

ON THE CLASSIFICATION OF SOLUTIONS OF QUANTUM FUNCTIONAL EQUATIONS WITH CYCLIC AND SEMI-CYCLIC SUPPORTS

LAN NGUYEN

Department of Mathematics, The University of Wisconsin-Parkside, Kenosha, Wisconsin, USA

ABSTRACT. In this paper, we classify all solutions with cyclic and semi-cyclic semigroup supports of the functional equations arising from multiplication of quantum integers with fields of coefficients of characteristic zero. This also solves completely the classification problem proposed by Melvyn Nathanson and Yang Wang concerning the solutions, with semigroup supports which are not prime subsemigroups of \mathbb{N} , to these functional equations for the case of rational field of coefficients. As a consequence, we obtain some results for other problems raised by Nathanson concerning maximal solutions and extension of supports of solutions to these functional equations in the case where the semigroup supports are not prime subsemigroups of \mathbb{N} .

Communicated by Jean-Paul Allouche

1. Introduction

The problems considered in this paper come from the study of symmetry of roots of polynomials called quantum integers and the functional equations arising from their arithmetics in the context of Additive and Combinatorial Number Theory. Such study was initiated by M. B. Nathanson [4, 5, 6].

In this paper, we solve an open problem proposed by Nathanson and Wang concerning the classification of solutions with supports which are not prime

© 2021 BOKU-University of Natural Resources and Life Sciences and Mathematical Institute, Slovak Academy of Sciences.

2010 Mathematics Subject Classification: 81R50; 11R18; 11T22; 11B13; 11C08; 39B05.

Key words: quantum integer; quantum algebra; q -series; semigroup; polynomial functional equation; cyclotomy.

Licensed under the Creative Commons Attribution-NC-ND 4.0 International Public License.

subsemigroups of \mathbb{N} . Together with [9], our results in this paper also provide a complete solution to this problem for the case of rational field of coefficients. An overview of the topic and some relevant background concerning quantum integers and the functional equations arising from their multiplication is given in this section. Results are given in section 2.

1.1. Preliminary Background

DEFINITION 1. For any integer n , the corresponding quantum integer is an expression of the form

$$[n]_q := q^{n-1} + \cdots + q + 1 = \frac{q^n - 1}{q - 1}. \quad (1)$$

Only the quantum integers with n being natural numbers are considered in the rest of this paper. The q -series expansion of the sumset identity

$$\begin{aligned} \{0, 1, \dots, mn - 1\} &= \{0, 1, \dots, m - 1\} + \{0, m, \dots, (n - 1)m\} \\ &= \{0, 1, \dots, n - 1\} + \{0, n, \dots, (m - 1)n\} \end{aligned}$$

defines in [5] a multiplication operation for quantum integers, called quantum multiplication, as follows

$$[m]_q \star [n]_q := [mn]_q = [m]_q \cdot [n]_{q^m} = [n]_q \cdot [m]_{q^n}, \quad (2)$$

where \star denotes quantum multiplication and \cdot denotes the usual multiplication of polynomials. The symmetry in equation (2) leads Nathanson and Wang to the study the symmetry of roots of sequences of functions

$$\Gamma = \{f_n(q) \mid n \in \mathbb{N}\},$$

with coefficients contained in some field, satisfying the following functional equations

$$f_m(q)f_n(q^m) \stackrel{(1)}{=} f_n(q)f_m(q^n) \stackrel{(2)}{=} f_{mn}(q) \quad (3)$$

for all $m, n \in \mathbb{N}$. In the rest of this paper, we refer to the first equality in (3) and the full functional equation (3) as Functional Equation (1) and Functional Equation (2), respectively. Let P be a set of primes and A_P be the subset of \mathbb{N} consisting of 1 and all natural numbers whose prime factors come from P . Then A_P is a multiplicative prime semigroup which is called the semigroup associated to P .

DEFINITION 2. Let Γ be a sequence of polynomials satisfying Functional Equation (2). Then the smallest field K which contains all the coefficients of all the polynomials in Γ is called the field of coefficients of Γ . The field \bar{K} denotes its algebraic closure.

In the rest of this paper, the fields of coefficients of all the sequences of polynomials considered are assumed to be of characteristic zero. Let $\Gamma = \{f_n(q) \mid n \in \mathbb{N}\}$ be a sequence of polynomials satisfying Functional Equation (2). The set of integers n in \mathbb{N} , where $f_n(q) \neq 0$ is called the support of Γ and is denoted by $\text{supp}\{\Gamma\}$. Some immediate and relevant relations between Functional Equations (1) and (2) are established by Nathanson in [4] and can be summarized as follows:

- A sequence of polynomials which satisfies Functional Equation (2) automatically satisfies Functional Equation (1) but not vice versa [4] or [7].
- If P is a set of primes and if $\{h_p(q) \mid p \in P\}$ is a sequence of polynomials satisfying Functional Equation (1), then there exists a unique sequence of polynomials $\Gamma := \{f_n(q) \mid n \in \mathbb{N}\}$ satisfying Functional Equation (2) with support A_P such that $f_p(q) = h_p(q)$ for each p in P .

THEOREM 1 ([4]). *Let $\Gamma = \{f_n(q) \mid n \in \mathbb{N}\}$ be a sequence of polynomials satisfying Functional Equation (2). Then $\text{supp}\{\Gamma\}$ is of the form A_P for some set of primes P , and Γ is completely determined by the collection of polynomials $\{f_p(q) \mid p \in P\}$.*

DEFINITION 3. Let P be the collection of primes associated to the support A_P , in the sense of Theorem 1, of a sequence of polynomials Γ satisfying Functional Equation (2). Then P is called the support base of Γ .

If P is a set of primes in \mathbb{N} , then there is at least one sequence Γ satisfying Functional Equation (2) with support base P . One such sequence can be defined as the set of polynomials:

$$\Gamma := \left\{ f_n(q) = \begin{cases} [n]_q, & n \in A_P; \\ 0, & \text{otherwise.} \end{cases} \mid n \in \mathbb{N} \right\}.$$

Moreover, for each natural number g , the sequence of polynomials

$$\Gamma_g := \left\{ f_{n,g}(q) = \begin{cases} [n]_{q^g}, & n \in A_P; \\ 0, & \text{otherwise.} \end{cases} \mid n \in \mathbb{N} \right\} \quad (4)$$

also satisfies Functional Equation (2) [5].

The following normalization result, similar to that of Nathanson (see [4]), is provided in [7] and is useful for us in the rest of this paper.

THEOREM 2 ([7]). *Let $\Gamma = \{f_n(q) \mid n \in \mathbb{N}\}$ be a nonzero sequence of polynomials satisfying Functional Equation (2). Then there exists a unique completely multiplicative arithmetic function $\psi(n)$, a rational number t , and a unique sequence $\Sigma = \{g_n(q) \mid n \in \mathbb{N}\}$ satisfying (2) with the same support such that*

$f_n(q) = \psi(n)q^{t(n-1)}g_n(q)$, where $g_n(q)$ is a monic polynomial with $g_n(0) \neq 0$ for all $n \in \text{supp}\{\Gamma\}$.

The sequence $\{g_n(q) \mid n \in \mathbb{N}\}$ above is called the *normalized sequence* associated to Γ . As a result of Theorem 2, we only need to consider normalized sequences in the rest of the paper, unless otherwise stated.

DEFINITION 4. If $\Gamma_1 = \{f_n(q) \mid n \in \mathbb{N}\}$ and $\Gamma_2 = \{g_n(q) \mid n \in \mathbb{N}\}$ are two nonzero sequences of polynomials satisfying Functional Equation (2), then $\Gamma_1 \cdot \Gamma_2$ denotes the collection $\{f_n g_n(q) \mid n \in \mathbb{N}; f_n(q) \in \Gamma_1, g_n(q) \in \Gamma_2\}$ with $f_n g_n(q) = f_n(q)g_n(q)$ and Γ_1/Γ_2 denotes the collection $\{f_n/g_n(q) := \frac{f_n(q)}{g_n(q)} \mid n \in \mathbb{N}; f_n(q) \in \Gamma_1, g_n(q) \in \Gamma_2\}$. A sequence Γ of rational functions satisfying Functional Equation (2) is said to be purely cyclotomic if all zeros and poles of each element of Γ are roots of unity.

THEOREM 3 ([4]). *If Γ_1 and Γ_2 are two nonzero sequences of polynomials satisfying Functional Equation (2), then the sequence $\Gamma_1 \cdot \Gamma_2$ also satisfies Functional Equation (2). Conversely, if $\text{supp}\{\Gamma_1\} = \text{supp}\{\Gamma_2\}$ and Γ_1 as well as $\Gamma_1 \cdot \Gamma_2$ satisfy Functional Equation (2), then Γ_2 also satisfies Functional Equation (2). The collection of all solutions of Functional Equation (2) is an abelian semigroup. Also for every set of primes P , the set of all sequences Γ satisfying Functional Equation (2) and having support A_P forms an abelian cancelation semigroup, which will be denoted by Υ_P .*

Recall that if Υ is an abelian cancelation semigroup, then there exists an abelian group $K(\Upsilon)$ and an injective semigroup homomorphism $i : \Upsilon \hookrightarrow K(\Upsilon)$ such that for any abelian group G and $\alpha : \Upsilon \hookrightarrow G$, there exists a unique group homomorphism $\alpha' : K(\Upsilon) \hookrightarrow G$ such that $\alpha = \alpha' \circ i$. The group $K(\Upsilon)$ is called the Grothendieck group of Υ .

THEOREM 4 ([4]). *Let P be a set of primes and A_P be the associated prime semigroup. Let Υ_P be the abelian cancelation semigroup of polynomial solutions of Functional Equation (2) with support A_P . Then the Grothendieck group $K(\Upsilon_P)$ of Υ_P is the group of all sequences of rational functions \mathcal{F}/\mathcal{G} , where \mathcal{F} and \mathcal{G} are in Υ_P .*

REMARK 1. If two sequences Γ_1 and Γ_2 of polynomials satisfy Functional Equation (2), then so does the sequence Γ_1/Γ_2 .

Now let us define some terminology concerning the multiplicative subsemigroups of the group of natural numbers \mathbb{N} which are not necessarily prime semigroups.

DEFINITION 5. Let \mathcal{A} be a multiplicative subsemigroup of \mathbb{N} , i.e., 1 is in \mathcal{A} and if a and b are in \mathcal{A} then ab is in \mathcal{A} . Then \mathcal{A} is said to be **semi-cyclic** with generator a if a is the greatest natural number such that every element of \mathcal{A} can be written in the form a^n for some nonnegative integer n . The integer n is called the **index power** with respect to a of the element a^n in \mathcal{A} . If \mathcal{A} also contains such an a , then it is called **cyclic**. If \mathcal{A} does not contain such an a , we call it **strict semi-cyclic**.

1.2. Problems

Let \mathcal{A} be a multiplicative subsemigroup of \mathbb{N} not necessarily a prime semigroup. The following problems concerning sequences of polynomials satisfying Functional Equation (2) with support \mathcal{A} , which are proposed by Melvyn Nathanson, correspond to the problems of decomposition, which are fundamental in additive number theory. It arises naturally from the study of the q -analogues of the Riemann Zeta functions and Bernoulli numbers [1, 2, 3, 13]:

PROBLEM 1. Determine all sequences of polynomials

$$\Gamma := \{f_m(q) \mid m \in \mathcal{A}\}$$

satisfying Functional Equation (2) where \mathcal{A} is a multiplicative subsemigroup of \mathbb{N} which is not necessarily a prime semigroup.

PROBLEM 2. Given a sequence of polynomials

$$\Gamma := \{f_m(q) \mid m \in \mathcal{A}\}$$

satisfying Functional Equation (2) with support a multiplicative subsemigroup \mathcal{A} of \mathbb{N} , not necessarily a prime semigroup. Let $\mathcal{A}' \supseteq \mathcal{A}$ be another multiplicative subsemigroup of \mathbb{N} which is not necessarily a prime semigroup. Determine the criteria for the existence of a sequence of polynomial satisfying Functional Equation (2)

$$\Gamma := \{f'_m(q) \mid m \in \mathcal{A}'\}$$

such that

$$f_m(q) = f'_m(q) \quad \text{for all } m \text{ in } \mathcal{A}.$$

These problems differ from those considered in previous papers on this subject in that the supports of the sequences of polynomials are not assumed to be prime semigroups. In the rest of the paper, all semigroups \mathcal{A} considered are *multiplicative* subsemigroups of \mathbb{N} so we drop the multiplicative part from the term for simplicity.

2. Main Results

Many results concerning solutions whose semigroup supports are prime sub-semigroups of \mathbb{N} are provided in [4]–[12], and it can be seen from these papers that obtaining such results requires the existences of prime-indexed elements in these solutions. Because of the lack of prime-indexed elements in the solutions whose semigroup supports are not prime sub-semigroups of \mathbb{N} , few results are known [9] concerning these solutions. For the case considered in this paper, we have to employ a completely different method from those used in [4]–[12] to obtain our results.

Our main results in this paper are stated below.

THEOREM 5. *Let \mathcal{A} be a subsemigroup of \mathbb{N} which is not necessarily a prime semigroup. If \mathcal{A} is semi-cyclic with generator a , then the following statements hold:*

- 1) *There exist infinitely many normalized polynomial solution $\Gamma = \{f_n(q) \mid n \in \mathcal{A}\}$ to Functional Equation (2) with support \mathcal{A} and fields of coefficients K of characteristic zero.*
- 2) *If $\Gamma = \{f_n(q) \mid n \in \mathcal{A}\}$ is a (normalized) solution to Functional Equation (2) with field of coefficients K of characteristic zero and support \mathcal{A} , then there exist monic polynomials $f(q)$ and $g(q)$ with nonzero constant terms such that $(f(q), g(q)) = 1$ in $\bar{K}[q]$, where \bar{K} is the algebraic closure of K and*

$$f_n(q) = \frac{f(q)}{g(q)} \frac{f(q^a)}{g(q^a)} \cdots \frac{f(q^{a^{i_n-1}})}{g(q^{a^{i_n-1}})} \quad (5)$$

for all $n > 1$ in \mathcal{A} , where i_n is the index power of n with respect to a . The rational function $\frac{f(q)}{g(q)}$ is unique and $g(q) = 1$ if \mathcal{A} is cyclic.

COROLLARY 1. *Let $\Gamma = \{f_n(q) \mid n \in \mathcal{A}\}$ be a polynomial solution to Functional Equation (2) with field of coefficients K of characteristic zero and support \mathcal{A} , a subsemigroup of \mathbb{N} not necessarily a prime semigroup. Suppose \mathcal{A} is semi-cyclic with generator a . If \mathcal{A}^* is a subsemigroup of \mathbb{N} strictly containing \mathcal{A} such that \mathcal{A}^* is also semi-cyclic, then there exists a polynomial solution $\Gamma^* = \{f_n^*(q) \mid n \in \mathcal{A}^*\}$ to Functional Equation (2) with field of coefficients of characteristic zero, support \mathcal{A}^* , and $f_n^*(q) = f_n(q)$ for all n in \mathcal{A} if and only if the following conditions hold:*

- *there exists a positive integer \hat{a} such that $a = \hat{a}^e$ as well as $a^* = \hat{a}^{e^*}$ for some positive integers e and e^* ;*

- there exist a unique rational function $\frac{\widehat{f}(q)}{\widehat{g}(q)}$, where $\widehat{f}(q)$ and $\widehat{g}(q)$ are monic polynomials with nonzero constant terms such that $(\widehat{f}(q), \widehat{g}(q)) = 1$ in $\bar{K}[q]$ and

$$\frac{f(q)}{g(q)} = \frac{\widehat{f}(q)}{\widehat{g}(q)} \frac{\widehat{f}(q^{\widehat{a}})}{\widehat{g}(q^{\widehat{a}})} \cdots \frac{\widehat{f}(q^{\widehat{a}^e - 1})}{\widehat{g}(q^{\widehat{a}^e - 1})}, \quad (6)$$

where $f(q)$ and $g(q)$ are the polynomials satisfying (5) in Theorem 5 for all $n > 1$ in \mathcal{A} ;

- for all n in $\mathcal{A}^* - \mathcal{A}$,
- $$\frac{\widehat{f}(q)}{\widehat{g}(q)} \frac{\widehat{f}(q^{\widehat{a}})}{\widehat{g}(q^{\widehat{a}})} \cdots \frac{\widehat{f}(q^{\widehat{a}^{i_n^*} - 1})}{\widehat{g}(q^{\widehat{a}^{i_n^*} - 1})} \quad (7)$$

are polynomials, where $n = \widehat{a}^{i_n^*}$.

