#A19 INTEGERS 9 (2009), 201-214

SYMMETRIC CNS TRINOMIALS

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

Received: 9/27/08, Accepted: 1/26/09

Abstract

Background material on α-shift radix systems and α-CNS polynomials is collected. Symmetric CNS trinomials of the shape $X^d + bX + c$ $(d > 2)$ are characterized, thereby extending known results on quadratic symmetric CNS polynomials.

1. Introduction

Generalizing the notions of shift radix systems introduced by Akiyama *et al.* [1] and of symmetric shift radix systems introduced by Akiyama–Scheicher [6], the concept of α-shift radix systems was recently established by Surer [14]. It may be seen as a unifying generalization of β-expansions and canonical number systems (see also [7, 4]). Many of the results known for shift radix systems can easily be carried over to α-shift radix systems. Some of these are collected here (Section 2) and applied to α-CNS polynomials (Section 3). In particular, α-CNS polynomials of the shape $X^d + c$ are characterized. Further, symmetric CNS trinomials are investigated insome detail (Section 4), thereby extending the characterization of quadratic symmetric CNS polynomials given by Akiyama–Scheicher.

2. Basic Facts on α-Shift Radix Systems

For $d \in \mathbb{N}_{>0}$, $\mathbf{r} = (r_1, \ldots, r_d) \in \mathbb{R}^d$ and $\alpha \in [0, 1)$ Surer [14] introduced and investigated the map $\tau_{\mathbf{r},\alpha} : \mathbb{Z}^d \to \mathbb{Z}^d$ defined by $\tau_{\mathbf{r},\alpha}(a_1, \ldots, a_d) = (a_2, \ldots, a_{d+1})$ where $a_{d+1} \in \mathbb{Z}$ is determined by the inequalities

$$0 \leq r_1 a_1 + \ldots + r_d a_d + a_{d+1} + \alpha < 1. \tag{1}$$

The map $\tau_{\mathbf{r},\alpha}$ is called an α-shift radix system if for all $\mathbf{a} \in \mathbb{Z}^d$ there is some $n \in \mathbb{N}$ such that[1] $\tau^n_{\mathbf{r},\alpha}(\mathbf{a}) = 0$. Thus the study of the sets

$$\mathcal{D}^0_{d,\alpha} \quad = \quad \left\{\mathbf{r} \in \mathbb{R}^d : \tau_{\mathbf{r},\alpha} \text{ is an } \alpha\text{-shift radix system}\right\} \tag{2}$$

[1] For $T : X \to X$ we let $T^0 = \mathrm{id}_X$ and $T^{n+1} = T \circ T^n \quad (n \in \mathbb{N})$.

and

$$\mathcal{D}_{d,\alpha} = \left\{\mathbf{r} \in \mathbb{R}^d \,:\, \text{for all } \mathbf{a} \in \mathbb{Z}^d \text{ the sequence } (\tau_{\mathbf{r},\alpha}^k(\mathbf{a}))_{k\geq 0} \text{ is ultimately periodic}\right\}$$

is appropriate. The goal of this section is the extension of some basic results on shift radix systems to α-shift radix systems.

For $\mathbf{r} = (r_1, \ldots, r_d) \in \mathbb{R}^d$ we denote by

$$R(\mathbf{r}) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ -r_1 & -r_2 & \cdots & \cdots & -r_d \end{pmatrix} \tag{3}$$

the companion matrix of the polynomial

$$\chi_{\mathbf{r}}(X) = X^d + r_d X^{d-1} + \cdots + r_2 X + r_1.$$

Note that $\chi_{\mathbf{r}}$ is the characteristic polynomial of $R(\mathbf{r})$.

Lemma 1 *Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}^d$. Then there exist reals $\delta_i \in [-\alpha, 1-\alpha)$ $(i = 0, \ldots, n-1)$ such that*

$$\tau_{\mathbf{r},\alpha}^n(a) = R(\mathbf{r})^n a + \sum_{i=0}^{n-1} R(\mathbf{r})^i (0, \ldots, 0, \delta_i)^T.$$

Proof. This can easily be proved by induction (see also [13]). □

Lemma 2 *If $\| \mathbf{r} \|_1 \leq 1$ then $\mathbf{r} \in \mathcal{D}_{d,\alpha}$.*

Proof. For all $a \in \mathbb{Z}^d$ we have

$$- \| a \|_\infty \quad \leq \quad r_1 a_1 + \cdots + r_d a_d + \alpha \quad \leq \quad \| a \|_\infty + \alpha,$$

hence

$$|\lfloor r_1 a_1 + \cdots + r_d a_d + \alpha \rfloor| \;\leq\; \| a \|_\infty$$

and therefore

$$\| \tau_{\mathbf{r},\alpha}(a) \|_\infty \;\leq\; \| a \|_\infty,$$

which implies $\mathbf{r} \in \mathcal{D}_{d,\alpha}$. □

By [14, Theorem 2.1] and Lemma 2 we have the useful inclusions

$$\mathcal{E}_d \cup \left\{\mathbf{r} \in \mathbb{R}^d \,:\| \mathbf{r} \|_1 \leq 1\right\} \cup \mathcal{D}_{d,\alpha}^0 \subseteq \mathcal{D}_{d,\alpha} \subseteq \overline{\mathcal{E}_d}. \tag{4}$$

The next two theorems extend results of [1] and of [4, Theorem 2.4], respectively, and can easily be checked by the definitions.

