Publ. Math. Debrecen
56 / 3-4 (2000), 405–414

Scarcity of finite polynomial orbits

By F. HALTER-KOCH (Graz) and W. NARKIEWICZ (Wrocław)

To Professor Kálmán Győry on his 60th birthday

Abstract. Let R be a finitely generated integral domain of zero characteristics. If the index of the group of units of R in the group of units of the integral closure of R is finite then R contains only finitely many inequivalent finite non-linear polynomial orbits. This applies in particular to all integrally closed domains.

1. Let R be an integral domain and $R^\times$ its group of units. For $n \geq 1$, a finite sequence

$$\bar{x} = \{x_0, x_1, \ldots, x_n\} \tag{1}$$

of elements $x_i \in R$ will be called a *polynomial sequence* (of *length* n) if there exists some polynomial $f \in R[X]$ such that for $i = 0, 1, 2, \ldots, n-1$ one has

$$f(x_i) = x_{i+1}. \tag{2}$$

In this case we say that (1) is a sequence of the polynomial f. A polynomial sequence (1) is called *linear* if it is a sequence of a linear polynomial, otherwise it is called *non-linear*. It has been observed in [HKN2] that a sequence (1) is a polynomial sequence if and only if the

Mathematics Subject Classification: 11C08, 11R09, 12E05, 58F08, 58F20.
Key words and phrases: polynomial mappings, integral domains, polynomial orbits, finitely generated rings, unit equations.

Lagrange interpolation polynomial (of degree at most $n-1$) satisfying (2) has its coefficients in R.

A polynomial sequence (1) is called a *finite orbit* if the elements $x_0, x_1, \dots, x_{n-1}$ are all distinct and $x_n = x_i$ holds for some $i < n$; if moreover $i = 0$ then (1) is called a *cycle*. By definition every finite orbit contains a unique cycle. A cycle of length 1 of a polynomial f is just a fixpoint of f.

Observe that if (1) is a polynomial sequence or an orbit or a cycle, $a \in R$ and $\epsilon \in R^{\times}$, then the sequence

$$\bar{y} = \{a + \epsilon x_0, a + \epsilon x_1, \dots, a + \epsilon x_n\}$$

is again a polynomial sequence, an orbit or a cycle, respectively. In such case we shall call the sequences $\bar{x}$ and $\bar{y}$ *equivalent*.

2. A cycle (1) is called *normalized* if $n \geq 2$, $x_0 = 0$ and $x_1 = 1$. It has been established in [HKN2] that if R is a finitely generated domain of zero characteristic then there can be only finitely many normalized cycles in R. The proof given there is essentially based on the existence of a uniform bound, depending only on R and n, for the cardinality of the set of non-trivial solutions of the unit equation

$$a_1 u_1 + a_2 u_2 + \dots + a_r u_r = b \tag{3}$$

(with arbitrary fixed non-zero $a_1, a_2, \dots, a_r, b \in R$) in such rings, a solution being called non-trivial if none of subsums of the left hand-side vanishes. In the case of finitely generated integral domains of zero characteristic this is assured by results of K. Győry, J. H. Evertse and H. P. Schlickewei ([EG], [S]) and if we assume that this condition is satisfied in a ring R of positive characteristic then the argument given in [HKN2] works, provided the characteristic is not equal to 2 or 3.

The purpose of this note is twofold. First we shall show that the arguments given in [HKN2] can be modified so that they work for rings of arbitrary characteristic, provided there is a uniform bound for the number of solutions of (3) in R in the cases $r = 2, 3$ and 5 (this is obviously satisfied if $R^{\times}$ is finite). Secondly we shall show that if R is a finitely generated domain of zero characteristic and the index of the group of units of R in the group of units of its integral closure is finite then there are only finitely many inequivalent non-linear finite polynomial orbits in R.

Theorem 1. *Let R be an integral domain and assume that for every non-zero $b \in R$ each of the equations*

$$x_1 + bx_2 = 1 \tag{4}$$

$$b(x_1 + x_2) + x_3 = 1 \tag{5}$$

$$x_1 + x_2 + x_3 + x_4 + x_5 = 1 \tag{6}$$

has only finitely many non-trivial solutions $x_i \in R^\times$. Then there are only finitely many normalized cycles of a given length n in R.

