Fields Institute Communications
Volume **00**, 0000

On a generalization of the radix representation - a survey

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

T. Borbély
Department of Computer Science, University of Debrecen,
P.O. Box 12, H-4010 Debrecen, HUNGARY
tborbely@delfin.klte.hu

H. Brunotte
Haus-Endt-Strasse 88
D-40593 Düsseldorf, GERMANY
brunoth@web.de

A. Pethő
Department of Computer Science, University of Debrecen,
P.O. Box 12, H-4010 Debrecen, HUNGARY
pethoe@math.klte.hu

J. M. Thuswaldner
Department of Mathematics and Statistics, Leoben University,
Franz-Josef-Strasse 18, A-8700 Leoben, AUSTRIA
joerg.thuswaldner@unileoben.ac.at

Dedicated to Hugh C. Williams on the occasion of his 60th Birthday

1 Introduction

Let $P(X) = p_d X^d + \cdots + p_0 \in \mathbb{Z}[X]$ with $p_0 \geq 2$ and $\mathcal{N} = \{0, 1, \ldots, p_0 - 1\}$. If $p_d = 1$ then $P(X)$ is called a CNS[1]-polynomial, whenever every non-zero element of $R := \mathbb{Z}[X]/P\mathbb{Z}[X]$ can be written uniquely in the form

$$a_0 + a_1 x + \cdots + a_\ell x^\ell \tag{1.1}$$

with $a_0, ..., a_\ell \in \mathcal{N}, a_\ell \neq 0$; here x denotes the image of X under the canonical epimorphism from $\mathbb{Z}[X]$ to R. This means that every coset $Q + P\mathbb{Z}[X]$ $(Q \in \mathbb{Z}[X])$

2000 *Mathematics Subject Classification.* 11A63.

The first author was supported by the Japanese Ministry of Education, Culture, Sports, Science and Technology, Grant-in Aid for fundamental research 14540015, 2002–2005.

The fourth author was supported partially by the Hungarian National Foundation for Scientific Research Grant Nos. T42985 and T38225.

The fifth author was supported by project S8310 of the Austrian Science Foundation.

[1]CNS is the abbreviation for Canonical Number System.

contains a polynomial with coefficients belonging to $\mathcal{N}$. The polynomial (1) will be called the CNS-representation of the coset. The set of CNS-polynomials will be denoted by $\mathcal{C}$.

This concept was introduced by the fourth author [23] as a natural generalization of bases of canonical number systems or radix representations in algebraic number fields, which were defined in [10] and [6]. A complex number α is the base of a canonical number system in the algebraic number field $\mathbb{K}$ if and only if α is a zero of an irreducible CNS-polynomial and $1, \alpha, \ldots, \alpha^{d-1}$ is an integral basis of $\mathbb{Z}_{\mathbb{K}}$, where $\mathbb{Z}_{\mathbb{K}}$ denotes the maximal order of $\mathbb{K}$.

In this paper we give a survey on results on canonical number systems in algebraic number fields and on CNS-polynomials. The "backward" division of polynomials, which will be defined in Section 2, plays a special rôle. Changing the bases $1, X, X^2, \ldots$ appropriately one obtains a mapping $\tau_P : \mathbb{Z}^d \mapsto \mathbb{Z}^d$, which enables one to decide quite efficiently whether $P \in \mathcal{C}$ or not. The properties and applications of τ_P will be described in Sections 4 and 5. This mapping can be generalized further and one obtains a decomposition of $\mathbb{R}^d$ into convex sets.

The CNS-concept was generalized to simultaneous representations of tuples of integers in [9] and studied recently in [24]. The generalization for polynomials over finite fields can be found in [27], where the complete characterization of CNS-polynomials over finite fields is given. Because of lack of space we will not deal with these generalizations.

