An irrationality criterion involving recurring sequences

Fabio Lucchini

An irrationality criterion involving recurring sequences

Fabio Lucchini
fabio.lucchini.83@gmail.com

December 11, 2011

Abstract

The main purpose of this paper is to prove an irrationality criterion involving recurring sequences. Let $f \in \mathbb{Z}[X]$ be a polynomial of degree $d > 1$ and leading coefficient $c \neq 0$. Suppose that there exists two unbounded sequences x_n, y_n $(n \in \mathbb{N})$ such that

$$x_{n+1} = f(x_n), \qquad y_{n+1} = cy_n^d$$

and $x_n \sim y_n$ as $n \to \infty$. If x_0 integer and y_0 is rational then there exists $a \in \mathbb{Q}$ such that

$$f(X) = c(X-a)^d + a.$$

1 Introduction

Let $f \in \mathbb{C}[X]$ be a polynomial of degree $d > 1$ and leading coefficient $c \neq 0$. Given $x_0, y_0 \in \mathbb{C}$, consider the recurring sequences x_n, y_n $(n \in \mathbb{N})$ defined by

$$x_{n+1} = f(x_n), \qquad y_{n+1} = cy_n^d.$$

Note that if $x_n \to \infty$ then $x_{n+1} \sim cx_n^d$. This lead to the following question: given $x_0 \in \mathbb{C}$ such that $x_n \to \infty$ there exists $y_0 \in \mathbb{C}$ such that $x_n \sim y_n$?

If f is a polynomial of the form $c(X-a)^d + a$ for some $a, c \in \mathbb{C}$ the answer is affirmative for if we take $y_0 = x_0 - a$ then $y_n = x_n - a$ for each $n \in \mathbb{N}$ hence $x_n \sim y_n$ whenever $x_n \to \infty$.

The next theorem states that, under certain arithmetical hypothesis, the polynomials $c(X-a)^d + a$ are the only ones with this property.

Theorem 1.1. *Let $f \in \mathbb{Z}[X]$ be a polynomial of degree $d > 1$ and leading coefficient $c \neq 0$. Suppose that there exists two unbounded sequences x_n, y_n $(n \in \mathbb{N})$ such that*

$$x_{n+1} = f(x_n), \qquad y_{n+1} = cy_n^d$$

and $x_n \sim y_n$ as $n \to +\infty$. If x_0 is integer and y_0 is rational then there exists $a \in \mathbb{Q}$ such that

$$f(X) = c(X - a)^d + a.$$

Note that the sequences x_n, y_n are actually divergent: this follows from the explicit formula

$$y_n = c^{\frac{d^n-1}{d-1}} y_0^{d^n}$$

which implies that y_n is unbounded if and only if

$$\left|cy_0^{d-1}\right| > 1 \tag{1}$$

and in this case $y \to \infty$.

The proof of 1.1 follows several steps. The first (section 2) consist to show that the sequence x_n admits a power series expansion in y_n of the form

$$x_n = y_n + a_0 + a_1 y_n^{-1} + a_2 y_n^{-2} + \cdots$$

with $a_i \in \mathbb{Q}$. This guarantees (section 3) that given $k \in \mathbb{N}$ there exists two polynomials $a, b \in \mathbb{Q}[X]$ with $a \neq 0$ such that

$$a(x_n)y_n = b(x_n) + o(y_n^{-k})$$

as $n \to +\infty$. If x_0 is integer and y_0 rational, then the error term $o(y_n^{-k})$ can be eliminated, so that y_n can be written as a rational function of x_n that's $y_n = \gamma(x_n)$ eventually, where $\gamma = b/a \in \mathbb{Q}(X)$. Then γ satisfy the functional equation

$$\gamma(f(X)) = c\gamma(X)^d$$

in $\mathbb{Q}(X)$. Doing arithmetic in $\mathbb{Q}[X]$ (section 4) we conclude that this is possible if and only if $f(X)$ is of the form $c(X + a)^d - a$ with $c \in \mathbb{Z}$ and $a \in \mathbb{Q}$.