Such a solution Γ^* , if exists, has the following properties:

$$f_n^*(q) = \frac{f^*(q)}{g^*(q)} \frac{f^*(q^{a^*})}{g^*(q^{a^*})} \cdots \frac{f^*(q^{(a^*)^{i_n^*} - 1})}{g^*(q^{(a^*)^{i_n^*} - 1})} \quad (8)$$

for all n in $\mathcal{A}^* - \{1\}$ and

$$\frac{f^*(q)}{g^*(q)} = \frac{\widehat{f}(q)}{\widehat{g}(q)} \frac{\widehat{f}(q^{\widehat{a}})}{\widehat{g}(q^{\widehat{a}})} \cdots \frac{\widehat{f}(q^{\widehat{a}^{e^*} - 1})}{\widehat{g}(q^{\widehat{a}^{e^*} - 1})}, \quad (9)$$

where $n = (a^*)^{i_n^*}$.

The results above provide solutions to the following problems:

- Problem 4 in [4] when the fields of coefficients are of characteristic zero and the supports \mathcal{A} are semi-cyclic but not necessarily prime subsemigroups of \mathbb{N} . Together with [9], these results provide a complete solution to Problem 1 for the case of rational fields of coefficients and supports \mathcal{A} , subsemigroups of \mathbb{N} not necessarily prime subsemigroups.
- Problem 3 in [4] concerning maximal solutions (see also [5, 8]) when the fields of coefficients are of characteristic zero and the support \mathcal{A} and \mathcal{A}' are both semi-cyclic subgroups of \mathbb{N} but not necessarily prime subsemigroups.

REMARK 2. The results of this paper and those of [9] are also used in [12] to resolve another problem in this area concerning extensions of supports, not necessarily prime subsemigroups of \mathbb{N} , of polynomial solutions with fields of coefficients K of characteristic zero. Moreover, we plan to establish in a future paper the analogues of the results in [9] for the rational function solutions with non-prime semigroup supports and fields of coefficients of characteristic zero (see [10, 11] for the existence and characterization of rational function solutions with prime semigroup supports and fields of coefficients of characteristic zero).

We divide The proof of Theorem 5 into three sections. In the first section, we prove (1) and provide some reduction results for the proof of (2) of Theorem 5. In the second section, we prove the existence in (2) of Theorem 5. In the third section, we prove the uniqueness in (2) of Theorem 5.

3. Some Reduction Results

Let \mathcal{A} be a subsemigroup of \mathbb{N} which is not necessarily a prime semigroup. Suppose that \mathcal{A} is semi-cyclic with generator a .

- 1) Let $f(q)$ be any monic polynomial with nonzero constant term and with coefficients contained in some field K of characteristic zero. Define $f_1(q) := 1$ and

$$f_n(q) := f(q)f(q^a) \dots f(q^{a^{i_n-1}})$$

for any n in $\mathcal{A} - \{1\}$, where i_n is the index power of n with respect to a . Then it is straightforward to check that the sequence of polynomials $\Gamma = \{f_n(q) \mid n \in \mathcal{A}\}$ is a normalized polynomial solution to Functional Equation (2) with support \mathcal{A} .

- 2) Let $\Gamma = \{f_n(q) \mid n \in \mathcal{A}\}$ be a polynomial solution to Functional Equation (2) with field of coefficients K of characteristic zero and support \mathcal{A} a subsemigroup of \mathbb{N} not necessarily a prime semigroup. Suppose that \mathcal{A} is either cyclic or strict semi-cyclic with generator a and suppose that there exist monic polynomials with nonzero constant terms $f(q)$ and $g(q)$ such that

$$f_n(q) := \frac{f(q)}{g(q)} \frac{f(q^a)}{g(q^a)} \dots \frac{f(q^{a^{i_n-1}})}{g(q^{a^{i_n-1}})}$$

for any n in $\mathcal{A} - \{1\}$. To prove the uniqueness of rational function $\frac{f(q)}{g(q)}$, let us suppose that $\frac{\tilde{f}(q)}{\tilde{g}(q)}$ is another rational function where $\tilde{f}(q)$ and $\tilde{g}(q)$ are monic polynomials with nonzero constant terms such that

$$f_n(q) := \frac{\tilde{f}(q)}{\tilde{g}(q)} \frac{\tilde{f}(q^a)}{\tilde{g}(q^a)} \dots \frac{\tilde{f}(q^{a^{i_n-1}})}{\tilde{g}(q^{a^{i_n-1}})}$$

for any n in $\mathcal{A} - \{1\}$. Then

$$1 = \frac{f\tilde{g}}{g\tilde{f}}(q) \frac{f\tilde{g}}{g\tilde{f}}(q^a) \dots \frac{f\tilde{g}}{g\tilde{f}}(q^{a^{i_n-1}})$$

for all n in $\mathcal{A} - \{1\}$. If $\frac{f\tilde{g}}{g\tilde{f}}(q) \neq 1$, then $\frac{f\tilde{g}}{g\tilde{f}}(q)$ is a nonconstant rational function and a simple argument, using its zeros or poles, shows that the RHS of the above equation cannot be equal to 1 and thus gives a contradiction.

CLASSIFICATION OF SOLUTIONS WITH CYCLIC AND SEMI-CYCLIC SUPPORTS

Now let us show that there exist polynomials $f(q)$ and $g(q)$ satisfying the conditions stated in (2) of Theorem 5.

I) \mathcal{A} is cyclic: This is the obvious case. Since a is in \mathcal{A} , let $f_a(q)$ be the element of Γ indexed by a . Let n be any element of \mathcal{A} and i_n be its index power with respect to a , the nonnegative integer such that $n = a^{i_n}$. Let $f_n(q)$ be the element of Γ indexed by n . Then

$$f_n(q) = f_a(q)f_{a^{i_n-1}}(q^a) = f_a(q)f_a(q^a) \dots f_a(q^{a^{i_n-1}}), \quad (10)$$

where the first equality of (10) follows since Γ is a solution to Functional Equation (2) and the second equality comes from induction on i_n . Let $f(q) = f_a(q)$ and Theorem 5 follows in this case.

II) \mathcal{A} is strict semi-cyclic: The rest of the proof of Theorem 5 is devoted to this case. First let us define some terminology.

DEFINITION 6. Let $\Gamma = \{f_n(q) \mid n \in \mathcal{A}\}$ be a sequence of polynomials satisfying Functional Equation (2) with support \mathcal{A} . Write

$$f_n(q) = f_n^{(1)}(q)f_n^{(2)}(q),$$

where:

- If α is not a root of unity, then α is a zero of $f_n(q)$ if and only if α is a zero $f_n^{(1)}(q)$.
- $f_n^{(2)}(q) = \frac{f_n(q)}{f_n^{(1)}(q)}$.

Then the polynomials $f_n^{(1)}(q)$ and $f_n^{(2)}(q)$ are called the **non-cyclotomic part** and the **cyclotomic part** of $f_n(q)$, respectively. Also, Γ is said to be generated by quantum integers if there exist ordered pairs of integers $\{(u_i, t_i)\}_i$ with $i = 1, \dots, s$ such that

$$f_n^{(2)}(q) = \prod_{i=1}^s ([n]_{q^{u_i}})^{t_i}$$

for all n in \mathcal{A} . We call the sequences $\Gamma^{(2)} := \{f_n^{(2)}(q) \mid n \in \mathcal{A}\}$ and $\Gamma^{(1)} := \{f_n^{(1)}(q) \mid n \in \mathcal{A}\}$ the cyclotomic and non-cyclotomic sequences respectively associated to Γ . We also denote $\sum_{i=1, \dots, s} u_i t_i$ by $t_{\Gamma^{(2)}}$ if Γ is generated by quantum integers.

It is straight forward to check that the sequences $\Gamma^{(1)}$ and $\Gamma^{(2)}$ also satisfy Functional Equation (2). Thus we may assume Γ to be either $\Gamma^{(1)}$ or $\Gamma^{(2)}$ in the rest of the proof of (II). If $\Gamma = \Gamma^{(2)}$ and $f_n(q)$ is a polynomial in Γ , then for any root α of $f_n(q)$, let l_α be the largest positive integer such that α^{l_α} is also a root $f_n(q)$. Then l_α is called the *root level* of α with respect to $f_n(q)$.

If l is the largest positive integer such that $l = l_\alpha$ for some roots α of $f_n(q)$, then such roots α are called *roots with highest level* of $f_n(q)$.

Let m be any element of $\mathcal{A} - \{1\}$. If α is a root of some polynomial $g(q)$, then let $\|\alpha\|_{g(q)}$ be the collection of all roots β (not necessarily distinct) with multiplicity of $g(q)$ such that $\beta^{a^i} = \alpha^{a^j}$ for some nonnegative integers i, j . Let $\text{Card}(\|\alpha\|_{g(q)})$ be the number of elements in $\|\alpha\|_{g(q)}$. We call $\|\alpha\|_{g(q)}$ the root class of α with respect to $g(q)$. It is clear that being in a root class of $g(q)$ is an equivalence relation on the set of roots, with multiplicity, of $g(q)$. If α_1 and α_2 are two roots of $f_m(q)$, then two sets $\|\alpha_1\|_{f_m(q)}$ and $\|\alpha_2\|_{f_m(q)}$ are said to be inequivalent if

$$\|\alpha_1\|_{f_m(q)} \cap \|\alpha_2\|_{f_m(q)} = \emptyset.$$

Let m and n be any two elements of $\mathcal{A} - \{1\}$. Let i_m and i_n be the index powers with respect to a of m and n respectively, i.e., the nonnegative integers such that $m = a^{i_m}$ and $n = a^{i_n}$. Then $i_m \neq i_n$ with $i_m > 1$ and $i_n > 1$ since \mathcal{A} is strict semi-cyclic. Let $f_m(q)$ and $f_n(q)$ be the elements of Γ indexed by m and n . Then Functional Equation (1) takes the form

$$f_{a^{i_m}}(q)f_{a^{i_n}}(q^{a^{i_m}}) = f_m(q)f_n(q^m) = f_n(q)f_m(q^n) = f_{a^{i_n}}(q)f_{a^{i_m}}(q^{a^{i_n}}). \quad (11)$$

Let α (resp. β) be a root of $f_m(q)$ (resp. $f_n(q)$) and let $\|\alpha\|_{f_m(q)}$ (resp. $\|\beta\|_{f_n(q)}$) be its root class with respect to $f_m(q)$ (resp. $f_n(q)$). Let $\{\|\alpha_s\|_{f_m(q)}\}_s$ (resp. $\{\|\beta_t\|_{f_n(q)}\}_t$) be the collection of all root (equivalence) classes of $f_m(q)$ (resp. $f_n(q)$).

Let $f_{\alpha, f_m(q)}(q)$ (resp. $f_{\beta, f_n(q)}(q)$) be the polynomial whose roots, with the same multiplicity, are exactly the elements of $\|\alpha\|_{f_m(q)}$ (resp. $\|\beta\|_{f_n(q)}$). We call this the *root class polynomial* associated to $(\alpha, f_m(q))$ (resp. $(\beta, f_n(q))$).

REMARK 3. $f_{\alpha, f_m(q)}(q)$ (resp. $f_{\beta, f_n(q)}(q)$) divides $f_m(q)$ (resp. $f_n(q)$) in $\bar{K}[q]$ and $\frac{f_m(q)}{f_{\alpha, f_m(q)}(q)}$ (resp. $\frac{f_n(q)}{f_{\beta, f_n(q)}(q)}$) has no root in $\|\alpha\|_{f_m(q)}$ resp. $\|\beta\|_{f_n(q)}$.

PROPOSITION 1.

- 1) Let μ be an element of $\|\alpha\|_{f_m(q)}$. There is a unique root class $\|\alpha'\|_{f_m(q^{a^{i_n}})}$ such that for every element ν of $\|\alpha'\|_{f_m(q^{a^{i_n}})}$ there exists nonnegative integers i and j such that $\mu^{a^i} = \nu^{a^j}$. Also,

$$\text{Card}(\|\alpha\|_{f_m(q)}) < \text{Card}(\|\alpha'\|_{f_m(q^{a^{i_n}})}).$$

CLASSIFICATION OF SOLUTIONS WITH CYCLIC AND SEMI-CYCLIC SUPPORTS

- 2) Let μ be an element of $\|\beta\|_{f_n(q)}$. There is a unique root class $\|\beta'\|_{f_n(q^{a^{im}})}$ such that for every element ν of $\|\alpha'\|_{f_n(q^{a^{im}})}$ there exist nonnegative integers i and j such that $\mu^{a^i} = \nu^{a^j}$. Also,

$$\text{Card}(\|\beta\|_{f_m(q)}) < \text{Card}(\|\beta'\|_{f_m(q^{a^{in}})}).$$

- 3) For each $\|\alpha_s\|_{f_m(q)}$ in the set $\{\|\alpha_s\|_{f_m(q)}\}_s$, there is a unique $\|\beta_{t_s}\|_{f_n(q)}$ in the set $\{\|\beta_t\|_{f_n(q)}\}_t$ such that: For any γ in $\|\alpha_s\|_{f_m(q)}$ and any δ in $\|\beta_{t_s}\|_{f_m(q)}$, there exist nonnegative integers i and j such that $\gamma^{a^i} = \delta^{a^j}$. Similarly, for each $\|\beta_t\|_{f_n(q)}$ in $\{\|\beta_t\|_{f_n(q)}\}_t$, there is a unique $\|\alpha_{s_t}\|_{f_m(q)}$ in $\{\|\alpha_s\|_{f_m(q)}\}_s$ such that: For any γ in $\|\beta_t\|_{f_n(q)}$ and any δ in $\|\alpha_{s_t}\|_{f_m(q)}$, there exist nonnegative integers i and j such that $\gamma^{a^i} = \delta^{a^j}$.

Proof. 1) and 2) follow immediately from the definition of root classes, the equivalence classes they define, and the fact that if α (resp. β) is a root of $f_m(q)$ (resp. $f_n(q)$), then $\alpha' = \alpha^{\frac{1}{a^{in}}}$ (resp. $\beta' = \beta^{\frac{1}{a^{im}}}$) is a root of $f_m(q^{a^{in}})$ (resp. $f_n(q^{a^{im}})$) with the required properties.

- 3) Let $\|\alpha_s\|_{f_m(q)}$ be an element of $\{\|\alpha_s\|_{f_m(q)}\}_s$. By (1),

$$\text{Card}(\|\alpha_s\|_{f_m(q)}) < \text{Card}(\|\alpha_s^{\frac{1}{a^{in}}}\|_{f_m(q^{a^{in}})}). \quad (12)$$

Let $f_{\alpha_s, f_m(q)}(q)$ and $f_{\alpha_s^{\frac{1}{a^{in}}, f_m(q^{a^{in}})}}(q)$ be the root class polynomials associated to

$$(\alpha_s, f_m(q)) \quad \text{and} \quad (\alpha_s^{\frac{1}{a^{in}}, f_m(q^{a^{in}})}),$$

respectively. Then (11) gives:

$$\frac{f_m(q)}{f_{\alpha_s, f_m(q)}(q)} f_{\alpha_s, f_m(q)}(q) f_n(q^{a^{im}}) = f_n(q) \frac{f_m(q^{a^{in}})}{f_{\alpha_s^{\frac{1}{a^{in}}, f_m(q^{a^{in}})}}(q)} f_{\alpha_s^{\frac{1}{a^{in}}, f_m(q^{a^{in}})}}(q). \quad (13)$$

By (12) and (13), at least one root of $f_{\alpha_s^{\frac{1}{a^{in}}, f_m(q^{a^{in}})}}(q)$ must be a root of either $\frac{f_m(q)}{f_{\alpha_s, f_m(q)}(q)}$ or $f_n(q^{a^{im}})$. However, if the former occurs, then it can be deduced that there exists another root class $\|\alpha_{s^*}\|_{f_m(q)}$ in $\{\|\alpha_s\|_{f_m(q)}\}_s$ such that

$$\|\alpha_{s^*}\|_{f_m(q)} \neq \|\alpha_s\|_{f_m(q)}$$

but

$$\|\alpha_{s^*}\|_{f_m(q)} \cap \|\alpha_s\|_{f_m(q)} \neq \emptyset.$$

This is impossible. Thus the latter must occur. It can be verified that every root class of $f_n(q^{a^{im}})$ is of the form $\|\beta^{\frac{1}{a^{im}}}\|_{f_n(q^{a^{im}})}$, where β is a root of $f_n(q)$. Thus there exists a root class $\|\beta_{t_s}\|_{f_n(q)}$ of $f_n(q)$ in $\{\|\beta_t\|_{f_n(q)}\}_t$ with the required

property. Uniqueness of $\|\beta_{t_s}\|_{f_n(q)}$ follows readily since if $\|\beta'\|_{f_n(q)}$ is another element of $\{\|\beta_t\|_{f_n(q)}\}_t$ with the required property, then it can be deduced, via the root classes of $f_n(q^{a^{im}})$, that

$$\|\beta_{t_s}\|_{f_n(q)} \cap \|\beta'\|_{f_n(q)} \neq \emptyset,$$

which is impossible.

