REDUCIBLE CUBIC CNS POLYNOMIALS

SHIGEKI AKIYAMA, HORST BRUNOTTE, AND ATTILA PETHŐ

Abstract. The concept of a canonical number system can be regarded as a natural generalization of decimal representations of rational integers to elements of residue class rings of polynomial rings. Generators of canonical number systems are CNS polynomials which are known in the linear and quadratic cases, but whose complete description is still open. In the present note reducible CNS polynomials are treated, and the main result is the characterization of reducible cubic CNS polynomials.

1. Introduction

Canonical number systems have been introduced as natural generalizations of the classical decimal representation of the rational integers to algebraic integers. We refer the reader to [7] for a detailed account on the historical development and the connections of the concept of canonical number systems to other theories, e.g. shift radix systems, finite automata or fractal tilings.

Let us briefly recall the main definitions for our purposes here. Consider a monic integral polynomial $P = X^d + p_{d-1}X^{d-1} + \cdots + p_0$ with $p_0 \neq 0$. P is called a *CNS polynomial* (see [18]) if for every $A \in \mathbb{Z}[X]$ there exist $a_0, ..., a_\ell \in \{0, 1, \ldots, |p_0| - 1\}$ such that

$$A \equiv a_0 + a_1 X + \cdots + a_\ell X^\ell \pmod{P}.$$

In this case, the pair $(\alpha, \{0, 1, \ldots, |P(0)| - 1\})$ is called a *canonical number system (CNS)* where α is a root of P. As the main ingredient of a canonical number system is the CNS polynomial P we restrict our attention to CNS polynomials.

The characterization of linear and quadratic CNS polynomials is well-known (see e.g. [14, 13, 10, 11]), however, for higher degrees only partial results have been achieved (see e.g. [15, 14, 13, 5, 6, 21, 4, 20, 9]). An important class of reducible CNS polynomials of arbitrary degrees has systematically been studied by Pethő [19] in connection with integral interpolation. Similar investigations have been performed by Kane [12].

In particular, the complete description of cubic CNS polynomials is still an open problem. Therefore, the characterization of reducible cubic CNS polynomials which is the main goal of this short note (Section 3) seems to be interesting. In Section 2 we collect some observations on reducible CNS polynomials.

2. On reducible CNS polynomials

It is well-known that a reducible quadratic polynomial is a CNS polynomial if and only if both factors are CNS polynomials. This equivalence does no longer hold for polynomials of higher degrees (see e.g. Example 3.3). In the following Proposition we resume some facts on factors of CNS polynomials.

Proposition 2.1. (i) *Let $P = \sum_{i=0}^{d} p_i X^i$ be a non-constant factor of a CNS polynomial. Then P is expanding (i.e. all of its zeroes have modulus greater than one) and without*

Date: 22nd July 2007.

2000 *Mathematics Subject Classification.* 11A63, 12D99.

Key words and phrases. CNS polynomial, canonical number system, radix representation.

The first author is supported by the Japanese Ministry of Education, Culture, Sports, Science and Technology, Grand-in Aid for fundamental research 18540022, 2006–2008.

The third author was supported partially by the Hungarian National Foundation for Scientific Research Grant No. K67580.

positive roots. Further, for every $A \in \mathbb{Z}[X]$ there are some $n, k \in \mathbb{N}, k < n$ such that

$$T^n(A) \equiv T^k(A) \bmod P$$

where

$$T\Big(\sum_{i=0}^{m} a_i X^i\Big) = \sum_{i=0}^{m-1} a_{i+1} X^i \; - \; \lfloor \frac{a_0}{p_0} \rfloor \sum_{i=0}^{d-1} p_{i+1} X^i.$$

(ii) *Let $a \in \mathbb{N}, a \geq 2$ and $Q \in \mathbb{Z}[X]$ be monic. If $(X+a) \cdot Q$ is a CNS polynomial then $a(Q(0) - Q(1)) \leq Q(1)$.*

Proof. (i) This is clear by [18], see also [6] and [19].
(ii) Let $Q = \sum_{i=0}^{d} q_i X^i, q_d = 1$, hence

$$(X+a) \cdot Q = X^{d+1} + \sum_{i=1}^{d} (q_{i-1} + a q_i) X^i + a q_0$$

which immediately yields the assertion by [5, Lemma 4], which is called 1-subsum condition in [6]. □

Now we exploit a fundamental theorem of Kovács - Pethő for the construction of examples of CNS polynomials of arbitrary degrees which are products of a linear factor and an irreducible CNS polynomial.