2 Power series expansion

It this section we show that the sequence x_n admit a power series expansion in y_n of the form

$$x_n = y_n + a_0 + a_1 y_n^{-1} + a_2 y_n^{-2} + \cdots$$

with $a_i \in \mathbb{Q}$.

In the sequel we consider complex sequences as functions $\mathbb{N} \to \mathbb{C}$. Given a complex sequence $\xi : \mathbb{N} \to \mathbb{C}$ and $n \in \mathbb{N}$ we indicate with ξ_n the value of ξ at n, as customary. If ξ, η are complex sequences then $\xi + \eta$ and $\xi\eta$ are complex sequences defined as

$$(\xi + \eta)_n = \xi_n + \eta_n \qquad\qquad (\xi\eta)_n = \xi_n \eta_n.$$

Finally, ξ^τ denote the translate sequence, that's $(\xi^\tau)_n = \xi_{n+1}$.

We start by formalizing the notion of power series of a sequences.

Definition 2.1. *Let θ be a complex sequences such that $\theta \to 0$ and $\theta \neq 0$ eventually. We say that a complex sequence ξ has a θ-expansion if for each $k \in \mathbb{N}$ there exists a polynomial $p \in \mathbb{Q}[X]$ such that*

$$\xi = p(\theta) + o(\theta^k).$$

The purpose of this section is to prove the following:

Theorem 2.1. *Let f be a complex polynomial with degree $d > 1$ and leading coefficient c, $x, y : \mathbb{N} \to \mathbb{C}$ be two complex sequences such that*

$$x^\tau = f(x), \qquad\qquad y^\tau = cy^d, \tag{2}$$

$x, y \to \infty$ and $x \sim y$. If $\theta := 1/y$ and $r := x - y$, then r has θ-expansion.

Note that $r = o(y)$ and from (2) we obtain a recurrence relation for r, namely

$$r^\tau = ducy^{d-1} r + v \tag{3}$$

where

$$u := \frac{x^{d-1} + \cdots + y^{d-1}}{dy^{d-1}} \sim 1, \qquad v := f(x) - cx^d = O(y^{d-1}).$$

The first step consist to show that r is bounded. Then an induction argument applied to the recurrence (3) will show that r has θ-expansion.

Lemma 2.2. *If r is unbounded then $r \to \infty$.*

Proof. From (3) we obtain

$$|r|^\tau - |r| \geq (du\,|c|\,|y|^{d-1} - 1)\,|r| - |v|\,.$$

Since $u \sim 1$ and $y \to \infty$, there exists $\bar{u} \sim 1$ such that

$$du\,|c|\,|y|^{d-1} - 1 = d\bar{u}\,|c|\,|y|^{d-1}\,;$$

in particular there exists $N \in \mathbb{N}$ such that $\bar{u}_n > \frac{1}{2}$ for $n > N$. Let $C > 0$ such that $|v| \leq C\,|y|^{d-1}$ and S be the set of $n \in \mathbb{N}$ with $n > N$ such that $|r_n| > \frac{2C}{d|c|}$. Then

$$|v_n| < (du_n\,|c|\,|y_n|^{d-1} - 1)\,|r_n| \qquad \text{for } n \in S,$$

consequently $|r_{n+1}| > |r_n| > \frac{2C}{cd}$ for $n \in S$. Thus if $n \in S$ then $n+1 \in S$, hence $|r_n| > \frac{2C}{d|c|}$ eventually. Since C can be choose great as we would, we obtain $r \to \infty$. □

Proposition 2.3. *The sequence r is bounded.*

Proof. Suppose r unbounded and let $\varrho := |r/y|$. From (3) we obtain

$$|\varrho^\tau - du\varrho| \leq |v|\,|y|^{-d} \tag{4}$$

where $u \sim 1$ and $vy^{-d} = O(y^{-1})$, from which

$$\frac{\varrho^\tau}{du\varrho} = 1 + O\Big(\frac{1}{r}\Big) \to 1$$

that's $\varrho^\tau \sim d\varrho$. In particular $r \neq 0$ eventually, that's $\varrho > 0$ eventually. Since $d > 1$ we have

$$\varrho^\tau - \varrho \sim (d-1)\varrho \implies \frac{\varrho^\tau - \varrho}{\varrho} \to d - 1$$

hence from $d - 1 > 0$ and $\varrho > 0$ follows that ϱ is eventually non-decreasing. Since $\varrho \to 0$ this implies $\varrho = 0$ eventually that's $r = 0$ eventually - a contradiction. □