Let $\|\beta_t\|_{f_n(q)}$ be in $\{\|\beta_t\|_{f_n(q)}\}_t$. Then by symmetry there exists a unique $\|\alpha_{s_t}\|_{f_m(q)}$ in $\{\|\alpha_s\|_{f_m(q)}\}_s$ with the required property. \square

PROPOSITION 2. *The polynomials $f_{\alpha_s, f_m(q)}(q)$ and $f_{\beta_{t_s}, f_n(q)}(q)$ satisfy*

$$f_{\alpha_s, f_m(q)}(q)f_{\beta_{t_s}, f_n(q)}(q^{a^{im}}) = f_{\beta_{t_s}, f_n(q)}(q)f_{\alpha_s, f_m(q)}(q^{a^{in}}) \quad (14)$$

while the polynomials $f_{\beta_t, f_n(q)}(q)$ and $f_{\alpha_{s_t}, f_m(q)}(q)$ satisfy

$$f_{\beta_t, f_n(q)}(q)f_{\alpha_{s_t}, f_m(q)}(q^{a^{in}}) = f_{\alpha_{s_t}, f_m(q)}(q)f_{\beta_t, f_n(q)}(q^{a^{im}}). \quad (15)$$

Proof. By symmetry, we only need to prove (14). Let us suppose that (14) does not hold. That is:

$$f_{\alpha_s, f_m(q)}(q)f_{\beta_{t_s}, f_n(q)}(q^{a^{im}}) \neq f_{\beta_{t_s}, f_n(q)}(q)f_{\alpha_s, f_m(q)}(q^{a^{in}}). \quad (16)$$

Thus there must be a root of the LHS of (16) which is not a root of the RHS or vice versa. Suppose there exists a root ω of the LHS which is not a root of the RHS. There are two cases:

a) Suppose ω is a root of $f_{\alpha_s, f_m(q)}(q)$. The roots of $f_{\alpha_s, f_m(q)}(q)$ form exactly the root class $\|\alpha_s\|_{f_m(q)}$ in $\{\|\alpha_s\|_{f_m(q)}\}_s$ by the definitions of $\|\alpha_s\|_{f_m(q)}$ and $f_{\alpha_s, f_m(q)}(q)$. Thus ω is an element of $\|\alpha_s\|_{f_m(q)}$. By (11), ω is a root of $f_n(q)f_m(q^{a^{in}})$. If ω is a root of $f_n(q)$, then it follows from 3) of Proposition 1 that its root class with respect to $f_n(q)$ must be $\|\beta_{t_s}\|_{f_n(q)}$. By definition, $\|\beta_{t_s}\|_{f_n(q)}$ forms exactly the roots of $f_{\beta_{t_s}, f_n(q)}(q)$. Hence ω is one of its root and thus a root of the RHS of (16), which contradicts our assumption. Thus ω must be a root of $f_m(q^{a^{in}})$ instead. By 1) of Proposition 1 and its proof, $\|\alpha_s^{\frac{1}{a^{in}}}\|_{f_m(q^{a^{in}})}$ must be the root class of ω with respect to $f_m(q^{a^{in}})$.

By definition, the roots of $f_{\alpha_s, f_m(q)}(q^{a^{in}})$ form exactly $\|\alpha_s^{\frac{1}{a^{in}}}\|_{f_m(q^{a^{in}})}$. Hence ω is a root of $f_{\alpha_s, f_m(q)}(q^{a^{in}})$ and thus of the RHS of (16), which again contradicts our assumption. Thus (14) holds in this case.

b) Suppose ω is a root of $f_{\beta_{t_s}, f_n(q)}(q^{a^{im}})$. Thus ω is a root of $f_n(q^{a^{im}})$ by Remark 3. By 2) of Proposition 1, its root class with respect to $f_n(q^{a^{im}})$ must then be $\|\beta_{t_s}^{\frac{1}{a^{im}}}\|_{f_n(q^{a^{im}})}$ which consist of exactly all the roots of $f_{\beta_{t_s}, f_n(q)}(q^{a^{im}})$. By (11), ω is a root of $f_n(q)f_m(q^{a^{in}})$. If ω is a root of $f_n(q)$, then $\|\omega\|_{f_n(q)} = \|\beta_{t_s}\|_{f_n(q)}$. This means ω is a root of $f_{\beta_{t_s}, f_n(q)}(q)$, which contradicts our assumption. Thus ω is a root of $f_m(q^{a^{in}})$ and the corresponding root class must be of the form $\|\alpha^{\frac{1}{a^{in}}}\|_{f_m(q^{a^{in}})}$, where α is a root of $f_m(q)$. But then it follows from the assumption of (b) and (3) of Proposition 1 that

$$\|\alpha\|_{f_m(q)} = \|\alpha_s\|_{f_m(q)}.$$

Hence,

$$\|\alpha^{\frac{1}{a^{in}}}\|_{f_m(q^{a^{in}})} = \|\alpha_s^{\frac{1}{a^{in}}}\|_{f_m(q^{a^{in}})},$$

which consists of exactly the roots of $f_{\alpha_s, f_m(q)}(q^{a^{in}})$. Thus ω is a root of the RHS of (16), which contradicts our assumption. Therefore (14) holds in both cases, and by symmetry so does (15). \square

By Propositions 1 and 2, we may assume henceforth – for the purpose of proving Theorem 5 – that

$$\text{Card}(\{\|\alpha_s\|_{f_m(q)}\}_s) = 1 = \text{Card}(\{\|\beta_t\|_{f_n(q)}\}_t)$$

for any m and n in $\mathcal{A} - \{1\}$.

4. Proof of Existence

In this section, we prove the existence of the pair of monic polynomials $f(q)$ and $g(q)$ in 2) of Theorem 5. From this point forward, unless stated otherwise, let m and n be distinct numbers in $\mathcal{A} - \{1\}$ such that m is the smallest element of $\mathcal{A} - \{1\}$. Thus $m < n$ and $i_m < i_n$. Let us also choose n so that i_n is not a multiple of i_m . Such an n exists since \mathcal{A} is strictly semi-cyclic. Let \mathcal{N} denote the set of all such n . It can be verified that the nonempty collection

$$I_m = \{(i_m, i_n) \mid n \in \mathcal{N}\}, \quad (17)$$

where (i_m, i_n) denotes the greatest common divisor of i_m and i_n , has a trivial common factor since otherwise a raised to this nontrivial common factor would be the generator of \mathcal{A} instead of a .

Let $g(q)$ (resp. $g^*(q)$) be the polynomial such that its roots are either all roots of unity of highest order which are roots of $f_n(q)$ (resp. $f_m(q)$) with the same multiplicities if $\Gamma = \Gamma^{(2)}$ or all roots of highest level which are roots of $f_n(q)$ (reps. $f_m(q)$) with the same multiplicities if $\Gamma = \Gamma^{(1)}$. Let $\{\alpha_j \mid j \geq 1\}$

(resp. $\{\beta_j \mid j \geq 1\}$) be the collection of nonnegative integers with the following properties:

- 1) α_1 (resp. β_1) is the maximal nonnegative integer such that $s_1(q) = r_1(q^{a^{\alpha_1}})$ divides $g(q)$ (resp. $s_1^*(q) = r_1^*(q^{a^{\beta_1}})$ divides $g^*(q)$) in $\bar{K}[q]$ for some nontrivial polynomials $s_1(q)$ and $r_1(q)$ (resp. $s_1^*(q)$ and $r_1^*(q)$) and $g^{(1)}(q) = l^{(1)}(q^{a^{\alpha_1}})$ (resp. $g^{*(1)}(q) = l^{*(1)}(q^{a^{\beta_1}})$) be the polynomials $s_1(q) = r_1(q^{a^{\alpha_1}})$ (resp. $s_1^*(q) = r_1^*(q^{a^{\beta_1}})$) with maximal degrees;
- 2) α_j (resp. β_j) is the maximal nonnegative integer such that $s_j(q) = r_j(q^{a^{\alpha_j}}) \mid \frac{g(q)}{\prod_{1 \leq t \leq j-1} l^{(t)}(q^{a^{\alpha_t}})}$ (resp. $s_j^*(q) = r_j^*(q^{a^{\beta_j}}) \mid \frac{g^*(q)}{\prod_{1 \leq t \leq j-1} l^{*(t)}(q^{a^{\beta_t}})}$) in $\bar{K}[q]$ for some nontrivial polynomials $s_j(q) = r_j(q^{a^{\alpha_j}})$ (resp. $s_j^*(q) = r_j^*(q^{a^{\beta_j}})$) and $g^{(j)}(q) = l^{(j)}(q^{a^{\alpha_j}})$ (resp. $g^{*(j)}(q) = l^{*(j)}(q^{a^{\beta_j}})$) be the polynomials $s_j(q) = r_j(q^{a^{\alpha_j}})$ (resp. $s_j^*(q) = r_j^*(q^{a^{\beta_j}})$) with maximal degrees.

LEMMA 1. *Let $g(q)$ and $g^*(q)$ be the polynomials defined above. Then:*

- 1) $g(q)T^{(n)}(q) = f_n(q) = f_{a^{i_n}}(q)$ and $g^*(q)T^{(m)}(q) = f_m(q) = f_{a^{i_m}}(q)$ for some polynomials $T^{(n)}(q)$ and $T^{(m)}(q)$ in $\bar{K}[q]$,
- 2) $g(q) = \prod_{j \geq 1} g^{(j)}(q) = \prod_{j \geq 1} l^{(j)}(q^{a^{\alpha_j}})$,
- 3) $g^*(q) = \prod_{j \geq 1} g^{*(j)}(q) = \prod_{j \geq 1} l^{*(j)}(q^{a^{\beta_j}})$.

Proof. These follow immediately from the definitions of $g(q)$ and $g^*(q)$. \square

Let $g_1(q) = \prod_{j \geq 1} g_1^{(j)}(q) = \prod_{j \geq 1} l_1^{(j)}(q^{a^{\alpha_{j1}}})$ and $g_1^*(q) = \prod_{j \geq 1} g_1^{*(j)}(q) = \prod_{j \geq 1} l_1^{*(j)}(q^{a^{\beta_{j1}}})$

denote

$$g(q) = \prod_{j \geq 1} g^{(j)}(q) = \prod_{j \geq 1} l^{(j)}(q^{a^{\alpha_j}}) \quad \text{and} \quad g^*(q) = \prod_{j \geq 1} g^{*(j)}(q) = \prod_{j \geq 1} l^{*(j)}(q^{a^{\beta_j}}),$$

respectively. Then we can iterate the above process:

- 1) if $\frac{f_{a^{i_n}}(q)}{\prod_{1 \leq s \leq i-1} g_s(q)} \neq 1$, then let

$$\frac{f_{a^{i_n}}(q)}{\prod_{1 \leq s \leq i-1} g_s(q)} \quad \text{and} \quad g_i(q) = \prod_{j \geq 1} g_i^{(j)}(q) = \prod_{j \geq 1} l_i^{(j)}(q^{a^{\alpha_{ji}}})$$

plays the role of

$$f_{a^{i_n}}(q) \quad \text{and} \quad g_1(q) = \prod_{j \geq 1} g_1^{(j)}(q) = \prod_{j \geq 1} l_1^{(j)}(q^{a^{\alpha_{j1}}}),$$

respectively as above;

- 2) $g_i(q)T_i^{(n)}(q) = \frac{f_{a^{i_n}}(q)}{\prod_{1 \leq s \leq i-1} g_s(q)}$ for some polynomial $T_i^{(n)}(q)$ in $\bar{K}[q]$;

3) if $\frac{f_{a^{i_m}}(q)}{\prod_{1 \leq s \leq i-1} g_s^*(q)} \neq 1$, then let

$$\frac{f_{a^{i_m}}(q)}{\prod_{1 \leq s \leq i-1} g_s^*(q)} \quad \text{and} \quad g_i^*(q) = \prod_{j \geq 1} g_i^{*(j)}(q) = \prod_{j \geq 1} l_i^{*(j)}(q^{a^{\beta j i}})$$

plays the role of

$$f_{a^{i_m}}(q) \quad \text{and} \quad g_1^*(q) = \prod_{j \geq 1} g_1^{*(j)}(q) = \prod_{j \geq 1} l_1^{*(j)}(q^{a^{\beta j 1}}),$$

respectively as above;

4) $g_i^*(q) T_i^{*(m)}(q) = \frac{f_{a^{i_m}}(q)}{\prod_{1 \leq s \leq i-1} g_s^*(q)}$ for some polynomial $T_i^{*(m)}(q)$ in $\bar{K}[q]$

to obtain a sequence of polynomials

$$g_i(q) = \prod_{j \geq 1} g_i^{(j)}(q) = \prod_{j \geq 1} l_i^{(j)}(q^{a^{\alpha j i}}) \quad \text{and} \quad g_i^*(q) = \prod_{j \geq 1} g_i^{*(j)}(q) = \prod_{j \geq 1} l_i^{*(j)}(q^{a^{\beta j i}})$$

for $i \geq 1$ such that

$$f_m(q) = \prod_{i \geq 1} g_i^*(q) = \prod_{i \geq 1} \prod_{j \geq 1} l_i^{*(j)}(q^{a^{\beta j i}}); \quad f_n(q) = \prod_{i \geq 1} g_i(q) = \prod_{i \geq 1} \prod_{j \geq 1} l_i^{(j)}(q^{a^{\alpha j i}}).$$

By re-indexing the polynomials so that their roots are in descending order (18) as order of roots of unity if $\Gamma = \Gamma^{(2)}$ or as level of roots if $\Gamma = \Gamma^{(1)}$, we can write the products in (18) as

$$\prod_{i \geq 1} \prod_{j \geq 1} l_i^{*(j)}(q^{a^{\beta j i}}) = \prod_{i \geq 1} l_i^*(q^{a^{\beta i}}) \quad \text{and} \quad \prod_{i \geq 1} \prod_{j \geq 1} l_i^{(j)}(q^{a^{\alpha j i}}) = \prod_{i \geq 1} l_i(q^{a^{\alpha i}}). \quad (19)$$

PROPOSITION 3. *Let $l_1(q)$, $l_1^*(q)$, α_1 and β_1 be as above. Then $l_1(q)$ and $l_1^*(q)$ are nontrivial polynomials, $\alpha_1 > \beta_1$, $\alpha_1 \geq i_n - i_m$ and*

$$l_1(q) = l_1^*(q). \quad (20)$$

Also, either

$$\frac{f_{a^{i_m}}(q)}{l_1^*(q^{a^{\beta_1}})} \quad \text{or} \quad \frac{f_{a^{i_n}}(q)}{l_1(q^{a^{\alpha_1}})}$$

is nontrivial.

Proof. From their definitions, $l_1(q)$ and $l_1^*(q)$ are nontrivial polynomials since Γ is a normalized solution. From (11) and (19), we have

$$\prod_{i \geq 1} l_i^*(q^{a^{\beta i}}) \prod_{i \geq 1} l_i(q^{a^{\alpha i + i_m}}) = \prod_{i \geq 1} l_i(q^{a^{\alpha i}}) \prod_{i \geq 1} l_i^*(q^{a^{\beta i + i_n}}). \quad (21)$$

If $\Gamma = \Gamma^{(2)}$, then it can be verified from the maximality of the orders of roots as roots of unity in the constructions of $l_i(q)$ and $l_i^*(q)$ together with Lemmas 3.12 and 3.15 of [7] that

$$\left(l_i(q^{a^{\alpha i}}, l_1(q^{a^{\alpha_1 + i_m}}) \right) = 1 \quad \text{and} \quad \left(l_1^*(q^{a^{\beta_1 + i_n}}, l_i^*(q^{a^{\beta i}}) \right) = 1 \quad (22)$$

in $\bar{K}[q]$ for $i \geq 1$.

Then

$$l_1\left(q^{a^{i_m+\alpha_1}}\right) = l_1^*\left(q^{a^{i_n+\beta_1}}\right) \quad \text{with} \quad \beta_1 + i_n = \alpha_1 + i_m > \alpha_1 \quad (23)$$

and thus (20) follows from the maximality of the orders of roots as roots of unity in the constructions of $l_i(q)$ and $l_i^*(q)$ and the maximality of in the definitions of α_1 and β_1 . If $\Gamma = \Gamma^{(1)}$, then (22) can be similarly deduced from the constructions of $l_i(q)$ and $l_i^*(q)$ and a simple argument using complex modulus of roots in $\bar{K}[q]$ and thus (23) and (20) also follow in this case. Therefore, $\alpha_1 > \beta_1$ and $\alpha_1 \geq i_n - i_m$ since $i_n > i_m$.