Proposition 2.2. *Let $m, a, q_1 \in \mathbb{N},\ m \geq 3,\ a \geq 2,\ q_1 \geq 1$ and q_0 a prime with $q_0 > m q_1$. For $i = 1, \ldots, m-2$ set*

$$q_{i+1} = \min\big\{m q_i, \Big\lfloor \frac{(a-1)q_i + q_{i-1}}{a} \Big\rfloor\big\}.$$

Then the polynomial

$$Q = X^m + \sum_{i=0}^{m-1} q_i X^i$$

is irreducible, and both Q and $(X+a) \cdot Q$ are CNS polynomials.

Proof. With $q_m := 1$ we have $q_i \leq q_{i-1} \quad (i = 0, \ldots, m)$. As $q_0 > m q_1 \geq \sum_{i=1}^{m} q_i$ the polynomial Q is irreducible by [17, Proposition 2.6.1]. Finally, by [2, Theorem 3.1] and [3, Theorem 3.4] the polynomials Q and $(X+a) \cdot Q$ are CNS polynomials. □

3. Reducible cubic CNS polynomials

In this section we completely describe reducible cubic CNS polynomials. Our proof makes extensive use of the results of [4]. Note that Theorem 3.1 shows that Gilbert's conjecture [10] holds for reducible cubic CNS polynomials (see also [4]).

Theorem 3.1. *Let $a, b, c \in \mathbb{Z}, a \geq 2$ and $P = (X+a)(X^2 + bX + c)$.*

(i) *Let $b^2 \geq 4c$. Then P is a CNS polynomial if and only if $3 \leq b \leq c$.*
(ii) *Let $b^2 < 4c$. Then P is a CNS polynomial if and only if the following conditions are satisfied.*
  (1) $a + b \geq 0$
  (2) $ab + a + b + c \geq -1$
  (3) $ab + c \leq 0 \implies a + b \leq ac - 2$
  (4) $1 \leq ab + c \leq ac - 1 \implies a + b \leq ac - 1$
  (5) $ab + c \geq ac \implies a + b \leq ac.$

Proof. (i) Clearly, P has only real roots.
If P is a CNS polynomial then all roots of it are less than -1 by [1], hence $c > 0$ and

$$\big(-b + \sqrt{b^2 - 4c}\big)/2 \;\; < \;\; -1$$

which implies the assertion.
On the other hand, if $3 \leq b \leq c$ then all roots of P are less than -1 and we are done by [8,

Corollary 5.2].
(ii) If P is a CNS polynomial then all conditions are satisfied by [4, Theorem 3.1].
On the other hand, if the conditions are satisfied then clearly $c \geq 1$. We distinguish several cases.
Case I. $ab + c \leq 0$.
If $ab + c = 0$ we are done by [4, Theorem 3.8]. If $ab + c < 0$ then $b \leq -1$. Now if $ab + a + b + c \leq 0$ we are done by [4, Proposition 3.2]. Therefore, let $ab + a + b + c > 0$. Then

$$(ab + c, a + b) \neq \frac{1}{3}\big(-(ac + 1), 2ac - 1\big),$$

and $a + b < 2ac/3$. Thus $c \geq 2$ and our assertion follows from [4, Proposition 3.3] (see Appendix, Proposition 4.2).
Case II. $0 < ab + c \leq ac - 1$.
If $a + b \leq (2ac - 1)/3$ we are done by [4, Proposition 3.10]. Therefore, let $a + b > (2ac - 1)/3$. Then $3(a + b) \geq 2ac$ and $c \geq 2$. The assumption $c = 2$ yields the polynomial $X^3 + 4X^2 + 5X + 6$ which is a CNS polynomial by [4, Theorem 3.9]. It is easy to check that $c > 2$ cannot occur.
Case III. $ab + c \geq ac$.
Then we find $4 > c\big(\frac{a-1}{a}\big)^2$ and one checks that $c \geq 6$ cannot occur. Thus we are left with $2 \leq c \leq 5$. The resulting polynomials and references for their CNS property are listed in Table 1.

c	b	a	$P(X) - X^3$	reference
2	1	2	$3X^2 + 4X + 4$	[4, Theorem 3.9]
2	1	≥ 2	$(a + 2)X^2 + 2(a + 1)X + 2a$	[4, Proposition 3.12]
3	2	2	$4X^2 + 7X + 6$	[4, Proposition 3.12]
3	2	3	$5X^2 + 9X + 9$	[4, Theorem 3.9]
3	3	≥ 3	$(a + 3)X^2 + 3(a + 1)X + 3a$	[4, Proposition 3.12]
4	2	2	$4X^2 + 8X + 8$	[4, Theorem 3.9]
4	3	2	$5X^2 + 10X + 8$	[4, Proposition 3.12]
4	3	3	$6X^2 + 13X + 12$	[4, Proposition 3.12]
4	3	4	$7X^2 + 16X + 16$	[4, Theorem 3.9]

Table 1

□

Corollary 3.2. (i) *The product of three linear CNS polynomials is a CNS polynomial.*
(ii) *The product of a linear and a quadratic CNS polynomial is a CNS polynomial.*

The converse of Corollary 3.2 (ii) does not hold for cubic polynomials with a non-real root as the following example shows.

