Representations of numbers without the digit zero

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

TU Graz, 28 June 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 is quite natural. We take:

- a monic nonconstant polynomial f with integral coefficients;
- a finite subset $\mathcal{D}$ of $\mathbb{Z}[X]$ that contains a complete residue system of $\mathbb{Z}[X]/(f)$ modulo X.

By the isomorphism theorem, we have

$$(\mathbb{Z}[X]/(f))\,/(X) \cong \mathbb{Z}/(f(0)).$$

We write $V = \mathbb{Z}[X]/(f)$.

Note 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 $v \bmod_{\mathcal{D}} X$, or simply $v \bmod X$, for the unique digit d such that $v - d$ is divisible by X.

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

$$T(v) = (v - (v \bmod X))/X,$$

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

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

Examples

A simple example is where $f = X - a$ for some integer a, $|a| \geq 2$. Here $V \cong \mathbb{Z}$, and modulo $X - a$, X is actually equal to a, so this is just the a-ary system, if we take digits

$$\{0, 1, \ldots, |a| - 1\},$$

the classical digits. $a = 2$: binary; $a = 10$: decimal; etc.

A cryptographical example: $f = X^2 + X + 2$, with zeros $\tau = \frac{-1 \pm \sqrt{-7}}{2}$. Now V is a quadratic ring; the classical digits here are

$$\{0, 1, \ldots, |f(0)| - 1\} = \{0, 1\}.$$

Here, every element $v \in V$ can be written as

$$v = \sum_{i=0}^{\ell} d_i X^i \pmod f,$$

with digits $d_i \in \mathcal{D}$.

Questions

1. given f and $\mathcal{D}$, can we write all elements of V in the form
$$\sum_{i=0}^{\ell} d_i X^i \pmod{f}$$
with d_i in $\mathcal{D}$?

2. given f, is there any digit set $\mathcal{D}$ with this property?

Theorem (B. Kovács, Pethő, Brunotte, et al.)
There is an algorithm that, given f and $\mathcal{D}$, decides question 1.

Theorem (A. Kovács and L. Germán, CvdW, 2007)
The answer to question 2 is Yes when all roots of f have (complex) absolute value bigger than 2.

More questions

Why do we want to consider digit sets without zero?

1. for a cryptographic reason: side channel attacks on (hyper)elliptic curve cryptography implementations
2. because they are there
3. specifically, because of the following construction of digit sets using the Chinese Remainder Theorem

SCA: we compute $nP = \left(\sum_{i=0}^{\ell} n_i \tau^i\right) P$.

That is, $\sum_{i=0}^{\ell} n_i(\tau^i P)$.

Observe when $n_i = 0$; know something about n!

Periodic and finite expansions

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

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

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

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

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

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

and this repeated indefinitely.

The zero period

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

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

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

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

$$0 \to T(0) = [0 - (0 \bmod X)]\,/X \to T^2(0) \to \ldots \to 0.$$

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.

Example

Consider $V = \mathbb{Z}$, and let M be an odd integer, $|M| \geq 2$. Take $f = X - M$. 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 $(\mathbb{Z}, \mathcal{D}_M)$ 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 Chinese Remainder Theorem (1)

Let f_1 and f_2 in $\mathbb{Z}[X]$ be coprime monic polynomials. The Chinese Remainder Theorem tells us that

$$\frac{\mathbb{Q}[X]}{(f_1 f_2)} \cong \frac{\mathbb{Q}[X]}{(f_1)} \times \frac{\mathbb{Q}[X]}{(f_2)} \; ;$$

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

The sequence $0 \to \dfrac{\mathbb{Z}[X]}{(f_1 f_2)} \xrightarrow{\psi} \dfrac{\mathbb{Z}[X]}{(f_1)} \times \dfrac{\mathbb{Z}[X]}{(f_2)} \rightrightarrows \dfrac{\mathbb{Z}[X]}{(f_1, f_2)} \to 0$ is exact.

Thus, ψ is an isomorphism iff $1 \in (f_1, f_2)$, iff $\mathrm{Res}(f_1, f_2) = \pm 1$.

The Chinese Remainder Theorem (2)

What do we want to do with the CRT? Suppose:

- $\mathbb{Z}[X]/(f_1)$ is a number system with digit set $\mathcal{D}_1$;
- $\mathbb{Z}[X]/(f_2)$ is a number system with digit set $\mathcal{D}_2$.