If both $\frac{f_{a^{i_m}}(q)}{l_1^*(q^{a^{\beta_1}})}$ and $\frac{f_{a^{i_n}}(q)}{l_1(q^{a^{\alpha_1}})}$ are trivial, then (23) means (21) can be written as

$$l_1^*\left(q^{a^{\beta_1}}\right) = l_1\left(q^{a^{\alpha_1}}\right)$$

which is impossible by (23) and the definitions of $l_1^*(q)$ and $l_1(q)$ since $\alpha_1 > \beta_1$. \square

For a polynomial of the form $l_j(q^{a^{\alpha_j+s i_m}})$ for some integer s (resp. $l_j^*(q^{a^{\beta_j+t i_n}})$ for some integer t) in (21), we call the polynomial $l_j(q)$ (resp. $l_j^*(q)$) its **base polynomial** with respect to n (resp. m). We say that the polynomials of the forms $l_j(q^{a^{\alpha_j}})$ and $l_j(q^{a^{\alpha_j+s i_m}})$ (resp. $l_j^*(q^{a^{\beta_j}})$ and $l_j^*(q^{a^{\beta_j+t i_n}})$) are **related polynomials** with respect to n (resp. m). If $s = 1$ (resp. $t = 1$), we say that $l_j(q^{a^{\alpha_j}})$ and $l_j(q^{a^{\alpha_j+c i_m}})$ (resp. $l_j^*(q^{a^{\beta_j}})$ and $l_j^*(q^{a^{\beta_j+d i_n}})$) are **directly related polynomials**. A base polynomial $l_j(q)$ (resp. $l_j^*(q)$) of $l_j(q^{a^{\alpha_j+s i_m}})$ (resp. $l_j^*(q^{a^{\beta_j+t i_n}})$) in (21) is said to be a **minimal base polynomial** with respect to n (resp. m) if $l_j(q)$ is not nontrivially divisible, in $\bar{K}[q]$, by any base polynomial $l_i(q)$ (resp. $l_i^*(q)$) of any polynomial of the form $l_i(q^{a^{\alpha_i}})$ (resp. $l_i^*(q^{a^{\beta_i}})$) appearing in (21).

Let $h_1(q) = l_1(q)$ and $h_1^*(q) = l_1^*(q)$. Then

$$\prod_{i>1} l_i^*\left(q^{a^{\beta_i}}\right) h_1^*\left(q^{a^{\beta_1}}\right) \prod_{i>1} l_i\left(q^{a^{\alpha_i+i_m}}\right) = h_1\left(q^{a^{\alpha_1}}\right) \prod_{i>1} l_i\left(q^{a^{\alpha_i}}\right) \prod_{i>1} l_i^*\left(q^{a^{\beta_i+i_n}}\right). \quad (24)$$

follows from (21) and (23). Equation (24) is called the 1st-iteration of (21).

PROPOSITION 4. *One of the following equations is necessarily true for $l_2(q)$ and $l_2^*(q)$:*

$$l_2\left(q^{a^{\alpha_2+i_m}}\right) = l_2^*\left(q^{a^{\beta_2+i_n}}\right) \quad \text{with} \quad \beta_2 + i_n = \alpha_2 + i_m > \alpha_1, \quad (25)$$

$$l_2\left(q^{a^{\alpha_2+i_m}}\right) = l_2^*\left(q^{a^{\beta_2+i_n}}\right) l_1\left(q^{a^{\alpha_1}}\right) \quad \text{with} \quad \beta_2 + i_n = \alpha_1 \leq \alpha_2 + i_m, \text{ or} \quad (26)$$

$$l_2\left(q^{a^{\alpha_2+i_m}}\right) = l_1\left(q^{a^{\alpha_1}}\right) \quad \text{with} \quad \beta_2 + i_n < \alpha_2 + i_m = \alpha_1. \quad (27)$$

PROOF. From Proposition 3, either $l_2(q)$ or $l_2^*(q)$ is nontrivial. It is straightforward then to verify from the maximality in the definitions of $l_i(q)$, $l_i^*(q)$, α_i , β_i , Proposition 3 and its proof that (25), (26) and (27) follow from equating the roots which are roots of unity of highest order if $\Gamma = \Gamma^{(2)}$ or roots of highest level if $\Gamma = \Gamma^{(1)}$ in the 1th-iteration of (21). \square

CLASSIFICATION OF SOLUTIONS WITH CYCLIC AND SEMI-CYCLIC SUPPORTS

From Proposition 4, if (25) occurs, let

$$h_2(q) = h_2^*(q) = l_2^*(q) = l_2(q).$$

and the 1th-iteration of (21) can be written as

$$\prod_{i>2} l_i^*(q^{a^{\beta_i}}) h_1^*(q^{a^{\beta_1}}) h_2^*(q^{a^{\beta_2}}) \prod_{i>2} l_i(q^{a^{\alpha_i+i_m}}) = h_1(q^{a^{\alpha_1}}) h_2(q^{a^{\alpha_2}}) \prod_{i>2} l_i(q^{a^{\alpha_i}}) \prod_{i>2} l_i^*(q^{a^{\beta_i+i_n}}).$$

If (26) occurs, let

$$h_2(q) = l_2(q) \quad \text{and} \quad h_2^*(q) = l_2(q^{a^{(\alpha_2+i_m)-(\beta_2+i_n)}})$$

and the 1st-iteration of (21) can be written as

$$\prod_{i>2} l_i^*(q^{a^{\beta_i}}) h_1^*(q^{a^{\beta_1}}) \frac{h_2^*(q^{a^{\beta_2}})}{l_{j_2}(q^{a^{\alpha_{j_2}-i_n}})} \prod_{i>2} l_i(q^{a^{\alpha_i+i_m}}) = h_1(q^{a^{\alpha_1}}) h_2(q^{a^{\alpha_2}}) \prod_{i>2} l_i(q^{a^{\alpha_i}}) \frac{\prod_{i>2} l_i^*(q^{a^{\beta_i+i_n}})}{l_{j_2}(q^{a^{(\alpha_{j_2}-i_n)+i_n}})},$$

where $\alpha_{j_2} - i_n = \beta_2$, $l_{j_2}(q)$, and α_{j_2} denotes $l_1(q)$ and α_1 , respectively in this case. If (27) occurs, let

$$h_2(q) = h_1(q)$$

and the 1st-iteration of (21) can be written as

$$\prod_{i>1} l_i^*(q^{a^{\beta_i}}) h_1^*(q^{a^{\beta_1}}) \prod_{i>2} l_i(q^{a^{\alpha_i+i_m}}) = h_2(q^{a^{\alpha_2}}) \prod_{i>2} l_i(q^{a^{\alpha_i}}) \prod_{i>1} l_i^*(q^{a^{\beta_i+i_n}}),$$

which we call the 2^{nd} -iteration of (21).

This process can be iterated to rewrite (24). To do this, first we have:

PROPOSITION 5. *For $i, j \geq 1k$ integers, one of the following equations is true:*

$$l_i(q^{a^{\alpha_i+i_m}}) = l_j^*(q^{a^{\beta_j+i_n}}) \tag{28}$$

with $\alpha_i + i_m = \beta_j + i_n$,

$$l_i(q^{a^{\alpha_i+i_m}}) = l_{j_i}(q^{a^{\alpha_{j_i}}}) l_j^*(q^{a^{\beta_j+i_n}}) \quad \text{or} \quad l_j(q^{a^{\alpha_j+i_m}}) l_{j_i}^*(q^{a^{\beta_{j_i}}}) = l_i^*(q^{a^{\beta_i+i_n}}) \tag{29}$$

with $\beta_j + i_n = \alpha_{j_i} \leq \alpha_i + i_m$ or $\alpha_j + i_m = \beta_{j_i} \leq \beta_i + i_n$, respectively,

$$l_j(q^{a^{\alpha_j}}) = l_i(q^{a^{\alpha_i+i_n}}) \quad \text{or} \quad l_i^*(q^{a^{\beta_i+i_m}}) = l_j^*(q^{a^{\beta_j}}) \tag{30}$$

with $\alpha_j = \beta_i + i_n$ or $\alpha_i + i_m = \beta_j$, respectively, or

$$l_i(q^{a^{\alpha_i}}) = l_j^*(q^{a^{\beta_j}}) \tag{31}$$

with $\alpha_i = \beta_j$.

Proof. As in the proof of Proposition 4, it follows from the maximality in the definitions of $l_i(q)$, $l_i^*(q)$, α_i , β_i , Propositions 3, 4 and their proofs that (28), (29), (30), and (31) follow from equating the roots which are roots of unity of highest order if $\Gamma = \Gamma^{(2)}$ or roots of highest level if $\Gamma = \Gamma^{(1)}$ in the $i - 1$ th-iteration of (21). \square

If (28) occurs, then let

$$h_i(q) = l_i(q) = l_j^*(q) = h_j^*(q). \quad (32)$$

If (29), then let

$$h_i(q) = l_i(q) \quad \text{and} \quad h_j^*(q) = l_j \left(q^{a^{(\alpha_i + i_m) - (\beta_j + i_n)}} \right) \quad (33)$$

or

$$h_i^*(q) = l_i^*(q) \quad \text{and} \quad h_j(q) = l_j^* \left(q^{a^{(\beta_i + i_n) - (\alpha_j + i_m)}} \right),$$

respectively. If (30), then let

$$h_i^*(q) = h_{u_i}(q) \quad \text{or} \quad h_i(q) = h_{u_i}^*(q), \quad (34)$$

respectively. Then substitute these functions into the $i - 1$ th-iteration of (21) and cancel the expression on LHS (resp. RHS) of each equation in (28), (29), (30) or (31) from the LHS (resp. RHS) of the $i - 1$ th-iteration of (21) to obtain the the i th-iteration of (21).

Since

$$\deg \left(\frac{f_n(q)}{\prod_{1 \leq j \leq i-1} l_j(q^{a^{\alpha_j}})} \right) \quad \text{and} \quad \deg \left(\frac{f_m(q)}{\prod_{1 \leq j \leq i-1} l_j^*(q^{a^{\beta_j}})} \right)$$

are decreasing as i increasing, it follows that there exist positive integers j_m and j_n such that

$$\frac{f_n(q)}{\prod_{1 \leq j \leq j_n} l_j(q^{a^{\alpha_j}})} = 1 \quad (35)$$

and

$$\frac{f_m(q)}{\prod_{1 \leq j \leq j_m} l_j^*(q^{a^{\beta_j}})} = 1. \quad (36)$$

Also, if (29) occurs for at least one $i \geq 2$, let

$$L_n(q) = \prod_{j_i} \hat{l}_{j_i}^* \left(q^{a^{\beta_{j_i} - i_m}} \right) = \prod_{j_i} \hat{l}_{j_i}^* \left(q^{a^{\alpha_i - i_m}} \right) \quad (37)$$

and

$$L_m^*(q) = \prod_{j_i} \hat{l}_{j_i} \left(q^{a^{\alpha_{j_i} - i_n}} \right) = \prod_{j_i} \hat{l}_{j_i} \left(q^{a^{\beta_i - i_n}} \right),$$

where

- $l_{j_i}(q)$ and $l_{j_i}^*(q)$ are the polynomials in (29);

CLASSIFICATION OF SOLUTIONS WITH CYCLIC AND SEMI-CYCLIC SUPPORTS

- $\hat{l}_{j_i}^*(q^{a^{\alpha_{j_i} - \overline{i_m}}})$ is the product of the polynomials of the form $l_{j_i}(q^{a^{\alpha_{j_i} - a_{it} i_m})}$ occurring in the denominator of the RHS of the above iterations for some integers a_{it} if at least one such polynomial is nontrivial and is trivial otherwise. This product can be rewritten as $\hat{l}_{j_i}^*(q^{a^{\alpha_i - \overline{i_m}}})$ which is the product of all the polynomials of the form $l_{j_i}^*(q^{a^{\alpha_i - b_{it} i_m})}$ occurring in the denominator of the RHS of the above iterations for some integers b_{it} if at least one such polynomial is nontrivial and is trivial otherwise;
- $\hat{l}_{j_i}(q^{a^{\alpha_{j_i} - \overline{i_n}}})$ is the product of all the polynomials of the form $l_{j_i}(q^{a^{\alpha_{j_i} - c_{it} i_n})}$ occurring in the denominator of the LHS of the above iterations for some integers c_{it} if at least one such polynomial is nontrivial and is trivial otherwise. This product can be rewritten as $\hat{l}_{j_i}(q^{a^{\beta_i - \overline{i_n}}})$ which is the products of all the polynomials of the form $l_{j_i}(q^{a^{\beta_i - d_{it} i_n})}$ occurring in the denominator of the LHS of the above iterations for some integers d_{it} if at least one such polynomial is nontrivial and is trivial otherwise.

Then it follows from (35), (36) and (37) that (11) can be rewritten as

$$\left(\frac{\prod_{1 \leq j \leq j_m} h_j^*(q^{a^{\beta_j}})}{L_m^*(q)} \right) \left(\frac{\prod_{1 \leq j \leq j_n} h_j(q^{a^{\alpha_j + i_m}})}{L_n(q^{a^{i_m}})} \right) = \left(\frac{\prod_{1 \leq j \leq j_n} h_j(q^{a^{\alpha_j}})}{L_n(q)} \right) \left(\frac{\prod_{1 \leq j \leq j_m} h_j^*(q^{a^{\beta_j + i_n}})}{L_m^*(q^{a^{i_n}})} \right). \quad (38)$$

From the definition of $L_n(q)$ and $L_m^*(q)$, it can be checked that

$$\deg(L_m^*(q)) < \deg(f_m(q)) \quad \text{and} \quad \deg(L_n(q)) < \deg(f_n(q)). \quad (39)$$

Next, let us show that

$$\left(\prod_{1 \leq j \leq j_m} h_j^*(q^{a^{\beta_j}}) \right) \left(\prod_{1 \leq j \leq j_n} h_j(q^{a^{\alpha_j + i_m}}) \right) = \left(\prod_{1 \leq j \leq j_n} h_j(q^{a^{\alpha_j}}) \right) \left(\prod_{1 \leq j \leq j_m} h_j^*(q^{a^{\beta_j + i_n}}) \right) \quad (40)$$

and thus

$$L_m^*(q)L_n(q^{i_m}) = L_n(q)L_m^*(q^{i_n}) \quad (41)$$

by Remark 1.

Let o_1, o_2, \dots be the orders of roots (resp. level of roots) of $h_1(q), h_2(q), \dots$ as roots of unity (resp. as complex roots) if $\Gamma = \Gamma^{(2)}$ (resp. $\Gamma = \Gamma^{(1)}$). Similarly, let o_1^*, o_2^*, \dots be the orders of roots (resp. level of roots) of $h_1^*(q), h_2^*(q), \dots$ as roots of unity (resp. as complex roots) if $\Gamma = \Gamma^{(2)}$ (resp. $\Gamma = \Gamma^{(1)}$). From the maximality in the definitions of $h_i(q)$ and $h_i^*(q)$ above, it can be deduced that

LAN NGUYEN

$$o_1 > o_2 > \cdots \quad (42)$$

and

$$o_1^* > o_2^* > \cdots \quad (43)$$

By (23), (28) and (32), there is some positive integer $l \geq 1$ maximal such that

$$h_j(q^{a^{\alpha_j+i_m}}) = l_j(q^{a^{\alpha_j+i_m}}) = l_j^*(q^{a^{\beta_j+i_n}}) = h_j^*(q^{a^{\beta_j+i_n}})$$

for all $1 \leq j \leq l$ with $\beta_j + i_n = \alpha_j + i_m$.

If $j > l$, then it can be deduced from Proposition 5, (32)–(34) that one of the following occurs either

$$h_i(q^{a^{\alpha_i+i_m}}) = l_i(q^{a^{\alpha_i+i_m}}) = l_j^*(q^{a^{\beta_j+i_n}}) = h_j^*(q^{a^{\beta_j+i_n}})$$

or

$$h_j(q^{a^{\alpha_j+i_m}}) = l_j(q^{a^{\alpha_j+i_m}}) = l_i^*(q^{a^{\beta_i+i_n}}) = h_i^*(q^{a^{\beta_i+i_n}})$$

with $\alpha_i + i_m = \beta_j + i_n$ or $\alpha_j + i_m = \beta_i + i_n$ respectively; either

$$h_j(q^{a^{\alpha_j+i_m}}) = h_i^*(q^{a^{\beta_i}}) \neq l_i^*(q^{a^{\beta_i}}) = l_j(q^{a^{\alpha_j+i_m}})$$

or

$$h_j^*(q^{a^{\beta_j+i_n}}) = h_i(q^{a^{\alpha_i}}) \neq l_i(q^{a^{\alpha_i}}) = l_j^*(q^{a^{\beta_j+i_n}}) \quad (44)$$

with $\beta_{u_j} = \alpha_j + i_m$ or $\alpha_{u_j} = \beta_i + i_n$, respectively;

$$h_i^*(q^{a^{\beta_i}}) = l_i^*(q^{a^{\beta_i}}) = l_j(q^{a^{\alpha_j+i_m}}) = h_j(q^{a^{\alpha_j+i_m}})$$

and

$$h_i(q^{a^{\alpha_i}}) = l_i(q^{a^{\alpha_i}}) = l_j^*(q^{a^{\beta_j+i_n}}) = h_j^*(q^{a^{\beta_j+i_n}})$$

with $\beta_i = \alpha_j + i_m$ or $\alpha_i = \beta_i + i_n$, respectively.

