Numeration Sytems in Sage

Attila Kovács

Eötvös Loránd University, Budapest

http://compalg.inf.elte.hu/∼attila

Sage Days 72
Prague

May 21-22, 2016

Table of contents

Notations

We consider a discrete linear model of number representation in euclidean spaces.

Given are

- a lattice Λ in $\mathbb{R}^n$
- a linear operator $M : \Lambda \to \Lambda$ such that $\det(M) \neq 0$
- $0 \in D \subseteq \Lambda$ a finite subset

Lattices have many significant applications in pure mathematics (Lie algebras, number theory and group theory), in applied mathematics (coding theory, cryptography) because of conjectured computational hardness of several lattice problems, and are used in various ways in the physical sciences.

Lattices in the Plane

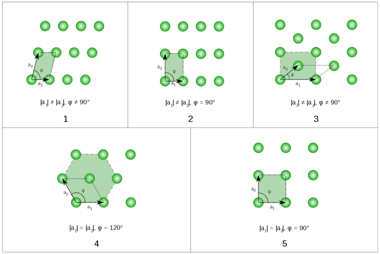


Figure : Lattices in the Euclidean plane

- A lattice Λ in $\mathbb{R}^n$ has the form $\Lambda = \{\sum_{i=1}^{n} \lambda_i \underline{a}_i \mid \lambda_i \in \mathbb{Z}\}$ where $\underline{a}_i$'s are linearly independent vectors
- Alternatively, Λ can be seen as a finitely generated free abelian group

Number Systems

Definition

The triple (Λ, M, D) is called a *number system* (GNS) if every element x of Λ has a unique, finite representation of the form $x = \sum_{i=0}^{\lambda} M^i d_i$, where $d_i \in D$ and $\lambda \in \mathbb{N}$. λ is the *length of the expansion*.

- A GNS satisfies the *unique representation property*.
- M is called the *base* and D is the *digit set*
- Exercise: Are the following number systems?
  - $(\mathbb{N}, 2, \{0, 1\})$
  - $(\mathbb{Z}, 10, \{0, 1, \dots, 9\})$

Remarks on the Base

- Similarity preserves the number system property, i.e, if M_1 and M_2 are similar via the matrix Q then (Λ, M_1, D) is a number system if and only if $(Q\Lambda, M_2, QD)$ is a number system
- If we change the basis in Λ a similar integer matrix can be obtained
- Hence, no loss of generality in assuming that M is integral acting on the lattice $\Lambda = \mathbb{Z}^n$
- An important case is when Q unimodular

Congruences

- If two elements of Λ are in the same coset of the factor group $\Lambda/M\Lambda$ then they are said to be congruent modulo M.
- Example. Let $\Lambda = \mathbb{Z}^2$, $M = \begin{pmatrix} 4 & 1 \\ 1 & 2 \end{pmatrix}$.

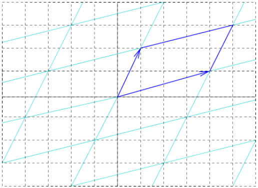


Figure : The lattices $\mathbb{Z}^2$ and $M\mathbb{Z}^2$

Then $v_1 = \binom{1}{1} \not\equiv \binom{2}{2} = v_2$ since there is not exist a $v_3 \in \mathbb{Z}^2$ for which $M \cdot z_3 = v_2 - v_1$. But $v_4 = \binom{-1}{1} \equiv \binom{3}{2} = v_5$ since $v_5 - v_4 = \binom{4}{1} = M \cdot \binom{1}{0}$.

Necessary conditions of GNS

Theorem

If (Λ, M, D) *is a number system then*

1. D *must be a full residue system modulo* M
2. M *must be expansive*
3. $\det(I - M) \neq \pm 1$*. ("Unit condition")*

If a system fulfills the first two conditions then it is called a radix system.

