Update: *25/01/2014*

Papua New Guinea PNG University of Technology,
International Conference on Pure and Applied Mathematics
ICPAM–LAE 2013, November 26 – 28, 2013

Diophantine approximation with applications to dynamical systems

by
Michel Waldschmidt

Abstract

Dynamical systems were studied by Henri Poincaré and Carl Ludwig Siegel, who developed the theory of celestial mechanics. The behavior of a holomorphic dynamical system near a fixed point depends on a Diophantine condition, already introduced by Joseph Liouville in 1844 when he constructed the first examples of transcendental numbers. One of the deepest results in Diophantine approximation is the Subspace Theorem of Wolfgang Schmidt. We give an application related with linear recurrence sequences and exponential polynomials, involving a dynamical system on a finite dimensional vector space.

`Classification:` primary 11J87, secondary 32H50 37F50
`Keywords:` Dynamical systems; Diophantine approximation; holomorphic dynamics; Thue–Siegel–Roth Theorem; Schmidt's Subspace Theorem; S-unit equations; linear recurrence sequences; exponential polynomials; Skolem–Mahler–Lech Theorem.

Acknowledgments

I was invited in January 2010 by Ashok Agrawal to participate to the 97th Indian Science Congress in Thiruvananthapuram (Kerala). During this meeting, following the suggestion of Jugal K. Verma, A. J. Parameswaran, then Director of the Kerala School of Mathematical Science (KSOM) in Kozikhode, invited me to visit his institute. During my visit just after the congress, we discussed some work by S.G.

Dani involving a question relating dynamical systems with Diophantine approximation (see Corollary 7.4 below). I had a correspondence with Pietro Corvaja and Umberto Zannier on this topic at that time.

After he became the Director of KSOM, M. Manickam suggested me to organize a workshop in his institute. With Yann Bugeaud, S.G. Dani and Pietro Corvaja, we selected the topic *number theory and dynamical systems.* This workshop took place in February 2013.

This text is a report on the lecture I gave in Lae, at the International Conference on Pure and Applied Mathematics ICPAM–LAE 2013, The Papua New Guinea (PNG) University of Technology (November 26 - 28, 2013), where I was invited by Kenneth Nwabueze.

I am pleased to express my thanks to Ashok Agrawal, Jugal K. Verma, A. J. Parameswaran, Yann Bugeaud, S.G. Dani, Pietro Corvaja, Umberto Zannier, M. Manickam and Kenneth Nwabueze.

I wish also to thank Ajaya Singh and Jorge Jimenez Urroz: when we did a trek together around the Annapurna in fall 2011 and to the Everest Base Camp in fall 2012, we carried with us some papers on dynamical systems ([21] in 2011, [2] and [10] in 2012) where I learned the basis facts on this topic.

1 Iteration of a map

Consider a set X and map $f : X \to X$. We denote by f^2 the composition map $f \circ f : X \to X$. More generally, we define inductively $f^n : X \to X$ by $f^n = f^{n-1} \circ f$ for $n \geq 1$, with f^0 being the identity. The *orbit* of a point $x \in X$ is the set

$$\{x, f(x), f^2(x), \dots\} \subset X.$$

A *fixed point* is an element $x \in X$ such that $f(x) = x$. Hence, a fixed point is a point x, the orbit of which has only the element x.

A *periodic point* is an element $x \in X$ for which there exists $n \geq 1$ with $f^n(x) = x$. The smallest such n is the length of the *period* of x, and all such n are the multiples of the period length. The orbit

$$\{x, f(x), \dots, f^{n-1}(x)\}$$

has n elements. For instance, a fixed point is a periodic point of period length 1.

2 Endomorphisms of a vector space

Take for X a finite dimensional vector space V over a field K and for $f : V \to V$ a linear map. A fixed point of f is nothing else than an eigenvector with eigenvalue 1. A periodic point of f is an element $x \in V$ such that there exists $n \geq 1$ with $f^n(x) = x$, hence, f has an eigenvalue λ with $\lambda^n = 1$ (λ is a root of unity).

If V has dimension d and if we choose a basis of V, then to f is associated a $d \times d$ matrix A with coefficients in K. Then, for $n \geq 1$, f^n is the linear map associated with the matrix A^n. To compute A^n, we write the matrix A as a conjugate to either a diagonal or a *Jordan* matrix

$$A = P^{-1} D P,$$

where P is a regular $d \times d$ matrix. Then, for $n \geq 0$,

$$A^n = P^{-1} D^n P.$$

If D is a diagonal matrix with diagonal $(\lambda_1, \ldots, \lambda_d)$, then D^n is a diagonal matrix with diagonal $(\lambda_1^n, \ldots, \lambda_d^n)$, so that

$$A^n = P^{-1} \begin{pmatrix} \lambda_1^n & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_d^n \end{pmatrix} P.$$

Two examples are given in the Appendix.