Example 3.3. The product of $X + 2$ and the non CNS polynomial $X^2 - 2X + 3$ (see e.g. [10]) is a CNS polynomial by Theorem 3.1.

4. Appendix

For the sake of completeness we give a modified statement (see Proposition 4.2 below) and proof of [4, Proposition 3.3]. Note that for instance the polynomial $X^3 + 5X^2 - 3X + 8$ satisfies the prerequisites of [4, Proposition 3.3], but is not a CNS polynomial by Counterexample (i) of the same paper.

Lemma 4.1. *The polynomial $X^3 + p_2X^2 + p_1X + p_0 \in \mathbb{Z}[X]$ is a CNS polynomial if*

$$p_1 \leq -1, 0 \leq p_2 < \min\{p_0 - 1, \frac{2}{3}p_0\}, 1 + p_1 + p_2 \geq 0, \text{ and } (p_1, p_2) \neq (-\frac{1}{3}(p_0 + 1), \frac{1}{3}(2p_0 - 1)).$$

Proof. In view of [4, Proposition 3.2] we may restrict to the case $p_1+p_2 \geq 1$, hence

$$1 \leq p_2 \leq \frac{1}{3}(2p_0-1).$$

If $p_1-p_2 > -p_0$ then $P=X^3+p_2X^2+p_1X+p_0 \in \mathbb{Z}[X]$ satisfies the dominant condition and [6, Theorem 5.3, Theorem 3.5] and [4] yield our assertion.

Finally, let $p_1-p_2 \leq -p_0$. Then we have

$$-\frac{2}{3}p_0+\frac{4}{3} \leq p_1 \leq -\frac{1}{3}p_0-\frac{1}{3},\ \ \frac{1}{3}p_0+\frac{4}{3} \leq p_2 \leq \frac{2}{3}p_0-\frac{1}{3},\ \ p_0 \geq 5,\ \ p_1+2p_2 \leq p_0-1.$$

One checks that the points $(0,0,1),(0,1,0),(0,1,1),(1,1,0),(1,0,0),(1,0,-1),(0,-1,0),$

$$(0,0,-1),(-1,0,0),(0,-1,-1),(-1,0,1),(1,1,-1),(0,1,2),(1,0,-2),(0,0,2),(0,2,1),(0,1,-1)$$

belong to the set N of elements of $\mathbb{Z}^3$ which fall into the zero cycle under the iterates of τ_P (we refer the reader to [4] for the definition). Now we distinguish several cases.

Case I. $p_1-p_2 < -p_0$

Then $p_1 \leq -\frac{1}{3}p_0-\frac{4}{3}, \frac{1}{3}p_0+\frac{7}{3} \leq p_2, 0 < p_1+2p_2 \leq p_0-2$, hence $(1,2,1),(2,1,-1),(1,-1,-1),$ $(-1,-1,1),(-1,-1,0),(1,-1,-2),(-1,-2,-1),(-1,1,1),(-1,1,2) \in N$.

Case I.1 $2p_2 \leq p_0-1$

Observing $(0,-2,-1),(-2,-1,1) \in N$ we have found a set of witnesses and conclude P is a CNS polynomial.

Case I.2 $2p_2 > p_0-1$

Now, $(1,2,0),(0,2,2),(2,2,0),(2,0,-2),(0,-2,-1),(-2,-1,1),(0,-2,-2),(0,2,0),(-2,0,2),$ $(2,1,-2),(1,-2,-2),(-2,-2,0),(1,1,1),(1,1,-2),(-1,2,2) \in N$, and we finish our argument as above.

Case II. $p_1-p_2=-p_0$

Then $p_1+2p_2 \leq p_0-1$.

