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

Notations I.

- Lattice Λ 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 (Λ, M, D) is called a *number system* (GNS) if every element x of Λ 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 (Λ, 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 Λ 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 (Λ, 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 *radix system*.

Notations IV.

- Let $\phi : \Lambda \to \Lambda$, $x \stackrel{\phi}{\mapsto} M^{-1}(x - d)$ 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 Λ 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 ϕ.
- This means that the sequence $x, \phi(x), \phi^2(x), \ldots$ is eventually periodic for all $x \in \Lambda$.

Notations V.

- (Λ, 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 (Λ, 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.

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

- A polynomial is said to be *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.

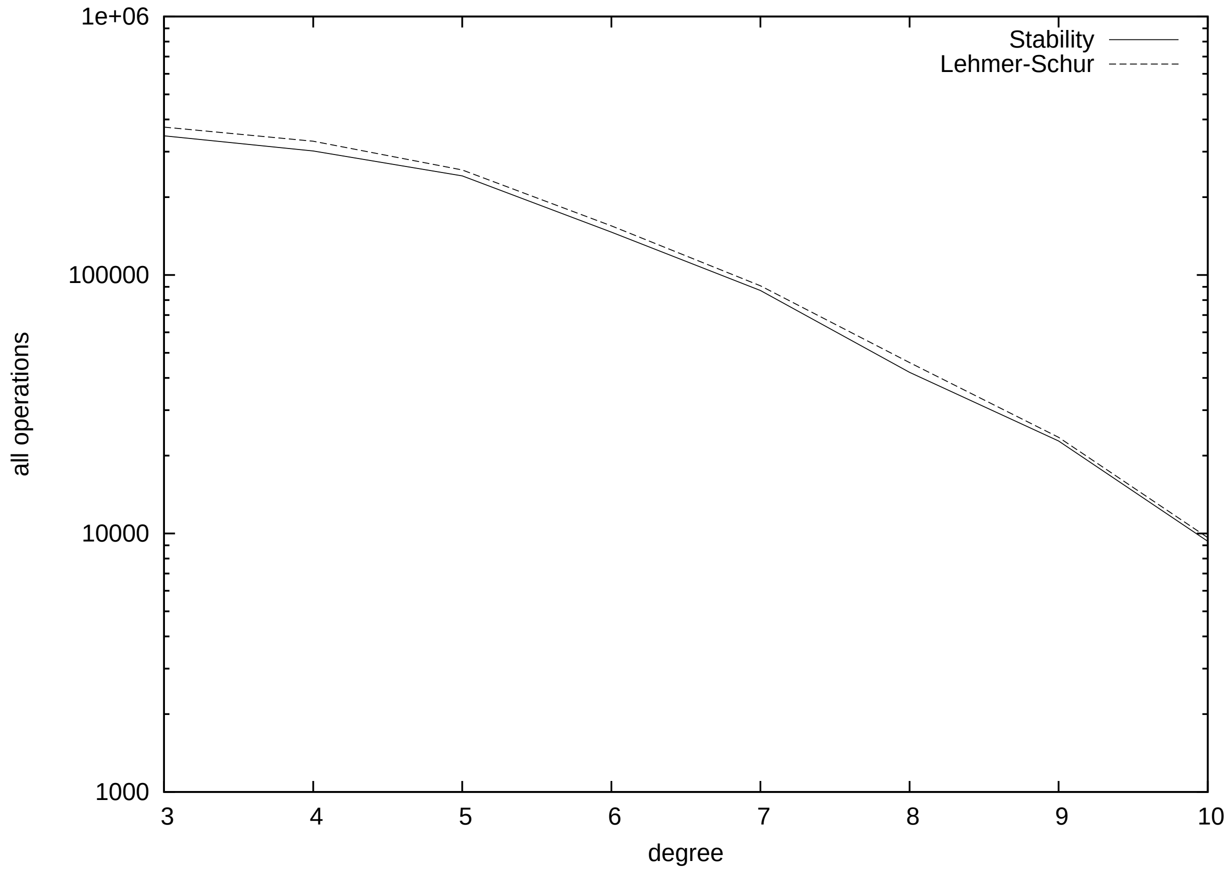
- Schur stability: Algorithm of Lehmer-Schur.
- Hurwitz stability: An n-terminating continued fraction algorithm of Hurwitz.

Results:

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

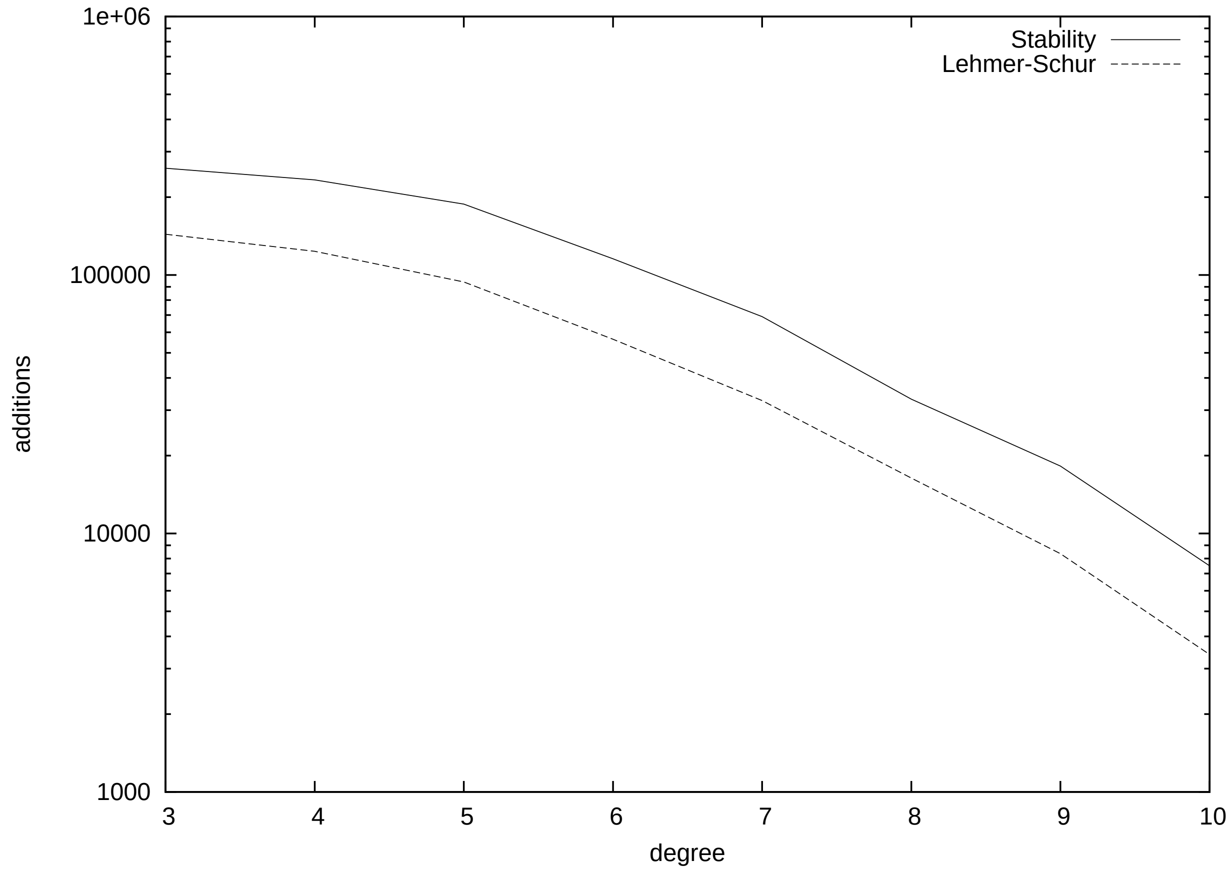
Expansivity III.

Comparision of the methods for stable polynomials.



