NEW CRITERIA FOR CANONICAL NUMBER SYSTEMS

SHIGEKI AKIYAMA AND HUI RAO

Abstract. Let $P(x) = x^d + p_{d-1}x^{d-1} + \cdots + p_0$ be an expanding monic polynomial with integer coefficients. If each element of $\mathbb{Z}[x]/P(x)\mathbb{Z}[x]$ has a polynomial representative with coefficients in $[0, |p_0| - 1]$ then $P(x)$ is called a canonical number system generating polynomial, or a CNS polynomial in short. A method due to Hollander [6] is employed to study CNS polynomials. Several new criteria for canonical number system generating polynomials are given and a conjecture of S.Akiyama & A.Pethő [3] is proved. The known results, especially an algorithm of H. Brunotte's in [4] and a recent work of K. Scheicher & J.M.Thuswaldner [15], can be derived by this new method in a simpler way.

1. Introduction

Let $P(x) = p_d x^d + p_{d-1}x^{d-1} + \cdots + p_0$ be a polynomial of x with integer coefficients and $p_d = 1$. Let R be the quotient ring $\mathbb{Z}[x]/P(x)\mathbb{Z}[x]$. As a $\mathbb{Z}$-module, R is naturally isomorphic to $\mathbb{Z}^d$ and each element ξ of R is represented uniquely in the form

$$\xi \equiv \sum_{i=0}^{d-1} a_i x^i \pmod{P(x)} \tag{1}$$

with $a_i \in \mathbb{Z}$. If an element $\xi \in R$ has an expression of the form

$$\xi \equiv b_0 + b_1 x + \cdots + b_{M-1}x^{M-1} \pmod{P(x)}$$

with $a_i \in [0, |p_0| - 1] \cap \mathbb{Z}$, then we say that ξ has a *canonical expression.* If every element $\xi \in R$ has a canonical expression, then $P(x)$ is called a *canonical number system generating polynomial*, or a *CNS polynomial* in short. Let $T : R \to R$ be a map defined by

$$T(\xi) \equiv \sum_{i=0}^{d-1} \left(a_{i+1} - p_{i+1} \left[\frac{a_0}{p_0} \right] \right) x^i \pmod{P(x)}.$$

1991 *Mathematics Subject Classification.* 11A63, 37B10.

Key words and phrases. Canonical number system, radix representation, symbolic dynamics.

The first author is supported by the Japanese Ministry of Education, Culture, Sports, Science and Technology, Grand-in Aid for fundamental research, 12640017, 2001.

The second author is supported by the Japan Society for the Promotion of Science.

Here we put $a_d = 0$. Let $\alpha = x \bmod P(x)$. Then $R/(\alpha)$ is isomorphic to $\mathbb{Z}/p_0\mathbb{Z}$ as a $\mathbb{Z}$-module. Denote this isomorphism as $\tau : R/(\alpha) \to \mathbb{Z}/p_0\mathbb{Z}$. Then the map T can be rewritten as

$$T(\xi) = (\xi - a)/\alpha$$

where $a \in [0, |p_0| - 1]$ is the representative of $\tau(\xi)$. Denote by T^m the m-th iteration of the map T. ξ has a canonical expression (obviously this expression is unique) if and only if there is a non-negative integer M such that $T^M(x) = 0$.

When $P(x)$ is irreducible, R is identified with $\mathbb{Z}[\alpha]$ with a root α of $P(x)$. This case had been extensively studied. In this case, a pair $(\alpha, \{0, 1, \dots, |p_0| - 1\})$ is said to form a *canonical number system* when $P(x)$ is a CNS polynomial. Here we only refer to the original studies in I. Kátai & J. Szabó [7], I. Kátai & B. Kovács [9], [10], W. Gilbert [5] and B. Kovács & A. Pethő [12].

A. Pethő [13] generalized this study to non irreducible polynomials. It is well known that (see [12])

If $P(x)$ is a CNS polynomial, then $P(x)$ is expanding (,that is, all root of $P(x)$ has modulus greater than one) and $P(x)$ has no positive real root. Especially the last condition implies

$$p_0 > 1. \tag{2}$$

It is not hard to work out an algorithm to determining whether a polynomial is a CNS polynomial. In Section 2, we will give such an algorithm. However, we want to see whether a given polynomial is a CNS polynomial or not by just looking its coefficients. Many papers are devoted to this problem. Generalizing former results of I. Kátai & B. Kovács [9], [10], B.Kovács proved

If $p_0 \geq 2$ and

$$p_d \leq p_{d-1} \leq \cdots \leq p_0 \tag{3}$$

hold, then $P(x)$ is a CNS polynomial (see also [5], [13]*) provided $P(x)$ is irreducible.*

In S. Akiyama & A.Pethő [3], it is proved that

$$p_2 \geq 0, p_3 \geq 0, \dots, p_{d-1} \geq 0, \sum_{i=1}^{d} p_i \geq 0, \text{ and } p_0 > 2\sum_{i=1}^{d} |p_i|$$

imply that $P(x)$ is a CNS polynomial. In the same paper, they conjectured that the last condition can be relaxed to

$$p_0 > \sum_{i=1}^{d} |p_i|. \tag{4}$$

In this paper, we employ a method of Hollander to study CNS polynomials (He deviced the method for studying of Pisot number system). In section 3, we give two criteria of CNS polynomials. First we will give an affirmative answer to the conjecture of [3] and also deal with a slightly generalized situation

$$p_0 \geq \sum_{i=1}^{d} |p_i| \tag{5}$$

in Theorem 3.2. Second, when $P(x)$ is a polynomial with (5) and has exactly one negative coefficient, $P(x)$ is a CNS polynomial or not is characterized by one inequality (see Theorem 3.5).

Section 4 is devoted to Bronotte's algorithm. H. Brunotte [4] discovered a nice method to determine CNS polynomials. The original argument looks not simple. We apply our method and give a short proof of Brunotte's Lemma (See Lemma 4.1). Also Theorem 4.2 shows that for any expanding $P(x)$, Brunotte's method actually gives a finite and efficient *algorithm* to determine CNS polynomials. Moreover, if the dominant condition (5) is assumed, then the algorithm becomes simpler (Theorem 4.3).

While preparing our paper, we are informed that similar results were shown recently by a different approach by K. Scheicher & J.M.Thuswaldner [15]. We would like to express our deep gratitude for their correspondences. It seems worthy to describe in detail the difference of ideas. The main difference is in the ways of description. Our way is algebraic having a flavor of symbolic dynamics. The idea of proofs is originally due to the thesis of M.Hollander [6]. On the other hand, their way depends on the transducer automata. Nevertheless, the basic ideas of two papers are close.

Corollary 4.4 is first proved by [15]. As a generalization of their result, we relax the condition (4) to (5) and get Theorem 4.3. Inspired by their result, easy characterizations of CNS polynomials with (4) of degree not larger than 5 will be given in §5. Our idea in §5 is to use not only Corollary 4.4 but also all known necessary conditions to simplify our arguments. It is shown that the known necessary conditions are not sufficient to characterize degree five CNS polynomials, even if we assume (4).

2. Algorithm.

Here we give a basic proposition.

Proposition 2.1. *Assume that $P(x)$ is an expanding polynomial. Then for any $\xi \in R$, the sequence*

$$\xi, T(\xi), T^2(\xi), \dots$$

is eventually periodic.

Remark 2.2. I. Kátai & I. Kőrnyei [8] proved this in the case when $P(x)$ is expanding and irreducible.

