1

Cubic CNS polynomials, notes on a conjecture of W.J. Gilbert

Shigeki Akiyama[†]
Department of Mathematics, Faculty of Science,
Niigata University, Ikarashi 2-8050, Niigata 950-2181, Japan,
Horst Brunotte
Haus-Endt-Str. 88, D - 40593 Düsseldorf, Germany
and
Attila Pethő[‡]
Institute of Mathematics and Computer Science, University of Debrecen,
P.O. Box 12, H - 4010 Debrecen, Hungary

October 14, 2002

Abstract

A conjecture of W. J. Gilbert's on canonical number systems which are defined by cubic polynomials is partially proved, and it is shown that the conjecture is not complete. Applications to power integral bases of simplest and pure cubic number fields are given thereby extending results of S. Körmendi.

1 Introduction

Let $P \in \mathbf{Z}[X]$ be a monic polynomial with $|P(0)| > 1$ and $\mathcal{N} = \{0, 1, \ldots, |P(0)| - 1\}$. The pair $(P, \mathcal{N})$ is called a canonical number system (CNS) if every non-zero element of $R := \mathbf{Z}[X]/P\mathbf{Z}[X]$ can uniquely be written in the form

$$a_0 + a_1 x + \cdots + a_l x^l \tag{1}$$

with $a_0, \ldots, a_l \in \mathcal{N}$, $a_l \neq 0$; here x denotes the image of X under the canonical epimorphism from $\mathbf{Z}[X]$ to R. In other words this means that every coset $Q + P\mathbf{Z}[X]$ $(Q \in \mathbf{Z}[X], \deg Q < \deg P)$ includes a polynomial with coefficients belonging to $\mathcal{N}$.

---

[*]Mathematics subject classification numbers: 11R04, 11R16, 11R21, 12D99

[†]Supported by the Japanese Ministry of Education, Culture, Sports, Science and Technology, Grand-in Aid for fundamental research 14540015, 2002–2005.

[‡]Research partially supported by Hungarian National Foundation for Scientific Research Grant Nos 29330 and 38225.

The concept of canonical number systems in the general form described above was introduced by the third author [16]; canonical number systems with more restrictions on the defining polynomials have been studied by several authors (see e.g. the introduction of [1] or [2] and the references given there). Remark that W.J. Gilbert [9] used the terminology radix representation instead of canonical number system.

The first and third authors [1] suggested that the characterization problem of canonical number systems is only related to the coefficients of the defining polynomial. Therefore the term CNS polynomial (see the definition below) seems to be reasonable (cf. [2]). CNS polynomials can be applied to cryptography [16] and fractal tilings of the Euclidean space [3].

The problem of characterizing CNS polynomials is still open. It is very easy to show that linear CNS polynomials are given by $X+p_0$ with $p_0 \geq 2$. Quadratic CNS polynomials were classified by I. Kátai and B. Kovács [10, 11] and independently by W. J. Gilbert [9] (see also S. Akiyama and H. Rao [2] or [5] for the general setting). Under additional hypotheses cubic and quartic CNS polynomials were characterized by K. Scheicher and J. M. Thuswaldner ([17], Theorem 7.1 and Theorem 7.2) and S. Akiyama and H. Rao ([2], Theorem 5.4 and Theorem 5.5); S. Akiyama and H. Rao also dealt with quintic polynomials ([2], Theorem 5.7). CNS trinomials were classified by the second author [5].

The present note aims at a partial proof of a conjecture of W. J. Gilbert [9] on the characterization of cubic CNS polynomials. We also show that his conjecture is not complete. Further applications to some classes of cubic number fields are described.

The second author would like to express his heartfelt gratitude for the hospitality of the University of Debrecen on the occasion of discussing the outline of this paper.

2 Notation and basic results on CNS polynomials

As usual we denote by $\mathbf{Z}$ the ring of integers and by $\mathbf{N}$ the set of nonnegative integers. Let $P = \sum_{i=0}^{d} p_i X^i \in \mathbf{Z}[X]$ with $d > 0, p_d = 1$ and $|p_0| > 1$.

Definition 2.1 *P is a CNS polynomial if the pair $(P, \mathcal{N})$ forms a canonical number system. The set of CNS polynomials will be denoted by $\mathcal{C}$.*

For the convenience of the reader we formally list some well known results which will be used in the sequel.

Lemma 2.2 *(W. J. Gilbert [9], A. Pethő [16]) If $P \in \mathcal{C}$ then all real zeroes of P are less than -1 and the absolute values of all complex roots of P exceed 1. In particular $p_0 > 1$.*

In view of Lemma 2.2 we shall suppose $p_0 > 1$ from now on.

Theorem 2.3 *(B. Kovács [12]) If $p_0 \geq p_1 \geq \ldots \geq p_{d-1} \geq 1$ and none of the roots of P is a root of unity then $P \in \mathcal{C}$.*

Remark 2.4 *B. Kovács proved this theorem under the hypothesis that P be irreducible; in this case the assumption on the roots of P is trivially satisfied. The extension to not necessarily irreducible polynomials is due to the third author [16].*

The algorithm to express any element of R in the form (1) can clearly be described by the map[1] $T : R \longrightarrow R$, $\sum_{j=0}^{d-1} z_j x^j \mapsto \sum_{j=0}^{d-1}(z_{j+1} - p_{j+1}\left\lfloor \frac{z_0}{p_0} \right\rfloor)x^j$ with $z_d := 0$ (cf. [1]). Using the $\mathbf{Z}$-basis $w_j = \sum_{i=j}^{d} p_i x^{i-j}$ $(j = 1, \ldots, d)$ of R and the group isomorphism $\iota : \mathbf{Z}^d \longrightarrow R$, $(z_1, \ldots, z_d) \mapsto \sum_{j=1}^{d} z_j w_j$, one easily verifies the relation

(2) $$\iota \circ \tau = T \circ \iota$$

with

$$\tau : \mathbf{Z}^d \longrightarrow \mathbf{Z}^d, (z_1, \ldots, z_d) \mapsto (-\left\lfloor \frac{p_1 z_1 + \cdots + p_d z_d}{p_0} \right\rfloor, z_1, \ldots, z_{d-1})$$

(cf. [4]).

