Comment. Math. Helv. 89 (2014), 597–616
DOI 10.4171/CMH/328

Commentarii Mathematici Helvetici

From Schanuel's Conjecture to Shapiro's Conjecture

Paola D'Aquino, Angus Macintyre and Giuseppina Terzo

Abstract. In this paper we prove Shapiro's 1958 Conjecture on exponential polynomials, assuming Schanuel's Conjecture.

Mathematics Subject Classification (2010). 11U09, 03C60, 30C15.

Keywords. Exponential fields, Zilber's fields, Schanuel's Conjecture, Shapiro's Conjecture, anomalous varieties.

1. Introduction

We work with exponential polynomial functions over $\mathbb{C}$ of the form

$$f(z) = \lambda_1 e^{\mu_1 z} + \cdots + \lambda_N e^{\mu_N z}. \tag{1}$$

The set of such functions forms a ring $\mathcal{E}$ under the usual addition and multiplication. We normally refer to exponential polynomial functions simply as exponential polynomials. In (1), we assume without loss of generality that the exponents μ's are distinct, and that the coefficients λ's are nonzero, unless f is the zero polynomial.

In 1974 during the Janos Bolyai Society Colloquium on Number Theory, H. L. Montgomery mentioned the following conjecture, which he attributed to H. S. Shapiro [15]:

Shapiro's Conjecture. If f and g are two exponential polynomials in $\mathcal{E}$ with infinitely many common roots, then there exists an exponential polynomial h in $\mathcal{E}$ such that h is a common divisor of f and g in the ring $\mathcal{E}$, and h has infinitely many zeros in $\mathbb{C}$.

Montgomery pointed out, via an example given in [5], that the problem was not likely to yield easily to any classical approximation argument.

It turns out that Shapiro's Conjecture is naturally connected to Schanuel's Conjecture in Transcendence Theory.

Schanuel's Conjecture. Let $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$. Then the transcendence degree of $\mathbb{Q}(\lambda_1, \ldots, \lambda_n, e^{\lambda_1}, \ldots, e^{\lambda_n})$ over $\mathbb{Q}$ is greater or equal than the linear dimension of $\lambda_1, \ldots, \lambda_n$ over $\mathbb{Q}$.

Schanuel's Conjecture has played a crucial role in exponential algebra (see [10], [17]), and in the model theory of exponential fields (see [11], [18], [12]).

In [13] Ritt obtained a factorization theory for exponential polynomials in $\mathcal{E}$. Subsequently, his ideas have been developed, and his results have been extended to more general exponential polynomials over $\mathbb{C}$, see [7], [9], [3], [4]. In [2], these ideas have been put in the much broader context of general exponential polynomials (with any iteration of exponentiation) over an algebraically closed field of characteristic 0 with an exponentiation.

In this paper we will study the Shapiro Conjecture in a context more general than that of the complex field. We will be working over an algebraically closed field of characteristic 0, with an exponential function, and having an infinite cyclic group of periods, whose exponential is surjective onto the multiplicative group. The class of such fields includes the very important fields introduced by Zilber (see [18] for the basic notions). The preceding assumptions play a minor role in our work on Shapiro's Conjecture. Of crucial importance is our further assumption, true for Zilber's fields, but unproved for the complex field, that we work with exponential fields satisfying Schanuel's Conjecture.

One should note that in an exponential field satisfying the above assumptions (even without the surjectivity of the exponential onto the multiplicative group) the two element set of generators of the periods is first-order definable [8], the sine and cosine function are unambiguously defined, and the two element set consisting of the quotients of the period generators by twice a square root of -1 is definable (the set does not depend on which root is chosen). In $\mathbb{C}$ this would define the set $\{\pi, -\pi\}$. Finally, we can define the one element subset consisting of the element x such that $\sin(x/2) = 1$. In a general field satisfying our assumptions, we call this element π.

In Section 2 we review the basic ideas of Ritt's factorization theory for exponential polynomials. His main theorem allows us to break the proof of Shapiro's Conjecture into two cases. One case was already done by van der Poorten and Tijdeman [5] for simple polynomials (in Ritt's sense) over $\mathbb{C}$, without any use of Schanuel's Conjecture. In Section 3, we modify that argument so as to apply to fields satisfying all the assumptions given above with the exception of Schanuel's Conjecture.

Section 4 explains recent work of Bombieri, Masser and Zannier [1] on anomalous subvarieties of powers of the multiplicative group.

The main result of this paper is in Section 5 where a positive solution to Shapiro's Conjecture is obtained for the remaining case of irreducible exponential polynomials, assuming Schanuel's Conjecture, using the work of Bombieri, Masser and Zannier, and work of Evertse, Schlickewei and Schmidt on linear functions of elements of multiplicative groups of finite rank.

A. Shkop has proved the Conjecture, assuming Schanuel's Conjecture, for the very special case of exponential polynomials over the algebraic numbers, see [16].

We feel obliged to make a philosophical remark about the use of Schanuel's Conjecture to "settle" a conjecture which emerged from complex analysis. A very distinguished number theorist has remarked that if one assumes Schanuel's Conjecture one can prove anything. The sense of this is clear if one restricts "anything" to refer to statements in transcendence theory. In that domain the Conjecture is almost a machine, leading one mechanically to "proofs" of any plausible conjectures about algebraic relations between complex numbers and their exponentials. We suspect that there is also a common intuition that statements about common zeros of exponential polynomials should be related to statements about the transcendence theory of the exponential function. However, the original motivation for Shapiro's Conjecture clearly comes from reflection on distribution of zeros of individual exponential polynomials, and predates Schanuel's Conjecture. Moreover, our argument involves combinatorial considerations not previously connected to routine applications of Schanuel's Conjecture.

2. Factorization theory

We briefly review the main ideas in Ritt's factorization for exponential polynomials in $\mathcal{E}$. Most of the theory adapts to the much more general context of the ring of exponential polynomials over an algebraically closed field of characteristic 0 with an exponential function (see [2]).

The fundamental idea due to Ritt was to transform problems of factorization of exponential polynomials to those of factorization of classical multivariate polynomials in the extended category of polynomials in fractional powers of the variables. This brings in the notion of power irreducible multivariate polynomial explained below.

In general, if we consider an irreducible polynomial $Q(x_1, \ldots, x_n)$ it can happen that for some positive integers $q_1, \ldots, q_n$ the polynomial $Q(x_1^{q_1}, \ldots, x_n^{q_n})$ is reducible.

If there is no sequence $q_1, \ldots, q_n$ of positive integers such that $Q(x_1^{q_1}, \ldots, x_n^{q_n})$ is reducible we will refer to Q as a *power irreducible polynomial*.

We briefly review how to associate a classical polynomial in one or more variables to an exponential polynomial in $\mathcal{E}$.

We collect some basic definitions and results.

Fact. The units in the ring $\mathcal{E}$ are the products of nonzero constants and $e^{\alpha z}$ for constant $\alpha \in \mathbb{C}$.

