Number systems over orders of algebraic number fields

Attila Pethő

Department of Computer Science, University of Debrecen, Hungary
and University of Ostrava, Faculty of Science, Czech Republic

Joint work with Jörg Thuswaldner, Leoben, Austria

Numeration 2018
Paris, May 22 - 25, 2018

1. Introduction

In the last century mainly through the work of Grünwald, Knuth, Penney, Kátai, Gilbert, Júlia Szabó, B. Kovács, Körmendi, Környei evolved the notation of number systems or equivalently the radix representations in $\mathbb{Z}[x]$ and in algebraic number fields.

Generalizations to larger ground rings:

• Jacob and Reveilles (1995), Brunotte, Kirschenhofer and Thuswaldner (2011): $\mathbb{Z}[i]$
• Scheicher, Surer, Thuswaldner and van de Woestijne (2014): commutative rings
• Pethő and Varga (2017): Euclidean imaginary quadratic number fields.

We generalize here the number system concept in two directions:

- Allow orders of algebraic number fields as ground rings. (Radix representation in relative extensions.)
- The digit set is defined on a uniform way, which allow the investigation of families of polynomials. *We show that the canonical digit set is extraordinary, it has very special properties.*

2. Definitions and basic properties

Notations:

- $\mathbb{K}$ number field of degree k,
- $\alpha^{(1)}, \ldots, \alpha^{(k)}$ the conjugates of $\alpha \in \mathbb{K}$,
- $\mathcal{O}$ an order in $\mathbb{K}$, *i.e.*, a ring which is a full $\mathbb{Z}$-module in $\mathbb{K}$.
- $1 = \omega_1, \omega_2, \ldots, \omega_k$ a $\mathbb{Z}$-basis of $\mathcal{O}$,
- $H(a) = \max\{|a_l^{(j)}|,\ l = 0, \ldots, n,\ j = 1, \ldots, k\}$ the *height* of a, provided $a(x) = \sum_{l=0}^{n} a_l x^l \in \mathcal{O}[x]$.

A *generalized number system over* $\mathcal{O}$ (GNS for short) is a pair $(p, \mathcal{D})$, where $p \in \mathcal{O}[x]$ is monic, $p_0 \neq 0$ and $\mathcal{D} \subset \mathcal{O}$ is a complete residue system modulo $p(0)$. The polynomial p is called *basis* of this number system, $\mathcal{D}$ is called its set of *digits*.

For the GNS $(p, \mathcal{D})$ denote $R(p, \mathcal{D})$ the set of $a \in \mathcal{O}[x]$ for which there exists $b \in \mathcal{D}[x]$ such that

$$a \equiv b \pmod{p}.$$

The GNS $(p, \mathcal{D})$ has the *finiteness property*, if $R(p, \mathcal{D}) = \mathcal{O}[x]$.

Let $\mathcal{F}$ be a bounded fundamental domain for the action of $\mathbb{Z}^k$ on $\mathbb{R}^k$, *i.e.*, a set that satisfies $\mathbb{R}^k = \mathcal{F} + \mathbb{Z}^k$ without overlaps. For $\alpha \in \mathcal{O}$ define

$$D_{\mathcal{F}} = D_{\mathcal{F},\alpha} = \Big\{ \tau \in \mathcal{O} \ : \ \frac{\tau}{\alpha} = \sum_{j=1}^{k} r_j \omega_j, \, (r_1, \dots, r_k) \in \mathcal{F} \Big\}. \qquad (1)$$

Lemma 1. *$D_{\mathcal{F},\alpha}$ is a complete residue system modulo α.*
Lemma 2. *Let $(p, \mathcal{D})$ be a GNS over $\mathcal{O}$. Then there is a bounded fundamental domain $\mathcal{F}$ for the action of $\mathbb{Z}^k$ on $\mathbb{R}^k$ such that $\mathcal{D} = D_{\mathcal{F},p(0)}$.*

