Tadeusz Pezda
On cycles and orbits of polynomial mappings $\mathbb{Z}^2 \rightarrow \mathbb{Z}^2$


**Terms of use:**

© University of Ostrava, 2002

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use.*

This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* [http://project.dml.cz](http://project.dml.cz)
On cycles and orbits of polynomial mappings $Z^2 \rightarrow Z^2$

T. Pezda

1. Introduction

For a commutative ring $R$ with unity and $\Phi = (\Phi^{(1)}, \ldots, \Phi^{(N)})$, where $\Phi^{(i)} \in R[X_1, \ldots, X_N]$, we define a cycle for $\Phi$ as a $k$-tuple $x_0, x_1, \ldots, x_{k-1}$ of different elements of $R^N$ such that

$$\Phi(x_0) = x_1, \Phi(x_1) = x_2, \ldots, \Phi(x_{k-1}) = x_0.$$

The number $k$ is called the length of this cycle.

We denote $\text{CYC}(R, N)$ as the set of all possible cycle lengths for polynomial mappings in $N$ variables with coefficients from $R$. We put $B(R, N)$ as the maximal element in $\text{CYC}(R, N)$ (if there is no such maximal element we put $B(R, N) = \infty$).

For $x \in R^N$ and $\Phi : R^N \rightarrow R^N$ we define the orbit

$$\text{ORB}(x, \Phi) = \{x, \Phi(x), \Phi^2(x), \ldots\}.$$

We call the orbit $\text{ORB}(x, \Phi)$ finite if it is a finite set.

Define $\text{ORB}(R, N)$ as the maximal number of elements of finite orbits $\text{ORB}(x, \Phi)$

with $x \in R^N$, and $\Phi = (\Phi^{(1)}, \ldots, \Phi^{(N)})$ with $\Phi^{(i)} \in R[X_1, \ldots, X_N]$. If there is no such number we put $\text{ORB}(R, N) = \infty$.

In 1998 W. Narkiewicz asked whether $B(Z, 2) \geq 7$. In this paper we shall give the positive answer to this question. Moreover, the set $\text{CYC}(Z, 2)$ will be completely determined.

As to orbits in $[N]$ it was shown that $\text{ORB}(Z_K, 1) < \infty$ where $Z_K$ is the ring of integers in a finite extension $K$ of $Q$. Moreover, it was shown that $\text{ORB}(Z, 1) = 4$.

Received: November 23, 2001.
2000 Mathematics Subject Classification: 11R04, 11S05.
2. Results

Theorem 2.1. \( \text{CyCC}(Z, 2) = \{24, 18, 16, 12, 9, 8, 6, 4, 3, 2, 1\} \).
So, in particular \( B(Z, 2) = 24 \).

Theorem 2.2. \( \text{ORB}(Z, 2) = \infty \). So, it follows that \( \text{ORB}(R, N) = \infty \) for \( R \), a ring of zero characteristic with unity and \( N \geq 2 \) (as \( Z \) can be embedded into \( R \)).

3. Auxiliary results and some notations

3.1. The main auxiliary theorem

Proposition 3.1. ([PcS]) Let \( R \) be a Dedekind domain. Let \( \mathcal{P}(R) \) denote the set of all non-zero prime ideals of \( R \). If \( N \geq 2 \) then

\[
\text{CyCC}(R, N) = \bigcap_{\mathfrak{p} \in \mathcal{P}(R)} \text{CyCC}(R_{\mathfrak{p}}, N) = \bigcap_{\mathfrak{p} \in \mathcal{P}(R)} \text{CyCC}(\widehat{R}_\mathfrak{p}, N),
\]

where \( \widehat{R}_\mathfrak{p} \) is the completion of \( R_{\mathfrak{p}} \) with respect to the obvious valuation. In particular, it holds for the rings of integers in finite extensions of \( Q \).

3.2. Cycles in some local domains

Owing to the proposition 3.1, it is useful to recall some results concerning cycles in discrete valuation domains.