Proof. Let $P(x)$ be an expanding polynomial as in §1 and A be its companion matrix, that is,

$$A = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -p_0 \\ 1 & 0 & 0 & \dots & 0 & -p_1 \\ 0 & 1 & 0 & \dots & 0 & -p_2 \\ & & \vdots & & & \vdots \\ 0 & \dots & 0 & 1 & 0 & -p_{d-2} \\ 0 & \dots & \dots & 0 & 1 & -p_{d-1} \end{pmatrix}.$$

Let D be a complete representative system of $\mathbb{Z}^d/A\mathbb{Z}^d$ of the form

$$D = \{k\mathbf{v} \mid k = 0, 1, \dots, p_0 - 1\}$$

with $\mathbf{v} = (0, \dots, 0, 1)$. Let $\xi \in R$ and

$$\xi = \xi_0 + \xi_1\alpha + \dots + \xi_{d-1}\alpha^{d-1}.$$

We can embed R into $\mathbb{R}^d$ by

$$\pi(\xi) := \begin{pmatrix} \xi_0 \\ \xi_1 \\ \vdots \\ \xi_{d-1} \end{pmatrix}.$$

It is easy to check $\pi(\alpha\xi) = A\pi(\xi)$. For any $y \in \mathbb{Z}^d$ there is a unique $v \in D$ such that $A^{-1}(y - v)$ is an integer. Define

$$S(y) := A^{-1}(y - v).$$

To prove $\{T^m(\xi)\}_{m\geq 0}$ is eventually periodic, we only need to show that $\{S^m(y)\}_{m\geq 0}$ is eventually periodic. As A is expanding there exists a positive integer k so that the map $f_k : x \to A^{-k}x$ is a contraction [1] on $\mathbb{R}^d$. This implies that $\{S^m(y)\}_{m\geq 0}$ is a bounded sequence in $\mathbb{Z}^d$, and thus it is eventually periodic. □

Let $\mathcal{P}$ be the set of purely periodic elements in R, i.e.,

$$\mathcal{P} = \{\xi \in R \mid \exists M > 0 \quad T^M(\xi) = \xi\}. \tag{6}$$

By Proposition 2.1, an expanding polynomial $P(x)$ is a CNS polynomial if and only if $\mathcal{P} = \{0\}$. It is important to get an algorithmic bound for searching elements of $\mathcal{P}$. In fact, it is easily seen that if $P(x)$ has no multiple root, then

$$\mathcal{P} \subset \left\{ \xi \in R \;\middle|\; |\xi(\alpha)| \leq \frac{|p_0| - 1}{|\alpha| - 1} \text{ for all root } \alpha \text{ of } P(x) \right\}, \tag{7}$$

(see [12], [8] and [13]). Here $\xi(\alpha)$ is well defined by substituting the indeterminate x with α.

[1] Note that f_1 is not necessary a contraction.

In the following, we shortly discuss a way to give an explicit upper bound suitable for computation, and this will give us an effective algorithm for determining whether a polynomial is a CNS polynomial.

Decompose the expanding polynomial $P(x) = \prod_{i=1}^{n}(x-\alpha_i)^{e_i+1}$ into factors in $\mathbb{C}(x)$. For $\xi \in R$, let

$$T^m(\xi) = \frac{T^{m-1}(\xi) - a_{m-1}}{\alpha}$$

where $a_{m-1} \in [0, |p_0|-1] \cap \mathbb{Z}$ is a representative of $\tau(T^{m-1}(\xi))$. Then we have

$$\xi = a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} + \alpha^m T^m(\xi). \tag{8}$$

We wish to give an upper bound of the set $\{T^m(\xi)\}_{m=0,1,\dots}$. Putting $\xi = E(x) \bmod P(x)$ and $T^m(\xi) = F_m(x) \bmod P(x)$, then (8) is rewritten into:

$$E(x) = a_0 + a_1 x + \cdots + a_{m-1}x^{m-1} + x^m F_m(x) + G_m(x)P(x), \tag{9}$$

for some $G_m(x) \in \mathbb{Z}[x]$. We claim that, for any $\varepsilon > 0$,

$$\left|\frac{d^j}{dx^j}F_m(\alpha_i)\right| \le K_j(\alpha_i) + \varepsilon \tag{10}$$

for a sufficiently large m where

$$K_j(\alpha_i) = \frac{j!(|p_0|-1)}{(|\alpha_i|-1)^{1+j}}.$$

This is shown by differentiating (9) several times and using an estimate:

$$\left|\sum_{\ell=1}^{m} a_{m-\ell}\frac{(-\ell)_j}{\alpha_i^{j+\ell}}\right| \le (|p_0|-1)\sum_{\ell=1}^{m}\frac{\ell(\ell+1)\dots(\ell+j-1)}{|\alpha_i|^{j+\ell}} = K_j(\alpha_i)$$

where

$$(r)_j = \begin{cases} r(r-1)\dots(r-j+1) & , \quad j \ge 1 \\ 1 & , \quad j = 0. \end{cases}$$

On the other hand by (1), there exist integers $c_{m,i}$ that

$$F_m(x) = \sum_{i=0}^{d-1} c_{m,i}x^i.$$

Then we can deduce an upper bound of $c_{m,i}$ from (10). This shows that $\{T^m(\xi)\}_{m=0,1,\dots}$ is contained in a bounded set which gives an alternative proof of Proposition 2.1. As $\xi = E(x) \bmod P(x)$ we may define, for $i = 1, \dots, e_i$,

$$\xi^{(j)}(\alpha_i) = \left.\frac{d^j}{dx^j}E(x)\right|_{x=\alpha_i}.$$

Then we see

Proposition 2.3.

$$\mathcal{P} \subset \left\{ \xi \in R \;\middle|\; |\xi^{(j)}(\alpha_i)| \le K_j(\alpha_i) \text{ for } i = 1, 2, \dots, n,\ j = 0, \dots, e_i \right\}, \tag{11}$$

Proof. If $\xi \in \mathcal{P}$, then there exist a positive integer M that $\xi = T^M(\xi)$. Thus $\xi = T^m(\xi) = F_m(x) \bmod P(x) \in \mathcal{P}$ for any m which is a multiple of M. This means that $|\xi^{(j)}(\alpha_i)| \le K_j(\alpha_i) + \varepsilon$ for any $\varepsilon > 0$, showing the assertion. □

3. Sufficient conditions on CNS

Put $\alpha = x \bmod P(x)$. Then by (1), R has a base $\{1, \alpha, \alpha^2, \dots, \alpha^{d-1}\}$ as a $\mathbb{Z}$-module. We introduce a different base $\{w_1, w_2, \dots, w_d\}$, which already appeared in [4] [3], [15] and implicitly in [5]:

$$\begin{pmatrix} w_1 \\ w_2 \\ w_3 \\ \vdots \\ w_d \end{pmatrix} = \begin{pmatrix} p_d & 0 & \dots & \dots & \dots & 0 \\ p_{d-1} & p_d & 0 & \dots & \dots & 0 \\ p_{d-2} & p_{d-1} & p_d & 0 & \dots & 0 \\ & & & \vdots & & \\ p_1 & p_2 & p_3 & \dots & p_{d-1} & p_d \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \\ \vdots \\ \alpha^{d-1} \end{pmatrix}.$$

Define $\iota : \mathbb{Z}^d \to R$ by $\iota(z_1, z_2, \dots, z_d) = \sum_{i=1}^d z_i w_i$ and

$$z_{d+1} = -\left[\frac{\sum_{i=1}^d z_i p_{d-i+1}}{p_0} \right].$$

Replace $(z_1, z_2, \dots, z_d)$ by $(z_2, z_3, \dots, z_{d+1})$, where z_{d+1} is determined by the above formula. In this way, once $(z_1, z_2, \dots, z_d) \in \mathbb{Z}^d$ is given, it defines an infinite sequence $(z_1, z_2, \dots, z_d, z_{d+1}, \dots)$. Let $\sigma : \mathbb{Z}^d \to \mathbb{Z}^d$ be a 'shift' map:

$$\sigma(z_1, z_2, \dots, z_d) = (z_2, z_3, \dots, z_{d+1}).$$

Then we can easily confirm the following commutative diagram:

$$\begin{tikzcd} \mathbb{Z}^d \arrow[r, "\sigma"] \arrow[d, "\iota"'] & \mathbb{Z}^d \arrow[d, "\iota"] \\ R \arrow[r, "T"'] & R \end{tikzcd} \tag{12}$$

Hereafter we employ the method due to M. Hollander [6] developed for a different number system attached to Pisot numbers. His main idea is to interpret the map T as a shift on bi-infinite words generated by $\mathbb{Z}$. Next proposition is merely a consequence of the definition of z_i but we restate it to emphasize his idea.

