Semigroup Forum
DOI 10.1007/s00233-013-9551-2

RESEARCH ARTICLE

On the variety of linear recurrences and numerical semigroups

Ivan Martino · Luca Martino

Received: 10 April 2013 / Accepted: 24 October 2013

Abstract In this work, we prove the existence of linear recurrences of order M with a non-trivial solution vanishing exactly on the set of gaps (or a subset) of a numerical semigroup S finitely generated by $a_1 < a_2 < \cdots < a_N$ and $M = a_N$.

Keywords Numerical semigroups · Linear recurrences · Generating function

1 Introduction and problem statement

In this work, we study certain issues posed by R. Fröberg and B. Shapiro in [5]. Inspired by the Skolem-Mahler-Lech Theorem [6], they have defined the variety $V_{(M;I)}$, the set of all M-order linear recurrence equations with a non-trivial solution vanishing at least at all the points of a given non-empty finite set $I \subset \mathbb{N}$. They have related the study of a particular open subvariety of $V_{(M;I)}$ to ideals generated by Schur functions [7]. They also stated certain open problems. For instance, one open issue is to understand for which pairs $(M; I)$ the variety $V_{(M;I)}$ is empty or not.

Here, we prove that the variety $V_{(M;I)}$ is non-empty when I is a subset of the gaps of a numerical semigroup S finitely generated by $a_1 < a_2 < \cdots < a_N$ and $M = a_N$. We provide the analytic form of these suitable recurrence equations, jointly with the proper initial conditions. The solutions become zero only at the gaps of S. In the sequel, we recall briefly some useful background material and introduce more specifically our goal.

Communicated by Fernando Torres.

I. Martino (✉)
Department of Mathematics, Stockholm University, Stockholm, Sweden
e-mail: martino@math.su.se

L. Martino
Department of Signal theory and Communications, Universidad Carlos III de Madrid, Leganes, Madrid, Spain
e-mail: luca@tsc.uc3m.es

Published online: 14 November 2013

1.1 Numerical semigroups

Numerical semigroups have been studied since the 19th century and they appear naturally in combinatorics and commutative algebra. In this work, we consider a numerical semigroup S embedded in $(\mathbb{N} \cup \{0\}, +)$. Given N integers $a_1, a_2, \dots, a_N \in \mathbb{N}$, a (finitely generated) numerical semigroup S [3] is defined as

$$S = \langle a_1, a_2, \dots, a_N \rangle = \left\{ \sum_{i=1}^{N} n_i a_i : n_i \in \mathbb{N} \cup \{0\} \right\}.$$

If a natural number does not belong to S it is called a *gap* of S. We denote as $\Delta(a_1, \dots, a_N) := \mathbb{N} \setminus S$, the set of the gaps of S. We have $|\Delta(a_1, \dots, a_N)| < \infty$ if and only if $\gcd(a_1, a_2, \dots, a_N) = 1$ (in literature, it is often required as necessary condition). However, one can always reduce to this case. We **do not** require that $a_1, a_2, \dots, a_N$ are a minimal set of generators for S and we always assume that $a_1 < a_2 < \cdots < a_N$ and $\gcd(a_1, \dots, a_N) = 1$.

The gaps of a numerical semigroup S are well studied [9] and strongly connected, for instance, with Frobenius number's problem and Hilbert function's problem [8]. The maximal element of $\Delta(a_1, \dots, a_N)$ (with respect to the canonical order of $\mathbb{N}$) is called the *Frobenius number*.

1.2 The variety of linear recurrences

We now present the open questions, stated in [5], that we deal with in the sequel. First of all, we associate to every M-tuple of complex numbers $\alpha = (\alpha_1, \dots, \alpha_M)$ the following linear recurrence equation $\mathcal{U}(\alpha)$:

$$\mathcal{U}(\alpha): \quad g_k + \alpha_1 g_{k-1} + \cdots + \alpha_i g_{k-i} + \cdots + \alpha_M g_{k-M} = 0. \tag{1}$$

If $\alpha_M \neq 0$, then $\mathcal{U}(\alpha)$ is of order M. The solutions of a linear homogeneous recurrence equation with constant coefficients are well-known [2] and they depend on the roots of the *characteristic polynomial* of $\mathcal{U}(\alpha)$,

$$p_\alpha(y): \quad y^M + \alpha_1 y^{M-1} + \cdots + \alpha_i y^i + \cdots + \alpha_M = 0.$$