In general, the matrix A can be written $A = P^{-1} D P$ with diagonal blocs

$$D = \begin{pmatrix} D_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & D_k \end{pmatrix}$$

where, for $i = 1, \ldots, k$, D_i is a $d_i \times d_i$ *Jordan matrix*

$$D_i = \begin{pmatrix} \lambda_i & 1 & 0 & \cdots & 0 \\ 0 & \lambda_i & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & \lambda_i \end{pmatrix}$$

with $d_1 + \cdots + d_k = d$ (the diagonal case is the case $d_1 = \cdots = d_k = 1$, $k = d$). Then, for $n \geq 1$,

$$D^n = \begin{pmatrix} D_1^n & & 0 \\ & \ddots & \\ 0 & & D_k^n \end{pmatrix}$$

with

$$D_i^n = \begin{pmatrix} \lambda_i^n & n\lambda_i^{n-1} & \binom{n}{2}\lambda_i^{n-2} & \cdots & \binom{n}{d_i-2}\lambda_i^{n-d_i-2} & \binom{n}{d_i-1}\lambda_i^{n-d_i-1} \\ 0 & \lambda_i^n & n\lambda_i^{n-1} & \cdots & \binom{n}{d_i-3}\lambda_i^{n-d_i-3} & \binom{n}{d_i-2}\lambda_i^{n-d_i-2} \\ \vdots & \vdots & \ddots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & n\lambda_i^{n-1} & \binom{n}{2}\lambda_i^{n-2} \\ 0 & 0 & 0 & \cdots & \lambda_i^n & n\lambda_i^{n-1} \\ 0 & 0 & 0 & \cdots & 0 & \lambda_i^n \end{pmatrix}.$$

3 Holomorphic dynamic

Our second and main example of a dynamical system is with an open set $\mathcal{V}$ in $\mathbb{C}$ and an *analytic* (=*holomorphic*) map $f : \mathcal{V} \to \mathcal{V}$. The main goal will be to investigate the behavior of f near a fixed point $z_0 \in \mathcal{V}$. So we assume $f(z_0) = z_0$. The local behavior of the dynamics defined by f depends on the derivative $f'(z_0)$ of f at the fixed point:

- If $f'(z_0) = 0$, then z_0 is a *super–attracting point*.
- If $0 < |f'(z_0)| < 1$, then z_0 is an *attracting point*.
- If $|f'(z_0)| > 1$, then z_0 is a *repelling point*.
- If $|f'(z_0)| = 1$, then z_0 is an *indifferent point*.

When $|f'(z_0)| = 1$, the point z_0 is a *rationally indifferent point* or a *parabolic* point if $f'(z_0)$ is a root of unity and is an *irrationally indifferent point* if $f'(z_0)$ is not a root of unity ([2], § 6.1, [10] §2.2).

We wish to mimic the situation of an endomorphism of a vector space: in place of a regular matrix P, we introduce a local change of coordinates h. Let $\mathcal{D}$ be the open unit disc in $\mathbb{C}$ and $g : \mathcal{D} \to \mathcal{D}$ an analytic map with $g(0) = 0$. We say that f and g are *conjugate* if there exists an analytic map $h : \mathcal{V} \to \mathcal{D}$ such that $h(z_0) = 0$, $h'(z_0) \neq 0$ and $h \circ f = g \circ h$:

$$\begin{array}{ccccc} z_0 \in \mathcal{V} & \xrightarrow{f} & \mathcal{V} \ni z_0 & \qquad & f(z_0) = z_0 \\ {\scriptstyle h}\downarrow & & \downarrow{\scriptstyle h} & & \\ 0 \in \mathcal{D} & \xrightarrow[g]{} & \mathcal{D} \ni 0 & \qquad & g(0) = 0 \end{array}$$

Assume $f : \mathcal{V} \to \mathcal{V}$ and $g : \mathcal{D} \to \mathcal{D}$ are conjugate: $h \circ f = g \circ h$. Then we have

$$h \circ f^2 = h \circ f \circ f = g \circ h \circ f = g \circ g \circ h = g^2 \circ h$$

and by induction $h \circ f^n = g^n \circ h$ for all $n \geq 0$.

An important special case is when g is a homothety: $g(z) = \lambda z$.

Lemma 3.1. *Assume $f : \mathcal{V} \to \mathcal{V}$ is conjugate to the homothety $g(z) = \lambda z$. Then*
(a) $\lambda = f'(z_0)$.
(b) Il λ is not a root of unity, then there exists a unique $h : \mathcal{D} \to \mathcal{D}$ with $h'(z_0) = 1$ and $h \circ f = g \circ h$.

Hence, in this case, f is conjugate to its linear part $z \to z_0 + (z - z_0) f'(z_0)$. One says that f is *linearizable*.

Proof. For part (a), take the derivative of $h \circ f = g \circ h$ at z_0:

$$h'(z_0) f'(z_0) = \lambda h'(z_0)$$

and use $h'(z_0) \neq 0$.