Exercise: Construct appropriate digit sets for the operators

- $\left(\begin{smallmatrix} 1 & 1 \\ 1 & m \end{smallmatrix}\right)$, $m \in \mathbb{Z}$
- $2I + S$ where S is strictly upper or lower triangular

GNS Composition

One can take the direct product of several systems as follows:
Let the radix systems (Λ_i, M_i, D_i) be given $(1 \leq i \leq k)$. Let

- $\Lambda = \otimes \Lambda_i$ (direct product)
- $M = \oplus_{i=1}^{k} M_i$ (direct sum)
- $D_h = \{(d_1^T \| d_2^T \| \cdots \| d_k^T)^T \ : \ d_i \in D_i\}$ (homomorphic digit set)

Theorem

(Λ, M, D_h) *is a number system if and only if* (Λ_i, M_i, D_i) *are number systems.*

Corollary

Many new GNS can be created via homomorphic construction.

Frobenius Normal Form

- The Frobenius normal form of a square $n \times n$ matrix M has the structure $\mathrm{diag}(C_1, \ldots, C_r)$ where C_i's are companion matrices associated with monic polynomials $p_1, \ldots, p_r$, where p_i's are factors of the characteristic polynomials of M with the property $p_i | p_{i+1}, (i = 1, \ldots, r-1)$
- The Frobenius normal form is unique and every matrix can be transformed by a similarity transformation to its Frobenius form
- We remark that the transformation is not necessary $\mathbb{Z}$-similar
- Frobenius normal form can be the starting point of the decomposition of systems

Dynamical Properties of Radix Systems

- Let $\varphi : \Lambda \to \Lambda$, $x \overset{\varphi}{\mapsto} M^{-1}(x-d)$ for the unique $d \in D$ satisfying $x \equiv d \pmod{M}$.
- Since M^{-1} is contractive and D is finite, there exists a norm $\|.\|$ on Λ and a constant C such that the orbit of every $x \in \Lambda$ eventually enters the finite set $S = \{x \in \Lambda \mid \|x\| < C\}$ for the repeated application of φ
- This means that the sequence $x, \varphi(x), \varphi^2(x), \ldots$ is eventually periodic for all $x \in \Lambda$
- (Λ, M, D) is a GNS iff for every $x \in \Lambda$ the orbit of x eventually reaches 0
- A point p is called periodic if $\varphi^k(p) = p$ for some $k > 0$
- The orbit of a periodic point p is a *cycle*
- All the periodic points are denoted by $\mathcal{P}$

Dynamical Properties (contd.)

- Let $\mathcal{G}(\mathcal{P})$ be a directed graph defined on $\mathcal{P}$ by drawing an edge from $p \in \mathcal{P}$ to $\varphi(p)$
- $\mathcal{G}(\mathcal{P})$ is a disjoint union of directed cycles (loops are allowed)
  - $\mathcal{P}$ is finite
  - if $p \in \mathcal{P}$ then $\varphi(p) \in \mathcal{P}$
  - if $p \in \mathcal{P}$ then $\|p\| \leq L = Kr/(1-r)$, where $r = \|M^{-1}\| = \sup_{\|x\| \leq 1} \|M^{-1}x\| < 1$, and $K = \max_{d \in D} \|d\|$

To be a bit more precise:

- If $\|z\| \leq L$ then $\|\varphi(z)\| \leq r(L+K) = L$
- If $\|z\| > L$ then $\|\varphi(z)\| \leq r\|z\| + L(1-r) < \|z\|(r+1-r) = \|z\|$

Problem Classes

- The *decision problem* for (Λ, M, D) asks if they form a GNS or not.
- The *classification problem* means finding all cycles (witnesses).
- The *parametrization problem* means finding parametrized families of GNS.
- The *construction problem* aims constructing a digit set D to M for which (Λ, M, D) is GNS.

We remark that the algorithmic complexity of the decision and classification problem is unknown. Regarding the construction problem even the two dimensional case is unknown.