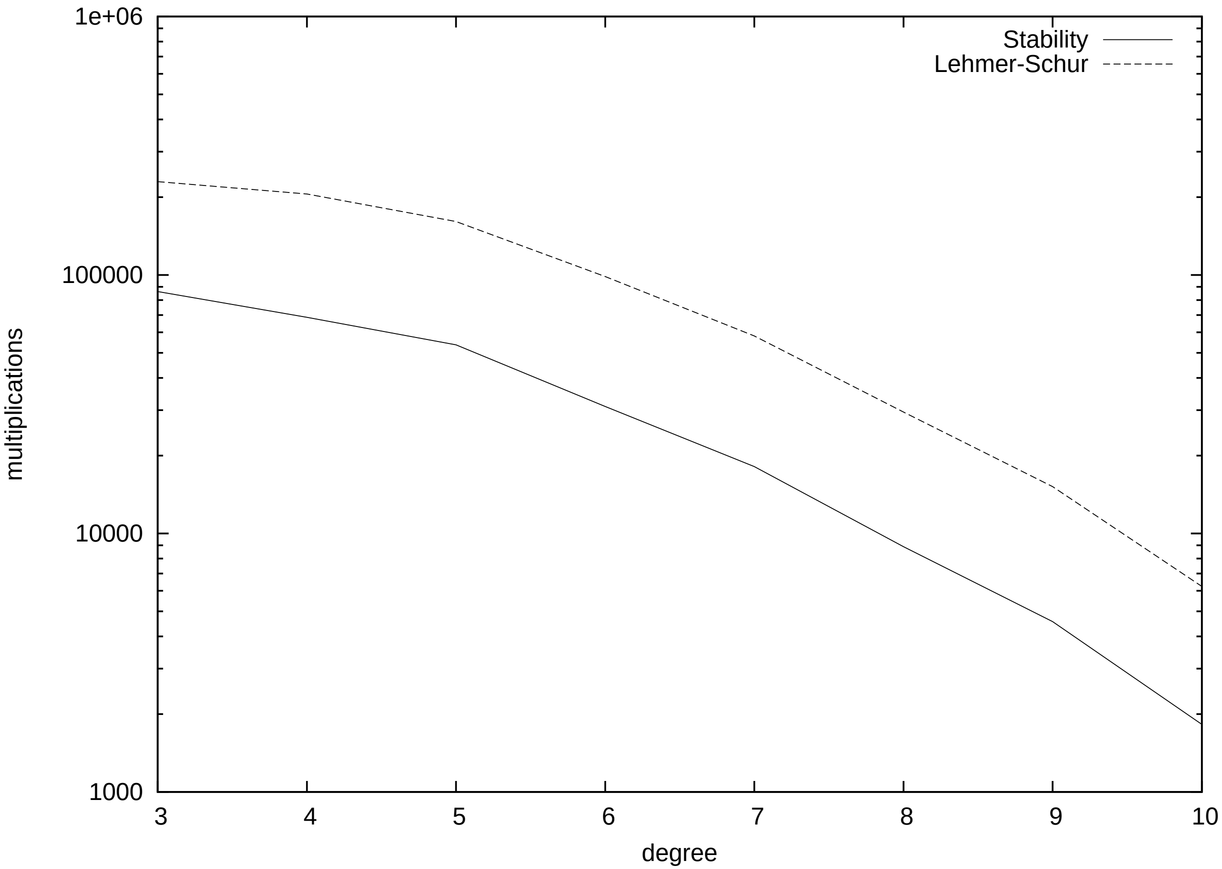
Expansivity III.

Comparision of the methods for stable polynomials.



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

$$\frac{3a_0 - a_1 - a_2 + 3}{a_0 - a_1 + a_2 - 1}, \frac{a_0 + a_1 + a_2 + 1}{3a_0 - a_1 - a_2 + 3}$$

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

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.

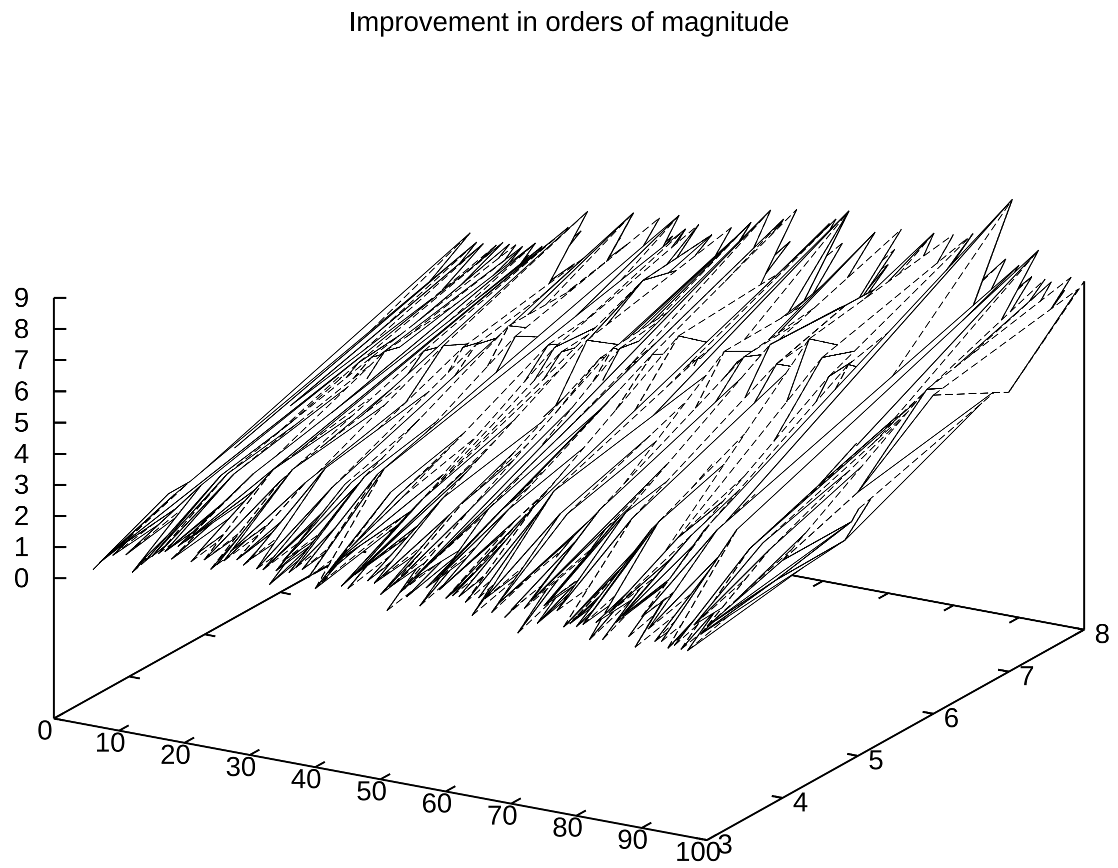
- Generating random expansive matrices seems difficult.
- One can apply an integer basis transformation to the companion matrix of a polynomial.
- This method generates all expansive matrices only if the class number of the order corresponding to the polynomial is 1.

GNS Decision I.

- 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.



GNS Decision III.

- 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 CONSTRUCT-SET-E(M, D)

```
E ← D , E′ ← ∅ ;
while E ≠ E′ do
    E′ ← E;
    forall e ∈ E and d ∈ D do
        put φ(e + d) into E;
    end
end
return E;
```

GNS Decision IV.

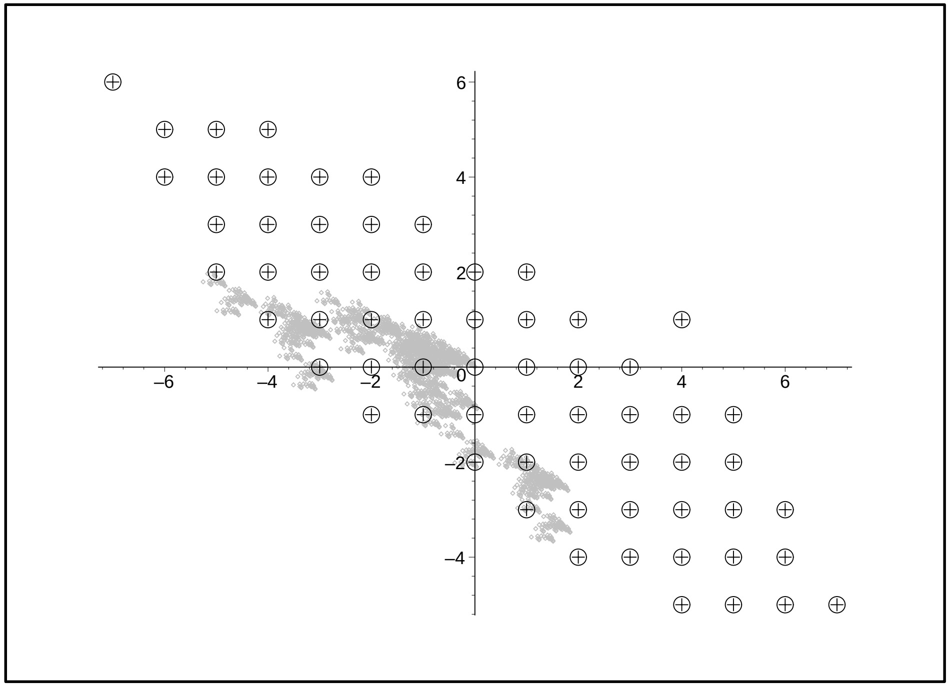
The previous algorithm terminates. Denote $B = \{(0, 0, \ldots, 0, \pm 1, 0, \ldots, 0\}$ the n basis vectors and their opposites.

