Digital expansions in abelian groups

Christiaan van de Woestijne
Montanuniversität Leoben, Austria
email: c.vandewoestijne@unileoben.ac.at

Number systems in abelian groups

To define a pre-number system in an abelian group V, we need the following ingredients.

- Let ϕ be an endomorphism of V, that is, a homomorphism
$$\phi : V \to V,$$
which we call the base.
- We assume that the image of ϕ has finite index D in V. In particular, in case V is a finite-dimensional $\mathbb{Z}$-lattice, we have $\det \phi = |D| \neq 0$.
- Let $\mathcal{D}$ be a finite subset of V containing a system of representatives of V modulo $\phi(V)$. We call this the digit set.

Now, a pre-number system $(V, \phi, \mathcal{D})$ as above is a number system if every $v \in V$ has a finite expansion of the form
$$v = \sum_{i=0}^{\ell} \phi^i(d_i) \quad \text{with the } d_i \in \mathcal{D}.$$
This definition was given for the case where V is a finite free $\mathbb{Z}$-module in [9], among others, in the context of replicating tilings of $\mathbb{R}^n$, and also in [4]. Many previous authors required that $0 \in \mathcal{D}$. We do not require this.
If we choose a basis for V, then we may assume that $V = \mathbb{Z}^n$, and ϕ is given by a nonsingular $n \times n$ matrix with integer coefficients.

Basic problems

1. Given a pre-number system $(V, \phi, \mathcal{D})$, how can we decide if it is a number system?
2. Given a lattice V and a base (endomorphism) ϕ, does there exist a valid digit set, i.e., a digit set $\mathcal{D}$ that makes $(V, \phi, \mathcal{D})$ into a number system?
3. Given V and ϕ, can we classify all valid digit sets $\mathcal{D}$?

Examples and motivation

- The basic example is $V = \mathbb{Z}$, with ϕ the map $v \mapsto bv$ for a fixed $b \neq 0$, and $\mathcal{D} = \{0, 1, \ldots, |b| - 1\}$. For $b \geq 2$, this gives the usual b-adic representation of the nonnegative integers.
  To satisfy our definition, also negative integers must have a representation. This is only possible, using the given digits, if $b \leq -2$. This was known already in 1885 to Grünwald.
- Complex bases of the form $a + bi$, where $a, b \in \mathbb{Z}$, were already considered by Knuth. The digit set was taken to be $\{0, 1, \ldots, a^2 + b^2 - 1\}$, and it was shown that we get a number system if and only if the base has the form $n \pm \mathrm{i}$ for some $n \neq 0 \in \mathbb{Z}$. Later, this result was generalised for arbitrary quadratic numbers [3].
- Let α be an algebraic integer, with minimal polynomial $f = \sum_i a_i X^i \in \mathbb{Z}[X]$. Then take $V = \mathbb{Z}[\alpha] \cong \mathbb{Z}[X]/(f)$, and let ϕ be multiplication by α. It is easy to see that $\mathcal{D} = \{0, 1, \ldots, |f(0)| - 1\}$ represents $V/\alpha V$.
  This is a pre-number system. If every $v \in \mathbb{Z}[\alpha]$ has a representation of the form $v = \sum_{i=0}^{\ell} d_i \alpha^i$, the resulting number system is called a canonical number system (CNS), because the digits are canonically chosen. A survey of results on CNS is given in [1].
- The previous definition can be extended. If α is algebraic but not necessarily integral, we obtain so-called rational bases (see [7]). Here, we take the minimal polynomial f to be integral and primitive. In this case, if f is not monic, then $V = \mathbb{Z}[X]/(f)$ is no longer a finite-dimensional lattice — in fact, it is not finitely generated.

A few years ago, there has been a lot of interest for nonstandard digital expansions, with the goal of speeding up operations in elliptic curve cryptography [2, Chapter III]. An important role is played by the base $\tau = \frac{1+\sqrt{-7}}{2}$, an algebraic integer that satisfies the same minimal polynomial of the Frobenius automorphism of so-called Koblitz elliptic curves, and also by powers of τ.

In another direction, number systems with only nonzero digits were proposed as a means to avoid Side Channel Attacks on elliptic curve cryptosystems. This leads to the natural question whether the known results for number systems continue to hold if we do not assume $0 \in \mathcal{D}$.