Let $v \in V = \mathbb{Z}[X]/(f_1 f_2)$; we expand

$$v \bmod f_1 = \sum_{i \geq 0} d_i^{(1)} X^i; \qquad v \bmod f_2 = \sum_{i \geq 0} d_i^{(2)} X^i.$$

Suppose that for all $i \geq 0$ we can solve $\begin{cases} d_i \equiv d_i^{(1)} \pmod{f_1} \\ d_i \equiv d_i^{(2)} \pmod{f_2} \end{cases}$ for $d_i \in V$; then we have an

$$\text{expansion} \quad v = \sum_{i \geq 0} d_i X^i \quad \text{modulo } f_1 f_2!$$

CRT problems (1)

Problem 1: when is $\begin{cases} d \equiv d^{(1)} \pmod{f_1} \\ d \equiv d^{(2)} \pmod{f_2} \end{cases}$ solvable?

From the exact sequence, we see: iff

$$d^{(1)} \bmod (f_1, f_2) = d^{(2)} \bmod (f_1, f_2).$$

This is satisfied, e.g., if we have $\mathrm{Res}(f_1, f_2) = \pm 1$.

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

Note, by the way, that $\mathbb{Z}[X]/(f_1, f_2)$ is a finite ring, as we assume f_1 and f_2 to be coprime.

Example

Let $f_1 = X - 5$ and $f_2 = X - 7$, 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 $|\operatorname{Res}(X - 5, X - 7)| = 2$.

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

$$v \bmod f_1 = \sum_{i \geq 0} d_i^{(1)} X^i \quad \text{and} \quad v \bmod f_2 = \sum_{i \geq 0} d_i^{(2)} X^i$$

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 $\sum_{i=0}^{N-1} d_i X^i = v$?

Let $D \in \mathbb{Z}[X]$ be such that all digits in $\mathcal{D}_1$ and $\mathcal{D}_\in$ are congruent to D modulo (f_1, f_2). We saw that such a D must exist.

Phasing in

Then $\sum_{i=0}^{\ell} d_i X^i \equiv D \sum_{i=0}^{\ell} X^i \pmod{f_1, f_2}$. Let $r = \mathrm{Res}(f_1, f_2)$. We have:

Lemma. The sequence $0, 1, 1+X, 1+X+X^2, \ldots$ has period r modulo (f_1, f_2).

Lemma. Let $v \in \mathbb{Z}[X]/(f_1 f_2)$. 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 f_i. Then $L_1 \equiv L_2 \pmod{r}$.

Theorem

Let f_1 and f_2 be monic polynomials in $\mathbb{Z}[X]$, and let $\mathcal{D}_1$ and $\mathcal{D}_2$ be digit sets such that $\mathbb{Z}[X]/(f_1)$ and $\mathbb{Z}[X]/(f_2)$ become number systems. Put $r = \mathrm{Res}(f_1, f_2)$, and assume $r \neq 0$. For $i = 1, 2$, let L_i be the length of the zero period for $\mathcal{D}_i$ modulo f_i. Then the following are equivalent:

- all elements of $\mathcal{D}_1 \cup \mathcal{D}_2$ are pairwise congruent modulo (f_1, f_2), the sequence $s_0 = 0, s_\ell = Xs_{\ell-1} + 1$ has period r modulo (f_1, f_2),
  and $\gcd(L_1, L_2) = |r|$;
- $\mathbb{Z}[X]/(f_1 f_2)$ becomes a number system with digit set

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

The half-linear case

If $f_1 = X - a$, then we have $\mathbb{Z}[X]/(f_1, f_2) \cong \mathbb{Z}/(r)$, so we can simplify the conditions. In particular, we have $r = f_2(a)$. Thus, condition 2 becomes:

$$
\begin{aligned}
X &\equiv 1 \pmod{p} \text{ for all primes } p|r, \\
X &\equiv 1 \pmod{4} \text{ if } 2|r.
\end{aligned}
$$

independently of the chosen digit sets.

Example (continued)

Still, let $f_1 = X - 5$ and $f_2 = X - 7$, 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 $\{1,\ -1,\ 3,\ -3,\ 5,\ X,\ X-2,\ -X+2,\ X-4,\ -X+4,\ X-6,\ -X+6,\ X-8,\ -X+8,\ -X+10,\ 2X-7,\ 2X-9,\ -2X+9,\ 2X-11,\ -2X+11,\ 2X-13,\ -2X+13,\ -2X+15,\ 3X-14,\ 3X-16,\ -3X+16,\ -3X+18,\ 3X-18,\ -3X+20,\ 4X-21,\ 4X-23,\ -4X+23,\ -4X+25,\ 5X-28,\ -5X+30\}$.

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.