On Noncanonical Number Systems

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

Journées de Numération (Zö’tåg’) in Graz
12–16 April 2007

Definition of number systems

A canonical number system is given by

- an algebraic integer α, the base, and
- a complete residue system $\mathcal{D}$ of $\mathbb{Z}[\alpha]$ modulo α, usually taken as $\{0, \ldots, |\,\mathrm{Norm}(\alpha)| - 1\}$, the digit set,

with the property that every $a \in \mathbb{Z}[\alpha]$ has a finite expansion

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

This definition represents a step in an ongoing chain of generalisations, and is the last one that has a recognisable "number" as a base.

Definition of number systems (2)

The following generalisation still has all the “structure” that we need to study number systems. We take:

- a finite free $\mathbb{Z}$-module V;
- a $\mathbb{Z}$-linear map $\phi : V \to V$ with nonzero determinant;
- a finite subset $\mathcal{D}$ of V that contains a complete residue system of V modulo its subgroup $\phi(V)$.

Note that V does not have a natural norm; we cannot yet talk about “large” or “small” elements of V. Later, we will choose a suitable norm.

Note also that we do not require $0 \in \mathcal{D}$.

Digits

If the digit set $\mathcal{D}$ is exactly a complete residue system, we call it irredundant, otherwise it is redundant.

If $\mathcal{D}$ is irredundant, then for each $v \in V$, we write $v \bmod_{\mathcal{D}} \phi$, or simply $v \bmod \phi$, for the unique digit d such that $v - d \in \phi(V)$.

We then define the transformation $T : V \to V$ by

$$T(v) = \phi^{-1}(v - (v \bmod \phi)),$$

and the $(\phi, \mathcal{D})$-expansion of $v \in V$ by

$$\sum_{i \geq 0} \phi^i(d_i) \quad \text{with} \quad d_i = T^i(v) \bmod \phi.$$

Periodic and finite expansions

We know: if ϕ is expanding, then for all $v \in V$, the $(\phi, \mathcal{D})$-expansion is eventually periodic.

When is $\sum_{i \geq 0} \phi^i d_i$ a finite expansion?

Answer: when $\sum_{i \geq 0} \phi^i d_i = \sum_{i=0}^{N-1} \phi^i d_i$, so $\sum_{i=N}^{\infty} \phi^i d_i = 0$!

If 0 is a digit, this is simple: $d_i = 0$ for $i = N, N+1, \ldots$

If 0 is not a digit, and ϕ is expanding, the only way is to have a zero period:

$$\sum_{i=0}^{\ell-1} \phi^i d_i = 0,$$

and this repeated indefinitely.

The zero period

Assume $\mathcal{D}$ is irredundant and ϕ is expanding. Then we saw

$$d_i = T^i(v) \bmod \phi;$$

because expansions are unique, we see that the zero period is unique and is found as the $(\phi, \mathcal{D})$-expansion of 0.

Let's see what this means for the transformation T on V. The zero period can be represented as

$$0 \to T(0) = \phi^{-1}\,[0 - (0 \bmod \phi)] \to T^2(0) \to \ldots \to 0.$$

If any nonzero element v has a finite expansion, then the sequence $(T^n(v))_{n \geq 0}$ must reach 0, and return there periodically. In particular, 0 must be a purely periodic element under T.

Conversely: if 0 is not purely periodic, then for all $n \geq 0$, $T^n(0)$ does not have a finite expansion.

Definition of number systems (3)

Before I forget... let me complete the definition! Let ϕ be expanding. I call a triple $(V, \phi, \mathcal{D})$ a number system if every $v \in V$ has a finite $(\phi, \mathcal{D})$-expansion, as defined above.

If $\mathcal{D}$ is irredundant, the expansion is automatically unique.

It is also interesting to look at redundant digit sets:

- simply add all elements that do not have a finite expansion to the digit set (if you can't beat 'em, join 'em)! The digit set remains finite;
- add some syntactic or other conditions on the expansions to ensure uniqueness (Non-Adjacent Form, etcetera).

Example

Consider $V = \mathbb{Z}$, and let M be an odd integer, $|M| \geq 2$. Take ϕ_M to be multiplication by M. Consider the irredundant digit set

$$\mathcal{D}_M = \{-M+2,\ -M+4,\ \ldots,\ -1,\ 1,\ \ldots,\ M-2,\ M\}.$$

I claim that this digit set makes $(\mathbb{Z}, \phi_M, \mathcal{D}_M)$ into a number system.

We have here $T(a) = \dfrac{a - (a \bmod_{\mathcal{D}_M} M)}{M}$; it's easy to prove that whenever $|a| > \dfrac{M}{M-1}$, we have $|T(a)| < |a|$.