Proposition 3.1. *We have*

$$0 \le z_i p_d + z_{i+1} p_{d-1} + \cdots + z_{i+d-1} p_1 + z_{i+d} p_0 < p_0,$$

and z_{d+i} is determined uniquely by this condition.

Theorem 3.2. *Assume that $P(x)$ is an expanding polynomial whose coefficients satisfy $p_2 \geq 0, p_3 \geq 0, \dots, p_{d-1} \geq 0, \sum_{i=1}^{d} p_i \geq 0$ and the dominant condition $p_0 > \sum_{i=1}^{d} |p_i|$. Then $P(x)$ is a CNS polynomial. The dominant condition can be replaced by $p_0 \geq \sum_{i=1}^{d} |p_i|$ if one of the following conditions holds:*

(1) $p_1 < 0$,
(2) $p_i > 0$ *for all* $i = 1, \dots, d-1$.

Remark 3.3. The dominant condition $p_0 > \sum_{i=1}^{d} |p_i|$ guarantees that the polynomial $P(x)$ is expanding (c.f. Lemma 1 of [3].)

Remark 3.4. The above supplementary condition is necessary when $p_0 = \sum_{i=1}^{d} |p_i|$. For example, $x^3 + 3x^2 + 4$ is not a CNS polynomial. H. Brunotte kindly pointed out an error in the original manuscript and the example is also due to him.

The proof of Theorem 3.2 is divided into two parts. First we settle the case $p_1 \geq 0$. The case $p_1 < 0$ will be shown in a more generalized form in Theorem 3.5.

Proof of Theorem 3.2 when $p_1 \geq 0$. Recall that $\mathcal{P}$ is the set of purely periodic elements in R defined by (6). To prove $P(x)$ is CNS polynomial, it suffices to show that $\mathcal{P} = \{0\}$. Otherwise let $\xi = \sum_{i=0}^{d-1} z_i w_i$ be a non zero element of $\mathcal{P}$ and $z_0 z_1 z_2 \dots$ be the infinite sequence determined by Proposition 3.1. Since ξ is a non zero purely periodic element, we have $z_0 z_1 z_2 \dots \neq 0^\infty$ and it is purely periodic. So we can extend it to be a bi-infinite word $\Xi = \dots z_{-2} z_{-1} z_0 z_1 z_2 \dots$ and it is easy to see that

$$0 \leq z_i p_d + z_{i+1} p_{d-1} + \dots + z_{i+d-1} p_1 + z_{i+d} p_0 < p_0 \tag{13}$$

hold for all $i \in \mathbb{Z}$.

First we argue that there exist $i \in \mathbb{Z}$ such that $z_i < 0$. For if $z_i \geq 0$ for all $i \in \mathbb{Z}$, then for an index i such that $z_{i+d} > 0$ we have

$$z_i p_d + z_{i+1} p_{d-1} + \dots + z_{i+d-1} p_1 + z_{i+d} p_0 \geq p_0,$$

which is a contradiction.

Let $\min_{i \in \mathbb{Z}} z_i = -\kappa \leq -1$ and $\max_{i \in \mathbb{Z}} z_i = \eta$. Note that both κ and η are finite since Ξ is a periodic word. Now we take i such that $z_{i+d} = -\kappa$. Then by the left side of (13),

$$z_i p_d + z_{i+1} p_{d-1} + \dots + z_{i+d-1} p_1 \geq \kappa p_0 \tag{14}$$

$$\eta(p_d + p_{d-1} + \dots + p_1) \geq \kappa p_0 \tag{15}$$

which yields

$$\eta > \kappa \geq 1 \tag{16}$$

provided $p_0 > \sum_{i=1}^{d} |p_i|$.

We shall show that the inequality (16) holds in case $p_i > 0$ for $i = 1, \dots, d-1$ and $p_0 = \sum_{i=1}^{d} p_i$. The above argument shows

$$\eta \geq \kappa \geq 1.$$

Assume $\eta = \kappa$. By (14) and (15), $\eta = \kappa$ and $p_i > 0$ implies

$$z_i = z_{i+1} \cdots = z_{i+d-1} = \eta. \tag{17}$$

Let us consider (13) with $i \to i-1$. By (17) and the right side of (13),

$$\begin{aligned} z_{i-1} + \eta(p_{d-1} + p_{d-2} + \cdots + p_0) &< p_0 \\ -\kappa \leq z_{i-1} &< -\eta(p_{d-1} + p_{d-2} + \cdots + p_1) + (1-\eta)p_0 \\ \kappa &> \eta(p_{d-1} + p_{d-2} + \cdots + p_1). \end{aligned}$$

As $p_{d-1} + p_{d-2} + \cdots + p_1 > 0$ we get $\kappa > \eta$ which is absurd. This shows $\eta > \kappa$ in any cases.

Let j be an index such that $z_{j+d} = \eta$. Now we use (13) again with $i = j$ to get:

$$\begin{aligned} z_j p_d + z_{j+1} p_{d-1} + \cdots + z_{j+d-1} p_1 &< (1-\eta)p_0 \leq -\kappa p_0 \\ -\kappa(p_d + p_{d-1} + \cdots + p_1) &< -\kappa p_0, \end{aligned}$$

which yields $p_d + p_{d-1} + \cdots + p_1 > p_0$. This contradicts our assumption. Hence $\mathcal{P} = \{0\}$. $\square$

Reviewing the above proof, we get a necessary condition for $P(x)$ to be a CNS polynomial. Let k be an integer, $0 < k \leq d$, and consider the sum

$$C_k(\ell) = \sum_{0 \leq ki+\ell \leq d} p_{ki+\ell}, \quad \ell = 0, 1, \dots, k-1.$$

For certain k, if $C_k(\ell) \in [0, p_0 - 1]$ for all ℓ, then $P(x)$ is not a CNS polynomial. Indeed, a bi-infinite word

$$\Xi = (\overbrace{00...0}^{k-1}1)^{\infty}$$

obviously gives an element of $\mathcal{P}$. Therefore, if $P(x)$ is a CNS polynomial then for any k, $0 < k \leq d$, there exist ℓ that $C_k(\ell) \notin [0, p_0 - 1]$, which we call the *$k$-subsum condition.*

Since $P(x)$ has no positive roots, we see $\sum_{i=0}^{d} p_i \geq 0$. Hence 1-subsum condition is nothing but

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

appeared in the condition of Theorem 3.2. This 1-subsum condition is also seen in Lemma 4 of [3].

Now let us treat polynomials having an isolated negative coefficient $p_k < 0$ and satisfying the *dominant condition* $p_0 \geq \sum_{i=1}^{d} |p_i|$. Under these assumptions, $C_k(\ell)$ ($\ell > 0$) must be in $[0, p_0 - 1]$. Thus $C_k(0) \geq p_0$, i.e.,

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

is necessary for $P(x)$ to be a CNS polynomial (Note that this implies that k is not greater than $d/2$). Theorem 3.5 shows that this condition is also sufficient.

Theorem 3.5. *Assume that $P(x)$ is an expanding polynomial with the dominant condition $p_0 \geq \sum_{i=1}^{d} |p_i|$ whose coefficients are non-negative except $p_k < 0$ for a single index $0 < k < d$. Then $P(x)$ is a CNS polynomial if and only if*

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

As stated before, the proof of Theorem 3.2 for the case $p_1 < 0$ is completed at the same time.

