A second look at binary digits

Christiaan van de Woestijne
(Supported by FWF Project S9606)

Institut für Mathematik B
Technische Universität Graz
Lehrstuhl für Mathematik und Statistik
Montanuniversität Leoben

ÖMG-DMV-Kongreß 2009, Graz
21–25 September 2009
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 $T : \mathbb{Z} \rightarrow \mathbb{Z} : a \mapsto \begin{cases} \frac{a}{2} & \text{if } a \text{ even;} \\ \frac{a-1}{2} & \text{if } a \text{ odd.} \end{cases}$

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

Example: $27 \rightarrow 13 \rightarrow 6 \rightarrow 3 \rightarrow 1 \rightarrow 0$.

However, $-1 \rightarrow -1$...

Try other digits: $D = \{d_0, d_1\}$, 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 $\{0, 1\}$:

$-27 \rightarrow 14 \rightarrow -7 \rightarrow 4 \rightarrow -2 \rightarrow 1 \rightarrow 0$, 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 $0 \rightarrow 0$ !

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 $\pm 2$ 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 $-27$:

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

Interesting: $0 \mapsto 4 \mapsto 2 \mapsto 1 \mapsto 0$, a 3-cycle!

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

**Theorem** Any valid digit set gives rise to a nontrivial expansion of zero.
The figure plots all pairs of integers \((x, y)\), with \(|x|, |y| \leq 200\), that are valid digit sets for basis \(-2\).
Results

Theorem 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 \quad \text{(trivial)}

(ii) either \( dD = 0 \) or \( 3 \nmid dD \) \quad \text{(avoid 1-cycles except 0)}

(iii) we have \( 2d \leq D \) and \( 2D \geq d \) \quad \text{(0 is expansible)}

(iv) \( D - d = 3^i \) for some \( i \geq 0 \) \quad \text{(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:

- $\mathcal{O}$ is a $\mathbb{Z}$-order.
- $\alpha \in \mathcal{O}$ is nonzero.
- $\mathcal{D}$ represents $\mathcal{O}$ modulo $\alpha$ (we have $|\mathcal{D}| = |\text{Norm}(\alpha)| < \infty$).

Then we can define $T : \mathcal{O} \rightarrow \mathcal{O} : a \mapsto \frac{a - d_a}{\alpha}$, where $d_a \in \mathcal{D}$ has $a \equiv d_a \pmod{\alpha}$.

Easy necessary conditions to have finite expansibility of all $a \in \mathcal{O}$:

- $\alpha$ and $\alpha - 1$ must be non-units of $\mathcal{O}$
- $\alpha$ must be expanding, i.e., for all $\sigma : \mathcal{O} \hookrightarrow \mathbb{C}$ we have $|\sigma(\alpha)| > 1$. 
The periodic set

With this setup, we call \((\mathcal{O}, \alpha, D)\) a \textit{pre-number system}.

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

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

In higher dimensions, the geometric structure of the periodic set is quite complicated.
The tile

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

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

In higher dimensions, these tiles usually have fractal boundary.

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.
More-or-less-theorem Let $\alpha$ be an expanding algebraic integer of norm $\pm 2$. 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) $\delta \equiv 1 \pmod{\alpha}$ and $(d_0, \alpha - 1) = (1)$

(ii) there is a nontrivial zero expansion

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

Note that for a given degree $d$, there are only finitely many expanding $\alpha$ of degree $d$ and norm $\pm 2$. A famous example is $\tau = \frac{-1 + \sqrt{-7}}{2}$ satisfying $x^2 + x + 2$. 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).