ICPAM2 - GOROKA 2014

International Conference on Pure and Applied Mathematics.
"Contemporary Developments in the Mathematical Sciences as Tools for Scientific and Technological Transformation of Papua New Guinea"

Linear recurrence sequences and twisted binary forms

Claude Levesque and *Michel Waldschmidt*

Abstract

Let $\prod_{i=1}^d (X-\alpha_i Y) \in \mathbb{C}[X,Y]$ be a binary form and let $\epsilon_1, \dots, \epsilon_d$ be nonzero complex numbers. We consider the family of binary forms $\prod_{i=1}^d (X-\alpha_i \epsilon_i^a Y)$, $a \in \mathbb{Z}$, which we write as

$$X^d - U_1(a)X^{d-1}Y + \cdots + (-1)^{d-1}U_{d-1}(a)XY^{d-1} + (-1)^d U_d(a)Y^d.$$

In this paper we study these sequences $\big(U_h(a)\big)_{a\in\mathbb{Z}}$ which turn out to be linear recurrence sequences.

Résumé

Soit $\prod_{i=1}^d (X-\alpha_i Y)$ une forme binaire de $\mathbb{C}[X,Y]$ et soit $\epsilon_1, \dots, \epsilon_d$ des nombres complexes non nuls. Nous considérons la famille des formes binaires $\prod_{i=1}^d (X-\alpha_i \epsilon_i^a Y)$, $a \in \mathbb{Z}$, que nous écrivons sous la forme

$$X^d - U_1(a)X^{d-1}Y + \cdots + (-1)^{d-1}U_{d-1}(a)XY^{d-1} + (-1)^d U_d(a)Y^d.$$

Le but de cet article est d'étudier ces suites $\big(U_h(a)\big)_{a\in\mathbb{Z}}$ qui s'avèrent être des suites récurrentes linéaires.

`Keywords:` Linear recurrence sequences; binary forms; units of algebraic number fields; families of Diophantine equations; exponential polynomials

`AMS Mathematics Subject Classification(2010):` primary 11B37
Secundary: 05A15 11D61 33B10 39A10 65Q30

1 Introduction

Let us consider a binary form $F_0(X,Y) \in \mathbb{C}[X,Y]$ which satisfies $F_0(1,0) = 1$. We write it as

$$F_0(X,Y) = X^d + a_1 X^{d-1} Y + \cdots + a_d Y^d \ = \ \prod_{i=1}^{d} (X - \alpha_i Y).$$

Let $\epsilon_1, \ldots, \epsilon_d$ be d nonzero complex numbers not necessarily distinct. Twisting F_0 by the powers $\epsilon_1^a, \ldots, \epsilon_d^a$ ($a \in \mathbb{Z}$), we obtain the family of binary forms

$$F_a(X,Y) = \prod_{i=1}^{d} (X - \alpha_i \epsilon_i^a Y), \tag{1}$$

which we write as

$$F_a(X,Y) = X^d - U_1(a) X^{d-1} Y + \cdots + (-1)^{d-1} U_{d-1}(a) X Y^{d-1} + (-1)^d U_d(a) Y^d. \tag{2}$$

Therefore

$$U_h(0) = (-1)^h a_h \qquad (1 \le h \le d).$$

In [6] and [7], we consider some families of diophantine equations

$$F_a(x,y) = m$$

obtained in the same way from a given irreducible form $F(X,Y)$ with coefficients in $\mathbb{Z}$, when $\epsilon_1, \ldots, \epsilon_d$ are algebraic units and when the algebraic numbers $\alpha_1 \epsilon_1, \ldots, \alpha_d \epsilon_d$ are Galois conjugates with $d \ge 3$. The results in [7] are effective, the results in [6] are more general but not effective. The next result follows from Theorem 3.3 of [6].

Theorem 1. *Let K be a number field of degree $d \ge 3$, S a finite set of places of K containing the places at infinity. Denote by $\mathcal{O}_S$ the ring of S–integers of K and by $\mathcal{O}_S^\times$ the group of S–units of K. Assume $\alpha_1, \ldots, \alpha_d, \epsilon_1, \ldots, \epsilon_d$ belong to $K^\times$. Then there are only finitely many (x,y,a) in $\mathcal{O}_S \times \mathcal{O}_S \times \mathbb{Z}$ satisfying*

$$F_a(x,y) \in \mathcal{O}_S^\times, \quad xy \neq 0 \quad \textit{and} \quad \mathrm{Card}\{\alpha_1 \epsilon_1^a, \ldots, \alpha_d \epsilon_d^a\} \ge 3.$$

Section 2 is an introduction to linear recurrence sequences. In Section 3 we observe that in the general case each of the sequences $\big(U_h(a)\big)_{a \in \mathbb{Z}}$ coming from the coefficients of the relation (2) is a linear recurrence sequence.

2 Linear recurrence sequences

Let us recall some well known facts about linear recurrence sequences; (see for instance [10], Chapter C of [11], and also [1], [2], [4], [5], [9]). Then we apply these results to the families of binary forms given in (1) and (2).

