Canonical number systems and algebraic number theory

Christiaan van de Woestijne
Lehrstuhl für Mathematik und Statistik
Montanuniversität Leoben, Austria

Supported by the FWF, project S9611

Workshop on Digital expansions, Dynamics and Tilings
Aussois, 4-11 April 2010

Abstract

Let A be a square integer matrix of determinant ± 2, and assume A is expanding, that is, all its eigenvalues are greater than 1 in absolute value. Let $\{d, D\}$ be integer vectors such that d is in the image of A and D is not. If every integer vector v has a representation of the form

$$v = d_0 + Ad_1 + A2d_2 + \ldots + A^k d_k$$

with the d_i being either d or D, we call the triple $(A, \mathbb{Z}^n, \{d, D\})$ a number system.

Our goal, which will not be achieved in this talk, is to classify all such number systems with two digits, which generalise the well-known binary number system. We will show the technical obstacles for such a classification and also give some partial results, such as a complete classification in the 1-dimensional case.

Enumerating expanding polynomials (1)

Let $f = a_n X^n + \ldots + a_1 X + a_0 \in \mathbb{Z}[X]$. For given a_n and a_0, the number of expanding f is finite. But how to find them?

Lemma If f is expanding, then $|a_i| < |a_0|\binom{n-1}{n-i+1} + |a_n|\binom{n-1}{n-i}$.

Proof. These are the coefficients of $(X+1)^{n-1}(a_n X + a_0)$, which is an extremal point of the space of expanding polynomials.

Let s_i $(1 \le i \le n)$ denote the elementary symmetric functions of the roots of f; we have $a_{n-i} = (-1)^i a_n s_i$. Also, let σ_i be the sum of ith powers of the roots.

Lemma. $|\sigma_i| < n - 1 + |a_0/a_n|^i$.

Enumerating expanding polynomials (2)

By Newton's theorem,

$$\sigma_i = P(s_1, \ldots, s_{i-1}) - (-1)^i \cdot i \cdot s_i$$

for some $P \in \mathbb{Z}[X_1, \ldots, X_{i-1}]$. Now assume that $a_{n-1}, \ldots, a_{n-i+1}$ are already known. We obtain an interval for a_{n-i} as follows.

Lemma (Browkin/CvdW)

$$\left| \frac{a_{n-i}}{a_n} - \frac{P(s_1, \ldots, s_{i-1})}{i} \right| < \frac{n - 1 + |a_0/a_n|^i}{i}.$$

Next, we use the Schur-Cohn criterion for expansiveness.

Lemma f is expanding if and only if $\Delta_i(f) > 0$ for $i = 1, \ldots, n$.

The Schur-Cohn determinants (1)

Here the Δ_i are subdeterminants of the Sylvester matrix of f and its reciprocal polynomial f^* (actually, of f^* and f), which has size $2n \times 2n$:

$$\begin{bmatrix} a_n & a_{n-1} & \dots & a_0 & & \\ & a_n & \dots & a_1 & a_0 & \\ & & \dots & & \dots & \\ & & a_n & a_{n-1} & \dots & a_0 \\ a_0 & a_1 & \dots & a_n & & \\ & a_0 & \dots & a_{n-1} & a_n & \\ & & \dots & & \dots & \\ & & a_0 & a_1 & \dots & a_n \end{bmatrix}$$

For Δ_i, take columns and rows $1, \dots, i$ and $n+1, \dots, n+i$.

We note that Δ_i is a homogeneous polynomial in the a_i of degree $2i$, and contains terms a_n^{2i} and a_0^{2i}. We have $\Delta_1 = a_0^2 - a_n^2$.

