General shift radix systems and discrete rotation

Attila Pethő

Department of Computer Science
University of Debrecen Debrecen, Hungary

Numeration 2019
Erwin Schrödinger Institut, Wien, July 3, 2019.

Talk is base on joint works with Jan-Hendrik Evertse, Kálmán Győry, Carolin Hannusch and Jörg Thuswaldner.

1. CNS and SRS

Let $p = p_n X^n + \ldots + p_1 X + p_0 \in \mathbb{Z}[X], p_n = 1, |p_0| > 1$ and $\mathcal{D} = \{0, 1, \ldots, |p_0| - 1\}$. The pair $(p, \mathcal{D})$ is called *canonical number system polynomial* - CNS - if there exist for all $0 \neq a \in \mathbb{Z}[X]$ integers ℓ and $a_0, \ldots, a_\ell \in \mathcal{D}$ such that

$$a \equiv a_0 + \ldots + a_\ell X^\ell \pmod{p}.$$

- This is a generalization of radix representation of integers. It was initiated by D. Knuth, and developed further by Penney, I. Kátai, J. Szabó, B. Kovács, etc.
- Not all $(p, \mathcal{D})$ is a CNS! For example $\left(X^2 + 2X + 2, \{0.1\}\right)$ is, but $\left(X^2 - 2X + 2, \{0.1\}\right)$ is not a CNS. Characterization of CNS is a hard problem.

To $\mathbf{r} \in \mathbb{R}^n$ associate the nearly linear mapping $\tau_{\mathbf{r}} \quad \mathbb{Z}^n \mapsto \mathbb{Z}^n$ such that if $(a_1, \ldots, a_n) = \mathbf{a} \in \mathbb{Z}^n$ then

$$\tau_{\mathbf{r}}(\mathbf{a}) = (a_2, \ldots, a_n, -[\mathbf{ar}]),$$

where [.] denotes the integer part, and $\mathbf{ar}$ the inner product.

Akiyama et al., 2005, called $\tau_{\mathbf{r}}$ a *shift radix system* - SRS - if the orbit $\tau_{\mathbf{r}}^k(\mathbf{a}), k = 0, 1, \ldots$ is eventually zero for all $\mathbf{a} \in \mathbb{Z}^n$.

They proved: $(p, \mathcal{D})$ is a CNS iff for $\mathbf{r} = \left(\frac{1}{p_0}, \frac{p_{n-1}}{p_0}, \ldots, \frac{p_n}{p_0}\right)$ the mapping $\tau_{\mathbf{r}}$ is a SRS.

Found relation between SRS and β-expansions too.

2. Generalized number system - GNS

Let $\mathcal{O}$ denote an order, that is a commutative ring with 1 whose additive group is free abelian of rank d. Identify $m \in \mathbb{Z}$ with $m \cdot 1$, and thus assume $\mathbb{Z} \subset \mathcal{O}$.

The order $\mathcal{O}$ may be given explicitly by a basis $\{1 = \omega_1, \omega_2 \ldots \omega_d\}$ and a multiplication table

$$\omega_i \omega_j = \sum_{l=1}^{d} a_{ijl} \omega_l \quad (i, j = 2 \ldots d) \quad \text{with } a_{ijl} \in \mathbb{Z}, \tag{1}$$

satisfying the commutativity and associativity rules.

A *generalized number system* over $\mathcal{O}$ (GNS over $\mathcal{O}$ for short) is a pair $(p, \mathcal{D})$, where $p \in \mathcal{O}[X]$ is a monic polynomial such that $p(0)$ is not a zero divisor of $\mathcal{O}$, and where $\mathcal{D}$ is a (necessarily finite) complete residue system of $\mathcal{O}$ modulo $p(0)$ containing 0.

An element $a \in \mathcal{O}[X]$ is *representable in* $(p, \mathcal{D})$ if there exist an integer $L \geq 0$ and $a_0, \ldots, a_L \in \mathcal{D}$ such that

$$a \equiv \sum_{j=0}^{L} a_j X^j \pmod{p}. \tag{2}$$

The set of in $(p, \mathcal{D})$ representable elements is $R(p, \mathcal{D})$. If $R(p, \mathcal{D}) = \mathcal{O}$ then $(p, \mathcal{D})$ is called *GNS with finiteness property*.

