# Algebraic aspects of number systems

**Christiaan van de Woestijne**
**Institut für Mathematik B**
**Technische Universität Graz, Austria**

**Supported by the FWF, project S9606**

**Journées de Numération (cítací dni)**
**Prague, 25–30 May 2008**

# Definitions

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

- $V$ is a finite free $\mathbb{Z}$-module;
- $\phi$ 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 ... (answer at end of talk)

- $(\mathbb{Z}[X]/((X-5)(X-7)), X, \{1, -1, 3, -3, 5, X, X-2, -X+2, X-4, -X+4, X-6, -X+6, X-8, -X+8, -X+10, 2X-7, 2X-9, -2X+9, 2X-11, -2X+11, 2X-13, -2X+13, -2X+15, 3X-14, 3X-16, -3X+16, -3X+18, 3X-18, -3X+20, 4X-21, 4X-23, -4X+23, -4X+25, 5X-28, -5X+30\})$ is a number system (recall from last year?)

# Example: the odd digits

Assume $V = \mathbb{Z}$ and $\phi$ 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 | $\bar{1}3$ | 5 | $1\bar{1}\bar{1}$ | $-1$ | $\bar{1}$ | $-6$ | $\bar{1}133$ |
| 1 | $1$ | 6 | $13$ | $-2$ | $\bar{1}1$ | $-7$ | $\bar{1}1\bar{1}$ |
| 2 | $1\bar{1}$ | 7 | $1\bar{1}1$ | $-3$ | $\bar{1}13$ | $-8$ | $\bar{1}131$ |
| 3 | $3$ | 8 | $3\bar{1}$ | $-4$ | $\bar{1}\bar{1}$ | $-9$ | $\bar{1}\bar{1}3$ |
| 4 | $11$ | 9 | $1\bar{1}3$ | $-5$ | $\bar{1}11$ | $-10$ | $\bar{1}13\bar{1}$ |

# 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 $T$.

# The easy case

Theorem (Kovács-Germán-vdW) Given $(V, \phi)$, let $\mathcal{D}$ be a set of shortest (nonzero) digits modulo $\phi$, with respect to a norm $\|\cdot\|$ on $V$ that satisfies $\|\phi^{-1}\| < \frac{1}{2}$. Then $(V, \phi, \mathcal{D})$ is a number system.

Such a norm exists when $|\alpha| > 2$ for all eigenvalues $\alpha$ of $\phi$.

Theorem (Curry, others?) Let $n \geq 1$, let $\phi$ be an endomorphism of $\mathbb{Z}^n$, and let

$$\mathcal{D} = \phi\left(\left[-\frac{1}{2}, \frac{1}{2}\right)^n\right) \cap \mathbb{Z}^n.$$

If we have $|\alpha| > 2$ for all singular values of $\phi$, then $(\mathbb{Z}^n, \phi, \mathcal{D})$ is a number system.

# Algebra

A finite free $\mathbb{Z}$-module $V$ with endomorphism $\phi$ is automatically a module over the ring $\mathbb{Z}[\phi] \subseteq \mathrm{End}_{\mathbb{Z}}(V)$. We have

$$\mathbb{Z}[\phi] \cong \mathbb{Z}[X]/(f_{\mathrm{min}}(\phi)).$$

If $\dim V = \dim \mathbb{Z}[\phi] = \deg(f_{\mathrm{min}}(\phi))$, then $V$ is isomorphic, as a $\mathbb{Z}[\phi]$-module, to an ideal of $\mathbb{Z}[\phi]$.

Theorem (Jordan-Zassenhaus) If $f \in \mathbb{Z}[X]$ is squarefree, then the number of isomorphism classes of ideals of $\mathbb{Z}[X]/(f)$ is finite.

It is important to consider also the classes of noninvertible ideals!

# Algebra (2)

Example: let $R = \mathbb{Z}[\sqrt{5}]$. The maximal order $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ is isomorphic to the non-principal ideal $I_2 = (2, 1+\sqrt{5})$ of $R$! Ugly: $N(I_2) = 2$, but $N(I_2^2) = 8$!!

The matrix of multiplication by $\sqrt{5}$ on $I_2$ is $M = \begin{bmatrix} -1 & 2 \\ 2 & 1 \end{bmatrix}$. It follows that this matrix is not similar over $\mathbb{Z}$ to the companion matrix of $X^2 - 5$, although it has the same characteristic polynomial.