2 "Backward" division of polynomials

If $p_d = 1$ then it is clear that every coset of $\mathbb{Z}[X]/P(X)\mathbb{Z}[X]$ has an element of degree at most $d-1$ with coefficients, which can be arbitrarily large, say

$$A(x) = A_0 + A_1 x + \cdots + A_{d-1} x^{d-1}. \tag{2.1}$$

To transform $A(x)$ into the form (1) it is straightforward to use the following "backward" division process. Let $\mathbb{Z}'[X] = \{A(X) \in \mathbb{Z}[X] \ : \ \deg A < d\}$ and

$$T_P(A) = \sum_{i=0}^{d-1} (A_{i+1} - q p_{i+1}) X^i,$$

where $A_d = 0$ and $q = [A_0/p_0]$. Then $T_P \ : \ \mathbb{Z}'[X] \to \mathbb{Z}'[X]$ and

$$A(X) = a_0 + X T_P(A), \text{ with } a_0 = A_0 - q p_0.$$

If it causes no confusion we omit the subscript P.

Thus, to obtain the CNS representation of $A(X)$ one has to compute the iterates $T(A), T^2(A), \ldots$ until $T^\ell(A) = 0$ for some $\ell > 0$. This "backward" division process can become divergent (e.g. $A(X) = -1$ for $P(X) = X^2 + 4X + 2$) or ultimately periodic (e.g. $A(X) = -1$ for $P(X) = X^2 - 2X + 2$) or can terminate after finitely many steps (e.g. $A(X) = -1$ for $P(X) = X^2 + 2X + 2$). This means that $\mathcal{C}$ is a proper subset of $\mathbb{Z}[X]$.

Let

$$\Pi(P) = \{A \ : \ T_P^\ell(A) = A \text{ for some } \ell > 0\}$$

denote the set of periodic elements with respect to the mapping T_P. It is clear that we always have $0 \in \Pi(P)$. Moreover $P(X) \in \mathcal{C}$ if and only if $\Pi(P) = \{0\}$. Hence, it is enough to study the map $T_P \ : \ \mathbb{Z}^d \to \mathbb{Z}^d$ defined as

$$T_P((A_0, \ldots, A_{d-1})) = (A_1 - q p_1, \ldots, A_{d-1} - q p_{d-1}, -q p_d), \ q = [A_0/p_0].$$

The following theorem is easy to prove.

Theorem 2.1 (Analytical conditions) *If $P(X) \in \mathcal{C}$ then*

- *all roots of $P(X)$ are lying outside the closed unit circle, and*
- *all real roots of $P(X)$ are less than -1.*

This theorem implies that if $P \in \mathcal{C}$ then $p_0 \geq 2$.
For monic $P(X) \in \mathbb{Z}[X]$ and for $c > 0$ let

$$P_c = \{A(X) = \sum_{i=0}^{d-1} A_i X^i \in \mathbb{Z}'[X] \ : \ |A_i| \leq c, \ 0 \leq i \leq d-1\}.$$

The next theorem was proved for irreducible polynomials in [20], for square-free polynomials in [23] and in the general case in [3] and [24].

Theorem 2.2 *Assume that for $P(X) \in \mathbb{Z}[X]$ the conditions of Theorem 2.1 hold. Then there exists a computable constant $c > 0$ such that $P(X) \in \mathcal{C}$ if and only if every $A(X) \in P_c$ has a CNS-representation.*

As the set P_c is finite for all $c > 0$, the CNS property is algorithmically decidable. Unfortunately the constant c in Theorem 2.2 is usually large, therefore it is hard to apply it (cf. [20]). However, there are important special cases of CNS-polynomials. The first was discovered by B. Kovács [19] and proved in the general case in [23].

Theorem 2.3 *Let $P(X) = X^d + p_{d-1}X^{d-1} + \cdots + p_0$. If $p_0 \geq 2$ and $p_{d-1} \leq \cdots \leq p_1 \leq p_0$ and $P(X)$ is not divisible by a cyclotomic polynomial then $P(X) \in \mathcal{C}$.*

The second special case appeared in [2] and has been generalized slightly in [26] and [3]:

Theorem 2.4 *Assume that $p_2 \geq 0, \ldots, p_{d-1} \geq 0$, $\sum_{i=1}^d p_i \geq 0$ and $p_0 > \sum_{i=1}^d |p_i|$, then $P(X) \in \mathcal{C}$.*

3 CNS in algebraic number fields

By the remark after Theorem 2.1 the bases of radix representations in $\mathbb{Q}$ correspond to the roots of $X + p_0$ with $p_0 \geq 2$, i.e., they are negative integers. The negative base representations were studied for the first time in [7]. The radix representations in the Gaussian integers $\mathbb{Z}[\sqrt{-1}]$ were studied by Knuth [13] (see also [14]) and by Penney [22]. In [10] all CNS in Gaussian integers were characterized. This characterization has been extended to algebraic integers in real and imaginary quadratic number fields in [11, 12]. The same characterization was established independently in [6]. Brunotte [4] gave a new proof without assuming irreducibility of the quadratic polynomials.