A fixed fundamental domain $\mathcal{F}$ defines a whole class of GNS, namely,

$$\mathcal{G}_{\mathcal{F}} := \{(p, D_{\mathcal{F}}) \ : \ p \in \mathcal{O}[x]\}.$$

Examples:

- *Classical CNS* Let $\mathbb{K} = \mathbb{Q}$ and $\mathcal{O} = \mathbb{Z}$. Choose $\mathcal{F} = [0, 1)$ which obviously is a fundamental domain of $\mathbb{Z}$ acting on $\mathbb{R}$. We look at the class $\mathcal{G}_{\mathcal{F}} := \{(p, D_{\mathcal{F}})\ :\ p \in \mathbb{Z}[x]\}$. For an integer $\alpha \geq 2$ we have

$$D_{\mathcal{F},\alpha} = \left\{\tau \in \mathbb{Z}\ :\ \frac{\tau}{\alpha} = r, r \in [0, 1)\right\} = \{0, \ldots, |\alpha| - 1\},$$

which is the digit set of a canonical number system.

If, however, $\alpha \leq -2$ then

$$D_{\mathcal{F},\alpha} = \left\{\tau \in \mathbb{Z}\ :\ \frac{\tau}{\alpha} = r, r \in [0, 1)\right\} = \{\alpha+1, \ldots, 0, \} = -\{0, \ldots, |\alpha|-1\}.$$

- *Symmetric CNS* $(p,\mathcal{D})$ is a symmetric CNS if $p \in \mathbb{Z}[x]$ and

$$\mathcal{D} = \Big[-\frac{|p(0)|}{2}, \frac{|p(0)|-1}{2}\Big) \cap \mathbb{Z}.$$

These number systems were studied for instance by Akiyama and Scheicher (2007), Brunotte (2009), Kátai (1995) and Scheicher, Surer, Thuswaldner and van de Woestijne (2014). They are equal to the class $\mathcal{G}_{\mathcal{F}} := \{(p, D_{\mathcal{F}}) \ : \ p \in \mathbb{Z}[x]\}$ with $\mathcal{F} = [-\frac{1}{2}, \frac{1}{2})$ of GNS.

Proposition 3. *Let $(p, \mathcal{D})$ be a GNS with finiteness property. Then all roots of each conjugate polynomial $p^{(j)}(x)$, $j \in \{1, \dots, k\}$, lie outside the closed unit disk.*

Adapting the proof of Akiyama and Rao (2004) or Pethő (2006) to orders one can prove the following algorithmic criterion for checking the finiteness property of a given GNS $(p, \mathcal{D})$.

Theorem 4. *Let $\mathbb{K}$ be a number field of degree k and let $\mathcal{O}$ be an order in $\mathbb{K}$. Let $(p, \mathcal{D})$ be a GNS over $\mathcal{O}$. There exists a computable constant $C = C(p, \mathcal{D})$ such that $(p, \mathcal{D})$ is a GNS with finiteness property if and only if the polynomial $\prod_{i=1}^{k} p^{(i)}(x)$ is expansive and*

$$\{a \in \mathcal{O}[x] \ : \ \deg a < \deg p \text{ and } H(a) \leq C\} \subset R(p, \mathcal{D}).$$

3. General criterion for the finiteness property

Theorem 5 (B. Kovács (1981)). *Let* $p = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$ *such that* $1 \leq a_{n-1} \leq \ldots \leq a_0, a_0 \geq 2$. *Then* $(p, \{0, 1, \ldots, a_0 - 1\})$ *is a GNS.*

Generalizations: Akiyama and Pethő (2002), Scheicher and Thuswaldner (2004), or Pethő and Varga (2017).
In each of these results $|p(0)|$ dominates over the other coefficients of p. In general, $\mathcal{O}$ does not have a natural ordering. However, inclusion properties of some sets can be used to express dominance of coefficients in $\mathcal{O}$.