Proof of Theorem 3.5. Suppose $P(x)$ is a polynomial satisfying the assumptions of the theorem and it is not a CNS polynomial. Then similar to the proof of Theorem 3.2, we can construct a non-zero bi-infinite periodic word $\Xi = \dots z_{-2} z_{-1} z_0 z_1 z_2 \dots$ satisfying (13). We shall derive a contradiction from the existence of such a word.

Let $\kappa = 0$ if $z_i \geq 0$ for all $i \in \mathbb{Z}$. Otherwise we define $-\kappa = \min_{i \in \mathbb{Z}} z_i$. Let $\eta = \max_{i \in \mathbb{Z}} z_i$.

First we claim that $\eta > \kappa$. In case of $\kappa = 0$ this is trivial. Suppose $\kappa < 0$. Let i be an index such that $z_{i+d} = -\kappa$. Without loss of generality, we assume $i = 0$. Then

$$\begin{aligned} 0 &\leq z_0 p_d + z_1 p_{d-1} + \cdots + z_{d-1} p_1 + z_d p_0 < p_0 && (18) \\ \kappa p_0 &\leq z_0 p_d + z_1 p_{d-1} + \cdots + z_{d-1} p_1 && \\ \kappa p_0 &\leq \kappa |p_k| + \eta \sum_{i \neq 0, k} p_i && (19) \end{aligned}$$

Inequality (19) implies $\eta \geq \kappa$. Moreover if $z_{d-k} \neq -\kappa$, then we have the strict inequality:

$$\kappa p_0 < \kappa |p_k| + \eta \sum_{i \neq k} p_i$$

which implies $\eta > \kappa$. The remaining case is that $z_d = z_{d-k} = -\kappa$. If there is some $\ell > 0$ such that $z_{d-k\ell} \neq -\kappa$, then by shifting indices, we may assume $z_d = -\kappa \neq z_{d-k}$ and $\eta > \kappa$ follows. If $z_{d-k\ell} = -\kappa$ for all $\ell = 0, 1, 2, \dots$, using the left side of (18), we have

$$\kappa(p_0 + p_k + \cdots + p_{k[\frac{d}{k}]}) \le \eta \sum_{k\nmid i} |p_i| < \eta \sum_{i=1}^{d} |p_i| \le \eta p_0.$$

Hence $\kappa < \eta$ by the assumption $\sum_{1\le ki\le d} p_{ki} \ge 0$. So our claim is proved.

Our next aim is to show $z_j = \eta$ implies $z_{j+k\ell} = \eta$ for all $\ell \in \mathbb{Z}$. Without loss of generality, we may assume $z_d = \eta$. If $z_{d-k} \ne \eta$, then by the right side of (18),

$$\begin{aligned} p_0 &> z_0 p_d + z_1 p_{d-1} + \cdots + z_{d-1} p_1 + z_d p_0 \\ &\ge -\kappa \sum_{\substack{i\ne 0,\ k \\ 1\le i\le d}} |p_i| - (\eta - 1)|p_k| + \eta p_0 \\ &\ge p_0 + (\eta - 1)(p_0 - \sum_{1\le i\le d} p_i) \\ &\ge p_0. \end{aligned}$$

This is a contradiction. So $z_{d+k\ell} = \eta$ for all $\ell \in \mathbb{Z}$. Now (18) become

$$\begin{aligned} p_0 &> z_0 p_d + z_1 p_{d-1} + \cdots + z_{d-1} p_1 + z_d p_0 \\ &\ge -\kappa \sum_{k\nmid i} |p_i| + \eta \sum_{\substack{k|i \\ i\ne 0}} p_k + \eta p_0. \end{aligned}$$

By the assumption $\sum_{\substack{k|i \\ i\ne 0}} p_i \ge 0$, we see $\kappa > 0$. Moreover

$$\kappa \sum_{k\nmid i} |p_i| > (\eta - 1)p_0.$$

This shows

$$\sum_{1\le i\le d} |p_i| > \sum_{\substack{1\le i\le d \\ k\nmid i}} |p_i| > p_0,$$

which is a desired contradiction. □

Classification of quadratic CNS polynomials $x^2 + p_1 x + p_0$ was already done by [9], [10], [5] and [16] in several ways. We reprove this result as an application of our discussion.

Corollary 3.6. *Let $P(x) = x^2 + p_1 x + p_0$ be a quadratic polynomial. Then $P(x)$ is a CNS polynomial if and only if $-1 \le p_1 \le p_0$ and $p_0 \ge 2$.*

Proof. If $P(x)$ is a CNS polynomial, then $p_0 \ge 2$ by (2). Since there are no roots in $[-1, 0]$, we have $P(-1) > 0$ which shows $p_1 \le p_0$ and 1-subsum condition implies $-1 \le p_1$.

Conversely if $-1 \le p_1 \le p_0$ and $p_0 \ge 2$ then $P(x)$ must be expanding. If $p_1 < p_0$, then Theorem 3.2 implies that $P(x)$ is a CNS polynomial as coefficients satisfy the dominant condition. The remaining case $p_1 = p_0$ is settled down by (3), a result of B.Kovács. $\square$

For an expanding polynomial $P(x)$, (7) gives an algorithmic bound of the set $\mathcal{P}$. If $P(x)$ satisfies dominant condition, we can get a bound in another way. Theorem 3.7 is an improvement of Theorem 1 of S.Akiyama and A.Pethő [3], giving such a bound of $\mathcal{P}$. [2]

Theorem 3.7. *Assume $|p_0| > \sum_{i=1}^d |p_i|$ and $\xi = \sum_{i=1}^d w_i z_i \in \mathcal{P}$. Then we have*

$$\left| z_i - \frac{p_0}{2\sum_{i=0}^d p_i} \right| \le \frac{|p_0|}{2\left(|p_0| - \sum_{i=1}^d |p_i|\right)}.$$

Proof. First we prove the case $p_0 > 0$. Putting $\tau = \frac{p_0}{2(\sum_{i=0}^d p_i)}$, by (13), we have

$$-\frac{p_0}{2} \le \sum (z_{i+j} - \tau) p_{d-j} < \frac{p_0}{2}.$$

Let $\eta = \max_{i \in \mathbb{Z}} |z_i - \tau|$ and choose i such that $\eta = |z_{i+d} - \tau|$. If $z_{i+d} - \tau = -\eta$ then

$$\eta \left(|p_d| + |p_{d-1}| + \cdots + |p_1|\right) \ge \left(\eta - \frac{1}{2}\right) p_0.$$

If $z_{i+d} - \tau = \eta$ then

$$-\eta \left(|p_d| + |p_{d-1}| + \cdots + |p_1|\right) < \left(\frac{1}{2} - \eta\right) p_0.$$

Thus in any case, we have

$$\begin{aligned} \eta \sum_{i=1}^d |p_i| &\ge \left(\eta - \frac{1}{2}\right) p_0 \\ \eta &\le \frac{p_0}{2\left(p_0 - \sum_{i=1}^d |p_i|\right)}, \end{aligned}$$

which shows our assertion.

Now we wish to show the case $p_0 < 0$. For the moment, we permit negative leading coefficient $p_d = -1$ and substitute $P(x)$ by $-P(x)$ to make $p_0 > 0$ and $p_d = -1$. Then we easily see that Proposition 3.1 remains true in the same notation. Thus the above proof also works for the case $p_0 < 0$. $\square$

[2] Though it is not explicitly mentioned, the bound of Theorem 1 of [3] is nothing but the bound for $\mathcal{P}$. This fact is easily seen from its proof. Note that we do not assume $p_0 > 0$.

4. Some remarks on H. Brunotte's result

H. Brunotte [4] found an interesting algorithm to determine a polynomial is a CNS polynomial or not. The original proof is not so easy. Recently K. Scheicher & J.M.Thuswaldner [15] gave a simple proof of a similar result by using finite automata. In this section, we give another proof of Brunotte's Lemma based on the techniques of Section 3. The idea is inspired by [15]. Beside of this, we give several remarks on Brunotte's algorithm.