2.1 Generalities

Let $\mathbb{K}$ be a field of characteristic 0. The sequences $\big(u(a)\big)_{a\in\mathbb{Z}}$, with values in $\mathbb{K}$ and indexed by $\mathbb{Z}$, form a vector space $\mathbb{K}^{\mathbb{Z}}$ over $\mathbb{K}$. Let $\mathbf{c}=(c_1,\dots,c_d)\in\mathbb{K}^d$ with $c_d\neq 0$. The sequences, satisfying the linear recurrence relation of order d given by

$$u(a+d)=c_1u(a+d-1)+\cdots+c_du(a), \tag{3}$$

form a $\mathbb{K}$–vector subspace $E_{\mathbf{c}}$ of $\mathbb{K}^{\mathbb{Z}}$ of dimension d, a natural canonical basis being given by the d sequences $u_0,\dots,u_{d-1}$ defined by the initial conditions

$$u_j(a)=\delta_{ja}\quad(0\le j,a\le d-1),$$

δ_{ja} being the Kronecker symbol

$$\delta_{ja}=\begin{cases}1 & \text{if } j=a,\\ 0 & \text{if } j\neq a.\end{cases}$$

For $u\in E_{\mathbf{c}}$, we have

$$u=u(0)u_0+u(1)u_1+\cdots+u(d-1)u_{d-1}.$$

By definition, the characteristic polynomial of the linear recurrence relation (3) is

$$P(T)=T^d-c_1T^{d-1}-\cdots-c_{d-1}T-c_d\in\mathbb{K}[T],$$

where $P(0)=-c_d\neq 0$.

A sequence $u\in\mathbb{K}^{\mathbb{Z}}$ satisfies a linear recurrence relation of order $\le d$ if and only if the sequences

$$\big(u(a+j)\big)_{a\in\mathbb{Z}}\quad(j=0,1,2,\dots)$$

generate a vector space over $\mathbb{K}$ of dimension $\le d$. Remark that a linear recurrence relation of order d may be viewed as a linear recurrence relation of order $d+s$ for any $s\ge 1$. The dimension d_0 of this vector space is the minimal order of the linear recurrence relation satisfied by u. The linear recurrence relation of order d_0 satisfied by u is unique; the characteristic polynomial of this relation generates an ideal of $\mathbb{K}[T]$ and the characteristic polynomials of these linear recurrence relations satisfied by u are the monic polynomials of this ideal.

2.2 Decomposed characteristic polynomial

As a preliminary step, let us assume that the polynomial $P(T)$ of degree d splits completely in $\mathbb{K}[T]$ as a product of linear factors:

$$P(T) = \prod_{j=1}^{\ell} (T - \gamma_j)^{t_j}$$

with $t_j \geq 1,\ \ t_1 + \cdots + t_\ell = d$ and with nonvanishing pairwise distinct elements $\gamma_1, \ldots, \gamma_\ell$. Let us prove that a basis of $E_{\mathbf{c}}$ is given by the d sequences

$$\left(a^i \gamma_j^a\right)_{a\in\mathbb{Z}} \quad (1 \leq j \leq \ell,\ \ 0 \leq i \leq t_j - 1).$$

Firstly, we will show that these d sequences belong to the vector space $E_{\mathbf{c}}$ (this part was omitted in [5]). Next, we will prove that they form a linearly independent subset of $E_{\mathbf{c}}$.

By hypothesis, for $1 \leq j \leq \ell$ and $0 \leq i \leq t_j - 1$, the derivative of order i of the polynomial $P(T)$ is vanishing at the point γ_j. Let us recall that the characteristic of $\mathbb{K}$ is 0. Instead of using the operator $\mathrm{d}/\mathrm{d}T$, we will use the operator $T\mathrm{d}/\mathrm{d}T$ which has the property

$$\left(T\frac{\mathrm{d}}{\mathrm{d}T}\right)^i T^h = h^i T^h$$

for $i \geq 0$ and $h \geq 0$; we stipulate that $h^i = 1$ for $i = h = 0$. For $a \in \mathbb{Z}$, $1 \leq j \leq \ell$ and $0 \leq i \leq t_j - 1$, the equation

$$\left(T\frac{\mathrm{d}}{\mathrm{d}T}\right)^i (T^a P)(\gamma_j) = 0$$

can be written as

$$(a+d)^i \gamma_j^{a+d} = \sum_{k=1}^{d} (a+d-k)^i c_k \gamma_j^{a+d-k} \qquad (a \in \mathbb{Z}),$$

with the convention that for $k = a + d$, the term $(a + d - k)^i$ takes the value 1 for $i = 0$ and the value 0 for $i \geq 1$. Therefore the sequence $\left(a^i \gamma_j^a\right)_{a \in \mathbb{Z}}$ belongs to the vector space $E_{\mathbf{c}}$ for $1 \leq j \leq \ell$ and $0 \leq i \leq t_j - 1$.

Remark. In the literature, there are at least two further classical proofs of this fact. One is to write the linear recurrence relation in a matrix form

$$U(a+1) = CU(a)$$

with

$$U(a) = \begin{pmatrix} u(a) \\ u(a+1) \\ \vdots \\ u(a+d-1) \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ c_d & c_{d-1} & c_{d-2} & \cdots & c_1 \end{pmatrix}.$$

The determinant of $I_d T - C$ (the characteristic polynomial of C) is nothing but $P(T)$. To obtain the result, one writes the matrix C in its Jordan normal form.

The other method consists in introducing the formal power series

$$U(z) = \sum_{a \geq 0} u(a) z^a.$$

One has

$$\left(1 - \sum_{i=1}^{d} c_i z^i\right) U(z) = \sum_{j=0}^{d-1} \left(u(j) - \sum_{i=1}^{j} c_i u(j-i)\right) z^j.$$

Hence $U(z)$ is a rational fraction, with denominator

$$1 - \sum_{i=1}^{d} c_i z^i = z^d P(1/z) = \prod_{j=1}^{\ell} (1 - \gamma_j z)^{t_j},$$

while the numerator is of degree $< d$. This rational fraction can be rewritten using a partial fraction decomposition:

$$U(z) = \sum_{j=1}^{\ell} \sum_{i=0}^{t_j - 1} \frac{q_{ij}}{(1 - \gamma_j z)^{i+1}}.$$

For $1 \le j \le \ell$, one develops $(1-\gamma_j z)^{-i-1}$ as a power series expansion to get

$$\frac{1}{(1-\gamma_j z)^{i+1}} = \frac{1}{i!\gamma_j^i}\left(\frac{\mathrm{d}}{\mathrm{d}z}\right)^i \frac{1}{1-\gamma_j z} = \sum_{a\ge 0} \frac{(a+1)(a+2)\cdots(a+i)}{i!}\gamma_j^a z^a.$$

This allows to write $u(a)$ as a linear combination of the elements γ_j^a with coefficients being polynomials of degree $< t_j$ evaluated at a.