Function SIMPLE-DECIDE(M, D)

$E \leftarrow$ CONSTRUCT-SET-E(M, D);
forall $p \in B \cup E$ **do**
    if p *has no finite expansion* **then**
        return false ;
end
return true;

GNS Decision V.

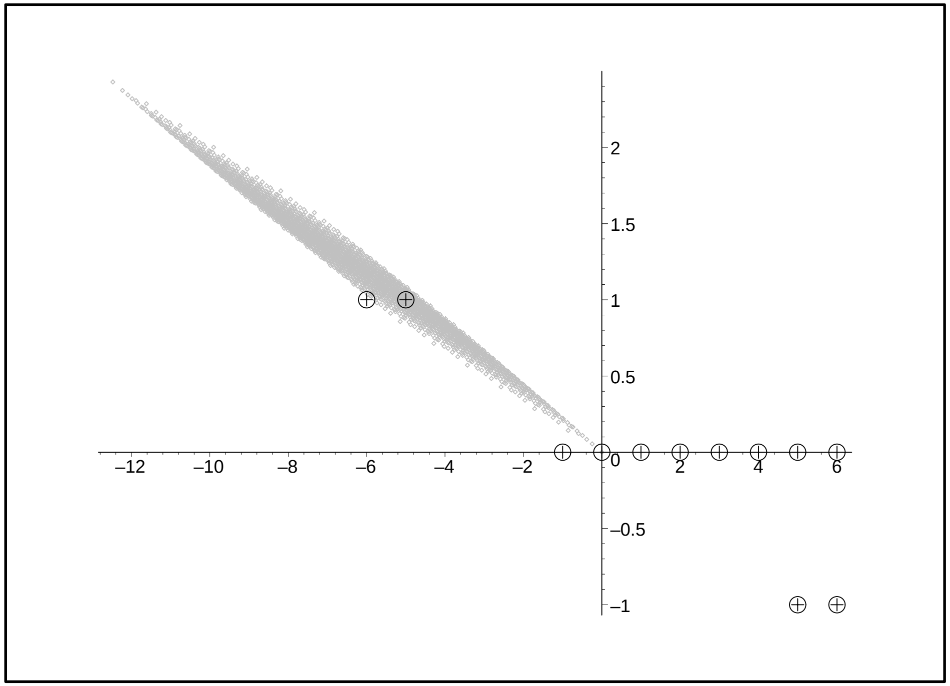
$M = \begin{pmatrix} 1 & -2 \\ 1 & 3 \end{pmatrix}, D = \{(0,0),(1,0),(0,1),(4,1),(-7,6)\}.$



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

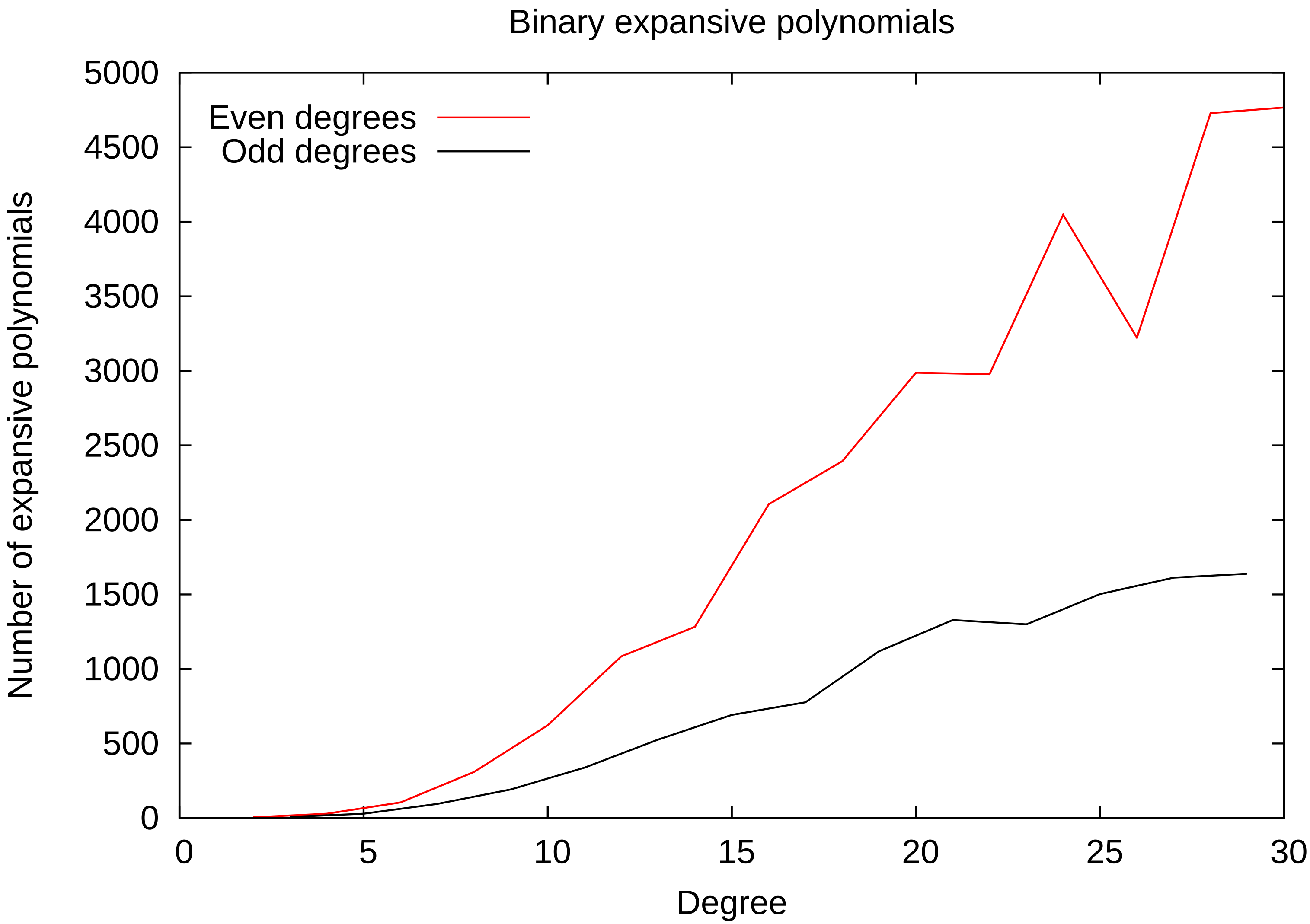
GNS Decision VI.

$M = \begin{pmatrix} 0 & -7 \\ 1 & 6 \end{pmatrix}$, D is canonical.



Replacing the basis vector $(0, 1)$ with $(-5, 1)$ gives volume 4 instead of 64. $|E| = 12$.

Binary Case I.



Binary Case II.

Degree	2	3	4	5	6	7	8	9	10	11
Expansive	5	7	29	29	105	95	309	192	623	339
CNS	4	4	12	7	25	12	20	12	42	11

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 $21\,223\,091$, 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 sapmle is $226\,508\,480\,352\,000$.

GNS Classification I.