The singular values of $M$ also equal to $\pm\sqrt{5}$, so by Curry's theorem, a valid digit set for basis $M$ on $\mathbb{Z}^2$ is given by $\left(M\left[-\frac{1}{2}, \frac{1}{2}\right)^2\right) \cap \mathbb{Z}^2 = \{(\pm 1, 0), (0, \pm 1), (0, 0)\}$.

It follows that $\{0, 2, -2, 1+\sqrt{5}, -1-\sqrt{5}\}$ is a valid digit set for basis $\sqrt{5}$ on $I_2$. The same digits divided by 2 form a valid digit set for $\sqrt{5}$ on the maximal order.

# Algebra (3)

If $\dim \mathbb{Z}[\phi] < \dim V$, then things become complicated. Sometimes, we have a direct sum decomposition:

- if $\phi$ is the identity, then $\mathbb{Z}[\phi] \cong \mathbb{Z}$, and we have $V \cong \mathbb{Z}^n$ as a $\mathbb{Z}$-module.
- if $V$ is the integral quaternions $\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k$ and $\phi$ is (left) multiplication by $i$, then $V \cong \mathbb{Z}[i] \oplus \mathbb{Z}[i]j$.

However, $V$ may be indecomposable as a $\mathbb{Z}[\phi]$-module.

Theorem (Heller-Reiner-Dade) If $p$ is a prime and $f = X^{p^i} - 1$, with $i \geq 3$, then there exist infinitely many isomorphism classes of indecomposable modules over the ring $\mathbb{Z}[X]/(f)$.

# Tiles and translation

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

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

The set $\mathcal{T}$ covers $V \otimes \mathbb{R}$, with tiling lattice Λ, which is the $\mathbb{Z}[\phi]$-submodule of $V$ generated by $\mathcal{D} - \mathcal{D}$, the differences of the digits. Translation of the digit set just induces a translation of $\mathcal{T}$; the attractor $\mathcal{A}$ is contained in $-\mathcal{T}$. This provides an easy proof of

Theorem. Given a pre-number system $(V, \phi, \mathcal{D})$, for each $t \in V$, let $\mathcal{D}_t = \{d + t : d \in \mathcal{D}\}$. Then there are only finitely many $t \in V$ such that $(V, \phi, \mathcal{D}_t)$ is a number system.

Another method shows that we can leave $0 \in \mathcal{D}$ in place, and obtain the same conclusion.

# $n$-fold pre-number systems

Let $(V, \phi, \mathcal{D})$ be a pre-number system with attractor $\mathcal{A}$. For every positive integer $n$, define

$$\mathcal{D}^n = \left\{ \sum_{i=0}^{n-1} \phi^i(d_i) : d_i \in \mathcal{D} \right\},$$

the set of all length-$n$ expansions on base $\phi$ with digits in $\mathcal{D}$. Then $(V, \phi^n, \mathcal{D}^n)$ is again a pre-number system, called the $n$-fold pre-number system of $(V, \phi, \mathcal{D})$, and we have

- $\mathcal{A}^n$, the attractor of $(V, \phi^n, \mathcal{D}^n)$, is equal to $\mathcal{A}$.
- $(V, \phi^n, \mathcal{D}^n)$ is a number system if and only if $(V, \phi, \mathcal{D})$ is a number system, and $\gcd(n, |\mathcal{A}|) = 1$.

This theorem is very useful for the computation of attractors, since the bounds on the size of $\mathcal{A}$ derived from $\mathcal{D}^n$ are often smaller than those derived from $\mathcal{D}$.

# $n$-fold pre-number systems (2)

Theorem (folklore) Let $\|\cdot\|$ be a norm on $V \otimes \mathbb{R}$, and let

$$S = \left\{ v \in V : \|v\| \leq \max_{d \in \mathcal{D}} \|d\| \frac{\|\phi^{-1}\|}{1 - \|\phi^{-1}\|} \right\};$$

then the attractor of $(V, \phi, \mathcal{D})$ is contained in $S$.

Example: let $V = \mathbb{Z}[i]$, with the complex norm $\|\cdot\|$, and let $\phi$ be multiplication by $b = -1 + i$. We let $\mathcal{D} = \{0, 1, 2, 3\}$, and compute

$$L_n = \frac{\max_{d \in \mathcal{D}^n} \|d\|}{\|b\|^n - 1}$$

for $n = 1, 2, \ldots$:

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| $L_n$ | 7.24 | 4.24 | 3.67 | 3.61 | 3.28 | 3.46 | 3.32 | 3.22 |

Of course, the computation of $L_n$ takes exponential time in $n$.