For part (b), the unicity when z_0 is not a rationally indifferent point, follows by induction from the equality between the Taylor expansions of $h \circ f$ and $g \circ h$ at $z = z_0$. $\square$

Define $\lambda = f'(z_0)$. The following result is due to G. Kœnigs and H. Poincaré (1884) — see for instance, [2], § 6.3, [10] Th. 2.2, [13] §1, [14] § 6. Several proofs are given in [2], § 6.3.

Theorem 3.2 (Kœnigs–Poincaré)**.** *Assume $\lambda \neq 0$ and $|\lambda| \neq 1$. Then f is linearizable.*

When $\lambda = 0$, f has a zero of multiplicity $n \geq 2$ at z_0 and is conjugate to $z \mapsto z^n$ (A. Böttcher) - see [14] Th. 6.7.

Assume now $|\lambda| = 1$. Write $\lambda = e^{2i\pi\theta}$. The real number θ is the rotation number of f at z_0. It was conjectured in 1912 by E. Kasner that f is always linearizable, meaning that f is conjugate to the rotation $z \mapsto e^{2i\pi\theta} z$. In 1917, G.A. Pfeiffer produced a counterexample. In 1927, H. Cremer proved that in the *generic* case, f is not linearizable. In 1942, C.L. Siegel proved that if θ satisfies a *Diophantine condition* (see §4), then f is linearizable. In 1965, A.D. Brjuno relaxed Siegel's assumption. In 1988, J.C. Yoccoz showed that if θ does not satisfies Brjuno's condition, then the dynamic associated with

$$f(z) = \lambda z + z^2$$

has infinitely many periodic points in any neighborhood of 0, hence, is not linearizable. See [10] §2.2, [13] §3 and [14] §8.

4 Diophantine condition

Siegel's Diophantine condition on the rotation number θ is that no *good* rational approximation p/q of θ can have a *small denominator* q. The same condition was introduced earlier by Liouville, who proved in 1844 that Siegel's Diophantine condition is satisfied if θ is an algebraic number.

Recall that a complex number α is *algebraic* if there exists a nonzero polynomial $f \in \mathbb{Z}[X]$ such that $f(\alpha) = 0$. The smallest degree of such a polynomial is the degree of the algebraic number α. For instance, $\sqrt{2}$, $i = \sqrt{-1}$, $\sqrt[3]{2}$, $e^{2i\pi a/b}$ (for a and b integers, $b > 0$) are algebraic numbers. There exist quintic polynomials $X^5 + aX + b$ with a and b in $\mathbb{Z}$ having Galois group the symmetric group $\mathfrak{S}_5$ or the alternating group $\mathfrak{A}_5$ which are not solvable, their roots are algebraic numbers but cannot be expressed using radicals.

A number which is not algebraic is *transcendental*. The existence of transcendental numbers was not known before 1844, when Liouville produced the first examples, like

$$\xi = \sum_{n\geq 0} \frac{1}{10^{n!}}\cdot$$

The idea of Liouville is to prove a *Diophantine property* of algebraic numbers, namely that rational numbers with small denominators do not produce sharp approximations. Hence, a real number with too good rational approximations cannot be algebraic. For instance, with the above number ξ and $q = 10^{N!}$,

$$p = \sum_{n=0}^{N} 10^{N!-n!}, \qquad 0 < \xi - \frac{p}{q} < \frac{2}{10^{(N+1)!}} = \frac{2}{q^{N+1}}\cdot$$

Theorem 4.1 (Liouville's inequality, 1844)**.** *Let α be an algebraic number of degree $d \geq 2$. There exists $c(\alpha) > 0$ such that, for any $p/q \in \mathbb{Q}$ with $q > 0$,*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^d}\cdot$$

A real number θ satisfies a *Diophantine condition* if there exists a constant $\kappa > 0$ such that

$$\left|\theta - \frac{p}{q}\right| > \frac{1}{q^\kappa}$$

for all $p/q \in \mathbb{Q}$ with $q > 1$.

An irrational real number is a *Liouville number* if it does not satisfy a Diophantine condition.

In dynamical systems, a property is satisfied for a *generic rotation number* θ if it is true for all real numbers in a countable intersection of dense open sets — these sets are called G_δ sets by Baire, who calls *meager* the complement of a G_δ set. According to *Baire's Theorem*, a G_δ set is dense in $\mathbb{R}$.

The set of numbers which do not satisfy a Diophantine condition is a generic set. However, for Lebesgue measure, the set of Liouville numbers (i.e. the set of numbers which do not satisfy a Diophantine condition) has measure zero.