Now a proof of 2.1:

Proof. Since r is bounded and $\theta^{d-1}v$ is convergent, from

$$r = \frac{1}{cdu}(\theta^{d-1}r^\tau - \theta^{d-1}v)$$

follows that r is convergent, that's r has a θ-expansion of order 0. Suppose that r admit a θ-expansion of order $k \in \mathbb{N}$, that's there exists $p \in \mathbb{Q}[X]$ such that $r = p(\theta) + o(\theta^k)$. Then $r^\tau = p(\theta^d/c) + o(\theta^{dk})$ and since $x\theta = 1 + \theta r$

$$v\theta^{d-1} = c_1(1+\theta r)^{d-1} + \cdots + c_d, \qquad \text{with } c_i \in \mathbb{Z}$$

hence $v\theta^{d-1} = g(\theta) + o(\theta^{k+1})$ for some $g \in \mathbb{Q}[X]$. Similarly

$$u = \frac{(1+\theta r)^{d-1} + \cdots + 1}{d} = h(\theta) + o(\theta^{k+1}).$$

Since $u \to 1$ we have $h(0) = 1$ and

$$r = \frac{1}{cd}\frac{\theta^{d-1}p(\theta^d/c) - g(\theta) + o(\theta^{k+1})}{h(\theta) + o(\theta^{k+1})} = q(\theta) + o(\theta^{k+1})$$

for some $q \in \mathbb{Q}[X]$. □

3 Approximation by rational functions

In this section we use the power series expansion obtained in the previous section to show that y can be approximated as a rational function of x, that's given $k \in \mathbb{N}$ there exists two polynomials $a, b \in \mathbb{Q}[X]$ with $a \neq 0$ such that

$$a(x)y = b(x) + o(\theta^k).$$

Let $\mathscr{E}(\theta)$ be denote the set of infinitesimal complex sequences which has a θ-expansion.

Lemma 3.1. *Let ξ be a complex sequence which as a θ-expansion. For all $k \in \mathbb{N}$ there exists $p \in \mathbb{Q}[X]$ and $\eta \in \mathscr{E}(\theta)$ such that $\xi = p(\theta) + \theta^k\eta$.*

Proof. Given k, by definition there exists a polynomial $p \in \mathbb{Q}[X]$ such that $\xi = p(\theta) + o(\theta^k)$. Define

$$\eta := \frac{\xi - p(\theta)}{\theta^k}.$$

We prove that $\eta \in \mathscr{E}(\theta)$. Certainly η is infinitesimal. Given $h \in \mathbb{N}$, we claim that there exists a polynomial $q \in \mathbb{Q}[X]$ such that $\eta = q(\theta) + o(\theta^h)$. Let $\bar{p} \in \mathbb{Q}[X]$ such that $\xi = \bar{p}(\theta) + o(\theta^{h+k})$. Then $\bar{p}(\theta) - p(\theta) = o(\theta^k)$ hence there exists a polynomial $q \in \mathbb{Q}[X]$ such that $\bar{p} - p = X^k q$. Consequently,

$$\eta = \frac{\bar{p}(\theta) - p(\theta) + o(\theta^{h+k})}{\theta^k} = q(\theta) + o(\theta^h)$$

which conclude the proof. □

Now we shall investigate the structure of the set of sequences that admit θ-expansion. From the relation $x\theta = 1 + r\theta$, follows that the vector space $\mathscr{S} := \mathbb{Q}[x] + \mathscr{E}(\theta)$ is closed by multiplication by x. More explicit:

Proposition 3.2. *For every $\xi \in \mathscr{S}$ and $a \in \mathbb{Q}[X]$ there exists $b \in \mathbb{Q}[X]$ such that $a(x)\xi - b(x) \in \mathscr{E}(\theta)$.*