Let us define

$$\sigma^*(z_1, \dots, z_d) = -\sigma(-z_1, -z_2, \dots, -z_d),$$

where σ is defined as in Section 3. As it is seen that $\sigma^*(z_1, \dots, z_d) = \sigma(z_1 + p_0 - 1, z_2, \dots, z_d)$. Lemma 2 of [4] reads

Lemma 4.1. *Let $P(x)$ be a monic polynomial of degree d with $p_0 \geq 2$. If there is a set $E \subset \mathbb{Z}^d$ satisfying the following properties, then $P(x)$ is a CNS polynomial.* [3]

(i) $(0, \dots, 0), (-1, 0, \dots, 0), (1, 0, \dots, 0) \in E$
(ii) $(\sigma(E) \cup \sigma^*(E)) \subseteq E$.
(iii) *For any $x \in E$, there exist a positive integer M such that $\sigma^M(x) = 0$.*

Proof. Again let $\alpha = x \bmod P(x)$. Suppose $\xi \in R$ has a canonical expansion and $\eta \in \iota(E)$, we argue that $\xi + \eta$ also has a canonical expansion. Suppose

$$T(\xi) = \frac{\xi - k_1}{\alpha}, \quad T(\eta) = \frac{\eta - k_2}{\alpha},$$

where $k_1, k_2 \in \{0, 1, \cdots, p_0 - 1\}$. If $k_1 + k_2 < p_0$, then

$$T(\xi + \eta) = \frac{\xi + \eta - (k_1 + k_2)}{\alpha} = T(\xi) + T(\eta).$$

If $k_1 + k_2 \geq p_0$, then $k_2 > 0$ and

$$T(-\eta) = \frac{-\eta - (p_0 - k_2)}{\alpha}.$$

So we have

$$T(\xi + \eta) = \frac{\xi + \eta - (k_1 + k_2) + p_0}{\alpha} = T(\xi) - T(-\eta).$$

By the assumption (ii),

$$-T(-\eta) = -\iota(\sigma(\iota^{-1}(-\eta))) = \iota(\sigma^*(\iota^{-1}(\eta))) \in \iota(E).$$

Repeat this argument, we have for any n,

$$T^n(\xi + \eta) = T^n(\xi) + \eta^*$$

[3] There is a minor difference between (i) and the corresponding assumption of Lemma 2 in [4], which is

$$(0, \dots, 0), (-1, 0, \dots, 0), (0, \dots, 0, -1) \in E.$$

for some $\eta^* \in \iota(E)$. Since ξ has a canonical expansion, so $T^n(\xi + \eta) \in \iota(E)$ for a large n. Now from assumption (iii), we conclude that $\xi + \eta$ has a canonical expansion.

As $\pm 1 \in \iota(E)$ is seen by the assumption (i), ξ has a canonical expansion implies $\xi \pm 1$ have canonical expansions. Note that ξ has canonical expansion implies $\alpha\xi$ has a canonical expansion. Since every element of $\mathbb{Z}(x)$ can be obtain from 0 by these two operations, so every element of R has a canonical expansion. ☐

This Lemma 4.1 gives a handy way to determine whether $P(x)$ is a CNS polynomial or not.

(a): Let $E_1 = \{(0, \dots, 0), (-1, 0, \dots, 0), (1, 0, \dots, 0)\}$.
(b): If E_i is defined for $i < n$, then E_n is defined by $E_n = E_{n-1} \cup \sigma(E_{n-1}) \cup \sigma^*(E_{n-1})$.
(c): If $E_n \neq E_{n-1}$ then continue this emerging process (b). If $E_n = E_{n-1}$ then we proceed to the next step (d).
(d): For each element x of E_n, we confirm that there exists M such that $T^M(x) = 0$.

Note that $E_n = -E_n$ for any n. When $P(x)$ is an expanding polynomial, the last process (d) will terminate in finite steps since the sequence $\{T^i(x)\}_{i=0,1,2,\dots}$ is eventually periodic by Proposition 2.1.

Further it is important to point out that the above emerging process (b) also terminate in finite steps. Indeed, as $P(x)$ expanding, we know that both σ and σ^* are eventually contractive. So the sets E_n $(n = 1, 2, \dots)$ must be uniformly bounded. By the discreteness of $\mathbb{Z}^d$ in $\mathbb{R}^d$ and $E_n \supset E_{n-1}$ we conclude that the process (b) will certainly stop. Especially, if $P(x)$ is separable then we can give a concrete bound of the sets E_n.

Theorem 4.2. *If $P(x)$ is an expanding separable polynomial. Let*

$$W = \left\{ \xi \in R \;\middle|\; |\xi(\theta)| \leq \frac{|p_0| - 1}{|\theta| - 1} \text{ for all root } \theta \text{ of } P(x) \right\}.$$

Then we have $E_n \subset \iota(W)$ for all n.

Proof. Let us go back to the representation in base $\{1, \alpha, \dots, \alpha^{d-1}\}$ and consider the action of T and define $T^*(\xi) = -T(-\xi)$. As $P(x)$ is expanding, $E_1 \subset \iota(W)$ is clear. It suffices to show $T(W) \cup T^*(W) \subset W$. Indeed, it is equivalent to $\sigma(\iota(W)) \cup \sigma^*(\iota(W)) \subset \iota(W)$, and so we have $\sigma(E_n) \cup \sigma^*(E_n) \subset \iota(W)$ provided $E_n \subset \iota(W)$.

One can easily see that $T(\xi) = (\xi - k_1)/\alpha$ and $T^*(\xi) = (\xi - k_2)/\alpha$ with $k_1, k_2 \in [-p_0+1, p_0-1]$. Let θ be a root of $P(x)$. Then we see that $T(\xi(\theta)) = (\xi(\theta) - k_1)/\theta$ and $T_1(\xi(\theta)) = (\xi(\theta) - k_2)/\theta$. Put $K(\theta) = (|p_0| - 1)/(|\theta| - 1)$. Then $|\xi(\theta)| \leq K(\theta)$ implies

$$\left| \frac{\xi(\theta) - k_1}{\theta} \right| \leq \frac{K(\theta) + p_0 - 1}{|\theta|} = K(\theta),$$

showing $|T(\xi(\theta))| \leq K(\theta)$ and also $|T_1(\xi(\theta))| \leq K(\theta)$. This shows $T(W) \cup T^*(W) \subset W$. $\square$

Thus we have another algorithm to determine whether an polynomial is CNS. This bound W in Theorem 4.2 is the same as (7). Thus this algorithm can not be worse than the one in [12]. If we have a dominant condition as before, then we can say more.

Theorem 4.3. *Let $P(x)$ be a monic polynomial with dominant condition $p_0 \geq \sum_{i=1}^d |p_i|$. Then $P(x)$ is a CNS polynomial if and only if every element of*

$$S = \{\xi \in R \mid \xi = \sum_{i=1}^d z_i w_i \text{ and } |z_i| \leq 1\}$$

has a canonical expression.

Proof. We need only show that the condition is sufficient. Let

$$S' = \{(z_1, \dots, z_d) \mid z_i \in \{-1, 0, 1\}\}.$$

Then S' fulfills the property (i) of Lemma 4.1. Under dominant condition, it is easy to check that S' satisfies the property (ii). The assumption on S implies that S' satisfies the property (iii). Hence $P(x)$ is a CNS polynomial. $\square$

Corollary 4.4. *Let $P(x)$ be a monic polynomial satisfying $p_0 > \sum_{i=1}^d |p_i|$. Then $P(x)$ is a CNS polynomial if and only if every element of*

$$\{\xi \in R \mid \xi = \sum_{i=1}^d z_i w_i \text{ and } z_i = 0, 1\}$$

has a canonical expression.

