A second look at binary digits

Christiaan van de Woestijne

(Supported by FWF Project S9611)

Lehrstuhl für Mathematik und Statistik

Montanuniversität Leoben

Budapest, mathematical seminar
13 October 2010

Binary digits

Everybody knows that $(10)_2 = 2$ and $(11011)_2 = 27$.

Also, $-27 = (-11011)_2$. Or is it?

Some computers know that $-27 = (1111111111100101)$ (signed word), and that $32767 + 1 = -32768$.

Some people know that $-1 = (11111\ldots)_2 \in \mathbb{Z}_2$ (start with LSD here), and

$$-27 = (101001111\ldots)_2.$$

Can we do better?

The expansion algorithm

Define the dynamic mapping $T : \mathbb{Z} \to \mathbb{Z} : a \mapsto \begin{cases} \frac{a}{2} & \text{if } a \text{ even;} \\ \frac{a-1}{2} & \text{if } a \text{ odd.} \end{cases}$

Now to expand a, write 0 if a even and 1 otherwise, and continue with $T(a)$. Done when $T^n(a) = 0$.

Example: $27 \xrightarrow{1} 13 \xrightarrow{1} 6 \xrightarrow{0} 3 \xrightarrow{1} 1 \xrightarrow{1} 0$.

However, $-1 \xrightarrow{1} -1 \ldots$

Try other digits: $\mathcal{D} = \{d_0, d_1\}$, with $d_i \equiv i \pmod 2$.

Criterion for the existence of a 1-cycle: $\frac{a-d}{2} = a \Leftrightarrow a = -d$.
So this is hopeless!

Negabinary expansions

Try other basis -2, with digits $\{0, 1\}$:

$-27 \xrightarrow{1} 14 \xrightarrow{0} -7 \xrightarrow{1} 4 \xrightarrow{0} -2 \xrightarrow{0} 1 \xrightarrow{1} 0$, so $-27 = (100101)_{-2}$.

Theorem (Grünwald 1885) All integers have a finite expansion on the integer basis $b \leq -2$ and digits $\{0, 1, \ldots, |b| - 1\}$.

Proof: there are no cycles except $0 \xrightarrow{0} 0$!

Excursion: the balanced ternary expansion uses basis $+3$ and digits $\{-1, 0, 1\}$, and expands all integers finitely. If only computers had three-way switches!

Theorem Let $a \in \mathbb{Z}_3$. Then $a \in \mathbb{Z}$ if and only if its balanced ternary expansion is finite.

A curious question

Definition A digit set $\mathcal{D}$ is valid for basis ± 2 if all integers have a finite representation

$$\sum_{i=0}^{\ell} d_i(\pm 2)^i \quad (d_i \in \mathcal{D}).$$

We know that no digit sets are valid for basis $+2$; for basis -2, we know the valid digit set $\{0, 1\}$, and thus also $\{0, -1\}$ by an automorphism of the additive group.

Question Are there any others?

Answer Yes, infinitely many!

Expansions of zero

Is it possible to have a digit set without zero? Yes!

The definition of the mapping T and of the stopping criterion is the same (if you formulate it like I do!).

Example: basis -2, digits $\{1, 4\}$. Expand -27:

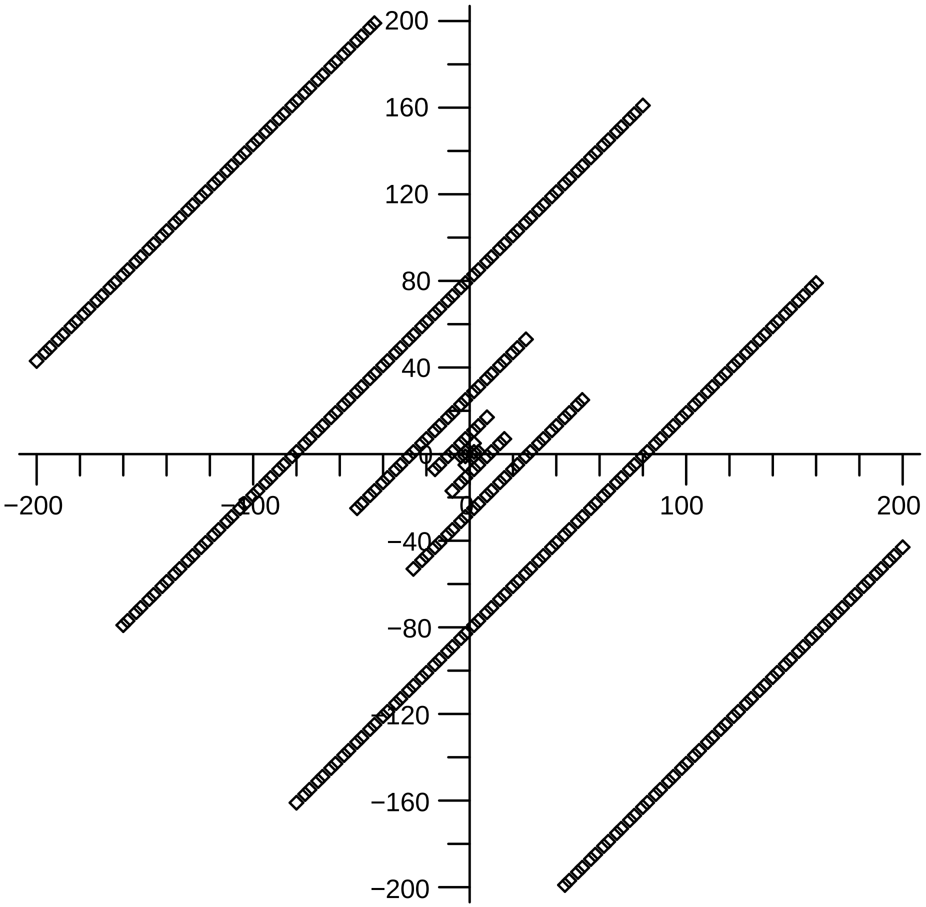
$-27 \xrightarrow{1} 14 \xrightarrow{4} -5 \xrightarrow{1} 3 \xrightarrow{1} -1 \xrightarrow{1} 1 \xrightarrow{1} 0$, so $-27 = (111141)_{-2}$.

Interesting: $0 \xrightarrow{4} 2 \xrightarrow{4} 1 \xrightarrow{1} 0$, a 3-cycle!

So, $0 = ()_{-2} = (144)_{-2} = (144144)_{-2} = \ldots$

Theorem Any valid digit set gives rise to a nontrivial expansion of zero.

Experiments



The figure plots all pairs of integers (x, y), with $|x|, |y| \leq 200$, that are valid digit sets for basis -2.

Results

Theorem (CvdW 2008) The digit set $\{d, D\}$ with $d < D$ is valid for basis -2 if and only if

(i) one of d, D is even and one is odd (trivial)

(ii) if $3 \mid dD$, then one of d, D is 0 and 3 does not divide the other (avoid 1-cycles except 0)

(iii) we have $2d \leq D$ and $2D \geq d$ (0 is expansible)

(iv) $D - d = 3^i$ for some $i \geq 0$ (the real stuff!)

For example, the only valid digit sets with 0 are $\{0, \pm 1\}$. On the other hand, the sets $\{1, 3^i + 1\}$ are valid for all $i \geq 0$.

Higher-dimensional analogues

There is no reason to limit the theory of number systems to $\mathbb{Z}$. Consider this setup:

- V is an abelian group.
- $\phi : V \to V$ is an endomorphism of V, with $[V : \phi(V)] < \infty$.
- $\mathcal{D}$ represents V modulo $\phi(V)$.

Then we can define $T : V \to V : a \mapsto \phi^{-1}(a - d_a)$, where $d_a \in \mathcal{D}$ has $a \equiv d_a \pmod{\phi(V)}$. We call $(V, \phi, \mathcal{D})$ a pre-number system, and additionally a number system when all elements of V are finitely expansible.

Theorem (Okazaki-CvdW) If $(V, \phi, \mathcal{D})$ is a number system, then V^{tor} is a direct summand of V and is bounded, and V/V^{tor} has finite rank.

Generalised binary systems

Here, we will consider generalised binary pre-number systems:

- α is an algebraic integer of norm ± 2.
- V is a fractional ideal of $\mathbb{Q}(\alpha)$.

If $V_2 = \beta V_1$ for some $\beta \in \mathbb{Q}(\alpha)$, then $(V_1, \alpha, \mathcal{D})$ and $(V_2, \alpha, \beta\mathcal{D})$ are isomorphic as pre-number systems.

Easy necessary conditions to have finite expansibility of all $a \in V$:

- α and $\alpha - 1$ must be non-units of $\mathbb{Z}[\alpha]$.
- α must be expanding: for all $\sigma : \mathbb{Z}[\alpha] \hookrightarrow \mathbb{C}$ we have $|\sigma(\alpha)| > 1$.