Definition 2.1. An element f in $\mathcal{E}$ is irreducible, if there are no non-units g and h in $\mathcal{E}$ such that $f = gh$.

Definition 2.2. Let $f = \sum_{i=1}^{N} \alpha_i e^{\mu_i z}$ be an exponential polynomial. The *support* of f, denoted by $\mathrm{supp}(f)$, is the $\mathbb{Q}$-space generated by $\mu_1, \ldots, \mu_N$.

Definition 2.3. An exponential polynomial $f(z)$ of $\mathcal{E}$ is simple if $\dim \mathrm{supp}(f) = 1$.

It is easily seen that, up to a unit, a simple exponential polynomial is a polynomial in $e^{\mu z}$, for some $\mu \in \mathbb{C}$. An example of a simple exponential polynomial is

$$g(z) = \frac{e^{2\pi i z} - e^{-2\pi i z}}{2i} = \sin(2\pi z).$$

Remark 2.4. A simple exponential polynomial factorizes, up to units, into a finite product of factors of the form $1 - \alpha e^{\mu z}$, where $\alpha, \mu \in \mathbb{C}$. This simply uses the fact that the complex field is algebraically closed. If fractional powers of the variables are allowed then a simple exponential polynomial may have infinitely many factors, e.g. $1 - \alpha e^{\frac{\mu z}{k}}$, for each $k \in \mathbb{N}, k \neq 0$.

Let $f(z) = \lambda_1 e^{\mu_1 z} + \cdots + \lambda_N e^{\mu_N z}$ where λ_i and μ_i are complex numbers, and let $\beta_1, \ldots, \beta_r$ be a $\mathbb{Z}$-basis of the additive group generated by the μ_i's. Let $Y_j = e^{\beta_j z}$, with $j = 1, \ldots, r$. If each μ_i is expressed in terms of the β_j's we have that f is transformed into a classical Laurent polynomial Q over $\mathbb{C}$ in the variables $Y_1, \ldots, Y_r$. The best way to think of Q is as a function on the product of r copies of the multiplicative group variety. Remember that the Y's are exponentials and so take value in the multiplicative group. More prosaically, one can write Q as a product of a polynomial in the Y's and a quotient of monomials in the Y's.

Clearly, any factorization of f determines a factorization of $Q(Y_1, \ldots, Y_r)$. Ritt saw the relevance, in terms of factorization theory, of understanding the ways in which an irreducible polynomial $Q(Y_1, \ldots, Y_r)$ can become reducible once the variables are replaced by their powers. It is a fundamental problem to determine the set of integer r-tuples $q_1, \ldots, q_r$ for which the reducibility occurs. Ritt gave a uniform bound for the number of irreducible factors of $Q(Y_1^{q_1}, \ldots, Y_r^{q_r})$, depending only on the degree of Q.

For the factorization theorem of Ritt the following lemma is crucial.

Lemma 2.5. *Let* $f(z) = \sum_{i=1}^{N} \alpha_i e^{\mu_i z}$ *and* $g(z) = \sum_{j=1}^{M} l_j e^{m_j z}$ *be non-zero exponential polynomials. If* f *is divisible by* g *then* supp(ag) *is contained in* supp(bf), *for some units* a *and* b, *i.e., every element of* supp(ag) *is a linear combination of elements of* supp(bf) *with rational coefficients.*

Note that if f is a simple polynomial and g divides f then g is also simple. The factorization theorem that we need is the following (see [13], [7] and [9]).

Theorem 2.6. *Let* $f(z) = \lambda_1 e^{\mu_1 z} + \cdots + \lambda_N e^{\mu_N z}$, *where* $\lambda_i, \mu_i \in \mathbb{C}$. *Then* f *can be written uniquely up to order and multiplication by units as*

$$f(z) = S_1 \ldots S_k \cdot I_1 \ldots I_m$$

where S_j *are simple polynomials with* supp$(S_{j_1}) \neq$ supp(S_{j_2}) *for* $j_1 \neq j_2$, *and* I_h *are irreducible polynomials in* $\mathcal{E}$.

We observe that the proof has nothing to do with analytic functions, and works over any characteristic 0 exponential field which is an algebraically closed field (see [4], [2]). This is the context where we will be working.

Since a common zero of two products is a common zero of two factors, Theorem 2.6 trivially implies that only two cases of the Shapiro Conjecture have to be considered.

Case 1. At least one of the exponential polynomials f and g is simple.

Case 2. Both of the exponential polynomials f and g are irreducible.

3. Shapiro Conjecture: Case 1

The case when either f or g is simple has been proved unconditionally by van der Poorten and Tijdeman for the complex field, see [5].

Their proof uses various results from Ritt divisibility theory in [14] and a variant of the usual p-adic argument from the proof of the Skolem–Mahler–Lech Theorem on recurrence sequences with infinitely many vanishing terms. Ritt's result most specific to the complex field says that if f/g is an entire function, where f and g are exponential polynomials, then f divides g. The proof ultimately relies on a fundamental result of Tamarkin, Polya and Schwengler on the distribution of zeros for exponential polynomials as in (1). We observe that it is not obvious what interpretation to give this result in more general exponential fields, and for that reason we have sought and found a proof that avoids this result of Ritt. We do not, however, avoid appeal to the Skolem–Mahler–Lech Theorem. The latter theorem, as used in [5] on page 62, in a formulation for exponential functions, is as follows:

Theorem 3.1 (Skolem, Mahler, Lech). *If $f(z)$ is a function as in (1) which vanishes for infinitely many integers z then there exists an integer Δ and positive residues $d_1, \ldots, d_l$ modulo Δ, such that $f(z)$ vanishes for all integers $z \equiv d_i \pmod{\Delta}$, $i = 1, \ldots, l$, and $f(z)$ vanishes only finitely often on other integers.*

Inspection of the proof (by a suitable p-adic embedding) shows that it works for all exponential fields of characteristic 0.

We extend the van der Poorten–Tijdeman result to the more general setting of an exponential algebraically closed field K of characteristic 0, with standard periods and exponential map surjective to the multiplicative group, making no use of analytic methods. We need the following lemma.

Lemma 3.2. *Let $h(z) = \lambda_1 e^{\mu_1 z} + \cdots + \lambda_N e^{\mu_N z}$, where $\lambda_j, \mu_j \in K$. If h vanishes at all integers then $\sin(\pi z)$ divides h.*

Proof. We proceed by induction on the length N of h. If $N = 2$ the proof is a trivial direct computation.