In this subsection let \( R \) be a discrete valuation domain of characteristic zero, \( P \) is the unique maximal ideal of \( R \). We assume that the quotient field \( R/P \) is finite and has \( N(P) = p^e \) elements (\( p \) is prime). Let \( \pi \) be a generator of the principal ideal \( P \) and let \( v \) be the norm of \( R \), normalized so that \( v(\pi) = 1 \). By \( w \) we denote the corresponding exponent, defined by \( w(x) = \frac{\log v(x)}{\log p} \) for \( x \neq 0 \) and \( w(0) = \infty \).

We extend \( v \) and \( w \) to \( R^N \) by putting

\[
v(x) = v((x_1, \ldots, x_N)) = \max\{v(x_i), i = 1, \ldots, N\}
\]

and

\[
w(\bar{x}) = w((x_1, \ldots, x_N)) = \min\{w(x_i), i = 1, \ldots, N\}.
\]

The congruence symbol \( x \equiv y \pmod{P^d} \) will be used for vectors \( x, y \) in \( R^N \) to indicate that corresponding components are congruent \( \pmod{P^d} \), or equivalently \( w(x - y) \geq d \).

Denote the image of some \( \bar{x} \in R^N \) under the canonical mapping \( R^N \rightarrow R^N/P^N = (R/P)^N \) by \( x + P^N \).

A cycle \( x_0, \ldots, x_{k-1} \) will be called a \((\ast)\)-cycle if for all \( i, j \) one has \( w(x_i - x_j) \geq 1 \).

Definition 3.2. A \((\ast)\)-cycle \( x_0, \ldots, x_{k-1} \) with \( k \geq 2 \) we call normalized provided \( x_0 = 0 \) and \( w(x_1) = 1 \).

Proposition 3.3. If there is a \((\ast)\)-cycle in \( R^N \) of length \( k \geq 2 \) then there exists a normalized \((\ast)\)-cycle in \( R^N \) of the same length.
Proof. Let a k-tuple $x_0, x_1, \ldots, x_{k-1}$ be a (*)-cycle in $\mathbb{R}^N$ for a mapping $\Phi$. Then the k-tuple $0, x_1 - x_0, \ldots, x_{k-1} - x_0$ forms a (*)-cycle of length $k$ for a mapping $\Psi(X) = \Phi(X + x_0) - x_0$, which is a polynomial mapping with coefficients from $F$.

So without any loss of generality we can assume that $x_0 = 0$. Put $w(x_i) = d_i > 1$. Then the vectors $0, x_1 - x_0, \ldots, x_{k-1} - x_0$ form a (*)-cycle of length $k$ for $\Psi((X) = d_i x_i$, which is a polynomial mapping with coefficients from $\mathbb{R}$ as $\Psi(0) = x_0 = 0 \in \mathbb{R}^N$.

The cosets of elements of $\mathbb{R}^N$ (mod $P$) consist a linear space over $\mathbb{R}/P$ and $\text{Lin}(S)$ means a linear space spanned on a set $S$ as a linear subspace of $(\mathbb{R}/P)^N$.

For a cycle $x_0, x_1, \ldots, x_{k-1}$ we sometimes extend the indices by putting $x_k = x_0, x_{k+1} = x_1, \ldots$, and so on.

Proposition 3.4. (Pe3) Let $0, x_1, \ldots, x_{k-1}$ be a (*)-cycle in $\mathbb{R}^N$ (i.e. for a suitable polynomial mapping with coefficients from $F$). Then one has that $w(x_m) < w(x_n)$ for $m \neq n$ (also for $m, n > k$).