Lemma 2.5 *(i) $P \in \mathcal{C}$ if and only if for every $z \in \mathbf{Z}^d$ we can find some $l \in \mathbf{N}$ such that $\tau^l(z) = 0$.*

(ii) If there exists $0 \neq z \in \mathbf{Z}^d$ and $0 \neq k \in \mathbf{N}$ with $\tau^k(z) = z$ (i.e. z is a non-zero periodic element) then $P \notin \mathcal{C}$.

Proof. The first part is a consequence of (2) and ([1], Lemma 4) and obviously implies the second part. □

Lemma 2.6 *Let $E \subseteq \mathbf{Z}^d$ have the following properties:*

(i) $(1, 0, \ldots, 0) \in E$

(ii) $-E \subseteq E$

(iii) $\tau(E) \subseteq E$

(iv) For every $e \in E$ there exists some $k \in \mathbf{N}$ with $\tau^k(e) = 0$.

Then $P \in \mathcal{C}$.

Proof. Observing that we have

$$\tau(z_1, \ldots, z_d + a) \in \{\tau(z), -\tau(-z)\}$$

for every $z = (z_1, \ldots, z_d) \in \mathbf{Z}^d$ and $a \in \mathcal{N}$ the proof of ([4], Lemma 2) can be adapted. □

[1] $\lfloor \ldots \rfloor$ denotes the integer part function.

3 Cubic CNS polynomials

From now on we shall concentrate on cubic polynomials. Therefore we let $P = X^3 + p_2X^2 + p_1X + p_0 \in \mathbf{Z}[X]$ be a monic cubic polynomial throughout this section.

Under the additional hypothesis that P be irreducible W.J. Gilbert [9] stated the following

Conjecture. $P \in \mathcal{C}$ if and only if

(i) $p_0 \geq 2$,

(ii) $p_2 \geq 0$,

(iii) $p_1 + p_2 \geq -1$,

(iv) $p_1 - p_2 \leq p_0 - 2$,

(v) $p_2 \leq \begin{cases} p_0 - 2, & \text{if} \quad p_1 \leq 0, \\ p_0 - 1, & \text{if} \quad 1 \leq p_1 \leq p_0 - 1, \\ p_0, & \text{if} \quad p_1 \geq p_0. \end{cases}$ □

The next theorem shows that W.J. Gilbert's conditions are in fact necessary. It was proved by him [9] for irreducible polynomials.

Theorem 3.1 *Let $P \in \mathcal{C}$. Then*

(i) $p_0 \geq 2$,

(ii) $1 + p_1 + p_2 \geq 0$,

(iii) $p_1 - p_2 \leq p_0 - 2$,

(iv) $p_1 \leq 0$ *implies* $0 \leq p_2 \leq \min\{p_0 - 2, (p_0^2 + p_1 - 2)/p_0\}$,

(v) $1 \leq p_1 \leq p_0 - 1$ *implies* $0 \leq p_2 \leq p_0 - 1$,

(vi) $p_1 \geq p_0$ *implies* $2 \leq p_2 \leq p_0$.

Proof. In view of ([1], Proposition 1) we are left to show that the following values of p_2 are excluded: $p_2 = p_0 - 1$ in case (iv), $p_2 = p_0$ in case (v) and $p_2 = p_0 + 1$ in case (vi). In all these cases we easily check that the element $(1, 0, -1) \in \mathbf{Z}^3$ is periodic and so the assertion follows from Lemma 2.5. □

The following four counterexamples show that W. J. Gilbert's conditions are not sufficient. We continue to assume $p_0 \geq 2$ throughout. We thank Tibor Borbély, whose program made it possible to find counterexamples (ii) and (iii).

Counterexamples. (i) $\mathbf{p_1 \leq 0}$. Let $2 \leq p_1 + p_2 \leq -p_1$ and $p_0 \leq \min\{p_2 - p_1, p_1 + 2p_2 + 1\}$ then the element $(1, -1, -1)$ is periodic and the period is always $(1, -1, -1), (2, 1, -1), (1, 2, 1), (-1, 1, 2), (-1, -1, 1)$. Taking $p_2 = 2m, p_1 = -m$ or $-m - 1, p_0 = 3m$ $(m > 2)$ we obtain a parametrized family of non CNS polynomials.

(ii) $\mathbf{1 \leq p_1 \leq p_0 - 1}$. Let $\frac{7p_0-5p_2}{6}+1 \leq p_1 \leq -p_0+\frac{3}{2}p_2$. Then the element $(1,-3,1)$ is periodic with period $(1,-3,1),(3,1,-3),(-2,3,1),(-2,-2,3),(3,-2,-2),(1,3,-2),(-3,1,3)$ provided $p_0 \geq 28$.

(iii) $\mathbf{p_1 > p_0}$. Let $p_0+\frac{1}{2}p_2+1 \leq p_1 < p_0+\frac{2}{3}p_2-\frac{1}{3}$. Then the element $(3,-2,1)$ is periodic with period $(3,-2,1),(-2,3,-2),(1,-2,3),(1,1,-2),(-2,1,1)$. The same element is periodic, but with period $(3,-2,1),(-3,3,-2),(3,-3,3),(-2,3,-3),(1,-2,3),(1,1,-2),(-2,1,1)$ provided $p_0+\frac{2}{3}p_2-\frac{1}{3} \leq p_1 \leq 2p_2-4$. One can easily find parametrized families of non CNS polynomials satisfying these conditions. □

In the following proofs we often use Lemma 2.6. In these cases we restrict ourselves to explicitly specifying an appropriate (finite) set $E \subset \mathbf{Z}^3$ such that $E_+ \cup (0,0,0) \cup (-E_+)$ satisfies the prerequisites of this lemma where we put $E_+ = E \cup \{(0,0,1),(1,0,0)\}$. The verification that this set does in fact have the required properties can easily be performed by looking at the respective graphs (see [2] or [4]) and is left to the reader (an example of this graph is drawn in the proof of Proposition 3.2).