But 1 and -1 are digits, and $0 \to \dfrac{0-M}{M} = -1 \to 0$, so we have a finite zero-period.

We will call these digits the odd digits modulo M.

The spectral radius

Theorem. Assume that the spectral radius ρ of ϕ^{-1} is less than $\frac{1}{2}$.

Let $\varepsilon > 0$ be less than $\frac{1}{2} - \rho(\phi^{-1})$, and let $\|\cdot\|$ be a norm on V, such that the induced operator norm $\|\phi^{-1}\| < \rho(\phi^{-1}) + \varepsilon$.

Let $\mathcal{D}$ be an irredundant digit set with the property that, for all $d \in \mathcal{D}$ and all $v \in V$,

$$v \equiv d \pmod{\phi} \Rightarrow \|d\| \leq \|v\|.$$

We call $\mathcal{D}$ a set of shortest digits for the norm $\|\cdot\|$.

Then $(V, \phi, \mathcal{D})$ is a number system.

(This result was also proved by Germán & Kovács (2007).)

The spectral radius (2)

Proof. We have, for all $v \in V$,

$$\|T(v)\| = \left\|\phi^{-1}\left(v - (v \bmod \phi)\right)\right\| < c \cdot 2\|v\| < \|v\|,$$

where $c = \rho(\phi^{-1}) + \varepsilon < \frac{1}{2}$, unless $v = v \bmod \phi$. It follows that for all $v \in V$, the sequence $T^n(v)$ must reach 0. Q.E.D.

We note that it is possible to construct a positive definite inner product on V such that the induced norm has the required properties. This yields an effective algorithm to find a set of shortest digits for a given V and ϕ.

Ideal class groups

The following are equivalent:

- $\phi : V \to V$ is a $\mathbb{Z}$-endomorphism;
- V is a $\mathbb{Z}[\phi]$-module.

Lemma. Assume that the minimal polynomial and characteristic polynomial of ϕ are equal. Then V is isomorphic, as a $\mathbb{Z}[\phi]$-module, to an ideal of $\mathbb{Z}[\phi]$.

Under this assumption, V is isomorphic to $\mathbb{Z}[X]/(P)$, for a polynomial P, iff the mentioned ideal is principal. Equivalently: if ϕ has matrix A for some basis of V, then

$$A = C^{-1} R_P C \qquad (R_P \text{ the companion matrix of } P)$$

for some unimodular matrix C.

The Chinese Remainder Theorem (1)

From now on, we take all (V, ϕ) to be isomorphic, as a $\mathbb{Z}[\phi]$-module, to $\mathbb{Z}[X]/(P)$, for some monic polynomial P.

Let P_1 and P_2 in $\mathbb{Z}[X]$ be coprime monic polynomials. The Chinese Remainder Theorem tells us that

$$\frac{\mathbb{Q}[X]}{(P_1P_2)} \cong \frac{\mathbb{Q}[X]}{(P_1)} \times \frac{\mathbb{Q}[X]}{(P_2)} \;;$$

but what about $\mathbb{Z}[X]$?

The sequence $0 \to \frac{\mathbb{Z}[X]}{(P_1P_2)} \xrightarrow{\psi} \frac{\mathbb{Z}[X]}{(P_1)} \times \frac{\mathbb{Z}[X]}{(P_2)} \rightrightarrows \frac{\mathbb{Z}[X]}{(P_1, P_2)} \to 0$ is exact.

Thus, ψ is an isomorphism iff $1 \in (P_1, P_2)$, iff $\text{Res}(P_1, P_2) = \pm 1$.

The Chinese Remainder Theorem (2)

What do we want with the CRT? Suppose:

- $\mathbb{Z}[X]/(P_1)$ is a number system with digit set $\mathcal{D}_1$;
- $\mathbb{Z}[X]/(P_2)$ is a number system with digit set $\mathcal{D}_2$.

Let $v \in V = \mathbb{Z}[X]/(P_1 P_2)$; we expand

$$v \bmod P_1 = \sum_{i \geq 0} d_i^{(1)} X^i; \qquad v \bmod P_2 = \sum_{i \geq 0} d_i^{(2)} X^i.$$

Suppose that for all $i \geq 0$ we can solve $\begin{cases} d_i \equiv d_i^{(1)} \pmod{P_1} \\ d_i \equiv d_i^{(2)} \pmod{P_2} \end{cases}$ for $d_i \in V$; then we have an

expansion $\quad v = \sum_{i \geq 0} d_i X^i \quad$ modulo $P_1 P_2$!

CRT problems (1)

Problem 1: when is $\begin{cases} d \equiv d^{(1)} \pmod{P_1} \\ d \equiv d^{(2)} \pmod{P_2} \end{cases}$ solvable?

