Digital expansions in abelian groups

CHRISTIAAN VAN DE WOSTIJNE
Montanuniversitat Leoben, Austria
e-mail: 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 \( \phi \) be an endomorphism of \( V \), that is, a homomorphism \( \phi : V \to V \),
- which we call the base.
- We assume that the image of \( \phi \) has finite index \( D \) in \( V \). In particular, in case \( V \) is a finite-dimensional \( \mathbb{Z} \)-lattice, we have \( \phi - \mathbb{Z} \nsubseteq D \).
- Let \( D \) 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 \((V,\phi,D)\) as above is a number system if every \( v \in V \) has a finite expansion of the form

\[
\sum_{n \in \mathbb{Z}} a_n \phi^n(v) \quad \text{with the } a_n \in D.
\]

This definition was given for the case where \( V \) is a finite free \( \mathbb{Z} \)-module in [8], among others, in the context of explicating tilings of \( \mathbb{R}^n \), and also in [3]. Many previous authors required that \( 0 \notin D \). We do not require this.

If we choose a basis for \( V \), then we may assume that \( V = \mathbb{Z}^2 \), and \( \phi \) is given by a non-singular \( \times 2 \) matrix with integer coefficients.

Basic problems

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

Examples and motivation

- The base example is \( V = \mathbb{Z} \), with \( \phi \) the map \( v \mapsto 2v \) for a fixed \( b \neq 0 \), and \( D = \{ 0, 1, \ldots, b - 1 \} \).
- For \( b \geq 1 \), this gives the usual base-\( b \) representation of the non-negative 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 Grassmann.

- Complete bases of the form \( a + b \mathbb{Z} \), where \( a, b \in \mathbb{Z} \), were already considered by Knuth. The digit set was taken to be \( \{ 0, 1, \ldots, b - 1 \} \), and it was shown that \( V \) is a number system if and only if the base has the form \( \mathbb{Z} \), \( a = 0 \), or \( b \leq 2 \). Later, this result was generalized for arbitrary quadratic numbers [3].

- Let \( \phi \) be an algebraic integer, with minimal polynomial \( f = \sum_{n=0}^s a_n x^n \) in \( \mathbb{Z}[x] \). Then \( V = \mathbb{Z}[\phi] \cong \mathbb{Z}[1/\phi] \), and \( f \) is a multiplicative norm on \( V \). It is easy to see that \( D = \{ 0, 1, \ldots, (b - 1)/[\phi] \} \) represents \( V/\phi(V) \).

This is a pre-number system. If every \( v \in \mathbb{Z}[\phi] \) has a representation of the form \( \sum_{n \in \mathbb{Z}} a_n \phi^n(v) \), the resulting number system is called a canonical number system (CNS), because the digits are canonically chosen. A survey of CNSs is given in [6].

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 [6, Chapter III]. An important role is played by the base \( b = \sum_{n \in \mathbb{Z}} a_n \phi^n \), where \( a_n \) is an integer that satisfies the same minimal polynomial of the Frobenius automorphism of so-called Koblitz elliptic curves, and also by powers of \( \phi \).

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 \( 0 \notin D \).

The assumption \( 0 \notin D \) 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

\[
0 = 2 \cdot (-2^0 + 1 + 2^2).
\]

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

References