In terms of continued fraction (see [10] §2.2, [13] §4), the Diophantine condition (of Liouville and Siegel) can be written

$$\sup_{n\ge 1} \frac{\log q_{n+1}}{\log q_n} < \infty,$$

while the *condition of Brjuno* is

$$\sum_{n\ge 1} \frac{\log q_{n+1}}{q_n} < \infty.$$

If a number θ satisfies the Diophantine condition, then it satisfies Brjuno's condition. However, there are (transcendental) numbers which do not satisfy the Diophantine condition, but satisfy Brjuno's condition.

5 Schmidt's Subspace Theorem

In the lower bound

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^d}$$

for α real algebraic number of degree $d \ge 3$, the exponent d of q in the denominator of the right hand side was replaced by κ with

- any $\kappa > (d/2) + 1$ by A. Thue (1909),
- any $\kappa > 2\sqrt{d}$ by C.L. Siegel in 1921,
- any $\kappa > \sqrt{2d}$ by F.J. Dyson and A.O. Gel'fond in 1947,
- any $\kappa > 2$ by K.F. Roth in 1955.

Theorem 5.1 (Thue–Siegel–Roth Theorem). *For any real algebraic number α, for any $\epsilon > 0$, the set of $p/q \in \mathbb{Q}$ with $|\alpha - p/q| < q^{-2-\epsilon}$ is finite.*

An equivalent statement is:

For any real algebraic number α and for any $\epsilon > 0$, the set of $p/q \in \mathbb{Q}$ such that

$$q|q\alpha - p| < q^{-\epsilon}$$

is finite.

The conclusion can be phrased:

For any real algebraic number α and for any $\epsilon > 0$, the set of $(p, q) \in \mathbb{Z}^2$ such that

$$q|q\alpha - p| < q^{-\epsilon}$$

is contained in the union of finitely many lines in $\mathbb{Z}^2$.

A powerful generalization has been achieved in 1970 by W.M. Schmidt. Here is a special case of his Subspace Theorem [5, 6, 9, 12, 17, 24, 25].

Theorem 5.2 (Schmidt's Subspace Theorem)**.** *Let $m \geq 2$ be an integer and $L_0, \ldots, L_{m-1}$ be m independent linear forms in m variables with algebraic coefficients. Let $\epsilon > 0$. Then the set*

$$\left\{\mathbf{x} = (x_0, \ldots, x_{m-1}) \in \mathbb{Z}^m \; ; \; |L_0(\mathbf{x}) \cdots L_{m-1}(\mathbf{x})| \leq |\mathbf{x}|^{-\epsilon}\right\}$$

is contained in the union of finitely many proper subspaces of $\mathbb{Q}^m$.

Example: For $m = 2$, $L_0(x_0, x_1) = x_0$, $L_1(x_0, x_1) = \alpha x_0 - x_1$, we recover Roth's Theorem.

6 Generalized S–unit equation

The proof of Schmidt's Subspace Theorem has an arithmetic nature; the fact that the linear forms have algebraic coefficients is crucial. The conclusion does not hold without this assumption.

However, there are *specializations arguments*[1] ([16] §4, [18] §2, [19] §9) which enable one to deduce consequences without any arithmetic assumption: these corollaries are valid for fields of zero characteristic in general.

[1] As pointed out to me by Umberto Zannier, there are also independent (and easier) arguments based on derivations which give Theorem 6.1 in the "transcendental case" (reducing it to the algebraic case or proving it completely, depending on the assumptions).

An example is the so–called *Theorem of the generalized S–unit equation*, achieved in the 1980's by J.H. Evertse, A.J. van der Poorten and H.P. Schlickewei. It relies on a generalization of Schmidt's Subspace Theorem which rests on works by Schmidt, Schlickewei and others, involving p–adic numbers [6, 12, 24].

Theorem 6.1 (Evertse, van der Poorten, Schlickewei)**.** *Let K be a field of characteristic zero, let G be a finitely generated multiplicative subgroup of the multiplicative group $K^\times = K \setminus \{0\}$ and let $n \geq 2$. Then the equation*

$$u_1 + u_2 + \cdots + u_n = 1,$$

where the unknowns $u_1, u_2, \cdots, u_n$ take their values in G, for which no non-trivial subsum

$$\sum_{i \in I} u_i \qquad \emptyset \neq I \subset \{1, \ldots, n\}$$

vanishes, has only finitely many solutions.