The Schur-Cohn determinants (2)

Theorem For all i, $\Delta_i = \Delta_i^+ \Delta_i^-$ with Δ_i^+ and Δ_i^- of degree i. For $i = 0, \ldots, \lceil n/2 \rceil - 1$, we have

$$\Delta_{i+1} = (a_0 \Delta_{i-1}^- a_i - a_n \Delta_{i-1}^- a_{n-i} + P) \times \\ (-a_0 \Delta_{i-1}^+ a_i + a_n \Delta_{i-1}^+ a_{n-i} + R),$$

where P and R are homogeneous in $a_0, \ldots, a_{i-1}, a_{n-i+1}, \ldots, a_n$ of degree i. It follows that, given a_i, and assuming $\Delta_k(f) > 0$ for $k = 1, \ldots, i$, we obtain an interval for a_{n-i}, with bounds that are linear in a_0 and a_n.

For n even, we also obtain an interval for $a_{n/2}$ in terms of all the other coefficients, with bounds that are quadratic in a_0 and a_n.

Finally, one can prove that

$$\Delta_n = \mathrm{Res}(f^*, f) = (\Delta_{n-1}^-)^2 f(1) f(-1),$$

which again gives linear inequalities on the a_i.

Enumerating expanding polynomials (3)

We now use the following enumeration algorithm. Let

$$f = X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + 2.$$

Then:

1: use the interval $a_{n-1} \in [-n..n]$.

2: use Δ_2 to find an interval for a_1.

3: use the Browkin lemma to bound a_{n-2} in terms of a_{n-1}.

4: use Δ_3 to bound a_2.

5: and so on...

Here, at all points we check whether the bounds from the first Lemma still hold. Now, for all f within this region:

6: check whether $f(1)$ and $f(-1)$ have the same sign.

7: check whether $\Delta_{\lceil n/2 \rceil}(f), \ldots, \Delta_{n-1}(f)$ are positive.

Results and timings

The algorithm was implemented in Magma 2.16 and run for degree ≤ 10 on an Athlon 64 X2 Dual Core 3800+ CPU. We list the time used (t), amount of tests done (d), and number of remaining polynomials (r):

n	3	4	5	6	7	8	9	10
t	0.01	0.01	0.06	0.38	$4.89s$	$26.47s$	$8m18s$	$59m29s$
d	35	92	1165	3549	58459	159421	3532745	7877246
r	7	21	29	71	95	201	192	408

For r, we choose one polynomial from each orbit $\{f(x), f(-x)\}$. For odd degree, this means taking $f(0) = 2$. For even degree, we may have $f(0) = -2$, but we require the highest odd-degree nonzero term to be positive.

For degree 10, the precomputation of the Δ_i as polynomials in $a_1, \ldots, a_9$ and factoring them takes about $32m$ time and 300Mb of memory, taking into account that Δ_{10} is already known.

Enumerating Pisot polynomials (1)

The algorithm can be applied to enumerate all Pisot polynomials of given degree and given constant coefficient (unequal to ± 1, unfortunately).

Following Akiyama-Gjini (2005), let $f = X^n + a_{n-1}X^{n-1} + a_1 X + a_0$ be a Pisot polynomial. Then putting $Tf = a_0 f - a_n f^*$, with f^* the reciprocal, we find

$$Tf = \sum_{i=1}^{n-1} (a_0 a_i - a_n a_{n-i}) X^i + (a_0^2 - 1).$$

Because $a_0^2 - 1 \neq 0$, it follows from the Schur-Cohn theory that $(Tf)^*$ is an expanding polynomial of degree $n-1$ and leading coefficient $a_0^2 - 1$.

Enumerating Pisot polynomials (2)

Lemma Let $a_0 \in \mathbb{Z}$ with $|a_0| \geq 2$, and let

$$g = (a_0^2 - 1)X^{n-1} + b_{n-2}X^{n-2} + \ldots + b_1 X + b_0$$

be expanding, and such that $b_i \equiv -a_0 b_{n-i} \pmod{a_0^2 - 1}$ for all $i \geq 1$. Then there exists exactly one Pisot polynomial f as above with $Tf = g$.

It is easy to incorporate the above congruences into the algorithm. Thus running the algorithm for constant coefficient $a_0^2, a_0^2 + 1, \ldots$ and their negatives, we must obtain all Pisot polynomials f of degree n and with $f(0) = a_0$.