Example

Let $\Lambda = \mathbb{Z}$, $M = -3$, $D = \{0, -4, 7\}$.
Then $K = 7$, $r = 1/3$, $L = 3.5$, therefore $\mathcal{P} \subseteq [-3, 3]$.
It is a radix system but not a GNS since

$$\begin{aligned} 1 &= 7 + 2 \cdot (-3) \Rightarrow \phi(1) = 2, \\ 2 &= -4 + (-2) \cdot (-3) \Rightarrow \phi(2) = -2 \\ 3 &= 0 + (-1) \cdot (-3) \Rightarrow \phi(3) = -1 \\ -3 &= 0 + 1 \cdot (-3) \Rightarrow \phi(-3) = 1 \\ -2 &= 7 + 3 \cdot (-3) \Rightarrow \phi(-2) = 3 \\ -1 &= -4 + (-1) \cdot (-3) \Rightarrow \phi(-1) = -1 \end{aligned}$$

Hence $\mathcal{G}(\mathcal{P}) = \{0 \to 0, -1 \to -1\}$.

Estimation for the Length of Expansions

Let $z \in \Lambda$. If $z_0 := z \notin \mathcal{P}$ then there is a unique $\lambda \in \mathbb{N}$ (length of expansion) and $d_0, d_1, \ldots, d_{\lambda-1} \in D$ such that

$$z_j = d_j + Mz_{j+1} \; (j = 0, \ldots, \lambda - 1), \; z_\lambda = p \in \mathcal{P}$$

and none of $z_0, z_1, \ldots, z_{\lambda-1}$ do belong to $\mathcal{P}$. Then the *standard expansion* of z is

$$z = (d_0, d_1, \ldots, d_{\lambda-1} \mid p) \, .$$

In this case $z = d_0 + Md_1 + \ldots + M^{\lambda-1} d_{\lambda-1} + M^l p$.
For a given (Λ, M, D) and $z \in \Lambda$ there is a constant $c \in \mathbb{N}$ for which

$$\lambda(z) \leq \frac{\log \|z\|}{\log (1/\|M^{-1}\|)} + c$$

Fractions or Fundamental Domain

- The set of "fractions" in (Λ, M, D) is

$$H = \left\{ \sum_{i=1}^{\infty} M^{-i} d_i : d_i \in D \right\} \subseteq \mathbb{R}^n$$

- H is compact.
- H has interior points. More specifically $\bigcup_{p\in\mathcal{P}}(p+H)$ contains a neighborhood of the origin.
- $\mathbb{R}^n = \bigcup(H + \Lambda)$
- For every $x \in \mathbb{R}^n$ there is a $z \in \Lambda$ and $h \in H$ such that $x = z + h$.
- $\mu(H) > 0$ (μ is the Lebesgue measure on $\mathbb{R}^n$).
- $x \in \mathcal{P} \Rightarrow x \in -H$

Shape of H

Let $g_d : \mathbb{R}^n \to \mathbb{R}^n$, $g_d(z) = Mz - d$, $d \in D$ and let $K(H)$ be a bounded subset of $\mathbb{R}^n$ containing H.

Escape Algorithm$(K(H), lim)$

for all $z \in K(H)$ **do**
  $S_0 \leftarrow \{z\}$, $j \leftarrow 0$
  while $j < lim$ or $S_j \neq \varnothing$ **do**
    $S_j \leftarrow \{g_{d_i}(z) : z \in S_{j-1}, d_i \in D, g_{d_i}(z) \in K(H)\}$
    $j \leftarrow j + 1$
  end while
  if $j < lim$ **then**
    $z \notin H$
  else
    $z \in H$
  end if
end for