Let $\{\rho_1, \dots, \rho_M\}$ be the set of the roots of $p_\alpha(y)$ (called *characteristic roots* or *poles*). If the roots ρ_i are real and distinct, i.e., $\rho_i \in \mathbb{R}$, $\rho_i \neq \rho_j$ with $i \neq j$ and $i, j \in \{1, \dots, M\}$, a generic solution of the recurrence equation has the following analytic form

$$g_k = c_1 \rho_1^k + c_2 \rho_2^k + \cdots + c_M \rho_M^k, \tag{2}$$

where the coefficients c_i depend on the initial conditions associated to the recurrence equation (1). With multiple roots and complex roots, other functional forms appear in the solutions like cosine and sine functions [2].

Definition 1.1 Let $M \in \mathbb{N}$ and let I be a non empty finite subset of $\mathbb{N}$. The *open linear recurrence variety* associated to the pair $(M; I)$, $V_{(M;I)}$, is the set of all linear recurrences of order exactly M having a non-trivial solution vanishing at least in all the points of I.

Using the bijection $\mathcal{U}(-)$, we can always think the set of all linear recurrences (of order at most M) as the affine space $\mathbb{A}^M_{\mathbb{C}}$. Being of order exactly M means that they belong to the affine principal open set $\mathbb{A}^M_{\mathbb{C}} \setminus \{\alpha_M \neq 0\}$.

In [5], Fröberg and Shapiro prove that $V_{(M;I)}$ is a algebraic variety and they ask the following questions:

Question (a) For which pairs $(M; I)$ the variety $V_{(M;I)}$ is empty/not empty? and (b), if $V_{(M;I)} \neq \emptyset$, is there a recurrence vanishing in a finite number of points?

In the rest of this work, we show that to each numerical semigroup $S = \langle a_1, a_2, \ldots, a_N\rangle$ it is possible to associate a recurrence $\mathcal{U}_S$ of order a_N vanishing *exactly* on its *finite number* of gaps $\Delta(a_1, \ldots, a_N)$, so that $V_{(a_N;\Delta(a_1,\ldots,a_N))} \neq \emptyset$.

2 The recurrence associated to a numerical semigroup

In this section, we first provide a novel characteristic function related to the semigroup S. Then, we construct the recurrence $\mathcal{U}_S$ associated to the semigroup $S = \langle a_1, a_2, \ldots, a_N\rangle$. Let $w_1, w_2, \ldots, w_N$ be strictly positive real numbers. Let us define the polynomial $F_1(z) = \sum_{i=1}^N w_i z^{a_i}$. We also set

$$G(z) = \frac{1}{1 - F_1(z)} = \frac{1}{1 - w_1 z^{a_1} - \cdots - w_N z^{a_N}}. \tag{3}$$

We denote by g_k the coefficient of z^k in the power series expansion of $G(z)$, i.e., $G(z) = \sum_{k=0}^{+\infty} g_k z^k$.

Lemma 2.1 *The sequence of coefficients,* $\{g_k\}_{k\in\mathbb{N}\cup\{0\}}$, *is the solution of the recurrence*

$$\mathcal{U}_S\colon \quad g_k = w_1 g_{k-a_1} + \cdots + w_N g_{k-a_N}, \qquad \forall k > 0, \tag{4}$$

with initial condition $g_0 = 1$ *and* $g_j = 0$, *for* $-a_N < j < 0$.

Proof We can rewrite Eq. (3) as $G(z)(1 - w_1 z^{a_1} - \cdots - w_N z^{a_N}) = 1$. Since $G(z) = \sum_{k=0}^{+\infty} g_k z^k$, replacing above, we obtain easily $\sum_{k=0}^{+\infty} g_k z^k - w_1 \sum_{k=0}^{+\infty} g_k z^{k+a_1} - \cdots - w_N \sum_{k=0}^{+\infty} g_k z^{k+a_N} = 1$, and also

$$\sum_{k=0}^{+\infty} g_k z^k - w_1 \sum_{i=a_1}^{+\infty} g_{i-a_1} z^i - \cdots - w_N \sum_{j=a_N}^{+\infty} g_{j-a_N} z^j = 1.$$

Now, setting $g_j = 0$, for $-a_N < j < 0$, we can also rewrite the left-side of the previous equation as $g_0 + \sum_{k=1}^{+\infty} (g_k - w_1 g_{k-a_1} - \cdots - w_N g_{k-a_N}) z^k = 1$. Finally, note that to hold the equality we need that $g_0 = 1$ and $g_k - w_1 g_{k-a_1} - \cdots - w_N g_{k-a_N} = 0$. $\square$

The recurrence in (4) is denoted by $\mathcal{U}_S$ and it is *associated* to the semigroup $S = \langle a_1, a_2, \ldots, a_N \rangle$. In the sequel, we link this result with the questions stated in the previous section. We recall that we do not require that $a_1, a_2, \ldots, a_N$ is a minimal set of generators of S.