In an effort to prove sufficiency of the conditions of the conjecture W.J. Gilbert's result suggests the treatment of four different types of polynomials according to the size of the linear coefficient of the polynomial.

Therefore we first deal with negative coefficients p_1.

Proposition 3.2 *Let $p_1 \leq -1$, $p_2 \leq p_0 - 2$ and $-1 \leq p_1 + p_2 \leq 0$. Then $P \in \mathcal{C}$.*

Proof. Let $E_0 = \{(0,1,0),(0,1,1),(1,0,-1),(1,1,0)\}$ and choose $E = E_0 \cup \{(1,1,1)\}$ in case $p_1+p_2=-1$ and $E = E_0$ otherwise. To illustrate our method the graph of this case is shown in Figure 1. □

Proposition 3.3 *Let $p_1 \leq -1$, $0 \leq p_2 < min\{p_0-1, 2p_0/3\}$ and $1+p_1+p_2 \geq 0$. Then $P \in \mathcal{C}$.*

Proof. Using Proposition 3.2 we may suppose $p_1+p_2 \geq 1$. In view of ([17], Theorem 7.1) or ([2], Theorem 5.4) we may assume $p_1-p_2 \leq -p_0+1$. Let $E_0 = \{(0,1,0),(0,1,1),(0,2,1),(1,-1,-1),(1,0,-2),(1,0,-1),(1,1,-1),(1,1,0),(1,2,1),$ $(2,0,-2),(2,1,-1)\}$. We distinguish two cases.

Case I. $p_1+2p_2 \leq p_0-1$

Let $E_1 = E_0 \cup \{(0,1,2),(1,-1,-2)\}$. If $2p_1 \leq -p_0+1$ let

$$E_{11} = E_1 \cup \{(0,2,2),(1,-2,-2),(1,1,-2),(1,2,0),(2,1,-2),(2,2,0)\}$$

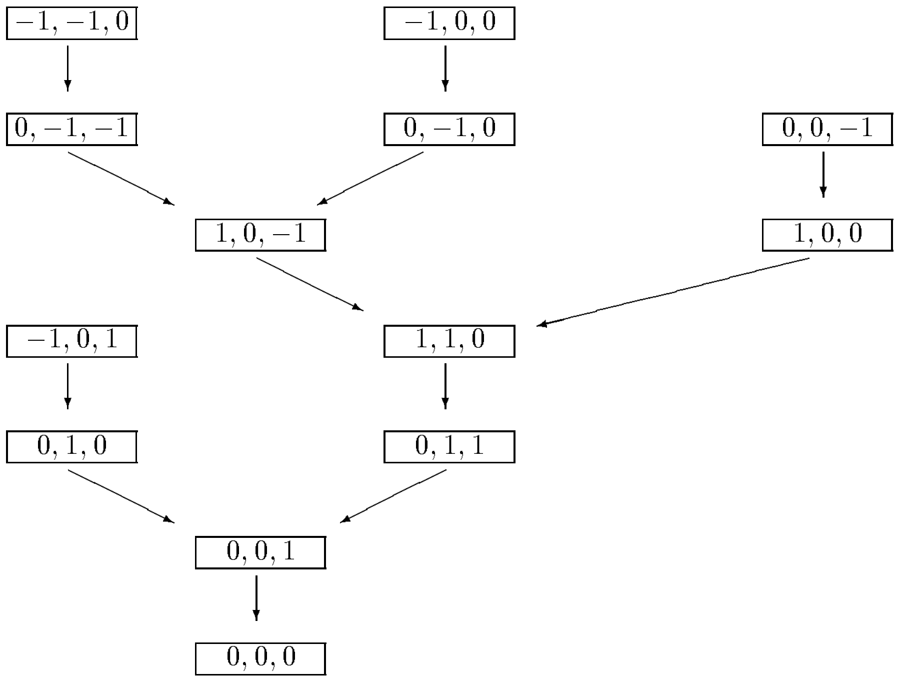

Figure 1: $-p_0 + 2 \leq p_1 \leq -1, p_2 = -p_1$

and put $E = E_{11} \cup \{(1,1,1)\}$ if $p_1 + p_2 = 1$ and $E = E_{11}$ otherwise. If $2p_1 \geq -p_0 + 2$ put $E = E_1 \cup \{(0,2,0),(1,2,0)\}$.

Case II. $p_1 + 2p_2 = p_0$

Let $E = E_0 \cup \{(0,1,2),(0,2,0),0,2,2),(1,-2,-2),(1,-1,-2),(1,1,-2),(1,2,-1),$
$(1,2,0),(2,-1,-2),(2,1,-2),(2,2,-1)\}$. □

Proposition 3.4 *If* $1 + p_1 + p_2 \geq 0$, $-p_0 + p_2 + 1 \leq p_1 \leq -1$ *then* $P \in \mathcal{C}$.

Proof. In case $p_1 + p_2 \leq 0$ the assertion is a consequence of Proposition 3.3, otherwise we assume $p_1 + p_2 > 0$ and define $E = \{(0,1,-1),(0,1,0),(0,1,1),(1,-1,-1),(1,0,-1),(1,1,-1),(1,1,0)\}$. □

The following statement which is an immediate consequence of Proposition 3.4 shows that W.J. Gilbert's conjecture holds in case $p_1 = -1$.

Corollary 3.5 *If* $p_1 = -1$ *and* $0 \leq p_2 \leq p_0 - 2$ *then* $P \in \mathcal{C}$.

In contrast to Proposition 3.3 we add some results valid for $p_2 = p_0 - 2$.