Let $N > 2$, and consider the first N positive solutions $1, \dots, N$. The following identities hold:

$$\begin{aligned} \lambda_1 e^{\mu_1} + \lambda_2 e^{\mu_2} + \cdots + \lambda_N e^{\mu_N} &= 0, \\ \lambda_1 (e^{\mu_1})^2 + \lambda_2 (e^{\mu_2})^2 + \cdots + \lambda_N (e^{\mu_N})^2 &= 0, \\ &\vdots \\ \lambda_1 (e^{\mu_1})^N + \lambda_2 (e^{\mu_2})^N + \cdots + \lambda_N (e^{\mu_N})^N &= 0. \end{aligned}$$

Let $\delta_1 = e^{\mu_1}, \cdots, \delta_N = e^{\mu_N}$, so by substitution we can rewrite the identities in matrix notation as follows:

$$\begin{pmatrix} \delta_1 & \delta_2 & \dots & \delta_N \\ \delta_1^2 & \delta_2^2 & \dots & \delta_N^2 \\ \vdots & \vdots & \ddots & \vdots \\ \delta_1^N & \delta_2^N & \dots & \delta_N^N \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_N \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Because of the existence of a non trivial solution of the system the determinant of the matrix vanishes,

$$\begin{vmatrix} \delta_1 & \delta_2 & \dots & \delta_N \\ \delta_1^2 & \delta_2^2 & \dots & \delta_N^2 \\ \vdots & \vdots & \ddots & \vdots \\ \delta_1^N & \delta_2^N & \dots & \delta_N^N \end{vmatrix} = 0,$$

that is,

$$\delta_1 \delta_2 \dots \delta_N \cdot \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \delta_1 & \delta_2 & \dots & \delta_N \\ \vdots & \vdots & \ddots & \vdots \\ \delta_1^{N-1} & \delta_2^{N-1} & \dots & \delta_N^{N-1} \end{vmatrix} = 0.$$

This is a Vandermonde determinant, so

$$(\delta_1 \delta_2 \dots \delta_N) \cdot \prod_{1 \le i < \ell \le N} (\delta_i - \delta_\ell) = 0.$$

So, $\delta_i = \delta_\ell$ for some $i \neq \ell$, i.e., $e^{\mu_i} = e^{\mu_\ell}$ for some $i \neq \ell$, and without loss of generality we can assume $e^{\mu_1} = e^{\mu_2}$. So, $e^{\mu_1 n} = e^{\mu_2 n}$ for each $n \in \mathbb{Z}$. The polynomial

$$(\lambda_1 + \lambda_2) e^{\mu_1 z} + \sum_{j \ge 3} \lambda_j e^{\mu_j z}$$

also vanishes on all integers, and since it has length strictly less than N it is divisible by $\sin(\pi z)$. Note that

$$h(z) = (\lambda_1 + \lambda_2)e^{\mu_1 z} + \sum_{j\geq 3} \lambda_j e^{\mu_j z} + \lambda_2(e^{\mu_1 z} - e^{\mu_2 z}),$$

and therefore all integers are roots of $e^{\mu_2 z} - e^{\mu_1 z}$. It follows that $\sin(\pi z)$ divides $e^{\pi ijz} - e^{-\pi ijz}$, a trivial exercise as noted for case $N = 2$. □

The Shapiro Conjecture for the case when one of the polynomials is simple follows from the following theorem which implies that if one of the two polynomials is simple so is the other one.

Theorem 3.3. *Let f be a simple exponential polynomial, and let g be an arbitrary exponential polynomial such that f and g have infinitely many common roots. Then there exists an exponential polynomial which divides both f and g.*

Proof. If f is simple then up to a constant, f is of the form, $f = \prod(1 - ae^{\alpha z})$, where $a, \alpha \in K$. If f and g have infinitely common zeros then g has infinitely common zeros with one factor of f, say $1 - ae^{\alpha z}$. So g has infinitely many zeros of the form $z = (2k\pi i - \log a)/\alpha$ with $k \in \mathbb{Z}$, and for a fixed value of $\log a$. If $g^*(z) = g((2\pi iz - \log a)/\alpha)$ then g^* has infinitely many zeros in $\mathbb{Z}$. By Theorem 3.1, $g^*(z)$ vanishes on the set $M = \{d_0 + j\Delta : j \in \mathbb{Z}\}$, for some Δ and d_0 in $\mathbb{Z}$, and $0 \leq d_0 < \Delta$. If $h(z) = g^*(d_0 + z\Delta)$ then h vanishes on $\mathbb{Z}$, and Lemma 3.2 implies that h is divisible by $\sin(\pi z)$. This is a contradiction if h is irreducible, which is the case when g is irreducible. This forces g to be simple (up to a unit), e.g. $g(z) = 1 - be^{\beta z}$ for some $b, \beta \in K$. So, without loss of generality we can consider the system

$$\begin{aligned} f(z) &= 1 - ae^{\alpha z} = 0, \\ g(z) &= 1 - be^{\beta z} = 0, \end{aligned} \tag{2}$$

where $a, b, \alpha, \beta \in K$, with infinitely many common zeros. The roots of f are of the form $z = \frac{1}{\alpha}(-\log a + 2k\pi i)$, $k \in \mathbb{Z}$. It follows that, for infinitely many t in $\mathbb{Z}$, g vanishes on $z = \frac{1}{\alpha}(-\log a + 2t\pi i)$. We argue now as before, using Theorem 3.1, to conclude that f and g vanish on

$$\frac{1}{\alpha}(-\log a + 2(d + \Delta j)\pi i),$$

where d and Δ are integers, $d < \Delta$, and for all $j \in \mathbb{Z}$. Via the change of variable $T(z) = \frac{1}{\alpha}(-\log a + 2(d + \Delta z)\pi i)$ the exponential polynomials $f(T(z))$ and $g(T(z))$ both vanish on $\mathbb{Z}$, and by Lemma 3.2 they are both divisible by $\sin(\pi z)$. Thus $f(w)$ and $g(w)$ are both divisible by $\sin(\pi T^{-1}(w)) = \sin(\frac{1}{2\Delta i}(\alpha w + \log a - 2d\pi i))$ which is a simple polynomial. □

4. Group varieties associated to exponential polynomials

We now adapt, to the system $f = g = 0$ the procedure of Ritt, thereby converting the system to one defined by two conventional polynomials, defining a subvariety of a power of the multiplicative group.

We work over an algebraically closed characteristic 0 exponential field K with standard periods, with the exponential surjective onto the multiplicative group, and satisfying Schanuel's Conjecture (SC).

Consider a system with no restriction on f and g:

$$\begin{aligned} f(z) &= \lambda_1 e^{\mu_1 z} + \cdots + \lambda_N e^{\mu_N z} = 0, \\ g(z) &= l_1 e^{m_1 z} + \cdots + l_M e^{m_M z} = 0, \end{aligned} \tag{3}$$

where $\lambda_i, \mu_i, l_j, m_j \in K$.

Let D be the linear dimension of $\mathrm{supp}(f) \cup \mathrm{supp}(g)$, and $b_1, \ldots, b_D$ a $\mathbb{Z}$-basis of the group generated by $\bar{\mu}, \bar{m}$. We introduce new variables

$$Y_1 = e^{b_1 z}, \ \ldots, \ Y_D = e^{b_D z},$$

and as in Section 2 we associate the Laurent polynomials

$$F(Y_1, \ldots, Y_D), G(Y_1, \ldots, Y_D) \in \mathbb{Q}(\bar{\lambda}, \bar{l})[Y_1, \ldots, Y_D]$$

to $f(z)$ and $g(z)$, respectively. As far as zeros from the multiplicative group are concerned, one may replace F and G by ordinary polynomials got by multiplying them by monomials. Note that F and G are polynomials over $\mathbb{Q}(\bar{\lambda}, \bar{l})$. Let L be the algebraic closure of this field. Obviously L has finite transcendence degree, a fact which will be crucial later.