A GNS $(p, \mathcal{D})$ over $\mathcal{O}$ may be viewed as a matrix number system introduced by Vince, 1993, with lattice $\Lambda = \mathcal{O}[x]/(p)$, the linear mapping $\varphi : f \pmod{p} \mapsto x \cdot f \pmod{p}$, and digit set $D = \mathcal{D}$.

We may view $\mathcal{O}[X]$ as a free $\mathbb{Z}[X]$-module of finite rank, and $a \mapsto p \cdot a$ as a $\mathbb{Z}[X]$-linear map from $\mathcal{O}[X]$ to itself. The determinant of this $\mathbb{Z}[X]$-linear map is a monic polynomial in $\mathbb{Z}[X]$, which we denote by Np.

Theorem 1 (Evertse, Győry, Pethő, Thuswaldner, 2019). *Let $(p, \mathcal{D})$ be a GNS over $\mathcal{O}$ with $\deg p = n \geq 1$. Then there is an effectively computable number C'', depending on $\mathcal{O}$, p and $\mathcal{D}$, such that the following are equivalent:*
(i) $(p, \mathcal{D})$ has the finiteness property;
(ii) the polynomial Np is expansive, and every $a \in \mathcal{O}[X]$ with $\|a\| \leq C''$, $\deg a < n$ belongs to $R(p, \mathcal{D})$.

3. Families of GNS

We view $\mathcal{O}$ as a full rank sublattice of the $\mathbb{R}$-algebra $\mathcal{O}\otimes_{\mathbb{Z}}\mathbb{R}$. We recall that *$\theta \in \mathcal{O}$ is not a zero divisor of $\mathcal{O}$ if and only if it is invertible in $\mathcal{O}\otimes_{\mathbb{Z}}\mathbb{R}$.*

A fundamental domain for $\mathcal{O}\otimes_{\mathbb{Z}}\mathbb{R}/\mathcal{O}$ is a subset of $\mathcal{O}\otimes_{\mathbb{Z}}\mathbb{R}$ containing precisely one element from every residue class of $\mathcal{O}\otimes_{\mathbb{Z}}\mathbb{R}$ modulo $\mathcal{O}$. For a fundamental domain $\mathcal{F}$ for $\mathcal{O}\otimes_{\mathbb{Z}}\mathbb{R}/\mathcal{O}$ with $0 \in \mathcal{F}$ and $\theta \in \mathcal{O}$ which is not a zero divisor, we define

$$\mathcal{D}_{\mathcal{F},\theta} := \theta\mathcal{F} \cap \mathcal{O} = \{\alpha \in \mathcal{O} :\ \theta^{-1}\alpha \in \mathcal{F}\}.$$

Lemma 1. *Let $\mathcal{F}$ be a fundamental domain for $\mathcal{O}\otimes_{\mathbb{Z}}\mathbb{R}/\mathcal{O}$ with $0 \in \mathcal{F}$ and $\theta \in \mathcal{O}$ not a zero divisor. Then $\mathcal{D}_{\mathcal{F},\theta}$ is a complete residue system for $\mathcal{O}$ modulo θ containing* 0*.*

If $\mathcal{F}$ is a fundamental domain for $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}/\mathcal{O}$ with $0 \in \mathcal{F}$ and $p \in \mathcal{O}[X]$ runs through the monic polynomials such that $p(0)$ is not a zero divisor then $(p, \mathcal{D}_{\mathcal{F},p(0)})$ is a family of GNS over $\mathcal{O}$.

For example put $\mathcal{O} = \mathbb{Z}$, $\mathcal{F} = [0, 1)$ and $p \in \mathbb{Z}[X]$ with $p(0) > 1$ then $\mathcal{D}_{\mathcal{F},p(0)} = \{0, 1, \ldots, p(0) - 1\}$, thus $(p, \mathcal{D})$ is exactly the CNS.

4. Generalization of SRS

Let $0 \in \mathcal{F}$ be a fundamental domain for $\mathbb{R}^d$. For any $\mathbf{v} \in \mathbb{R}^d$ there exist a unique $\mathbf{a} \in \mathbb{Z}^d$, such that $\mathbf{v} - \mathbf{a} \in \mathcal{F}$, which will be denoted by $\lfloor \mathbf{v} \rfloor_{\mathcal{F}}$.