Theorem 3.1 *We have $P(X) = X^2 + p_1X + p_0 \in \mathcal{C}$ if and only if $-1 \leq p_1 \leq p_0$ and $p_0 \geq 2$.*

A. Kovács [15, 17] considered the possible length of periods and the size of $\Pi(P)$ corresponding to irreducible quadratic polynomials $P(X)$ with two complex roots. Let θ be a root of $P(X)$ and assume that its representation in the canonical integral basis $1, \omega$ of $\mathbb{Q}(\theta)$ is $\theta = a + b\omega, b > 0$. Then he proved in [17] among others that the cardinality of $\Pi(P)$ can only be $b, b+1$ or $b+2$. A full characterization of $\Pi(P)$ for quadratic polynomials can be found in Thuswaldner [28].

For cubic number fields much less is known. Körmendi [21] described up to one possible exception all bases of CNS in $\mathbb{Q}(\sqrt[3]{2})$ and B. Kovács and Pethő [20] in all but one totally real fields with discriminant at most 564. In the field defined by one root of the polynomial $X^3 + 1749X^2 + 5975X + 5108$ their result was not complete, because the constant appearing in Theorem 2.2 was to large. These gaps were filled in [4]. In [1] all CNS in infinite parametric families of number rings were established.

After some computation and proving that the conditions are necessary, Gilbert [6] proposed the following conjecture for irreducible cubic polynomials.

Conjecture 3.2 Let $P = X^3 + p_2X^2 + p_1X + p_0$. Then $P \in \mathcal{C}$ 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) $p_2 \leq \begin{cases} p_0 - 2, & \text{if} \quad p_1 \leq 0, \\ p_0 - 1, & \text{if} \quad 1 \leq p_1 \leq p_0 - 1, \\ p_0, & \text{if} \quad p_1 \geq p_0. \end{cases}$

We will come back later to this conjecture, but will mention already here that the situation is much more complicated if $p_0 \geq 6$.

For higher degree fields nearly nothing is known. The only general result is due to B. Kovács [19].

Theorem 3.3 *There exists in $\mathbb{Z}_{\mathbb{K}}$ a CNS if and only if $\mathbb{Z}_{\mathbb{K}}$ is monogenic, i.e., there exists an $\alpha \in \mathbb{Z}_{\mathbb{K}}$ such that $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is an integral basis in $\mathbb{Z}_{\mathbb{K}}$.*

Combining this theorem with a result of Győry [8] we obtain that up to translation by integers there exist only finitely many CNS in $\mathbb{Z}_{\mathbb{K}}$.

4 Brunotte's mapping

As we mentioned before, Theorem 2.2 is not efficient enough to decide the CNS property of a polynomial. Brunotte [4] observed that the basis transformation

$$\begin{aligned} \{1, x, \ldots, x^{d-1}\} &\rightarrow \{w_1, \ldots, w_d\}, \\ w_j &= \sum_{i=j}^{d} p_i x^{i-j}, \ j = 1, \ldots, d \end{aligned}$$

of R implies a nicer and much better applicable transformation as T_P is. Indeed, if

$$\begin{aligned} A(x) &= \sum_{j=1}^{d} \bar{A}_j w_j, \quad \text{then} \\ T_P(A) &= -tw_1 + \sum_{j=2}^{d} \bar{A}_{j-1} w_j, \text{ where } t = \left[\frac{p_1\bar{A}_1 + \cdots + p_d\bar{A}_d}{p_0}\right]. \end{aligned}$$

Hence T_P implies the mapping $\tau_P : \mathbb{Z}^d \rightarrow \mathbb{Z}^d$

$$\tau_P(\underline{A}) = \left(-\left[\frac{p_1A_1 + \cdots + p_dA_d}{p_0}\right], A_1, \ldots, A_{d-1}\right),$$

where $\underline{A} = (A_1, \ldots, A_d)$. The mapping τ_P will be called **Brunotte's mapping**. Scheicher and Thuswaldner [26] made the same discovery independently.