Clearly, if s is a common zero of f and g then $(e^{b_1 s}, \ldots, e^{b_D s})$ is a common zero of F and G in the Dth power of the multiplicative group. The study of the set of solutions of system (3) will be reduced to studying the solutions of the system

$$\begin{aligned} F(Y_1, \ldots, Y_D) &= 0, \\ G(Y_1, \ldots, Y_D) &= 0. \end{aligned} \tag{4}$$

Remark 4.1. Let $V(F)$ and $V(G)$ be the subvarieties in the Dth power of the multiplicative group G_m^D, associated to F and G, respectively. If f and g are irreducible then F and G are power irreducible. In this case $\dim V(F) = \dim V(G) = D - 1$. If we assume that f and g are distinct irreducibles (i.e. neither is a unit times the other) then F and G are power irreducibles, with neither a scalar multiple of the other. It follows that the algebraic set defined by $F = G = 0$ has dimension no more than $D - 2$. This is crucial in what follows.

Recall that an algebraic subgroup in the group variety G_m^D is given by a finite set of conditions each of the form

$$Y_1^{a_1} \dots Y_D^{a_D} = 1$$

where $a_1, \dots, a_D \in \mathbb{Z}$. We will refer to $(a_1, \dots, a_D) \in \mathbb{Z}^D$ as the exponent vector. For such a variety, the dimension is $D - h$ where h is the rank of the subgroup of $\mathbb{Z}^D$ generated by the exponent vectors. A translate or coset of a subgroup is obtained by replacing 1 by other constants in the finite set of conditions. A torus is a connected algebraic subgroup.

The algebraic set C defined by (4) may be a reducible subvariety of the algebraic group G_m^D over L. As remarked above, its dimension is at most $D - 2$ if F and G are distinct irreducible over L.

Later, in the proof of the Shapiro Conjecture, we will work on a suitable irreducible component of C.

Note that if f and g have infinitely many common zeros, and f is irreducible, the algebraic set C above cannot be contained in any coset of any proper algebraic subgroup of G_m^D. For otherwise, let

$$Y_1^{a_1} \dots Y_D^{a_D} = \theta \tag{5}$$

be one of the equations defining the coset. This corresponds to a simple polynomial in Ritt's sense which has infinitely common zeros with f. By van der Poorten and Tijdeman result and Lemma 2.5 we have a contradiction since f is not simple.

We now review the basic concepts concerning the notion of anomalous subvariety, as used in [1] by Bombieri, Masser and Zannier. We will not give the full details of the analysis obtained by Bombieri, Masser and Zannier but we will describe those properties of anomalous varieties which we will need in the proof of our main result. Their discussion is first done over the complexes, but they observe that it works over any algebraically closed field of characteristic 0, and we use this fact. For us the case of the L introduced earlier is crucial because of its finite transcendence degree. We will follow [1] for the notion of a subvariety of the algebraic group G_m^n, and when necessary we will specify if the variety is irreducible.

Let V be an irreducible subvariety of G_m^n.

Definition 4.2. An irreducible subvariety W of V is anomalous in V if W is contained in a coset of an algebraic subgroup Γ of G_m^n with

$$\dim W > \max\{0, \dim V - \operatorname{codim}\Gamma\}$$

Note that this definition has the same meaning in any algebraically closed field over which V is defined.

Definition 4.3. An anomalous subvariety of V is maximal if it is not contained in a strictly larger anomalous subvariety of V.

Theorem 4.4. *Let V be an irreducible variety in G_m^n of positive dimension defined over $\mathbb{C}$. Then there exists a finite collection Φ_V of proper tori H such that $1 \leq n - \dim H \leq \dim V$ and every maximal anomalous subvariety W of V is a component of the intersection of V with a coset $H\theta$ for some $H \in \Phi_V$ and $\theta \in G_m^n$.*

For the proof see [1]. Note that this result is true (as is stated in [1]) when $\mathbb{C}$ is replaced by any algebraically closed field K of characteristic 0, in the sense that the cosets involved, for W defined over K, are also defined over K.

Theorem 4.4 implies, since every anomalous subvariety is contained in a maximal one, that there is a finite number of subgroups of codimension 1, such that any anomalous subvariety is included in a coset of one of them.

5. The full Shapiro Conjecture

We concentrate now on Case 2 of Shapiro's Conjecture. In this case the conjecture has the following formulation: *If f and g are distinct irreducible exponential polynomials then f and g have at most finitely many common zeros.*

We will prove the following equivalent version (see [5]): *Let f and g be exponential polynomials, and assume f is irreducible. If f and g have infinitely many common zeros then f divides g.*

In the following unless otherwise specified the linear dimension and the transcendence degree of a tuple will always be over $\mathbb{Q}$.

Let $D = \text{l.d.}(\text{supp}(f) \cup \text{supp}(g))$, and let $b_1, \dots, b_D$ a $\mathbb{Z}$-basis of the group generated by $\bar{\mu}, \bar{m}$. We will denote the transcendence degree of $\bar{\lambda}, \bar{l}$ by δ_1, and the transcendence degree of $\bar{\mu}, \bar{m}$ by δ_2, i.e. $\delta_1 = \text{t.d.}(\bar{\lambda}, \bar{l})$, and $\delta_2 = \text{t.d.}(\bar{\mu}, \bar{m})$. We denote by $\bar{b}$ the sequence $(b_1, \dots, b_D)$ and by B the set $\{b_1, \dots, b_D\}$.

Assume that f and g have infinitely many common zeros. Let S be an infinite set of nonzero common solutions. We will "thin" this set inductively to infinite subsets using arguments of Schanuel type, and work of Bombieri, Masser and Zannier on anomalous intersections, to reach an infinite S such that the $\mathbb{Q}$-space generated by S is finite dimensional. We will then get a contradiction from using, inter alia, work of Evertse, Schlickewei and Schmidt on linear functions of elements of finite rank groups.

We begin with some simple bounds on Schanuel data. For any $s \in S$ let $\bar{b}s$ stand for the sequence $(b_1 s, \dots, b_D s)$ and $e^{\bar{b}s}$ stand for the sequence $(e^{b_1 s}, \dots, e^{b_D s})$. In terms of the set, for any $s \in S$ we denote by $Bs = \{b_1 s, \dots, b_D s\}$, and by

$e^{Bs} = \{e^{b_1 s}, \dots, e^{b_D s}\}$. For any subset T of the set of solutions S,

$$BT = \bigcup_{s \in T} Bs,$$

and

$$e^{BT} = \{e^{b_i s} : 1 \le i \le D, b_i \in B, s \in T\}.$$

For any finite subset T of S, let $D(T)$ be the linear dimension of the space spanned by BT. Notice that $D(T) = D$ if T is a singleton, since $0 \notin S$. Moreover, $D(T) \le D|T|$, where $|T|$ denotes the cardinality of T. We show now that there is an upper bound to the cardinality of T for which the equation $D(T) = D|T|$ holds.