Definitions

We define a pre-number system as a triple $(V, \phi, \mathcal{D})$, where

- V is a finite free $\mathbb{Z}$-module;
- ϕ is an expanding endomorphism of V;
- $\mathcal{D}$ is a system of representatives of V modulo $\phi(V)$.

A pre-number system $(V, \phi, \mathcal{D})$ is a number system if there exist finite expansions

$$a = \sum_{i=0}^{\ell} \phi^i(d_i) \qquad (d_i \in \mathcal{D})$$

for all $a \in V$.

We are ultimately interested in the classification of all number systems.

Examples

- $(\mathbb{Z}, b, \{0, \ldots, |b|-1\})$ is a pre-number system whenever $|b| \geq 2$, and a number system if and only if $b \leq -2$.
- $(\mathbb{Z}[i], b, \{0, \ldots, |b|^2-1\})$ is a pre-number system whenever $|b| > 1$, and a number system if and only if $b = -a \pm \mathrm{i}$, for some $a \in \mathbb{N}$.
- $(\mathbb{Z}, -2, \{d, D\})$ is a number system if and only if ... (see later)
- $(\mathbb{Z}[X]/((X-5)(X-7)), X, \{1, -1, 3, -3, 5, X, X-2, -X+2, X-4, -X+4, X-6, -X+6, X-8, -X+8, -X+10, 2X-7, 2X-9, -2X+9, 2X-11, -2X+11, 2X-13, -2X+13, -2X+15, 3X-14, 3X-16, -3X+16, -3X+18, 3X-18, -3X+20, 4X-21, 4X-23, -4X+23, -4X+25, 5X-28, -5X+30\})$ is a number system

Example: the odd digits

Assume $V = \mathbb{Z}$ and ϕ is multiplication by some integer b. Let b be odd, $|b| \geq 3$, and let

$$\mathcal{D}_{\text{odd}} := \{-|b| + 2, -|b| + 4, \ldots, -1, 1, \ldots, |b| - 2, b\}.$$

This is a valid digit set for all odd b.

For $b = 3$: it's $\{-1, 1, 3\}$. We get $0 = 3 \cdot 1 + (-1) \cdot 3$.

a	$(a)_{3,\text{odd}}$	a	$(a)_{3,\text{odd}}$	a	$(a)_{3,\text{odd}}$	a	$(a)_{3,\text{odd}}$
0	$\overline{1}3$	5	$1\overline{1}\overline{1}$	-1	$\overline{1}$	-6	$\overline{1}133$
1	1	6	13	-2	$\overline{1}1$	-7	$\overline{1}1\overline{1}$
2	$1\overline{1}$	7	$1\overline{1}1$	-3	$\overline{1}13$	-8	$\overline{1}131$
3	3	8	$3\overline{1}$	-4	$\overline{1}\overline{1}$	-9	$\overline{1}\overline{1}3$
4	11	9	$1\overline{1}3$	-5	$\overline{1}11$	-10	$\overline{1}13\overline{1}$

The dynamic mapping

Define functions

$$d : V \to \mathcal{D} : d(a) \text{ is the unique } d \in \mathcal{D} \text{ with } a - d \in \phi(V);$$
$$T : V \to V : T(a) = \phi^{-1}(a - d(a)).$$

We call T the dynamic mapping of $(V, \phi, \mathcal{D})$.

Theorem $(V, \phi, \mathcal{D})$ is a number system if and only for all $v \in V$ there exists $n \geq 0$ with $T^n(v) = 0$.

Recall that a pre-number system has a finite attractor $\mathcal{A} \subseteq V$ with the properties

- for all $a \in V$ we have $T^n(a) \in \mathcal{A}$ if n is large enough.
- T is bijective on $\mathcal{A}$.

Theorem $(V, \phi, \mathcal{D})$ is a number system if and only if the attractor contains 0, and consists exactly of one cycle under T.