Brunotte's mapping is easy to implement and it is immediately clear that $P \notin \mathcal{C}$ if either the analytical conditions of Theorem 2.1 do not hold or there exists $0 \neq \underline{A} \in \mathbb{Z}^d$ and $\ell > 0$ such that $\tau_P^\ell(\underline{A}) = \underline{A}$. Its importance relies on the following theorem, which is in some sense the converse of the last statement and makes it possible to decide the CNS property. Moreover it enables a far reaching generalization. It was proved originally in [4] and refined in [3]. The present version was published in [1].

Theorem 4.1 *Suppose that $E \in \mathbb{Z}^d$ has the following properties:*

- $(1, 0, \ldots, 0) \in E$,
- $-E \subseteq E$,
- $\tau_P(E) \subseteq E$,
- *for each $e \in E$ there exists some $\ell > 0$ with $\tau_P^\ell(e) = 0$.*

Then $P(X) \in \mathcal{C}$.

Such a set E will be called the *set of witnesses* of $P \in \mathcal{C}$.

5 Applications of Brunotte's mapping

Applying Theorem 4.1 Brunotte was able to characterize all CNS trinomials [5].

Theorem 5.1 *If $d > 2$ then the following assertions hold:*

(i) *$X^d + bX + c$ belongs to $\mathcal{C}$ if and only if $-1 \leq b \leq c - 2$,*
(ii) *if $1 < q < d$ and $q \not| d$ then $X^d + bX^q + c \in \mathcal{C}$ if and only if $0 \leq b \leq c - 2$.*

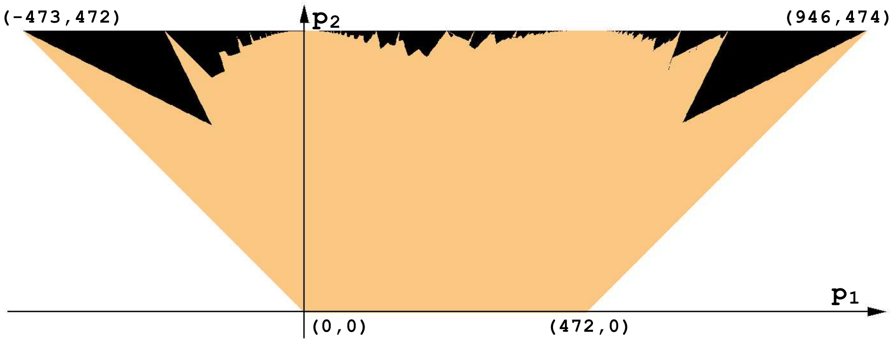
Akiyama et al. [1] examined Gilbert's Conjecture 3.2 and proved it in some cases, e.g. if

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

On the other hand they found that Gilbert's Conjecture does not hold if $p_0 \geq 6$. We present some 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 $(1, -1, -1)$ is a periodic element whose period is $(1, -1, -1); 2, 1, -1, -1$. Here and in the sequel we present a period by giving a vector and the first coordinate of the following vectors.
(ii) $\mathbf{1 \leq p_1 \leq p_0 - 1}$. Let $p_0 \geq 28$ and $\frac{7p_0 - 5p_2}{6} + 1 \leq p_1 \leq -p_0 + \frac{3}{2}p_2$. Then the element $(1, -3, 1)$ is periodic with period $(1, -3, 1); 3, -2, -2, 3, 1, -3$.
(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 $(3, -2, 1); -2, 1, 1, -2$.

We visualize the situation with the example $p_0 = 474$. In this case there are $396,830$ CNS-polynomials and $52,046$ polynomials that violate Gilbert's conjecture. The point (p_1, p_2) on Picture 1 corresponds to the polynomial $X^3 + p_2X^2 + p_1X + p_0$. The displayed region is defined by the inequalities from Conjecture 3.2. The gray points correspond to members of $\mathcal{C}$ and the black ones to those, which violate Gilbert's conjecture. From this picture it is to be expected that the set of cubic CNS polynomials has a complicated structure.



Picture 1. CNS polynomials for $p_0 = 474$.