Theorem 3 *Let $d > 1$ and $r_2, \ldots, r_d \in \mathbb{R}$. Then $(r_2, \ldots, r_d) \in \mathcal{D}^0_{d-1,\alpha}$ if and only if*

$$(0, r_2, \ldots, r_d) \in \mathcal{D}^0_{d,\alpha}.$$

Theorem 4*Let $q, m \in \mathbb{N}_{>0}, \mathbf{s} \in \mathbb{R}^m$ and*

$$\mathbf{r} = (\underbrace{s_1, 0, \ldots, 0}_{q}, \ldots, \underbrace{s_m, 0, \ldots, 0}_{q}) \in \mathbb{R}^{mq}.$$

Then $\mathbf{r} \in \mathcal{D}^0_{mq,\alpha}$ if and only if $\mathbf{s} \in \mathcal{D}^0_{m,\alpha}$.

Lemma 5 provides some necessary conditions on the elements of $\mathcal{D}^0_{d,\alpha}$.

Lemma 5 *Let $\mathbf{r} = (r_1, \ldots, r_d) \in \mathbb{R}^d$.*

(i) If $-\alpha \le \chi_{\mathbf{r}}(1) < 1 - \alpha$ then $\tau_{\mathbf{r},\alpha}(1, \ldots, 1) = (1, \ldots, 1)$.

(ii) If $-1 + \alpha < \chi_{\mathbf{r}}(1) \le \alpha$ then $\tau_{\mathbf{r},\alpha}(-1, \ldots, -1) = (-1, \ldots, -1)$.

(iii) If d is even, $-1 + \alpha < \chi_{\mathbf{r}}(-1) \le \alpha$ and $-\alpha \le \chi_{\mathbf{r}}(-1) < 1 - \alpha$ then

$$\tau^2_{\mathbf{r},\alpha}(-1, 1, \ldots, -1, 1) = (-1, 1, \ldots, -1, 1).$$

(iv) If d is odd, $-1 + \alpha < \chi_{\mathbf{r}}(-1) \le \alpha$ and $-\alpha \le \chi_{\mathbf{r}}(-1) < 1 - \alpha$ then

$$\tau^2_{\mathbf{r},\alpha}(-1, 1, \ldots, -1, 1, -1) = (-1, 1, \ldots, -1, 1, -1).$$

(v) If $\mathbf{r} \in \mathcal{D}^0_{d,\alpha}$ then $\chi_{\mathbf{r}}(-1)\chi_{\mathbf{r}}(1) \ne 0$, and

$$\operatorname{sgn}(\chi_{\mathbf{r}}(-1)\chi_{\mathbf{r}}(1)) = (-1)^\rho$$

where ρ denotes the number of real roots of $\chi_{\mathbf{r}}$ counted by multiplicity.

(vi) If $\mathbf{r} \in \mathcal{D}^0_{d,\alpha}$ and $\zeta \in \mathbb{R}$ is a root of $\chi_{\mathbf{r}}$ then $-1 < \zeta < 1$.

Proof. (i), (ii), (iii) and (iv) immediately stem from the definition.

(v) By the above we know $\chi_{\mathbf{r}}(-1) \ne 0$ and $\chi_{\mathbf{r}}(1) \ne 0$.

(vi) This is clear by (v) and (4). □

The following lemma exploits the idea of an algorithm introduced in [1, Theorem 5.1].

Lemma 6 *Let $(X, +)$ be a finitely generated commutative monoid with neutral element 0 and $T : X \longrightarrow X$ be a map. Let E, F be subsets of X with the following properties:*

(i) $0 \in F$.

(ii) F is invariant under T, i.e., $T(F) \subseteq F$.

(iii) If $x \in X$ and $Tx \in F$ then $x \in F$.

(iv) E contains a full set of generators of X.

(v) For every $e \in E$ there is some $k \in \mathbb{N}$ such that $T^k e \in F$.

(vi) For every $f \in F$ there is some $k \in \mathbb{N}$ such that $E + T^k(f) \subseteq F$.

(vii) For every $e \in E, f \in F$ we have $T(e+f) \in E + T(f)$.

Then $X = F$.

Proof. Let $e \in E$ and $f \in F$. We claim that for all $k \in \mathbb{N}$ there is some $e' \in E$ such that $T^k(e+f) = e' + T^k(f)$. Trivially, this is true for $k = 0$. Assume the statement holds for k. Then $f' := T^k f \in F$, hence by (vii) $T(e' + f') = e'' + T(f')$ for some $e'' \in E$ and further

$$T^{k+1}(e+f) = T(e'+f') = e'' + T(f') = e'' + T^{k+1}(f).$$

Now we establish $E + F \subseteq F$. Indeed, let $e \in E$ and $f \in F$. By (vi) there is some k such that $E + T^k(f) \subseteq F$, and by the above there is some $e' \in E$ such that $T^k(e+f) = e' + T^k(f) \in F$. Thus, the assertion stems from (iii).