7 Linear recurrence sequences and exponentials polynomials

Let K be a field of zero characteristic. A sequence $(u_n)_{n\geq 0}$ of elements of K is a *linear recurrence sequence* if there exist an integer $d \geq 1$ and elements $a_0, a_1, \ldots, a_{d-1}$ of K with $a_0 \neq 0$ such that, for $n \geq 0$,

$$u_{n+d} = a_{d-1}u_{n+d-1} + \cdots + a_1 u_{n+1} + a_0 u_n. \tag{7.1}$$

In matrix notation, (7.1) can be written $U_{n+1} = AU_n$, with

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ a_0 & a_1 & a_2 & \cdots & a_{d-1} \end{pmatrix} \quad \text{and} \quad U_n = \begin{pmatrix} u_n \\ u_{n+1} \\ \vdots \\ u_{n+d-2} \\ u_{n+d-1} \end{pmatrix}.$$

Hence $U_n = A^n U_0$ for all $n \geq 0$. Such a sequence $(u_n)_{n\geq 0}$ is determined by the coefficients $a_0, a_1, \ldots, a_{d-1}$ and by the initial values $u_0, u_1, \ldots, u_{d-1}$. Given $\underline{a} = (a_0, a_1, \ldots, a_{d-1}) \in K^d$, the set of sequences $(u_n)_{n\geq 0}$ of elements of K satisfying (7.1) is a K vector space $V_{\underline{a}}$ of dimension d. A basis of $V_{\underline{a}}$ is obtained by taking for $(u_0, u_1, \ldots, u_{d-1})$ the elements of a basis of K^d.

Let

$$\det(XI_d - A) = X^d - a_{d-1}X^{d-1} - \cdots - a_1X - a_0$$

be the characteristic polynomial of A. Denote by $\alpha_1, \ldots, \alpha_k$ its distinct roots and by $s_1, \ldots, s_k$ their multiplicities, so that

$$X^d - a_{d-1}X^{d-1} - \cdots - a_1X - a_0 = \prod_{i=1}^{k}(X - \alpha_i)^{s_i}.$$

Computing A^n as mentioned in §2, one deduces that there exist polynomials $A_1, \ldots, A_k$ with A_i of degree $< s_i$ such that

$$u_n = \sum_{i=1}^{k} A_i(n)\alpha_i^n. \tag{7.2}$$

In other terms, the d sequences $(n^j\alpha_i^n)_{n\geq 0}$, $0 \leq j < d_i$, $1 \leq i \leq k$ constitute a basis for $V_{\underline{a}}$. Equation (7.2) shows that a linear recurrence sequence is given by an *exponential polynomial*. Conversely, a sequence given by an exponential polynomial (7.2) is a linear recurrence sequence. Another characterization is that $(u_n)_{n\geq 0}$ is a linear recurrence sequence if and only if the generating series

$$u_0 + u_1z + \cdots + u_nz^n + \cdots$$

is the Taylor series of a rational fraction $A(z)/B(z)$, where the degree of the denominator B is larger than the degree of the numerator A. Dropping this condition on the degrees amounts to asking that there exists $n_0 \geq 0$ such that the sequence $(u_{n-n_0})_{n\geq 0}$ is a linear recurrence sequence.

Theorem 6.1 on the generalized S–unit equation, applied to the multiplicative subgroup of $K^\times$ generated by $\alpha_1, \ldots, \alpha_k$, yields the following theorem — see [7, 11, 15, 19, 20, 23, 27]:

Theorem 7.3 (Skolem–Mahler–Lech)**.** *Given a linear recurrence sequence $(u_n)_{n\geq 0}$, the set of indices $n \geq 0$ such that $u_n = 0$ is a finite union of arithmetic progressions.*

An *arithmetic progression* is a set of positive integers of the form

$$\{n_0, n_0 + r, n_0 + 2r, \ldots\}.$$

Here, we allow $r = 0$, which means that we consider a single point as an arithmetic progression of ratio 0.

The original proofs of Theorem 7.3 did not use the arguments involved in the proof of Theorem 6.1, but were more elementary. T.A. Skolem treated the case $K = \mathbb{Q}$ of in 1934, and K. Mahler the case $K = \overline{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$, in 1935. The general case was settled by C. Lech in 1953, who also pointed out that such a result may not hold if the characteristic of K is positive: he gave as an example the sequence $u_n = (1+x)^n - x^n - 1$, a third-order linear recurrence over the field of rational functions in one variable over the field $\mathbb{F}_p$ with p elements, where $u_n = 0$ for $n \in \{1, p, p^2, p^3, \dots\}$. A substitute is provided by a result of Harm Derksen (2007), who proved that the zero set in characteristic p is a p–automatic sequence; see [1].

A generalization of Theorem 7.3 has been achieved by Jason P. Bell, Stanley Burris and Karen Yeats [4] who prove that the same conclusion as in the Skolem–Mahler–Lech Theorem holds if the sequence $(u_n)_{n\geq 0}$ satisfies a polynomial-linear recurrence relation

$$u_n = \sum_{i=1}^{d} P(n) u_{n-i}$$

where d is a positive integer and $P_1, \dots, P_d$ are polynomials with coefficient in the field K of zero characteristic, provided that $P_d(x)$ is a nonzero constant. There are also analogues of Theorem 7.3 for algebraic maps on varieties [3]. A version of the Skolem–Mahler–Lech Theorem for any algebraic group is Thm. 4.25, p. 175 of [27].