Proof. Let S' be the set defined in Theorem 4.3. Pick any $(z_1, \dots, z_d) \in S'$, it define a infinite word $(z_1, \dots, z_d, z_{d+1}, \dots)$. The dominant condition $p_0 > \sum_{i=1}^d |p_i|$ implies that $d_i \in \{0, 1\}$ for any $i > d$. Hence there is an integer $M > 0$ such that $\sigma^M(z_1, \dots, z_d) = (0, \dots, 0)$. Hence $P(x)$ is a CNS polynomial by Lemma 4.1. $\square$

5. Characterizations of CNS polynomials with a dominant condition

This section is inspired by the recent work by K. Scheicher & J.M.Thuswaldner [15]. We shall give some simple necessary and sufficient conditions of CNS polynomial of degree 3, 4 and 5 under the dominant condition $p_0 \geq \sum_{i=1}^d |p_i|$.

Theorem 3 in S. Akiyama & A. Pethő [3] says that

$$p_\ell + \sum_{k=\ell+1}^d |p_k| \geq 0 \tag{20}$$

is a necessary condition for CNS polynomials with $p_0 \geq \sum_{i=1}^d |p_i|$. The same idea allows us to show a slightly stronger assertion under the dominant condition (4). Namely, if $P(x)$ is a CNS polynomial then

$$p_\ell + \sum_{\substack{k=\ell+1 \\ p_k > 0}}^{d} p_k \geq 0$$

under (4). To show it, only thing to check is that there are no case $\varepsilon_j = -1$ under their notation in [3]. An analogous method allows us to show [4]

Lemma 5.1. *If $P(x)$ is a CNS polynomial satisfying $p_0 \geq \sum_{i=1}^d |p_i|$, then $1 + p_{d-1} + p_{d-2} \geq 0$.*

Proof. If $d = 2$, then $1 + p_{d-1} + p_{d-2} \geq 0$ is clear. Thus we show the case $d > 2$. Assume that $1+p_{d-1}+p_{d-2} < 0$ and $P(x)$ is a CNS polynomial. Since $1+p_{d-1} \geq 0$ by (20), we have $p_{d-2} < 0$. If $p_{d-1} \geq 0$ then $|p_d| + |p_{d-1}| + p_{d-2} < 0$ gives a contradiction again by (20). Thus we see that $p_{d-1} = -1$ and $p_{d-2} < 0$ holds. Put $T^m(x) = \sum_{i=0}^{d-1} T_i^m(x)\alpha^j$ for $x \in R$. Reviewing the definition of the basis $\{w_i\}$, we have $w_j = \sum_{k=0}^{j-1} p_{d+1+k-j}\alpha^k$. Using this we have $T_i^m(x) = \sum_{j=i}^{d-1} z_{j+m+1}p_{d+i-j}$ with $z_j \in \mathbb{Z}$ defined at the beginning of §3. Now we specify $x = -1$ and define an integer sequence $\{z_i\}_{i=1}^\infty$. By using (5), it is easily seen that $z_i \in \{0, \pm 1\}$. Our aim is to show that for any non-negative integer m, there exist j that $T_j^m(-1) < 0$ which proves that $P(x)$ is not a CNS polynomial. This is obviously true when $m = 0$. If $T_0^{m-1}(-1) \geq 0$ then it is shown, similarly as in Theorem 3 in [3], that there exist j that $T_j^m(-1) < 0$. Let us assume that $T_0^{m-1}(-1) < 0$. By (5), we have $z_{m+d} = 1$. If $z_{m+d-1} \leq 0$ then,

$$T_{d-2}^m(-1) = z_{m+d-1} - z_{m+d} < 0.$$

If $z_{m+d-1} > 0$ then,

$$T_{d-3}^m(-1) = z_{m+d-2} - z_{m+d-1} + z_{m+d}p_{d-2} \leq 1 - 1 + p_{d-2} < 0.$$

Thus we have shown the Lemma. □

Here it may be convenient to summarize necessary conditions for CNS polynomials with (5).

Theorem 5.2. *Let $P(x)$ be an expanding polynomial with the dominant condition (5). Then $P(x)$ is a CNS implies*

(a) $1 + p_{d-1} \geq 0$;
(b) $1 + p_{d-1} + p_{d-2} \geq 0$;
(c) $\sum_{i=1}^d p_d \geq 0$;

[4] One might hope that $\sum_{k=\ell}^d p_k \geq 0$ for any $\ell = 1, 2, \ldots, d-1$ are necessary for a CNS polynomial $P(x)$. Unfortunately this is not the case. A counter example is given that

$$x^{10} - x^9 + x^8 - 2x^7 + 4x^6 + 4x^5 + 4x^4 - 3x^3 - x^2 + 20$$

is a CNS polynomial but $p_d + p_{d-1} + p_{d-2} + p_{d-3} < 0$.

(d) $\sum_{2|i,1\le i\le d} p_d \ge 0$.

Proof. Lemma 5.1 and (20) imply (a) and (b). Condition (c) follows from 1-subsum condition. We need only prove (d). Suppose not, than by (c), we know $\sum_{2\nmid i,1\le i\le d} p_d \ge 0$. By using (5), $P(x)$ is not a CNS polynomial since it does not satisfy 2-subsum condition. □

Theorem 5.3. *Let $P(x) = x^3 + p_2x^2 + p_1x + p_0$ be a polynomial in $\mathbb{Z}[x]$ with $p_0 > 1 + |p_2| + |p_1|$. Then $P(x)$ is a CNS polynomial if and only if $p_2 \ge 0$ and $1 + p_2 + p_1 \ge 0$.*

Proof. Assume that $P(x)$ is a CNS polynomial. Then Theorem 5.2 (b) or (c) implies $1 + p_2 + p_1 \ge 0$ and (d) gives $p_2 \ge 0$. (These facts were shown in a different way in Proposition 1 of [3].) The sufficiency follows from Theorem 3.2. □

Theorem 5.4. *Let $P(x) = x^4 + p_3x^3 + p_2x^2 + p_1x + p_0$ be a polynomial in $\mathbb{Z}[x]$ with $p_0 > 1+|p_3|+|p_2|+|p_1|$. Then $P(x)$ is a CNS polynomial if and only if five conditions:*

$$\begin{array}{rcl} p_3 & \ge & -1 \\ p_2 & \ge & -1 \\ p_3 + p_2 & \ge & -1 \\ 1 + p_3 + p_2 + p_1 & \ge & 0 \\ p_3 = -1 & \Rightarrow & p_1 \le -2 \end{array}$$

holds.

Proof. Assume that $P(x)$ is a CNS polynomial. Theorem 5.2 says the first four conditions are necessary. Let $p_3 = -1$. Then $1 + p_3 + p_2 \ge 0$ implies $p_2 \ge 0$. Let us consider the 3-subsum condition. As $p_3 + p_0$ and p_2 are in $[0, p_0 - 1] \cap \mathbb{Z}$, we see $1 + p_1$ must be negative.