Theorem 2.1 implies that for fixed degree and given $p_0 \geq 2$ there exist only finitely many CNS-polynomials. Especially interesting is the case $p_0 = 2$, i.e. the generalizations of the binary expansion. Using Brunotte's algorithm A. Kovács [18] computed all binary CNS polynomials of degree $d \leq 8$. The result of his computation is displayed in the next table.

Degree	1	2	3	4	5	6	7	8
Number of CNS-polynomials	1	3	4	12	7	25	12	20

To show how hard it is to decide whether a polynomial belongs to $\mathcal{C}$ we give two examples: For $X^8 + 2X^7 + 3X^6 + 3X^5 + 3X^4 + 3X^3 + 3X^2 + 3X + 2$ the smallest set of witnesses has $241,719$ elements, while for $X^3 + 317X^2 + 632X + 317$ has $1,308,322$ elements.

A natural question is whether the CNS-property belongs to the NP or to the coNP class? The above examples indicate that the CNS-property cannot be decided in polynomial time. In the other direction Scheicher and Thuswaldner [26] noticed that if $P(X) = X^3 + 196X^2 + 341X + 199$ then the length of the period of $(-11, 10, -6)$ is 84. They conjecture that already cubic polynomials can have arbitrarily long cycles. Note that $(3, -2, 1)$ is another periodic point of τ_P, but with period length 7.

6 Generalization of Brunotte's mapping

In an earlier stage of our investigations we tried to prove algebraic properties of the set $\mathcal{C}$. It turned out that $\mathcal{C}$ is not closed under addition, multiplication and incrementation by 1. However, some of these algebraic properties are valid for large subsets of $\mathcal{C}$. Especially, the examples (e.g. $x^3 + 80x^2 + 117x + 89$) where $P(x) \in \mathcal{C}$ but $P(x) + 1 \notin \mathcal{C}$ seem to be rather exceptional.

There are of course trivial algebraic results (which do not show anything new) if one appropriately restricts to subsets of $\mathcal{C}$. Let for example M be the set of CNS polynomials of degree 2 or of degree 3 which satisfy the assumptions of Proposition 3.3 in [1]. Then, if $Q = X + k, k \geq 2$ and $P \in M$ then $P + Q \in \mathcal{C}$.

The only non-trivial algebraic result was proved in [5]. It asserts that if $P(X) \in \mathcal{C}$ and $k \geq 1$ then $P(X^k) \in \mathcal{C}$.

A closer look at $\mathcal{C}$ showed that it (or a related set) has to be the union of convex bodies. To show this property we followed Paul Erdős instruction: "If you cannot solve a problem, then try to generalize it and solve the more general problem." Brunotte's mapping allows such a generalization.

Let $r=(r_1,\dots,r_d)\in\mathbb{R}^d, r_d\neq 0$. With r we associate the mapping $\tau_r\ :\ \mathbb{Z}^d\to\mathbb{Z}^d$ by the following way: if $a=(a_1,\dots,a_d)\in\mathbb{Z}^d$ then let

$$\tau_r(a)=(-[ra],a_1,\dots,a_{d-1}),$$

where $ra=r_1a_1+\cdots+r_da_d$. Obviously this is a generalization of Brunotte's mapping by taking $r=(\frac{p_1}{p_0},\dots,\frac{p_d}{p_0})$.

Let

$$\mathcal{C}_d=\{r\ :\ \text{for all } a\in\mathbb{Z}^d \text{ there exists } \ell>0 \text{ such that } \tau_r^\ell(a)=0\}.$$

The next theorem shows that the set of mappings τ_r has some convexity property.

Theorem 6.1 *Let $r_1,\dots,r_k\in\mathbb{R}^d$ and $a\in\mathbb{Z}^d$ be such that $\tau_{r_1}(a)=\cdots=\tau_{r_k}(a)$. Let s be any convex linear combination of $r_1,\dots,r_k$. Then we have $\tau_s(a)=\tau_{r_1}(a)=\cdots=\tau_{r_k}(a)$.*

This theorem implies immediately the following corollary

Corollary 6.2 *Let $r_1,\dots,r_k\in\mathbb{R}^d$ have the same period, i.e. $\tau_{r_1}^\ell(a)=\cdots=\tau_{r_k}^\ell(a), \ell=0,\dots,v$ and $a=\tau_{r_1}^v(a)$. Then if s lies in the convex hull of $r_1,\dots,r_k$ the mapping τ_s is periodic and has the same period as τ_{r_1}.*

For example, it is easy to check that for the plane vectors $r_1=\left(\frac{381}{254},\frac{253}{254}\right), r_2=\left(\frac{421}{254},\frac{253}{254}\right)$ and $r_3=\left(\frac{344}{254},\frac{176}{254}\right)$ the corresponding mappings have the same period $(-2,1);3,-2,1,1,-2$, hence, the corresponding mapping for any point lying in the triangle r_1,r_2,r_3 has this period too.