Tiles and translation

The tile of the pre-number system $(V, \phi, \mathcal{D})$ is

$$\mathcal{T} = \left\{ \sum_{i=1}^{\infty} \phi^{-i}(d_i) : d_i \in \mathcal{D} \right\}.$$

By results of Lagarias and Wang (building on earlier authors), $\mathcal{T}$ is a compact set of positive measure that is the closure of its interior. Let Λ be the $\mathbb{Z}[\phi]$-submodule of V generated by $\mathcal{D} - \mathcal{D}$, the differences of the digits; then we can tile $V \otimes \mathbb{R}$ with $\mathcal{T}$ by a sublattice M of Λ, and we have

$$\mu(\mathcal{T}) = [V : M] = [\Lambda : M] \cdot [V : \Lambda].$$

If the characteristic polynomial of ϕ is irreducible, then we may take $\Lambda = M$.

One can prove that the attractor $\mathcal{A}$ is equal to $-\mathcal{T} \cap V$.

Binary number systems

Suppose $|\det(\phi)| = 2$; then there are exactly 2 digits, and we speak of a binary (pre-)number system. There are many special properties:

- The tile is connected
- The characteristic polynomial χ_ϕ is irreducible
- The tiling lattice is generated by one element

We may assume V is an ideal in $R = \mathbb{Z}[\alpha]$, where α is a zero of $f = \chi_\phi$.

Write $\mathcal{D} = \{d, D\}$ with d divisible by α in V and D not, and let

$$\delta = d - D.$$

Then the tiling lattice is the ideal generated by δ, and $\mu(\mathcal{T}) = |\operatorname{Norm}(\delta)|$.

The goal

We want to classify all binary number systems, that is, for all algebraic integers α of norm ± 2 and all ideals $V \subseteq \mathbb{Z}[\alpha]$, find all pairs $\{d, D\}$ such that $(V, \alpha, \{d, D\})$ is a number system.

To do this, we have three tasks:

1. compute and/or characterise all such α and all such ideals V;
2. for all possible δ, compute how many elements are in $\mathcal{A}$;
3. find their cycle structure under the dynamic map T.

Note that if all points of $\mathcal{A}$ are interior points of $-\mathcal{T}$, then $|\mathcal{A}| = |\,\mathrm{Norm}(\delta)|$, since only boundary points can be in more than one tile translate.

Note also that when $\alpha - 1$ is a unit, then $d/(\alpha - 1)$ and $D/(\alpha - 1)$ both start 1-cycles in $\mathcal{A}$, so α is not the base of any number system.

Order structure (1)

We notice that if V_1 and V_2 are isomorphic as $\mathbb{Z}[\phi]$-modules, then they carry the same number systems. For the binary case, for a given α, this means we need only consider one representative from each ideal class of $\mathbb{Z}[\alpha]$.

Thus we need an algorithm to compute the ideal class semigroup of $\mathbb{Z}[\alpha]$. The ideal class group is not enough!

Unfortunately, there is no algorithm known to compute the representatives of the class semigroup of nonmaximal orders. It is not even true that all singular ideal classes of such orders belong to an overorder; this is equivalent to the order being Cohen-Macaulay (H.W.Lenstra, pers.comm.).

See also Lagarias-Wang (1996 and corrigendum/addendum 1999) for some small examples.

Order structure (2)

Among all computed expanding polynomials f, fortunately there are many examples where $\mathbb{Z}[X]/(f)$ is a maximal order with trivial class group, so we need only consider $\mathbb{Z}[\alpha]$ itself.

In degree 4, we find that the equation order $x^4 + x^2 + 2$ has conductor 2.

In degree 6, there are 2 examples with conductor 2, one with 3 and one with 4.