For fixed matrices $R_1, \ldots, R_n \in \mathbb{R}^{d \times d}$ define the sequence of integer vectors by the initial terms $\mathbf{a}_1, \ldots \mathbf{a}_n \in \mathbb{Z}^d$ and for $m > n$ by the nearly linear recursive relation

$$\mathbf{a}_m = -\left\lfloor \sum_{\ell=1}^{n} R_\ell \mathbf{a}_{m-n+\ell-1} \right\rfloor_{\mathcal{F}}. \tag{3}$$

With the n-tuple $\mathbf{R} = (R_1, \ldots, R_n)$ of matrices define the mapping $\tau_{\mathbf{R}} : \mathbb{Z}^{d\times n} \mapsto \mathbb{Z}^{d\times n}$ such that if $\mathbf{A} = (\mathbf{a}_1, \ldots, \mathbf{a}_n) \in \mathbb{Z}^{d\times n}$ then

$$\tau_{\mathbf{R}}(\mathbf{A}) = (\mathbf{a}_2, \ldots, \mathbf{a}_n, \mathbf{a}_{n+1}), \tag{4}$$

where $\mathbf{a_{n+1}}$ is defined by (3) with $m = n + 1$. The mapping $\tau_{\mathbf{R}}$ is called *generalized SRS, or short GSRS*.

For $k = 1$ identify the matrices $R_1, \ldots, R_n$, with their real entries and $\mathbf{R}$ with a n-dimensional real vector. Similarly $\mathbf{A}$ can be identified with a n-dimensional integer vector. Further in (3) in the bracket stays the inner product of $\mathbf{R}$ and $\mathbf{A}$. Choosing finally $\mathcal{F} = [0, 1)$ we get the familiar definition of SRS.

5. Relation between GNS and GSRS

We show similar relation between GNS and GSRS as between CNS and SRS.

Let $p \in \mathcal{O}[X]$ of degree n be monic, such that $p(0)$ is not a zero divisor and consider the GNS $(p, \mathcal{D})$, where $\mathcal{D} = \mathcal{D}_{\mathcal{F},p(0)}$. Let $a \in \mathcal{O}_n[X]$, where $\mathcal{O}_n[X]$ denotes the elements of $\mathcal{O}[X]$ of degree at most $n-1$.

Let $T_p : \mathcal{O}_n[x] \mapsto \mathcal{O}_n[x]$ be the *backward division mapping*, which is defined as

$$T_p(a)(X) = \frac{a(X) - qp(X) - d}{X},$$

where $d \in \mathcal{D}$ is the unique element of $\mathcal{D}$ with $d \equiv a(0) \pmod{p_0}$ and $q = \frac{a(0)-d}{p_0}$. This means $q = \left\lfloor \frac{a(0)}{p_0} \right\rfloor_{\mathcal{F}}$.

Iterating T_p for h-times we obtain $d_0, \ldots, d_{h-1} \in \mathcal{D}$, and $r \in \mathcal{O}[X]$ such that

$$a(X) = \sum_{j=0}^{h-1} d_j X^j + X^h T_p^h(a)(X) + r(X)p(X). \tag{5}$$

Clearly, $a \in R(p, \mathcal{D})$ if and only if there exists h_0 such that $T_p^h(a) = 0$ for all $h \geq h_0$.

The mapping T_p acts essentially on the coefficient vector $\mathbf{a} = (a_0, \ldots, a_{n-1})$ of $a = \sum_{i=0}^{n-1} a_i X^i$ by the rule

$$T_p(\mathbf{a}) = (a_1 - qp_1, \ldots, a_{n-1} - qp_{n-1}, -qp_n) = T\mathbf{a} - q\mathbf{p},$$

where $q = \left\lfloor \frac{a(0)}{p_0} \right\rfloor_{\mathcal{F}}$, $\mathbf{p} = (p_1, \ldots, p_n)$ and $T = (t_{ij})_{i,j=1,\ldots,n}$ is the matrix with $t_{i,i+1} = 1, i = 1, \ldots, n-1$ and all other entries are zero.

Choosing a different basis for $\mathcal{O}_n[x]$, as in Brunotte (2001) or Scheicher and Thuswaldner (2003)

$$w_j = \sum_{m=1}^{j} p_{n-j+m} X^{m-1},\ j = 1, \ldots, n$$

we get a different form of this transformation. Writing

$$a = \sum_{j=0}^{n-1} a_j X^j = \sum_{j=1}^{n} c_j w_j$$

then

$$T_p(\mathbf{c}) = \left(c_2, \ldots, c_n, -\left\lfloor \mathbf{c}\mathbf{p}' \right\rfloor_{\mathcal{F}}\right),$$

where $\mathbf{c} = (c_1, \ldots, c_n)$ and $p' = \left(\frac{p_n}{p_0}, \ldots, \frac{p_1}{p_0}\right)$.