A three-dimensional example is: $r_1=\left(\frac{382}{254},\frac{253}{254},\frac{1}{254}\right), r_2=\left(\frac{421}{254},\frac{253}{254},\frac{1}{254}\right)$ and $r_3=\left(\frac{344}{254},\frac{176}{254},\frac{1}{254}\right)$. Here is the period $(3,-2,1);-2,1,1,-2,3$.

Theorem 4.1 can be generalized for this setting.

Theorem 6.3 *Let $r_1,\dots,r_k\in\mathbb{R}^d$ and denote by H the convex hull of $r_1,\dots,r_k$. For $z\in\mathbb{Z}^d$ take $m(z)=\min_{1\le i\le k}\{-[r_iz]\}$ and $M(z)=\max_{1\le i\le k}\{-[r_iz]\}$. Suppose that there exists a finite set E, which satisfies the following conditions:*

- *$\pm e\in E$ for all d-dimensional unit vectors e,*
- *for each $z=(z_1,\dots,z_d)\in E$ and*

  $$j\in[\min\{m(z),-M(-z)\},\max\{-m(-z),M(z)\}]\cap\mathbb{Z}$$

  we have $(j,z_1,\dots,z_{d-1})\in E$,
- *$\cap_{j=1}^\infty\tau_{r_i}^j(E)=\{0\}$ for each $i\in\{1,\dots,k\}$.*

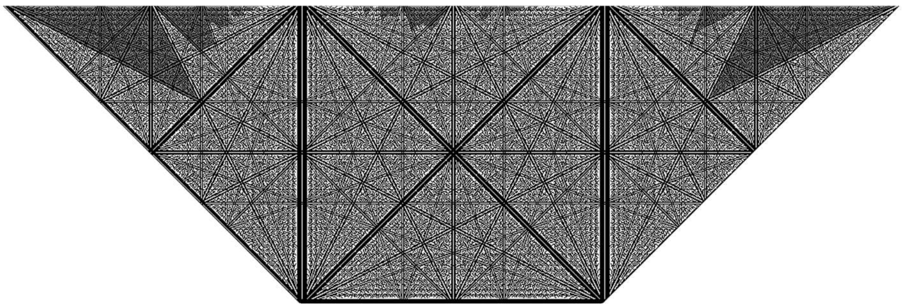
Then $H\subseteq\mathcal{C}_d$.

For example the square with vertices $\left(\frac{1}{3},\frac{1}{3}\right),\left(\frac{1}{3},\frac{2}{3}\right),\left(\frac{2}{3},\frac{1}{3}\right),\left(\frac{2}{3},\frac{1}{3}\right)$ is a subset of $\mathcal{C}_2$ as one can show by using the set of witnesses $E=E_1\cup(-E_1)\cup\{(0,0)\}$, where $E_1=\{(1,0),(0,1),(1,-1),(1,1),(2,-1),(1,-2),(2,0),(0,2),(1,2),(2,-2)\}$.

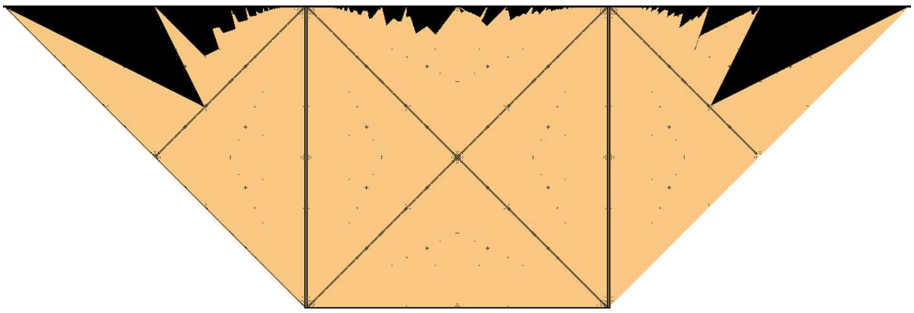
It is easy to see that $\mathcal{C}_2$ is a subset of the region

$$R_2=\{(\gamma_1,\gamma_2)\ :\ -1\le\gamma_1<2, 0\le\gamma_2<1,-\gamma_1\le\gamma_2<\gamma_1+1\}.$$