Proving the linear independence of the set of the d sequences

$$\left(a^i \gamma_j^a\right)_{a\in\mathbb{Z}}, \qquad \text{with } 1 \le j \le \ell \text{ and } 0 \le i \le t_j - 1,$$

boils down to showing that the determinant of the matrix

$$A = \left(\begin{array}{ccccccc}
1 & \gamma_1 & \gamma_1^2 & \dots & \gamma_1^k & \dots & \gamma_1^{d-1} \\
0 & 1 & 2\gamma_1 & \dots & k\gamma_1^{k-1} & \dots & (d-1)\gamma_1^{d-2} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \dots & \binom{k}{t_1-1}\gamma_1^{k-t_1+1} & \dots & \binom{d-1}{t_1-1}\gamma_1^{d-t_1} \\
\hline
1 & \gamma_2 & \gamma_2^2 & \dots & \gamma_2^k & \dots & \gamma_2^{d-1} \\
0 & 1 & 2\gamma_2 & \dots & k\gamma_2^{k-1} & \dots & (d-1)\gamma_2^{d-2} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \dots & \binom{k}{t_2-1}\gamma_2^{k-t_2+1} & \dots & \binom{d-1}{t_2-1}\gamma_2^{d-t_2} \\
\hline
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\hline
1 & \gamma_\ell & \gamma_\ell^2 & \dots & \gamma_\ell^k & \dots & \gamma_\ell^{d-1} \\
0 & 1 & 2\gamma_\ell & \dots & k\gamma_\ell^{k-1} & \dots & (d-1)\gamma_\ell^{d-2} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \dots & \binom{k}{t_\ell-1}\gamma_\ell^{k-t_\ell+1} & \dots & \binom{d-1}{t_\ell-1}\gamma_\ell^{d-t_\ell}
\end{array}\right) \tag{4}$$

is different from 0. Note that $\displaystyle\binom{r}{k} = 0$ for $r < k$. Let us define s_j to be

$$s_j = t_1 + \cdots + t_{j-1} \quad \text{for} \quad 1 \le j \le \ell \text{ with } s_1 = 0.$$

For $1 \le j \le \ell$, $0 \le i \le t_j - 1$, $0 \le k \le d-1$, the $(s_j + i, k)$ entry of the matrix A is

$$\frac{1}{i!}\left(\frac{\mathrm{d}}{\mathrm{d}T}\right)^i T^k \bigg|_{T=\gamma_j} = \binom{k}{i}\gamma_j^{k-i}.$$

As a matter of fact, A is best described as being made of ℓ vertical blocks $A_1, A_2, \dots, A_\ell$ where for $1 \le j \le \ell$, A_j is the $t_j \times d$ matrix

$$A_j = \begin{pmatrix} 1 & \gamma_j & \gamma_j^2 & \cdots & \gamma_j^{t_j-1} & \gamma_j^{t_j} & \cdots & \gamma_j^{d-1} \\ 0 & 1 & \binom{2}{1}\gamma_j & \cdots & \binom{t_j-1}{1}\gamma_j^{t_j-2} & \binom{t_j}{1}\gamma_j^{t_j-1} & \cdots & \binom{d-1}{1}\gamma_j^{d-2} \\ 0 & 0 & 1 & \cdots & \binom{t_j-1}{2}\gamma_j^{t_j-3} & \binom{t_j}{2}\gamma_j^{t_j-2} & \cdots & \binom{d-1}{2}\gamma_j^{d-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & \binom{t_j}{t_j-1}\gamma_j & \cdots & \binom{d-1}{t_j-1}\gamma_j^{d-t_j} \end{pmatrix}. \tag{5}$$

Denote by $C_0, \dots, C_{d-1}$ the d columns of A. Let $b_0, \dots, b_{d-1}$ be complex numbers such that

$$b_0 C_0 + \cdots + b_{d-1} C_{d-1} = \mathbf{0}.$$

The left side of this equality is an element of $\mathbb{K}^d$, the d components of which are all 0, and these d relations mean that the polynomial

$$b_0 + b_1 T + \cdots + b_{d-1} T^{d-1}$$

vanishes at the point γ_j with multiplicity at least t_j for $1 \le j \le \ell$. Since $t_1 + \cdots + t_\ell = d$, we deduce that $b_0 = \cdots = b_{d-1} = 0$.

The determinant of A was calculated in [5]:

$$\det A = \prod_{1 \le i < j \le \ell} (\gamma_j - \gamma_i)^{t_i t_j}.$$

2.3 Interpolation.

The matrix A is associated with the linear system of d equations in d unknowns which amounts to finding a polynomial $f \in \mathbb{K}[z]$ of degree $< d$ for which the d numbers

$$\frac{\mathrm{d}^i f}{\mathrm{d} z^i}(\gamma_j), \qquad (1 \le j \le \ell,\ 0 \le i \le t_j - 1)$$

take prescribed values. Sharp estimates related with this linear system are provided by Lemma 3.1 of [8].

Before stating and proving the next proposition, we introduce the following notation.