Lemma 5.1 (SC). *For any finite subset T of S with $D(T) = D|T|$ we have that $|T| \le \delta_1 + \delta_2$.*

Proof. Enumerate the set T as $s_1, \dots, s_k$, of elements of S. By previous observations, upper bounds on the respective transcendence degrees of the sets e^{BT} and BT are

$$\text{t.d.}(e^{BT}) \le k(D-2) + \delta_1,$$

(because of the dimension estimate on $F = G = 0$ given in Remark 4.1) and

$$\text{t.d.}(BT) \le \delta_2 + k.$$

By Schanuel's Conjecture we have

$$\text{t.d.}(BT, e^{BT}) \ge D(T),$$

and this implies

$$D(T) \le kD - k + \delta_1 + \delta_2. \tag{6}$$

If $D(T) = kD$, inequality (6) implies that

$$\delta_1 + \delta_2 \ge k, \tag{7}$$

for all $k \in \mathbb{N}$, proving the result since δ_1 and δ_2 are fixed and depend only on the coefficients of the polynomials f and g. □

Remark 5.2. Let k_0 be the maximum cardinality of a T for which the equation $D(T) = D|T|$ holds. Let S_0 be such a T. If we extend S_0 to a set S_1, by adding k_1 distinct elements, then we clearly have the following estimates:

$$D(S_0) \le D(S_1) \le \delta_1 + \delta_2 + k_1(D-1).$$

Lemma 5.1 has a fundamental consequence on the transcendence degree of the set BS which will be crucial in the following.

Lemma 5.3 (SC). *The transcendence degree of BS over $\mathbb{Q}$ is less or equal than $\delta_1 + 2\delta_2$.*

Proof. Fix any $s \in S - S_0$. Then by maximality of S_0 for the equation $D(T) = D|T|$, we have a nontrivial linear function Λ over $\mathbb{Q}$, such that $\Lambda(\bar{b}s)$ belongs to the $\mathbb{Q}$-vector space generated by the BS_0. We note that $\bar{b}$ is linearly independent over $\mathbb{Q}$ and Λ is linear, so we get that

$$s = \Lambda(\bar{b})^{-1} \cdot a$$

where a is in the $\mathbb{Q}$-vector space generated by the BS_0. Let F be the field generated by $BS_0 \cup B$.

The transcendence degree of F is clearly finite, and the following inequalities hold

$$\text{t.d.}_{\mathbb{Q}}(F) \le \text{t.d.}(B) + \text{t.d.}_{\mathbb{Q}(B)}(BS_0) \le \delta_2 + k_0 \le \delta_1 + \delta_2 + \delta_2 = \delta_1 + 2\delta_2. \quad \square$$

The following result will be crucial for completing the proof of Shapiro's Conjecture.

Main Lemma (SC). *For some infinite subset S' of S the $\mathbb{Q}$-vector space generated by S' is finite dimensional.*

Proof. Consider the subvariety C of G_m^D defined by

$$\begin{aligned} F(Y_1, \ldots, Y_D) = 0, \\ G(Y_1, \ldots, Y_D) = 0 \end{aligned} \tag{8}$$

over $L = \mathbb{Q}(\bar{\lambda}, \bar{l})^{\text{alg}}$. This may be a reducible subvariety of the algebraic group G_m^D, so we work now with a fixed irreducible component V of C containing solutions of the form $(e^{b_1 s}, \ldots, e^{b_D s})$, for infinitely many $s \in S$.

An upper bound on the dimension of V over L is $D - 2$, and so $D - 2 + \delta_1$ is the corresponding upper bound over $\mathbb{Q}$ (see Remark 4.1).

We now thin S to an infinite subset S' such that for $s \in S'$, the D-tuple $e^{\bar{b}s}$ is a point of V. This might force to throw out part of the original S_0 but this is irrelevant for the estimates on the linear dimension of S'.

Fix a finite sequence $\bar{s} = (s_1, \ldots, s_k)$ of distinct elements of S, of length k, and let T be the set of entries $\bar{s}$. The $\mathbb{Q}$-linear relations among $\bar{b}s_1, \ldots, \bar{b}s_k$ can be converted into $\mathbb{Z}$-linear ones, and these naturally induce multiplicative relations of group type among the corresponding exponentials $e^{\bar{b}s_1}, \ldots, e^{\bar{b}s_k}$. Thus we determine an algebraic subgroup Γ_k of G_m^{Dk} on which $e^{\bar{b}s_1}, \ldots, e^{\bar{b}s_k}$ lie. Clearly, the codimension of Γ_k is $Dk - D(T)$, and dimension of Γ_k over $\mathbb{Q}$ is $D(T)$.

Let V^k be the product variety in the multiplicative group G_m^{Dk}. The Dk-tuple

$$(e^{\bar{b}s_1}, \dots, e^{\bar{b}s_k}) \tag{9}$$

lies on it, and this is true for any choice of k solutions $s_1, \dots, s_k$. An upper bound for the transcendence degree of any tuple as in (9) over L is $k(D-2)$, and $k(D-2)+\delta_1$ is a corresponding upper bound over $\mathbb{Q}$.

The Dk-tuple

$$(e^{\bar{b}s_1}, \dots, e^{\bar{b}s_k})$$

belongs to the intersection of V^k and Γ_k, which might be reducible, and we will work with the variety $W_{\bar{s}}$ of the point $(e^{\bar{b}s_1}, \dots, e^{\bar{b}s_k})$ over L.

Claim 1. For $k > \delta_1 + \delta_2$ the variety $W_{\bar{s}}$ is either anomalous or of dimension 0 over L.

Suppose $\dim(W_{\bar{s}}) \le \dim(V^{Dk}) - \operatorname{codim}(\Gamma_k)$, i.e.

$$\dim(W_{\bar{s}}) \le k(D-2) - (kD - D(T)) + \delta_1.$$

Again Schanuel's Conjecture implies

$$D(T) \le k(D-2) - (kD - D(T)) + \delta_1 + \delta_1 + 2\delta_2,$$

and so

$$2k \le 2\delta_1 + 2\delta_2.$$

Hence the claim is proved.