Proposition 3.6 *Let* $-p_0 + 1 \leq p_1 \leq -1$ *and* $p_2 = p_0 - 2$.

(i) If $p_0 \leq 5$ *or if* $p_0 \geq 6$ *and* $p_1 = -p_0 + 1$ *or* $p_1 = -p_0 + 2$ *then* $P \in \mathcal{C}$*.*

(ii) If $p_0 \geq 6$ *and* $-p_0 + 4 \leq p_1 \leq 1 - p_0/2$ *then* $P \notin \mathcal{C}$*.*

(iii) If $p_0 \geq 6$ *and* $p_1 = -p_0 + 3$ *then for every element of the form* $e = (e_1, e_2, e_3) \in \mathbf{Z}^3$ *such that* $e_i = -1, 0, 1,\ i = 1, 2, 3$ *we can find some* $l \in \mathbb{N}$ *such that* $\tau^l(e) = 0$*.*

Proof. (i) The case $p_0 \leq 5$ can easily be derived from Corollary 3.5, Proposition 3.2 and Proposition 3.3. While the cases for $p_0 \geq 6$ follow immediately from Proposition 3.2.

(ii) The element $(1, -1, -1)$ is periodic.

(iii) This can easily be checked. □

Remark 3.7 (i) *This result shows in particular that W.J. Gilbert's conjecture does not hold for* $p_1 = -2$*. The polynomial* $X^3 + 4X^2 - 2X + 6$*, for example, is irreducible, satisfies Gilbert's conjecture, but is not a CNS polynomial.*

(ii) *If Conjecture 2 of [1] holds true then* $X^3 + (p_0 - 2)X^2 - (p_0 - 3)X + p_0 \in \mathcal{C}$ *for any* $p_0 \geq 6$ *(see also the remarks on this conjecture in [17]). We checked by a computer that* $X^3 + (p_0 - 2)X^2 - (p_0 - 3)X + p_0 \in \mathcal{C}$ *for any* $6 \leq p_0 \leq 20$*. The program showed that the set of witnesses, i.e. the sets* $E = E(p_0)$*, is growing with* p_0*. So far we were unable to understand the structure of* $E(p_0)$*.*

In case of vanishing linear coefficient we immediately derive a necessary and sufficient condition from the result on trinomials quoted above (see ([5], Theorem 3) thereby showing the truth of W.J. Gilbert's conjecture in this case.

Theorem 3.8 $X^3 + p_2 X^2 + p_0 \in \mathbf{Z}[X]$ *is a CNS polynomial if and only if* $0 \leq p_2 \leq p_0 - 2$*.*

Thirdly, we deal with small positive coefficients p_1.

Theorem 3.9 *If*

(1) $1 \leq p_2 \leq p_1 \leq p_0 - 1$

or

(2) $p_1 = p_0$ *and* $2 \leq p_2 \leq p_0$

then $P \in \mathcal{C}$*.*

Proof. As P does not vanish at any root of unity this is clear by Theorem 2.3. □

For not necessarily monotonously increasing coefficients we can prove the following results.

Proposition 3.10 *If* $1 \le p_1 \le p_0 - 1$ *and* $0 \le p_2 \le (2p_0 - 1)/3$ *then* $P \in \mathcal{C}$.

Proof. In view of Theorem 3.9 we assume $p_2 > p_1$. Notice that $p_2 = p_0 - 1 \le (2p_0 - 1)/3$ implies $p_0 \le 2$. Hence $p_0 = 2, p_2 = 1$ and $p_1 = 0$, which is excluded. Thus $p_2 \le p_0 - 2$.

Let $E_0 = \{(0,1,-1),(0,1,0),(1,-1,0),$
$(1,0,-1),(1,1,-1)\}$. We distinguish two cases.

Case I. $p_1 + p_2 \le p_0$

Put $E = E_0 \cup \{(0,1,1),(1,-1,-1)\}$.

Case II. $p_1 + p_2 > p_0$

Let $E_2 = E_0 \cup \{(0,1,-2),(0,2,-1),(1,-2,0),(1,-2,1),(1,-1,-1),(1,0,-2),(1,1,-2),$
$(2,-1,-1),(2,0,-2)\}$. If $p_1 + p_2 = p_0 + 1$ put $E = E_2 \cup \{(0,1,1),(0,2,0)\}$. Finally suppose $p_1 + p_2 > p_0 + 1$. Then $2p_1 > p_2 + 2$. If $2p_1 \le p_0 + 1$ take $E = E_2 \cup \{(0,2,0)\}$ otherwise put $E = E_2 \cup \{(0,2,-2),(1,-1,-2),(1,2,-2),(2,-2,0),(2,-1,-2)\}$. □

As we are particularly interested in relatively small p_1 we state the following result.

Proposition 3.11 *Let* $1 \le t \le p_0$. *Then* $X^3 + (p_0 - t)X^2 + X + p_0 \in \mathcal{C}$ *if and only if* $(p_0, t) \ne (2,2)$.

Proof. Let $E_0 = \{(0,1,-1),(0,1,0),(1,-1,0),(1,0,-1)\}$. We distinguish three cases.

Case I. $t = 1$

Put $E = E_0$ if $p_0 = 2$ and $E = E_0 \cup \{(0,1,1),(1,-1,-1),(1,1,-1)\}$ otherwise.

Case II. $t = 2$

If $p_0 = 2$ then the assertion follows from Theorem 3.1 (iii). If $p_0 = 3$ choose $E = E_0$. Finally if $p_0 > 3$ put $E = E_0 \cup \{(0,1,1),(1,-1,-1),(1,1,-1)\}$.

Case III. $t > 2$

The assertion follows from ([17], Theorem 7.1) or ([2], Theorem 5.4). □

Finally, we deal with large positive coefficients p_1. The case $p_1 = p_0$ was completely described in Theorem 3.9. Therefore we assume $p_1 > p_0$ in the next proposition.