Finally, let $g_1, \ldots, g_n \in E$ constitute a full set of generators of X. By induction we see $kg_1 \in F$ for all $k \in \mathbb{N}$ because

$$(k+1)g_1 = g_1 + kg_1 \in E + F \subseteq F.$$

Similarly we find that the monoid generated by $\{g_1, \ldots, g_i\}$ is contained in F for $i = 2, \ldots, n$. This completes the proof. □

We are now applying Lemma 6 to $X = \mathbb{Z}^d$, the canonical basis vectors $\mathbf{e}_1, \ldots, \mathbf{e}_d$ of $\mathbb{R}^d$ and $T = \tau_{\mathbf{r},\alpha}$ where $\mathbf{r} \in \mathbb{R}^d$ and $\alpha \in [0,1)$. Observe that Lemma 6 (vii) can be checked comparatively easily because by [14, proof of Theorem 2.6] we have

$$\tau_{\mathbf{r},\alpha}(a+b) \in \{\tau_{\mathbf{r},\alpha}(a) + \tau_{\mathbf{r},0}(b), \quad \tau_{\mathbf{r},\alpha}(a) - \tau_{\mathbf{r},0}(-b)\} \qquad (a, b \in \mathbb{Z}^d). \tag{5}$$

For convenience we write

$$N_{\mathbf{r},\alpha} = \left\{x \in \mathbb{Z}^d \,:\, \tau_{\mathbf{r},\alpha}^k x = 0 \text{ for some } k \in \mathbb{N}\right\},$$

$$P_{\mathbf{r},\alpha} = \left\{x \in \mathbb{Z}^d \,:\, \tau_{\mathbf{r},\alpha}^k x = x \text{ for some } k \in \mathbb{N}_{>0}\right\}.$$

Lemma 6 can be useful for proving $\mathbf{r} \in \mathcal{D}_{d,\alpha}^0$ by taking $F = N_{\tau_{\mathbf{r},\alpha}}$.

Corollary 7 *Let E be a subset of $N_{\mathbf{r},\alpha}$ with the following properties:*

(i) $\pm\mathbf{e}_1, \ldots, \pm\mathbf{e}_d \in E$.

(ii) For every $e \in E$ we have $\tau_{\mathbf{r},0}(e), -\tau_{\mathbf{r},0}(-e) \in E$.

Then $\mathbf{r} \in \mathcal{D}_{d,\alpha}^0$.

Proof. Clear by Lemma 6 and (5). □

As the last component of the image under $\tau_{\mathbf{r},\alpha}$ of a vector of $\mathbb{Z}^d$ is most interesting we use the notation

$$A_m = \{(a_1, \dots, a_d) \in A \ : \ a_d = m\}$$

for $A \subset \mathbb{Z}^d$ and $m \in \mathbb{Z}$.

Corollary 8 *Let $E \subset \mathbb{Z}^d$ have the following properties:*

(i) $\pm\mathbf{e}_1, \dots, \pm\mathbf{e}_d \in E$

(ii) For every $e \in E$ we have $\tau_{\mathbf{r},0}(e), -\tau_{\mathbf{r},0}(-e) \in E$.

(iii) $\tau_{\mathbf{r},\alpha}(E) \subseteq E \cap E_0$

Then $\mathbf{r} \in \mathcal{D}^0_{d,\alpha}$.

Proof. In view of Corollary 2.7 the observation $E \subseteq N_{\mathbf{r},\alpha}$ suffices. □

Corollary 9 *Let $E \subset \mathbb{Z}^d$ have the the following properties:*

(i) E is finite.

(ii) E is $\tau_{\mathbf{r},\alpha}$-invariant.

(iii) $\pm\mathbf{e}_1, \dots, \pm\mathbf{e}_d \in E$.

(iv) For every $e \in E$ we have $\tau_{\mathbf{r},0}(e), -\tau_{\mathbf{r},0}(-e) \in E$.

(v) $E \cap P_{\mathbf{r},\alpha} = \{0\}$.

Then $\mathbf{r} \in \mathcal{D}^0_{d,\alpha}$.

Proof. By Corollary 2.7 it suffices to show that $E \subseteq N_{\mathbf{r},\alpha}$. Assume that there is some $e \in E$ with $\tau^k_{\mathbf{r},\alpha}(e) \neq 0$ for all $k \in \mathbb{N}$. By (i) and (ii) there are $k < m$ with $\tau^k_{\mathbf{r},\alpha}(e) = \tau^m_{\mathbf{r},\alpha}(e)$, hence $\tau^{m-k}_{\mathbf{r},\alpha}(\tau^k_{\mathbf{r},\alpha}(e)) = \tau^k_{\mathbf{r},\alpha}(e)$, thus $\tau^k_{\mathbf{r},\alpha}(e) \in E \cap P_{\mathbf{r},\alpha} = \{0\}$: Contradiction. □

The next lemma is trivial, but often used in the following.