We recall first certain simple properties of normalized cycles which will be used in the sequel. For the proof of Lemma 1 (i)–(iv) see Lemma 12.8 and its corollaries in [N] and the assertion (v) is trivial (cf. [HKN2]).

Lemma 1. *Let (1) be a normalized cycle in an integral domain R. For any integer i put $x_i = x_r$ if r is the smallest non-negative residue of i modulo n.*

(i) *For all i we have $x_{i+1} - x_i \in R^\times$.*

(ii) *If $i \mid j$ then $x_i \mid x_j$.*

(iii) *If n does not divide $r - s$ then $(x_r - x_s)/x_{r-s} \in R^\times$.*

(iv) *If $(k, n) = 1$ then $x_k \in R^\times$.*

(v) *If $r \mid n$ and $r < n$ then*

$$\left(0, 1, \frac{x_{2r}}{x_r}, \frac{x_{3r}}{x_r}, \ldots, \frac{x_{n-r}}{x_r}, 0\right)$$

and

$$\left(0, 1, \frac{x_{1+2r} - 1}{x_{1+r} - 1}, \frac{x_{1+3r} - 1}{x_{1+r} - 1}, \ldots, \frac{x_{1+n-r} - 1}{x_{1+r} - 1}, 0\right)$$

are normalized cycles of length n/r in R.

Lemma 2 ([HKN2]). *Let R be an integral domain in which the equation (5) has for $b = 1$ only finitely many non-trivial solutions in $R^\times$. If a non-zero element $a \in R$ has at least two distinct representations as a sum of two units, then the principal ideal aR lies in a finite set of principal ideals of R.*

Lemma 3 ([HKN2]). *Let R be an integral domain in which each equation* (5) *has only finitely many non-trivial solutions in $R^\times$. Then there are only finitely many normalized cycles of length $n \geq 3$ in R in which one of the elements $x_2, x_3, \ldots, x_{n-1}$ is fixed.*

Lemma 4 ([HKN2]). *Let R be a domain in which each equation* (4) *has only finitely many solutions in $R^\times$. For every non-zero principal ideal aR of R there exists a finite set $E \subset R$ with the following property: if* (1) *is a normalized cycle of length $n \geq 2$ and $x_2 R = aR$ then $x_2 \in E$.*

3. Now we can prove the theorem. One argues by recurrence and since the assertion is trivially true for $n = 2$ assume it to be true for all integers smaller than n. If n is not twice an odd prime then one can simply repeat the arguments from [HKN2] given there in cases (a) to (d), where the characteristic of R is irrelevant.

So let (1) be a cycle of length $n = 2p$ with prime $p > 2$ and assume that the assertion holds for cycles of length p. Lemma 1 (i) shows that

$$\alpha = x_2 - 1, \beta = x_3 - x_2, \gamma = x_4 - x_3$$

lie in $R^\times$ and the inductional assumption and Lemma 1 (v) imply that the ratio $\lambda = x_4/x_2$ lies in a fixed finite set. Observe now that λ is invertible. Indeed if a is a solution of the congruence $4a \equiv 2 \bmod 2p$ then by Lemma 1 (ii) we get $x_4 \mid x_{4a} = x_2$ and $x_2 \mid x_4$.

We have to consider two cases. First assume that the element x_3 is invertible. Then

$$x_3 - \alpha - \beta = 1$$

and if this equality is non-trivial then x_3 lies in a fixed finite set and it suffices to apply Lemma 3 to get the assertion. Otherwise one of the summands must be equal to 1 and since $x_3 = 1$ and $\alpha = -1$ (which implies $x_2 = 0$) are both impossible, we must have $x_3 - x_2 = \beta = -1$ which leads to

$$x_2 = \lambda^{-1} x_3 + \lambda^{-1}\gamma = x_3 + 1.$$

If these two representations of x_2 as sums of two units are distinct then $x_2 R$ lies in a finite set by Lemma 2, thus x_2 lies in a finite set by Lemma 4 and the assertion follows by Lemma 3. Otherwise one has either $\lambda^{-1} x_3 = x_3$, implying $\lambda = 1$ and $x_2 = x_4$ which is not possible, or $\lambda^{-1} x_3 = 1$, giving

$x_3 = \lambda$ and since λ lies in a finite set it suffices to use Lemma 3. This settles the case $x_3 \in R^\times$.