Let $g \in \mathbb{K}(z)$, let $z_0 \in \mathbb{K}$ and let $t \geq 1$. Assume z_0 is not a pole of g. We set

$$T_{g,z_0,t}(z) = \sum_{i=0}^{t-1} \frac{\mathrm{d}^i g}{\mathrm{d}z^i}(z_0) \frac{(z-z_0)^i}{i!}.$$

In other words, $T_{g,z_0,t}$ is the unique polynomial in $\mathbb{K}[z]$ of degree $< t$ such that there exists $r(z) \in \mathbb{K}(z)$ having no pole at z_0 with

$$g(z) = T_{g,z_0,t}(z) + (z-z_0)^t r(z).$$

Notice that if g is a polynomial of degree $< t$, then $g = T_{g,z_0,t}$ for any $z_0 \in \mathbb{K}$.

Proposition 1. *Let γ_j ($1 \leq j \leq \ell$) be distinct elements in $\mathbb{K}$, t_j ($1 \leq j \leq \ell$) be positive integers, η_{ij} ($1 \leq j \leq \ell$, $0 \leq i \leq t_j - 1$) be elements in $\mathbb{K}$. Set $d = t_1 + \cdots + t_\ell$. There exists a unique polynomial $f \in \mathbb{K}[z]$ of degree $< d$ satisfying*

$$\frac{\mathrm{d}^i f}{\mathrm{d}z^i}(\gamma_j) = \eta_{ij}, \qquad (1 \leq j \leq \ell,\ 0 \leq i \leq t_j - 1). \tag{6}$$

For $j = 1, \ldots, \ell$, define

$$h_j(z) = \prod_{\substack{1 \leq k \leq \ell \\ k \neq j}} \left(\frac{z-\gamma_k}{\gamma_j - \gamma_k} \right)^{t_k} \quad \text{and} \quad p_j(z) = \sum_{i=0}^{t_j-1} \eta_{ij} \frac{(z-\gamma_j)^i}{i!}.$$

Then the solution f of the interpolation problem (6) *is given by*

$$f = \sum_{j=1}^{\ell} h_j T_{\frac{p_j}{h_j},\gamma_j,t_j}. \tag{7}$$

Proof. The conditions (6) can be written

$$T_{f,\gamma_k,t_k} = p_k \quad \text{for} \quad k = 1, \ldots, \ell.$$

The unicity is clear: the difference between two solutions is a polynomial of degree $< d$ which vanishes at d points (including multiplicity), hence is the zero polynomial.

Since $h_j(\gamma_j) = 1$, the quantity $q_j = T_{\frac{p_j}{h_j},\gamma_j,t_j}$ is well defined and is a polynomial of degree $< t_j$. Since h_j is a polynomial of degree $d - t_j$, the polynomial f in (7), namely

$$f = h_1 q_1 + \cdots + h_\ell q_\ell,$$

is a polynomial of degree $< d$. Let us prove that this polynomial f verifies the equalities in (6). For $1 \leq k \neq j \leq \ell$ and $0 \leq i \leq t_k - 1$, we have

$$\frac{\mathrm{d}^i h_j}{\mathrm{d}z^i}(\gamma_k) = 0,$$

and therefore also

$$\frac{\mathrm{d}^i (h_j q_j)}{\mathrm{d}z^i}(\gamma_k) = 0.$$

Hence, for the function f given by (7) and for $1 \leq k \leq \ell$, $0 \leq i \leq t_k - 1$, we have

$$\frac{\mathrm{d}^i f}{\mathrm{d}z^i}(\gamma_k) = \frac{\mathrm{d}^i (h_k q_k)}{\mathrm{d}z^i}(\gamma_k).$$

In other words, for $1 \leq k \leq \ell$, we have

$$T_{f,\gamma_k,t_k} = T_{h_k q_k,\gamma_k,t_k}.$$

By definition of T, the function $q_k - \dfrac{p_k}{h_k}$ has a zero of multiplicity $\geq t_k$ at γ_k, hence the same is true for the function $h_k q_k - p_k$. Therefore, for any $k \in \{1, \ldots, \ell\}$, we have

$$T_{h_k q_k,\gamma_k,t_k} = p_k,$$

whereupon, $T_{f,\gamma_k,t_k} = p_k$. This completes the proof. □

The Lagrange–Hermite interpolation formula [3] deals with this question when $\mathbb{K} = \mathbb{C}$ and when the values η_{ij} are of the form

$$\eta_{ij} = \frac{\mathrm{d}^i F}{\mathrm{d}z^i}(\gamma_j) \qquad (1 \leq j \leq \ell,\ 0 \leq i \leq t_j - 1)$$

for a function F which is analytic in a domain containing the points $\gamma_1, \ldots, \gamma_\ell$.

Proposition 2. *Let D be a domain in $\mathbb{C}$, F an analytic function in D, $\gamma_1, \ldots, \gamma_\ell$ distinct points in D and Γ a simple curve inside which the points $\gamma_1, \ldots, \gamma_\ell$ are located. Then the unique polynomial $f \in \mathbb{C}[z]$ of degree $< d$ satisfying*

$$\frac{\mathrm{d}^i f}{\mathrm{d}z^i}(\gamma_j) = \frac{\mathrm{d}^i F}{\mathrm{d}z^i}(\gamma_j), \qquad (1 \leq j \leq \ell,\ 0 \leq i \leq t_j - 1)$$

is given, for z inside Γ, by

$$f(z) = F(z) + \frac{1}{2i\pi} \int_\Gamma \Phi(\zeta) d\zeta$$

with

$$\Phi(\zeta) = \frac{F(\zeta)}{z-\zeta} \prod_{j=1}^{\ell} \left(\frac{z-\gamma_j}{\zeta-\gamma_j} \right)^{t_j}.$$