Lemma 10

(i) If $A \subseteq \mathbb{Z}^d$ with $\tau_{\mathbf{r},\alpha}(A) \subseteq A \cap A_0$ then $A \subseteq N_{\mathbf{r},\alpha}$.

(ii) Let $E = [-b, b]^d \cap \mathbb{Z}^d$ with $b \in \mathbb{N}$. If

$$-b \leq \sum_{i=1}^{d} r_i e_i < b + 1$$

for all $e \in E$ then we have

$$\tau_{(r_1,\dots,r_d),0}(e), \quad -\tau_{(r_1,\dots,r_d),0}(-e) \in E.$$

(iii) Let $E = \{-1, 0, 1\}^d$ *and assume*

$$-1 \le \sum_{i=1}^{d} r_i e_i < 2 - \alpha$$

for all $e \in E$. *If* $(1, \ldots, 1) \in N_{\mathbf{r},\alpha}$ *and* $E_0 \cup E_{-1} \subseteq N_{\mathbf{r},\alpha}$ *then* $\mathbf{r} \in \mathcal{D}^0_{d,\alpha}$.

Proof. (i) and (ii) are obvious, while (iii) is clear by (ii) and Corollary 9. □

The following statement essentially is a result of Akiyama *et al.* [3, Theorem 3.3] where an idea of Hollander [11] was exploited.

Theorem 11 *If one of the following conditions holds then* $(r_1, \ldots, r_d) \in \mathcal{D}^0_{d,\alpha}$*:*

(i) $r_1, \ldots, r_d \ge 0$ *and* $\sum_{i=1}^{d} r_i < 1 - \alpha$.

(ii) $0 < \alpha < \frac{1}{2}$, $r_1, \ldots, r_d \le 0$ *and* $\sum_{i=1}^{d} r_i \ge -\alpha$.

(iii) $\alpha \ge \frac{1}{2}$, $r_1, \ldots, r_d \le 0$ *and* $\sum_{i=1}^{d} r_i > -1 + \alpha$.

Proof. Let $E = \{-1, 0, 1\}^d$. Then (i) is proved analogously as [3, Theorem 3.3] using Lemma 10 and Corollary 9, (ii) is clear by Corollary 8, and for (iii) we use Corollary 9. □

Now we are in a position to determine the above sets (2) in the nearly trivial case $d = 1$, thereby slightly extending results of [1, Proposition 4.4] and [6]. In Section 3 we shall use Proposition 12 to completely describe α-CNS polynomials of the simple shape $X^d + c$.

Proposition 12 *We have* $\mathcal{D}_{1,\alpha} = [-1, 1]$ *and*

$$\mathcal{D}^0_{1,\alpha} = \begin{cases} [-\alpha, 1 - \alpha) & \text{if} \quad \alpha < 1/2, \\ (-1 + \alpha, \alpha] & \text{if} \quad \alpha \ge 1/2. \end{cases}$$

Proof. By (4) we have $[-1, 1] \subseteq \mathcal{D}_{1,\alpha} \subseteq \overline{\mathcal{E}_1} = [-1, 1]$. □

Many examples suggest that the open unit circle contains all eigenvalues of the matrix $R(\mathbf{r})$ provided $\mathbf{r} \in \mathcal{D}^0_{d,\alpha}$ (cf. [2]).

Conjecture 13 If $\alpha \in [0, 1)$ and $\mathbf{r} \in \mathcal{D}^0_{d,\alpha}$ then all roots of $\chi_{\mathbf{r}}$ lie inside the open unit circle.

Note that Conjecture 13 holds for real roots of $\chi_{\mathbf{r}}$ (see Lemma 5). It would be helpful in carrying over results for α-CNS polynomials (see Section 3, in particular Theorem 15) to arbitrary elements of $\mathbb{R}^d$.

3. α-CNS Polynomials

In this section we study the set $\mathcal{C}_{d,\alpha}$ of α-CNS polynomials, i.e., the nonconstant integral polynomials $P(X) = p_d X^d + p_{d-1}X^{d-1} + \cdots + p_1 X + p_0$ with $p_d = 1$ and $|p_0| > 1$ (see [14, Theorem 4.2]) such that

$$\mathbf{r} = \left(\frac{1}{p_0}, \frac{p_{d-1}}{p_0}, \ldots, \frac{p_1}{p_0}\right) \in \mathcal{D}^0_{d,\alpha}.$$

Thus the components of $\mathbf{r}$ and the coefficients of P are related by

$$\mathbf{r}_i = \frac{p_{d+1-i}}{p_0} \qquad (i = 1, \ldots, d), \tag{6}$$

and for the characteristic polynomial $\chi_{\mathbf{r}}$ of $\mathbf{r}$ we have the relation

$$X^d \chi_{\mathbf{r}}\left(\frac{1}{X}\right) = \frac{1}{p_0} P(X). \tag{7}$$

We first state a direct consequence of [12, Proposition 2.2]; it was already mentioned by Surer [14].