One main open problem related with Theorem 7.3 is that it is not effective: explicit upper bounds for the number of arithmetic progressions, depending only on the order d of the linear recurrence sequence, are known [18, 19, 25, 26, 27], but no upper bound for the arithmetic progressions themselves is known. A related open problem raised by T.A. Skolem and C. Pisot (see [22, 23]) is:

> *Given an integer linear recurrence sequence, is the truth of the statement "$x_n \neq 0$ for all n" decidable in finite time?*

We conclude this survey with a simple application of Theorem 7.3 to a dynamical system. Let V be a finite dimensional vector space over a field of zero characteristic, H a hyperplane of V, $f : V \to V$ an endomorphism (linear map) and x an element in V.

Corollary 7.4. *If there exist infinitely many $n \geq 1$ such that $f^n(x) \in H$, then there is an infinite arithmetic progression of integers n for which it is so.*

Proof. Choose a basis of V. The endomorphism f is given by a square $d \times d$ matrix A, where d is the dimension of V. Consider the characteristic polynomial of A, say

$$X^d - a_{d-1}X^{d-1} - \cdots - a_1X - a_0.$$

By the Theorem of Cayley–Hamilton, we have

$$A^d = a_{d-1}A^{d-1} + \cdots + a_1A + a_0I_d,$$

where I_d is the identity $d \times d$ matrix. Hence, for $n \geq 0$,

$$A^{n+d} = a_{d-1}A^{n+d-1} + \cdots + a_1A^{n+1} + a_0A^n.$$

It follows that each entry $a_{ij}^{(n)}$, $1 \leq i, j \leq d$, satisfies a linear recurrence sequence, the same for all i, j.

Let $b_1x_1 + \cdots + b_dx_d = 0$ be an equation of the hyperplane H in the selected basis of V. Let ${}^t\underline{b}$ denote the $1 \times d$ (row) matrix $(b_1, \ldots, b_d)$ (transpose of a column matrix $\underline{b}$). Using the notation $\underline{v}$ for the $d \times 1$ (column) matrix given by the coordinates of an element v in V, the condition $v \in H$ can be written ${}^t\underline{b}\,\underline{v} = 0$.

Let x be an element in V and $\underline{x}$ the column matrix given by its coordinates. The condition $f^n(x) \in H$ can now be written

$${}^t\underline{b}A^n\underline{x} = 0.$$

Denote by u_n the entry of the 1×1 matrix ${}^t\underline{b}A^n\underline{x}$. Then there exists $n_0 \geq 0$ such that the sequence $(u_{n-n_0})_{n \geq 0}$ is a linear recurrence sequence (with $n_0 = 0$ if the matrix A is regular), hence, the Skolem–Mahler–Lech Theorem 7.3 applies. $\square$

As pointed out to me by Pietro Corvaja, in Corollary 7.4, one may replace H by a hypersurface, and more generally an algebraic subvariety.

Exponential Diophantine equations involving linear recurrence sequences also occur in the work of P. Corvaja [8] on linear algebraic groups, where he investigates semi–groups of matrices, with rational entries and rational eigenvalues.

Appendix: two examples

In this appendix, we explain how to use the previous theory for computing A_1^n and A_2^n, when

$$A_1 = \begin{pmatrix} 1 & 0 \\ -1 & 2 \end{pmatrix} \quad \text{and} \quad A_2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

The matrix A_1 has trace 3, determinant 2 and characteristic polynomial $X^2 - 3X + 2$, hence the associated linear recurrence is

$$u_{n+2} = 3u_{n+1} - 2u_n.$$

From

$$A_1^{n+2} = 3A_1^{n+1} - 2A_1^n \quad \text{with} \quad A_1^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 1 & 0 \\ -1 & 2 \end{pmatrix},$$

one easily deduces by induction, for $n \geq 0$

$$A_1^n = \begin{pmatrix} 1 & 0 \\ 1 - 2^n & 2^n \end{pmatrix}.$$

This result also can be obtained by diagonalizing A_1 as follows. Since

$$X^2 - 3X + 2 = (X - 1)(X - 2),$$

the two eigenvalues of A_1 are 1 and 2 with eigenvectors $(1, 1)$ and $(0, 1)$ respectively, so that

$$A_1 = P^{-1}DP$$

with

$$P = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}, \quad D = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \quad P^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Hence

$$A_1^n = P^{-1}D^nP = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2^n \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 - 2^n & 2^n \end{pmatrix}.$$

Consider now the matrix A_2. The trace is 1, the determinant is -1, the characteristic polynomial is $X^2 - X - 1$, the linear recurrence is

$$u_{n+2} = u_{n+1} + u_n.$$

From

$$A_2^{n+2} = A_2^{n+1} + A_2^n \quad \text{with} \quad A_2^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$

it follows by induction that for $n \geq 0$,

$$A_2^n = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix},$$

where $(F_n)_{n\geq 0}$ is the linear recurrence sequence $F_{n+2} = F_{n+1} + F_n$ given by the initial conditions $F_0 = 0$, $F_1 = 1$. This is the *Fibonacci sequence*:

$$0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ 89,\ 144,\ 233,\ 377,\ 610,\ 987,\ 1597, \ldots;$$

see reference

`http://www.research.att.com/~njas/sequences/A000045`

in the *On-Line Encyclopedia of Integer Sequences* of Neil J. A. Sloane.