Proposition 3.12 *If* $p_0 < p_1$ *then* $P \in \mathcal{C}$ *if one of the following conditions holds:*

(1) $p_1 = p_0 + 1$ *and* $3 \le p_2 \le p_0$,

(2) $p_1 = p_0 + 2$ *and* $p_2 = (p_0 + 4)/2$,

(3) $p_0 < p_1, p_1 - p_2 < p_0 - 1, 3p_2 < 2p_0, 4p_1 - 3p_2 < 4p_0 - 2$,

(4) $p_2 \leq p_0, p_1 - p_2 < p_0 - 2, 0 \leq p_1 - 2p_2, 2p_1 - p_2 \leq 2p_0$,

(5) $p_1 - p_2 < p_0 - 1, -2 \leq p_1 - 2p_2, 2p_1 - p_2 < 2p_0$,

(6) $3 \leq p_2 \leq p_0, p_1 - p_2 < p_0 - 1, p_1 - 2p_2 \leq -2, 2p_1 - p_2 \leq 2p_0, p_0 - 1 \leq 2p_1 - 2p_2, p_1 + p_2 \leq 2p_0 + 2$.

Proof. Let $E_0 = \{(0,1,-1),(1,-1,0),(1,-1,1),(1,0,-1),(2,-1,0)\}$.

(1) Take $E_{01} = \{(0,1,-2),(1,-2,2),(2,-2,1)\}$ and $E_{02} = \{(1,-1,-1),(1,1,-2),(2,-1,-1)\}$.

Case I. $p_2 < p_0/2 + 2$

Put $E_1 = E_0 \cup E_{01} \cup \{(1,-2,1),(1,-1,2),(2,-2,2)\}$ and choose $E = E_1 \cup E_{02}$ if $p_1 - 2p_2 = -2$ and $E = E_1$ otherwise.

Case II. $p_2 \geq p_0/2 + 2$

Let $E = E_0 \cup E_{01} \cup E_{02} \cup \{(0,2,-2),(1,0,-2),(2,-2,0),(2,0,-2)\}$.

(2) Take $E = E_0 \cup \{(0,1,-2),(1,-2,2),(1,-2,1),(1,1,-2),(2,-2,1),(2,-2,2),(2,-1,-1)\}$.

(3) Using (1) we may assume $p_1 > p_0 + 1$.

Case I. $2p_1 - p_2 \leq 2p_0 - 1$

Define $E_1 = E_0 \cup \{(0,1,-2),(1,-2,1),(2,-2,1)\}$.

Case I.1 $p_1 - 2p_2 \leq -2$

Let $E_{11} = E_1 \cup \{(1,-1,-1),(1,1,-2),(2,-1,-1)\}$.

Case I.1.1 $2p_1 - 2p_2 \leq p_0 - 2$

Put $E_{111} = E_{11} \cup \{(0,1,-3),(0,2,-3),(0,2,-2),(1,-2,2),(1,-2,3),(1,0,-2),(1,1,-3),$ $(2,-3,2),(2,-2,0),(2,-2,1),(2,0,-2),(3,-2,0)\}$ and choose $E = E_{111} \cup \{(1,-3,2)\}$ if $3p_1 - 2p_2 \leq 2p_0 - 1$ and $E = E_{111} \cup \{(1,-3,3),(2,-3,3),(3,-3,2))\}$ otherwise.

Case I.1.2 $2p_1 - 2p_2 > p_0 - 2$

Let $E = E_{11} \cup \{(2,-2,2)\}$.

Case I.2 $p_1 - 2p_2 > -2$

Choose $E = E_1 \cup \{(1,-2,2),(1,-1,2),(2,-2,2)\}$.

Case II. $2p_1 - p_2 > 2p_0 - 1$

Define $E_2 = E_0 \cup \{(0,1,-2),(1,-2,2),(1,-1,2),(2,-2,1),(2,-2,2),(3,-2,1)\}$.

Case II.1 $3p_1 - 2p_2 \leq 3p_0 - 2$

Let $E_{21} = E_2 \cup \{((1,-2,3),2,-3,2),(2,-3,3),(3,-3,2),(3,-3,3)\}$ and choose $E = E_{21} \cup \{(0,2,-3),(1,0,-2),(2,-2,0),(2,0,-2),(3,-2,0)\}$ if $2p_1 - 3p_2 \leq p_0 - 3$ and $E = E_{21} \cup \{(2,-2,3)\}$ otherwise.

Case II.2 $3p_1 - 2p_2 > 3p_0 - 2$

Let $E_{22} = E_2 \cup \{(2,-3,3),(3,-3,2),(3,-3,3),(4,-3,2)\}$.

Case II.2.1 $2p_1 - 3p_2 \leq p_0 - 4$

Put $E_{221} = E_{22} \cup \{(0,1,-3),(0,2,-3),(1,-3,4),(1,-2,3),((1,-1,-1),1,0,-2),(1,1,-3),$ $(2,-3,4),(2,-1,-1),(2,0,-2),(3,-4,3),(3,-4,4),(3,-2,0),(4,-4,3),(4,-4,4)\}$ and choose $E = E_{221}$ if $p_1 + p_2 \leq 2p_0 + 2$ and $E = E_{221} \cup \{(3,-3,1),(3,-1,-1),(4,-3,1)\}$ otherwise.

Case II.2.2 $2p_1 - 3p_2 > p_0 - 4$

Take $E_{222} = E_{22} \cup \{(1,-2,3),(2,-2,3),(3,-4,3),(3,-4,4),(4,-4,3),(4,-4,4)\}$.

Case II.2.2.1 $3p_1 - 4p_2 \leq 2p_0 - 4$

Define $E_{2221} = E_{222} \cup \{(1,-3,4),(2,-3,4)\}$.