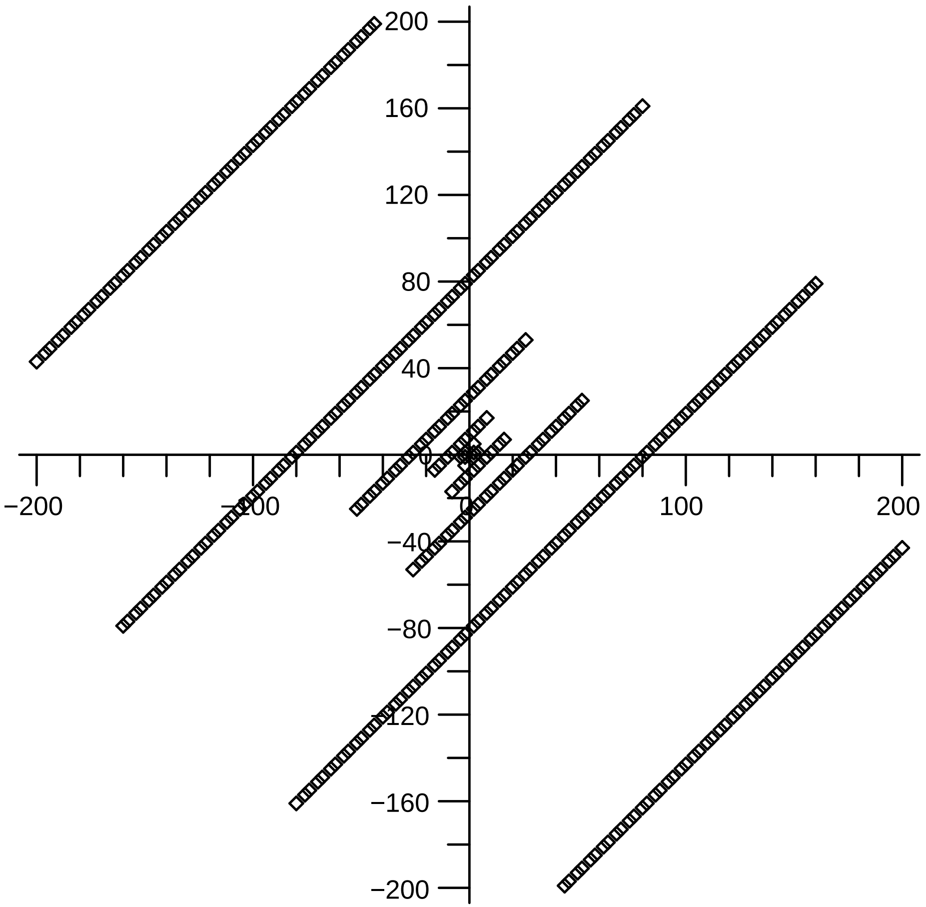
In degree 7, there is one example of conductor 2 and one with 5.

In degree 8, we find that $x^8 - x^6 - x^2 + 2$ has class group $C(2)$, which answers a question of Browkin. Several others have conductor up to 8 or 9.

In degree 10, we find conductors 5, 9, 11 and 16, and some class groups of $C(2)$.

Example: the case $V = \mathbb{Z}$

Let $V = \mathbb{Z}$; then $\alpha = \pm 2$. If $\alpha = 2$, then $\alpha - 1$ is a unit.



In the figure, we see all valid digit sets for $\alpha = -2$ with both digits less than 200 in absolute value.

What is the structure of this set?

The fundamental lemma

We are interested in the cycles in V under the dynamic map T. Now $a_0 \in V$ starts a cycle of length ℓ if and only if

$$a_0(1-\alpha^\ell) = \sum_{i=0}^{\ell-1} d_i \alpha^i.$$

Now because the only digits are d and $d-\delta$, this means

$$a_0(1-\alpha^\ell) = d\frac{\alpha^\ell - 1}{\alpha - 1} - \delta \sum_{i=0}^{\ell-1} \varepsilon_i \alpha^i,$$

so that

$$(d+(\alpha-1)a_0)\frac{\alpha^\ell - 1}{(\alpha-1)\delta} = \sum_{i=0}^{\ell-1} \varepsilon_i \alpha^i,$$

with $\varepsilon_i = 0, 1$ for all i.

This is our fundamental tool to study the cycle structure.

Algebraic number theory

Theorem Suppose $\delta = \prod \pi_i^{h_i}$, where the π_i are regular totally split primes of $\mathbb{Z}[\alpha]$ dividing $\alpha - 1$ lying above distinct primes of $\mathbb{Z}$, and such that π_i divides $\alpha + 1$ exactly once if π_i lies above 2. Then

$$(\alpha - 1)\delta \text{ divides } \alpha^\ell - 1$$

if and only if $\mathrm{Norm}(\delta)$ divides ℓ.