Theorem 14 (Pethő) *Let $P \in \mathcal{C}_{d,\alpha}$ and $A \in \mathbb{Z}[X] \setminus \{0\}$. Then there are uniquely determined*

$$a_0, \ldots, a_\ell \in [-\alpha\,|P(0)|\,, (1-\alpha)\,|P(0)|) \cap \mathbb{Z}, \qquad a_\ell \neq 0,$$

such that

$$A \equiv \sum_{i=0}^{\ell} a_i X^i \pmod{P}.$$

The following statement is well-known for the case $\alpha = 0$ [12, Theorem 6.1]. For the convenience of the reader we repeat its proof in our surroundings.

Theorem 15 (Pethő) *Let $P \in \mathcal{C}_{d,\alpha}$. Then all roots of P lie outside the closed unit circle.*

Proof. By [14, Theorem 2.1] and (7) all roots of P have modulus at least 1. Now, assume that ζ is a root of P with $|\zeta| = 1$. By [10, Satz 3] ζ is an algebraic unit, hence it must be a root of unity. Let $m \geq 1$ such that $\zeta^m = 1$. Clearly, the polynomial $Q = (P, X^m - 1)$ is nonconstant. Let $T \in \mathbb{Z}[X]$ such that $QT = P$. Then

$$T \equiv X^m T \pmod{P}$$

and P does not divide T. By Theorem 14 we find uniquely determined

$$a_0, \dots, a_\ell \in [-\alpha\,|P(0)|\,, (1-\alpha)\,|P(0)|) \cap \mathbb{Z}, \qquad a_\ell \neq 0,$$

such that

$$T \equiv \sum_{i=0}^{\ell} a_i X^i \pmod{P}.$$

On the other hand we also have

$$\sum_{i=0}^{\ell} a_i X^{m+i} \equiv X^m T \equiv T \pmod{P}$$

contradicting the uniqueness of the representation. □

Corollary 16 *Let $P \in \mathcal{C}_{d,\alpha}$. Then*

$$\operatorname{sgn}(P(-1)) = \operatorname{sgn}(P(1)) = \operatorname{sgn}(P(0)).$$

In Section 4 we shall extensively use Proposition 17 which plays a key role in finding necessary conditions on α-CNS polynomials. It slightly extends [5, Lemma 2].

Proposition 17 *Let $X^d + \sum_{i=0}^{d-1} p_i \in \mathcal{C}_{d,\alpha}$.*

(i) If $p_0 > 0$ then $\sum_{i=1}^{d-1} p_i \geq -1 - \alpha p_0$, and

$$\sum_{i=1}^{d-1} (-1)^i p_i > (-1)^{d-1} - (1-\alpha)p_0 \qquad \text{or} \qquad \sum_{i=1}^{d-1} (-1)^i p_i \geq (-1)^{d-1} - \alpha p_0.$$

(ii) If $p_0 < 0$ then $\sum_{i=1}^{d-1} p_i \leq -1 - \alpha p_0$, and

$$\sum_{i=1}^{d-1} (-1)^i p_i < (-1)^{d-1} - (1-\alpha)p_0 \qquad \text{or} \qquad \sum_{i=1}^{d-1} (-1)^i p_i \leq (-1)^{d-1} - \alpha p_0.$$

(iii) If $\alpha \geq \frac{1}{2}$ then $\sum_{i=1}^{d-1} p_i \neq -1 - \alpha p_0$.

Proof. This follows from Lemma 5, Corollary 16, and (7). □

We can now completely describe α-CNS polynomials with the least number of nonzero coefficients.

Theorem 18 *Let $d, c \in \mathbb{Z}, d > 0, |c| > 1$.*

(i) If $0 \leq \alpha < \frac{1}{2}$ then $X^d + c \in \mathcal{C}_{d,\alpha}$ if and only if $c \geq 2$ or $\alpha > 0$ and $c \leq -\frac{1}{\alpha}$.

(ii) If $\alpha \geq \frac{1}{2}$ then $X^d + c \in \mathcal{C}_{d,\alpha}$ if and only if $c \geq 2$ or $c < -\frac{1}{1-\alpha}$.

Proof. This is a direct consequence of Theorem 4 and Proposition 12. □

4. Symmetric CNS Trinomials

From now on, we concentrate on symmetric CNS polynomials, i.e., on the sets $\mathcal{C}_d^\star = \mathcal{C}_{d,1/2}$, which were first introduced by Akiyama–Scheicher [6]. We aim at an extension of a theorem of Akiyama–Scheicher on quadratic symmetric CNS polynomials. More specifically, we characterize symmetric CNS trinomials of the shape

$$X^d + bX + c \qquad (d > 2). \tag{8}$$

Furthermore, several results for arbitrary symmetric CNS trinomials are given if no extra effort is required.

We first describe trinomials with vanishing linear coefficient. This is the simplest case and it directly stems from Theorem 18.