The characteristic polynomial of A_2 splits as

$$X^2 - X - 1 = (X - \phi)(X + \phi^{-1}),$$

where ϕ is the *Golden Ratio*:

$$\phi = \frac{1+\sqrt{5}}{2} = 1.618033\ldots, \qquad \phi^{-1} = \frac{-1+\sqrt{5}}{2}$$

and

$$\phi - \phi^{-1} = 1, \quad \phi + \phi^{-1} = \sqrt{5}.$$

The eigenvalues of A_2 are ϕ and $-\phi^{-1}$ with eigenvectors $(1, \phi)$ and $(1, -\phi^{-1})$. Hence

$$A_2 = P^{-1} D P$$

with

$$P = \frac{-1}{\sqrt{5}} \begin{pmatrix} -\phi^{-1} & -1 \\ -\phi & 1 \end{pmatrix}, \quad D = \begin{pmatrix} \phi & 0 \\ 0 & -\phi^{-1} \end{pmatrix}, \quad P^{-1} = \begin{pmatrix} 1 & 1 \\ \phi & -\phi^{-1} \end{pmatrix}.$$

From

$$\begin{aligned} A_2^n &= P^{-1} D^n P \\ &= \frac{-1}{\sqrt{5}} \begin{pmatrix} 1 & 1 \\ \phi & -\phi^{-1} \end{pmatrix} \begin{pmatrix} \phi^n & 0 \\ 0 & (-\phi)^{-n} \end{pmatrix} \begin{pmatrix} -\phi^{-1} & -1 \\ -\phi & 1 \end{pmatrix} \\ &= \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix} \end{aligned}$$

we deduce the so–called *De Moivre–Euler–Binet formula*

$$F_n = \frac{1}{\sqrt{5}} \left(\phi^n - (-\phi)^{-n} \right),$$

proved by A. De Moivre in 1730, L. Euler in 1765 and P.M. Binet in 1843. It follows that for $n \geq 0$, F_n is the nearest integer to $\phi^n/\sqrt{5}$. Further,

$$F_0 + F_1 z + F_2 z^2 + \cdots + F_n z^n + \cdots = \frac{z}{1 - z - z^2}.$$

References

[1] B. ADAMCZEWSKIAND J. BELL, *On vanishing coefficients of algebraic power series over fields of positive characteristic*. Invent. Math. **187** (2012), no. 2, 343–393.

[2] A.F. BEARDON, *Iteration of rational functions*. New York : Springer-Verlag, Graduate texts in mathematics **132** (1991).
`http://trove.nla.gov.au/result?q=text%3A%22Graduate+texts+in+mathematics+%3B%22`

[3] J. BELL, *A generalised Skolem-Mahler-Lech theorem for affine varieties*. `arXiv:math/0501309v2 [math.NT]`

[4] J. BELL, S. N. BURRIS AND K. YEATS, *On the set of zero coefficients of a function satisfying a linear differential equation*. Math. Proc. Cambridge Philos. Soc. **153** (2012), no. 2, 235–247.

[5] YU. BILU, *The many faces of the subspace theorem [after Adamczewski, Bugeaud, Corvaja, Zannier...]*. Séminaire Bourbaki. Vol. 2006/2007. Astérisque No. **317** (2008), Exp. No. 967, vii, 1–38.
`http://www.math.u-bordeaux1.fr/~ybilu/publ/preprs/subspace.pdf`

[6] E. BOMBIERI AND W. GUBLER, *Heights in Diophantine geometry*. New Mathematical Monographs, **4**. Cambridge University Press, Cambridge, 2006.
`http://www.cambridge.org/fr/academic/subjects/mathematics/number-theory/heights-diophantine-geometry?format=PB`

[7] L. CERLIENCO, M. MIGNOTTE AND F. PIRAS, *Suites récurrentes linéaires — Propriétés algébriques et arithmétiques*. L'Enseignement Mathématique, **33** (1987) 67–108.
`http://retro.seals.ch/digbib/erez4?rid=ensmat-001:1987:33::200`

[8] P. CORVAJA, *Rational fixed points for linear group actions*. Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) **6** (2007), no. 4, 561–597.
`http://annaliscienze.sns.it/index.php?page=Article&id=107`

[9] P. CORVAJA AND U. ZANNIER, *Applications of the Subspace Theorem to certain Diophantine problems: a survey of some recent results*. Diophantine approximation, 161–174, Dev. Math., **16**, Springer Verlag, 2008.
`http://www.springer.com/mathematics/algebra/book/978-3-211-74279-2`