Proof. The residue at $\zeta = z$ of $\Phi(\zeta)$ is $-F(z)$. Under the assumptions of Proposition 2 and with the notations of Proposition 1, we have

$$p_j = T_{F,\gamma_j,t_j}.$$

It remains to show that for $1 \leq j \leq \ell$, the residue at $\zeta = \gamma_j$ of $\Phi(\zeta)$ is

$$h_j(z) T_{\frac{p_j}{h_j},\gamma_j,t_j}(z).$$

We first notice that for $m \in \mathbb{Z}$ and $t \in \mathbb{Z}$ with $t \geq 0$, the residue at $\zeta = 0$ of

$$\zeta^m \left(\frac{z}{\zeta} \right)^t \frac{1}{z-\zeta}$$

is z^m for $m \leq t-1$ and $z \neq 0$, and is 0 otherwise, namely for $z = 0$ as well as for $m \geq t$. Therefore, when $\varphi(\zeta)$ is analytic at $\zeta = \gamma$, the residue at $\zeta = \gamma$ of

$$\varphi(\zeta) \left(\frac{z-\gamma}{\zeta-\gamma} \right)^t \frac{1}{z-\zeta}$$

is $T_{\varphi,\gamma,t}(z)$. Since

$$\Phi(\zeta) = \frac{F(\zeta)}{z-\zeta} \left(\frac{z-\gamma_j}{\zeta-\gamma_j} \right)^{t_j} \frac{h_j(z)}{h_j(\zeta)},$$

and since $h_j(\gamma_j) \neq 0$, the residue at $\zeta = \gamma_j$ of $\Phi(\zeta)$ is

$$h_j(z) T_{\frac{F}{h_j},\gamma_j,t_j}(z).$$

Finally, we notice that when φ_1 and φ_2 are analytic at γ, then $T_{\varphi_1\varphi_2,\gamma,t} = T_{\widetilde{\varphi}_1\varphi_2,\gamma,t}$ with $\widetilde{\varphi}_1 = T_{\varphi_1,\gamma,t}$. This final remark with $\gamma = \gamma_j$, $t = t_j$, $\varphi_1 = F$, $\widetilde{\varphi}_1 = p_j$, $\varphi_2 = 1/h_j$ completes the proof.

□

There are other formulae for the solution to the interpolation problem (6). For instance, writing t_j times each γ_j, one gets a sequence $z_1, \ldots, z_d$, and the so–called *Newton's divided differences interpolation polynomials* give formulae for the coefficients $c_0, \ldots, c_{d-1}$ in

$$f(z) = c_0 + c_1(z-z_1) + c_2(z-z_1)(z-z_2) + \cdots + c_{d-1}(z-z_1)(z-z_2)\cdots(z-z_{d-1}).$$

2.4 Polynomial combinations of powers.

From the preceding sections, we deduce that the linear recurrence sequences over an algebraically closed field of characteristic 0 are in bijection with the linear combinations of the powers γ_j^a $(1 \leq j \leq \ell)$ with polynomial coefficients of the form

$$u(a) = \sum_{j=1}^{\ell} \sum_{i=0}^{t_j-1} v_{ij} a^i \gamma_j^a \qquad (a \in \mathbb{Z}). \tag{8}$$

The piece of data $\mathbf{c} = (c_1, \ldots, c_d) \in \mathbb{K}^d$ is equivalent to being given ℓ distinct nonzero complex numbers $\gamma_1, \ldots, \gamma_\ell$ and ℓ positive integers $t_1, \ldots, t_\ell$ together with the property that

$$T^d - c_1 T^{d-1} - \cdots - c_{d-1} T - c_d = \prod_{j=1}^{\ell} (T - \gamma_j)^{t_j}$$

with $d = t_1 + \cdots + t_\ell$.

A change of basis for $\mathbb{K}^d$, involving the transition matrix

$$\left(a^i \gamma_j^a\right)_{\substack{0 \leq a \leq d-1 \\ 1 \leq j \leq \ell, 0 \leq i \leq t_j - 1}},$$

allows to switch from the initial conditions $u(a)$ for $0 \leq a \leq d-1$ to the d coefficients v_{ij} of (8).

Since

$$\frac{1}{1 - \gamma_j z} = \sum_{a \geq 0} (\gamma_j z)^a$$

and

$$\left(z \frac{\mathrm{d}}{\mathrm{d}z}\right)^i (\gamma_j z)^a = a^i (\gamma_j z)^a,$$

the generating function of the sequence $\big(u(a)\big)_{a \in \mathbb{Z}}$ given by (8) is

$$U(z) = \sum_{a \geq 0} u(a) z^a = \sum_{j=1}^{\ell} \sum_{i=0}^{t_j-1} v_{ij} \left(z \frac{\mathrm{d}}{\mathrm{d}z}\right)^i \left(\frac{1}{1 - \gamma_j z}\right),$$

which is a rational fraction with denominator $\displaystyle\prod_{j=1}^{\ell} (1 - \gamma_j z)^{t_j}$, as expected.

2.5 The ring of linear recurrence sequences.

A sum and a product of two polynomial combinations of powers is still a polynomial combination of powers. If U_1 and U_2 are two linear recurrence sequences of characteristic polynomials P_1 and P_2 respectively, then $U_1 + U_2$ satisfies the linear recurrence, the characteristic polynomial of which is

$$\frac{P_1 P_2}{\gcd(P_1, P_2)}.$$

Consequently, the union of all vector spaces $E_{\mathbf{c}}$, with $\mathbf{c}$ running through the set of d–tuples $(c_1, \ldots, c_d) \in \mathbb{K}^d$ subject to $c_d \neq 0$, and d running through the set of integers ≥ 1, is still a vector subspace of $\mathbb{K}^{\mathbb{Z}}$.