We want to get results not sensitive to any particular enumeration. Now suppose we rearrange the sequence $\bar{s}$ to $\overline{s^*}$. The set T does not change. It is easy to see that we still get points on V^k, and dimension of Γ_k does not change. What may change is $W_{\overline{s^*}}$. But consider the automorphisms (of affine Dk-space, of V^k, and of G_m^{Dk}) got by simply permuting the natural D-blocks. These transform the $W_{\bar{s}}$ to the $W_{\overline{s^*}}$, and one sees easily that $W_{\bar{s}}$ has dimension 0 if and only if $W_{\overline{s^*}}$ has, and that $W_{\bar{s}}$ is anomalous if and only if $W_{\overline{s^*}}$ is. So the claim implies that for every k, if $k > \delta_1 + \delta_2$ then either each $W_{\overline{s^*}}$ has dimension 0, or each $W_{\overline{s^*}}$ is anomalous.

Claim 2. If $\dim W_{\bar{s}} = 0$ then $D(T) \le 2\delta_1 + 2\delta_2$.

Suppose $\dim W_{\bar{s}} = 0$. Hence the coordinates of all elements of $W_{\bar{s}}$ are algebraic over L, which implies that

$$\text{t.d.}(e^{\bar{b}s_1}, \dots, e^{\bar{b}s_k}) \le \delta_1.$$

From Lemma 5.3 it follows that

$$\text{t.d.}(\bar{b}s_1, \dots, \bar{b}s_k) \le \delta_1 + 2\delta_2,$$

and Schanuel's Conjecture implies

$$D(T) \leq 2\delta_1 + 2\delta_2.$$

This now gives that for any k-element subset T of S, if

$$D(T) > 2\delta_1 + 2\delta_2$$

then $W_{\bar{s}}$ is anomalous, for any enumeration $\bar{s}$ of T.

We consider now a countably infinite subset of S enumerated as $s_1, s_2, \ldots$, which we will continue to call S. Define S_k as the set $\{s_1, \ldots, s_k\}$. Let W_k be one of the $W_{\bar{s}}$ for a sequence $\bar{s}$ enumerating S_k. If infinitely many W_k are of dimension 0, then the set $\{e^{b_j s} : b_j \in B, s \in S\}$ is contained in L, and so by Schanuel's Conjecture and the preceding calculations, $D(S_k) \leq 2(\delta_1 + \delta_2)$ for infinitely many k's. So S spans a finite dimensional space over $\mathbb{Q}$, which is the required conclusion. Thus, there is a k_1 such that for k at least k_1 no W_k has dimension 0. Thus by Claim 1, all W_k are anomalous. Since W_k was chosen for an arbitrary enumeration of S_k, we conclude that each $W_{\overline{s^*}}$ is anomalous, for any enumeration $\overline{s^*}$ of S_k.

We will make use of the Bombieri, Masser and Zannier results. Though the W_k are defined relative to an enumeration, and would change if the enumeration did, there are some basic results independent of the enumeration, and these will be needed in the remaining stages of the proof.

Let $k_2 \in \mathbb{N}$ be the least integer k such that for any $k_2 + 1$ elements of S, $\eta_1, \ldots, \eta_{k_2+1}$, the variety W of the $k_2 + 1$-tuple $e^{\bar{b}\eta_1}, \ldots, e^{\bar{b}\eta_{k_2+1}}$ is anomalous in V^{k_2+1}. From [1] it follows that there is a finite collection $\Phi_{V^{k_2+1}}$ of proper tori $H_1, \ldots, H_t$ of $G_m^{(k_2+1)D}$ such that each maximal anomalous subvariety of V^{k_2+1} is a component of the intersection of V^{k_2+1} with a coset of one of the H's.

We use a much less precise version for general anomalous subvarieties. This version follows from the very precise Structure Theorem of Bombieri, Masser and Zannier. We proceed as follows: from the above list $H_1, \ldots, H_t$ for each one we pick one of the multiplicative conditions defining each of them. These define a finite set $\{J_1, \ldots, J_t\}$ of codimension 1 subgroups so that every anomalous subvariety is contained in a coset of one of them. Crucially, these cosets can be chosen defined over L.

Let W be anomalous as above. Then there is a codimension 1 subgroup J_j from the above finite list defined by a nonzero $D(k_2 + 1)$ integer vector,

$$\overline{\alpha_j} = \alpha_{j1}, \ldots, \alpha_{jD(k_2+1)}$$

and $\theta_W \in L$ such that the following relation holds

$$\overline{w}^{\overline{\alpha_j}} = \theta_W \tag{10}$$

for all $\overline{w} \in W$. Notice that the finitely many vectors $\overline{\alpha_1}, \dots, \overline{\alpha_t}$ depend only on the variety V^{k_2+1}. Fix an order on the finite set of $\overline{\alpha_j}$'s, $j = 1, \dots, t$. To any subset of S of cardinality $k_2 + 1$, $E = \{\eta_1, \dots, \eta_{k_2+1}\}$, where $\eta_1 < \cdots < \eta_{k_2+1}$ with respect to the fixed order on S, we associate the anomalous variety of the tuple $e^{\bar{b}\eta_1}, \dots, e^{\bar{b}\eta_{k_2+1}}$.

We now define a coloring of the subsets of S of cardinality $k_2 + 1$. Consider the function

$$\Phi\colon [S]^{k_2+1} \to \{\overline{\alpha_1}, \dots, \overline{\alpha_t}\}$$

that associates to any set in $[S]^{k_2+1}$ the tuple $\overline{\alpha_j}$ for the minimum j such that the anomalous variety corresponding to the subset is included in a coset (defined over L) of J_j.

By Ramsey's Theorem there is an infinite set $T \subseteq S$ and a fixed j_0 such that Φ takes the constant value $\overline{\alpha_{j_0}}$ on the set of $k_2 + 1$ cardinality subsets of T. Let $F \in [T]^{k_2+1}$ and order the elements of F as $\epsilon_1 < \cdots < \epsilon_{k_2+1}$, where $<$ is the order of T inherited from S. We write the $D(k_2 + 1)$-tuple $\overline{\alpha_{j_0}}$ as the concatenation of two parts $\overline{\alpha_{j_0}} = \overline{\alpha_{j_0}}_+ \, \overline{\alpha_{j_0}}_-$, where the *minus* part denotes the last block of D elements.

Case a) $\overline{\alpha_{j_0}}_- \neq \bar{0}$. We fix the first k_2 elements of F, $\epsilon_1 < \cdots < \epsilon_{k_2}$, and we consider all elements s of T greater than ϵ_{k_2}. There are infinitely many such elements s, and if we append the D-tuple $b_1 s, \dots, b_D s$ to $\bar{b}\epsilon_1 \dots \bar{b}\epsilon_{k_2}$, we get an element of $[T]^{k_2+1}$. We now exploit the indiscernibility of $[T]^{k_2+1}$. For each s as chosen, there is an element θ_s in L such that

$$(e^{\bar{b}\epsilon_1} \dots e^{\bar{b}\epsilon_{k_2}})^{\overline{\alpha_{j_0}}_+} (e^{\bar{b}s})^{\overline{\alpha_{j_0}}_-} = \theta_s. \tag{11}$$

Let $A_F = (e^{\bar{b}\epsilon_1} \dots e^{\bar{b}\epsilon_{k_2}})^{\overline{\alpha_{j_0}}_+}$. Notice that the inner product $\bar{b} \cdot \overline{\alpha_{j_0}}_- \neq 0$ since $\overline{\alpha_{j_0}}_- \neq \bar{0}$ and the $\bar{b}$ are linearly independent over $\mathbb{Q}$. (Recall that we always assume s is nonzero). So

$$(e^{\bar{b}s})^{\overline{\alpha_{j_0}}_-} = \frac{\theta_s}{A_F} \in L(A_F)$$

for each fixed s.