PROPOSITION 6.

1) If (44) does not occur for any j , then the following statements hold:

1) For the fixed positive integer m , $i_m \mid j_m$ and for each positive integer $1 \leq g \leq \frac{j_m}{i_m}$,

$$*_s(q) = h_t^*(q)$$

for all positive integers $(g-1)i_m < s, t \leq gi_m$ and

$$f_m(q) = \prod_{1 \leq g \leq \frac{j_m}{i_m}} \prod_{1 \leq i \leq i_m} h_{(g-1)i_m+1}^*(q^{a^{\beta(g-1)i_m+1+i-1}}).$$

2) For each positive integer n in \mathcal{N} , $i_n \mid j_n$ and for each positive integer $1 \leq g \leq \frac{j_n}{i_n}$,

$$h_s(q) = h_t(q)$$

for all positive integers $(g-1)i_n < s, t \leq gi_n$ and

$$f_n(q) = \prod_{1 \leq g \leq \frac{j_n}{i_n}} \prod_{1 \leq i \leq i_n} h_{(g-1)i_n+1}(q^{a^{\alpha(g-1)i_n+1+i-1}}).$$

CLASSIFICATION OF SOLUTIONS WITH CYCLIC AND SEMI-CYCLIC SUPPORTS

3) $\frac{j_m}{i_m} = \frac{j_n}{i_n}$ and $\alpha_{(g-1)i_n+1} = \beta_{(g-1)i_m+1}$ for $1 \leq g \leq L_\Gamma$, where $L_\Gamma = \frac{j_m}{i_m} = \frac{j_n}{i_n}$.

II) If (44) occurs for at least one j , then

1) For the fixed positive integer m , $i_m \mid j_m$ and for each positive integer $1 \leq g \leq \frac{j_m}{i_m}$,

$$h_s^*(q) = h_t^*(q)$$

for all positive integers $(g-1)i_m < s, t \leq gi_m$ and

$$\left(\prod_{1 \leq j \leq j_m} h_j^*(q^{a^{\beta_j}}) \right) = \prod_{1 \leq g \leq \frac{j_m}{i_m}} \prod_{1 \leq i \leq i_m} h_{(g-1)i_m+1}^*(q^{a^{\beta_{(g-1)i_m+1}+i-1}}). \quad (45)$$

2) For each positive integer n in \mathcal{N} , $i_n \mid j_n$ and for each positive integer $1 \leq g \leq \frac{j_n}{i_n}$,

$$h_s(q) = h_t(q)$$

for all positive integers $(g-1)i_n < s, t \leq gi_n$ and

$$\left(\prod_{1 \leq j \leq j_n} h_j(q^{a^{\alpha_j}}) \right) = \prod_{1 \leq g \leq \frac{j_n}{i_n}} \prod_{1 \leq i \leq i_n} h_{(g-1)i_n+1}(q^{a^{\alpha_{(g-1)i_n+1}+i-1}}). \quad (46)$$

3) $\frac{j_m}{i_m} = \frac{j_n}{i_n}$ and $\alpha_{(g-1)i_n+1} = \beta_{(g-1)i_m+1}$ for $1 \leq g \leq L_\Gamma$, where $L_\Gamma = \frac{j_m}{i_m} = \frac{j_n}{i_n}$.

PROOF. As shown before in Proposition 3, (29) does not occur at $i = 1$. The proof is divided into two parts depending on whether (29) occurs for some $i \geq 2$ (and thus (44) occurs at some $j > i$). For $i = 1$, let us cancel the quantities on the LHS and the RHS of (28) from the LHS and the RHS of (21), respectively. Then we continue by iterating this process where the quantities on the LHS and the RHS of (28), (29), (30) or (31) are cancelled from the LHS and the RHS of the $i - 1$ th-iteration of (21), respectively, to obtain the i th-iteration of (21).

For $i \geq 1$ and $j \geq 1$ for which (28) occurs, if we cancel the factors

$$l_i(q^{a^{\alpha_i+i_m}}) = l_j^*(q^{a^{\beta_j+i_n}}) \quad (47)$$

from the LHS and the RHS of (21), respectively, and if this cancelation is the only action taken, then we obtain a new equation with the directly related (same indexes) factors $l_j^*(q^{a^{\beta_j}})$ and $l_i(q^{a^{\alpha_i}})$ still remaining in the LHS and the RHS of (21), respectively.

For $i, j \geq 1$ such that (29) occurs,

$$l_i(q^{a^{\alpha_i+i_m}}) = l_{j_i}(q^{a^{\alpha_{j_i}}}) l_{j_i}^*(q^{a^{\beta_{j_i}+i_n}}) \quad \text{or} \quad l_j(q^{a^{\alpha_j+i_m}}) l_{j_i}^*(q^{a^{\beta_{j_i}}}) = l_i^*(q^{a^{\beta_i+i_n}}) \quad (48)$$

with $\beta_j + i_n = \alpha_{j_i} \leq \alpha_i + i_m$ for some j_i such that $l_{j_i}(q^{a^{\alpha_{j_i}}})$ is still left in the RHS, respectively, of (21) or $\alpha_j + i_m = \beta_{j_i} \leq \beta_i + i_n$ for some j_i such that $l_{j_i}^*(q^{a^{\beta_{j_i}}})$ is still left in the LHS of (21) respectively after cancelation is performed at the previous iteration of this process. Then $l_i^*(q) \neq l_j(q)$ and $l_{j_i}(q) \neq l_j(q)$ or $l_j(q) \neq l_i^*(q)$

and $l_{j_i}^*(q) \neq l_i^*(q)$ for such i, j and j_i since they are all nontrivial polynomials. If we cancel the factors in (48), whichever occurs, from the LHS and the RHS of (21), respectively and if this cancelation is the only action taken, then we obtain a new equation with the directly related polynomials $l_i(q^{a^{\alpha_i}})$, $l_{j_i}(q^{a^{\alpha_{j_i} + i_m}})$ and $l_j^*(q^{a^{\beta_j}})$ or the directly related polynomials $l_j(q^{a^{\alpha_j}})$, $l_{j_i}^*(q^{a^{\beta_{j_i} + i_n}})$ and $l_i^*(q^{a^{\beta_i}})$, respectively still remaining in (21). Equation (48) also implies that the polynomials involved must not have all equal corresponding base polynomials.

For $i, j \geq 1$ for which (30) occurs, if we cancel the factors

$$l_i(q^{a^{\alpha_i + i_m}}) = l_j(q^{a^{\alpha_j}}) \quad \text{or} \quad l_j^*(q^{a^{\beta_j}}) = l_i^*(q^{a^{\beta_i + i_n}}), \quad (49)$$

whichever occurs, from the LHS and the RHS of (21), respectively, and if this cancelation is the only action taken, then we obtain a new equation with the directly related polynomials $l_i(q^{a^{\alpha_i}})$ and $l_j(q^{a^{\alpha_j + i_m}})$ or the directly related polynomials $l_i^*(q^{a^{\beta_i}})$ and $l_j^*(q^{a^{\beta_j + i_n}})$ still remaining in this equation respectively.

For $i > 1$ and $j > 1$ such that (31) occurs, if we cancel the factors

$$l_i^*(q^{a^{\beta_i}}) = l_j(q^{a^{\alpha_j}}), \quad (50)$$

from the LHS and the RHS of (21), respectively, and if this cancelation is the only action taken, then we obtain a new equation with the directly related polynomials $l_i^*(q^{a^{\beta_i + i_n}})$ and $l_j(q^{a^{\alpha_j + i_m}})$ still remaining in this equation respectively.

Now let us use (28)–(31) and the cancelation procedure similar to the one used in (47)–(50) in the following process, starting at $i = t_0$ and $j = t_1$ for some t_0 and t_1 , in which step by step we cancel from both sides of (21) polynomials (or factors of polynomials) and their related polynomials (or factors of related polynomials) involved in the cancelation starting at $i = t_0$ and $j = t_1$.

Suppose that $l_{t_0}^*(q)$ is the base polynomial of some polynomial $l_{t_0}^*(q^{a^{\beta_{t_0}}})$ which appears in (21). Let us choose t_0 so that $h_{t_0}^*(q)$ is also a minimal base polynomial with respect to $f_m(q)$ if (44) occurs at some i . Then it follows that t_0 must take on one of the following possibilities:

- 1) t_0 can be equal to j in (47);
- 2) t_0 can be equal to j in the first equation in (48) by the minimality condition;
- 3) t_0 can be equal to i in the second equation in (49);
- 4) t_0 can be equal to i in (50).

It can also be deduced from (21), the minimality of the base polynomial $l_{t_0}^*(q)$ with respect to $f_m(q)$ and the definitions of $l_j(q)$'s and $l_i^*(q)$'s that one of the followings is true for the polynomial $l_{t_0}^*(q^{a^{\beta_{t_0}}})$:

$$l_{t_0}^*(q^{a^{\beta_{t_0}}}) = l_{t_1}(q^{a^{\alpha_{t_1}}}) \quad (51)$$

for some t_1 with $\beta_{t_0} = \alpha_{t_1}$;

CLASSIFICATION OF SOLUTIONS WITH CYCLIC AND SEMI-CYCLIC SUPPORTS

$$l_{t_0}^*(q^{a^{\beta_{t_0}}}) = l_{t_1}^*(q^{a^{\beta_{t_1} + i_n}}) \quad (52)$$

for some t_1 with $\beta_{t_0} = \beta_{t_1} + i_n$;

or

$$l_{t_2}(q^{a^{\alpha_{t_2} + i_m}}) l_{t_0}^*(q^{a^{\beta_{t_0}}}) = l_{t_1}^*(q^{a^{\beta_{t_1} + i_n}}) = l_{t_0}^*(q^{a^{\beta_{t_0}}}) \frac{l_{t_1}^*(q^{a^{\beta_{t_1} + i_n}})}{l_{t_0}^*(q^{a^{\beta_{t_0}}})} \quad (53)$$

for some t_1 and t_2 with $\alpha_{t_2} + i_m = \beta_{t_0} \leq \beta_{t_1} + i_n$.

If (51) occurs, let us cancel $l_{t_0}^*(q^{a^{\beta_{t_0}}})$ and $l_{t_1}(q^{a^{\alpha_{t_1}}})$ from the LHS and the RHS of (21) respectively to obtain a new equation and move to consider the directly related polynomial $l_{t_1}(q^{a^{\alpha_{t_1} + i_m}})$ of $l_{t_1}(q^{a^{\alpha_{t_1}}})$ using (28)–(31) with $i = t_1$ and $j = t_2$:

1) If (28) occurs with $i = t_1$ and $j = t_2$, then

$$l_{t_1}(q^{a^{\alpha_{t_1} + i_m}}) = l_{t_2}^*(q^{a^{\beta_{t_2} + i_n}}).$$

Next we cancel $l_{t_1}(q^{a^{\alpha_{t_1} + i_m}})$ and $l_{t_2}^*(q^{a^{\beta_{t_2} + i_n}})$ from the LHS and the RHS of (21), respectively. It follows that

$$\beta_{t_2} = \beta_{t_0} + (i_m - i_n) \quad (54)$$

since $\beta_{t_2} + i_n = \alpha_{t_1} + i_m$ and $\beta_{t_0} = \alpha_{t_1}$. Next we move to consider the directly related polynomials $l_{t_2}^*(q^{a^{\beta_{t_2}}})$ of $l_{t_2}^*(q^{a^{\beta_{t_2} + i_n}})$ and $l_{t_1}(q^{a^{\alpha_{t_1}}})$ of $l_{t_1}(q^{a^{\alpha_{t_1} + i_m}})$. Since the polynomial $l_{t_1}(q^{a^{\alpha_{t_1}}})$ is already canceled in a previous step, we just repeat this procedure, using (28)–(31), with $l_{t_2}^*(q^{a^{\beta_{t_2}}})$.

2) If (29) occurs, then it follows from the minimality of $h_{t_0}^*(q)$ with respect to $f_m(q)$ that

$$l_{t_1}(q^{a^{\alpha_{t_1} + i_m}}) l_{j_{t_2}}^*(q^{a^{\beta_{t_2}}}) = l_{t_2}^*(q^{a^{\beta_{t_2} + i_n}}) = l_{t_1}(q^{a^{\alpha_{t_1} + i_m}}) \frac{l_{t_2}^*(q^{a^{\beta_{t_2} + i_n}})}{l_{t_1}(q^{a^{\alpha_{t_1} + i_m}})}. \quad (55)$$

for some j_{t_2} . Next we cancel $h_{t_1}(q^{a^{\alpha_{t_1} + i_m}})$ from the LHS and the RHS of (55). Unlike (54), we have instead

$$\beta_2 \geq \beta_{t_0} + (i_m - i_n)$$

in this case since $\beta_{t_2} + i_n \geq \alpha_{t_1} + i_m$ and $\beta_{t_0} = \alpha_{t_1}$. Next we move to the directly related polynomial $l_{t_1}(q^{a^{\alpha_{t_1}}})$ of $l_{t_1}(q^{a^{\alpha_{t_1} + i_m}})$ and the directly related polynomial, a factor of $l_{t_2}^*(q^{a^{\beta_{t_2}}})$ of the form $l_{t_1, t_2}(q)$ with $l_{t_1, t_2}(q^{a^{i_n}}) = l_{t_1}(q^{a^{\alpha_{t_1} + i_m}})$, of the factor of $l_{t_2}^*(q^{a^{\beta_{t_2} + i_n}})$ equal to $l_{t_1}(q^{a^{\alpha_{t_1} + i_m}})$. Again since $l_{t_1}(q^{a^{\alpha_{t_1}}})$ is already canceled in a previous step, we repeat this procedure, using (28)–(31), with the factor $l_{t_1, t_2}(q)$ defined above of $l_{t_1}^*(q^{a^{\beta_{t_1}}})$. We also move at the same time to the directly related polynomial $l_k^*(q^{a^{\beta_k + i_n}})$ of $l_k^*(q^{a^{\beta_k}})$ and the directly related polynomial, a factor of $l_{t_2}^*(q^{a^{\beta_{t_2}}})$ of the form $l_{k, t_2}(q)$ with $l_{k, t_2}(q^{a^{i_n}}) = l_k^*(q^{a^{\beta_k}})$, of the factor

of $l_{t_2}^*(q^{a^{\beta t_2} + i_n})$ equal to $l_k^*(q^{a^{\beta k}}) = \frac{l_{t_2}^*(q^{a^{\beta t_2} + i_n})}{l_{t_1}(q^{a^{\alpha t_1} + i_m})}$. Then we repeat the procedure, using (28)–(31) with $h_k^*(q^{a^{\beta k} + i_n})$ and with $h_{k,t_2}(q)$.

3) If (30) occurs, then it follows that

$$l_{t_1}(q^{a^{\alpha t_1} + i_m}) = l_{t_2}(q^{a^{\alpha t_2}})$$

for some t_2 . Then we cancel $l_{t_1}(q^{a^{\alpha t_1} + i_m})$ and $l_{t_2}(q^{a^{\alpha t_2}})$ from the LHS and the RHS of (21), respectively. Next we move to consider again only the directly related polynomial $h_{t_2}(q^{a^{\alpha t_2} + i_m})$ of $l_{t_2}(q^{a^{\alpha t_2}})$ for the same reason as in 1) and 2) above. Now repeat the procedure in 1) and 2) above, with $l_{t_2}(q^{a^{\alpha t_2} + i_m})$ replacing $l_{t_1}(q^{a^{\alpha t_1} + i_m})$.

4) It is clear that (31) does not occur here.

This process stops when there are no directly related polynomials, which have not been canceled, to move to.

If (52) occurs, let us cancel $l_{t_0}^*(q^{a^{\beta t_0}})$ and $l_{t_1}^*(q^{a^{\beta t_1} + i_n})$ from the LHS and the RHS of (21) respectively to obtain a new equation and move to consider the related polynomial $l_{t_1}^*(q^{a^{\beta t_1}})$ of $l_{t_1}^*(q^{a^{\beta t_1} + i_n})$ using (28)–(31) with $i = t_1$:

1) (47) does not apply.

2) (48) does not apply.

3) (49) does not apply.