Theorem 19 *Let $d, c \in \mathbb{Z}, d > 0, |c| > 1$. Then $X^d + c \in \mathcal{C}_d^\star$ if and only if $c \leq -3$ or $c \geq 2$.*

For completeness sake we restate the result of Akiyama–Scheicher in the following form (see [6, Theorem 5.2]).

Theorem 20 (Akiyama–Scheicher) *Let $b, c \in \mathbb{Z},\ |c| > 1$. Then $X^2 + bX + c \in \mathcal{C}_2^\star$ if and only if*

$$-\frac{1}{2}(c+1) \leq b \leq \frac{1}{2}(c+2) \qquad (c > 0),$$

or

$$\frac{1}{2}(c+2) \leq b \leq -\frac{1}{2}(c+3) \qquad (c < 0).$$

Our first goal is a collection of necessary CNS conditions. These are derived from easy to state root properties of CNS polynomials and from the exclusion of certain patterns of periodic elements.

Lemma 21 *Let $d, q \in \mathbb{N}, 0 < q < d$ and $f = X^d + bX^q + c \in \mathbb{R}[X]$.*

(i) If $|b| > 1 + |c|$ then f has q roots in the open unit circle.

(ii) Let $|c| \geq 1$ and $b = c + \eta$ where $\eta \in \{0, 1\}$ if c is positive, and $\eta \in \{-1, 0\}$ if c is negative. If $1 < q < d$ and q does not divide d then f has a root inside the open unit circle.

(iii) Let $d \geq 3, q = 1,\ |b| = |c| = 2$ and $f \neq X^3 - 2X - 2, X^3 - 2X + 2$. Then f has a root inside the open unit circle.

Proof. (i) is clear by Rouché's theorem. For (ii), we make use of Bohl's theorem [8] and denote by t the greatest common divisor of q and d. Observe that the integer $a = q/t$ is at least 2.

For $\eta = 0$ the first part of this theorem applies. Hence, it suffices to show that the open interval $I = (\gamma - \delta, \gamma + \delta)$ contains an integer where γ is some real number and $\delta = (dw_1 + qw_2)/(2\pi t)$; here w_1 (resp. w_2) is the size of the angle opposite to the side of length 1 (resp. $|c|$) of the triangle with sides of lengths $1, |c|, |c|$. Clearly $w_2 < \pi/2$ and therefore $\delta = (d\pi + (q - 2d)w_2)/(2\pi t) > a/4$. Thus I contains the closed interval $[\gamma - a/4, \gamma + a/4]$ of length $a/2 \geq 1$. Hence there is at least one integer in I, and we conclude that f has a root inside the unit circle.

Finally let $\eta \neq 0$. By the second part of Bohl's theorem the polynomial f has at least $a - 1$ roots inside the unit circle.

(iii) Cubic polynomials can be checked directly. Analogously as above, for $d > 3$ the statement can be derived from the first case of Bohl's theorem [8]. □

From now on, let $P = X^d + bX^q + c \in \mathbb{Z}[X]$ be a monic trinomial with $0 < q < d \geq 3$ and $|c| > 1$. The corresponding maps $\tau, \tau_0 : \mathbb{Z}^d \to \mathbb{Z}^d$ are given by (see (6))

$$\tau(a_1, \ldots, a_d) = \left(a_2, \ldots, a_d, -\left\lfloor \frac{a_1 + ba_{d+1-q}}{c} + \frac{1}{2} \right\rfloor\right),$$

and

$$\tau_0(a_1, \ldots, a_d) = \left(a_2, \ldots, a_d, -\left\lfloor \frac{a_1 + ba_{d+1-q}}{c} \right\rfloor\right).$$

Thus, only the components a_1 and a_{d+1-q} control the actions of τ and τ_0 on $a \in \mathbb{Z}^d$. Therefore the case $q = 1$ is particularly simple because then only the first and last components of $a \in \mathbb{Z}^d$ have to be taken into account.

We often need the set $E = \{-1, 0, 1\}^d$.

Example 22 For $d \geq 3$ we have $X^d - X + 2 \in \mathcal{C}_d^\star$ by Corollary 2.7: It can easily be checked that $\tau_0(e), -\tau_0(-e) \in E$ for all $e \in E$. By induction on m we see

$$(\underbrace{-1, \ldots, -1}_{m}, 0, \ldots, 0) \in N_\tau.$$

Successively we deduce

$$(0, \ldots, 0, \underbrace{-1, \ldots, -1}_{m}) \in N_\tau \qquad (m = 1, \ldots, d),$$

$$(\underbrace{1, \ldots, 1}_{m}, 0, \ldots, 0, \underbrace{-1, \ldots, -1}_{t}) \in N_\tau \qquad (m = 1, \ldots, d-1, \quad 1 \leq t \leq d - m),$$

$$(\underbrace{1, \ldots, 1}_{m}, 0, \ldots, 0) \in N_\tau \qquad (m = 1, \ldots, d).$$

Now, we show $E_0 \cup E_{-1} \subset N_\tau$ by induction on the number of final zeros of $e \in E_0 \cup E_{-1}$. Finally, we have $E \subset N$ because if $e \in E_1$ then either $\tau^k(e) = (1, \ldots, 1)$ or $\tau^k(e) \in E_0 \cup E_{-1}$ for some $k \in \mathbb{N}$.