Moreover, if the characteristic polynomials of the two linear recurrence sequences U_1 and U_2 are respectively

$$P_1(T) = \prod_{j=1}^{\ell} (T - \gamma_j)^{t_j} \quad \text{and} \quad P_2(T) = \prod_{k=1}^{\ell'} (T - \gamma'_k)^{t'_k},$$

then $U_1 U_2$ satisfies the linear recurrence, the characteristic polynomial of which is

$$\prod_{j=1}^{\ell} \prod_{k=1}^{\ell'} (T - \gamma_j \gamma'_k)^{t_j + t'_k - 1}.$$

As a consequence, the linear recurrence sequences form a ring.

2.6 Non homogeneous linear recurrence sequences

Let us suppose now that a factorisation of the characteristic polynomial $P(T)$ of a linear recurrence relation is of the form $P = QR$, with R completely decomposed in $\mathbb{K}[T]$. Let us write

$$P(T) = T^d - \sum_{i=1}^{d} c_i T^{d-i}, \quad Q(T) = T^m - \sum_{i=1}^{m} b_i T^{m-i}, \quad R(T) = \prod_{j=1}^{\ell} (T - \gamma_j)^{t_j}.$$

Hence $d = m + t_1 + \cdots + t_\ell$. Then the elements of $E_{\mathbf{c}}$ are the sequences $\big(u(a)\big)_{a \in \mathbb{Z}}$ for which there exist $d - m$ elements

$$\lambda_{ij} \qquad (1 \leq j \leq \ell, \quad 0 \leq i \leq t_j - 1)$$

in $\mathbb{K}$ such that

$$u(a+m) = b_1 u(a+m-1) + \cdots + b_m u(a) + \sum_{j=1}^{\ell} \sum_{i=0}^{t_j-1} \lambda_{ij} a^i \gamma_j^a. \tag{9}$$

In order to define an element $\big(u(a)\big)_{a\in\mathbb{Z}}$ of $E_{\mathbf{c}}$ by using the homogenous recurrence relation in (3), we have to give d initial values, for instance $u(0), \ldots, u(d-1)$. In order to define this sequence by using the non homogeneous recurrence relation (9), it is sufficient to have m initial conditions, say $u(0), \ldots, u(m-1)$, but we also have to know the elements λ_{ij} for $1 \le j \le \ell$ and $0 \le i \le t_j - 1$ (which altogether are d conditions, as is required in a vector space of dimension d).

Consider the transition matrix associated to the change of basis, allowing to switch from the initial conditions

$$u(a) \text{ for } 0 \le a \le d-1$$

to the initial conditions

$$u(a) \text{ for } 0 \le a \le m-1 \text{ and } \lambda_{ij} \text{ for } 1 \le j \le \ell \text{ and } 0 \le i \le t_j - 1.$$

It is a matrix which has only a diagonal of two blocks,

$$\begin{pmatrix} I_m & 0 \\ 0 & A \end{pmatrix} \quad \text{with} \quad A = \begin{pmatrix} A_1 \\ \vdots \\ A_\ell \end{pmatrix}.$$

The first block I_m is the $m \times m$ identity matrix. The second block A is a generalized Vandermonde matrix similar to the matrix in (4) made of the blocks $A_1, \ldots, A_\ell$ described in (5).

A particular case is the trivial one when $P = Q$, $m = d$ and $R = 1$. Another one is when $P = R$, $Q = 1$ and $m = 0$, which corresponds to the case studied in Section 2.2.

Example. Let us consider

$$P(T) = (T-\gamma)^2, \quad Q(T) = R(T) = T - \gamma.$$

There are three ways of defining an element $\big(u(a)\big)_{a\in\mathbb{Z}}$ of the vector space $E_{\mathbf{c}}$ when $\mathbf{c} = (2, -1)$. The first one is to mention that the sequence satisfies the binary linear recurrence relation

$$u(a+2) = 2u(a+1) - u(a) \quad (a \in \mathbb{Z})$$

and give two initial values, for, say $u(0)$ and $u(1)$. The second one is to write

$$u(a) = (\lambda_1 + \lambda_2 a)\gamma^a \quad (a \in \mathbb{Z})$$

and give the values of λ_1 and λ_2. The third one is in-between the previous ones; one writes that the sequence satisfies

$$u(a+1) = \gamma u(a) + \lambda\gamma^a \quad (a \in \mathbb{Z})$$

while providing an initial value, for, say $u(0)$, and the value of λ.

2.7 Exponential polynomials

The sequence of derivatives of an exponential polynomial evaluated at one point satisfies a linear recurrence relation. This allows us to deduce the following well known result (Ch. I, §7 of [12]).

Lemma 1. *Let $a_1(z), \dots, a_\ell(z)$ be nonzero polynomials of $\mathbb{C}[z]$ of degrees smaller than $t_1, \dots, t_\ell$ respectively. Let $\gamma_1, \dots, \gamma_\ell$ be distinct complex numbers. Let us suppose that the function*

$$F(z) = a_1(z)e^{\gamma_1 z} + \cdots + a_\ell(z)e^{\gamma_\ell z}$$

is not identically 0. Then its vanishing order at a point z_0 is smaller than or equal to $t_1 + \cdots + t_\ell - 1$.

Proof. Define $d = t_1 + \cdots + t_\ell$. We give two proofs of Lemma 1. A short one by induction on d is as follows. For $d = 1$ we have $\ell = 1$ and F has no zero. Assume $\ell \geq 2$. Without loss of generality we may assume $\gamma_1 = 0$. If F has a zero of multiplicity $\geq T_0$ at z_0, then $F(z) - a_1(z)$ has a zero of multiplicity $\geq T_0 - t_1$ at z_0. The result follows.