Proposition 3.5. (Pe3) Let $0, x_1, \ldots, x_{k-1}$ be a (*)-cycle in $\mathbb{R}^N$ for $\Phi$. Put $\Phi(0) = 0$. Write

$$w(x_i), \ldots, w(x_{k-1}) = \{d_1 < d_2 < \cdots < d_r\} \quad \text{and} \quad m_i = \min \{j : w(x_j) = d_i\}.
$$

Then $1 = m_1[m_2] \cdots m_r[k]$ and

$$\min = \min \{i : (1 + A_{m_1} + \cdots + A_{m_r}) w_{m_i} = 0 \pmod{P}\} \quad \text{for} \quad i = 1, 2, \ldots, r \quad \text{where we put} \quad m_{r+1} = k.
$$

Moreover, for $i = 1, \ldots, r$ we have $\frac{m_i}{m_{i+1}} \leq P^{N}$ and

(3.1) $(1 + A^{m_1} + \cdots + A^{(m_1-1)m_i})|_{\text{Lin}(e_{2m_1} + PRN, e_{2m_2} + PRN, \ldots)} = 0$

and

(3.2) $(1 + A^{m_1} + \cdots + A^{(m_1-1)m_i})|_{\text{Lin}(e_{2m_1} + PRN, e_{2m_2} + PRN, \ldots)} = 0$

So in particular

$$(A_{m_1} + I)|_{\text{Lin}(e_{2m_1} + PRN, e_{2m_2} + PRN, \ldots)} = 0 \quad \text{and} \quad (A_{m_1} + I)|_{\text{Lin}(e_{2m_1} + PRN, e_{2m_2} + PRN, \ldots)} = 0.
$$

Proof. From the very definition of the numbers $m_i$ we have that the cosets $0, x_{m_i} + PRN, \ldots, x_{m_i} + PRN$ are all different (mod $P$). So $\frac{m_i}{m_{i+1}} \leq P^{N}$.

The formula (2) follows from (1) and the following formula (which could be derived from the Taylor's expansion)

$$\pi d \in [m_i]_{m_{i+1} - 1} = 0 + PRN.
$$

The rest was proved in [Pe3].

Proposition 3.6. (Pe3) Let $\Phi : R^N \rightarrow R^N$ be a polynomial mapping with, as always, coefficients from $F$. Put $\Phi(0) = 0, w(x) = d, \Phi(0) = A$. Then $\Phi(0) = (A^{m_1} + A^{m_2} + \cdots + A + I)|_{\text{Lin}(e_{2m_1} + PRN, e_{2m_2} + PRN, \ldots)} = 0$.
Let \( Q(R/P, M) \) denote the set of orders prime to \( p \) of cyclic subgroups of the linear group \( GL_M(R/P) \) of invertible matrices \( M \times M \) with coefficients from the field \( R/P \).

Let \( H(R/P, M) \) denote the set of orders prime to \( p \) of elements \( A \in GL_M(R/P) \) such that for some \( y \in (R/P)^M \), the vectors \( y, Ay, A^2y, \ldots \) span the whole \( (R/P)^M \).

**Proposition 3.7.** ([Pe3]) Let \( R \) be as above. Then

(a) the length of a polynomial cycle in \( R^n \) can be written in the form \( ab \), where \( a \) is the length of a certain \((*)\)-cycle in \( R^n \) and \( b \leq p^N \). Conversely, every number of that form is a length of a suitable cycle in \( R^n \). As \( 1 \)-tuple \( 0 \) forms a \((*)\)-cycle for zero mapping we have in particular:

\[ \{1, 2, \ldots, p^N\} \subseteq CYC(R, N); \]

(b) the length of a \((*)\)-cycle for a polynomial mapping in \( R^n \) is of the form:

\[ p^a \prod_{i=1}^b h_i, \]

where \( h_i \in H(R/P, l_i), l_1 + \cdots + l_t \leq N \);

(c) Let \( \tilde{R} \) be the completion of the ring \( R \) with respect to the norm \( v \). Then \( CYC(R, N) = CYC(\tilde{R}, N) \).

**Remark 3.1.** For every ring \( S \) we have that \( k \in CYC(S, N) \) implies \( l \in CYC(S, N) \) for every divisor \( l \) of \( k \) (it suffices to take a suitable iteration).

**Proposition 3.8.** ([Pe2]) If \( \tilde{x}_0, \ldots, \tilde{x}_{k-1} \) is a cycle in \( R^n \) then \( w(\tilde{x}_{i+j} - \tilde{x}_i) = w(\tilde{x}_{i+j} - \tilde{x}_j) \) for every possible \( i, j, l \), even bigger than \( k \).