Lemma 23 *Let $(q,d)=1$ and $P \in \mathcal{C}_d^\star$.*

(i) Let $c>0$. If d is even then we have

$$-\frac{1}{2}(c+1) \le b \le \frac{1}{2}(c+2).$$

If d is odd then we have

$$-\frac{1}{2}(c-2) \le b \le c-1 \qquad (q \text{ even}),$$

and

$$-\frac{1}{2}(c+1) \le b \le \frac{1}{2}(c-2) \qquad (q \text{ odd}).$$

(ii) Let $c<0$. Then we have $b \le -\frac{1}{2}(c+3)$. If d is even then $\frac{1}{2}(c+2) \le b$, and if d is odd then we have $\frac{1}{2}(c-2) \le b$.

Proof. By Theorem 15 and Lemma 21 (i) we have $|b| \le 1+|c|$. An easy application of Proposition 17 and Lemma 21 (ii) completes the proof. □

In view of Theorem 4 the following result describes all symmetric CNS trinomials of degree at least 3 whose constant term moduli equal 2.

Theorem 24 *Let $d \ge 3$, $0<q<d$, $(q,d)=1$, and $P = X^d + bX^q + c$ with $c \in \{-2,2\}$. Then P is a symmetric CNS trinomial if and only if $P = X^d+2$ or $P = X^d - X + 2$.*

Proof. First assume $P \in \mathcal{C}_d^\star$. Let $c=2$. If d is odd then Lemma 4.5 implies $b \in \{0,1\}$ (q even) and $b \in \{-1,0\}$ (q odd). But for q even the polynomial $X^d+X^q+2 \notin \mathcal{C}_d^\star$ because $(-1,0,\dots,0,-1,0,\dots,0)$ (with -1 at positions 1 and $d+1-q$) is periodic for τ. Otherwise, if $q>1$ then $X^d - X^q + 2 \notin \mathcal{C}_d^\star$ because the element $(B,\dots,B,0,\dots,0)$, whose first elements are $t-1$ strings $B=(0,\dots,0,-1)$ of length q, is periodic for τ; here $t \in \mathbb{N}$ is defined by $(t-1)q < d+1 \le tq$. If d is even then Lemma 4.5 and Lemma 4.3 (iv) show $-1 \le b \le 1$, but $b \ne 1$: $X^d+X^q+2 \notin \mathcal{C}_d^\star$ because if $(q,d)=(1,3)$ then $(1,-1,1)$ is periodic for τ, and otherwise $(-1,0,\dots,0,-1,0,\dots,0)$ (with -1 at positions 1 and $d+1-q$) is periodic for τ.

Now, let $c=-2$. Lemma 4.5 and Theorem 4.1 show $-2 \le b \le -1$ and d odd. If $b=-2$ then Lemma 4.3 (ii) gives $q=1$ and then by Lemma 4.3 (iii) we find $P = X^3-2X-2$. But this polynomial is not a symmetric CNS polynomial because its τ has the periodic element $(-1,0,0)$. Likewise, the assumption $b=-1$ is impossible: $X^d-X^q-2 \notin \mathcal{C}_d^\star$ because $(-1,0,\dots,0)$ is periodic for τ.

On the other hand, Theorem 4.1 and Example 4.4 show that both X^d+2 and X^d-X+2 belong to $\mathcal{C}_d^\star$. □

For larger values of c the next Lemma prepares useful conditions on the coefficient b such that P be a symmetric CNS polynomial.

Lemma 25 *If $|c| \geq 3$ and $|b| \leq \frac{1}{2}(|c|+2)$ then we have for every $e \in E$:*

(i) $\tau(e) \in E$,

(ii) $\tau_0(e), -\tau_0(-e) \in E$ *provided*

$$-\frac{1}{2}(c+1) \leq b \quad (\textit{if } c > 0) \qquad \textit{or} \qquad b \leq -\frac{1}{2}(c+3) \quad (\textit{if } c < 0).$$

Proof. (i) It suffices to check that for $\delta, \eta \in \{-1, 0, 1\}$ we have

$$-1 \leq \frac{\delta + \eta b}{c} + \frac{1}{2} < 2.$$

(ii) This can easily be checked. □

We can now exhibit some symmetric CNS trinomials with large constant terms. Note that Theorem 11 yields Proposition 26 in case $b \geq 0$.