Case II.2.2.1.1 $p_1 - 3p_2 \leq -5$

Let $E_{22211} = E_{2221} \cup \{(0,1,-3),(1,1,-3),(2,-1,-1)\}$ and choose $E = E_{22211} \cup \{(1,-1,-1)\}$ if $p_1 + p_2 \leq 2p_0 + 2$ and $E = E_{22211} \cup \{(3,-3,1),(3,-3,3),(3,-1,-1),(4,-3,1)\}$ otherwise.

Case II.2.2.1.2 $p_1 - 3p_2 > -5$

Let $E = E_{2221} \cup \{(0,1,-3),(1,1,-3)\}$.

Case II.2.2.2 $3p_1 - 4p_2 > 2p_0 - 4$

Define $E = E_{222} \cup \{(2,-3,4),(3,-3,3),(3,-3,4)\}$.

(4) Choose $E = E_0 \cup \{(0,1,-2),(1,-2,1),(1,-2,2),(1,-1,2),(2,-2,1),(2,-2,2)\}$.

(5) Using (1) we may assume $p_1 > p_0 + 1$ and using (4) we may further assume $p_1 - 2p_2 \leq -1$. Define $E_1 = E_0 \cup \{(0,1,-2),(1,-2,1),(1,-2,2),(2,-2,1),(2,-2,2)\}$ and choose $E = E_1 \cup \{(1,-1,2)\}$ if $p_1 - 2p_2 = -1$ and $E = E_1 \cup \{(1,-1,-1),(1,1,-2),(2,-1,-1)\}$ otherwise.

(6) Choose $E = E_0 \cup \{(0,1,-2),(1,-2,1),(1,-2,2),(1,-1,-1),(1,1,-2),(2,-2,1),$ $(2,-2,2),(2,-1,-1)\}$. □

Example. Using the same method as in the proof of the last Proposition it can easily be checked that $X^3 + p_0X^2 + (p_0+2)X + p_0 \in \mathcal{C}$ for $p_0 = 4,5,6$. By Theorem 3.1 (iii) it is clearly not a CNS polynomial for $p_0 = 2,3$.

4 Applications

In this section we apply the known results on cubic CNS polynomials to two classes of algebraic number fields which have extensively been studied in the literature. For convenience we make use of the following definition.

Definition 4.1 *Let α be an algebraic integer. We call α a basis of a canonical number system if the minimal polynomial of α is a CNS polynomial.*

4.1 Canonical number systems in simplest cubic fields

Let $f = X^3 - tX^2 - (t+3)X - 1$, where t denotes a positive integer parameter. Let $\vartheta = \vartheta_1$ denote the root of f with $t+1 < \vartheta < t+1+1/t$. It is easy to see that the other roots of f are $\vartheta_2 = -\frac{\vartheta+1}{\vartheta}$ and $\vartheta_3 = -\frac{1}{\vartheta+1}$. E. Thomas and M. Mignotte proved the following theorem.

Theorem 4.2 *(E. Thomas [18], M. Mignotte [14]) Let $t \geq 3$. Then the only integer solutions of the Thue equation*

$$X^3 - tX^2Y - (t+3)XY^2 - Y^3 = 1$$

are $(x,y) = (1,0), (0,-1), (-1,1)$.

From this result it is easy to derive the following theorem (see also I. Gaál [8], Theorem 5.2.1)

Theorem 4.3 *Up to translation by an integer the only $\beta \in \mathbf{Z}[\vartheta]$ with $\mathbf{Z}[\beta] = \mathbf{Z}[\vartheta]$ are $\beta = \vartheta, -t\vartheta + \vartheta^2$ and $(t+1)\vartheta - \vartheta^2$. In particular, if $\mathbf{Z}[\vartheta]$ coincides with the maximal order $\mathbf{Z}_{\mathbf{K}}$ of the algebraic number field $\mathbf{K} = \mathbf{Q}(\vartheta)$ then up to translation by a rational integer the only power integral bases are generated by are $\beta = \vartheta, -t\vartheta + \vartheta^2$ and $(t+1)\vartheta - \vartheta^2$.*

Using this theorem we will establish all bases of CNS in $\mathbf{Z}[\vartheta]$.

Theorem 4.4 *The element $\gamma \in \mathbf{Z}[\vartheta]$ is the basis of a CNS in $\mathbf{Z}[\vartheta]$ if and only if*
$\gamma = \vartheta + n, n \leq -t-3,$
$\gamma = -\vartheta + n, n \leq -3,$
$\gamma = \vartheta^2 - t\vartheta + n, n \leq -t-5,$
$\gamma = -\vartheta^2 + t\vartheta + n, n \leq -1,$
$\gamma = \vartheta^2 - (t+1)\vartheta + n, n \leq -t-5,$
$\gamma = -\vartheta^2 + (t+1)\vartheta + n, n \leq -1.$

Proof. For every β listed in Theorem 4.3 we have to find all integers n such that $\beta + n$ and $-\beta + n$ respectively are bases of CNS in $\mathbf{Z}[\vartheta]$. First we establish the largest (if $\beta > 0$) or least (if $\beta < 0$) n_0 such that all conjugates of $\beta + n_0$ and $-\beta + n_0$ respectively are less than -1 (cf. Lemma 2.2). To simplify the text assume that $\beta > 0$. Then for all $n \leq n_0$ all conjugates of $\beta + n$ are less than -1. In the second step we compute the minimal polynomial of $\beta + n_0$ and check whether it belongs to $\mathcal{C}$. If not then test the minimal polynomials of $\beta + n_0 - 1, \beta + n_0 - 2, \ldots$

until one of them, for the first time, belongs to $\mathcal{C}$. For simplicity denote this integer again by n_0. Hence n_0 is the largest integer such that $\beta + n_0$ generates a CNS.

It follows from the proof of the Theorem of Kovács [12] that there exists n_1 such that the minimal polynomial of $\beta + n$ satisfies for all $n \le n_1$ the conditions of Theorem 2.3. One has obviously $n_1 \le n_0$. Finally one has to test the elements of the finite set $\{\beta + n \ : \ n_1 \le n \le n_0\}$ to determine which ones generate a CNS. Notice that in the actual proof we always have $n_1 = n_0$, which considerably simplifies the proof.