4. **Proof of Theorem 2.1**

Owing to proposition 3.1 we have

\[ CYC(Z, 2) = \bigcap_p CYC(Z_p, 2), \]

where \( Z_p \) is the \( p \)-adic ring.

In what follows we put \( \tilde{x}_k = (x_{i_k}) \). So \( x_k \) is the first coordinate of \( \tilde{x}_k \).

For \( p = 2 \) we try to find the shape of a \((*)\)-cycles in \( Z_2^2 \). In this case we apply the results of subsection 3.2 to \( R = \mathbb{Z}_2, P = 2\mathbb{Z}_2, \pi = 2. \) Note that in this case \( G(R/P, 2) = \{1, 3\} \) and \( G(R/P, 1) = \{1\} \). This gives, by proposition 3.6 that \((*)\)-cycles in \( Z_2^2 \) could have lengths only of the form \( 2^a \cdot 3 \cdot 2^b \).

Note that a tuple \( (\tilde{x}, \tilde{y}), (\tilde{z}, \tilde{w}), (\tilde{v}, \tilde{t}) \) is a \((*)\)-cycle of length 4 for \( \Phi(x, y) = (-y, x) \).

On the other hand a tuple \( (\tilde{x}, \tilde{y}), (\tilde{z}, \tilde{w}), (\tilde{v}, \tilde{t}) \) is a \((*)\)-cycle of length 6 for \( \Phi(x, y) = (-y, x + y) \).

Note that two just mentioned \((*)\)-cycles of length 4, 6 are suitable for every discrete valuation ring of characteristic zero with unity.

**Lemma 4.1.** There are no \((*)\)-cycles of length 12 in \( Z_2^2 \).
Proof. Assume a contrary. By proposition 3.2 we then have a normalized (*)-cycle \(0, \ldots, x_1\) for a suitable \(\Phi\). Put \(\Phi'(0) = A\) and \(\pi = 2\). Let \(m_1, m_2, \ldots, m_r, d_1, \ldots, d_r, k\) be as in the proposition 3.4. So \(k = 12, m_2 \leq 4\) and therefore \(r \geq 2\).

1st case. \(m_2 \in \{2, 4\}\). In this case \(3\frac{A}{m_2} = m_2, \ldots, A_{m_2}\) and all the quotients are \(\leq 4\) (by proposition 3.4) we have that there is unique \(i > 2\) such that \(3 = m_2^i + 1\).

Again by proposition 3.4 we have

\[(A^{2m_2} + A^{m_2} + I)\pi^{-d_2} x_{m_2} \equiv 0 \pmod{P}\]

But \(\pi^{-d_2} x_{m_2} + 2Z_2, \pi^{-d_2} x_{2m_2} + 2Z_2\) are non-zero, distinct and hence linearly independent over \(R/P = Z_2\). Hence \(A^{2m_2} + A^{m_2} + I \equiv 0 \pmod{P}\), i.e. it is a zero mapping, treated as a linear mapping of \((R/P)^2\).

By raising to the power 4, in view of the divisibility of suitable binomial coefficients by 2 (which is an element of \(P = 2Z_2\)), we get that \(A^{8m_2} + A^{4m_2} + 1 \equiv 0 \pmod{P}\).

By proposition 3.5, \((A^3 + A^2 + A + I)\pi x_1 = x_2 \equiv 0 \pmod{4}\) and hence \((A^3 + A^2 + A + I)\pi x_1 = 0 \pmod{2}\), whence \(A^{3} x_1 = x_1 \pmod{2}\) (mod 2).

Hence we obtain \((A^{2m_2} + A^{m_2} + I)\pi x_1 \equiv 3 \cdot \frac{1}{2}x_1 \neq 0 \pmod{2}\), a contradiction.

2nd case. \(m_2 = 3\). In this case by proposition 3.4 \((A^2 + A + I)\pi x_1 = x_2 \equiv 0 \pmod{2}\) and hence \((A^2 + A + I)\pi x_1 = 0 \pmod{2}\), whence \(A^{2} x_1 = x_1 \pmod{2}\) (mod 2).