Now we prove that T_p is a special case of $\tau_{\mathbf{R}}$.

Write $c_j = \mathbf{c}_j(\omega_1, \ldots, \omega_d)$ with $\mathbf{c}_j \in \mathbb{Z}^d, j = 1, \ldots, d$

The multiplication with any fixed element of $\mathcal{O}$ is a linear mapping of $\mathcal{O}$ into itself. As $p(0)$ is not a zero divisor, $1/p(0)$ is a well defined element of $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}/\mathcal{O}$. One can extend the multiplication to $1/p(0)$ such that it is again a linear mapping on $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}/\mathcal{O}$. Thus there exist $M_1, \ldots, M_n \in \mathbb{Q}^{d \times d}$ associated to the multiplication by $p_n/p_0, \ldots, p_1/p_0$. Thus

$$\mathbf{c}\mathbf{p}' = \sum_{j=1}^{n} M_j \mathbf{c_j}, \text{ i.e, } T_p(\mathbf{c}) = \tau_{M_1, \ldots, M_n}(\mathbf{c_1}, \ldots, \mathbf{c_n}).$$

which proves the claim.

Theorem 2. *Let $p \in \mathcal{O}[X]$ be monic and such that $p(0)$ is not a zero divisor. Let $\mathcal{F}$ be, a fundamental domain for $\mathbb{R}^d$. Then $a\mathcal{O}[X]$ is representable in $(p, \mathcal{D}_{\mathcal{F},p(0)})$ if and only if the orbit of $\tau^k_{(M_1,\ldots,M_n)}(\mathbf{c_1}, \ldots, \mathbf{c_n})$ is ultimately zero.*

An example

Let $\mathcal{O} = \sqrt{-7}, \omega_1 = 1, \omega_2 = \frac{1+\sqrt{-7}}{2}, \omega = (\omega_1, \omega_2)$ and $\mathcal{F} = [0,1)^2$. Then

$$\omega_1 \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \omega_2 \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -2 & 1 \end{pmatrix}.$$

Let $p = X + \frac{-1+\sqrt{-7}}{2}$. Then

$$\frac{1}{p(0)} = -\frac{1+\sqrt{-7}}{4} = -\frac{\omega_2}{2}.$$

Hence $\mathcal{D} = \{0, -1\}$ and the matrix associated to the multiplication by $1/p(0)$ is $M = \begin{pmatrix} 0 & -1/2 \\ 1 & -1/2 \end{pmatrix}$.

Finally the searched dynamical system is

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \mapsto \begin{pmatrix} \lfloor -a_2/2 \rfloor \\ \lfloor a_1 - a_2/2 \rfloor \end{pmatrix},$$

where $a_1, a_2 \in \mathbb{Z}$.

6. Closer look at the case $n = 1$

In the case $n = 1$ the GSRS simplifies to

$$\mathbf{a}_m = \tau_R(\mathbf{a}_{m-1}) = -\lfloor R\mathbf{a}_{m-1} \rfloor_{\mathcal{F}}, \text{ for } m \geq 1,$$

where $R \in \mathbb{R}^{d \times d}$ and $\mathbf{a}_0 \in \mathbb{Z}^d$.

Theorem 3. *If all orbits of τ_R are periodic then the spectral radius of R is at most 1, consequently $|\det R| \leq 1$.*

Theorem 4. *If the spectral radius of R is less than 1 then all orbits of τ_R are periodic.*

Notice that the above properties are independent from $\mathcal{F}$. In the sequel $\mathcal{F} = [0, 1)^d$.

What happens when all eigenvalues of R lie on the unit circle?

6.1. Discrete rotation on the plane

We consider the case $n = 1, d = 2$ and $R \in \mathbb{R}^{2\times 2}$, which has two different eigenvalues on the unit circle. (Only ± 1 can be multiple eigenvalues.) A convenient representation of R is

$$R = TA_\varphi T^{-1}, \qquad A_\varphi = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$$

where $T \in \mathbb{R}^{2\times 2}$ is an invertible matrix and $0 \leq \varphi < 2\pi$.