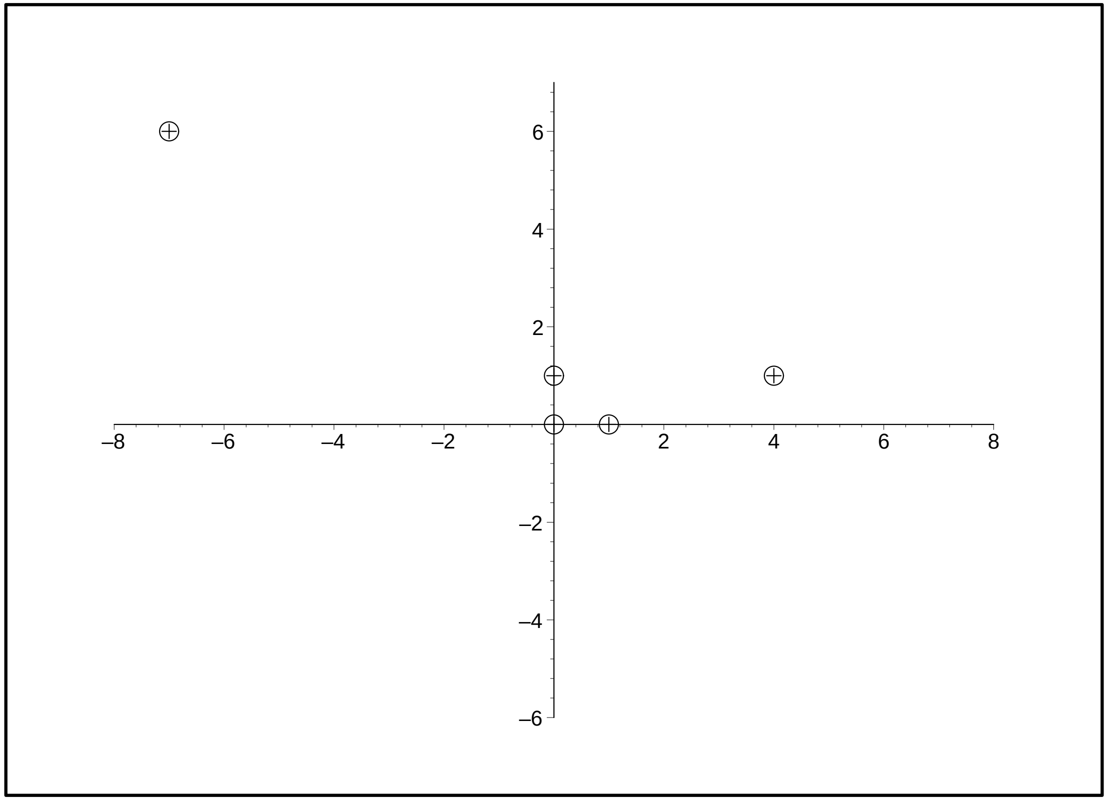
Two methods: covering and simple classify.

Function SIMPLE-CLASSIFY(M, D)

$\mathcal{D} \leftarrow D$;
finished $\leftarrow$ false;
while *not finished* **do**
  $\mathcal{E} \leftarrow$ CONSTRUCT-SET-E$(M, \mathcal{D})$;
  finished $\leftarrow$ true;
  forall $p \in \mathcal{E} \cup B$ **do**
    if p *does not run eventually into* $\mathcal{D}$ **then**
      put newly found periodic points into $\mathcal{D}$;
      finished $\leftarrow$ false;
  end
end
return $\mathcal{D} \setminus D$ (the set of non-zero periodic points);