Proof. It's enough to prove the statement for $\xi \in \mathscr{E}(\theta)$ and $a \neq 0$. By previous Lemma there exists $a_0 \in \mathbb{Q}$ and $\eta \in \mathscr{E}(\theta)$ such that

$$\xi = a_0\theta + \eta\theta.$$

Since $x\theta - 1 = r\theta \in \mathscr{E}(\theta)$, we have

$$x\xi - a_0 = \eta + a_0 r\theta + r\eta\theta \in \mathscr{E}(\theta),$$

because $r, \theta, \eta \in \mathscr{E}(\theta)$. Conclude by induction on the degree of a. □

Theorem 3.3. *Given $\xi \in \mathscr{S}$, for every positive integer k there exists $a, b \in \mathbb{Q}[X]$, with $a \neq 0$ and $\deg a \leq k$, such that $a(x)\xi = b(x) + o(\theta^k)$.*

Proof. By Proposition 3.2 for every $j = 0, \ldots, k$ there exists $b_j \in \mathbb{Q}[X]$ such that $x^j\xi - b_j(x) \in \mathscr{E}(\theta)$, that's

$$x^j\xi - b_j(x) = p_j(\theta) + o(\theta^k),$$

where $p_j \in \mathbb{Q}[X]$. We can assume $p_j = 0$ or $\deg p_j \leq k$, for all j. Since $p_j(0) = 0$ for every j, the polynomials $p_0, \ldots, p_k$ are linearly dependent over $\mathbb{Q}$. Thus there exists $a_0, \ldots, a_k \in \mathbb{Q}$ not all 0 such that $a_0p_0 + \cdots + a_kp_k = 0$ in $\mathbb{Q}[X]$. Put $a := a_0 + \cdots + a_kX^k \neq 0$ and $b := a_0b_0 + \cdots + a_kb_k$, then

$$a(x)\xi = b(x) + o(\theta^k).$$

□

Theorem 3.4. *Under the assumption of 1.1, there exists $\gamma \in \mathbb{Q}(X) \setminus \mathbb{Q}$ such that*

$$\gamma(f(X)) = c\gamma(X)^d.$$

Proof. If $x_0 \in \mathbb{Z}$ then x is an integer valued sequence. If y_0 is rational, there exists u_0, v_0 integer with $v_0 > 0$ (without common factors) such that $y_0 = \frac{u_0}{v_0}$. The sequences $u^\tau = cu^d$ and $v^\tau = v^d$ are integral valued and $y = \frac{u}{v}$. Moreover, by (1), there exists $k \in \mathbb{N}$ such that $v\theta^k \to 0$.

Since $y = x - r \in \mathscr{S}$, there exists $a, b \in \mathbb{Q}[X]$, with $a \neq 0$, such that

$$a(x)y = b(x) + o(\theta^k).$$

We can assume $a, b \in \mathbb{Z}[X]$. Consequently, $a(x)u - b(x)v$ is a integer valued infinitesimal sequence, hence $a(x)u - b(x)v = 0$ eventually.

Then we have $\frac{b(x)}{a(x)} = \frac{u}{v}$ eventually, from which

$$\frac{b(f(x))}{a(f(x))} = c\frac{b(x)^d}{a(x)^d},$$

that's

$$ca(f(x))b(x)^d - b(f(x))a(x)^d = 0.$$

Since x is unbounded, it follows that

$$ca(f(X))b(X)^d - b(f(X))a(X)^d = 0$$

identically in $\mathbb{Z}[X]$. The rational function $\gamma = \frac{b}{a} \in \mathbb{Q}(X)$ satisfy $\gamma(f(X)) = c\gamma(X)^d$. □

4 Rational functional equation

In this section we prove the following:

Theorem 4.1. *Let $f \in \mathbb{C}[X]$ be a non-constant polynomial with degree $d > 1$ and leading coefficient $c \neq 0$. If there exists a non-constant rational function $\gamma \in \mathbb{C}(X)$ such that*

$$\gamma(f(X)) = c\gamma(X)^d$$

then there exists $a \in \mathbb{C}$ such that $f(X) = c(X - a)^d + a$.

Recall that $\mathbb{C}[X]$ is a unique factorization domain with field of fractions $\mathbb{C}(X)$. In $\mathbb{C}[X]$ irreducible elements are the polynomials of degree 1. If $p \in \mathbb{C}[X]$ is an irreducible polynomial and $\gamma \in \mathbb{C}(X)$ then we can define the order $\operatorname{ord}_p \gamma$ of γ at p and it's an integer.