The assumption $0 \notin \mathcal{D}$ implies that there exists a special expansion for 0, which we call the zero expansion of the pre-number system. As an example, with base -2 and digits $\{1, 2\}$, we have
$$0 = 2 \cdot (-2)^0 + 1 \cdot (-2)^1.$$
The length of this expansion (2 in the example) becomes an important parameter of the pre-number system.

General structure questions

Together with Ryotaro Okazaki, we have shown the following result, which means that the presence of a number system on a group V is a quite severe restriction on its structure.

Theorem 1. *Suppose V is an abelian group supporting a number system, i.e., suppose there exists some endomorphism ϕ of V and some digit set $\mathcal{D} \subset V$ such that $(V, \phi, \mathcal{D})$ is a number system. Then:*

1. *the torsion of V is a direct summand of V and is a bounded group;*
2. *the torsion-free rank of V is finite;*
3. *the torsion-free quotient of V can be p-divisible for only finitely many primes p.*

This does not mean that every number system automatically splits into a torsion and a non-torsion part; this depends on the structure of the digit set, whereas also the torsion-free summands of V need not be invariant under the endomorphism ϕ.

These results are to be submitted soon.

Existence results

As a partial converse to the above theorem and in generalisation of previous results, we have

Theorem 2. *Let V be finite-dimensional $\mathbb{Z}$-lattice. Suppose $(V, \phi, \mathcal{D})$ is a pre-number system such that all eigenvalues α of ϕ satisfy $|\alpha| > 2$. Let $\| \cdot \|$ be a norm on V such that we have $\|\phi^{-1}\| < \frac{1}{2}$ for the induced operator norm, and suppose that every $d \in \mathcal{D}$ has minimal norm in its coset modulo $\phi(V)$. Then $(V, \phi, \mathcal{D})$ is a number system.*
Furthermore, the same result holds if every d is a smallest nonzero element in its coset.

If $\mathcal{D}$ satisfies the hypotheses, it is called a set of shortest (nonzero) digits.
It is not known if this result is optimal. To investigate this matter, we project to show that if V has dimension 2 and ϕ is expanding with at least one eigenvalue between 1 and 2 in absolute value, there exists some valid digit set as well.

In cooperation with Okazaki, we are working to make this result work for more general groups V.

Relation with Chinese Remainder Theorem

In the case where V is a lattice, obviously the classification of number systems depends on a suitable classification of lattices-with-endomorphism. However, such a classification is far from complete. For example, it is clear that if V has an endomorphism ϕ, then V becomes a module over the subring $R = \mathbb{Z}[\phi]$ of its endomorphism ring. This subring is commutative, and it is in fact isomorphic to $\mathbb{Z}[X]/(f)$, where f is the minimal polynomial of ϕ.
Now if f is squarefree, the Jordan-Zassenhaus theorem tells us that there are only finitely many indecomposable R-modules that are $\mathbb{Z}$-torsion-free, up to isomorphism. On the other hand,if f has square factors, there are examples that show that R may have infinitely many non-isomorphic indecomposable modules over it.
If we assume that the minimal polynomial f is equal to the characteristic polynomial of f, then it is easy to show that V is isomorphic to an ideal of R. To avoid unnecessary complications, for the time being we restrict ourselves to this case.
Then, a natural question is whether we can reduce to the case where f is irreducible. Unfortunately, this is in general impossible, as the next result shows (the second condition may be impossible to satisfy).

Theorem 3. *For $i = 1, 2$, let $f_i \in \mathbb{Z}[X]$ be coprime, monic and expanding, let $(V_i, X, \mathcal{D}_i)$ be a pre-number system, where V_i is a full-rank ideal of $\mathbb{Z}[X]/(f_i)$, let L_i be the length of the zero expansion of this number system. Let ψ be defined by*
$$\psi : \mathbb{Z}[X]/(f_1 f_2) \to \mathbb{Z}[X]/(f_1) \times \mathbb{Z}[X]/(f_2) : a \mapsto (a \bmod f_1, a \bmod f_2).$$
Let $R_{12} = \mathbb{Z}[X]/(f_1, f_2)$, and define the sequence $(S_i)_{i \geq 0} \subseteq R_{12}$ by $s_i = \sum_{j=0}^{i} X^j$. Because R_{12} is finite, the sequence (s_i) is periodic; we let S be the period length. Then
$$\left(\psi^{-1}(V_1 \times_{R_{12}} V_2), X, \psi^{-1}(\mathcal{D}_1 \times \mathcal{D}_2)\right)$$
is a number system if and only if the following conditions are satisfied:

(i) *$(V_1, X, \mathcal{D}_1)$ and $(V_2, X, \mathcal{D}_2)$ are actually number systems;*
(ii) *all digits in $\mathcal{D}_1 \cup \mathcal{D}_2$ are pairwise congruent modulo (f_1, f_2), and*
(iii) *we have $\gcd(L_1, L_2) = S$.*

A paper containing a proof of this result will be submitted soon.