The points $R^k(a, b)^T$, $(a, b) \in \mathbb{Z}^2$ form a **bounded set**; generally they lie on an ellipse, in the case $T = E$, i.e., $R = A_\varphi$ on the unit circle.

Akiyama, Brunotte, Pethő and Steiner (2006) studied the case $n = 2, d = 1$, when $a_{m+1} = -\lfloor \lambda a_m + a_{m-1} \rfloor$ with $|\lambda| < 2$.

We can write

$$\begin{aligned} a_{m+1} &= -\lfloor \lambda a_m + a_{m-1} \rfloor \\ a_m &= -\lfloor -a_m \rfloor. \end{aligned}$$

Putting $R = \begin{pmatrix} \lambda & 1 \\ -1 & 0 \end{pmatrix}$ we obtain

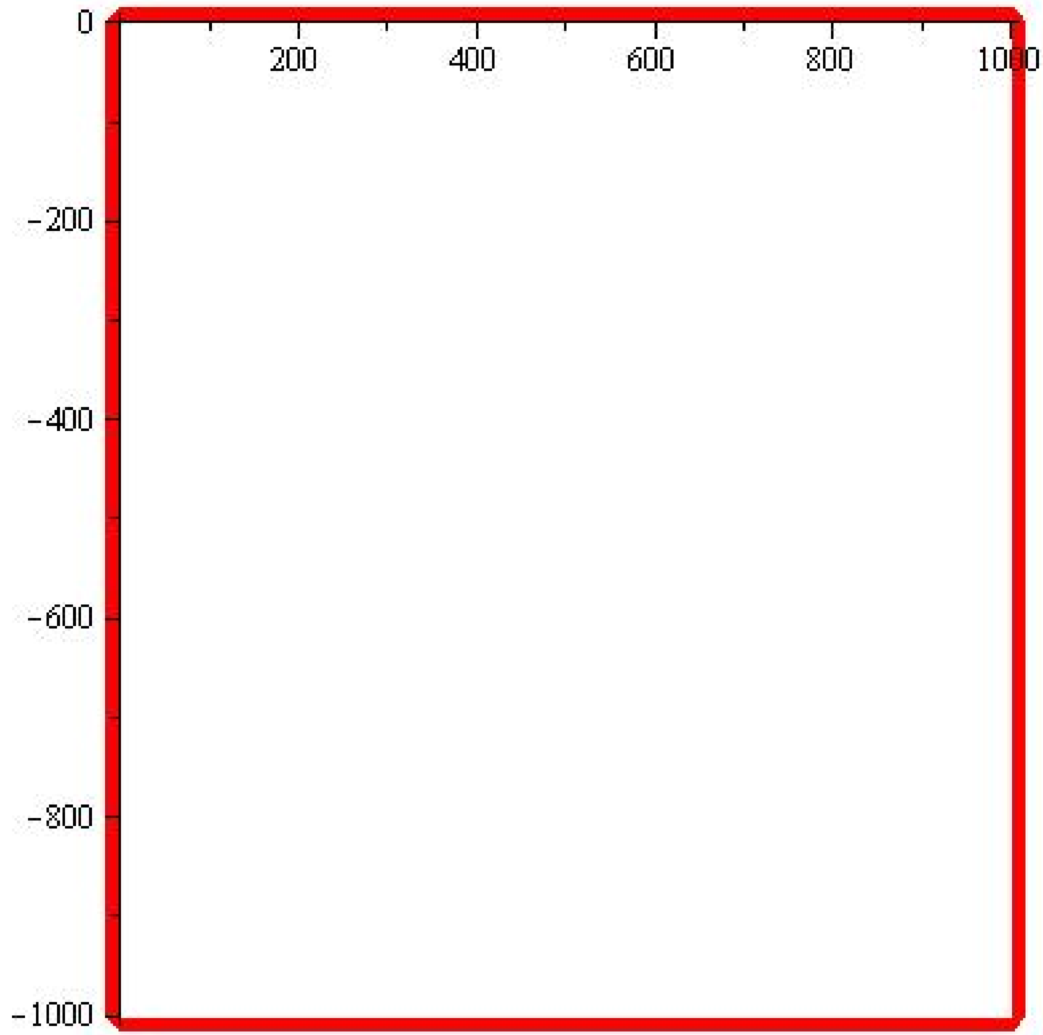
$$\begin{pmatrix} a_{m+1} \\ a_m \end{pmatrix} = -\left\lfloor R \begin{pmatrix} a_m \\ a_{m-1} \end{pmatrix} \right\rfloor.$$

Thus $n = 2, d = 1$ is a special case of $n = 1, d = 2$.