Proposition 26 *If $|c| \geq 3$ and $|b| \leq \frac{1}{2}(|c|-3)$ then $X^d + bX^q + c$ is a symmetric CNS trinomial.*

Proof. Using Lemma 25 and observing $\pm\mathbf{e}_1, \ldots, \pm\mathbf{e}_d \in E$ it suffices to show that $E \cap P_\tau = \{0\}$ because then our assertion follows from Corollary 9. Assume that there is a nonzero periodic element $(e_i)_{i\geq 1}$ with components in $\{-1, 0, 1\}$ having at least one negative component (see (1)). Without loss of generality, let $e_{d+1} = -1$. Hence, by (1)

$$0 \leq \frac{e_1 + be_{d+1-q}}{c} - 1 + \frac{1}{2} < 1,$$

which is impossible. Therefore all components must be nonnegative and by shifting indices if necessary we may assume $e_{d+1} = 1$. Hence,

$$0 \leq \frac{e_1 + be_{d+1-q}}{c} + 1 + \frac{1}{2} < 1,$$

which is impossible, too. □

In view of Theorem 4, the following result extends Theorem 20 for symmetric CNS trinomials of the shape (8) whose constant term magnitudes exceed 2.

Theorem 27 *Let $d \geq 3$ and $|c| \geq 3$. Then $X^d + bX + c$ is a symmetric CNS trinomial if and only if one of the following conditions (i) or (ii) holds:*

(i) *c is positive, $-\frac{1}{2}(c+1) \le b$, and*

$$b \le \frac{1}{2}(c+2) \quad (\textit{if } d \textit{ is even}) \qquad \textit{or} \qquad b \le \frac{1}{2}(c-2) \quad (\textit{if } d \textit{ is odd}).$$

(ii) *c is negative, $b \le -\frac{1}{2}(c+3)$, and*

$$\frac{1}{2}(c+2) \le b \quad (\textit{if } d \textit{ is even}) \qquad \textit{or} \qquad \frac{1}{2}(c-2) \le b \quad (\textit{if } d \textit{ is odd}).$$

Proof. If $X^d + bX + c \in \mathcal{C}_d^\star$ then the assertion follows from Lemma 23. Now, let us assume that conditions (i) holds. We distinguish three cases.

`Case 1:` $-\frac{1}{2}(c+1) \le b < -\frac{1}{2}(c-3)$. The assertion is a consequence of Lemma 25 and Lemma 10 once the following easy steps are verified successively:

(i) $\tau(E_0) \subseteq E_0 \subseteq N_\tau$.

(i) $\tau(E_{-1}) \in E_0 \cup E_{-1}$.

(iii) $\tau(E_1) \in E_0 \cup E_1$.

(iv) $E_{-1} \subset N_\tau$.

(v) $(1, \dots, 1) \in N_\tau$.

`Case 2:` $-\frac{1}{2}(c-3) \le b \le \frac{1}{2}(c-3)$. This is clear by Proposition 26.

`Case 3:` $\frac{1}{2}(c-3) < b$. Similarly as above, Corollary 9 and Lemma 10 apply here by showing the following facts:

(i) If $e \in E$ then $\tau(E) \in E_0 \cup E_{-e_d}$.

(ii) If $e \in E_{-1}$ and $e_1 = 1$ then $\tau(e) \in E_0$.

(iii) By the above and Lemma 2.10 we have $E_0 \subset N_\tau$.

(iv) $E_{-1} \subset N_\tau$: Let $e \in E_{-1}$. If d is even then either $\tau^k(e) \in E_0$ for some $k \le d$ or $\tau^d(e) = (1, -1, \dots, 1, -1)$ which implies $\tau^{d+1}(e) \in E_0$. If d is odd, c is even, and $b = \frac{1}{2}(c-2)$ then $\tau^d(e) \in E_0$.

(v) $E \subset N_\tau$ because for $e \in E \setminus (E_0 \cup E_{-1})$ we have $\tau(e) \in E_0 \cup E_{-1}$.

The proof for $c < 0$ can be completed analogously and is left to the reader. □

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, T. Borbély, H. Brunotte, A. Pethő and J. M. Thuswaldner, *Basic properties of shift radix systems*, Acta Math. Acad. Paed. Nyiregyhaziensis **22** (2006), 19 – 25.

[3] S. Akiyama, H. Brunotte, A. Pethő and J. M. Thuswaldner, *Generalized radix representations and dynamical systems II*, Acta Arith. **121** (2006), 21 – 61.

[4] S. Akiyama, H. Brunotte, A. Pethő and J. M. Thuswaldner, *Generalized radix representations and dynamical systems III*, Osaka J. Math. **45** (2008), 347 – 374.

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

[6] S. Akiyama and K. Scheicher, *Symmetric shift radix systems and finite expansions*, Mathematica Pannonica **18**, no. 1 (2007), 101 – 124.

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

[8] P. Bohl, *Zur Theorie der trinomischen Gleichungen*, Math. Ann. **65** (1908), 556 – 566.

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

[10] F. Halter-Koch, *Algebraische Zahlen mit Konjugierten auf dem Einheitskreis*, Arch. Math. **22** (1971), 161 – 164.

[11] M. Hollander, *Linear Numeration Systems, Finite Beta Expansions, and Discrete Spectrum of Substitution Dynamical Systems*, PhD Thesis, Washington University, 1996.

[12] 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 – 43.

[13] A. Pethő, *Notes on CNS polynomials and integral interpolation*, More sets, graphs and numbers, pp. 301 – 315, Bolyai Soc. Math. Stud., 15, Springer, Berlin, 2006.

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