Algorithmic problems in the research of number expansions

Péter Burcsi & Attila Kovács

{peter.burcsi,attila.kovacs}@compalg.elte.hu

Department of Computer Algebra
Faculty of Informatics
Eötvös Loránd University, Budapest
Lattice $\Lambda$ in $\mathbb{R}^n$

$M : \Lambda \to \Lambda$ such that $\det(M) \neq 0$

$0 \in D \subseteq \Lambda$ a finite subset

**Definition** The triple $(\Lambda, M, D)$ is called a *number system* (GNS) if every element $x$ of $\Lambda$ has a unique, finite representation of the form

$$x = \sum_{i=0}^{l} M^i d_i,$$

where $d_i \in D$ and $l \in \mathbb{N}$. 

Notations II.

- Similarity preserves the number system property, i.e., if $M_1$ and $M_2$ are similar via the matrix $Q$ and $(\Lambda, M_1, D)$ is a number system then $(Q\Lambda, M_2, QD)$ is a number system as well.

- No loss of generality in assuming that $M$ is integral acting on the lattice $\mathbb{Z}^n$.

- If two elements of $\Lambda$ are in the same coset of the factor group $\Lambda/M\Lambda$ then they are said to be congruent modulo $M$. 
Notations III.

Theorem 1[1] If \((\Lambda, M, D)\) is a number system then

1. \(D\) must be a full residue system modulo \(M\),
2. \(M\) must be expansive,
3. \(\det(I - M) \neq \pm 1\).

If a system fulfills these conditions it is called a \textit{radix system}. 
Let \( \phi : \Lambda \to \Lambda, \ x \mapsto M^{-1}(x - d) \) for the unique \( d \in D \) satisfying \( x \equiv d \pmod{M} \).

Since \( M^{-1} \) is contractive and \( D \) is finite, there exists a norm on \( \Lambda \) and a constant \( C \) such that the orbit of every \( x \in \Lambda \) eventually enters the finite set \( S = \{ p \in \Lambda \mid \|x\| < C \} \) for the repeated application of \( \phi \).

This means that the sequence \( x, \phi(x), \phi^2(x), \ldots \) is eventually periodic for all \( x \in \Lambda \).
Notations V.

- \((\Lambda, M, D)\) is a GNS iff for every \(x \in \Lambda\) the orbit of \(x\) eventually reaches 0.

- A point \(x\) is called periodic if \(\phi^k(x) = x\) for some \(k > 0\).

- The orbit of a periodic point is called a cycle.

- The decision problem for \((\Lambda, M, D)\) asks if they form a GNS or not.

- The classification problem means finding all cycles.
Content

- How to decide expansivity?
- How to generate expansive operators?
- How to decide the number system property?
- Case study: generalized binary number systems.
- How to classify the expansions?
- How to construct number systems?
Expansivity I.

\[ \Lambda = \mathbb{Z}^n. \text{ Given operator } M \text{ examine } P = \text{charpoly}(M). \]

- A polynomial is said to be \textit{stable} if
  1. all its roots lie in the open left half-plane, or
  2. all its roots lie in the open unit disk.

The first condition defines Hurwitz stability and the second one Schur stability.

- There is a bilinear mapping between these criterions (Möbius map).
Expansivity II.

- Schur stability: Algorithm of Lehmer-Schur.
- Hurwitz stability: An \( n \)-terminating continued fraction algorithm of Hurwitz.

Results:

- For arbitrary polynomials Lehmer-Schur is faster.
- For stable polynomials Hurwitz-method is faster.
- Caution: Intermediate expression swell may occur.
Expansivity III.

Comparision of the methods for stable polynomials.

![Graph showing comparison of stability and Lehmer-Schur methods.](image-url)
Expansivity III.

Comparision of the methods for stable polynomials.

![Graph showing comparison of stability and Lehmer-Schur methods for additions versus degree.](image-url)
Expansivity III.

Comparision of the methods for stable polynomials.
Expansivity IV.

Hurwitz-method works also for symbolic coeffs. Let \( a(x) = a_0 + a_1 x + a_2 x^2 + x^3 \in \mathbb{Z}[x] \).

Hurwitz-method gives that \( a(x) \) is expansive if

\[
\frac{3a_0 - a_1 - a_2 + 3}{a_0 - a_1 + a_2 - 1}, \quad \frac{a_0 + a_1 + a_2 + 1}{3a_0 - a_1 - a_2 + 3}, \quad \frac{8(a_0^2 - a_0 a_2 + a_1 - 1)}{(a_0 - a_1 + a_2 - 1)(3a_0 - a_1 - a_2 + 3)}
\]

are all positive.

For the details (with Maple code) see [2].
Expansivity V.

How to generate expansive integer polynomials with given degree and constant term?