For $p(x) = x^n + p_{n-1}x^{n-1} + \cdots + p_0 \in \mathcal{O}[x]$ let $(p, \mathcal{D})$ be a GNS and let $\mathcal{F}$ be an associated fundamental domain.

We call $\mathbf{z}' \in \mathbb{Z}^k$ a *neighbor* of $\mathbf{z} \in \mathbb{Z}^k$ if $\mathcal{F} + \mathbf{z}$ "touches" $\mathcal{F} + \mathbf{z}'$, *i.e.*, if $(\overline{\mathcal{F}} + \mathbf{z}) \cap (\overline{\mathcal{F}} + \mathbf{z}') \neq \emptyset$. Let $\mathcal{N}$ be the set of neighbors of $\mathbf{0}$.

Set (letting $p_n = 1$)

$$\Delta = \left\{ \sum_{j=1}^{k} \eta_j \omega_j \ : \ (\eta_1, \ldots, \eta_k) \in \mathcal{N} \right\} \quad \text{and} \quad Z = \left\{ \sum_{j=1}^{n} \delta_j p_j \ : \ \delta_j \in \Delta \right\}, \qquad (2)$$

and note that, since $\mathcal{F}$ is bounded, these sets are finite.

Theorem 6. *Let* $p(x) = x^n + p_{n-1}x^{n-1} + \cdots + p_0 \in \mathcal{O}[x]$ *and* $(p, \mathcal{D})$ *be a GNS. Let* $\mathcal{F}$ *be an associated fundamental domain and define* Δ *and* Z *as in* (2). *Assume that the following conditions hold:*

(i) $Z + \mathcal{D} \subset \bigcup_{\delta \in \Delta}(\mathcal{D} + p_0\delta)$,

(ii) $Z \subset \mathcal{D} \cup (\mathcal{D} - p_0)$,

(iii) $\left\{\sum_{j \in J} p_j \ : \ J \subseteq \{1, \ldots, n\}\right\} \subseteq \mathcal{D}$.

Then $(p, \mathcal{D})$ *has the finiteness property.*

4. The finiteness property for large constant terms

Notations:

- $(M)_\varepsilon$ ε-neighborhood of a set $M \subset \mathbb{R}^k$,
- int_+ is the interior taken w.r.t. the subspace topology on $\{(r_1, \ldots, r_k) \in \mathbb{R}^k \ : \ r_1 \geq 0\}$. The symbol int_- is defined by replacing $r_1 \geq 0$ with $r_1 \leq 0$.

Theorem 7. *Let $\mathbb{K}$ be a number field of degree k and let $\mathcal{O}$ be an order in $\mathbb{K}$. Let a monic polynomial $p \in \mathcal{O}[x]$ and a bounded fundamental domain $\mathcal{F}$ for the action of $\mathbb{Z}^k$ on $\mathbb{R}^k$ be given. Suppose that*

- $\mathbf{0} \in \mathrm{int}(\mathcal{F} \cup (\mathcal{F} - \mathbf{e}_1))$, *where* $\mathbf{e}_1 = (1, 0, \ldots, 0)$ *and*
- $\mathbf{0} \in \mathrm{int}_+(\mathcal{F})$.

Then there is $\eta > 0$ such that $(p(x+\alpha), D_{\mathcal{F}})$ has the finiteness property whenever $\alpha = m_1\omega_1 + \cdots + m_k\omega_k \in \mathcal{O}$ satisfies $\max\{1, |m_2|, \ldots, |m_k|\} < \eta m_1$.

If $\mathcal{F}$ satisfies the conditions of Theorem 7 the set $\{(p, \mathcal{D}_{\mathcal{F},p(0)}\}$ contains infinitely many GNS with finiteness property.

Theorem 7 immediately admits the following corollary.