Shape of H

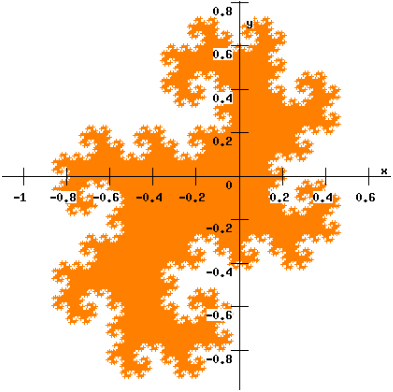
... or simply plot the points of the set

$$\left\{ \sum_{i=1}^{iterNum} M^{-i} d_i : d_i \in D \right\}$$

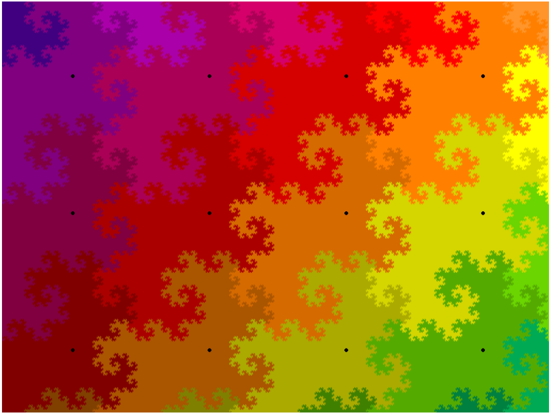
- Exercise: Implement it!

Example - Twindragon

$$M = \begin{pmatrix} -1 & -1 \\ 1 & -1 \end{pmatrix}, D = \{(0,0)^T, (1,0)^T\}.$$



Example - Twindragon Tiling



Algorithmical Aspects

- How to compute φ efficiently?
- How to decide the number system property?
- How to classify the expansions?
- How to construct number systems?

Hashing by the Adjoint method

- Using the fact that $M^* M = t \cdot I$ where M^* denotes the adjoint of M and $t = \det(M)$ one can easily compute the congruent element of a given point in $\mathbb{Z}^n$. Let

$$ListD = \left[0 = a_1, a_2, \ldots, a_{|t|}\right]$$

  where $a_i \in D$. Let $ListD_1 = M^* \cdot ListD \pmod{t \cdot I}$. Due to the CRS property of D for every $z \in \mathbb{Z}^n$ there exist a unique $d_j \in ListD_1$ such that $d_j = M^* z \pmod{t \cdot I}$
- Exercise: Implement the Adjoint method in Sage
- What about the running time?

Hashing by Smith normal form

- For fast computation of φ we can use the Smith normal form: there are linear transformations U, V mapping $\mathbb{Z}^n$ onto itself such that $UMV = G$ has diagonal form with positive integer elements $g_1, \ldots, g_n$ in the diagonal such that $g_i \mid g_{i+1}$ for $i = 1, 2, \ldots, n-1$, and $\prod_{i=1}^n g_i = |\det(M)|$
- The Smith normal form can be obtained by doing elementary row and column operations of M
- U and V are unimodular operators
- $z_1 \equiv z_2 \pmod{M}$ iff $Uz_1 \equiv Uz_2 \pmod{G}$
- Exercise: Implement it! What about the running time?

Determining the congruent digit

- Exercise: Implement the searching of the congruent digit
- What about the running time?
- Why Smith method is more efficient than the Adjoint method?
- Is there an even better method?

Congruence Hash

Theorem

Let $u_1, u_2, \ldots, u_n$ *denote the coordinates of* Uz, $z \in \Lambda$ *and let* $h : \Lambda \to \{0, 1, \ldots, |\det(M)| - 1\}$,

$$h(z) = \sum_{i=s+1}^{n} (u_i \mod g_i) \prod_{j=s+1}^{i-1} g_j \, ,$$

where $g_i = 1$, $i = 1, \ldots, s$. *Then* $z_1 \equiv z_2$ *modulo* M *if and only if* $h(z_1) = h(z_2)$

