

# Lattice-based number systems with the same radix

Jakub Krásenský  
joint work with Attila Kovács

Charles University (Prague)

24.5.2023

- 1 Number systems in rings
- 2 Number systems in lattices

# Definitions

Let  $R$  be a ring,  $\beta \in R$  (*radix*) and  $\mathcal{A} \ni 0$  a finite subset of  $R$  (*alphabet*).  
A  $(\beta, \mathcal{A})$ -*representation* of  $x \in R$  is

$$x = \sum_{i=0}^N \beta^i a_i, \quad \text{where } N \in \mathbb{N}_0, a_i \in \mathcal{A}, a_N \neq 0.$$

## Definition

We call  $(\beta, \mathcal{A})$  a *number system (GNS)* on  $R$  if every nonzero  $x \in R$  has a **unique**  $(\beta, \mathcal{A})$ -representation.

Which of the following are GNSs (in  $\mathbb{Z}$  or  $\mathbb{Z}[i]$ )?

$(10, \{0, \dots, 9\})$ ;  $(2, \{0, 1\})$ ;  $(2, \{-1, 0, 1\})$ ;  $(-2, \{0, 1\})$ ;  $(3, \{-1, 0, 1\})$ ;  
 $(10, \{-5, \dots, 5\})$ ;  $(1 + i, \{0, 1\})$ ;  $(-1 + i, \{0, 1\})$ .

Answer: The negabinary, the balanced ternary and the Penney number system.

# Definitions

Let  $R$  be a ring,  $\beta \in R$  (*radix*) and  $\mathcal{A} \ni 0$  a finite subset of  $R$  (*alphabet*).  
A  $(\beta, \mathcal{A})$ -*representation* of  $x \in R$  is

$$x = \sum_{i=0}^N \beta^i a_i, \quad \text{where } N \in \mathbb{N}_0, a_i \in \mathcal{A}, a_N \neq 0.$$

## Definition

We call  $(\beta, \mathcal{A})$  a *number system (GNS)* on  $R$  if every nonzero  $x \in R$  has a **unique**  $(\beta, \mathcal{A})$ -representation.

Which of the following are GNSs (in  $\mathbb{Z}$  or  $\mathbb{Z}[i]$ )?

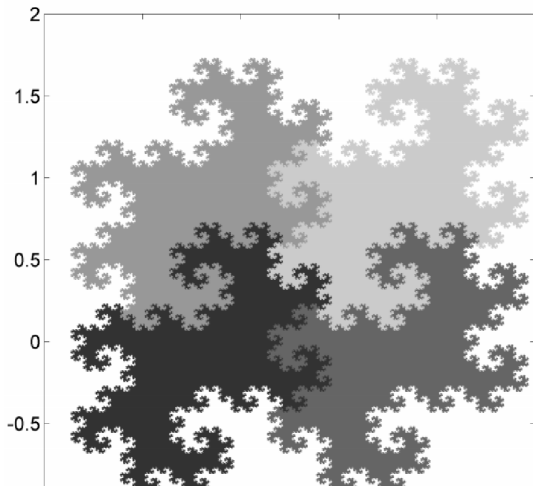
$(10, \{0, \dots, 9\})$ ;  $(2, \{0, 1\})$ ;  $(2, \{-1, 0, 1\})$ ;  $(-2, \{0, 1\})$ ;  $(3, \{-1, 0, 1\})$ ;  
 $(10, \{-5, \dots, 5\})$ ;  $(1 + i, \{0, 1\})$ ;  $(-1 + i, \{0, 1\})$ .

Answer: The negabinary, the balanced ternary and the Penney number system.

Penney, 1965:  $(-1 + i, \{0, 1\})$  is a GNS on  $\mathbb{Z}[i]$ .

(For example,  $-1 = \beta^4 + \beta^3 + \beta^2 + 1$  for  $\beta = -1 + i$ .)

Negative powers  $\sum_{j=-\infty}^N \beta^j a_j$  allow to represent all of  $\mathbb{C}$ :



Let  $(\beta, \mathcal{A})$  be a GNS in a number field order ( $\mathcal{O} \subset \mathcal{O}_K$  for a number field  $K$ ). Then:

- ①  $\mathcal{A}$  is a FRS modulo  $\beta$ ,
- ②  $|\beta_i| > 1$  for every conjugate of  $\beta$ .

If (1) and (2) hold, then:

- ①  $(\beta, \mathcal{A})$ -representations are unique.
- ② There exists a simple algorithm for computing them.
- ③ To decide the GNS property, it suffices to check finitely many elements  $x$ .

Situation in  $\mathbb{Z}$ :

- No GNS with radix 2.
- Radix  $-2$ : The only good alphabets are  $\pm\{0, 1\}$ .
- Good alphabets for 3: Difficult open question.