- Using Las Vegas type randomized algorithm, which produces an expansive polynomial in $\mathbb{R}[x]$, then makes round.

- Using the algorithm of Dufresnoy and Pisot [3], which works well for small constant term.
Expansivity VI.

- Generating random expansive matrices seems difficult.

- One can apply an integer basis transformation to the companion matrix of a polynomial.

- This method generates all expansive matrices only if the class number of the order corresponding to the polynomial is 1.
The original method uses a covering of the set of fractions $H$ (all periodic points lie in the set $-H$). Since $H$ is compact, it gives lower and upper bounds on the coordinates of periodic points [4].

It can be combined with a basis transformation using a simulated annealing type randomized algorithm in order to improve the bounds [5].
GNS Decision II.

The average improvement in the volume of the covering set expressed in orders of magnitude.
Brunotte’s canonical number system decision algorithm [6] can be extended ($M$ is the companion of the monic, integer polynomial, $D = \{(i, 0, 0, \ldots 0)^T \mid 0 \leq i < |\det M|\}$).

**Function** \texttt{CONSTRUCT-SET-E}(M, D)

1. $E \leftarrow D$, $E' \leftarrow \emptyset$
2. while $E \neq E'$ do
   3. $E' \leftarrow E$
4.   forall $e \in E$ and $d \in D$ do
5.       put $\phi(e + d)$ into $E$
6.   end
7. end
8. return $E$
The previous algorithm terminates. Denote $B = \{(0, 0, \ldots, 0, \pm 1, 0, \ldots, 0)\}$ the $n$ basis vectors and their opposites.

**Function** \textsc{Simple-Decision} \((M, D)\)

1. \(E \leftarrow \text{Construct-set-E}(M, D);\)
2. \(\text{forall } p \in B \cup E \text{ do}\)
3. \(\text{if } p \text{ has no finite expansion then}\)
4. \(\text{return false ;}\)
5. \(\text{end}\)
6. \(\text{return true;}\)
GNS Decision V.

\[ M = \begin{pmatrix} 1 & -2 \\ 1 & 3 \end{pmatrix}, \quad D = \{(0, 0), (1, 0), (0, 1), (4, 1), (-7, 6)\}. \]

Changing the basis to \( \{(1, 0), (-1, 1)\} \) decreases the volume from 42 to 24. \( |E| = 65. \)
GNS Decision VI.

\[ M = \begin{pmatrix} 0 & -7 \\ 1 & 6 \end{pmatrix}, \quad D \text{ is canonical.} \]

Replacing the basis vector \((0, 1)\) with \((-5, 1)\) gives volume 4 instead of 64. \[ |E| = 12. \]
Binary Case II.

<table>
<thead>
<tr>
<th>Degree</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expansive</td>
<td>5</td>
<td>7</td>
<td>29</td>
<td>29</td>
<td>105</td>
<td>95</td>
<td>309</td>
<td>192</td>
<td>623</td>
<td>339</td>
</tr>
<tr>
<td>CNS</td>
<td>4</td>
<td>4</td>
<td>12</td>
<td>7</td>
<td>25</td>
<td>12</td>
<td>20</td>
<td>12</td>
<td>42</td>
<td>11</td>
</tr>
</tbody>
</table>

Problems: in higher dimensions the volume of the covering set or the set $E$ are sometimes too big. The largest $E$ encountered is of size $21223091$, for $2 + 3x + 3x^2 + 3x^3 + 3x^4 + 3x^5 + 3x^6 + 3x^7 + 3x^8 + 2x^9 + x^{10}$. The number of points in the covering set of this sample is $226508480352000$. 

Algorithmic problems in the research of number expansions, Graz, 16th April, 2007. – p.21/29
GNS Classification I.

Two methods: covering and simple classify.

**Function** \( \text{SIMPLE-CLASSIFY}(M, D) \)

1. \( D \leftarrow D; \)
2. \( \text{finished} \leftarrow \text{false}; \)
3. **while** not \( \text{finished} \) **do**
   4. \( \mathcal{E} \leftarrow \text{CONSTRUCT-SET-E}(M, D); \)
   5. \( \text{finished} \leftarrow \text{true}; \)
   6. **forall** \( p \in \mathcal{E} \cup B \) **do**
      7. **if** \( p \) does not run eventually into \( D \) **then**
          8. put newly found periodic points into \( D; \)
          9. \( \text{finished} \leftarrow \text{false}; \)
   10. **end**
7. **end**
12. **return** \( D \setminus D \) (the set of non-zero periodic points);
\[ M = \begin{pmatrix} 1 & -2 \\ 1 & 3 \end{pmatrix}, \quad D = \{(0, 0), (1, 0), (0, 1), (4, 1), (-7, 6)\}. \]
\[ M = \begin{pmatrix} 1 & -2 \\ 1 & 3 \end{pmatrix}, \quad D = \{(0, 0), (1, 0), (0, 1), (4, 1), (-7, 6)\}. \]
\[ M = \begin{pmatrix} \frac{1}{1} & -2 \\ 1 & 3 \end{pmatrix}, \quad D = \{(0, 0), (1, 0), (0, 1), (4, 1), (-7, 6)\}. \]
\[ M = \begin{pmatrix} 1 & -2 \\ 1 & 3 \end{pmatrix}, \quad D = \{(0, 0), (1, 0), (0, 1), (4, 1), (-7, 6)\}. \]
SIMPLE-CLASSIFY