4) (50) is the only case that applies and thus must be the case that occurs. That is

$$l_{t_1}^*(q^{a^{\beta t_1}}) = l_{t_2}(q^{a^{\alpha t_2}}) \quad \text{for some } t_2.$$

We then cancel $l_{t_1}^*(q^{a^{\beta t_1}})$ and $l_{t_2}(q^{a^{\alpha t_2}})$ from the LHS and the RHS of (21), respectively. Next we move to consider the directly related polynomial $l_{t_2}(q^{a^{\alpha t_2} + i_m})$ of $l_{t_2}(q^{a^{\alpha t_2}})$. Now repeat the procedure in 1), 2), 3) and 4) above (in the case, where (51) occurs) with $l_{t_2}(q^{a^{\alpha t_2} + i_m})$ replacing $l_{t_1}(q^{a^{\alpha t_1} + i_m})$.

Again this process stops when there are no directly related polynomials to move to.

If (53) occurs, then the same process performed at (55) can be repeated. Even though the process proceeds in several directions in (55) and in this case, it stops in the same way as in the previous cases when there are no directly related polynomials which have not been canceled to move to in each of these directions.

Let us denote a polynomial of the form $l_i^*(q^{a^{\beta_i} + a_i i_n})$ for some nonnegative integer a_i or a factor of such a polynomial if (53) occurs (resp. $l_i(q^{a^{\alpha_i} + b_i i_m})$, for some nonnegative integer b_i , or a factor of such a polynomial if (53) occurs) which is canceled in the above process starting at $i = t_0$ by $l_i^*(q^{\widehat{a^{\beta_i} + a_i i_n}})$ (resp. $l_i(q^{\widehat{a^{\alpha_i} + b_i i_m}})$).

CLASSIFICATION OF SOLUTIONS WITH CYCLIC AND SEMI-CYCLIC SUPPORTS

In other words, $l_i^*(\widehat{q^{a\beta_i+a_i i_n}}) = l_i^*(q^{a\beta_i+a_i i_n})$ if $l_i^*(q^{a\beta_i+a_i i_n})$ is canceled in the above process and $l_i^*(q^{a\beta_i+b_i i_n})$ is equal to a factor of $l_i^*(q^{a\beta_i+a_i i_n})$ if this factor is the greatest factor of $l_i^*(q^{a\beta_i+a_i i_n})$ canceled in the above process (resp. $l_i(\widehat{q^{a\alpha_i+b_i i_m}}) = l_i(q^{a\alpha_i+b_i i_m})$, if $l_i(q^{a\alpha_i+b_i i_m})$ is canceled in the above process and $l_i(\widehat{q^{a\alpha_i+b_i i_m}})$ is equal to a factor of $l_i(q^{a\alpha_i+b_i i_m})$ if this factor is the greatest factor of $l_i(q^{a\alpha_i+b_i i_m})$ canceled in the above process). Let $U_m^{(t_0)} = \{i\}$ (resp. $V_n^{(t_0)} = \{i\}$) be the collection of indexes i such that a polynomial of the form $l_i^*(\widehat{q^{a\beta_i}})$ (resp. $l_i(\widehat{q^{a\alpha_i}})$) is canceled in the above process starting at $i = t_0$. Let

$$\Omega_{U_m^{(t_0)}} := \{l_i^*(\widehat{q^{a\beta_i}}) \mid i \in U_m^{(t_0)}\} \quad \text{and} \quad \Omega_{V_n^{(t_0)}} := \{l_i(\widehat{q^{a\alpha_i}}) \mid i \in V_n^{(t_0)}\}.$$

We call $\Omega_{U_m^{(t_0)}}$ and $\Omega_{V_n^{(t_0)}}$ (resp. $U_m^{(t_0)}$ and $V_n^{(t_0)}$) the **cycle** (resp. **cycle index**) of (38), at $i = t_0$, with respect to m and n , respectively. We call the pair of cycles $\Omega_{U_m^{(t_0)}}$ and $\Omega_{V_n^{(t_0)}}$ the pair of corresponding cycles, associated to t_0 , of $f_m(q)$ and $f_n(q)$. We refer to $|\Omega_{U_m^{(t_0)}}|$ and $|\Omega_{V_n^{(t_0)}}|$, the number of elements in $\Omega_{U_m^{(t_0)}}$ and $\Omega_{V_n^{(t_0)}}$, respectively, as their lengths.

There are two possible cases to be considered:

I) Suppose that (29) does not occur for any i and j when n ranges over \mathcal{N} , the collection of all n in $\mathcal{A} - \{1\}$ such that i_n is not a multiple of i_m defined before. This means in particular that (53) does not occur, and thus no minimality condition needs to be assumed on the base polynomial $l_{t_0}^*(q)$. It also means that

- 1) $l_i^*(\widehat{q^{a\beta_i}}) = l_i^*(q^{a\beta_i}) = h_i^*(q^{a\beta_i})$ and $l_i(\widehat{q^{a\alpha_i}}) = l_i(q^{a\alpha_i}) = h_i(q^{a\alpha_i})$ for each i ;
- 2) $L(q) = L^*(q) = 1$ and thus (38) becomes (40).

Thus we may start at $j = t_0$ where $o_{t_0}^*$ is smallest such that the second equation in (49) occurs. As a result, it can be noted from the above process that at every step, one polynomial is canceled from the LHS and one polynomial is canceled from the RHS of (40) and yet there is only one directly related polynomial to these polynomials which has not been canceled by the previous step. Thus the procedure only goes in one direction. Also, it can be verified that this cancellation process only ends when it has circled back to $j = t_0$. That is, when the factor $h_{t_0}^*(q^{a\beta_{t_0}+i_n})$ is canceled from the RHS of (40) so that the next directly related polynomial to be considered in the process is $h_{t_0}^*(q^{a\beta_{t_0}})$. It is clear that the base polynomials of all the polynomials which are canceled in this procedure are all equal. In particular, the base polynomials of all the polynomials with indexes contained in $U_m^{(t_0)}$ and $V_n^{(t_0)}$ are all equal.

By continuing with the above process until it ends in this case, it can be verified that the following statements hold:

LAN NGUYEN

- 1) For all β_i and β_j involved in this cancelation process, there exist integers a_{ij} and b_{ij} such that

$$\beta_i = \beta_j + a_{ij}i_m + b_{ij}i_n.$$

- 2) For all α_i and α_j involved in this cancelation process, there exist integers c_{ij} and d_{ij} such that

$$\alpha_i = \alpha_j + c_{ij}i_m + d_{ij}i_n.$$

- 3) For all α_i and β_j involved in this cancelation process, there exist integers e_{ij} and f_{ij} such that

$$\alpha_i = \beta_j + e_{ij}i_m + f_{ij}i_n.$$

Now, let us show that $i_m \mid j_m$ and $i_n \mid j_n$ where j_m and j_n are the integers in (40). It can be verified from the above process and from the fact that the cancelation process starts at $i = t_0$ and ends at the same place, there must be integers a_{t_0} and b_{t_0} such that

$$\beta_{t_0} + a_{t_0}i_m + b_{t_0}i_n = \beta_{t_0}.$$

Thus

$$a_{t_0}i_m + b_{t_0}i_n = 0.$$

Hence, there is some positive integer L_{t_0} such that

$$L_{t_0} \frac{i_n}{(i_m, i_n)} = |a_{t_0}|$$

and

$$L_{t_0} \frac{i_m}{(i_m, i_n)} = |b_{t_0}|,$$

and thus

$$i_m \mid L_{t_0} \frac{i_m}{(i_m, i_n)} i_n = \left(L_{t_0} \frac{i_n}{(i_m, i_n)} \right) i_m$$

and

$$i_n \mid L_{t_0} \frac{i_n}{(i_m, i_n)} i_m = \left(L_{t_0} \frac{i_m}{(i_m, i_n)} \right) i_n.$$

It can also be verified from the process above that

$$|\Omega_{U_m^{(t_0)}}| = |U_m^{(t_0)}| = |b_{t_0}|$$

and

$$|\Omega_{V_n^{(t_0)}}| = |V_n^{(t_0)}| = |a_{t_0}|.$$

From the iteration process and the fact that (29) does not occur, we obtain a collection of disjoint cycles $\Omega_{U_m^{(t_0)}} \dots, \Omega_{U_m^{(t_k)}}$ with respect to m and a collection of disjoint cycles $\Omega_{V_n^{(t_0)}} \dots, \Omega_{V_n^{(t_k)}}$ with respect to n such that

$$\bigcup_{1 \leq j \leq k} U_m^{(t_j)} = j_m$$

CLASSIFICATION OF SOLUTIONS WITH CYCLIC AND SEMI-CYCLIC SUPPORTS

and

$$\bigcup_{1 \leq j \leq k} V_n^{(t_j)} = j_n.$$

Also, for each $j = 1, \dots, k$, all polynomials in $\Omega_{U_m^{(t_j)}}$ and $\Omega_{V_n^{(t_j)}}$ have the same base polynomial. For each i , we call the pairs of cycles $\Omega_{U_m^{(t_i)}}$ and $\Omega_{V_n^{(t_i)}}$ the corresponding cycles, associated to t_i , of $f_m(q)$ and $f_n(q)$. For a similar reason as the case t_0 , there exists a positive integer L_{t_j} such that

$$\left| \Omega_{U_m^{(t_j)}} \right| = \left| U_m^{(t_j)} \right| = L_{t_j} \frac{i_m}{(i_m, i_n)}$$

and

$$\left| \Omega_{V_n^{(t_j)}} \right| = \left| V_n^{(t_j)} \right| = L_{t_j} \frac{i_n}{(i_m, i_n)},$$

and thus

$$i_m \left| L_{t_j} \frac{i_m}{(i_m, i_n)} i_n \right| = \left(L_{t_j} \frac{i_n}{(i_m, i_n)} \right) i_m$$

and

$$i_n \left| L_{t_j} \frac{i_n}{(i_m, i_n)} i_m \right| = \left(L_{t_j} \frac{i_m}{(i_m, i_n)} \right) i_n$$

for each $0 \leq j \leq k$. As a result, it follows that

$$j_m = \frac{\sum_{1 \leq j \leq k} L_{t_j} i_m}{(i_m, i_n)} i_m. \quad (56)$$

Similarly,

$$j_n = \frac{\sum_{1 \leq j \leq k} L_{t_j} i_n}{(i_m, i_n)} i_n. \quad (57)$$

Thus

$$\frac{\sum_{1 \leq j \leq k} L_{t_j} i_n}{(i_m, i_n)} i_n \quad (58)$$

is an integer for each n in \mathcal{N} , and the rational number

$$L := \frac{\sum_{1 \leq j \leq k} L_{t_j}}{(i_m, i_n)} \quad (59)$$

is independent of n in \mathcal{N} by (56). As a result, if L is not an integer, it can be verified from (57)–(59) that the set $I_m = \{(i_m, i_n) \mid n \in \mathcal{N}\}$ defined earlier must then have a nontrivial common factor, which contradicts the fact that a is the generator of \mathcal{A} (see (17)). Therefore, $i_m \mid j_m$ and $i_n \mid j_n$ by (56) and (57) respectively. We also have from (56) and (57) that

$$\frac{j_m}{j_n} = \frac{i_m}{i_n}.$$

Since we have chosen t_0 so that $o_{t_0}^* < o_i^*$ for all i , $t_0 = j_m$ by (43). It can then be verified from (42) and the fact (29) does not occur that

$$\beta_{t_0} = \beta_{j_m} = \alpha_{j_n}$$

and

$$h_{j_m}^* \left(q^{a^{\beta_{j_m}}} \right) = h_{j_n} \left(q^{a^{\alpha_{j_n}}} \right).$$

As a result, we can partition the collection of indexes $\{1, \dots, j_m\}$ and $\{1, \dots, j_n\}$ into disjoint subsets $J_{0,m}^{(n)}, \dots, J_{k,m}^{(n)}$ and $J_{0,n}^{(m)}, \dots, J_{l,n}^{(m)}$ with the following properties:

- 1) $t_0 = j_m$ is contained in $J_{0,m}^{(n)}$ and j_n is contained in $J_{0,n}^{(m)}$.
- 2) i is in $J_{0,m}^{(n)}$ (resp. $J_{0,n}^{(m)}$) if and only if $\beta_i \leq \beta_{j_m} + i_m - 1$ (resp. $\alpha_i \leq \alpha_{j_n} + i_n - 1$).
- 3) i is in $J_{t,m}^{(n)}$ (resp. $J_{t,n}^{(m)}$) if and only if $\beta_{j_m} + t i_m \leq \beta_i < \beta_{t_0} + (t+1)i_m$ (resp. $\alpha_{j_n} + t(i_n) \leq \alpha_i < \alpha_{j_n} + (t+1)j_n$).

As a result, it can be verified from (40), the definitions of $h_i(q)$'s and $h_i^*(q)$'s and the fact (29) does not occur that

$$\prod_{i \in J_{0,m}^{(n)}} h_i^* \left(q^{a^{\beta_i}} \right) \prod_{i \in J_{0,n}^{(m)}} h_i \left(q^{a^{\alpha_i + i_m}} \right) = \prod_{i \in J_{0,m}^{(n)}} h_i \left(q^{a^{\alpha_i}} \right) \prod_{i \in J_{0,n}^{(m)}} h_i^* \left(q^{a^{\beta_i + i_n}} \right). \quad (60)$$

Thus $U_m^{(t_0)}$ and $V_n^{(t_0)}$ are contained in $J_{0,m}^{(n)}$ and $J_{0,n}^{(m)}$, respectively. Let the collection of disjoint cycles $\Omega_{U_m^{(t_0)}} \dots, \Omega_{U_m^{(t_{r_{m,n}})}}$ with respect to m (resp. the collection of disjoint cycles $\Omega_{V_n^{(t_0)}} \dots, \Omega_{V_n^{(t_{r_{m,n}})}}$ with respect to n) be all the cycles with indexes in $J_{0,m}^{(n)}$ (resp. $J_{0,n}^{(m)}$). From (60), every index in $J_{0,m}^{(n)}$ (resp. $J_{0,n}^{(m)}$) is included in exactly one of the sets $U_m^{(t_0)}, \dots, U_m^{(t_{r_{m,n}})}$ (resp. $V_n^{(t_0)}, \dots, V_n^{(t_{r_{m,n}})}$). Then it can be verified from 1)–3) above and (60) that

$$L_{t_j} = 1$$

for all $0 \leq j \leq r_{m,n}$ and thus

$$|J_{0,m}^{(n)}| = \sum_{1 \leq j \leq r_{m,n}} |\Omega_{U_m^{(t_j)}}| = \sum_{1 \leq j \leq r_{m,n}} L_{t_j} \frac{i_m}{(i_m, i_n)} = \sum_{1 \leq j \leq r_{m,n}} \frac{i_m}{(i_m, i_n)} = \frac{r_{m,n}}{(i_m, i_n)} i_m \quad (61)$$

and

$$|J_{0,n}^{(m)}| = \sum_{1 \leq j \leq r_{m,n}} |\Omega_{V_n^{(t_j)}}| = \sum_{1 \leq j \leq r_{m,n}} L_{t_j} \frac{i_n}{(i_m, i_n)} = \sum_{1 \leq j \leq r_{m,n}} \frac{i_n}{(i_m, i_n)} = \frac{r_{m,n}}{(i_m, i_n)} i_n.$$

Let us show that $r_{m,n} = (i_m, i_n)$ for all n in \mathcal{N} . From 1)–3) above,

$$r_{m,n} \leq (i_m, i_n) \quad (62)$$

for any n in \mathcal{N} since $|J_{0,n}^{(m)}| \leq i_m$. From (61), it follows that the number

$$\frac{r_{m,n}}{(i_m, i_n)} = \frac{U}{V}, \quad (63)$$

CLASSIFICATION OF SOLUTIONS WITH CYCLIC AND SEMI-CYCLIC SUPPORTS

where U and V are natural numbers such that $(U, V) = 1$, is independent of n since the left-hand side of (61) is independent of n . As a result, if $V \neq 1$, then all the elements of I_m have a nontrivial common factor V , which is a contradiction. Thus $V = 1$ and

$$r_{m,n} = (i_m, i_n).$$

Thus

$$|J_{0,m}^{(n)}| = i_m, \quad |J_{0,n}^{(m)}| = i_n$$

and (60) becomes

$$\prod_{1 \leq i \leq i_m} h_{j_m}^* \left(q^{a^{\beta_{j_m} + i - 1}} \right) \prod_{1 \leq i \leq i_n} h_{j_n} \left(q^{a^{\alpha_{j_n} + i - 1 + i_m}} \right) = \prod_{1 \leq i \leq i_n} h_{j_n} \left(q^{a^{\alpha_{j_n} + i - 1}} \right) \prod_{1 \leq i \leq i_m} h_{j_m}^* \left(q^{a^{\beta_{j_m} + i - 1 + i_n}} \right). \quad (64)$$

It can be verified that the collection of disjoint cycles $\Omega_{U_m^{(t_0)}} \dots, \Omega_{U_m^{(t_{r_{m,n}})}}$ with respect to m (resp. the collection of disjoint cycles $\Omega_{V_n^{(t_0)}} \dots, \Omega_{V_n^{(t_{r_{m,n}})}}$ with respect to n) above can be partitioned into nonempty subcollections $\Pi_{1,m}, \dots, \Pi_{r,m}$ (resp. $\Theta_{1,n}, \dots, \Theta_{s,n}$) for some positive integer s with the following properties:

- 1) All polynomials in any cycle in $\Pi_{i,m}$ and $\Theta_{i,n}$ have the same base polynomial for each i in $\{1, \dots, s\}$.
- 2) For $i \neq j$, a polynomial in any cycle in $\Pi_{i,m}$ or $\Theta_{i,n}$ and a polynomial in any cycle in $\Pi_{j,m}$ or $\Theta_{j,n}$ have different base polynomials.