Now assume that x_3 is not invertible. Then Lemma 1 (iv) implies that $n = 6$ and x_5 is invertible by Lemma 1 (iv). Lemma 1 (v) and the inductional assumption show that the element $\mu = (x_5 - 1)/(x_3 - 1)$ lies in a fixed finite set and since

$$\mu = \frac{(x_5 - 1)/x_4}{(x_3 - 1)/x_2} \cdot \frac{x_4}{x_2},$$

Lemma 1 (ii),(iii) show that that μ is invertible.

Since

$$x_5 - \alpha\mu - \beta\mu = 1$$

and $x_5 \in R^\times$ by Lemma 1 (iv) our assumption on unit equations in R implies that either x_5 lies in a fixed finite set or $x_5 = 1$ or $-\alpha\mu = 1$ or $-\beta\mu = 1$. In the first case we are done by Lemma 3. If $\alpha\mu = -1$ then α and x_2 lie in a finite set and again Lemma 3 is applicable. Since $x_5 = 1$ is impossible we have to deal with the remaining case

$$\beta\mu = -1, \quad x_5 = \alpha\mu.$$

Now Lemma 1 (i) implies

$$\delta = x_5 - x_4 = x_5 - \lambda x_2 \in R^\times,$$

and Lemma 1 (iii) yields (in view of $\lambda \in R^\times$)

$$\epsilon = (x_5 - 1)/x_2 = \lambda(x_5 - 1)/x_4 \in R^\times.$$

Thus we obtain three representations of x_2 as sums of two units, namely

$$x_2 = \lambda^{-1}x_5 - \lambda^{-1}\delta = \epsilon^{-1}x_5 - \epsilon^{-1} = 1 + \alpha.$$

If at least two of them are distinct then the assertion follows from Lemmas 2, 4 and 3 as above. If $\lambda^{-1}x_5 = 1$ then x_5 lies in a finite set and the assertion follows by Lemma 3. Hence it remains to consider the cases $\lambda^{-1}x_5 = \alpha = -\epsilon^{-1}$ and $\lambda^{-1}x_5 = \alpha = \epsilon^{-1}x_5$.

First case: $\lambda^{-1}x_5 = \alpha = -\epsilon^{-1}$. Here we have also $\epsilon^{-1}x_5 = 1$ and thus $x_5^2 = \epsilon x_5 = -\lambda$, hence x_5 lies in a finite set and we are done by Lemma 3.

Second case: $\lambda^{-1}x_5 = \alpha = \epsilon^{-1}x_5$. Here we also have $\lambda^{-1}\delta = \epsilon = -1$ and hence $\lambda = -\delta$. Since $x_5 = \alpha\mu = -\alpha = \lambda\alpha$ we obtain $\lambda = \mu = -1$ and $\beta = 1$. Now $x_4 = \lambda x_2 = -x_2 \neq x_2$ implies that the characteristic of R is different from 2.

The obvious five-term unit equation

$$1 = (1 - x_2) + (x_2 - x_3) + (x_3 - x_4) + (x_4 - x_5) + x_5$$

takes now the form

$$1 = (-\alpha) + (-1) + (3 + 2\alpha) + (-1) + (-\alpha).$$

If it is non-trivial, then α lies in a finite set and so does x_2, and the assertion follows by Lemma 3. If it is trivial, then in view of $char(R) \neq 2$ we must have $\alpha = -1$ which leads to $x_2 = 0$, contradiction. This completes the proof of Theorem 1. □

4. An integral domain R is called a *finite factorization domain*, if every non-zero element of R belongs to only finitely many principal ideals of R. By [HK], Krull domains and orders in algebraic number fields are examples of finite factorization domains. From Theorem 1 we derive the following finiteness result for inequivalent non-linear cycles:

Theorem 2. *Let R be a finite factorization domain satisfying the assumptions of Theorem 1. Then there are only finitely many inequivalent non-linear cycles of a given length $n \geq 2$ in R.*

Note that the assumptions of Theorem 2 are satisfied by all finitely generated integral domains of zero characteristic and in particular by all rings of integers of algebraic number fields. Note also that the non-linearity assumption is essential. Indeed, if R is the ring of integers of the n-th cyclotomic field $Q(\zeta_n)$ then every non-zero element of R lies in a cycle of length n realized by the linear polynomial $f(X) = \zeta_n X$ and therefore in this case there are infinitely many inequivalent cycles of length n.