After describing the general strategy, we turn to the concrete cases.

Case I+, $\beta = \vartheta$. We have $t+1 < \beta_1 < t+1+1/t, -1-1/t < \beta_2 < -1, -1/t < \beta_3 < 0$. The largest integer n_0 such that $\beta_i + n_0 < -1, i = 1,2,3$ is $n_0 = -t-3$. The minimal polynomial of $\beta - t - 3$ is $X^3 + (2t+9)X^2 + (t^2 11t + 24)X + 2t^2 + 12t + 17$. It is easy to check that the conditions of Theorem 2.3 are satisfied for this polynomial. If $n = -t-3-k, k \ge 0$ then the difference of the minimal polynomial of $\beta + n$ and of $\beta - t - 3$ is

$$3X^2k + (18k + 3k^2 + 4tk)X + 9k^2 + 24k + 11tk + t^2k + 2tk^2 + k^3,$$

thus the conditions of Theorem 2.3 remain true for the minimal polynomial of $\beta + n$, too. This solves the first case.

Case I-, $\beta = -\vartheta$. As $-(t+1+1/t) < -\beta_1 < -(t+1), 1 < -\beta_2 < 1+1/t, 0 < -\beta_3 < 1/t$ we may take $n_0 = -3$. The minimal polynomial of $-\beta - 3$ is $X^3 + (t+9)X^2 + (24+5t)X + 6t + 19$ and we can conclude that $-\beta + n$ is a basis of a CNS if and only if $n \le -3$.

Case II+, $\beta = -t\vartheta + \vartheta^2$. The minimal polynomial of β is $X^3 - (2t+6)X^2 + (t^2+7t+9)X - t^2 - 3t - 1$. Using the same order of conjugates as above we have $t+3 < \beta_1 < t+3+1/t, t+2 < \beta_2 < t+2+1/t, 1-2/t < \beta_3 < 1$ hence we have to take $n_0 = -(t+5)$. The minimal polynomial of $\beta - t - 5$ is $X^3 + (t+9)X^2 + (5t+24)X + 6t + 19$. Hence $\beta + n$ is a basis of a CNS if and only if $n \le -t-5$.

Case II-, $\beta = t\vartheta - \vartheta^2$. As $-(t+3+1/t) < \beta_1 < -(t+3), -(t+2+1/t) < \beta_2 < -(t+2), -1 < \beta_3 < -1+2/t$ we may take $n_0 = -1$. The minimal polynomial of $\beta - 1$ is $X^3 + (2t+9)X^2 + (t^2 + 11t + 24)X + 2t^2 + 12t + 17$. Hence $\beta + n$ is a basis of a CNS if and only if $n \le -1$.

Case III+, $\beta = -(t+1)\vartheta + \vartheta^2$. It is easy to see that $\vartheta_2 = -\frac{1}{\vartheta+1} = \vartheta^2 - (t+1)\vartheta - 2$, i.e. $\beta = \vartheta_2$. In Case I+ we proved that $\vartheta + n$ is a CNS basis if and only if $n \le -(t+3)$. This implies that $\vartheta_2 + n$ is a CNS basis if and only if $n \le -(t+3)$. As $\beta + n = \vartheta_2 + n + 2$ the element $\beta + n$ is a CNS basis if and only if $n + 2 \le -t - 3$, i.e. $n \le -t - 5$.

Case III-, $\beta = (t+1)\vartheta - \vartheta^2$. Arguing analogously as in Case III+ we obtain that $\beta + n$ is a CNS basis if and only if $n \le -1$. The theorem is completely proved. □

4.2 Canonical number systems in pure cubic fields

B. N. Delaunay [6]and T. Nagell [15] proved that if $d \in \mathbb{N}$ is cube free then the diophantine equation

$$X^3 - dY^3 = 1 \tag{3}$$

has at most one solution $(x, y) \in \mathbf{Z}^2$ with $xy \neq 0$. Moreover, if d is square free then an integral basis of the algebraic number field $\mathbf{K} = \mathbf{Q}(\vartheta)$, $\vartheta = \sqrt[3]{d}$ is given by $1, \vartheta, \vartheta^2$ if $d \not\equiv \pm 1 \pmod 9$ and $1, \vartheta, (\vartheta^2 \pm \vartheta + 1)/3$ otherwise.

In the first case the index form equation of $\mathbf{K}$ is the diophantine equation (3), i.e. for $\beta = n + x\vartheta + y\vartheta^2 \in \mathbf{Z}[\vartheta]$ we have: $\mathbf{Z}[\beta] = \mathbf{Z}[\vartheta]$ if and only if $(x, y) \in \mathbf{Z}^2$ is a solution of (3).

Generally, it is hard to decide when (3) has a non-trivial solution, i.e. one with $xy \neq 0$. But in the special case $d = m^3 + 1$ this is a simple task because $(x, y) = (-m, -1)$. Therefore if d is square free and $m \not\equiv 0 \pmod 3$ then $\pm\vartheta + n$ and $\pm(\vartheta^2 + m\vartheta) + n$ $(n \in \mathbf{Z})$ are the only generators of power integral bases of $\mathbf{K}$.

Choosing $m = 3k \pm 1$, m is certainly not divisible by 3. Then $d = 27k^3 + 27k^2 + 9k + 2$. By a result of P. Erdős [7] there exist infinitely many values of k for which d is square-free. In these cases $\vartheta = \sqrt[3]{d}$ generates the maximal order $\mathbf{Z_K}$ of the algebraic number field $\mathbf{K} = \mathbf{Q}(\vartheta)$.