- Exercise: Implement it!
- Note: this is called *mixed radix representation*

Computing the orbit

- Implement the function φ
  - $y = \varphi(z)$
  - $y, d = \varphi(z)$, where $z \equiv d \pmod{()}M)$
- Implement the procedure OrbitFrom which computes the orbit of a given element v

Decide and Classify

- There are various deterministic methods for solving the decision and the classification problem
- Consider the decision problem. Our task is to find a witness for a non-trivial period
- Consider the classification problem. In this case we have to find all periods
- Since the possible periodic points are in the set $-H$ we have to analyze the orbits starting from a finite set of points (H is compact)

IFS-Method

- Iterated Function System Method: The functions

$$f_d : \mathbb{R}^n \to \mathbb{R}^n$$

$$f_d(z) = M^{-1}(z + d)$$

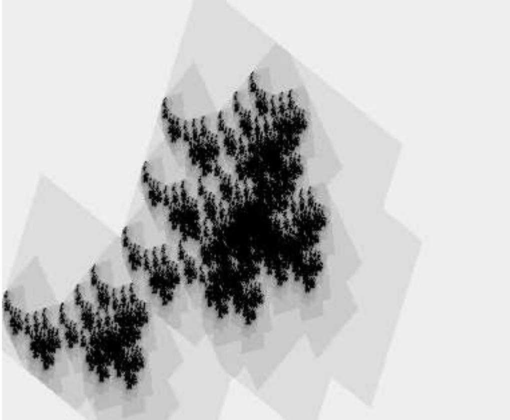
  for all $d \in D$ are linear contractions.
- If $z \in H$ then $f_d(z) \in H$ for all $d \in D$.
- Hence f_d are right shift maps and

$$H = \bigcup_{d \in D} f_d(H)$$

- H is a self-affine attractor of the IFS generated by $\{f_d\}$

Example for the IFS-Method

$$M = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}, D = \{(0,0)^T, (1,0)^T, (0,1)^T, (0,-1)^T, (-2,-3)^T\}.$$



Box Coverage

- This method uses a covering of the set of fractions $-H$.
- Since $-H$ is compact, it gives lower and upper bounds on the coordinates of periodic points.
- The basic idea is the following: since M is expansive there is a constant C such that $\|M^{-c}\|_\infty < 1$ for all $c \geq C$. Hence $(I - M^{-C})^{-1}$ exists and

$$\gamma := \frac{1}{1 - \|M^{-C}\|_\infty} \geq \|(I - M^{-C})^{-1}\|_\infty$$

Box Coverage (contd.)

- Let $\xi_m^{(j)} = \max_{d \in D} Proj_m(M^{-j}d)$ and $\eta_m^{(j)} = \min_{d \in D} Proj_m(M^{-j}d)$ for all $1 \leq m \leq n$.
- Then $M^{-j}d$ can be covered by the sets X_j where $\eta_m^{(j)} \leq Proj_m X_j \leq \xi_m^{(j)}$
- Similarly, the set $\sum_{j=1}^{C} M^{-j}d_j$ can be covered by an appropriate set W, where $\sum_{j=1}^{C} \eta_m^{(j)} \leq Proj_m W \leq \sum_{j=1}^{C} \xi_m^{(j)}$.
- Hence,
$$H \subseteq W + M^{-C}W + M^{-2C}W + \cdots$$

Box Coverage (contd.)

- Putting together, if p is a periodic point then $l_i \leq Proj_m p \leq u_i$ where

$$l_i = -\lceil \gamma \sum_{j=1}^{C} \eta_m^{(j)} \rceil \text{ and } u_i = -\lfloor \gamma \sum_{j=1}^{C} \xi_m^{(j)} \rfloor$$

- Implement the Box Coverage method
- Let us denote this box by $K(\Lambda, M, D)$
- The volume of $K(\Lambda, M, D)$ is $Vol = \prod_{i=1}^{n}(u_i - l_i + 1)$

Decide-Method-A

- For each element z of $K(\Lambda, M, D)$ one could determine the orbit of z
- If the orbit ends up with a non-zero cycle we have found a witness of the non-numeration-system
- Implement the method
- Can the method make parallel?