Proof. It suffices to show that for every $n \geq 2$ there are only finitely many cycles of the form

$$(0, x_1, x_2, \ldots, x_{n-1}, 0). \tag{7}$$

Let (7) be a cycle of the polynomial $f \in R[X]$. We may assume that f is the Lagrange interpolation polynomial corresponding to the data (2) with $x_0 = 0$, and then we have

$$f(X) = a_M X^M + \cdots + A_0 \in R[X],$$

where $2 \le M \le n-1$ and $a_M \neq 0$. Since $f(0) = x_1$ it follows easily that the polynomial

$$g(X) = \frac{1}{x_1} f(x_1 X) = 1 + \sum_{i=1}^{n-1} a_i x_1^{i-1} X^i$$

lies in $R[X]$,

$$\left(0, 1, \frac{x_2}{x_1}, \ldots, \frac{x_{n-1}}{x_1}, 0\right)$$

is a cycle of g, and since $M < n$, g is uniquely determined by this cycle. By Theorem 1 R contains only finitely many normalized cycles and thus the coefficients of g lie in a finite set. In particular $a_M x_1^{M-1}$ lies in a finite set, say $a_M x_1^{M-1} \in \{c_1, \ldots, c_k\} \subset R$ and in view of $a_M \neq 0$ and $M \ge 2$ we see that for some i we have $c_i \in x_1 R$ for some i and therefore there are only finitely many possibilities for the principal ideal $x_1 R$. The polynomial g together with x_1 uniquely determines f and thus the cycle (7). If we replace x_1 by $x_1 \epsilon$ for some $\epsilon \in R^\times$ then instead of (7) we get the equivalent cycle $(0, \epsilon x_1, \ldots, \epsilon x_{n-1}, 0)$. This proves the theorem. □

The preceding theorem does not cover linear cycles. They are described by the following statement which can be easily directly verified:

Theorem 3. *Let R be an arbitrary integral domain and let $f(X) = AX + B \in R[X]$, $A \neq 0$.*

(i) *If A is a primitive root of unity of order $n > 1$ and $A - 1$ does not divide B then every element of R lies in a cycle of f having length n. If $A - 1 \mid B$ then $x_0 = B/(1 - A)$ is a fixpoint and every element $x \neq x_0$ lies in a cycle of length n.*

(ii) *If $A = 1$ and $B \neq 0$ and R has positive characteristic p then every element of R lies in a cycle of f having length p. If R has zero characteristic then f does not have any cycles in R.*

(iii) *If A is not a root of unity and $1 - A \mid B$ then the element $B/(1 - A)$ is a fixpoint of f. If $1 - A$ does not divide B then f does not have any cycles in R.*

Corollary. *Let R be any infinite integral domain and $n \geq 2$. If R contains a root of unity of order n or if n is the characteristic of R, then R contains infinitely many inequivalent linear cycles of length n. In all other cases R contains only finitely many inequivalent linear cycles of length n.*

5. Now we shall consider finite polynomial orbits which contain a cycle of length exceeding 2 and prove the following result:

Theorem 4. *Assume that R is a finite factorization domain satisfying the following condition:*

For any fixed non-zero $a, b, c \in R$ the equation

$$ax + by = c$$

has at most finitely many solutions $x, y \in R^{\times}$.

(i) *Let (x_0, x_1, x_2) be a polynomial sequence in R where $x_0 \neq x_1$ and $x_0 \neq x_2$. Then there are only finitely many $y \in R$ such that (y, x_0, x_1, x_2) is also a polynomial sequence.*

(ii) *Let $\overline{x}$ be a cycle of length $n \geq 3$ in R. Then there are only finitely many finite orbits of a given length $k \geq n$ in R which contain the cycle $\overline{x}$.*

Proof. (i) Let $y \in R$ be such that (y, x_0, x_1, x_2) is a polynomial sequence of some polynomial $f \in R[X]$. Then

$$x_0 - x_1 = f(y) - f(x_0) \in (y - x_0)R,$$
$$x_0 - x_2 = f(y) - f(x_1) \in (y - x_1)R.$$

Since R is a finite factorization domain, there are only finitely many possibilities for the principal ideals $(y - x_0)R$ and $(y - x_1)R$. Hence we obtain

$$y - x_i = A_i \epsilon_i \quad (i = 0, 1),$$

where $\epsilon_0, \epsilon_1 \in R^{\times}$ and A_0, A_1 belong to a finite set of non-zero elements of R. By assumption, the equation

$$A_0 \epsilon_0 - A_1 \epsilon_1 = x_1 - x_0$$

has only finitely many solutions $\epsilon_0, \epsilon_1 \in R^{\times}$, and the assertion follows.