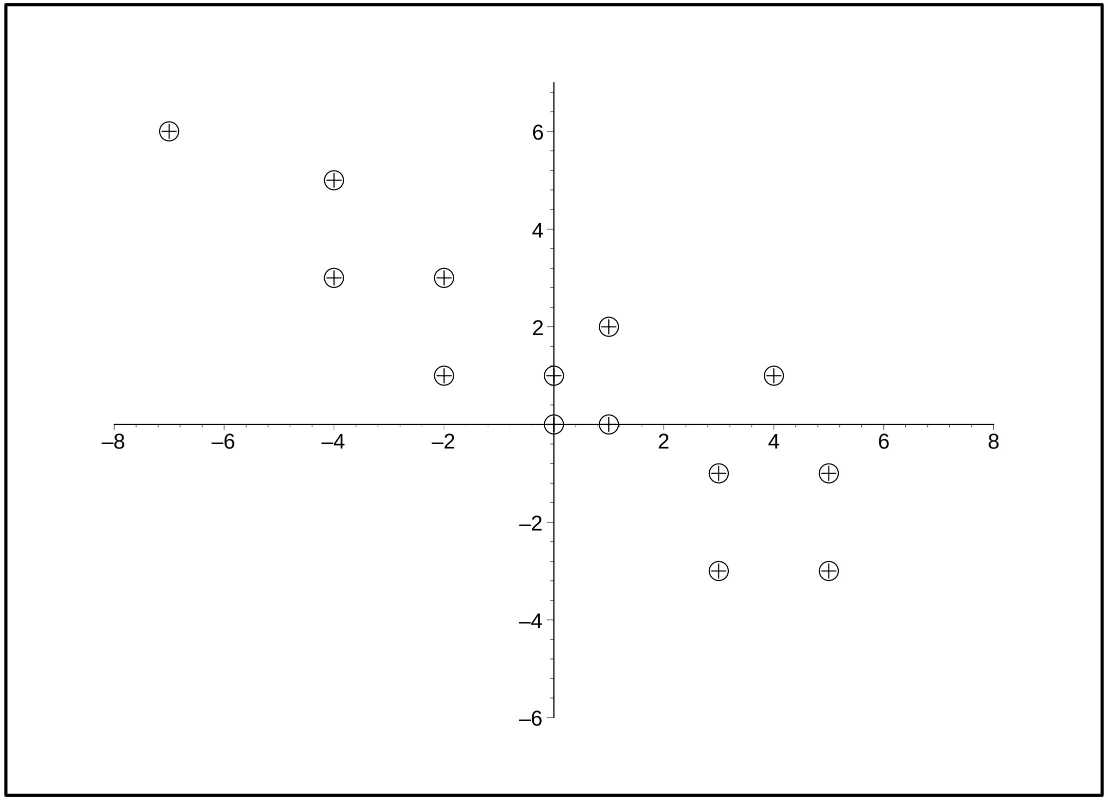
SIMPLE-CLASSIFY

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



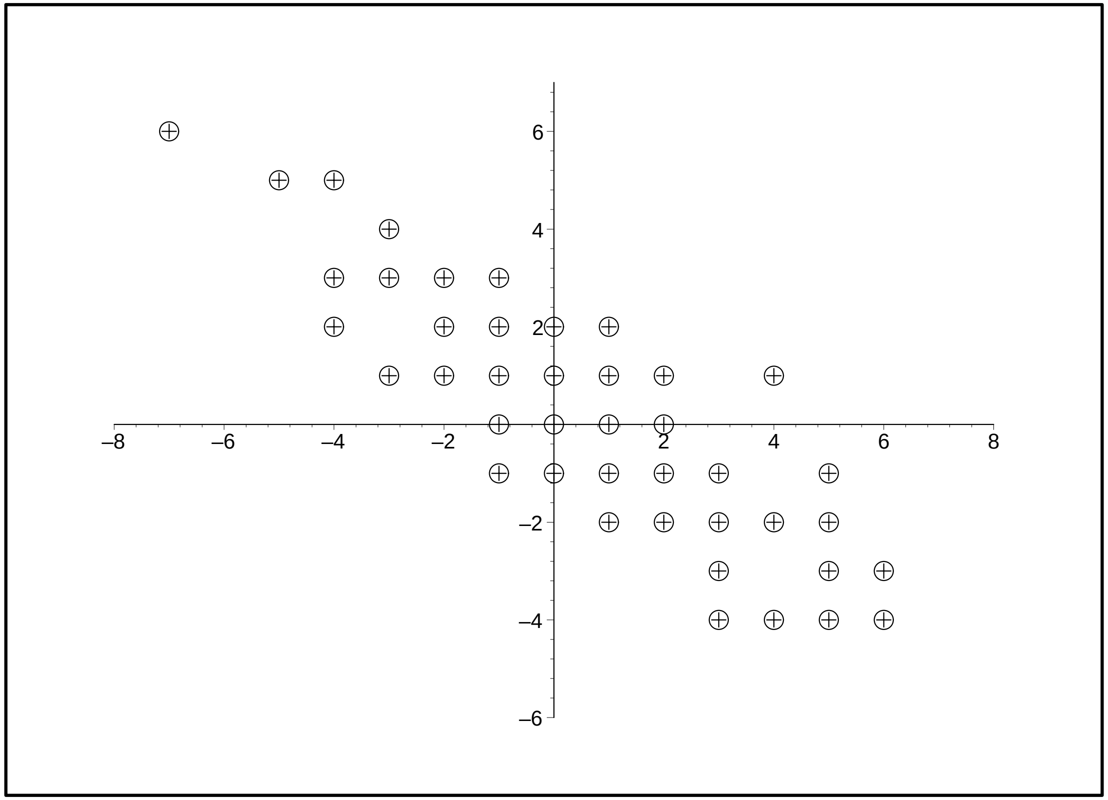
SIMPLE-CLASSIFY

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



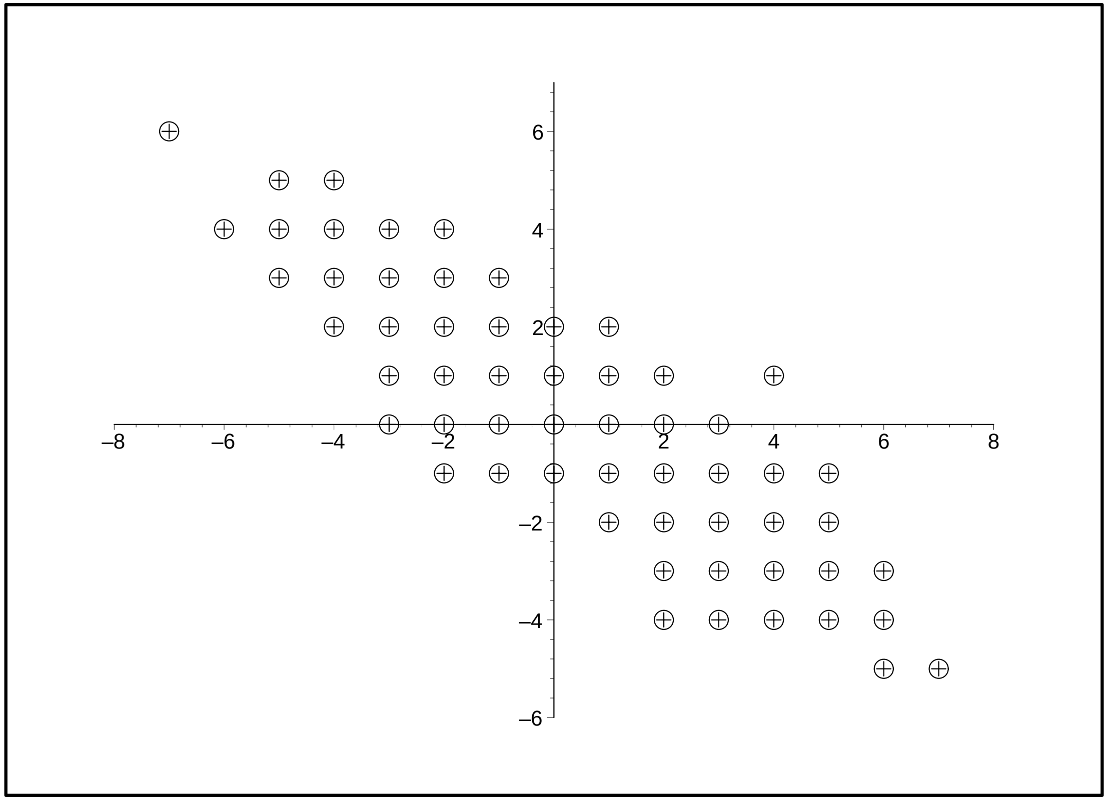
SIMPLE-CLASSIFY

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



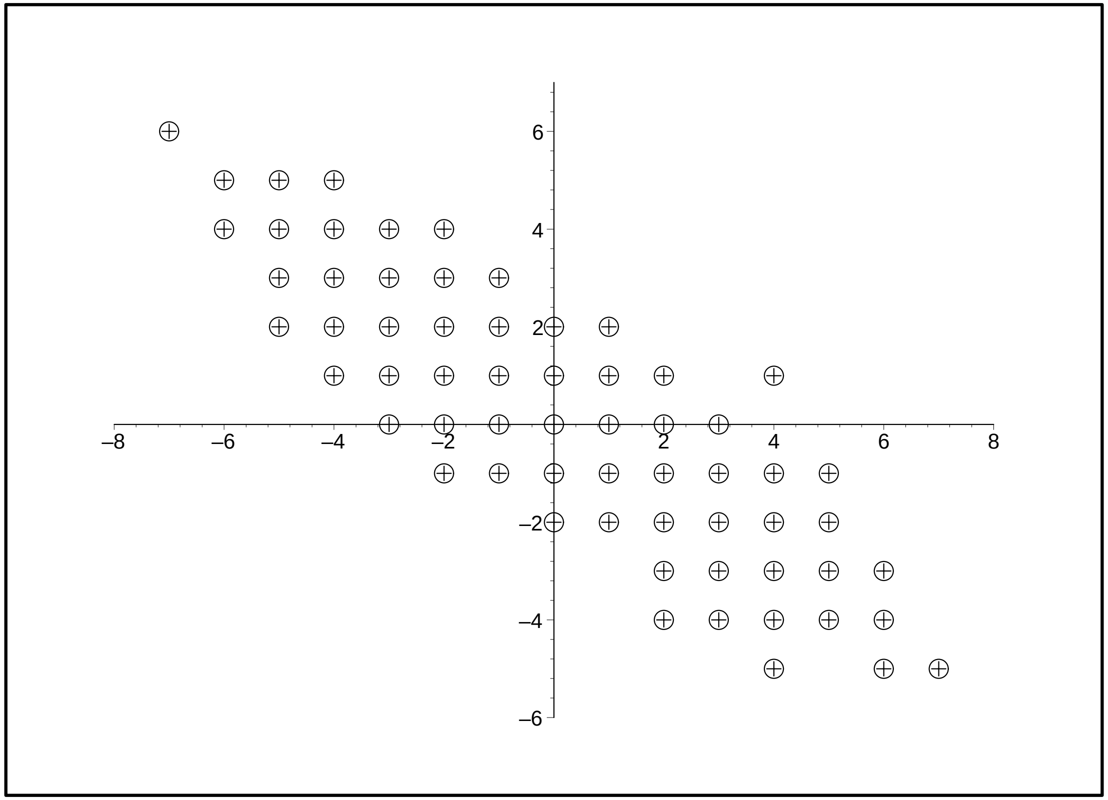
Simple-Classify

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



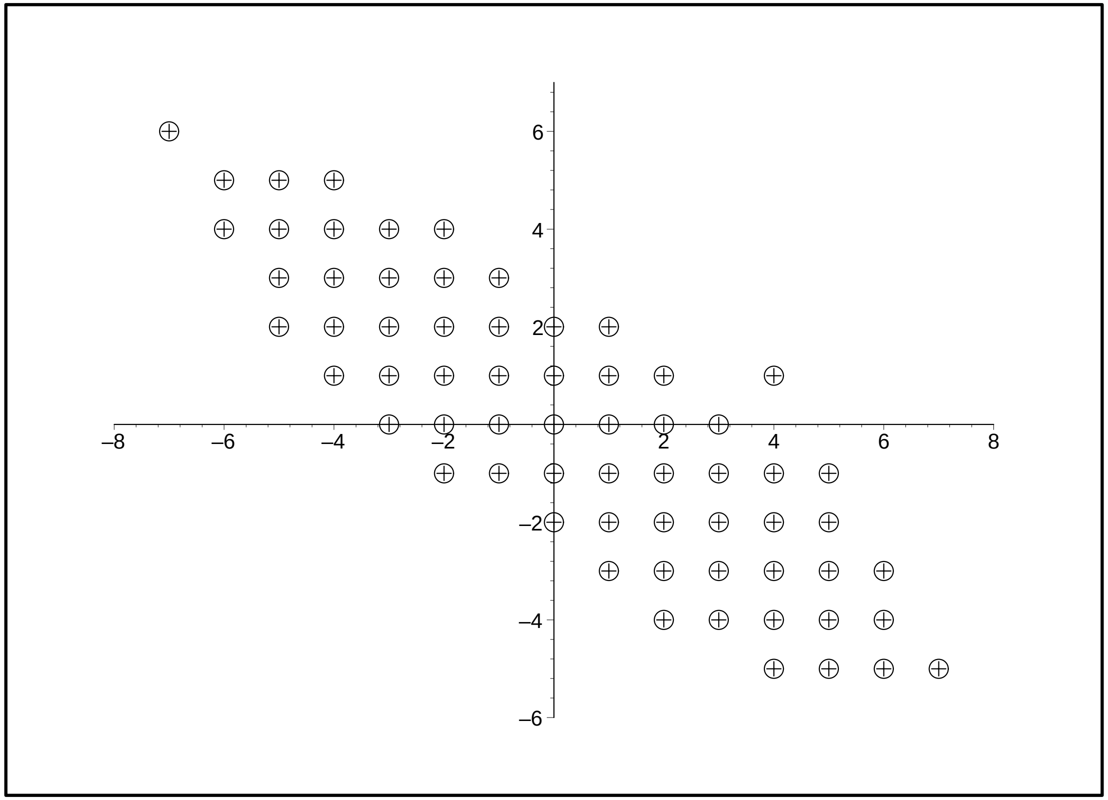
SIMPLE-CLASSIFY

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



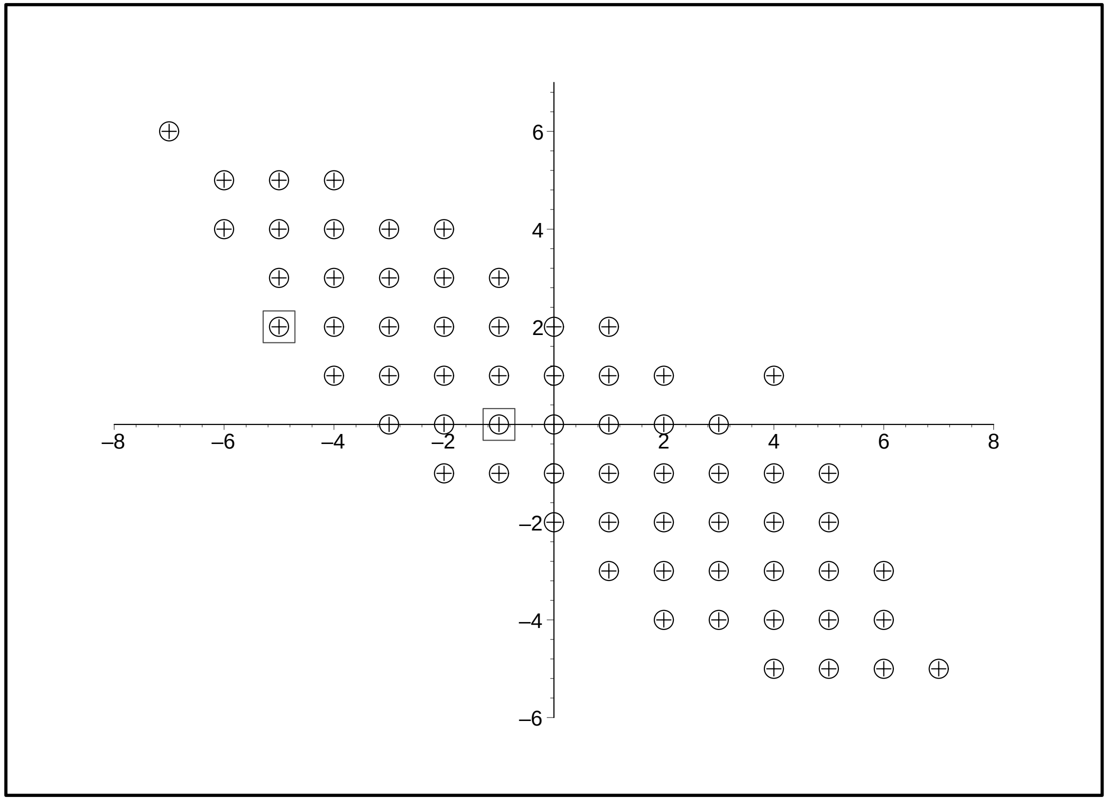
SIMPLE-CLASSIFY

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



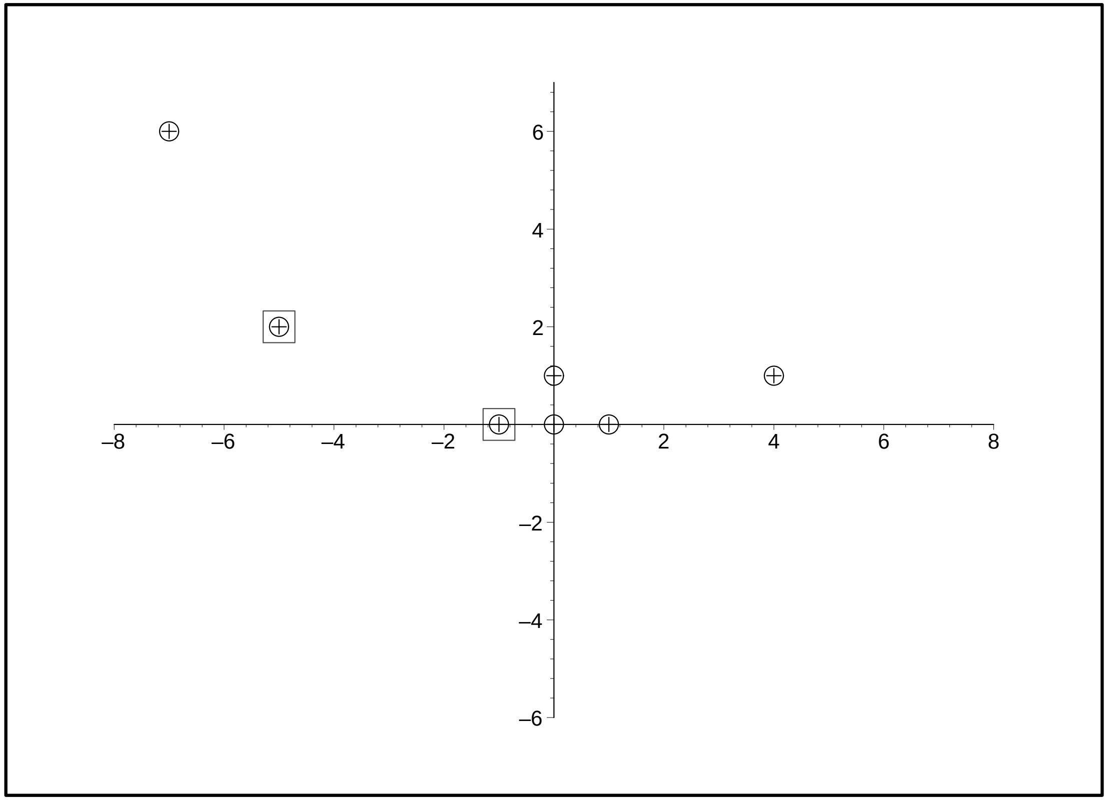
SIMPLE-CLASSIFY

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



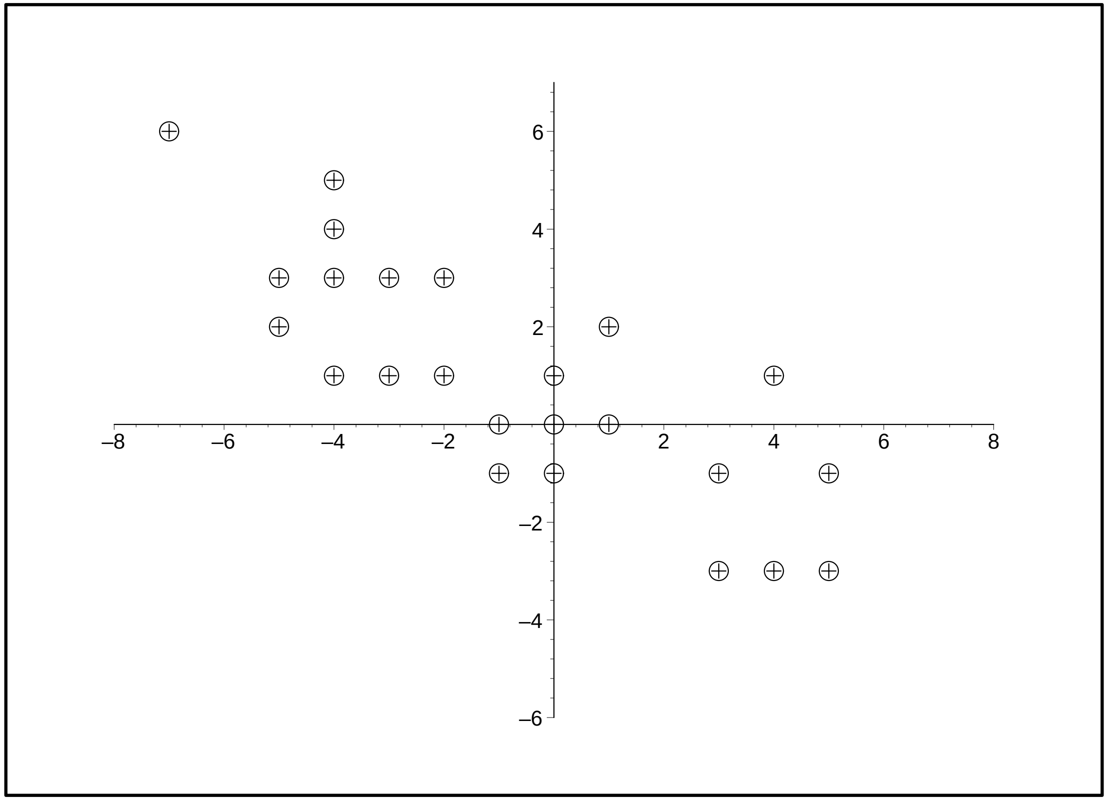
SIMPLE-CLASSIFY

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