# $n$-fold pre-number systems (3)

Assume $V = \mathbb{Z}$.

Theorem (Matula 1982) Let $k \leq d \leq K$ for all $d \in \mathcal{D}$, and let $a \in \mathcal{A}$. Then

$$\begin{cases} \dfrac{-K}{b-1} \leq a \leq \dfrac{-k}{b-1} & \text{if } b > 0; \\ \dfrac{-kb-K}{b^2-1} \leq a \leq \dfrac{-Kb-k}{b^2-1} & \text{if } b < 0. \end{cases}$$

One should compare these bounds with the generic $|a| \leq \frac{\max |d|}{|b|-1}$.

The proof uses the twofold number system, in case $b < 0$, to reduce to the case $b > 0$.

# Infinitely many digit sets in $\mathbb{Z}$

Question: can one shift just one digit to obtain other good digit sets?

Answer: under all kinds of technical assumptions, Yes.

Theorem (A generalisation of Matula 1982 and Kovács and Pethő 1983) Let $(\mathbb{Z}, b, \mathcal{D})$ be a number system, where $B = |b| \geq 3$ and where $|d| \leq B$ for all $d \in \mathcal{D}$. Fix some $d \in \mathcal{D}$ and some integer $u$ with $|u| \leq B - 1$; if $0 \notin \mathcal{D}$, assume $|u| \leq B - 2$. Let $\mathcal{B}$ be the set of digits in $\mathcal{D}$ that occur in the expansions of 0, $u + 1$, $u$, and $u - 1$. If $d \notin \mathcal{B}$, then we may replace $d$ in $\mathcal{D}$ by $\tilde{d} = d - ub^k$, for any $k \geq 1$, without affecting the number system property.

Note that $|\mathcal{B}| \leq 6$ if $b > 0$ and $|\mathcal{B}| \leq 8$ if $b < 0$. For $|b| = 3$, the Theorem does not work.

# Examples of infinite families

We write $B = |b|$. For $B = 3$ (Matula): $\{0, 1, 2 - 3^k\}$ when $b = 3$, and $\{0, 1, 2 - 9^k\}$ when $b = -3$. Can take $\tilde{d} = d - ub^k$, for $d \notin \mathcal{B}$.

| $b$ | $\mathcal{D}$ | $u$ | $\mathcal{B}$ |
|---|---|---|---|
| $\geq 4$ | $\{-1, 0, 1, \ldots, b-2\}$ | 1 | $\{0, 1, 2\}$ |
| | | $-1$ | $\{-1, 0, b-2\}$ |
| $\leq -4$ | $\{0, 1, \ldots, B-1\}$ | 1 | $\{0, 1, 2\}$ |
| | | $-1$ | $\{0, 1, B-2, B-1\}$ |
| | $\{1, 2, \ldots, B\}$ | 1 | $\{1, 2, B\}$ |
| | | $-1$ | $\{1, B-2, B-1, B\}$ |
| | $\{-B, 1, 2, \ldots, B-1\}$ | 1 | $\{1, 2, B-1, -B\}$ |
| $\geq 5$ odd | odd digits | 1 | $\{-1, 1, -b+2, b\}$ |
| | | $-1$ | $\{-1, b-2, b\}$ |
| $\leq -5$ odd | odd digits | 1 | $\{-1, 1, b+2, b\}$ |
| | | $-3$ | $\{1, -1, -3, B-4, B-2\}$ |

