Lattice-based number systems with the same radix

Jakub Krásenský and Attila Kovács

Let us first briefly recall the much-studied concept of *canonical number systems*: Let β be an algebraic integer, and put $D_{\text{can}} = \{0, 1, \dots, \mathrm{N}(\beta) - 1\}$. We say that β is a radix of a CNS if every $x \in \mathbb{Z}[\beta]$ has a unique representation of the form

$$x = \sum_{k=0}^{N} \beta^k a_k, \qquad \text{where } N \in \mathbb{N}_0,\ a_k \in D_{\text{can}},\ a_N \neq 0.$$

If D_{can} is replaced by another finite subset of $\mathbb{Z}[\beta]$ containing zero, and the condition of existence of unique representations is kept, we get a more general notion of a number system, sometimes called GNS (generalized number system). For example, G. Steidl [5] showed that for every $\beta \in \mathbb{Z}[\mathrm{i}]$ satisfying $|\beta| \neq 1$, $|1 - \beta| \neq 1$, there is a suitable $D \subset \mathbb{Z}[\mathrm{i}]$ such that every element of $\mathbb{Z}[\mathrm{i}]$ has a unique representation. In other words: In $\mathbb{Z}[\mathrm{i}]$, almost every element β can serve as a radix of a GNS. Soon afterwards, I. Kátai [3] extended this result to all rings of integers of imaginary quadratic fields.

Another important generalization of canonical number systems are the so-called CNS-polynomials, where one aims to represent elements of the factor ring $\mathbb{Z}[x]/(f)$, with $f \in \mathbb{Z}[x]$ a not-necessarily irreducible monic polynomial.

Both the CNS-polynomials and the number systems in orders of number fields are captured by the following concept, which is often the more convenient framework to study them:

Suppose that a regular matrix (*radix*) $L \in \mathbb{Z}^{d \times d}$ and a finite set of *digits* $0 \in D \subset \mathbb{Z}^d$ are given. The pair (L, D) is called a *GNS* in $\mathbb{Z}^d$ if every $z \in \mathbb{Z}^d$ has a unique representation of the form

$$z = \sum_{k=0}^{N} L^k a_k, \qquad \text{where } N \in \mathbb{N}_0,\ a_k \in D,\ a_N \neq 0.$$

The GNS in dimension higher than 1 were probably first studied by A. Vince [6]; some of the main ideas go back to I. Kátai, topological aspects were studied among

Jakub Krásenský
Charles University in Prague, Czech Republic, e-mail: jakub.krasensky@mff.cuni.cz

Attila Kovács
Eötvös Loránd University, Budapest, Hungary, e-mail: attila.kovacs@inf.elte.hu

others by W. Gilbert, and a significant contribution was made by A. Barbé and F. von Haeseler [1].

Since even determining all GNSs with radix 3 in $\mathbb{Z}$ is a notoriously hard and possibly unsolvable task, the focus is on other questions. For example, given a radix $L \in \mathbb{Z}^{d\times d}$, is there at least one digit set D such that (L,D) is a GNS? The answer depends largely on the spectral radius of L^{-1}: Already Vince showed that there can be no GNS with radix L if $\rho(L^{-1}) \geq 1$; on the other hand, L. Germán and A. Kovács showed that a similar condition is already sufficient:

Theorem ([2])**.** *If $L \in \mathbb{Z}^{d\times d}$ satisfies $\rho(L^{-1}) < 1/2$, then there always exists a digit set D such that (L,D) is a GNS in $\mathbb{Z}^d$.*

In this talk, we study a more refined question then just the mere existence of one suitable digit set:

Question. *Given $L \in \mathbb{Z}^{d\times d}$, for how many digit sets D is (L,D) a GNS?*

For $d = 1$, this problem was fully solved by D. Matula [4]: For radices $-1, 0, 1, 2$, the answer is zero, and for -2, the answer is two; in all other cases there are infinitely many good digit sets.

We conjecture that unless $\det L = \pm 2$ (which was essentially solved by Barbé and von Haeseler), the existence of one GNS for a given radix already implies the existence of infinitely many. This is still out of reach, but by a combination of many ideas we obtained the following main result (which significantly improves the above theorem of Germán and Kovács):

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

One of the crucial parts of the proof is a reduction step which allows to restrict to operators with irreducible characteristic polynomials. For such operators, the solution is fairly simple unless $d = 2$ and L has complex eigenvalues – but this case, which is a slight generalization of number systems in imaginary quadratic fields, turned out to be very involved. Nevertheless, using a construction which starts from one GNS and exchanges one particular digit for a congruent one, we obtained the following missing result which is interesting on its own:

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

References

1. A. Barbé and F. von Haeseler, *Binary number systems for $\mathbb{Z}^k$*, J. Number Theory 117 (2006), 14–30.
2. L. Germán and A. Kovács, *On number system constructions*, Acta Math. Hungar. 115 (2007), 155–167.
3. I. Kátai, *Number systems in imaginary quadratic fields*, Ann. Univ. Sci. Budapest. Sect. Comput. 14 (1994), 91–103.
4. D. W. Matula, *Basic digit sets for radix representation*, J. ACM 29 (1982) 1131–1143.
5. G. Steidl, On symmetric radix representation of Gaussian integers, BIT, Numerical Mathematics 29 (1989), 563–571.
6. A. Vince, *Replicating Tessellations*, SIAM J. Discrete Math. 6 (1993), 501–521.