Our second proof relates Lemma 1 with linear recurrence sequences. We now assume $\gamma_1, \dots, \gamma_\ell$ all nonzero, as we may without loss of generality. Write the Taylor expansion of $F(z + z_0)$ at $z = 0$:

$$F(z + z_0) = \sum_{a \geq 0} \frac{u(a)}{a!} z^a.$$

Let us show that the sequence $(u(0), u(1), \dots, u(a), \dots)$ satisfies a linear recurrence relation of order $\leq d$. Define $a_{ij} \in \mathbb{C}$ by

$$a_j(z + z_0)e^{\gamma_j z_0} = \sum_{i=0}^{t_j - 1} a_{ij} z^i \quad (1 \leq j \leq \ell),$$

so that

$$F(z+z_0)=\sum_{j=1}^{\ell}\sum_{i=0}^{t_j-1} a_{ij}z^i e^{\gamma_j z}.$$

Since $\gamma_j\neq 0$ for $j=1,\ldots,\ell$,

$$u(a)=\sum_{j=1}^{\ell}\sum_{i=0}^{t_j-1} a_{ij}a(a-1)\cdots(a-i+1)\gamma_j^{a-i}$$

has the same form as in (8). Therefore the sequence $\bigl(u(a)\bigr)_{a\in\mathbb{Z}}$ satisfies a linear recurrence relation of order $\leq d$. It follows that the conditions

$$u(0)=\cdots=u(d-1)=0$$

imply $u(a)=0$ for any $a\geq 0$. $\square$

We can state this lemma in the following way: When the complex numbers γ_j are distinct, the determinant

$$\left|\left(\frac{\mathrm{d}}{\mathrm{d}z}\right)^a \left(z^i e^{\gamma_j z}\right)_{z=0}\right|_{\substack{0\leq i\leq t_j-1,\ 1\leq j\leq \ell\\ 0\leq a\leq d-1}}$$

is different from 0. This is no surprise that we come across the determinant of the matrix (4).

3 Families of binary forms

The equations (1) and (2) give, for $1\leq h\leq d$ and $a\in\mathbb{Z}$,

$$U_h(a)=\sum_{1\leq i_1<\cdots<i_h\leq d}\alpha_{i_1}\cdots\alpha_{i_h}(\epsilon_{i_1}\cdots\epsilon_{i_h})^a. \tag{10}$$

For example, for $a\in\mathbb{Z}$,

$$U_1(a)=\sum_{i=1}^{d}\alpha_i\epsilon_i^a,\quad U_d(a)=\prod_{i=1}^{d}\alpha_i\epsilon_i^a.$$

The relations (10) show that for $1\leq h\leq d$, the sequence $\bigl(U_h(a)\bigr)_{a\in\mathbb{Z}}$ is a linear combination of the sequences

$$\bigl((\epsilon_{i_1}\cdots\epsilon_{i_h})^a\bigr)_{a\in\mathbb{Z}},\quad (1\leq i_1<\cdots<i_h\leq d).$$

For $1 \leq h \leq d$, consider the set

$$\mathcal{E}_h = \{\epsilon_{i_1} \cdots \epsilon_{i_h} \ \mid \ 1 \leq i_1 < \cdots < i_h \leq d\}$$

and note m_h its cardinality. The elements of $\mathcal{E}_h$ are values of monomials in m_1 variables of degree h. The map from $\mathcal{E}_h$ to $\mathcal{E}_{d-h}$ defined by

$$\eta \mapsto \epsilon_1 \cdots \epsilon_d \eta^{-1}$$

is a bijection and we have

$$m_h = m_{d-h} \leq \min \left\{ \binom{d}{h}, \ \binom{m_1 + h - 1}{h}, \ \binom{m_1 + d - h - 1}{d - h} \right\}.$$

The sequence $\bigl(U_h(a)\bigr)_{a\in\mathbb{Z}}$ satisfies the linear recurrence relation of order m_h with the characteristic polynomial

$$\prod_{\eta \in \mathcal{E}_h} (T - \eta).$$

This polynomial is also written as

$$\prod_{\eta \in \mathcal{E}_{d-h}} (T - \epsilon_1 \cdots \epsilon_d \eta^{-1}),$$

which is matching (10) via

$$U_h(a) = U_d(a) \sum_{1 \leq j_1 < \cdots < j_{d-h} \leq d} (\alpha_{j_1} \cdots \alpha_{j_{d-h}})^{-1} (\epsilon_{j_1} \cdots \epsilon_{j_{d-h}})^{-a}.$$

For example, the sequence $\bigl(U_{d-1}(a)\bigr)_{a\in\mathbb{Z}}$ satisfies the linear recurrence relation of order d, the characteristic polynomial of which is

$$\prod_{i=1}^{d} (T - \epsilon_1 \cdots \epsilon_d \epsilon_i^{-1}) = (T - \epsilon_2 \cdots \epsilon_d)(T - \epsilon_1 \epsilon_3 \cdots \epsilon_d) \cdots (T - \epsilon_1 \cdots \epsilon_{d-1}).$$

The case $\epsilon_1 = \ldots = \epsilon_d$ is trivial: we have

$$U_h(a) = \epsilon_1^a U_h(0) = (-1)^h a_h \epsilon_1^a,$$

and each of the sequences $\bigl(U_h(a)\bigr)_{a\in\mathbb{Z}}$ satisfies

$$U_h(a+1) = \epsilon_1 U_h(a).$$

Let us consider the example

$$\epsilon_1 = \ldots = \epsilon_\ell = \epsilon, \quad \epsilon_{\ell+1} = \ldots = \epsilon_d = \eta,$$

with ϵ and η being two distinct complex numbers. We have

$$\mathcal{E}_1 = \{\epsilon, \eta\}, \qquad \mathcal{E}_{d-1} = \{\epsilon^{\ell-1}\eta^{d-\ell}, \epsilon^{\ell}\eta^{d-\ell-1}\}$$

and

$$\mathcal{E}_2 = \{\epsilon^2, \epsilon\eta, \eta^2\}, \quad \mathcal{E}_{d-2} = \{\epsilon^{\ell-2}\eta^{d-\ell}, \epsilon^{\ell-1}\eta^{d-\ell-1}, \epsilon^{\ell}\eta^{d-\ell-2}\}.$$