Suppose that $s > 1$. As we vary n in \mathcal{N} and fix m , let us denote $\Omega_{U_m^{(t_j)}}$, for any t_j , by $\Omega_{U_{m,n}^{(t_j)}}$ to show that it is the cycle at t_j , associated to the collections of indexes U_m in (40), with respect to m and n . Similarly, we denote

$$\begin{aligned} & \Pi_{i,m} \quad \text{and} \quad \Theta_{i,n} \\ \text{by} & \quad \Pi_{i,m,n} \quad \text{and} \quad \Theta_{1,m,n}, \end{aligned}$$

respectively, for any i . By re-indexing if necessary, we may assume that $\Omega_{U_{m,n}^{(t_0)}}$ is in $\Pi_{1,m,n}$. It can be verified that

$$\Pi_{1,m,n} \quad \text{and} \quad \bigcup_{\Omega_{U_{m,n}^{(t_j)}} \in \Pi_{1,m,n}} \Omega_{U_{m,n}^{(t_j)}}$$

must be the same for all n in \mathcal{N} and thus

$$\sum_{\Omega_{U_{m,n}^{(t_j)}} \in \Pi_{1,m,n}} \frac{i_m}{(i_m, i_n)} = |\Pi_{1,m,n}| \frac{i_m}{(i_m, i_n)} \quad (65)$$

is constant for all n in \mathcal{N} . Hence

$$|\Pi_{1,m,n}| \frac{i_m}{(i_m, i_n)} < i_m$$

since $s > 1$ and thus

$$|\Pi_{1,m,n}| < (i_m, i_n).$$

From (65),

$$\frac{|\Pi_{1,m,n}|}{(i_m, i_n)} \quad (66)$$

is constant for all n in \mathcal{N} . As a result, the same argument applying at (63) can be applied to (66), leading to the fact that all the elements of I_m must have a nontrivial factor which is a contradiction. Therefore $s = 1$, and thus

$$h_i^*(q) = h_j^*(q) \quad \text{for all } i \text{ and } j \text{ in } J_{0,m}^{(n)}$$

and

$$h_i(q) = h_j(q) \quad \text{for all } i \text{ and } j \text{ in } J_{0,n}^{(m)} \quad \text{for all } n \text{ in } \mathcal{N}.$$

As a result of (40), (60) and (64), we have

$$\begin{aligned} & \frac{\prod_{1 \leq i \leq j_m} h_i^*(q^{a^{\beta i}})}{\prod_{1 \leq i \leq i_m} h_{j_m}^*(q^{a^{\beta j_m + i - 1}})} \frac{\prod_{1 \leq i \leq j_n} h_i(q^{a^{\alpha i + i_m}})}{\prod_{1 \leq i \leq i_n} h_{j_n}(q^{a^{\alpha j_n + i - 1 + i_m}})} \\ &= \frac{\prod_{1 \leq i \leq j_m} h_i^*(q^{a^{\beta i}})}{\prod_{i \in J_{0,m}^{(n)}} h_i^*(q^{a^{\beta i}})} \frac{\prod_{1 \leq i \leq j_n} h_i(q^{a^{\alpha i + i_m}})}{\prod_{i \in J_{0,n}^{(m)}} h_i(q^{a^{\alpha i + i_m}})} \\ &= \frac{\prod_{1 \leq i \leq j_n} h_i(q^{a^{\alpha i}})}{\prod_{i \in J_{0,m}^{(n)}} h_i(q^{a^{\alpha i}})} \frac{\prod_{1 \leq i \leq j_m} h_i^*(q^{a^{\beta i + i_n}})}{\prod_{i \in J_{0,n}^{(m)}} h_i^*(q^{a^{\beta i + i_n}})} \\ &= \frac{\prod_{1 \leq i \leq j_n} h_i(q^{a^{\alpha i}})}{\prod_{1 \leq i \leq i_n} h_{j_n}(q^{a^{\alpha j_n + i - 1}})} \frac{\prod_{1 \leq i \leq j_m} h_i^*(q^{a^{\beta i + i_n}})}{\prod_{1 \leq i \leq i_m} h_{j_m}^*(q^{a^{\beta j_m + i - 1 + i_n}})}. \end{aligned} \quad (67)$$

By repeating the above argument, with (67) in place (40) and $J_{1,m}^{(n)}$ and $J_{1,n}^{(m)}$ in place of $J_{0,m}^{(n)}$ and $J_{0,n}^{(m)}$, respectively, and by reiterating this argument again and again until we reach $J_{\min\{k,l\},m}^{(n)}$ and $J_{\min\{k,l\},n}^{(m)}$ and

$$\begin{aligned} & \frac{\prod_{1 \leq i \leq j_m} h_i^*(q^{a^{\beta i}})}{\prod_{0 \leq t \leq \min\{k,l\}} \prod_{i \in J_{t,m}^{(n)}} h_i^*(q^{a^{\beta i}})} \frac{\prod_{1 \leq i \leq j_n} h_i(q^{a^{\alpha i + i_m}})}{\prod_{0 \leq t \leq \min\{k,l\}} \prod_{i \in J_{t,n}^{(m)}} h_i(q^{a^{\alpha i + i_m}})} = \\ & \frac{\prod_{1 \leq i \leq j_n} h_i(q^{a^{\alpha i}})}{\prod_{0 \leq t \leq \min\{k,l\}} \prod_{i \in J_{t,m}^{(n)}} h_i(q^{a^{\alpha i}})} \frac{\prod_{1 \leq i \leq j_m} h_i^*(q^{a^{\beta i + i_n}})}{\prod_{0 \leq t \leq \min\{k,l\}} \prod_{i \in J_{t,n}^{(m)}} h_i^*(q^{a^{\beta i + i_n}})}, \end{aligned} \quad (68)$$

it can be verified then that both sides of (68) are in fact trivial. Thus

$$k = l = \frac{j_m}{i_m} = \frac{j_n}{i_n}$$

and (40) takes the form

$$\begin{aligned} & \left(\prod_{1 \leq g \leq \frac{j_m}{i_m}} \prod_{1 \leq i \leq i_m} h_{(g-1)i_m+1}^* \left(q^{a^{\beta(g-1)i_m+1+i-1}} \right) \right) \\ & \times \left(\prod_{1 \leq g \leq \frac{j_n}{i_n}} \prod_{1 \leq i \leq i_n} h_{(g-1)i_n+1} \left(q^{a^{\alpha(g-1)i_n+1+i-1+i_m}} \right) \right) \\ & = \left(\prod_{1 \leq g \leq \frac{j_m}{i_m}} \prod_{1 \leq i \leq i_n} h_{(g-1)i_n+1} \left(q^{a^{\alpha(g-1)i_n+1+i-1}} \right) \right) \\ & \times \left(\prod_{1 \leq g \leq \frac{j_m}{i_m}} \prod_{1 \leq i \leq i_m} h_{(g-1)i_m+1}^* \left(q^{a^{\beta(g-1)i_m+1+i-1+i_n}} \right) \right). \end{aligned} \quad (69)$$

As a result, it can be verified that:

- 1) For the fixed positive integer m and for each positive integer $1 \leq g \leq \frac{j_m}{i_m}$, $h_i^*(q) = h_j^*(q)$ for all positive integers $(g-1)i_m < i, j \leq gi_m$.
- 2) For each positive integer n in \mathcal{N} and for each positive integer $1 \leq g \leq \frac{j_n}{i_n}$, $h_i(q) = h_j(q)$ for all positive integers $(g-1)i_n < i, j \leq gi_n$.
- 3) $\alpha_{(g-1)i_n+1} = \beta_{(g-1)i_m+1}$ for $1 \leq g \leq L_\Gamma$, where L_Γ denote the common value $\frac{j_m}{i_m} = \frac{j_n}{i_n}$.

Therefore, I) follows.

II) Suppose that (29) occurs for some $i = i_0 > 1$ and $j = j_0 > 1$. With the substitutions in (32)–(34) and (23), we have

$$h_1 \left(q^{a^{i_m+\alpha_1}} \right) = h_1^* \left(q^{a^{i_n+\beta_1}} \right) \text{ with } \beta_1 + i_n = \alpha_1 + i_m > \alpha_1. \quad (70)$$

Using the substitutions in (32)–(34) and (70), it can be verified that the argument in (I) can be applied to the functions in the numerators of (38) by equating the roots of the numerators on both side of (38) according to their orders as roots of unity if $\Gamma = \Gamma^{(2)}$ or their root levels if $\Gamma = \Gamma^{(1)}$ to obtain (40). As a result, the same argument in (I) also implies (45), (46) and the rest of II). Therefore II) and thus Proposition 6 follow. \square

5. Proof of Uniqueness

In this section, we prove the uniqueness of the pair of monic polynomials $f(q)$ and $g(q)$ in 2) of Theorem 5.

PROPOSITION 7. *There exists a unique rational function $\frac{f(q)}{g(q)}$ with $f(q)$ and $g(q)$ monic polynomials such that $(f(q), g(q)) = 1$ in $\bar{K}[q]$ and*

$$f_n(q) = \frac{f(q)}{g(q)} \frac{f(q^a)}{g(q^a)} \cdots \frac{f(q^{a^{i_n-1}})}{g(q^{a^{i_n-1}})} \quad (71)$$

for all n in $\mathcal{A} - \{1\}$.

Proof. Since $h_{(g-1)i_n+1} = h_1(q) = h_1^*(q) = h_{(g-1)i_m+1}^*$ for $g = 1$, it is straight forward to verified that

$$\begin{aligned} \prod_{1 \leq i \leq i_m} h_{(g-1)i_m+1}^* \left(q^{a^{\beta(g-1)i_m+1+i-1}} \right) \prod_{1 \leq i \leq i_n} h_{(g-1)i_n+1} \left(q^{a^{\alpha(g-1)i_n+1+i-1+i_m}} \right) = \\ \prod_{1 \leq i \leq i_n} h_{(g-1)i_n+1} \left(q^{a^{\alpha(g-1)i_n+1+i-1}} \right) \prod_{1 \leq i \leq i_m} h_{(g-1)i_m+1}^* \left(q^{a^{\beta(g-1)i_m+1+i-1+i_n}} \right) \end{aligned} \quad (72)$$

for $g = 1$. Hence, it follows from (69) that

$$\begin{aligned} \left(\prod_{2 \leq g \leq L_\Gamma} \prod_{1 \leq i \leq i_m} h_{(g-1)i_m+1}^* \left(q^{a^{\beta(g-1)i_m+1+i-1}} \right) \right) \\ \left(\prod_{2 \leq g \leq L_\Gamma} \prod_{1 \leq i \leq i_n} h_{(g-1)i_n+1} \left(q^{a^{\alpha(g-1)i_n+1+i-1+i_m}} \right) \right) = \\ \left(\prod_{2 \leq g \leq L_\Gamma} \prod_{1 \leq i \leq i_n} h_{(g-1)i_n+1} \left(q^{a^{\alpha(g-1)i_n+1+i-1}} \right) \right) \\ \left(\prod_{2 \leq g \leq L_\Gamma} \prod_{1 \leq i \leq i_m} h_{(g-1)i_m+1}^* \left(q^{a^{\beta(g-1)i_m+1+i-1+i_n}} \right) \right). \end{aligned}$$

Then an argument similar to that in Proposition 3 shows that

$$h_{(g-1)i_n+1}(q) = h_{(g-1)i_m+1}^*(q)$$

for $g = 2$ and thus (72) holds for $g = 2$. This process can then be iterated so that $h_{(g-1)i_n+1}(q) = h_{(g-1)i_m+1}^*(q)$ and (72) holds for $1 \leq g \leq L_\Gamma$.

CLASSIFICATION OF SOLUTIONS WITH CYCLIC AND SEMI-CYCLIC SUPPORTS

If (29) does not occur, let $g(q) = 1$ and $\delta_g = \alpha_{(g-1)i_n+1} = \beta_{(g-1)i_m+1}$ for $1 \leq g \leq L_\Gamma$. Let $f_g(q) = h_{(g-1)i_n+1}(q) = h_{(g-1)i_m+1}^*(q)$ for $1 \leq g \leq L_\Gamma$. Let

$$f(q) = \prod_{1 \leq g \leq L_\Gamma} f_g(q^{a^{\delta_g}}).$$

Then $f(q)$ is monic and

$$f_m(q) = \prod_{1 \leq i \leq i_m} f(q^{a^{i-1}}) = \prod_{1 \leq i \leq i_m} \frac{f(q^{a^{i-1}})}{g(q^{a^{i-1}})} \quad (73)$$

and

$$f_n(q) = \prod_{1 \leq i \leq i_n} f(q^{a^{i-1}}) = \prod_{1 \leq i \leq i_n} \frac{f(q^{a^{i-1}})}{g(q^{a^{i-1}})}. \quad (74)$$

If (29) occurs for some $i = i_0 > 1$ and $j = j_0 > 1$, then $L(q)$ and $L^*(q)$ are nontrivial and (41) holds since (40) holds in this case by Proposition 6. By (39), we can iterate this argument to obtain sequences of functions

$$\{L_{nt}(q) \mid 1 \leq t \leq T; L_{n1}(q) = L_n(q)\} \quad \text{and} \quad \{L_{mt}^*(q) \mid 1 \leq t \leq T; L_{m1}^*(q) = L_m^*(q)\}$$

for some integer $T \geq 1$ such that:

- 1) $L_{mT}^*(q) = L_{nT}(q) = 1$;
- 2) $\deg(L_{mt}^*(q)) < \deg(L_{m(t-1)}^*(q))$ and $\deg(L_{nt}(q)) < \deg(L_{n(t-1)}(q))$ for $2 \leq t \leq T$;
- 3) for $1 \leq t \leq T$,

$$L_{mt}^*(q)L_{nt}(q^{m_i}) = L_{nt}(q)L_{mt}^*(q^{n_i});$$

- 4) for $1 \leq t \leq T$,

$$L_{mt}^*(q) = \prod_{1 \leq s \leq P_\Gamma} \prod_{1 \leq i \leq i_m} f_s^{(t)}(q^{a^{\delta_s^{(t)}+i-1}}) = \prod_{1 \leq i \leq i_m} f^{(t)}(q^{a^{i-1}}) \quad (75)$$

and

$$L_{nt}(q) = \prod_{1 \leq s \leq P_\Gamma} \prod_{1 \leq i \leq i_n} f_s^{(t)}(q^{a^{\delta_s^{(t)}+i-1}}) = \prod_{1 \leq i \leq i_n} f^{(t)}(q^{a^{i-1}}) \quad (76)$$

where:

- $l_m^{(t)}$ and $l_n^{(t)}$ are positive integers with $\frac{l_m^{(t)}}{i_m} = \frac{l_n^{(t)}}{i_n} = P_\Gamma$ an integer for $1 \leq t \leq T$;
- $f_s^{(t)}(q) = f_{(s-1)i_m+1}^{*(mt)}(q) = f_{(s-1)i_n+1}^{(nt)}(q)$ is a polynomial for each $1 \leq s \leq P_\Gamma^{(t)}$ and $1 \leq t \leq T$;
- $f^{(t)}(q) = \prod_{1 \leq s \leq P_\Gamma} f_s^{(t)}(q^{\delta_s^{(t)}})$ for $1 \leq t \leq T$.

By (II) of Proposition 6, it follows from the same argument used to obtain (73) and (74) that

$$\left(\prod_{1 \leq j \leq j_m} h_j^*(q^{a^{\beta_j}}) \right) = \prod_{1 \leq i \leq i_m} \frac{F(q^{a^{i-1}})}{G(q^{a^{i-1}})} \quad (77)$$

and

$$\left(\prod_{1 \leq j \leq j_n} h_j^*(q^{a^{\alpha_j}}) \right) = \prod_{1 \leq i \leq i_n} \frac{F(q^{a^{i-1}})}{G(q^{a^{i-1}})} \quad (78)$$

for some monic polynomials $F(q)$ and $G(q)$. By combining (77) and (78) with (75) and (76), we also have

$$f_m(q) = \prod_{1 \leq i \leq i_m} \frac{f(q^{a^{i-1}})}{g(q^{a^{i-1}})}$$

and

$$f_n(q) = \prod_{1 \leq i \leq i_n} \frac{f(q^{a^{i-1}})}{g(q^{a^{i-1}})}$$

for some monic polynomials $f(q)$ and $g(q)$ with $(f(q), g(q)) = 1$ in $\bar{K}[q]$.