# The proof

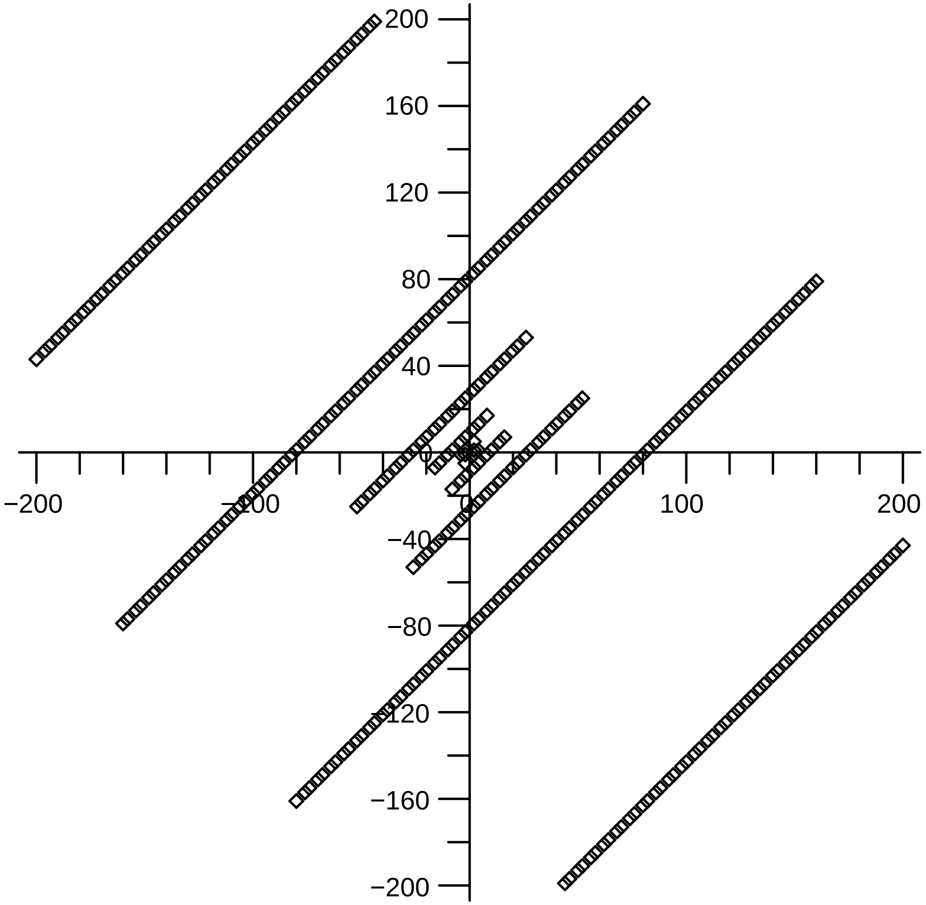
Let $\tilde{\mathcal{A}}$ be the attractor for base $b$ and digit set $\tilde{\mathcal{D}}$, which is $\mathcal{D}$ with $d$ replaced by $\tilde{d}$.

Lemma If $\tilde{d} = d - ub^k$, then the expansions of all $a \in \tilde{\mathcal{A}}$ on $\mathcal{D}$ have length bounded by $k + 2$ or so.

Now we construct a finite state transducer that replaces all occurrences of $d$ by $\tilde{d}$, and keeps the length under $k + 2$ or so.

Lemma If $d \notin \mathcal{B}$, then the finite state transducer always terminates on a word containing only $\tilde{d}$ and no $d$.

# Base $-2$




In the figure, we see all valid digit sets for $b = -2$ with both digits less than 200 in absolute value. What is the structure of this set?

# Base $-2$

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 $\{0, -1\}$.

# The proof (1)

It is clearly necessary that we have one even and one odd digit. Also, each digit $d$ divisible by 3 induces a 1-cycle $d/3$, so this is only admissible for $d = 0$.

Lemma When $|b| = 2$, the attractor $\mathcal{A}$ is an interval.

Lemma Let $d < D$ be digits for $b = -2$. Then

$$\mathcal{A} = \left\{ \left\lceil \frac{2d - D}{3} \right\rceil, \ldots, \left\lfloor \frac{2D - d}{3} \right\rfloor \right\}.$$

In other words, Matula's bounds are sharp for $b = -2$.

Lemma We have $0 \in \mathcal{A}$ if and only if $2d \leq D$ and $2D \geq d$.

# The proof (2)

It remains to determine the cycle structure of $\mathcal{A}$. Let $\mathcal{D} = \{d_0, d_1\}$, and let $\delta = d_0 - d_1$. If $a$ starts a cycle of length $\ell$, then

$$(1 - b^{\ell})a = \sum_{i=0}^{\ell-1} d_i b^i = d_0 \frac{b^{\ell} - 1}{b - 1} - \delta \sum_{i=0}^{\ell-1} \varepsilon_i b^i,$$

for some $\varepsilon \in \{0, 1\}$. With $b = -2$, we find

$$3\delta \text{ divides } (d_0 - 3a)((-2)^{\ell} - 1).$$

Because $\mathcal{A}$ is an interval of length $|\delta|$, except in some small cases we can assume that $\gcd(3\delta, d_0 - 3a) = 1$! Now we do some number theory to obtain

Lemma There is exactly one cycle in $\mathcal{A}$ if and only if $|\delta| = 3^i$ for some $i \geq 0$, and $3 \nmid (d_0 d_1)$ if $i \geq 1$.