The sequence $\bigl(U_1(a)\bigr)_{a\in\mathbb{Z}}$ satisfies the binary recurrence relation, the characteristic polynomial of which is

$$(T-\epsilon)(T-\eta);$$

the sequence $\bigl(U_{d-1}(a)\bigr)_{a\in\mathbb{Z}}$ satisfies the binary recurrence relation, the characteristic polynomial of which is

$$(T-\epsilon^{\ell-1}\eta^{d-\ell})(T-\epsilon^{\ell}\eta^{d-\ell-1}),$$

while the sequence $\bigl(U_2(a)\bigr)_{a\in\mathbb{Z}}$ satisfies the ternary recurrence relation, the characteristic polynomial of which is

$$(T-\epsilon^2)(T-\eta^2)(T-\epsilon\eta).$$

In particular, if one writes

$$(T-\epsilon^2)(T-\eta^2) = T^2 - AT - B,$$

then there exists a constant $C \in \mathbb{C}$ such that, for any $a \in \mathbb{Z}$, one has

$$U_2(a+2) = AU_2(a+1) + BU_2(a) + C(\epsilon\eta)^a.$$

Finally, the sequence $\bigl(U_{d-2}(a)\bigr)_{a\in\mathbb{Z}}$ satisfies the ternary recurrence relation, the characteristic polynomial of which is

$$(T-\epsilon^{\ell-2}\eta^{d-\ell})(T-\epsilon^{\ell-1}\eta^{d-\ell-1})(T-\epsilon^{\ell}\eta^{d-\ell-2}).$$

Acknowledgments

The authors want to thank the organizers of the *Second International Conference on Pure and Applied Mathematics* held in Goroka (Papua New Guinea) and to express their gratitude to Samuel Kopamu for having invited them to give lectures. We are also thankful to Pietro Corvaja for two courses he gave on linear recurrence sequences, one in Bamako (Mali) in 2010 and the next one in Kozhikode (Kerala, India) in 2013.

References

[1] L. Cerlienko & M. Mignotte & F. Piras, *Suites récurrentes linéaires, propriétés algébriques et arithmétiques*, L'Enseignement Mathématique **33** (1987), 67–108.
`http://retro.seals.ch/cntmng?pid=ensmat-001:1987:33::17`

[2] G. Everest & A. van der Poorten & I. Shparlinski & T. Ward, *Recurrence Sequences*, Mathematical Surveys and Monographs **104**, American Mathematical Society 2003; 318 pp.
`http://www.ams.org/`

[3] Hermite, Ch., *Sur la formule d'interpolation de Lagrange*, (Extrait d'une lettre de M. Ch. Hermite à M. Borchardt), J. reine angew. Math.(1878) **84**, 70–79. Œuvres de Charles Hermite, tome 3, Gauthier-Villars, 1905/1917, 432–443.
`gallica.bnf.fr/ark:/12148/bpt6k902200`

[4] C. Levesque, *On m–th order linear recurrences*, Fibonacci Quart. **23** no. 4 (1985), 290–293.
`http://www.fq.math.ca/Scanned/23-4/levesque.pdf`

[5] C. Levesque, *A basis of the set of sequences satisfying a given m-th order linear recurrence*, Elem. Math. **42** no. 2 (1987) 32–35.

[6] C. Levesque & M. Waldschmidt, *Familles d'équations de Thue-Mahler n'ayant que des solutions triviales*, Acta Arith. **155** (2012), no. 2, p. 117–138.

[7] C. Levesque & M. Waldschmidt, *Familles d'équations de Thue associées à un sous-groupe de rang* 1 *d'unités totalement réelles d'un corps de nombres*, in SCHOLAR — a Scientific Celebration Highlighting Open Lines of Arithmetic Research (volume dedicated to Ram Murty), CRM collection "Contemporary Mathematics", AMS, **655** (2015) 117–134.
`http://www.ams.org/books/conm/655/`

[8] V. Nguyen & D. Roy, *A small value estimate in dimension two involving translations by rational points*, Int. J. Number Theory, 19 pages (to appear).
`http://arxiv.org/abs/1412.5163`

[9] A.J. van der Poorten, *Some facts that should be better known, especially about rational functions*, in Number Theory and Applications, ed. Richard Mollin, (NATO - Advanced Study Institute, Banff, 1988) (Kluwer Academic Publishers Dordrecht, 1989), 497–528.

[10] W. M. Schmidt, *Linear recurrence sequences*, in *Diophantine approximation (Cetraro, 2000)*, Lecture Notes in Math., vol. **1819**, Springer, Berlin, 2003, 171–247.

[11] T.N. Shorey & R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Tracts in Mathematics **87**, Cambridge University Press, 1986.

[12] C.L. Siegel, *Transcendental numbers*, Annals of Math. Studies no. 16, Princeton University Press, 1949.

Claude LEVESQUE
Département de mathématiques et de statistique
Université Laval
Québec (Québec)
CANADA G1V 0A6
Claude.Levesque@mat.ulaval.ca

Michel WALDSCHMIDT
Sorbonne Universités
UPMC Univ Paris 06
UMR 7586 IMJ-PRG
F – 75005 Paris, France
michel.waldschmidt@imj-prg.fr