Classify-Method A

- Decide-Method-A can be extended for solving the classification problem
- Design and implement your solution

Decide-Method-B

Brunotte's canonical number system decision algorithm can be extended

CONSTRUCT-SET-E(M, D)

$E \leftarrow D,\ E' \leftarrow \varnothing$
while $E \neq E'$ **do**
    $E' \leftarrow E$
    for all $e \in E$ and $d \in D$ **do**
        put $\varphi(e + d)$ into E
    end for
end while
return E

It can be proved that the algorithm terminates

Decide-Method-B

Denote $B = \{(0, 0, \ldots, 0, \pm 1, 0, \ldots, 0)^T\}$ the n basis vectors and their opposites

$\underline{\textsc{Decide-Method-B}(M, D)}$

$E \leftarrow \textsc{Construct-set-E}(M, D)$
for all $p \in B \cup E$ **do**
  if p has no finite expansion **then**
    return false
  end if
end for
return true

Classification, Method B

The second method can also be modified for finding the all the cycles.

CLASSIFY-METHOD-B(M, D)

```
𝒟 ← D
finished ← false
while not finished do
    ℰ ← CONSTRUCT-SET-E(M, 𝒟)
    finished ← true
    for all p ∈ ℰ ∪ B do
        if p does not run eventually into 𝒟 then
            put newly found periodic points into 𝒟
            finished ← false
        end if
    end for
end while
return 𝒟 \ D (the set of non-zero periodic points)
```

- Can the method make parallel?

GNS and Algebraic Integers

- What are the connections between algebraic numbers and radix systems?
- Let

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} + x^n$$

  be a monic integer polynomial
- Let us denote the factor ring $\mathbb{Z}[x]/(f)$ by Λ_f
- Then Λ_f is a lattice and all the problems regarding number expansions can be formulated in $\mathbb{Z}^n$
- If f is irreducible then Λ_f is isomorphic with $\mathbb{Z}[\theta]$ where $f(\theta) = 0$ in an appropriate extension of $\mathbb{Q}$

Digit sets

- If the digit set D is restricted to the set of non-negative numbers $D = \{0, 1, \ldots, |a_0| - 1\}$ we get a straightforward generalization of traditional number systems in $\mathbb{Z}$.
- The set $D_{c,j} = \{i \cdot e_j \;:\; i = 0, \ldots, |\det(M)| - 1\} \subset \mathbb{Z}^n$ is called *j-canonical digit set*. 1-canonical sets are simple called canonical. Canonical GNS is called CNS.
- Canonicity depends on the chosen basis.
- *j-symmetrical digit sets* can be defined similarly, $D_{s,j} = \{i \cdot e_j, i = -\lfloor(|\det(M)| - 1)/2\rfloor, \ldots, \lfloor|\det(M)|/2\rfloor\}$
- Implement these constructions
- Write a Sage code which decides whether a given digit set is a full residue system or not

Example

- Consider the Gaussian ring $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$
- Let the base $\alpha = a + bi \in \mathbb{Z}[i]$ and the digit set $D = \{0, 1, 2, \ldots, a^2 + b^2\}$ (since $N(\alpha) = a^2 + b^2$)
- Let $a = 3, b = 1$. The Gaussian integer $\beta = -53 + 88i$ has the expansion $(4321)_\beta$ since $\beta = 1 + 2\alpha + 3\alpha^2 + 4\alpha^3$ (Verify!)
- Since the basis in $\mathbb{Z}[i]$ is $\{1, i\}$ and $(a + bi)i = -b + ai$ therefore the appropriate base in $\mathbb{Z}^2$ is $M = \left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$ and the digit set is $D = \{(0, 0)^T, (1, 0)^T, \ldots, (a^2 + b^2 - 1, 0)^T\}$.
- Again, let $a = -3, b = 1$. Compute the expansion of $[-53, 88]^T$.