Hence we obtain \((A^{2m_2} + A^{m_2} + I)\pi x_1 = 3 \cdot \frac{1}{2}x_1 \neq 0 \pmod{2}\), a contradiction.

Notice that the remark 3.1 now gives that in \(Z_2^2\) there are no (*)-cycles of length 24, 36, 48, ...
Sy + C2X + Dxy + e2;y2 + ... Furthermore m1,7712, ... ,di,... are defined in the similar manner like in lemma 4.1.

As r and m < 4 we have r = 6 {2,4}.

First case. m = 4. Since in this case x| 4 - PR, x| 4 - PR' are linearly independent over R/P, the matrix S = (\langle x, x \rangle) with entries from R = Z2 is invertible.

Then 0, B-2z, ... , B-2 are a (*)-cycle for P-1 o B with coefficients from i?. Moreover, note that w(B-2z) = w(x), so m1 is preserved.

Hence we can assume that x| (-), x| (.) •

As |x|, |T2, .., 3 are pairwise incongruent (mod P) we must have |x| = (1) (mod P). So \( z = g \) (mod P). From proposition 3.5 we have (*) = (1 ! A) (mod P') (mod P'). This gives (*) = (*/ A) \( \otimes \) (mod P') and a = 1 (mod P).

In the similar manner x| = (') = (1 + A - A) (mod P') and by easy calculation 1 \* E 0 (mod P), 6 = 1 (mod P).

So \( \forall \alpha = (j J J) (mod P') \).

If * = \( \otimes \) \( P^{**} = 2X1 \) then \# \* (,, ) (,, f, * ) (mod P').

Now

\[
\left( \begin{array}{c}
\alpha + dy_1 + dx_1 \\
\gamma + dy_2 + dx_2 \\
\delta + dy_3 + dx_3 \\
\epsilon + dy_4 + dx_4
\end{array} \right) = \left( \begin{array}{c}
\alpha + dy_1 \\
\gamma + dy_2 \\
\delta + dy_3 \\
\epsilon + dy_4
\end{array} \right) + \left( \begin{array}{c}
0 + dx_1 \\
0 + dx_2 \\
0 + dx_3 \\
0 + dx_4
\end{array} \right)
\]

Hence, by proposition 3.5 and w(x) > 2 we have 0 = x| = 1 + (S)?(0)212, (mod P'-1) \( \alpha \cdot d \)

0 S 1 d 1 \( (2\times) \) (mod p*(a)+2) \( \beta \) (mod P') in such a way that P is invertible.

2nd case. m = 2 As in the case m = 4 we can assume that 2i = Q (more strictly in the reasoning from the case m = 4 we take P(J) = |x| and we determine B(r') in such a way that P is invertible).
In view of $w(x^2) > 2$ and proposition 3.5 we have $0 = x^2 \equiv (1 + A)(\beta)$ (mod $P^2$) and $\alpha \equiv 1$ (mod $P$), $\gamma \equiv 0$ (mod $P$). Write $\alpha = 1 + 2\alpha, \gamma = 2\Gamma$. Proposition 3.7 gives $x_1 \equiv x_1 \equiv (\beta)$ (mod $P^2$).

Taking this into account we get

$$\Phi'(0) = \Phi'(x_3) \circ \Phi'(x_2) \circ \Phi'(x_1) \circ \Phi'(0) \equiv (\Phi'(x_1) \circ \Phi'(0))^2 \equiv$$

$$\left(1 + 2\alpha \beta + 2\delta \right)^2 \left(1 + 2\alpha \beta \delta + 2\delta^2 \right) \left(1 + \beta^2 + 2\delta \beta \right) \left(1 + \beta^2 + 2\delta \beta \delta \right) \quad (\text{mod } P^2).$$

From $w(x_2) \geq w(x_3) \geq 2$ and proposition 3.5 we have $0 = x_3 \equiv (I + (\Phi'(0)^2))x_4$ (mod $P^{w(x_4)} + 2$). So, we then have

$$x_4 = 0 \quad (\text{mod } P^{w(x_4)} + 2).$$

If in (3) we take $\delta \equiv 1$ (mod $P$) then we get $2x_4 \equiv 0$ (mod $P^{w(x_4)} + 2$), which leads to a contradiction.