Now we wish to show the sufficiency. Note that $1 + p_3 + p_2 \ge 0$ shows that not both p_2 and p_3 are negative. First we consider the case $p_3 = -1$. Then $p_1 \le -2$ and $p_2 \ge 2$. The proof is done by writing a directed graph consist of $2^4 = 16$ vertices formed by $(z_i, z_{i+1}, z_{i+2}, z_{i+3})$ with $z_i \in \{0,1\}$. Each vertex $(z_i, z_{i+1}, z_{i+2}, z_{i+3})$ represents an element of

$$\{\xi \in R \mid \xi = \sum_{i=1}^{4} z_iw_i \text{ and } z_i = 0, 1\}$$

which forms a test set in Corollary 4.4. We write a directed edge from $(z_i, z_{i+1}, z_{i+2}, z_{i+3})$ to $(z_{i+1}, z_{i+2}, z_{i+3}, z_{i+4})$ if there is a possibility that

$$\sigma(z_i, z_{i+1}, z_{i+2}, z_{i+3}) = (z_{i+1}, z_{i+2}, z_{i+3}, z_{i+4})$$

under these five conditions. This was done in Figure 1. Here we omit a self loop from $(0, \dots, 0)$ to itself. As this graph forms a directed tree having an only

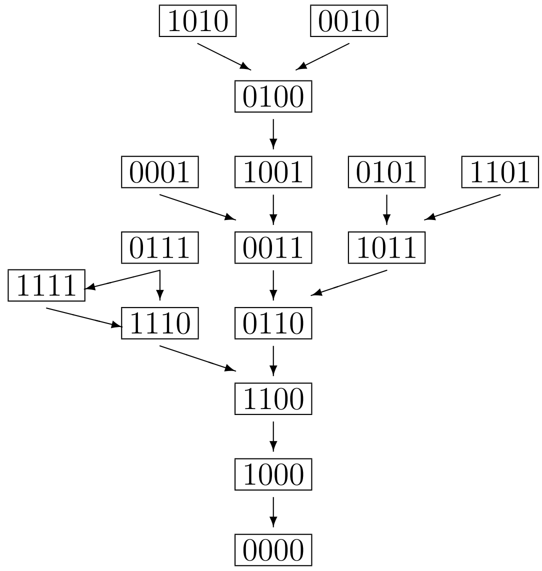

FIGURE 1. $p_3 = -1$, Quartic case

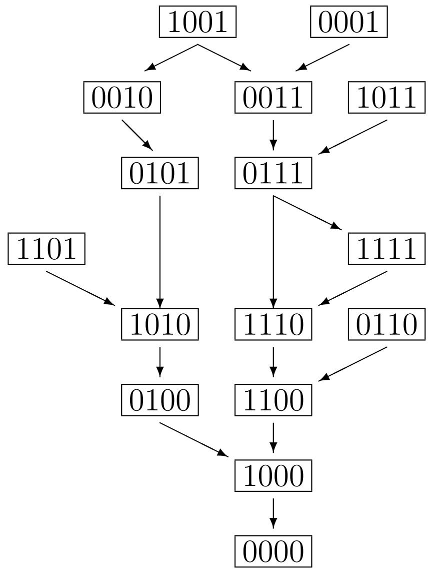

FIGURE 2. $p_2 = -1$, $p_1 < 0$, Quartic case

terminal vertex $(0,0,0,0)$, we have completed the case $p_3 = -1$. Second we treat the case $p_3 \geq 0$ and $p_2 = -1$. If $p_1 \geq 0$, then as $1+p_2 \geq 0$ we can apply Theorem 3.5 to show that $P(x)$ is a CNS polynomial. Let $p_1 \leq -1$. As $1+p_3+p_2+p_1 \geq 0$, we have $p_3 \geq 1$ and $p_3 + p_1 \geq 0$. Figure 2 gives a similar directed graph showing that $P(x)$ is a CNS polynomial.

Finally if $p_3 \geq 0$ and $p_2 \geq 0$ then as $1+p_3+p_2+p_1 \geq 0$ we can apply Theorem 3.2 to see that $P(x)$ is a CNS polynomial. Thus we have shown the assertion. $\square$

Remark 5.5. Proofs of Theorem 5.3 and 5.4 shows that CNS polynomial with a dominant condition (4) is completely characterized by the known necessary conditions: k-subsum condition, (20) and Lemma 5.1 provided the degree of the polynomial is less than 5.

Theorem 5.6. *Let $P(x) = x^5 + p_4x^4 + p_3x^3 + p_2x^2 + p_1x + p_0$ be a polynomial in $\mathbb{Z}[x]$ with $p_0 > 1 + |p_4| + |p_3| + |p_2| + |p_1|$. Then $P(x)$ is a CNS polynomial if and only if five conditions:*

$$\begin{aligned} p_2 + p_4 &\geq 0 \\ 1 + p_4 + p_3 + p_2 + p_1 &\geq 0 \\ p_4 < 0 &\Rightarrow p_4 = -1, p_3 \geq 1, p_1 \leq -2 \\ p_3 < 0, p_1 + p_4 \geq 0 &\Rightarrow p_3 \geq -1, p_2 \leq -2 \\ p_3 < 0, p_1 + p_4 < 0 &\Rightarrow p_4 \geq 0, p_4 + p_3 \geq 0 \end{aligned}$$

holds.

Proof. Assume that $P(x)$ is a CNS polynomial. First two conditions are shown in Theorem 5.2. Assume that $p_4 < 0$. In this case we see by $1 + p_4 \geq 0$ and $1 + p_4 + p_3 \geq 0$ that $p_4 = -1$ and $p_3 \geq 0$. $p_2 + p_4 \geq 0$ shows $p_2 \geq 1$. Using 4-subsum condition, $1 + p_1$ must be negative. Further we can show that $p_3 \geq 1$. For if $p_3 = 0$ then 1-subsum condition implies $p_2 + p_1 \geq 0$ and so we can confirm that

$$\Xi = (0011)^\infty$$

gives an element of $\mathcal{P}$. Thus we have shown that third necessary condition of Theorem 5.6.

Next consider the case $p_3 < 0$. As stated above, we have $p_4 \geq 0$. Further assume that $p_1 + p_4 \geq 0$. By 3-subsum condition, $1 + p_2 < 0$. It is also seen that $p_3 \geq -1$. For if $p_3 \leq -2$ then we can construct a bi-infinite word

$$\Xi = \begin{cases} (01001)^\infty & p_3 + p_1 \geq 0 \\ (01001011)^\infty & p_3 + p_1 < 0 \end{cases}$$

which corresponds to an element of $\mathcal{P}$. This shows the 4-th necessary condition. Assume that $p_3 < 0$ and $p_1 + p_4 < 0$. If $p_4 + p_3 < 0$ then we see that

$$\Xi = \begin{cases} (1001100)^\infty & 1 + p_4 + p_1 \geq 0 \\ (1001)^\infty & 1 + p_4 + p_1 < 0 \end{cases}$$

is a corresponding word of a non zero element of $\mathcal{P}$. Thus we have proved five necessary conditions.

We now prove the sufficiency. First note that p_4 or p_3 can not be an isolated negative coefficient by the claim before Theorem 3.5. Since $1+p_4+p_3+p_2+p_1 \geq 0$ and $p_2 + p_4 \geq 0$ are already assumed, Theorem 3.2 and 3.5 can be applied when there are at most one negative coefficient. Thus we only need to show the sufficiency in the case that there are at least two negative coefficients. In such 4 subcases, we can write down similar directed graphs used in the proof of Theorem 5.4:

(1): $p_4 = -1$
(2): $p_3 < 0$ and $p_1 + p_4 \geq 0$
(3): $p_3 < 0$ and $p_1 + p_4 < 0$
(4): $p_4 \geq 0$, $p_3 \geq 0$, $p_1 < 0$ and $p_2 < 0$

In fact, the case (1) is done in Figure 3. In the case (2), it is easy to confirm a directed graph of Figure 4. Here we performed out-going amalgamation for some vertices on the original graphs to simplify them. This means that if two vertices v_1, v_2 have exactly the same follower vertices then such vertices are unified into one vertex (v_1, v_2) in their graph expression. Last two cases are also completed easily. We left these cases to the reader.

□

Remark 5.7. Theorem 5.6 is restated as follows under the same condition. The polynomial $P(x)$ is a CNS polynomial if and only if it satisfies k-subsum condition (for $k = 1, 2, 3, 4$), $p_4 \geq -1$, $p_3 + p_4 \geq 0$ and

$$p_1 + p_4 \geq 0 \Rightarrow p_3 \geq -1.$$

To show this, we need only to review the above proof that all five conditions in Theorem 5.6 is derived by these conditions.

Note that last two conditions are not seen by combining k-subsum conditions, (20) and Lemma 5.1. Thus unfortunately, known necessary conditions on CNS are not enough to characterize CNS polynomials of degree 5.