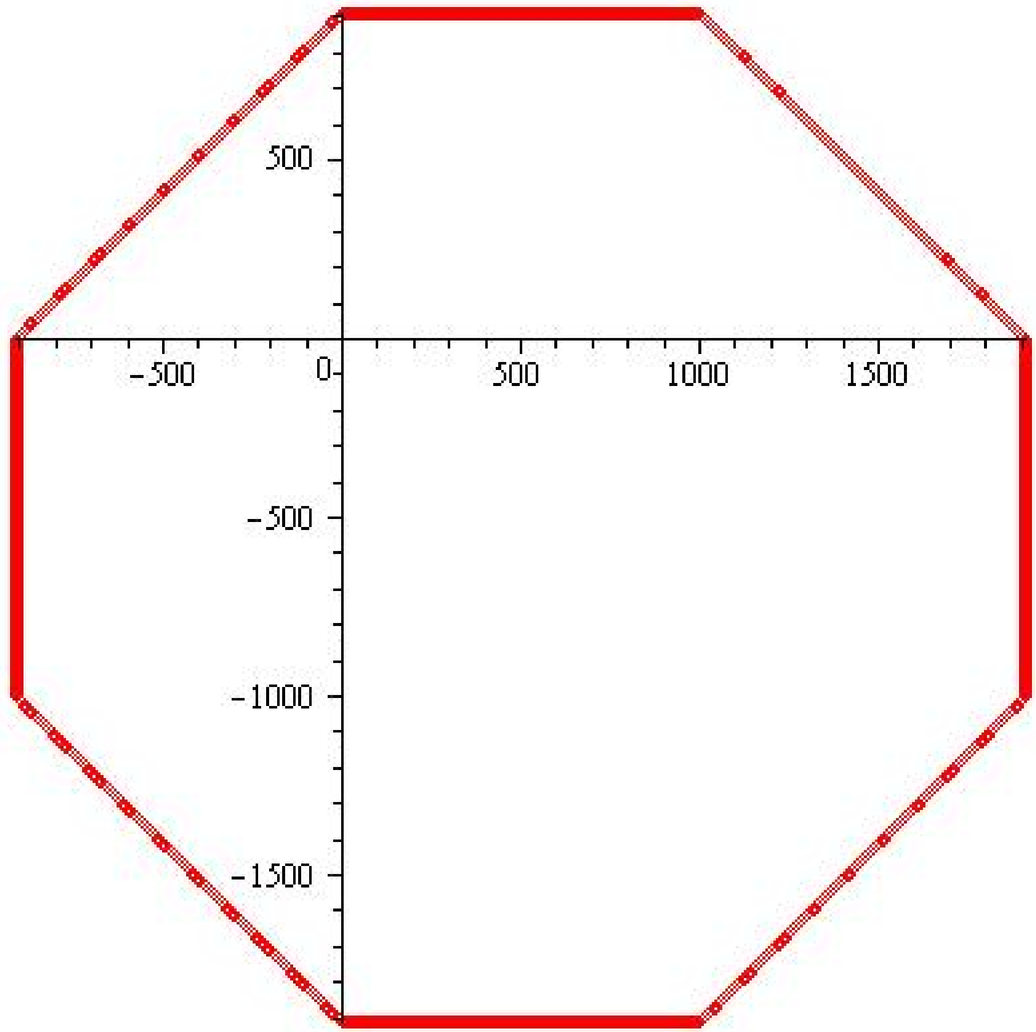
Akiyama et al. conjecture that the sequence (a_m) is always periodic.

In 2008 they verified this conjecture for $\lambda = \pm\sqrt{2}, \pm\frac{1\pm\sqrt{5}}{2}$.