Lemma 2.2 *The coefficient g_k is zero if and only if $k \notin S$.*

Proof Using that $\frac{1}{1-x} = \sum_{i \geq 0} x^i$, then $G(z) = \sum_{k=0}^{\infty} g_k z^k = \sum_{t=0}^{\infty} F_t(z)$ where we have set $F_t(z) = [F_1(z)]^t$ and $F_0(z) = 1$. The coefficients of $F_t(z) = (\sum_{i=1}^{N} w_i z^{a_i})^t$ are non-zero only on the z-powers having for exponent an element of the semigroup given by a sum of t generators of S (non necessarily different), that is $\sum_{q=1}^{t} a_{i_q}$ where $1 \leq i_q \leq N$. Indeed

$$F_t(z) = \left(\sum_{i=1}^{N} w_i z^{a_i} \right)^t = \sum \prod_{q=1}^{t} w_{i_q} z^{a_{i_q}} = \sum \left(\prod_{q=1}^{t} w_{i_q} \right) z^{(\sum_{q=1}^{t} a_{i_q})}. \tag{5}$$

For this reason, in the sum $\sum_{t=0}^{\infty} F_t(z)$ the exponents of the power z^i with non zero coefficients are exactly all the elements of S. Therefore, one gets the statement. $\square$

Theorem 2.1 *Let $S = \langle a_1, a_2, \ldots, a_N \rangle$ and let $I \subseteq \Delta(a_1, a_2, \ldots, a_N)$. Then $V_{(\beta;I)} \neq \emptyset$, for all $\beta \in S$, with $\beta \geq a_N$.*

Proof For every choice of strictly positive real numbers $\{w_i\}_{i=1}^{N}$, the recurrence equation $\mathcal{U}_S$, given in (4), belongs to $V_{(a_N;I)}$. Indeed, comparing Eqs. (1) and (4), we note easily that $\alpha_j = -w_k$ if $j = a_k$ and zero otherwise, with $w_N \neq 0$, so that $\alpha_{a_N} \neq 0$. Hence $\mathcal{U}_S$ is a recurrence equation of order a_N. Using Lemma 2.2, we know that a solution $\{g_k\}_{k \in \mathbb{N}}$ is zero if and only if $k \notin S$. This proves the result for $\beta = a_N$. For $\beta > a_N$, we observe that the semigroup S does not change if we add to the generators the element $\beta \in S$. Since we have never required that $\{a_1, \ldots, a_N\}$ is a minimal set of generators for S, we apply again the previous theorem with $a_1 < a_2 < \cdots < a_N < \beta$. $\square$

We have seen that for any finitely generated numerical semigroup S such that $\gcd(a_1, a_2, \ldots, a_N) = 1$, the Frobenius number, $g(S)$, exists and every integer k greater than $g(S)$ belongs to S. Then, we could narrow down the previous result:

Corollary 2.1 *Let $S = \langle a_1, a_2, \ldots, a_N \rangle$ and let $I \subseteq \Delta(a_1, a_2, \ldots, a_N)$. Then there exists a constant value $K \in \mathbb{N}$ such that for all $\beta > K$, we have $V_{(\beta;I)} \neq \emptyset$.*

We can also easily provide certain informations about the dimension of the variety $V_{(a_N,I)}$. We remark that in algebraic geometry one often uses the so-called *Krull dimension* instead of the topological dimension. A suitable definition is given in [1], for instance. However, in this article, the reader can suppose that the Krull dimension is the topological one, because we work on the complex field.

Corollary 2.2 *Let* $S = \langle a_1, a_2, \dots, a_N \rangle$ *and let* $I \subseteq \Delta(a_1, a_2, \dots, a_N)$. *Then the Krull dimension of* $V_{(a_N;I)}$, *is at least* N, *i.e.*, $\dim_{\mathbb{C}}(V_{(a_N;I)}) \geq N$.