If in (3) we take $x_4 \equiv \beta$ (mod $P^{w(x_4)} + 2$) then from $x_4 \equiv 0$ (mod $P^{w(x_4)}$) we get $1 + \beta^2 \equiv 0$ (mod $P$) and $\delta \equiv 1$ (mod $P$), what is impossible according to the previous reasoning.

So we must have $x_4 \equiv 0$ (mod $P^{w(x_4)} + 1$) and $\delta \equiv 0$ (mod $P$). Now (3) leads to $(2 + 2\beta^2)x_4 + 3y_3 \equiv 0$ (mod $P^{w(x_4)} + 2$). If we subtract from the first congruence the second multiplied by $\beta$ we get $2x_4 \equiv 0$ (mod $P^{w(x_4)} + 2$) and $x_4 \equiv 0$ (mod $P^{w(x_4)} + 2$). Hence $x_4 \equiv 0$ (mod $P^{w(x_4)} + 2$), a contradiction.

So we have obtained that an ($\ast$)-cycle of length $k$ exists in $Z_2^2$ if and only if $k = 1, 2, 3, 4, 6$. Now proposition 3.6(i) gives that a cycle of length $k$ exists in $Z_2^2$ if and only if $k \in \{1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24\}$.

To obtain the theorem 2.1 by remark 3.1 it suffices to show that for every prime $p \geq 3$ there are cycles of lengths $6, 4, 24, 18, 16$ in $Z_2^2$ (see the examples just before lemma 4.1) we arrive at the statement as $3, 4 \leq p^2$.

5. Proof of Theorem 2.2

We start with an auxiliary lemma:

**Lemma 5.1.** For every natural $n$ there are polynomials $f, g \in Z[T, X]$ and non-zero $m \in Z[T]$ such that

$$f(T, X)T^{2n+1} - \prod_{k=0}^{n-1}((XT)^{2^{k+1}-2^k} - 1) + g(T, X) \prod_{k=0}^{n-1}(X^{2^{k+1}-2^k} - 1) \equiv m(T).$$

**Proof.** The polynomials $T^{2n+1} - \prod_{k=0}^{n-1}((XT)^{2^{k+1}-2^k} - 1)$ and $\prod_{k=0}^{n-1}(X^{2^{k+1}-2^k} - 1)$ are coprime when treated as polynomials of variable $X$ over a field $Q(T)$. The rest is obvious.
To finish the proof of theorem 2.2 take fixed $s$ such that $m(s) \neq -1,0,1$ and $b = m(s)$. Now consider $(X, Y) = (X^2 - g(s, b)X(X - b)(X - b^2) \ldots (X - b^{2^{s - 1}}) - f(s, b)Y(Y - bs)(Y - b^2s^2) \ldots (Y - b^{s - 1}s^{s - 1}), Y^2 - s^{2^{s - 1}}g(s, b)X(X - b) \ldots (X - b^{2^{s - 1}}) - s^{2^{s - 1}}f(s, b)Y(Y - bs)(Y - b^2s^2) \ldots (Y - b^{s - 1}s^{s - 1})).$

An easy calculation gives $\Phi^j(b, bs) = (b^{2^j}, b^{2^j}s^{2^j})$ for $j = 0, 1, \ldots, n$ and $\Phi^{n+1}(b, bs) = \Phi^{n+2}(b, bs) = \cdots = (0, 0)$. From this we have $\#\mathcal{ORB}((b, bs), \Phi) = n+2$, as $b \neq -1,0,1$. As $n$ could be sufficiently large we arrive at the statement of the theorem.

References


Department of Mathematics, University of Wroclaw, Pl. Grunwaldzki 2/4, 50–384 Wroclaw, Poland
E-mail address: pezdafflmath.uni.wroc.pl