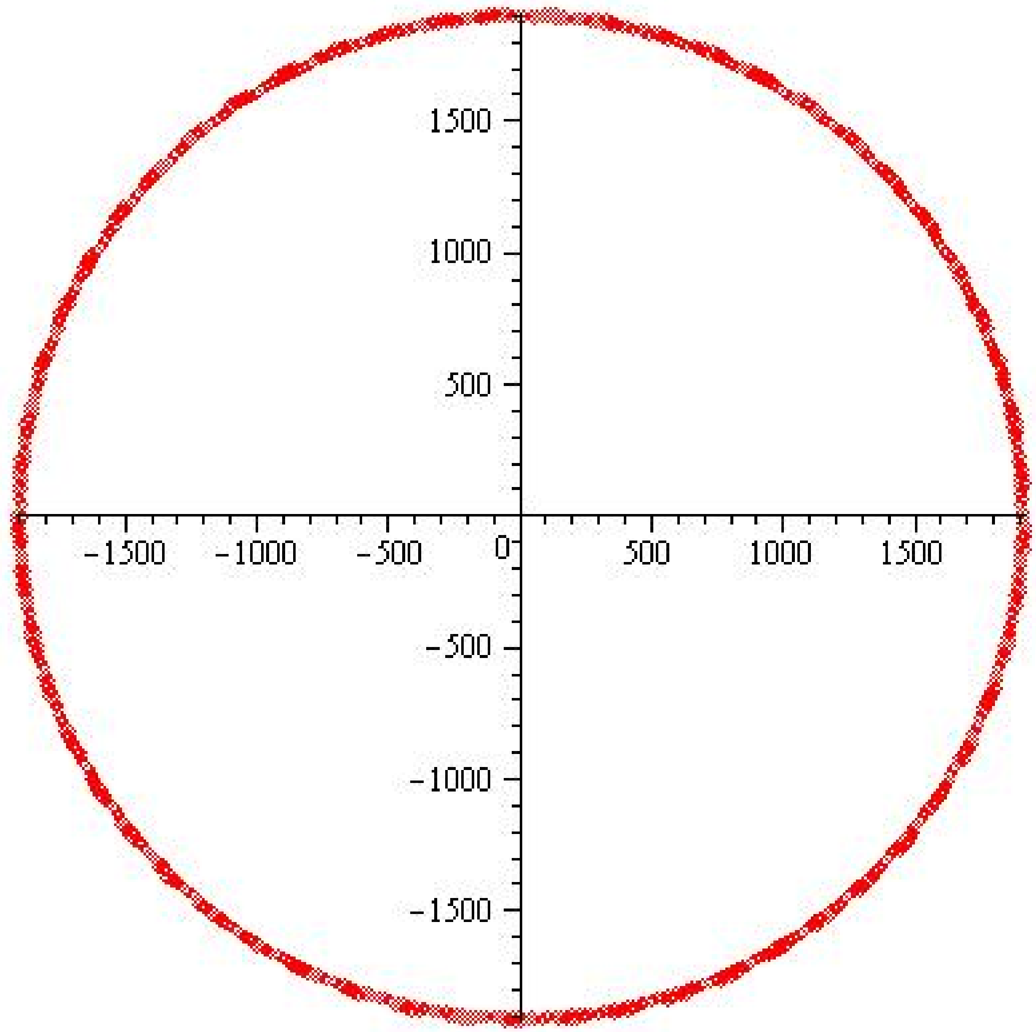
Akiyama and Pethő proved (2013) that for any λ there are infinitely many starting values a_0, a_1 such that (a_m) is periodic.



Staring value $(10, 9), \varphi = 0.001$.



Staring value $(0, 910), \varphi = 0.001$.



Staring value $(1904, 0), \varphi = 0.11.$

Theorem 5. *There are infinitely many* $(a, b) \in Z^2$ *such that the sequence* $\mathbf{x}_0 = (a, b), \mathbf{x}_{m+1} = \lfloor A_{\pi/4}\mathbf{x}_m, m = 0, 1, \ldots$ *is periodic of length* 8.

The proof is tiering computation with the integer part function. Its essence is:

Lemma 2. *Let* $a \in \mathbb{N}$, $\omega = \lfloor \frac{1}{\sqrt{2}} a \rfloor$ *and suppose* $\lfloor \sqrt{2}\omega \rfloor = a - 1$. *If* $\{\frac{1}{\sqrt{2}} a\} \in \left[1 - \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right]$, *and* $\{\sqrt{2}\omega\} \in \left[1 - \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right]$, *then* $A_\varphi^8(a, 0) = (a, 0)$.

Thank you for the attention!