Remark 5.8. Let us fix a positive integer d and consider expanding polynomials of degree d under the dominant condition (4). We may say that Corollary 4.4 provides an algorithm to describe all such CNS polynomials. However it seems impractical to accomplish it for a large degree.

Indeed, possible lengths of periods of $\mathcal{P}$ are not larger than 2^d. So we can characterize polynomials which admits non zero periodic words Ξ by finite sets of inequalities. Thus solving all these inequalities, we can describe the set of all CNS polynomials by ruling out such family of non CNS polynomials.

References

[1] S. Akiyama, On the boundary of the tiling generated by Pisot numbers, Journal of Math. Soc. Japan, **54** no. 2 (2002) 283-308.

[2] S. Akiyama and J.M.Thuswaldner, Topological properties of two-dimensional number systems, Journal de Théorie des Nombres de Bordeaux **12** (2000) 69–79.

[3] S. Akiyama and A. Pethő, On canonical number systems, Theoretical Computer Science, **270** (2002) 921-933.

[4] H. Brunotte, On trinomial basis of Radix Representations of Algebraic Integers. to appear in Acta Sci. Math. (Szeged) **67** (2001) 407–413.

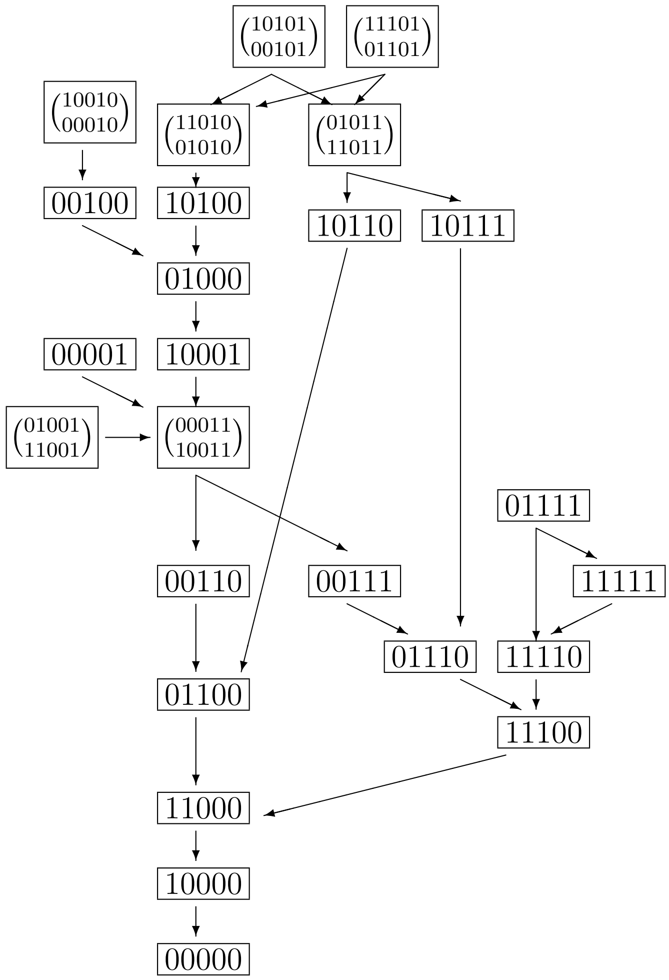

FIGURE 3. $p_4 = -1$, degree 5

[5] W.J.Gilbert, Radix representations of quadratic number fields, J. Math. Anal. Appl. **83** (1981) 263–274.

[6] M. Hollander, Linear Numeration systems, Finite Beta Expansions, and Discrete Spectrum of Substitution Dynamical Systems, Doctorial thesis for Washington Univ.

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

[8] I. Kátai and I. Kőrnyei, On number systems in algebraic number fields, Publ. Math. Debrecen **41** no. 3–4 (1992) 289–294.

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

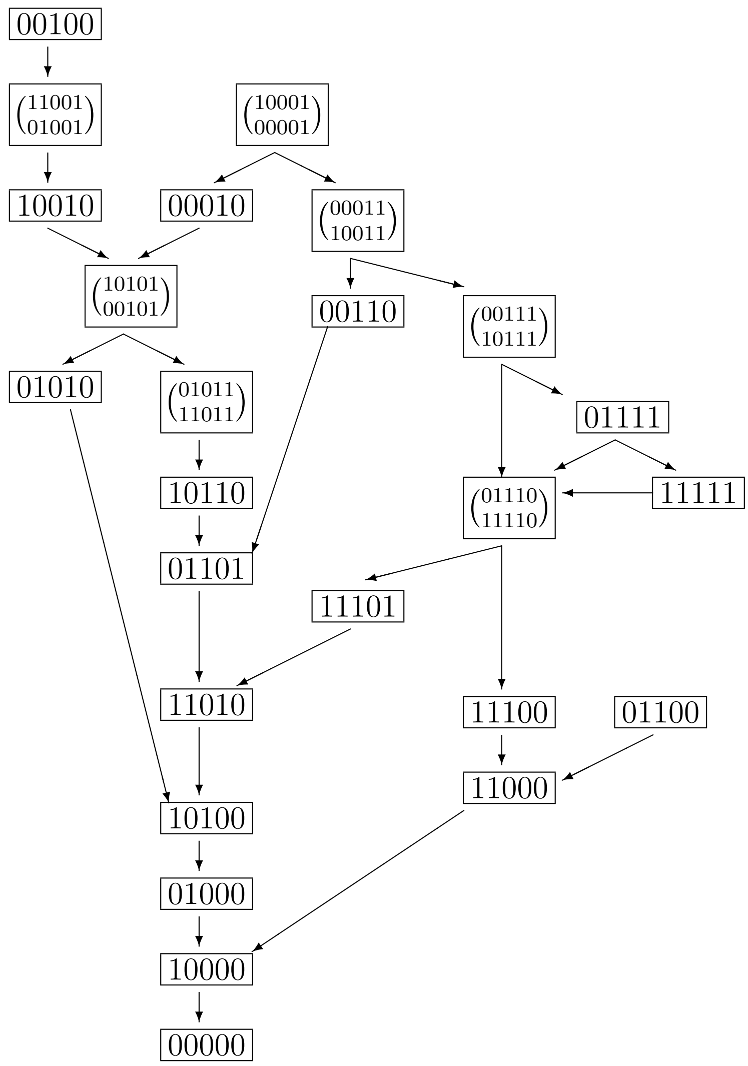

FIGURE 4. $p_4 \geq 0, p_3 < 0, p_1 + p_4 \geq 0$, degree 5

[10] I. Kátai and B. Kovács, Kanonische Zahlensysteme in der Theorie der quadratischen Zahlen, Acta Sci. Math. (Szeged) **42** (1980) 99–107.
[11] B. Kovács, Canonical number systems in algebraic number fields, Acta Math. Acad. Sci. Hungar. **37** (1981), 405–407.
[12] 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.
[13] A. Pethő, On a polynomial transformation and its application to the construction of a public key cryptosystem, Computational Number Theory, Proc., Walter de Gruyter Publ. Comp. Eds.: A. Pethő, M. Pohst, H.G. Zimmer and H.C. Williams, 1991, pp 31-44.

[14] K. Scheicher, Kanonische Ziffernsysteme und Automaten, Grazer Math. Ber., **333** (1997), 1–17.

[15] K. Scheicher and J.M.Thuswaldner, On the characterization of Canonical number system, to appear in Osaka J. Math.

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

Shigeki Akiyama
Department of Mathematics, Faculty of Science, Niigata University,
Ikarashi 2-8050, Niigata 950-2181, Japan
e-mail: akiyama@math.sc.niigata-u.ac.jp

Hui Rao
Department of Mathematics, Faculty of Science, Wuhan University,
430072, Wuhan, P.R. China
e-mail: myhacone@yahoo.com