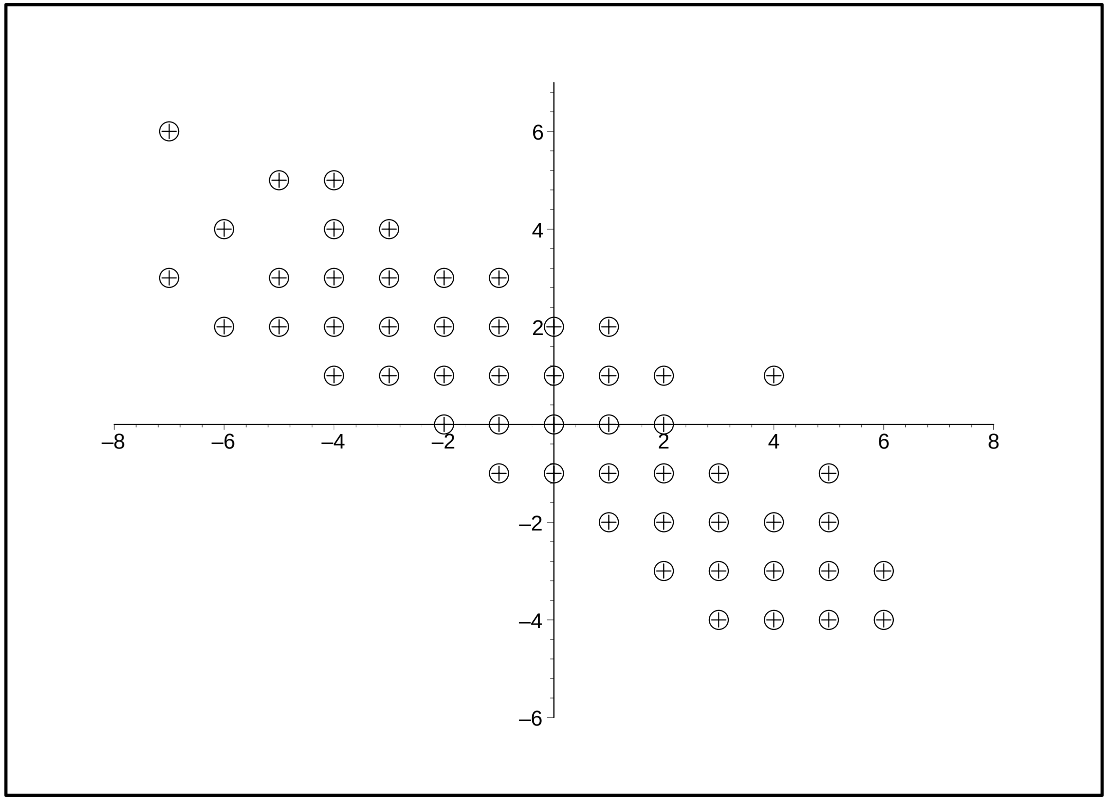
SIMPLE-CLASSIFY

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



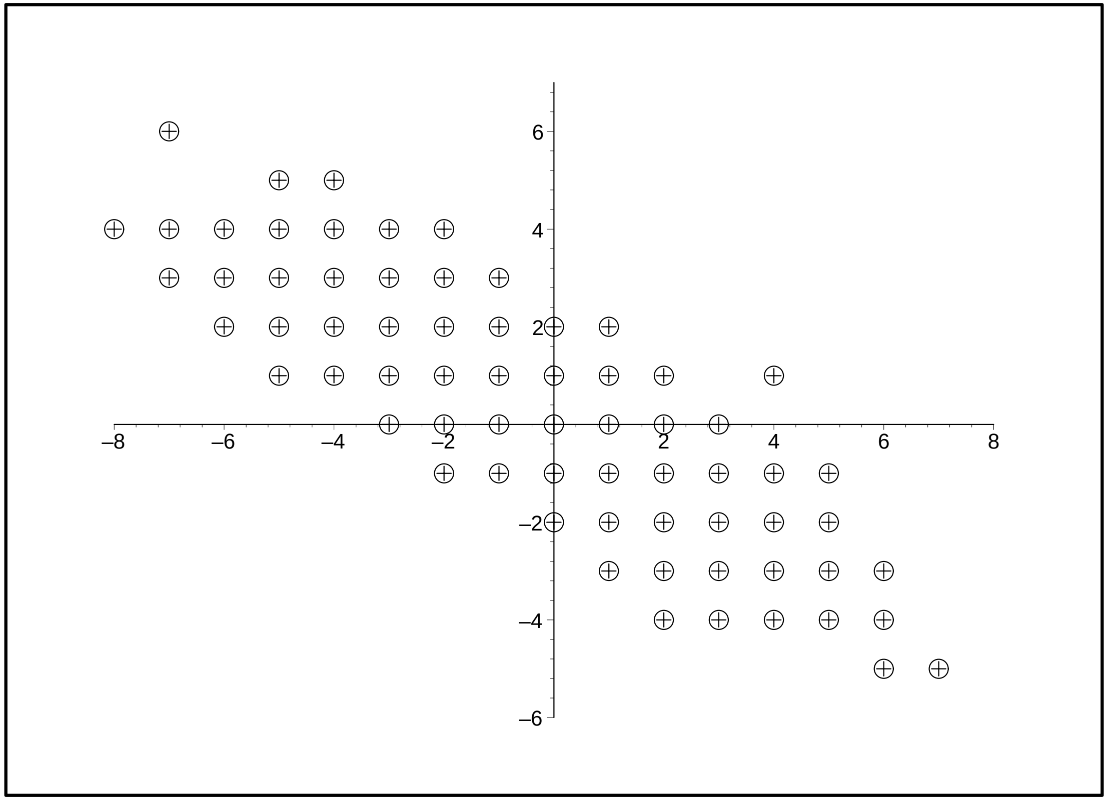
Simple-Classify

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



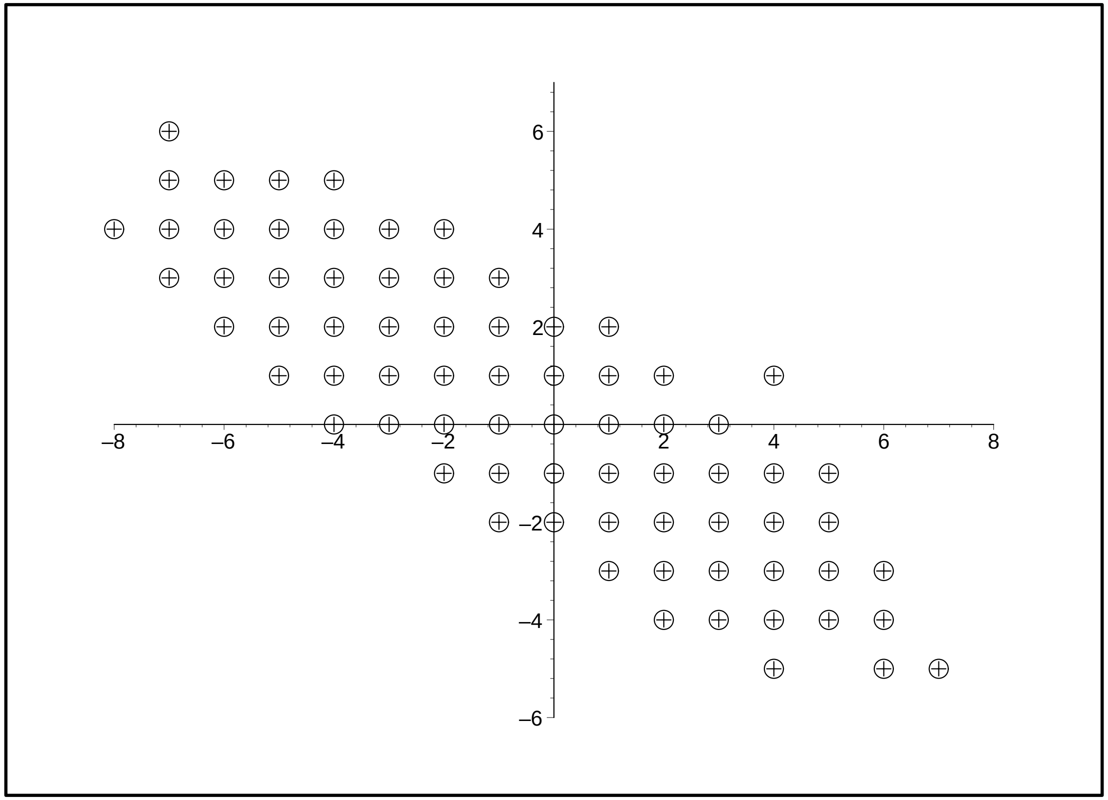
SIMPLE-CLASSIFY

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



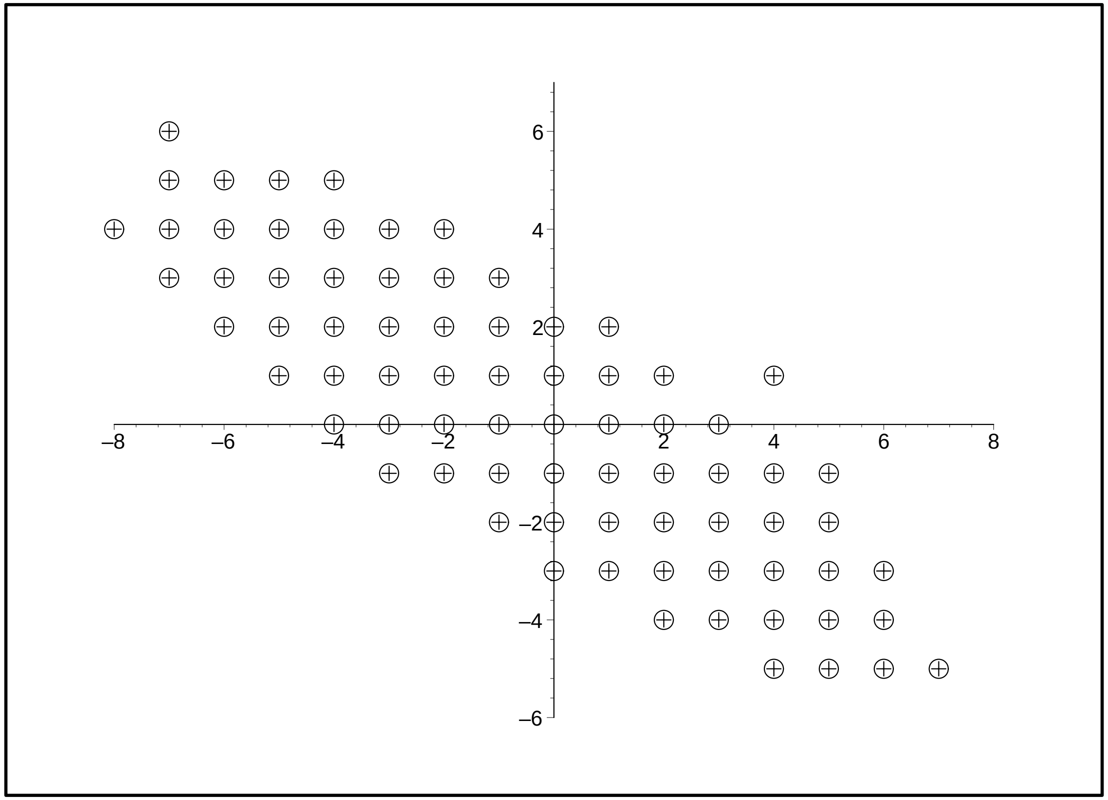
SIMPLE-CLASSIFY

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



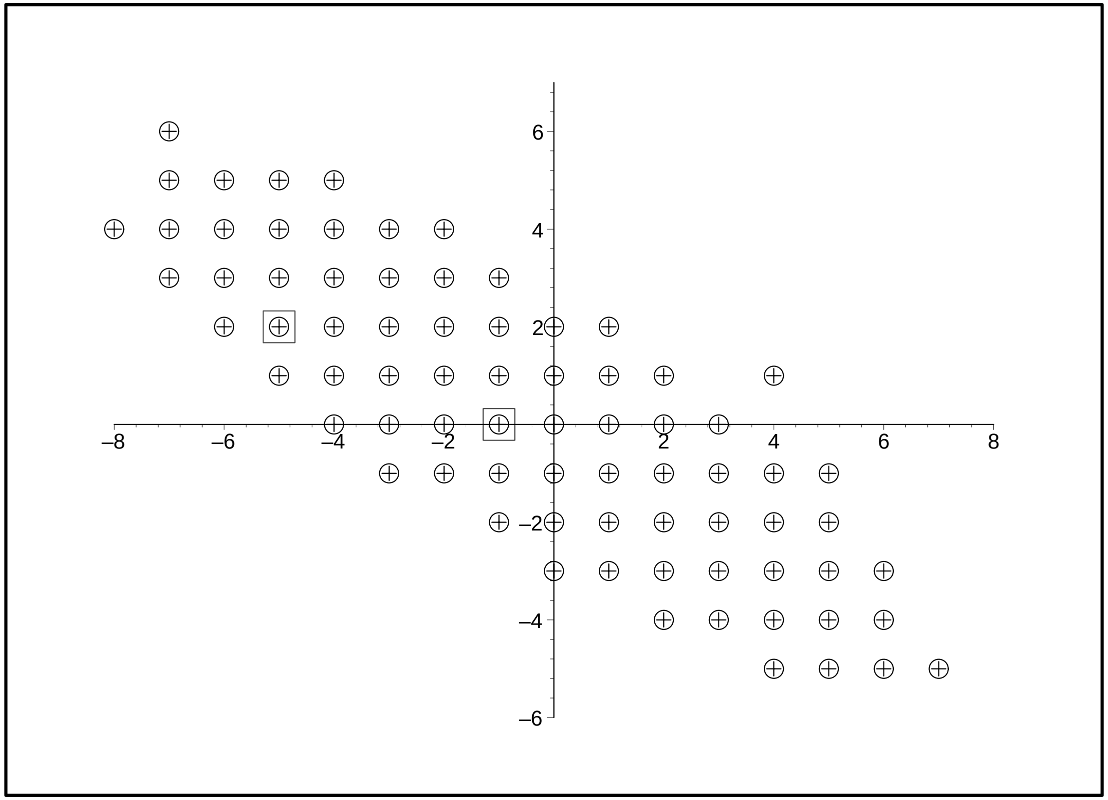
SIMPLE-CLASSIFY

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



Simple-Classify

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



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.

GNS Construction I.

- Given lattice Λ and operator M satisfying criteria 2) and 3) in Theorem 1 is there any suitable digit set D for which (Λ, M, D) is a number system?
- If yes, how many and how to construct them?

GNS Construction II.