Case II.1 $p_1+p_2=1$

Then $p_1=-\frac{1}{2}p_0+\frac{1}{2}, p_2=\frac{1}{2}p_0+\frac{1}{2},\ \ p_1+2p_2 \leq p_0-1$, hence $(-1,-1,1),(-1,1,2),(1,2,1),$

$$(2,1,-1),(1,-1,-1),(-1,-1,0),(0,2,2),(2,2,0),(2,0,-2),(1,-1,-2),(-1,-2,-1),$$

$$(0,-2,-1),(-2,-1,1),(-1,1,1),(0,-2,-2),(2,1,-2),(1,-2,-2),(-2,-2,-0),(-1,-2,0),$$

$(-2,0,2),(1,1,1),(1,1,-2),(-1,2,2),(1,2,0) \in N$, and we finish our argument as above.

Case II.2 $p_1+p_2>1$

Then $\frac{1}{2}p_0+1 \leq p_2 \leq \frac{2}{3}p_0-\frac{2}{3},\ \ -\frac{1}{2}p_0+1 \leq p_1$, hence $(0,1,2),(1,2,1),(2,1,-1),(1,2,0),$

$$(2,0,-2),(1,-1,-1),(-1,-1,0),(-1,-1,1),(0,-2,-1),(1,-1,-2),(-1,-2,-1),$$

$(-2,-1,1),(-1-2,0),(0,2,0),(-2,0,2),(0,-1,1),(-1,1,1),(-1,1,2) \in N$, and the proof is completed. □

Proposition 4.2. *Let $P=X^3+p_2X^2+p_1X+p_0 \in \mathbb{Z}[X]$ with $p_1 \leq -1,\ 0 \leq p_2 < \min\{p_0-1, \frac{2}{3}p_0\}$ and $1+p_1+p_2 \geq 0$. Then P is a CNS polynomial if and only if $p_0 \leq 7$ or $(p_1,p_2) \neq (-\frac{1}{3}(p_0+1), \frac{1}{3}(2p_0-1))$.*

Proof. Let P be a CNS polynomial. Then the assumption $p_0 > 7$ and $(p_1,p_2) = (-\frac{1}{3}(p_0+1), \frac{1}{3}(2p_0-1))$ contradicts Counterexample (i) of [4].

If $(p_1,p_2) \neq (-\frac{1}{3}(p_0+1), \frac{1}{3}(2p_0-1))$ the Lemma 4.1 yields our assertion. Let $p_0 \leq 7$. If $p_2=0$ then we use [4, Proposition 3.2], and if $p_2>0$ then we use Lemma 4.1 for $(p_1,p_2) \neq (-\frac{1}{3}(p_0+1), \frac{1}{3}(2p_0-1))$ or [6, Theorem 5.3, Theorem 3.5] and [4] for $(p_1,p_2) = (-\frac{1}{3}(p_0+1), \frac{1}{3}(2p_0-1))$ because then $p_0=5, p_1=-1, p_2=3$. □

References

[1] S. Akiyama, T. Borbély, H. Brunotte, A. Pethő and J. M. Thuswaldner, *On a generalization of the radix representation – a survey*, in "High Primes and Misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams", Fields Institute Commucations, vol. **41** (2004), 19–27.

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

[4] S. Akiyama, H. Brunotte and A. Pethő, *Cubic CNS polynomials, notes on a conjecture of W.J. Gilbert*, J. Math. Anal. and Appl. **281** (2003), 402–415.

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

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

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

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

[9] H. Brunotte, A. Huszti and A. Pethő, *Bases of canonical number systems in quartic algebraic number fields*, to appear in J. Th. Nombres Bordeaux

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

[11] E. H. Grossman, *Number bases in quadratic fields*, Studia Sci. Math. Hungar. **20** (1985), 55–58.

[12] D. M. Kane, *Generalized base representations*, J. Number Th. **120**, no. 1 (2006), 92–100.

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

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

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

[16] 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.

[17] M. Mignotte, D. Ştefănescu, *Polynomials – An algorithmic approach*, Springer, Berlin Heidelberg New York (1999)

[18] 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), 31–43.

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

[20] A. Pethő, *Connections between power integral bases and radix representations in algebraic number fields*, Proc. of the 2003 Nagoya Conf. "Yokoi-Chowla Conjecture and Related Problems", Furukawa Total Pr. Co. (2004), 115–125.

[21] K. Scheicher and J. M. Thuswaldner, *On the characterization of canonical number systems*, Osaka J. Math. **41**, no.2 (2004)

Department of Mathematics, Faculty of Science Niigata University, Ikarashi 2-8050, Niigata 950-2181, JAPAN
E-mail address: akiyama@math.sc.niigata-u.ac.jp

Haus-Endt-Strasse 88, D-40593 Düsseldorf, GERMANY
E-mail address: brunoth@web.de

Department of Computer Science, University of Debrecen, P.O. Box 12, H-4010 Debrecen, HUNGARY
E-mail address: pethoe@inf.unideb.hu