Using these results our aim is to extend the results which S. Körmendi [13] achieved for the particular cubic number field $\mathbf{Q}(\sqrt[3]{2})$. We can prove the following

Theorem 4.5 *Let m be a positive integer not divisible by 3 such that $d = m^3 + 1$ is square-free. Put $\vartheta = \sqrt[3]{d}$. Then $\gamma \in \mathbf{Z}[\vartheta]$ is the basis of a CNS in $\mathbf{Z}[\vartheta]$ if and only if*

$\gamma = \vartheta + n, n \leq -m - 2,$

$\gamma = -\vartheta + n, n \leq 0,$

$\gamma = \vartheta^2 + m\vartheta + n, n \leq -2m^2 - 2,$

$\gamma = -(\vartheta^2 + m\vartheta) + n, n \leq -m^2 - 2.$

Proof. As the case $m = 1$ has been treated by S. Körmendi ([13], see also [4]) we may assume $m > 1$.

Case I+, $\gamma = \vartheta + n$. The minimal polynomial of γ is $X^3 - 3nX^2 + 3n^2X - m^3 - n^3 - 1$. By Theorem 3.1 (iii) the inequality $3n^2 + 3n \leq -m^3 - n^3 - 3$ must hold, which implies $n \leq -m - 2$. If $n \leq -m - 2$ then $-3n < 3n^2 < -m^3 - n^3 - 1$, hence the converse follows from Theorem 2.3.

Case I-, $\gamma = -\vartheta + n$. The minimal polynomial of γ is $X^3 - 3nX^2 + 3n^2X + m^3 - n^3 + 1$. Hence clearly $n \leq 0$ by Theorem 3.1 (i) if γ is a CNS basis. On the other hand if $n = 0$ then γ is a

CNS basis by Theorem 3.8 (or by direct checking). Finally if $n \le -1$ the assertion follows from Theorem 2.3.

Case II+, $\gamma = \vartheta^2 + m\vartheta + n$. The minimal polynomial of β is $X^3 - 3nX^2 + (3n^2 - 3m^4 - 3m)X + 3m^4n - 2m^6 - 3m^3 - 1 + 3mn - n^3$. Let γ be a CNS basis and define $\beta = -n - 2m^2$. Using $\vartheta > m$ we find $\beta > 1$ by Lemma 2.2. Thus n has the desired shape. The converse can easily be derived from Theorem 2.3.

Case II-, $\gamma = -(\vartheta^2 + m\vartheta) + n$. The minimal polynomial of γ is $X^3 - 3nX^2 + (3n^2 - 3m^4 - 3m)X + 3m^4n + 2m^6 + 3m^3 + 1 + 3mn - n^3$. Let γ be a CNS basis. By Theorem 3.1 (ii) we find $n \le -m^2$ and we exclude equality by Theorem 3.1 (i). The assumption $n = -m^2 - 1$ contradicts the fact $p_2 \le p_0$.

Conversely, firstly assume $n \le -m^2 - 3$. Then our assertion follows from Theorem 2.3. Finally, if $n = -m^2 - 2$ then we can easily apply Proposition 3.12 (5) to complete the proof. □

5 Concluding Remarks

Summing up the results of K. Scheicher and J.M. Thuswaldner [17] and of ours we conclude that Gilbert's conjecture holds at least in the following cases:

(1) $p_1 = -1, 0, 1, p_0, p_0 + 1$,

(2) $1 \le p_2 \le p_1 \le p_0 - 1$,

(3) $1 + |p_1| + p_2 < p_0$,

(4) $1 \le p_1 \le p_0 - 1$ and $0 \le p_2 \le (2p_0 - 1)/3$.

The problem of characterizing CNS polynomials seems to be a hard one — it may even not be solved algebraically. Trivially, in case of non linear polynomials the conditions on the roots of the polynomial stated in Lemma 2.2 do not imply that the given polynomial is a CNS polynomial (e.g. the roots of the non CNS polynomial $X^2 - 2X + 2$ are $1 \pm \sqrt{-1}$). The class of CNS polynomials is not closed under addition (of polynomials of different degrees) or multiplication: By ([1], Theorem 3) the square of the CNS polynomial $X^2 - X + p_0$ is not a CNS polynomial in case $p_0 \ge 5$; the sum $X^3 + 5X^2 - 3X + 8$ of the CNS polynomials $X^3 + 4X^2 - 5X + 6$ (see Proposition 3.2) and $X^2 + 2X + 2$ (see [9], Theorem 1) is not a CNS polynomial since the element $(1, -1, -1)$ is periodic.

References

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

[2] S. Akiyama and H. Rao, New criteria for canonical number systems, preprint

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

[4] H. Brunotte, On trinomial bases of radix representations of algebraic integers, Acta Sci. Math. (Szeged) **67**, 521 – 527 (2001).

[5] H. Brunotte, Characterization of CNS trinomials, Acta Sci. Math. (Szeged), to appear

[6] B. N. Delaunay, Vollständige Lösung der unbestimmten Gleichung $X^3q + Y^3 = 1$ in ganzen Zahlen, Math. Z. **28**, 1 – 9 (1928).

[7] P. Erdős, Arithmetical properties of polynomials, J. London Math. Soc. **28**, 416-425 (1953).

[8] I. Gaál, Diophantine equations and power integral bases - New computational methods, Birhäuser Verlag, 2002.

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

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

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

[12] B. Kovács, Canonical number systems in algebraic number fields, Acta Math. Hung. **37**, 405 – 407 (1981).

[13] S. Körmendi, Canonical number systems in $\mathbf{Q}(\sqrt[3]{2})$, Acta Sci. Math. (Szeged) **50**, 351 – 357 (1986).

[14] M. Mignotte, Verification of a conjecture of E. Thomas, J. Number Theory **44**, 172 – 177 (1993).

[15] T. Nagell, Zur Theorie der kubischen Irrationalitäten, Acta Math. **55**, 33 – 65 (1930).

[16] 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, 31 – 44 (1991).

[17] K. Scheicher and J. M. Thuswaldner, On the characterization of canonical number systems, preprint.

[18] E. Thomas, Solutions to certain families of Thue equations, J. Number Theory **43**, 319–369 (1993).