Conversely, if the order of α modulo $(\alpha - 1)\delta$ is $|\,\mathrm{Norm}(\delta)|$, and δ is made up of regular primes, then up to a factor of bounded norm, δ is as described above.

I do not know if it is necessary for α to have order $|\,\mathrm{Norm}(\delta)|$ for δ large enough, in order to have a number system, but my examples lead me to conjecture that it is.

Sketch of proof

Suppose δ has the right form. Let π^h exactly divide δ. As π divides $\alpha - 1$, the order of α modulo π^g is 1, where $g = v_\pi(\alpha - 1)$. If π is regular and unramified and lies above p, then

$$\pi^{g+i} \parallel \alpha^{p^i} - 1.$$

Thus if also π has residue degree 1, we have $\mathrm{Norm}(\pi) = p$ and

$$\alpha^{|\,\mathrm{Norm}(\pi^h)|} \equiv 1 \pmod{(\alpha - 1)\pi^h},$$

where the exponent is minimal with this property.

Combining divisors of δ, the order of α modulo $\prod \pi_i^{h_i}$ is the l.c.m. of those modulo the $\pi_i^{h_i}$.

If π lies over p with ramification index e and residue class degree f, then the order of α modulo $(\alpha - 1)\pi^h$ is roughly $p^{h/e}$, whereas the norm of π^h is p^{fh}. Thus, we want $e = f = 1$.

Points in the tile

Given δ, first compute the order ℓ of α modulo $(\alpha - 1)\delta$. Then, we know that the length of every cycle in $\mathcal{A}$ is divisible by ℓ. Thus, ℓ divides $|\mathcal{A}| = |\mathcal{T} \cap V|$. Note that $\ell = 1$ if and only if δ is a unit.

If we embed $\mathbb{Z}[\alpha]$ into $\mathbb{R}^n$ using the canonical embedding, then $\mathcal{T}$ is congruent under translation to the tile corresponding to the digit set $\{0, 1\}$ multiplied by δ.

"Theorem" If δ is expanding and satisfies $\ell = |\text{Norm}(\delta)|$ and if ℓ is large enough, then $|\mathcal{A}| = \ell$. Equivalently, then all lattice points of $\mathcal{T}$ are interior.

If the statement is false, we can have huge numbers of lattice points on the tile boundary. Note that this is difficult when δ is not expanding.

Examples: factorisation of $\alpha - 1$

If $\alpha = 2$, then $\alpha - 1 = 1$, a unit. If $\alpha = -2$, then $\alpha - 1 = -3$, so the only prime dividing $\alpha - 1$ is 3.

If $f = x^4 + x + 2$, then $\alpha - 1 = (\alpha + 1)^2$, where $\alpha + 1$ is a totally split prime lying over 2. This implies that for $f = x^4 - x + 2$, we have $\alpha + 1 \sim (\alpha - 1)^2$!

If $f = x^4 + x^3 + 2x^2 + x + 2$, then $\alpha - 1$ is a totally split prime lying over 7. However, if $\{d, D\} = \{\alpha, 1\}$, $\mathcal{A}$ consists of a cycle of length 14, with elements pairwise congruent modulo $\alpha - 1$. If $\{d, D\} = \{\alpha^2 - 2, 2\alpha - 3\}$, we have $\delta = (\alpha - 1)^2$ and, indeed, $\mathcal{A}$ has one cycle of length 49.

If $f = x^4 + x^2 + x + 2$, then for $\{d, D\} = \{0, 1\}$, we have an 11-cycle! For digits $\{\alpha, 1\}$, we have two 5-cycles, one containing 0 and the other $\alpha - 1$. For digits $\{\alpha^2 + 2\alpha + 2, 1\}$, with $\delta = (\alpha - 1)^2$, we find a unique cycle of length 25.