From the exact sequence, we see: iff

$$d^{(1)} \bmod (P_1, P_2) = d^{(2)} \bmod (P_1, P_2).$$

This is satisfied, e.g., if we have $\mathrm{Res}(P_1, P_2) = \pm 1$.

But we can also select the digits in such a way that the above system is always satisfied!

Note, by the way, that $\mathbb{Z}[X]/(P_1, P_2)$ is a finite ring, as we assume P_1 and P_2 to be coprime.

Example

Let $P_1 = X - 5$ and $P_2 = X - 7$, and let's try the canonical digits on both sides.

Now suppose we have $d^{(1)} = 0$ and $d^{(2)} = 1$. Can we "merge"?

CRT: $d = \frac{1}{2}(X - 5) \pmod{(X-5)(X-7)}$. That's not integral!

And indeed, we have $|\mathrm{Res}(X - 5, X - 7)| = 2$.

Better idea: let all digits be pairwise congruent modulo 2. As we saw above, we can take

$$\mathcal{D}_1 = \{-3, -1, 1, 3, 5\} \quad \text{and} \quad \mathcal{D}_2 = \{-5, -3, -1, 1, 3, 5, 7\}.$$

Trick question: why can't we take all digits even (so 0 could be a digit)?

CRT problems (2)

Problem 2: if

$$v \bmod P_1 = \sum_{i \geq 0} d_i^{(1)} X^i \quad \text{and} \quad v \bmod P_2 = \sum_{i \geq 0} d_i^{(2)} X^i$$

are both finite, and we can "merge", is the merged expansion $v = \sum_{i \geq 0} d_i X^i$ again finite?

In other words, is there N with $\sum_{i=0}^{N-1} d_i X^i = v$?

This is a difficult question. We restrict to the case where at least one of P_1 and P_2 is linear.

Phasing in

Assume $P_1 = X - p_0$, and let $r = \text{Res}(P_1, P_2) = P_2(p_0)$. Then $\mathbb{Z}[X]/(P_1, P_2) \cong \mathbb{Z}/(r)$. Now, assume all digits are pairwise congruent modulo r.

Lemma. We have $X \equiv 1 \pmod{(P_1, P_2)}$. In other words, we must have $p_0 \equiv 1 \pmod{r}$.

Lemma. Let $v \in \mathbb{Z}[X]/(P_1 P_2)$. The lengths of any finite expansions for v "on the left" and "on the right" are congruent modulo r.

Lemma. For $i = 1, 2$, let L_i be the length of the zero period for $\mathcal{D}_i$ modulo P_i. Then $L_1 \equiv L_2 \pmod{r}$.

Theorem

Let P_1 and P_2 be monic polynomials in $\mathbb{Z}[X]$, with P_1 linear, and let $\mathcal{D}_1$ and $\mathcal{D}_2$ be digit sets such that $\mathbb{Z}[X]/(P_1)$ and $\mathbb{Z}[X]/(P_2)$ become number systems. Put $r = \mathrm{Res}(P_1, P_2)$, and assume $r \neq 0$. For $i = 1, 2$, let L_i be the length of the zero period for $\mathcal{D}_i$ modulo P_i. Then the following are equivalent:

- all elements of $\mathcal{D}_1 \cup \mathcal{D}_2$ are pairwise congruent modulo r, and $\gcd(L_1, L_2) = |r|$;
- $\mathbb{Z}[X]/(P_1 P_2)$ becomes a number system with digit set

$$\psi^{-1}(\mathcal{D}_1 \times \mathcal{D}_2).$$

Note: if all assumptions are satisfied, it follows that

$$P_1(0) \equiv -1 \pmod{r},$$

independently of the chosen digit sets.

Example (continued)

Still, let $P_1 = X - 5$ and $P_2 = X - 7$, with the given digits. They are all congruent to 1 modulo 2.

The zero periods of both are $0 \to -1$, of length 2.

It follows that $\mathbb{Z}[X]/((X-5)(X-7))$ becomes a number system with the digits $\{1,\ -1,\ 3,\ -3,\ 5,\ X,\ X-2,\ -X+2,\ X-4,\ X-6,\ -X+6,\ X-8,\ -X+8,\ -X+10,\ 2X-7,\ 2X-9,\ -2X+9,\ 2X-11,\ -2X+11,\ 2X-13,\ -2X+13,\ -2X+15,\ 3X-14,\ 3X-16,\ -3X+16,\ -3X+18,\ 3X-18,\ -3X+20,\ 4X-21,\ 4X-23,\ -4X+23,\ -4X+25,\ 5X-28,\ -5X+30\}$.

It also works with the digit sets $\{505, 1, -1, 3, -3\}$ at base 5 and $\{777, 1, -1, 3, -3, 5, -5\}$ at base 7. The corresponding zero periods have length 10 and 4, respectively.