Proof We remark that $V_{(a_N;I)}$ is an open *complex* algebraic variety (since defined by polynomial equation and by $\alpha_{a_N} \neq 0$, see [5]). Let W be the subset of $V_{(a_N;I)}$ defined by the recurrences (4) for every choice of strictly positive real number $\{w_1, \dots, w_N\}$. In Theorem 2.1, we have proved that $V_{(a_N;I)} \neq \emptyset$ by showing that $W \neq \emptyset$.

We observe that W is isomorphic to $\mathbb{R}^N_{>0}$. Each complex algebraic variety that contains the non-algebraic subset $\mathbb{R}^N_{>0}$ has a complex sub-variety C containing W and of Krull dimension at least N, $W \subset C \subseteq V_{(a_N;I)}$. Thus $\dim_{\mathbb{C}}(V_{(a_N;I)}) \geq N$. □

2.1 Probabilistic interpretation

If the coefficients $w_i \geq 0$, are chosen such that $\sum_{i=1}^N w_i = 1$, they define a probability mass, and the functions $F_t(z) = [F_1(z)]^t$ with $F_1(z) = \sum_{i=1}^N w_i z^{a_i}$, defined in the proof of Lemma 2.2, and $G(z)$ have a probabilistic interpretation. Let X_t be a discrete random variable taking values in $\mathbb{N}$, and $t \in \mathbb{N}$. We can define, for instance, a random walk associated to the semigroup $S = \langle a_1, a_2, \dots, a_N \rangle$ as $X_t = X_{t-1} + a_i$, with probability w_i, $i = 1, \dots, N$, starting with $X_0 = 0$. The function $F_t(z)$ represents the *probability generating function* (PGF) [4] associated to the probability of visiting the state k exactly at the time instant t, $f_{t,k} = \text{Prob}\{X_t = k\}$, i.e., $F_t(z) = \sum_{k=0}^{t \cdot a_N} f_{t,k} z^k$. Let us also consider now the probability of visiting the state k, i.e.,

$$g_k = \text{Prob}\{X_t = k \text{ for some } t \in \mathbb{N}\}, \quad k \in \mathbb{N}.$$

Basic statistical considerations [4] lead us to write the PGF $G(z)$ corresponding to these probability as $G(z) = \sum_{t=1}^{\infty} F_t(z)$ and so we obtain $G(z) = \frac{1}{1 - w_1 z^{a_1} - \cdots - w_N z^{a_N}}$. The probabilities $\{g_k\}_{k \in \mathbb{N}}$ of visiting a state k, satisfy the linear recurrence equation $\mathcal{U}_S$. They are zero if and only if these states k coincides exactly with the gaps of the numerical semigroup S, i.e., $k \in \Delta(a_1, a_2, \dots, a_N)$.

Acknowledgements We would like to thank Ralf Fröberg (Stockholm University, Department of Mathematics) and Boris Shapiro (Stockholm University, Department of Mathematics) for their help and several suggestions. Furthermore, we thank the reviewers for their useful comments which have helped us to improve this manuscript. Moreover, this work has been partially supported by Government of Spain (project COMONSENS, id. CSD2008-00010, project DEIPRO, and project COMPREHENSION, id. TEC2012-38883-C02-01).

References

1. Atiyah, M.F., Macdonald, I.G.: Introduction to Commutative Algebra. Addison-Wesley, Reading (1969)
2. Batchelder, P.M.: An Introduction to Linear Difference Equations. Dover, New York (1967)
3. Brauer, A., Shockley, J.E.: On a problem of Frobenius. J. Reine Angew. Math. **211**, 215–220 (1962)
4. DeGroot, M.H., Schervish, M.J.: Probability and Statistics, 3rd edn. Addison-Wesley, New York (2002)
5. Fröberg, R., Shapiro, B.: Linear recurrences and Vandermonde varieties. I. http://people.su.se/~shapiro/Articles/SML.pdf

6. Lech, C.: A note on recurring series. Ark. Mat. **2**, 417–421 (1953)
7. Macdonald, I.G.: Symmetric Functions and Hall Polynomials, 2nd edn. Oxford Mathematical Monographs. (1998)
8. Ramírez Alfonsín, J.L.: The Diophantine Frobenius Problem. Oxford Lecture Series in Mathematics and Its Applications, vol. 30. Oxford University Press, Oxford (2005)
9. Rosales, J.C., Branco, M.B.: The Frobenius problem for numerical semigroups. J. Number Theory **131**(12), 2310–2319 (2011)