Lemma 4.2. *Let f be a non-constant polynomial in $\mathbb{C}[X]$. For any monic irreducible polynomial $q \in \mathbb{C}[X]$ there exists a unique monic irreducible polynomial $p \in \mathbb{C}[X]$ such that $q(X) \mid p(f(X))$ in $\mathbb{C}[X]$. If e_q denote the order of $p(f)$ at q then $1 \leq e_q \leq \deg f$. Moreover for any rational function $\gamma \in \mathbb{C}(X)$ we have*

$$\operatorname{ord}_q \gamma(f) = e_q \operatorname{ord}_p \gamma.$$

Proof. If $q(X) = X - a$ for some $a \in \mathbb{C}$ then take $p(X) = X - f(a)$. Since $\deg p(f(X)) = \deg p \deg f$ it follows that $e_q \leq \deg f$.

For the last statement, let $n \in \mathbb{Z}$ be the order of γ at p and let $\bar{\gamma} \in \mathbb{C}(X)$ such that $\gamma = p^n \bar{\gamma}$; then p is not an irreducible factor of $\bar{\gamma}$. Then $\gamma(f) = p(f)^n \bar{\gamma}(f)$ and $p(f), \bar{\gamma}(f)$ has no common irreducible factors. Consequently the order of $\gamma(f)$ at q is ne_q. □

Proposition 4.3. *Let $f(X) \in \mathbb{C}[X]$ be a polynomial with degree $d > 1$ and leading coefficient c. If there exists a non-constant rational function $\gamma \in \mathbb{C}(X)$ such that*

$$\gamma(f(X)) = c\gamma(X)^d$$

then for any monic irreducible factor p of γ there exists an unique monic irreducible factor q of γ such that

$$p(f(X)) = cq(X)^d.$$

Proof. For any monic irreducible polynomial $q \in \mathbb{C}[X]$ let q_* denote the monic irreducible polynomial in $\mathbb{C}[X]$ such that $q(X) \mid q_*(f(X))$ and let e_q be the order of $q_*(f(X))$ at q. Let S be the set of monic irreducible factors of γ; since γ is not constant, S is non-empty. By previous lemma,

$$d \operatorname{ord}_q \gamma = e_q \operatorname{ord}_{q_*} \gamma;$$

in particular $q \in S$ if and only if $q_* \in S$. Consequently we have a map $* : q \mapsto q_*$ from S into S.

Note that this map is onto for if $p(X) = X - b \in S$ and $q(X) = X - a$ where $a \in \mathbb{C}$ is a root of the polynomial $f(X) - b$, then $q_* = p$ hence $q \in S$. Since S is finite, the map $* : q \mapsto q_*$ is a permutation of S.

We obtain

$$\prod_{q\in S} d \operatorname{ord}_q \gamma = \prod_{q\in S} e_q \operatorname{ord}_{q_*} \gamma$$

but since $\prod_q \operatorname{ord}_q \gamma = \prod_q \operatorname{ord}_{q_*} \gamma \neq 0$ it implies

$$d^{\sharp S} = \prod_{q\in S} e_q$$

where $\sharp S$ denote the number of elements in S. Since $1 \leq e_q \leq d$, must be $e_q = d$ for each q thus

$$q_*(f) = q^d. \qquad \square$$

Now we are able to prove 4.1:

Proof. Let p be a monic irreducible factor of γ. By 4.3 there exists a monic irreducible factor q of γ such that $p(f(X)) = cq(X)^d$. If $q(X) = X - a$ and $p(X) = X - b$ then $f(X) = c(X-a)^d + b$. Since q is a monic irreducible factor of γ, $q(f(X))$ is also a d-power of an irreducible factor of f. In particular, $q(f)$ has a multiple root r hence

$$0 = q(f(r))' = f'(r)$$

but since a is the only root of f', it follows that $r = f(a) = b$, that's $q(X) = p(X)$. Thus $a = b$, that's $f(X) = c(X-a)^d + a$. $\square$