\[ M = \begin{pmatrix} 1 & -2 \\ 1 & 3 \end{pmatrix}, \quad D = \{(0, 0), (1, 0), (0, 1), (4, 1), (-7, 6)\}. \]
$M = \begin{pmatrix} 1 & -2 \\ 1 & 3 \end{pmatrix}$, $D = \{(0, 0), (1, 0), (0, 1), (4, 1), (-7, 6)\}$. 
SIMPLE-CLASSIFY

$$M = \begin{pmatrix} 1 & -2 \\ 1 & 3 \end{pmatrix}, \quad D = \{(0, 0), (1, 0), (0, 1), (4, 1), (-7, 6)\}.$$
\[ M = \begin{pmatrix} \frac{1}{1} & -2 \\ 1 & 3 \end{pmatrix}, \quad D = \{(0, 0), (1, 0), (0, 1), (4, 1), (-7, 6)\} \]
\[ M = \begin{pmatrix} \frac{1}{1} & -2 \\ \frac{1}{3} & 1 \end{pmatrix}, \quad D = \{(0, 0), (1, 0), (0, 1), (4, 1), (-7, 6)\}. \]
$$M = \begin{pmatrix} \frac{1}{3} & -2 \\ 1 & 1 \end{pmatrix}, \ D = \{(0, 0), (1, 0), (0, 1), (4, 1), (-7, 6)\}.$$
$M = \begin{pmatrix} 1 & -2 \\ 1 & 3 \end{pmatrix}$, $D = \{(0, 0), (1, 0), (0, 1), (4, 1), (−7, 6)\}$. 
$$M = \begin{pmatrix} 1 & -2 \\ 1 & 3 \end{pmatrix}, \ D = \{(0, 0), (1, 0), (0, 1), (4, 1), (-7, 6)\}.$$
Simple-Classify

\[ M = \begin{pmatrix} \frac{1}{1} & -\frac{2}{3} \\ 1 & 3 \end{pmatrix}, \quad D = \{(0,0), (1,0), (0,1), (4,1), (-7,6)\}. \]
\[ M = \begin{pmatrix} 1 & -2 \\ 1 & 3 \end{pmatrix}, \quad D = \{(0, 0), (1, 0), (0, 1), (4, 1), (-7, 6)\}. \]
GNS Classification II.

Comparing covering and simple classify:

- Covering is parallelizable.
- Both give negative answers fast.
- Either can beat the other in some cases.
- Experiments show that the algorithmic complexity of the worst case is exponential.
Given lattice $\Lambda$ and operator $M$ satisfying criteria 2) and 3) in Theorem 1 is there any suitable digit set $D$ for which $(\Lambda, M, D)$ is a number system?

If yes, how many and how to construct them?
**Theorem** (Kátai) Let $\Lambda$ be the set of algebraic integers in an imaginary quadratic field and let $\alpha \in \Lambda$. Then there exists a suitable digit set $D$ by which $(\Lambda, \alpha, D)$ is a number system if and only if $|\alpha| > 1$, $|1 - \alpha| > 1$ hold.

**Theorem [8]** Let $\Lambda$ be the set of algebraic integers in the real quadratic field $\mathbb{Q}(\sqrt{2})$ and let $0 \neq \alpha \in \Lambda$. If $\alpha, 1 \pm \alpha$ are not units and $|\alpha|, |\overline{\alpha}| > \sqrt{2}$ then there exists a suitable digit set $D$ by which $(\Lambda, \alpha, D)$ is a number system.
Theorem [9] For a given matrix $M$ if $\rho(M^{-1}) < 1/2$ then there exists a digit set $D$ for which $(\Lambda, M, D)$ is a number system.

Theorem [9] Let the polynomial $c_0 + c_1x + \cdots + x^n \in \mathbb{Z}[x]$ be given and let us denote its companion matrix by $M$. If the condition $|c_0| > 2 \sum_{i=1}^{n} |c_i|$ holds then there exists a suitable digit set $D$ for which $(\mathbb{Z}^n, M, D)$ is a number system.
References

Thank you!