c \geq 2,\ -1 \leq b \leq c).$$

(ii) *For* $P := X^3 + 31X^2 - 8X + 31$ *we have* $P \in \mathcal{M} \setminus \mathcal{C}$ *and* $\alpha(P) = 3$.

(iii) *For* $n \geq 3$ *we have*

$$P := X^3 + 2nX^2 - nX + 3n \in \mathcal{M} \setminus \mathcal{C}$$

by [3, Counterexamples]. *We infer* $\alpha(P) = 1$ *from* [15, Theorem 3.5], *and numerical experiments suggest*

$$\alpha(P - \lfloor n/2 \rfloor) = n - 1 \qquad (n \geq 3).$$

(iv) *For*

$$P_n = X^3 + (15n + 50)X^2 + (22n + 73)X + 17n + 55 \qquad (n \in \mathbb{N}_0)$$

we have

$$2 \leq \alpha(P_n) \leq 5n + 18$$

by [14, Proposition 10] *and* [13, Corollary 6]. *Further, we suspect* $\alpha(P_n) = 2$.

(v) *For* $a + b \geq 0$, $b \geq -1$ *and* $c \geq 2$ *we have*

$$\alpha(X^4 - X^3 + aX^2 + bX + c) = \infty$$

by [5, Theorem 5.4].

(vi) *If* $a > 0$ *and* $1 < k < d$ *then* $X^d - aX^k + c \notin \mathcal{C}$ *by* [11, Theorem 3], *hence*

$$\alpha(X^d - aX^k + c) = \infty \qquad (c \geq 2).$$

Note that in case $a = 1$ *the condition of* [4, Lemma 5] *is satisfied.*

(vii) *The author is indebted to A. Pethő* [31] *for the following examples:*

$$X^3 + 98X^2 + 143X + p_0 \in \mathcal{C}\ (p_0 = 106, \ldots, 109),\ X^3 + 98X^2 + 143X + 110 \notin \mathcal{C}$$

and

$$X^3 + 410X^2 + 611X + p_0 \in \mathcal{C}\ (p_0 = 417, \ldots, 473),\ X^3 + 410X^2 + 611X + 474 \notin \mathcal{C}.$$

Now, using Proposition 2.2 one can easily check

$$\alpha(X^3 + 98X^2 + 143X + 106) = 5 \qquad \textit{and} \qquad \alpha(X^3 + 410X^2 + 611X + 417) = 57\,.$$

Note that in view of Proposition 2.4 (ii) this example shows that for any positive n there exists a CNS polynomials P of degree $3n$ with $\alpha(P) = 5$.

(viii) *For the CNS polynomials $P = X^2 - X + 2$ and $Q = X^2 - X + 3$ we have*

$$\alpha(P) = \alpha(Q) = 1\,,$$

but $\alpha(PQ) = \infty$, since for $n \geq 6$ the orbit of $(1,0,0,1) \in \mathbb{Z}^4$ under the iterates of τ_{PQ+n} is periodic (of period length 4).

In view of these examples we are lead to the following speculations.

Conjecture 2.8. (i) For every $n \in \mathbb{N}$ there exists a cubic CNS polynomial P such that

$$\alpha(P) = n\,.$$

(ii) For every cubic CNS polynomial P with negative linear coefficient we have $\alpha(P) = 1$.

Acknowledgement. The author is indebted to A. Kovács for pointing out that the analogue of Akiyama's Conjecture for symmetric CNS polynomials (see [6] for the definition) holds by using an easy application of [19, Theorem 8]. Further, the author is grateful to the anonymous referee whose comments helped to improve the first version of this note.

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(3) (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(1) (2003), 402-415.

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

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

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

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

[8] V. Berthé, *Numeration and discrete dynamical systems*, Computing, 94(2-4) (2012), 369-387.

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

[10] J. Borcea and P. Brändén, *The Lee-Yang and Pólya-Schur programs II, Theory of stable polynomials and applications*, Comm. Pure Appl. Math., 62(12) (2009), 1595-1631.

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

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

[13] H. Brunotte, *A unified proof of two classical theorems on CNS polynomials*, Integers, 12(4) (2012), 709-721.

[14] H. Brunotte, *Unusual CNS polynomials*, Math. Pannon., 24(1) (2013), 125-137.

[15] H. Brunotte, *Small degree CNS polynomials with dominant condition*, Math. Pannon., 25(1) (2014/15), 113-133.

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

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

[18] A. Dubickas, *Roots of polynomials with dominant term*, Int. J. Number Theory, 7(5) (2011), 1217-1228.

[19] L. Germán and A. Kovács, *On number system constructions*, Acta Math. Hungar., 115(1-2) (2007), 155-167.

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

[21] 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.

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

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

[24] I. Kátai and B. Kovács, *Canonical number systems in imaginary quadratic fields*, Acta Math. Acad. Sci. Hungar., 37(1-3) (1981), 159-164.

[25] I. Kátai and J. Szabó, *Canonical number systems for complex integers*, Acta Sci. Math. (Szeged), 37(3-4) (1975), 255-260.

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

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

[28] A. Kovács, *Generalized binary number systems*, Ann. Univ. Sci. Budapest. Sect. Comput., 20 (2001), 195-206.

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

[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, Private communication, 2000.

[32] 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", S. Katayama, C. Levesque, and T. Nakahara, eds., Saga Univ., Saga, (2004), 115-125.

[33] K. Scheicher and J. M. Thuswaldner, *On the characterization of canonical number systems*, Osaka J. Math., 41(2) (2004), 327-351.

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

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

Horst Brunotte
Haus-Endt-Straße 88
D-40593 Düsseldorf, Germany
e-mail: brunoth@web.de