Classification results

We have obtained some results towards the classification problem mentioned above. These first results are limited to the case $V = \mathbb{Z}$, where we may assume that the base is itself simply an integer, and have appeared as [8].

Theorem 4. *Let $b \in \mathbb{Z}$ with $|b| \geq 2$.*

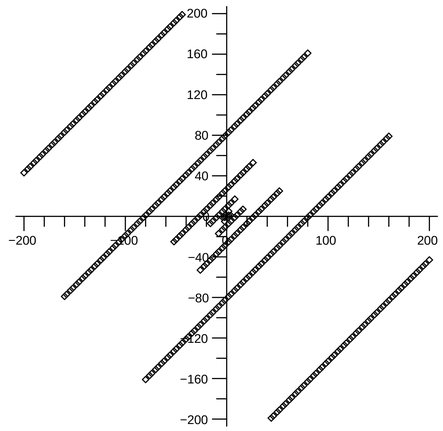
(i) *If $b = 2$, there are no valid digit sets.*
(ii) *If $b = -2$, and $\mathcal{D} = \{d, D\}$ is a digit set with $d < D$, then $\{d, D\}$ is valid if and only if*
  a) one of $\{d, D\}$ is even and one is odd;
  b) neither d nor D is divisible by 3, except that the even digit can be 0;
  c) we have $2d \leq D$ and $2D \geq d$;
  d) $D - d = 3^i$ for some $i \geq 0$.
(iii) *If $b = \pm 3$, then there exist infinitely many valid digit sets containing 0.*
(iv) *If $|b| \geq 4$, then there exist infinitely many valid digit sets both with and without 0.*

Here (iii) is taken from [6], whereas (iv) is a generalisation of [5].
We hope to extend the result for $|b| = 2$ to higher dimensions, subject to the condition that V is an ideal of $\mathbb{Z}[X]/(f)$, as mentioned above.

Digit sets for -2

On the right, we show the collection of all valid digit sets $\{d_0, d_1\}$ in $V = \mathbb{Z}$ for basis -2, with $0 \leq |d_0|, |d_1| \leq 200$. The exponential structure, which doubles itself every time, is clearly visible.

In general, we conjecture that in every binary number system on a lattice, the difference of the digits is made up only of prime factors that divide $\alpha - 1$, if the basis is α. Here we allow finitely many exceptions where the difference of the digits is small.
A binary number system is one that needs just two digits, i.e., $|V/\phi(V)| = 2$.



References

[1] G. Barat, V. Berthé, P. Liardet, and J. Thuswaldner. Dynamical directions in numeration. *Ann. Inst. Fourier (Grenoble)*, 56(7):1987–2092, 2006.

[2] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, editors. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications. Chapman & Hall/CRC, Boca Raton, FL, 2006.

[3] W. J. Gilbert. Radix representations of quadratic fields. *J. Math. Anal. Appl.*, 83(1):264–274, 1981.

[4] A. Kovács. *Radix expansion in lattices*. PhD thesis, Eötvös Loránd University, Budapest, 2001.

[5] B. Kovács and A. Pethő. Canonical systems in the ring of integers. *Publ. Math. Debrecen*, 30(1-2):39–45, 1983.

[6] D. W. Matula. Basic digit sets for radix representation. *J. Assoc. Comput. Mach.*, 29(4):1131–1143, 1982.

[7] W. Steiner and J. M. Thuswaldner. Rational self-affine tiles (preprint). Submitted, 2011.

[8] C. E. van de Woestijne. Noncanonical number systems in the integers. *J. Num. Th.*, 128:2914–2938, 2008.

[9] A. Vince. Replicating tessellations. *SIAM J. Discrete Math.*, 6(3):501–521, 1993.

Leoben, June 2012.