Note that any monic and expanding $f \in \mathbb{Z}[x]$ with $|f(0)|$ prime is automatically irreducible.

Expanding polynomials of given norm

On my website

`www.opt.math.tugraz.at/ cvdwoest/maths/expanding`

I collected some software and tables about enumeration of expanding and Pisot polynomials. Using a MAGMA implementation of ideas due to Schur, Dufresnoy-Pisot, Chamfy, and Kovács-Burcsi, I computed all monic expanding polynomials with integer coefficients and constant term ± 2 up to degree 20, as well as several cases with higher norm.

The computation for (e.g.) degree 13 and norm 2 takes less than 13 seconds on an Athlon.

The periodic set

Because α is expanding, the mapping T is almost a contraction on V, and the unique finite subset $\mathcal{P} \subset V$ that is invariant under T is called the periodic set of the pre-number system.

Lemma The periodic set of $(\mathbb{Z}, -2, \{d, D\})$ is the arithmetic progression $\left\{\left\lceil \frac{2d-D}{3} \right\rceil, \ldots, \left\lfloor \frac{2D-d}{3} \right\rfloor\right\}$.

In higher dimensions, the periodic set is usually quite irregular. Work of the Austro-Hungarian school has led to several (exponential) algorithms to compute the periodic set for any pre-number system.

Theorem $(V, \alpha, \mathcal{D})$ is a number system if and only if the action of T on $\mathcal{P}$ has exactly one cycle, which passes through 0.

The tile

There is a continuous variant of the (discrete) periodic set, called the tile of the pre-number system, because it usually tiles $V \otimes \mathbb{R}$.

For $(\mathbb{Z}, -2, \{d, D\})$, it is the interval $\left[\frac{2d-D}{3}, \frac{2D-d}{3}\right]$.

These tiles have the following properties:

- they are compact and the closure of their interior.
- they have fractal boundary.
- they may have infinitely many connected components, but they are connected when $|\mathcal{D}| = 2$.

To prove a higher-dimensional analogue of the main Theorem, we must characterise the lattice points in the tile, and describe the action of T on them.

Work in progress

More-or-less-theorem Let α be an expanding algebraic integer of norm ± 2. Then up to finitely many exceptions, a digit set $\mathcal{D} = \{d_0, d_0 + \delta\}$ makes $(\mathbb{Z}[\alpha], \alpha, \mathcal{D})$ into a number system if and only if:

(i) $(d_0, \alpha - 1) = (d_1, \alpha - 1) = (1)$

(ii) there is a nontrivial zero expansion

(iii) δ is a product of prime divisors of $\alpha - 1$ that are unramified, totally split and lie over different primes of $\mathbb{Z}$

Note that for a given degree d, there are only finitely many expanding α of degree d and norm ± 2. The smallest nonmaximal order among them is generated by $x^4 + x^2 + 4$ (Potiopa 1997). The smallest example with a nontrivial ideal class group is $x^8 - x^6 - x^2 + 2$ (CvdW 2009).

Technical assumptions

I need the following:

(i) $\alpha - 1$ is expanding;

(ii) the Hausdorff dimension of the tile is less than $\dim_{\mathbb{Z}} \mathbb{Z}[\alpha]$;

(iii) $\mathbb{Z}[\alpha]$ is a maximal order;

(iv) $(\mathbb{Z}[\alpha], \alpha, \{0, 1\})$ is a number system.

The last assumption says that the minimal polynomial of α is a CNS polynomial.

I hope to remove all of these assumptions.

Example

A famous example is $\tau = \frac{-1+\sqrt{-7}}{2}$ satisfying $x^2 + x + 2$. This basis has cryptographic significance because it can be used to speed up operations on Koblitz elliptic curves.

$x^2 + x + 2$ is a CNS polynomial, so (iv) is satisfied.

$\mathbb{Z}[\tau]$ is maximal, and $\tau - 1 = (\tau + 1)^2$, where $(\tau + 1)$ is an unramified prime of norm 2, and hence split.

All conjugates of τ have the same modulus, so the assumption on the Hausdorff dimension of the boundary follows from a theorem of Veerman.

So the Theorem holds for basis τ.

Experimental verification

This was verified experimentally for all pairs $\{a+b\tau, c+1+d\tau\}$ with $a, b, c, d \in \{-4, \ldots, 4\}$, a and c even. In all valid pairs, the difference is $\pm(\tau + 1)^e$, with $0 \leq e \leq 7$.

The attractors have the "right" number of elements, except (e.g.) for $\{\tau, \tau + 1\}$, where it has 3.