On Pictures 2 and 3 we present two approximations of $\mathcal{C}_2$. We displayed there all $(\gamma_1,\gamma_2)=\left(\frac{p_1}{p_0},\frac{p_2}{p_0}\right)\in R_2$ with $p_0,p_1,p_2\in\mathbb{Z}$. For Picture 2 we have chosen $p_0=60$, and for Picture 3 we took $p_0=174$. The light-gray points belong and the dark-gray points do not belong to $\mathcal{C}_2$. The status of the points lying on the black lines could not be decided for the chosen precision. However, it can be shown that a considerable part of the black points does indeed belong to $\mathcal{C}_2$.



Picture 2. An approximation of $\mathcal{C}_2$, $p_0 = 60$.



Picture 3. Better approximation of $\mathcal{C}_2$, $p_0 = 174$.

The top boundary of Pictures 1 and 3 seems to be very similar. Unfortunately we do not understand yet the relation between the two sets. By the last theorem $\mathcal{C}_d$ is the union of convex sets, but it is not clear whether finite or countably many sets appear in this union.

References

[1] S. Akiyama, H. Brunotte and A. Pethő, *Cubic CNS polynomials, notes on a conjecture of W.J. Gilbert*, J. Math. Anal. and Appl., to appear

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

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

[4] H. Brunotte, *On trinomial bases of radix representations of algebraic integers*, Acta Sci. Math. (Szeged), **67** (2001), 407-413.

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

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

[7] V. Grünwald, *Intorno all'aritmetica dei sistemi numerici a base negativa con particolare riguardo al sistema numerico a base negativo-decimale per lo studio delle sue analogie coll'aritmetica ordinaria (decimale)*, Giornale di matematiche di Battaglini, **23** (1885), 203-221, 367.

[8] K. Győry, *Sur les polynômes à coefficients entiers et de discriminant donné, III*, Publ. Math. Debrecen, **23** (1976), 141-165.

[9] K.-H. Indlekofer, I. Kátai and P. Racskó, *Number systems and fractal geometry*, Probability theory and applications, Essays to the Mem. of J. Mogyoródi, Math. Appl., **80** (1992), 319 -334.

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

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

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

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

[14] D. E. Knuth *The Art of Computer Programming, Vol. 2 Semi-numerical Algorithms*, Addison Wesley (1998) London 3rd-edition.

[15] A. Kovács, *On expansions of Gaussian integers with non-negative digits*, Math. Pannon., **10** (1999), 177-191.

[16] A. Kovács, *On the computation of attractors for invertible expanding linear operators in* $\mathbb{Z}^k$, Publ. Math. Debrecen, **56** (2000), 97-120.

[17] A. Kovács, *On canonical expansions of integers in imaginary quadratic fields*, Acta Math. Hung., **93** (2001), 347-357.

[18] A. Kovács, *Generalized binary number systems*, Ann. Univ. Sci. Budap. Rolando Etvös, Sect. Comput., **20** (2001), 195-206.

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

[20] 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.

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

[22] W. Penney, *A 'binary' system for complex numbers*, J. Assoc. Comput. Mach., **12** (1965), 247-248.

[23] 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.

[24] A. Pethő *Notes on CNS polynomials and integral interpolation*, to appear.

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

[26] K. Scheicher and J.M. Thuswaldner, *On the characterization of Canonical Number Systems*, Osaka J. Math., to appear.

[27] K. Scheicher and J.M. Thuswaldner, *Digit systems in polynomial rings over finite fields*, Finite Fields Appl., to appear.

[28] J.M. Thuswaldner, *Attractors for invertible expanding linear operators and number systems in* $\mathbb{Z}^2$, Publ. Math. Debrecen, **58** (2001), 423-440.