Corollary 8. *Let $\mathbb{K}$ be a number field of degree k and let $\mathcal{O}$ be an order in $\mathbb{K}$. Let a monic polynomial $p \in \mathcal{O}[x]$ and a bounded fundamental domain $\mathcal{F}$ for the action of $\mathbb{Z}^k$ on $\mathbb{R}^k$ be given. If $\mathbf{0} \in \text{int}(\mathcal{F})$ then there is $\eta > 0$ such that $(p(x+\alpha), D_{\mathcal{F}})$ has the finiteness property whenever $\alpha = m_1\omega_1 + \cdots + m_k\omega_k \in \mathcal{O}$ satisfies $\max\{1, |m_2|, \ldots, |m_k|\} < \eta|m_1|$.*

Under the conditions of Theorem 7

$\exists\, M \in \mathbb{N}:\ (p(x{+}m), \mathcal{F})$ *is a GNS with finiteness property for* $m \geq M$,

while under the more restrictive conditions of Corollary 8

$\exists\, M \in \mathbb{N}:\ (p(x{\pm}m), \mathcal{F})$ *is a GNS with finiteness property for* $m \geq M$.

The next Corollary answers partially a question of Akiyama.

Corollary 9. *Let $\mathbb{K}$ be a number field of degree k and let $\mathcal{O}$ be an order in $\mathbb{K}$. Let a monic polynomial $p \in \mathcal{O}[x]$ and a bounded fundamental domain $\mathcal{F}$ for the action of $\mathbb{Z}^k$ on $\mathbb{R}^k$ be given. Suppose that $\mathbf{0} \in \mathrm{int}(\mathcal{F})$ then there is $\eta > 0$ such that $(p(x) \pm \alpha, D_{\mathcal{F}})$ has the finiteness property whenever $\alpha = m_1\omega_1 + \cdots + m_k\omega_k \in \mathcal{O}$ satisfies $\max\{1, |m_2|, \ldots, |m_k|\} < \eta |m_1|$.*

If $k = 1$, and $0 < \varepsilon < 1$ then $\mathcal{F}_\varepsilon = [-\varepsilon, 1 - \varepsilon)$ satisfies the conditions of Corollary 9, hence for any $p \in \mathbb{Z}[x]$ there exists $M \in \mathbb{Z}$ such that $(p(x) \pm m, \mathcal{F}_\varepsilon)$ is a GNS with finiteness property in $\mathbb{Z}[x]$.

The assumptions of Theorem 7 hold for $\mathcal{F}_\varepsilon$ even if $\varepsilon = 0$. Hence, if all coefficients of p are non-negative, then we can conclude $(p(x) + m, \mathcal{F}_0)$ is a GNS with finiteness property in $\mathbb{Z}[x]$.

However, if some of the coefficients of p are negative, then our method fails and, we do not have similar statement. The example $p = x^2 - 2x + 2$ shows that $(p(x) + m, \mathcal{F}_0)$ is not a GNS with finiteness property in $\mathbb{Z}[x]$ for any $m \geq 0$.

If there are infinitely many units in $\mathcal{O}$ then for all $p \in \mathcal{O}[x]$ there exist infinitely many $\alpha \in \mathcal{O}$ such that the constant term of $p(x)+\alpha$, i.e., $p(0)+\alpha$ is a unit, hence $p(x)+\alpha$ is not GNS with finiteness property. Notice that Condition (iii) of Theorem 6 holds under the assumptions of Corollary 9 only if the norm of $p(0)+\alpha$ is large.

5. GNS without finiteness property

We start with a partial generalization of a Theorem of Kovács and Pethő (1991) to polynomials with coefficients of $\mathcal{O}$.

Lemma 10. *Let* $(p, \mathcal{D})$ *be a GNS. If there exist* $h \in \mathbb{N}$, $d_0, d_1, \ldots, d_{h-1} \in \mathcal{D}$ *not all equal to* 0 *and* $q_1, q_2 \in \mathcal{O}[x]$ *with*

$$\sum_{j=0}^{h-1} d_j x^j = (x^h - 1) q_1(x) + q_2(x) p(x). \tag{3}$$

then $(p, \mathcal{D})$ *doesn't have the finiteness property.*

Our main result in this section is the following theorem.