Examples: factorisation of $\alpha - 1$ (2)

Among all expanding $f \in \mathbb{Z}[x]$ with degree at most 8 and $|f(0)| = 2$, the only prime divisors of $\alpha - 1$ with residue degree more than 1 are non-regular.

However, many primes are ramified. For example, for $f = x^5 - x + 2$, $\alpha - 1$ lies over 2 with ramification index 4! We find, for example, that $\alpha^8 - 1$ is divisible by $(\alpha - 1)^9$, which has norm 2^9, whereas we would like to have only 3 factors, with norm 8.

An interesting case is $f = x^2 + x + 2$, with root $\tau = \frac{-1+\sqrt{-7}}{2}$, which is much used in cryptography. Here, $\tau - 1 = (\tau + 1)^2$, and $\tau + 1$ is a regular prime of norm 2. Thus, all conditions on τ are met.

Indeed, I have computed all valid digit sets for base τ of the form $\{a + b\tau, c + d\tau + 1\}$ with $a, b, c, d \in \{-4, \ldots, 4\}$, and it turns out that for all of them, δ is a power of $\tau + 1$. All attractors have the "right" number of elements, except when δ is a unit and $dD \neq 0$; in those cases, $|\mathcal{A}| = 3$.

Example: the case $V = \mathbb{Z}$ (2)

Let $\alpha = -2$, let $\delta \in \mathbb{Z}$ odd with $|\delta| > 1$; let $d, D \in \mathbb{Z}$ with $2 \mid d$ and $D = d - \delta$. We have:

1. $|\mathcal{A}| = |\delta|$ iff $3 \nmid dD$;
2. if $3 \nmid dD$, then $\mathcal{A}$ has one cycle if and only if $|\delta| = 3^i$ with $i \geq 1$; if $3 \mid dD$, then $\mathcal{A}$ has more than one cycle;
3. there is an easy criterion to see whether $0 \in \mathcal{A}$.

In fact, the only connected subsets of $\mathbb{R}$ are intervals, so $\mathcal{T}$ must be an interval.

If $|\delta| = 1$, then the only valid $\{d, D\}$ are $\{0, \pm 1\}$, $\{1, 2\}$ and $\{-1, -2\}$. For the latter, $\mathcal{T}$ has only boundary lattice points.

Main theorem

Let α be an expanding algebraic integer of norm ± 2, and suppose $\delta = \prod \pi_i^{h_i}$ where the π_i are regular totally split primes of $\mathbb{Z}[\alpha]$ dividing $\alpha - 1$ and lying above distinct primes of $\mathbb{Z}$, and such that π_i exactly divides $\alpha + 1$ if π_i lies above 2.

Let $d, D \in \mathbb{Z}[\alpha]$ have $d - D = \delta$, let $V = (d, D)$, and suppose that $d \in \alpha V$ (so that $D \notin \alpha V$, because α is prime).

Let $\mathcal{T}$ be the tile of $(V, \alpha, \{d, D\})$, and suppose $\mathcal{T} \cap V$ consists of interior points of $\mathcal{T}$, and that $0 \in \mathcal{T}$.

Then $(V, \alpha, \{d, D\})$ is a number system.

I conjecture that the converse holds: if Norm(δ) is large enough, and $(V, \alpha, \{d, D\})$ is a number system, then δ has the form given above and all points of $\mathcal{T} \cap V$ are interior.

Example: the case $V = \mathbb{Z}$ (3)

Theorem Let $d, D \in \mathbb{Z}$, with $d < D$. Then $(\mathbb{Z}, -2, \{d, D\})$ is a number system if and only if

1. one of $\{d, D\}$ is even and one is odd;
2. neither of d and D is divisible by 3, except when the even digit is 0;
3. we have $2d \leq D$ and $2D \geq d$;
4. $D - d = 3^i$ for some $i \geq 0$.

Example Thus, $\{1, 3^k + 1\}$ is valid for $b = -2$, for all $k \geq 0$.

The only valid digit sets for $b = -2$ that have 0 are $\{0, 1\}$ and $\{0, -1\}$.