Then the transcendence degree of

$$\{e^{(\bar{b}\cdot\overline{\alpha_{j_0}}_-)s} : s \in T \backslash \{\epsilon_1, \dots, \epsilon_{k_2}\}\}$$

over $\mathbb{Q}$ is bounded by the transcendence degree of L and A_F. Appealing to Schanuel's Conjecture we get the finiteness of the linear dimension of the $\mathbb{Q}$-space generated by $\{(\bar{b} \cdot \overline{\alpha_{j_0}}_-)s : s \in T \backslash \{\epsilon_1, \dots, \epsilon_{k_2}\}\}$. Clearly, then the set $T \backslash \{\epsilon_1, \dots, \epsilon_{k_2}\}$ is finite dimensional over $\mathbb{Q}$.

Case b) $\overline{\alpha_{j_0}}_- = \bar{0}$. We shift to the next block to the left in $\overline{\alpha_{j_0}}$ not identically zero suppose this corresponds to ℓ, with $\ell \leq k_2$. As before we make the corresponding coordinate in the ℓth position in $\epsilon_1 < \cdots < \epsilon_\ell$ vary over all elements of T strictly greater than $\epsilon_1 < \cdots < \epsilon_{\ell-1}$ and completing the $k_2 + 1$ tuple respecting the order of T. We argue then as before. □

An immediate consequence of the finite dimensionality of S is the following corollary which can be viewed as a multiplicative version of the statement of the Main Lemma.

Corollary 5.4. *Let $\widehat{G}$ be the divisible hull of G, the group generated by all $e^{\mu_j s}$'s where $s \in S$ and $j = 1, \ldots, N$. Then $\widehat{G}$ has finite rank.*

A basic result on linear functions on finite rank groups that will be relevant in the remaining part of the proof is due to Evertse, Schlickewei and Schmidt (see [6]).

We recall that a solution $(\alpha_1, \ldots, \alpha_n)$ of a linear equation

$$a_1 x_1 + \cdots + a_n x_n = 1 \tag{12}$$

over a field K is non degenerate if for every proper non empty subset I of $\{1, \ldots, n\}$ we have $\sum_{i \in I} a_i \alpha_i \neq 0$.

In our context we will be interested in solving the linear equation (12) in units of the field. Hence it is natural to consider equations of the form

$$a_1 x_1 + \cdots + a_n x_n = 0$$

instead than (12).

Lemma 5.5 ([6]). *Let K be a field of characteristic 0, n a positive integer, and Γ a finitely generated subgroup of rank r of the multiplicative group $(K^\times)^n$. There exists a positive integer $R = R(n, r)$ such that for any non zero $a_1, \ldots, a_n$ elements in K, the equation*

$$a_1 x_1 + \cdots + a_n x_n = 1 \tag{13}$$

does not have more than R non degenerate solutions $(\alpha_1, \ldots, \alpha_n)$ in Γ.

We now apply this result to our context. Let $p \in \mathbb{N}$, be the linear dimension of S, and $\{s_1, \ldots, s_p\}$ be a $\mathbb{Q}$-basis of S. For any $s \in S$ we have

$$s = \sum_{l=1}^{p} c_l s_l \tag{14}$$

where $c_l \in \mathbb{Q}$. Substituting the expression of s as in (14) in f we have

$$0 = f(s) = \lambda_1 e^{\mu_1 (\sum_{l=1}^{p} c_l s_l)} + \cdots + \lambda_N e^{\mu_N (\sum_{l=1}^{p} c_l s_l)} = \sum_{j=1}^{N} \lambda_j \prod_{l=1}^{p} (e^{\mu_j s_l})^{c_l} \tag{15}$$

Any solution $s \in S$ produces a solution $\bar{\omega}$ of the linear equation associated to f,

$$\lambda_1 X_1 + \cdots + \lambda_N X_N = 0 \tag{16}$$

where $\omega_i = e^{\mu_i (\sum_{l=1}^{p} c_l s_l)}$, $i = 1, \ldots, N$ and $\bar{\omega} \in \widehat{G}$ (a subgroup of $(\mathbb{C}^*)^N$, see Corollary 5.4).

Since the coefficients of f are nonzero, we can transform this equation to the form of the unit equation by replacing λ_N by $-\lambda_N$, and multiplying throughout by $(-\lambda_N)^{-1} e^{-\mu_N s}$.

Lemma 5.6. *Suppose $f(z) = \lambda_1 e^{\mu_1 z} + \cdots + \lambda_N e^{\mu_N z}$ is not simple, and s_1, s_2 are two distinct solutions of f. Then the solutions of* (16) *generated by s_1 and s_2 are different.*

Proof. Let $\bar{\omega} = \omega_1, \ldots, \omega_N$ and $\bar{\xi} = \xi_1, \ldots, \xi_N$ be the solutions of (16) corresponding to s_1 and s_2, respectively. If

$$(\omega_1, \ldots, \omega_N) = (\xi_1, \ldots, \xi_N),$$

then for $j = 1, \ldots, N$,

$$\prod_{l=1}^{p} (e^{\mu_j s_l})^{c_{1,l}} = \prod_{l=1}^{p} (e^{\mu_j s_l})^{c_{2,l}},$$

iff

$$\prod_{l=1}^{p} (e^{\mu_j s_l})^{c_{1,l} - c_{2,l}} = 1$$

iff

$$\mu_j \sum_{l=1}^{p} s_l (c_{1,l} - c_{2,l}) \in 2\pi i \mathbb{Z}.$$

So, for any $j = 1, \ldots, N$ we have

$$\sum_{l=1}^{p} s_l (c_{1,l} - c_{2,l}) = \frac{2\pi i}{\mu_j} h_j$$

where $h_j \in \mathbb{Z}$. This implies

$$\frac{2\pi i}{\mu_1} h_1 = \frac{2\pi i}{\mu_2} h_2 = \cdots = \frac{2\pi i}{\mu_N} h_N.$$

So we can write any exponents μ_j in the polynomial $f(z)$ in terms of μ_1, i.e.,

$$\begin{aligned}\mu_2 &= \frac{\mu_1}{h_1} h_2,\\ \mu_3 &= \frac{\mu_1}{h_1} h_3,\\ &\vdots\\ \mu_N &= \frac{\mu_1}{h_1} h_N.\end{aligned}$$

If $\alpha = \frac{\mu_1}{h_1}$ then $f(z)$ is a polynomial in $e^{\alpha z}$, i.e. f is a simple polynomial. We get a contradiction since f is not simple. □

We restate the remaining case of Shapiro's Conjecture.