Theorem (Kátai) Let Λ 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 (Λ, α, D) is a number system if and only if $|\alpha| > 1$, $|1 - \alpha| > 1$ hold.

Theorem [8] Let Λ 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 (Λ, α, D) is a number system.

GNS Construction III.

Theorem [9] For a given matrix M if $\rho(M^{-1}) < 1/2$ then there exists a digit set D for which (Λ, M, D) is a number system.

Theorem [9] Let the polynomial $c_0 + c_1 x + \cdots + x^n \in \mathbb{Z}[x]$ 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

[1] Kovács, A., *Number expansion in lattices*, Math. and Comp. Modelling, **38**, (2003), 909–915.

[2] Burcsi, P., Kovács, A., *An algorithm checking a necessary condition of number system constructions*, Ann. Univ. Sci. Budapest. Sect. Comput. **25**, (2005), 143–152.

[3] Dufresnoy, J., Pisot, Ch., *Etude de certaines fonctions méromorphes bornées sur le cercle unité. Application a un ensemble fermé d'entiers algébriques.* Annales scientifiques de l'École Normale Supérieure Sér. **3**, 72 no. 1., (1955), 69–92.

[4] Kovács, A., *On computation of attractors for invertible expanding linear operators in* $\mathbb{Z}^k$, Publ. Math. Debrecen **56**/1–2, (2000), 97–120.

[5] Burcsi, P., Kovács, A., Papp-Varga, Zs., *Decision and Classification Algorithms for Generalized Number Systems*, submitted.

[6] Brunotte, H., *On trinomial bases of radix representations of algebraic integers*, Acta Sci. Math. (Szeged), **67**, (2001), 407–413.

[7] Burcsi, P., Kovács, A., *Algorithms for finding generalized binary number systems*, in preparation.

[8] Farkas, G., Kovács, A., *Digital expansion in* $\mathbb{Q}(\sqrt(2))$, Annales Univ. Sci. Budapest, Sect. Comp. **22**, (2003), 83–94.

[9] Germán, L., Kovács, A., *On number system constructions*, Acta Math., Hungar., **115**, Numbers 1-2, 2007, 155–167.

Thank you!