Theorem 11. *Let $\mathbb{K}$ be a number field of degree k and let $\mathcal{O}$ be an order in $\mathbb{K}$. Let a monic polynomial $p \in \mathcal{O}[x]$ and a bounded fundamental domain $\mathcal{F}$ for the action of $\mathbb{Z}^k$ on $\mathbb{R}^k$ be given. Suppose that $\mathbf{0} \in \text{int}_-(\mathcal{F} - \mathbf{e}_1)$. There exists $M \in \mathbb{N}$ such that $(p(x-m), D_{\mathcal{F}})$ doesn't have the finiteness property for $m \geq M$.*

6. GNS in number fields

Let $\alpha \in \mathcal{O}_{\mathbb{L}}$ and let $\mathcal{N}$ be a complete residue system modulo α. The pair $(\alpha, \mathcal{N})$ is called a *number system in* $\mathcal{O}_{\mathbb{L}}$. If for each $\gamma \in \mathcal{O}_{\mathbb{L}}$ there exist integers $\ell \geq 0$, $d_0, \ldots, d_{\ell-1} \in \mathcal{N}$ such that

$$\gamma = \sum_{j=0}^{\ell-1} d_j \alpha^j$$

then we say that $(\alpha, \mathcal{N})$ has the *finiteness property*. If the digit set is chosen to be $\mathcal{N} = \{0, 1, \ldots, |N_{\mathbb{L}/\mathbb{Q}}(\alpha)| - 1\}$ then $(\alpha, \mathcal{N})$ is called a *canonical number system in* $\mathcal{O}_{\mathbb{L}}$.

Kovács (1981) proved that there exists a canonical number system with finiteness property in $\mathcal{O}_{\mathbb{L}}$ if and only if $\mathcal{O}_{\mathbb{L}}$ admits a power integral bases. Later Kovács and Pethő (1991) proved the stronger result.

Proposition 12. *Let $\mathcal{O}$ be an order in the algebraic number field $\mathbb{L}$. There exist $\alpha_1, \ldots, \alpha_t \in \mathcal{O}$, $n_1, \ldots, n_t \in \mathbb{Z}$, and $N_1, \ldots, N_t$ finite subsets of $\mathbb{Z}$, which are all effectively computable, such that $(\alpha, \mathcal{N}(\alpha))$ is a canonical number system with finiteness property in $\mathcal{O}$ if and only if $\alpha = \alpha_i - h$ for some integers i, h with $1 \leq i \leq t$ and either $h \geq n_i$ or $h \in N_i$.*

From Corollary 8 we derive that for number systems the relation is usually stronger, the theorem of Kovács and Pethő describes a kind of "boundary case" *viz.* a case where $0 \in \partial\mathcal{F}$.

Theorem 13. *Let $\mathbb{L}$ be a number field of degree l and let $\mathcal{O}$ be an order in $\mathbb{L}$. Let $\mathcal{F}$ be a bounded fundamental domain for the action of $\mathbb{Z}$ on $\mathbb{R}$. If $0 \in \mathrm{int}(\mathcal{F})$ then all but finitely many generators of power integral bases of $\mathcal{O}$ form a basis for a number system with finiteness property. Moreover, the exceptions are effectively computable.*

The proof combines a deep result of Győry (1978) with Corollary 8.

The assumption $0 \in \mathrm{int}(\mathcal{F})$ *implies that* $\{-1, 0, 1\} \subseteq D_{\mathcal{F}, p_j(\delta m)}$ *for all* m *large enough. Of course* $-1 \notin \mathcal{N}_0(\alpha + m)$, *hence, the proof of Theorem 13 does not work in the case of canonical number systems. Győry's theorem holds for relative extensions as well. To generalize Theorem 13 to this situation would require the generalization of Corollary 8 to all* $m \in \mathcal{O}$, *such that all conjugates of* m *are large enough. We have no idea how to prove such a result.*

Thank you for your attention!