Theorem 5.7 (SC). *Let $f(z)$ be an irreducible polynomial and suppose the following system*

$$\begin{cases} f(z) = \lambda_1 e^{\mu_1 z} + \cdots + \lambda_N e^{\mu_N z} = 0,\\ g(z) = l_1 e^{m_1 z} + \cdots + l_M e^{m_M z} = 0 \end{cases} \tag{17}$$

has infinitely common zeros. Then f divides g.

Proof. We will use induction on the length of the polynomial $g(z)$. Without loss of generality we may assume $N, M > 2$, and g not simple otherwise we would be in Case 1 solved by van der Poorten and Tijdeman.

Consider the linear equation associated to $g(z) = 0$,

$$l_1 X_1 + \cdots + l_M X_M = 0. \tag{18}$$

We can transform this equation to a unit equation as in Lemma 5.5. Lemma 5.6 implies that equation (18) has infinitely many solutions $\bar{\alpha} = (\alpha_1, \ldots, \alpha_M)$, where $\alpha_t = e^{m_t(\sum_{\ell=1}^{p} c_\ell s_\ell)}$ (each one generated by s, a solution of (17)). From Lemma 5.5 it follows that all but finitely many of them are degenerate.

By the Pigeonhole Principle there exists a proper subset $I = \{i_1, \ldots, i_r\}$ of $\{1, \ldots, M\}$ such that

$$l_{i_1} X_{i_1} + \cdots + l_{i_r} X_{i_r} = 0 \tag{19}$$

has infinitely many zeros of the right form. Notice that I has at least three elements since we are assuming that g is not a simple polynomial.

It is useful to write $g(z) = g_1(z) + g_2(z)$, where $g_1(z) = l_{i_1} e^{m_{i_1} z} + \cdots + l_{i_r} e^{m_{i_r} z}$, and $g_2(z) = g(z) - g_1(z)$. The polynomial g_1 has infinitely many common zeros with $f(z)$. Also, $g_2(z)$ has infinitely many common zero with $f(z)$. Both $g_1(z)$ and $g_2(z)$ have lengths strictly less than M.

By inductive hypothesis and by the irreducibility of f, we have that f divides g_1 and f divides g_2, and hence f divides g. So the proof is completed. □

Acknowledgements. This work has been supported by FIRB 2010 *New advances in the Model Theory of Exponentiation*.

References

[1] E. Bombieri, D. Masser and U. Zannier,Anomalous subvarieties structure theorems and applications. *Internat. Math. Res. Notices IMRN* **2007** (2007), no. 19, Art. ID rnm057, 33 pp. Zbl 1145.11049 MR 2359537

[2] P. D'Aquino, A. Macintyre and G. Terzo, Schanuel Nullstellensatz for Zilber fields. *Fund. Math.* **207** (2010), no. 2, 123–143. Zbl 1207.03044 MR 2586007

[3] A. J. van der Poorten, Factorisation in fractional powers. *Acta Arith.* **70** (1995), no. 3, 287–293. Zbl 0818.11011 MR 1322566

[4] A. J. van der Poorten and G. R. Everest, Factorisation in the ring of exponential polynomials. *Proc. Amer. Math. Soc.* **125** (1997), no. 5, 1293–1298. Zbl 1017.11009 MR 1401740

[5] A. J. van der Poorten and R. Tijdeman, On common zeros of exponential polynomials. *Enseignement Math.* (2) **21** (1975)), no. 1, 57–67. Zbl 0308.30006 MR 0379387

[6] J. H. Evertse, H. P. Schlickewei and W. M. Schmidt, Linear equations in variables which lie in a multiplicative group. *Ann. of Math.* **155** (2002), no. 3, 807–836. Zbl 1026.11038 MR 1923966

[7] E. Gourin, On irreducible polynomials in several variables which become reducible when the variables are replaced by powers of themselves. *Trans. Amer. Math. Soc.* **32** (1930), 485–501. JFM 56.0111.01 MR 1501547

[8] J. Kirby, A. Macintyre, and A. Onshuus, The algebraic numbers definable in various exponential fields. *J. Inst. Math. Jussieu* **11** (2012), no. 4, 825–834. Zbl 1270.03057 MR 2979823

[9] L. A. MacColl, A factorization theory for polynomials in x and in functions $e^{\alpha x}$. *Bull. Amer. Math. Soc.* **41** (1935), 104–109. Zbl 0011.20204 MR 1563030

[10] A. Macintyre, Exponential algebra. In *Logic and algebra* (Pontignano, 1994), ed. by A. Ursini et al., Lecture Notes in Pure and Appl. Math. 180, Marcel Dekker, New York 1996, 191–210. Zbl 0891.12006 MR 1404940

[11] A. Macintyre and A. Wilkie, On the decidability of the real exponential field. In *Kreiseliana: about and around Georg Kreisel*, A K Peters, Wellesley, MA, 441-467. Zbl 0896.03012 MR 1435773

[12] D. Marker, A remark on Zilber's pseudoexponentiation. *J. Symbolic Logic* **71** (2006), no. 3, 791–798. Zbl 1112.03029 MR 2250821

[13] J. F. Ritt, A factorization theorem of functions $\sum_{i=1}^{n} a_i e^{\alpha_i z}$. *Trans. Amer. Math. Soc.* **29** (1927), 584–596. JFM 53.0122.06 MR 1501406

[14] J. F. Ritt, *On the zeros of exponential polynomials*. *Trans. Amer. Math. Soc.* **31** (1929), 680-686. Zbl 55.0212.01 MR 1501506

[15] H. S. Shapiro, The expansion of mean-periodic functions in series of exponentials. *Comm. Pure Appl. Math.* **11** (1958), 1–21. Zbl 0168.31802 MR 0103387

[16] A. Shkop, Schanuel's conjecture and algebraic roots of exponential polynomials. *Commun. Algebra* **39** (2011), no. 10, 3813–3823. Zbl 1257.03061 MR 2845603

[17] G. Terzo, Some Consequences of Schanuel's Conjecture in exponential rings. *Commun. Algebra* **36** (2008), no. 3, 1171–1189. Zbl 1141.03011 MR 2394281

[18] B. Zilber, Pseudo-exponentiation on algebraically closed fields of characteristic zero. *Ann. Pure Appl. Logic* **132** (2005), no. 1, 67–95. Zbl 1076.03024 MR 2102856

Received May 23, 2012

P. D'Aquino, Department of Mathematics and Physics, Seconda Università di Napoli, Viale Lincoln 5, 81100 Caserta, Italy

E-mail: paola.daquino@unina2.it

A. Macintyre, School of Mathematical Sciences, Queen Mary, University of London, Mile End Road, London E1 4NS, England

E-mail: A.macintyre@qmul.ac.uk

G. Terzo, Department of Mathematics and Physics, Seconda Università di Napoli, Viale Lincoln 5, 81100 Caserta, Italy

E-mail: giuseppina.terzo@unina2.it