Construction

- Given lattice Λ and operator M satisfying criteria 2) and 3) in Theorem 1 is there any suitable digit set D for which (Λ, M, D) is a number system?
- If yes, how many and how to construct them?

Theorem

If $\rho(M^{-1}) < 1/2$ then there exists a digit set D for which (Λ, M, D) is GNS.

Theorem

Let the polynomial $c_0 + c_1 x + \cdots + x^n \in \mathbb{Z}[x]$ be given and let us denote its companion matrix by C_M. If the condition $|c_0| > 2\sum_{i=1}^{n} |c_i|$ holds then there exists a digit set D for which $(\mathbb{Z}^n, C_M, D)$ is GNS.

Existence of GNS

Is GNS **exist for all bases**?

- Is the digit set construction always possible?

Let

$$M = \begin{pmatrix} 1 & 1 & -1 & 0 \\ -1 & 0 & 1 & 1 \\ 1 & 0 & -1 & 1 \\ -1 & 0 & 0 & 0 \end{pmatrix}$$

M is expansive, its characteristic polynomial is $f(x) = x^4 + x^2 + 2$, $D = \{0, e_1\}$ is a complete residue system modulo the companion matrix C_M of $f(x)$ and $(\mathbb{Z}^4, C_M, D)$ is a number system, but it is not possible to give any digit set D', for which $(\mathbb{Z}^4, M, D')$ would be a number system (Barbé et al.).

Existence of GNS

Theorem

For every radix base $M_1 : \mathbb{Z}^{n_1} \to \mathbb{Z}^{n_1}$ *either*

1. *there is a digit set* D_1 *for which* $(\mathbb{Z}^{n_1}, M_1, D_1)$ *is GNS, or*
2. *there is a radix* $M_2 : \mathbb{Z}^{n_2} \to \mathbb{Z}^{n_2}$*, such that* $(\mathbb{Z}^{n_1} \otimes \mathbb{Z}^{n_2}, M_1 \oplus M_2, D)$ *is GNS for some digit set* D

The proof is constructive.

References

- Kátai, I., Szabó, J., *Canonical number systems for complex integers*, Acta Sci Math. **37**, (1975), 255–260.
- Vince, A., *Replicating tessellations*, SIAM J. Discrete Math., **6**, (1993), 501–521.
- Kovács, A., *On computation of attractors for invertible expanding linear operators in* $\mathbb{Z}^k$, Publ. Math. Debrecen **56**/1–2, (2000), 97–120.
- Brunotte, H., *On trinomial bases of radix representations of algebraic integers*, Acta Sci. Math. (Szeged), **67**, (2001), 407–413.
- Kovács, A., *Number expansion in lattices*, Math. and Comp. Modelling, **38**, (2003), 909–915.
- Burcsi, P., Kovács, A., *An algorithm checking a necessary condition of number system constructions*, Annales Univ. Sci. Budapest. Sect. Comput. **25**, (2005), 143–152.
- Barbé, A., von Haeseler, F., *Binary number systems for* $\mathbb{Z}^k$, Journal of Number Theory, **117**, (2006), 14–30.
- Germán, L., Kovács, A., *On number system constructions*, Acta Math., Hungar., **115**, Numbers 1-2, (2007), 155–167.
- Burcsi, P., Kovács, A., Papp-Varga, Zs., *Decision and Classification Algorithms for Generalized Number Systems*, **28**, (2008), 141–156.
- Burcsi, P., Kovács, A., *Exhaustive search methods for CNS polynomials*, Monatshefte für Mathematik, **155**, (2008), 421–430,
- Kovács, A., *Number System Constructions with Block Diagonal Bases*, RIMS Kokyuroku-Bessatsu, B**46**, 'Numeration and Substitution', (2014), 205–213.