(ii) By induction on k, using (i). □

Observe that in Theorem 4 the assumption $n \geq 3$ is necessary. In fact, if $n = 1$ then a counterexample is given already in $R = \mathbb{Z}$ where the cycle $(0,0)$ of length 1 is for any $k \geq 1$ contained in orbits $(k, 0, 0\}$ of the polynomial $f_k(X) = X(X - k)$ and all these orbits are inequivalent. In case $n = 2$ let R be an integral domain such that $R^\times$ is infinite. Then the cycle $(0,1,0)$ is for any $\epsilon \in R^\times \setminus \{\pm 1\}$ contained in the orbit $(\epsilon, 0, 1, 0)$ of the polynomial $f_\epsilon(X) = \epsilon^{-1}(X - \epsilon)(X - 1) \in R[X]$ and again all these orbits are inequivalent.

Theorem 5. *Let R be a finitely generated domain of zero characteristic, denote by $\overline{R}$ its integral closure and suppose that the unit index $\left[\overline{R}^\times : R^\times\right]$ is finite. Then there are only finitely many inequivalent finite non-linear orbits in R.*

Proof. By Theorem 7 of [HK] R is a finite factorization domain and by [EF], [S] all assumptions concerning unit equations in Theorems 1, 2 are satisfied.

Note that a nonlinear cycle has length $n \geq 3$. Indeed, the cycle (x_0, x_0) of length 1 is realized by $f(X) = X$ and the cycle (x_0, x_1, x_0) of length 2 is a cycle of $f(X) = -X + x_0 + x_1$, hence they are linear. By Theorem 4 every non-linear cycle is contained in only finitely many finite orbits of a given length. However it has been proved in [NP] that the lengths of finite orbits in R is bounded by a constant depending only on R. Hence there are only finitely many finite orbits containing a given non-linear cycle. By Theorem 2 there are only finitely many inequivalent non-linear cycles of a given length, and by [HKN1] the length of a cycle in R is bounded by a constant depending only on R. This shows that there are only finitely many inequivalent non-linear finite orbits in R at all. $\square$

Corollary. *Suppose that R is either an order in an algebraic number field or a finitely generated and integrally closed domain of zero characteristic. Then there are only finitely many inequivalent finite non-linear orbits in R.*

References

[EG] J. H. Evertse and K. Győry, On the number of solutions of weighted unit equations, *Compos. Math.* **66** (1988), 329–354.

[HK] F. Halter-Koch, Finiteness theorems for factorizations, *Semigroup Forum* **44** (1992), 112–117.

[HKN1] F. Halter-Koch and W. Narkiewicz, Polynomial cycles in finitely generated domains, *Monatsh. Math.* **119** (1995), 275–279.

[HKN2] F. Halter-Koch and W. Narkiewicz, Polynomial cycles and dynamical units, *Proc. Conf. Analytic and Elementary Number Theory, Wien* 1997, 70–80.

[N] W. Narkiewicz, Polynomial Mappings, *Lecture Notes in Math.* **1600**, Springer 1995.

[NP] W. Narkiewicz and T. Pezda, Finite polynomial orbits in finitely generated domains, *Monatsh. Math.* **124** (1997), 309–316.

[P] T. Pezda, Polynomial cycles in certain local domains, *Acta Arith.* **66** (1994), 11–22.

[S] H. P. Schlickewei, S-units equations over number fields, *Invent. Math.* **102** (1990), 95–107.

F. HALTER–KOCH
INSTITUT FÜR MATHEMATIK
KARL–FRANZENS UNIVERSITÄT
HEINRICHSTRASSE 36/IV
A–8010 GRAZ
AUSTRIA

E-mail: franz.halterkoch@balu.kfunigraz.ac.at

W. NARKIEWICZ
INSTITUTE OF MATHEMATICS
WROCŁAW UNIVERSITY
PLAC GRUNWALDZKI 2—4
PL–50–384 WROCŁAW
POLAND

E-mail: narkiew@math.uni.wroc.pl

(Received June 14, 1999)