- Kátai, Szabó, 1975: Classification of GNSs in  $\mathbb{Z}[i]$  with  $\mathcal{A} = \{0, 1, \dots, n\}$ . (So-called *canonical number systems (CNS)*.)
- Steidl, 1989: Classification of all  $\beta \in \mathbb{Z}[i]$  which admit at least one GNS  $(\beta, \mathcal{A})$ .
- Kátai, 1992: Generalisation to  $\mathcal{O}_K$  for imaginary quadratic  $K$ .
- K., 2015: The analogue for Hurwitz and Lipschitz integral quaternions.

In the latter three cases, the statement is as follows:

A GNS with radix  $\beta$  exists if and only if  $|\beta| > 1$  and  $|\beta - 1| \neq 1$ .

### Definition (GNS on a lattice, Vince, 1993)

Let  $\Lambda$  be a  $\mathbb{Z}$ -lattice and  $L$  a linear operator on  $\Lambda$ . (For our purposes WLOG  $\Lambda = \mathbb{Z}^d$  and  $L \in \mathbb{Z}^{d \times d}$ .) Let  $\mathcal{A} \ni 0$  be a finite subset of  $\Lambda$ . We call  $(\beta, \mathcal{A})$  a *GNS* on  $\Lambda$  if every nonzero  $x \in \Lambda$  has a **unique** representation of the form

$$x = \sum_{i=0}^N L^i a_i, \quad \text{where } N \in \mathbb{N}_0, a_i \in \mathcal{A}, a_N \neq 0.$$

Again: If  $(L, \mathcal{A})$  is a GNS, then:

- ①  $\mathcal{A}$  is a FRS modulo  $L$ ;
  - in particular,  $|\mathcal{A}| = |\det L|$ .
- ②  $L$  is expansive, i.e.  $\rho(L^{-1}) < 1$ ;
- ③  $\det(L - I) \neq \pm 1$ . “Unit condition.”



- If  $L$  is a radix of a GNS, then  $L$  is *expansive* ( $\rho(L^{-1}) < 1$ ).
- For expansive  $L$ , there is a vector norm  $\|\cdot\|$  such that  $\|L^{-1}\| < 1$ ; this again gives an algorithm for checking the GNS property.
- Germán, Kovács, 2007: If  $\rho(L^{-1}) < 1/2$ , then  $L$  is a radix of some GNS.
- K., 2018: If  $\rho(L^{-1}) \leq 1/2$  and 2 is not an eigenvalue, then  $L$  is a radix of some GNS.

**Question:** Given a radix  $L$ , how many  $\mathcal{A}$  are there such that  $(L, \mathcal{A})$  is a GNS?

Matula, 1978: In  $\mathbb{Z}$ : If  $|\beta| > 2$ , then  $\beta$  is a radix of infinitely many GNSs. (For  $-2$  there are two GNSs, otherwise zero.)

**Question 2:** Can the suitable alphabets be “arbitrarily sparse” in the sense that all nonzero digits are far from the origin?

## Theorem (Kovács, K.)

*If  $L \in \mathbb{Z}^{d \times d}$  satisfies  $\rho(L^{-1}) < 1/2$ , then there are infinitely many  $\mathcal{A}$  such that  $(L, \mathcal{A})$  is a GNS in  $\mathbb{Z}^d$ .*

If one excludes  $L = (-2)$  in one dimension, it suffices to assume  $\rho(L^{-1}) \leq 1/2$  with 2 not an eigenvalue.

In a number field order  $\mathcal{O}$ :  $\beta$  is a radix of infinitely many GNSs iff it is a radix of at least one GNS and  $|\mathbf{N}(\beta)| \geq 3$ .

**Conjecture:** If  $|\det L| \neq 2$ , then there are infinitely many GNSs for  $L$  if and only if there is at least one.

## Theorem (K.)

*Suppose that  $\rho(L^{-1}) < 1/2$  and 2 is not an eigenvalue of  $L$ . Then there exists a family of arbitrarily sparse GNSs except for the case when every eigenvalue of  $L$  is either an integer or a non-real algebraic number of degree 2, and has geometric multiplicity 1.*

The proof is based on a clever choice of infinitely many different but related vector norms.

## Theorem (Kovács, K.)

Let  $L \in \mathbb{Z}^{2 \times 2}$  with non-real eigenvalues be given. Consider the family of all digit sets  $\mathcal{A} \subset \mathbb{Z}^2$  such that  $(L, \mathcal{A})$  is a GNS.

- ① The family is empty if and only if  $\det L = 1$  or  $\det(L - I) = \pm 1$ .
- ② The family is nonempty but finite if and only if  $\det L = 2$  and  $\det(L - I) \neq \pm 1$ .
- ③ In all other cases, the family is infinite, i.e. there are infinitely many digit sets  $\mathcal{A}$  such that  $(L, \mathcal{A})$  is a GNS.

This was the hardest part – we needed to develop a new general strategy to handle this case of dimension two.

Thank you for your attention (and for all your eventual questions)!  
I also happily answer questions sent to krasensky (at) seznam.cz.