[10] R.L. Devaney, *Complex exponential dynamics.* In "Handbook of Dynamical Systems", Vol. **3**. Eds. H. Broer, F. Takens, B. Hasselblatt. 2010, 125-224.
`http://math.bu.edu/people/bob/papers/notes.pdf`

[11] G. Everest, A.J. Van Der Poorten, I.E. Shparlinski and T. Ward *Recurrence sequences.* Mathematical Surveys and Monographs **104**, American Mathematical Society 2003; 318 pp.
`http://www.ams.org/bookstore?fn=20&arg1=survseries&item=SURV-104`

[12] Hu, Pei-Chu and Yang, Chung-Chun *Distribution theory of algebraic numbers.* de Gruyter Expositions in Mathematics, **45**. Walter de Gruyter GmbH and Co. KG, Berlin, 2008.

[13] S. Marmi, *An Introduction to small divisors.* (2000), 91p.
`arXiv:math/0009232 [math.DS]`

[14] J. Milnor, *Dynamics in one complex variable: introductory lectures.* Report Number Stony Brook IMS 1990/5.
`arXiv:math/9201272 [math.DS]`

[15] A.J. Van der Poorten, *Some determinants that should be better known.* J. Austral. Math. Soc. Ser. A **21** (1976), no. 3, 278–288.
`http://dx.doi.org/10.1017/S1446788700018577`

[16] H.P. Schlickewei, W.M. Schmidt and M. Waldschmidt, *Zeros of linear recurrence sequences.* Manuscripta Mathematica, **98** n°2 (1999), 225–241.
`http://link.springer.com/article/10.1007/s002290050136`

[17] W.M. Schmidt, *Diophantine approximations and Diophantine equations.* Lecture Notes in Mathematics, **1467**. Springer-Verlag, Berlin, 1991.
`http://link.springer.com/book/10.1007/BFb0098246`

[18] W.M. Schmidt, *The zero multiplicity of linear recurrence sequences.* Acta Math. **182** (1999), no. 2, 243–282.
`http://link.springer.com/article/10.1007/BF02392575`

[19] W.M. Schmidt, *Linear recurrence sequences.* In "Diophantine approximation (Cetraro 2000)", Lecture Notes in Math., **1819**, Springer, Berlin (2003), 171–247.
`http://www.springer.com/mathematics/numbers/book/978-3-540-40392-0`

[20] T.N. Shorey and R. Tijdeman, *Exponential Diophantine equations.* Cambridge Tracts in Mathematics, **87**. Cambridge University Press, Cambridge, 1986.
http://www.cambridge.org/us/academic/subjects/mathematics/number-theory/exponential-diophantine-equations

[21] S. Smale, *Differentiable dynamical systems.* Bulletin of the American Mathematical Society. Volume **73**, N°6 (1967), 747-817.
http://projecteuclid.org/ euclid.bams/1183529092

[22] T. Tao, *Effective Skolem Mahler Lech theorem.* In "Structure and Randomness: pages from year one of a mathematical blog", American Mathematical Society (2008), 298 pages.
http://terrytao.wordpress.com/2007/05/25/open-question-effective-skolem-mahler-lech-theorem/

[23] N. Tosel, *Le théorème de Skolem–Mahler–Lech.* Revue de la filière mathématique RMS **116**, no.1, 2005-2006, 47–58.
http://www.rms-math.com/index.php?option=com_staticxt&Itemid=66&staticfile=RMS116-18.html

[24] P. Vojta, *Diophantine approximations and value distribution theory.* Lecture Notes in Mathematics, **1239**. Springer-Verlag, Berlin, 1987.
http://link.springer.com/book/10.1007/BFb0072989

[25] U. Zannier, *Some applications of Diophantine Approximation to Diophantine Equations. With Special Emphasis on the Schmidt Subspace Theorem.* Forum Editrice Universitaria Udinese, Udine, 2003, 70 pages.
www.unilibro.it/find_buy/Scheda/libreria/autore-zannier_umberto/sku-12027409/some_applications_of_diophantine_approx

[26] U. Zannier, *Diophantine equations with linear recurrences. An overview of some recent progress.* J. Théor. Nombres Bordeaux, **17** n°1 (2005), 423–435.
http://jtnb.cedram.org/jtnb-bin/fitem?id=JTNB_2005__17_1_423_0

[27] U. Zannier, *Lecture Notes on Diophantine Analysis.* Appunti. Scuola Normale Superiore di Pisa (Nuova Serie) [Lecture Notes. Scuola Normale Superiore di Pisa (New Series)], **8**. Edizioni della Normale, Pisa, 2009.
http://books.google.fr/books/

Michel WALDSCHMIDT
UPMC Univ Paris 06, UMR 7586-IMJ
F–75005 Paris France
e-mail: miw@math.jussieu.fr
URL: http://www.math.jussieu.fr/∼miw/