For $n = m^\alpha$ for some positive integer $\alpha > 1$, it follows from the fact that Γ is a solution to Functional Equation (2) that

$$\begin{aligned} f_n(q) &= f_{m^\alpha}(q) = f_m(q)f_{m^{\alpha-1}}(q^m) = \cdots \\ &\cdots = f_m(q)f_m(q^m) \cdots f_m(q^{m^{\alpha-1}}) = f_m(q)f_m(q^{a^{i_m}}) \cdots f_m(q^{(a^{i_m})^{\alpha-1}}). \end{aligned}$$

Thus,

$$\begin{aligned} f_n(q) &= \left(\frac{f(q)}{g(q)} \frac{f(q^a)}{g(q^a)} \cdots \frac{f(q^{a^{i_m-1}})}{g(q^{a^{i_m-1}})} \right) \left(\frac{f(q^{a^{i_m}})}{g(q^{a^{i_m}})} \frac{f(q^{a^{i_m+1}})}{g(q^{a^{i_m+1}})} \cdots \frac{f(q^{a^{2i_m-1}})}{(q^{a^{2i_m-1}})} \right) \cdots \\ &\quad \cdots \left(\frac{f(q^{a^{(\alpha-1)i_m}})}{g(q^{a^{(\alpha-1)i_m}})} \frac{f(q^{a^{(\alpha-1)i_m+1}})}{g(q^{a^{(\alpha-1)i_m+1}})} \cdots \frac{f(q^{a^{(\alpha-1)i_m+(i_m-1)}})}{g(q^{a^{(\alpha-1)i_m+(i_m-1)}})} \right) \\ &= \left(\frac{f(q)}{g(q)} \frac{f(q^a)}{g(q^a)} \cdots \frac{f(q^{a^{i_m-1}})}{g(q^{a^{i_m-1}})} \right) \left(\frac{f(q^{a^{i_m}})}{g(q^{a^{i_m}})} \frac{f(q^{a^{i_m+1}})}{g(q^{a^{i_m+1}})} \cdots \frac{f(q^{a^{2i_m-1}})}{g(q^{a^{2i_m-1}})} \right) \cdots \\ &\quad \cdots \left(\frac{f(q^{a^{(\alpha-1)i_m}})}{g(q^{a^{(\alpha-1)i_m}})} \frac{f(q^{a^{(\alpha-1)i_m+1}})}{g(q^{a^{(\alpha-1)i_m+1}})} \cdots \frac{f(q^{a^{\alpha i_m-1}})}{g(q^{a^{\alpha i_m-1}})} \right) \\ &= \left(\frac{f(q)}{g(q)} \frac{f(q^a)}{g(q^a)} \cdots \frac{f(q^{a^{i_m-1}})}{g(q^{a^{i_m-1}})} \right) \left(\frac{f(q^{a^{i_m}})}{g(q^{a^{i_m}})} \frac{f(q^{a^{i_m+1}})}{g(q^{a^{i_m+1}})} \cdots \frac{f(q^{a^{i_m 2^{-1}}})}{g(q^{a^{i_m 2^{-1}}})} \right) \cdots \\ &\quad \cdots \left(\frac{f(q^{a^{i_m(\alpha-1)}})}{g(q^{a^{i_m(\alpha-1)}})} \frac{f(q^{a^{i_m(\alpha-1)+1}})}{g(q^{a^{i_m(\alpha-1)+1}})} \cdots \frac{f(q^{a^{i_m \alpha-1}})}{g(q^{a^{i_m \alpha-1}})} \right). \end{aligned}$$

Therefore,

$$f_n(q) = \frac{f(q)}{g(q)} \frac{f(q^a)}{g(q^a)} \dots \frac{f(q^{a^{i_n-1}})}{g(q^{a^{i_n-1}})} \quad \text{for all } n \text{ in } \mathcal{A} - \{1\} \text{ as desired.}$$

For uniqueness, suppose

$$f_n(q) = \frac{f(q)}{g(q)} \frac{f(q^a)}{g(q^a)} \dots \frac{f(q^{a^{i_n-1}})}{g(q^{a^{i_n-1}})} = \frac{\check{f}(q)}{\check{g}(q)} \frac{\check{f}(q^a)}{\check{g}(q^a)} \dots \frac{\check{f}(q^{a^{i_n-1}})}{\check{g}(q^{a^{i_n-1}})}$$

for some polynomial $\check{f}(q)$ and $\check{g}(q)$. Then

$$\begin{aligned} 1 &= \frac{f(q)\check{g}(q)}{g(q)\check{f}(q)} \frac{f(q^a)\check{g}(q^a)}{g(q^a)\check{f}(q^a)} \dots \frac{f(q^{a^{i_n-1}})\check{g}(q^{a^{i_n-1}})}{g(q^{a^{i_n-1}})\check{f}(q^{a^{i_n-1}})} \\ &= \frac{f\check{g}}{g\check{f}}(q) \frac{f\check{g}}{g\check{f}}(q^a) \dots \frac{f\check{g}}{g\check{f}}(q^{a^{i_n-1}}). \end{aligned}$$

Then the same argument as in the cyclic case (proved earlier) shows that

$$f(q) = g(q)$$

as required and thus Proposition 7 follows. \square

Theorem 5 follows from Propositions 1, 2 and 3–7.

6. Proof of Corollary 1

Let $\Gamma = \{f_n(q) \mid n \in \mathcal{A}\}$ be a (normalized) polynomial solution to Functional Equation (2) with field of coefficients of characteristic zero and support \mathcal{A} a subsemigroup of \mathbb{N} not necessarily a prime semigroup. Suppose \mathcal{A} is semi-cyclic with generator a . Suppose that \mathcal{A}^* is a subsemigroup of \mathbb{N} strictly containing \mathcal{A} such that \mathcal{A}^* is also semi-cyclic with generator a^* .

The following example shows that (7) is necessary for the existence of Γ^* : let \mathcal{A} a nonprime semicyclic subsemigroup of \mathbb{N} of the form $\{p^n \mid n \geq 0, n \neq 1\}$ for some prime P . Let

$$\Gamma = \left\{ f_{p^n}(q) = \begin{cases} \prod_{1 \leq i \leq n} \frac{(q^{p^i-1})(q^{p^i}+1)}{q^{p^i-1}+1}, & \text{if } n \neq 0; \\ 1, & \text{if } n = 0. \end{cases} \middle| n \in \mathcal{A} \right\}.$$

Then it can be checked that there is no extension to the support $\mathcal{A}^* = \{p^n \mid n \geq 0\}$.

Suppose that there is a polynomial solution $\Gamma^* = \{f_n^*(q) \mid n \in \mathbb{N}\}$ with support \mathcal{A}^* such that $f_n^*(q) = f_n(q)$ for all n in \mathcal{A} . If the generator a^* of \mathcal{A}^* is a prime p , then since a is the generator of $\mathcal{A} \subseteq \mathcal{A}^*$, $a = p^{t_a} = (a^*)^{t_a}$ for some positive integer t_a . Then for any n in \mathcal{A} , there exist unique rational functions $\frac{f(q)}{g(q)}$ and $\frac{f^*(q)}{g^*(q)}$ with

$$\begin{aligned} \frac{f(q)}{g(q)} \frac{f(q^a)}{g(q^a)} \cdots \frac{f(q^{a^{i_n-1}})}{g(q^{a^{i_n-1}})} &= f_n(q) = f_n^*(q) \\ &= \frac{f^*(q)}{g^*(q)} \frac{f^*(q^p)}{g^*(q^p)} \cdots \frac{f^*(q^{p^{t_n-1}})}{g^*(q^{p^{t_n-1}})} \\ &= \left(\frac{f^*(q)}{g^*(q)} \frac{f^*(q^p)}{g^*(q^p)} \cdots \frac{f^*(q^{p^{t_a-1}})}{g^*(q^{p^{t_a-1}})} \right) \\ &\quad \times \left(\frac{f^*(q^{p^{t_a}})}{g^*(q^{p^{t_a}})} \frac{f^*(q^{p^{t_a+1}})}{g^*(q^{p^{t_a+1}})} \cdots \frac{f^*(q^{p^{2t_a-1}})}{g^*(q^{p^{2t_a-1}})} \right) \cdots \\ &\quad \cdots \left(\frac{f^*(q^{p^{(\frac{t_n}{t_a}-1)t_a}})}{g^*(q^{p^{(\frac{t_n}{t_a}-1)t_a}})} \cdots \frac{f^*(q^{p^{\frac{t_n}{t_a}t_a-1}})}{g^*(q^{p^{\frac{t_n}{t_a}t_a-1}})} \right), \end{aligned}$$

where $f(q)$, $g(q)$, $f^*(q)$ and $g^*(q)$ are monic polynomials with nonzero constant terms and $(f(q), g(q)) = 1 = (f^*(q), g^*(q))$ in $\bar{K}[q]$ by Theorem 2.1. Therefore,

$$\frac{f(q)}{g(q)} = \frac{f^*(q)}{g^*(q)} \frac{f^*(q^p)}{g^*(q^p)} \cdots \frac{f^*(q^{p^{t_a-1}})}{g^*(q^{p^{t_a-1}})} = \frac{\widehat{f}(q)}{\widehat{g}(q)} \frac{\widehat{f}(q^{\widehat{a}})}{\widehat{g}(q^{\widehat{a}})} \cdots \frac{\widehat{f}(q^{\widehat{a}^{t_a-1}})}{\widehat{g}(q^{\widehat{a}^{t_a-1}})}$$

with

$$\widehat{a} := p \quad \text{and} \quad \frac{\widehat{f}(q)}{\widehat{g}(q)} := \frac{f^*(q)}{g^*(q)}$$

having the required properties. Suppose that \mathcal{A}^* is a semigroup with generator not necessarily a prime number. Let n_0 be an element of $\mathcal{A} - \{1\}$. Then there are positive integers u_0 and v_0 such that $a^{v_0} = n_0 = (a^*)^{u_0}$ since both a and a^* generate \mathcal{A} . Thus

$$(a^*)^{\frac{u_0}{v_0}} = a. \tag{79}$$

If $\frac{u_0}{v_0}$ is an integer, then it can be verified that $\widehat{a} := a^*$ with $e = \frac{u_0}{v_0}$ and $e^* = 1$ has the required properties since for any n in \mathcal{A} , there exist unique rational functions

$$\frac{f(q)}{g(q)} \quad \text{and} \quad \frac{f^*(q)}{g^*(q)},$$

where

$$\begin{aligned}
 \frac{f(q)}{g(a)} \frac{f(q^a)}{g(q^a)} \cdots \frac{f(q^{a^{i_n-1}})}{g(q^{a^{i_n-1}})} &= f_n(q) = f_n^*(q) \\
 &= \frac{f^*(q)}{g^*(q)} \frac{f^*(q^{a^*})}{g^*(q^{a^*})} \cdots \frac{f^*(q^{(a^*)^{i_n^*-1}})}{g^*(q^{(a^*)^{i_n^*-1}})} \\
 &= \left(\frac{f^*(q)}{g^*(q)} \frac{f^*(q^{a^*})}{g^*(q^{a^*})} \cdots \frac{f^*(q^{(a^*)^{e-1}})}{g^*(q^{(a^*)^{e-1}})} \right) \\
 &\quad \times \left(\frac{f^*(q^{(a^*)^e})}{g^*(q^{(a^*)^e})} \frac{f^*(q^{(a^*)^{e+1}})}{g^*(q^{(a^*)^{e+1}})} \cdots \frac{f^*(q^{(a^*)^{2e-1}})}{g^*(q^{(a^*)^{2e-1}})} \right) \cdots \\
 &\quad \cdots \left(\frac{f^*(q^{(a^*)^{(\frac{i_n^*}{e}-1)e}})}{g^*(q^{(a^*)^{(\frac{i_n^*}{e}-1)e}})} \cdots \frac{f^*(q^{(a^*)^{\frac{i_n^*}{e}e-1}})}{g^*(q^{(a^*)^{\frac{i_n^*}{e}e-1}})} \right)
 \end{aligned} \tag{80}$$

with $f(q)$, $g(q)$, $f^*(q)$ and $g^*(q)$ monic polynomials having nonzero constant terms and $(f(q), g(q)) = 1 = (f^*(q), g^*(q))$ in $\bar{K}[q]$ by Theorem 2.1. Therefore,

$$\frac{f(q)}{g(q)} = \frac{f^*(q)}{g^*(q)} \frac{f^*(q^{a^*})}{g^*(q^{a^*})} \cdots \frac{f^*(q^{(a^*)^{e-1}})}{g^*(q^{(a^*)^{e-1}})} \tag{81}$$

$$= \frac{\widehat{f}(q)}{\widehat{g}(q)} \frac{\widehat{f}(q^{\widehat{a}})}{\widehat{g}(q^{\widehat{a}})} \cdots \frac{\widehat{f}(q^{\widehat{a}^{e-1}})}{\widehat{g}(q^{\widehat{a}^{e-1}})}, \tag{82}$$

where $\frac{\widehat{f}(q)}{\widehat{g}(q)} := \frac{f^*(q)}{g^*(q)}$. Thus let us suppose that

$$\frac{u'_0}{v'_0} = \frac{u_0}{v_0}$$

is not an integer where $(u'_0, v'_0) = 1$. Let us show then that $a^* = \alpha^{v'_0}$ for some positive integer α . If not, then it can be verified that there exists a positive integer β such that

$$(a^*)^{\frac{u'_0}{v'_0}} = \beta \frac{u''_0}{v''_0}$$

with v''_0 minimum. Then $v''_0 > 1$ and thus has a prime factor p . For any n in $\mathcal{N} \cup \{m\} \subseteq \mathcal{A}$, we have

$$n = a^{i_n} = \left((a^*)^{\frac{u_0}{v_0}} \right)^{i_n} = \left(\beta \frac{u''_0}{v''_0} \right)^{i_n}.$$

Thus p divides i_n . As a result, $I_m = \{(i_m, i_n) \mid n \in \mathcal{N}\}$ has a nontrivial common factor, which is a contradiction. Therefore, we can define $\widehat{a} := \alpha$, and thus $a = \widehat{a}^e$ and $a^* = \widehat{a}^{e^*}$ with $e = u'_0$ and $e^* = v'_0$. Since $a = \widehat{a}^e$ and $a^* = \widehat{a}^{e^*}$ are the generators of \mathcal{A} and \mathcal{A}^* , respectively, e and e^* are the greatest common factor of the collection

$\{ei_n \mid n \in \mathcal{A}\}$ and $\{e^{*i_n^*} \mid n \in \mathcal{A}^*\}$, respectively. Together with the fact that $i_n e = i_n^* e^*$ for each n in $\mathcal{A} - \{1\}$, it follows that $e^* r = e$ for some positive integer r . Thus, $a = (a^*)^r$, which contradicts our assumption since it means that $\frac{u_0}{v_0}$ is an integer. Therefore, $\frac{u_0}{v_0}$ is an integer and the result follows from (79)–(81).

To prove the other direction, let \mathcal{A} be a subsemigroup of \mathbb{N} which is not necessarily a prime semigroup. Suppose \mathcal{A} is semi-cyclic with generator a . Let \mathcal{A}^* be another subsemigroup of \mathbb{N} strictly containing \mathcal{A} which is also semi-cyclic with generator a^* . Let $\Gamma = \{f_n(q) \mid n \in \mathbb{N}\}$ be a (normalized) polynomial solution with field of coefficients of characteristic zero and support \mathcal{A} . Suppose that there exists a number \hat{a} such that $a = \hat{a}^e$ and $a^* = \hat{a}^{e^*}$ for some positive integers e and e^* , and a rational function $\frac{\hat{f}(q)}{\hat{g}(q)}$, with $\hat{f}(q)$ and $\hat{g}(q)$ monic polynomials having nonzero constant terms and $(\hat{f}(q), \hat{g}(q)) = 1$ in $\bar{K}[q]$, such that

$$f_n(q) = \frac{f(q)}{g(q)} \frac{f(q^a)}{g(q^a)} \cdots \frac{f(q^{a^{i_n-1}})}{g(q^{a^{i_n-1}})}, \quad (83)$$

for all n in $\mathcal{A} - \{1\}$, where i_n is the index power of n with respect to a and $\frac{f(q)}{g(q)}$ is the unique rational function associated to Γ by Theorem 2.1, and

$$\frac{f(q)}{g(q)} = \frac{\hat{f}(q)}{\hat{g}(q)} \frac{\hat{f}(q^{\hat{a}})}{\hat{g}(q^{\hat{a}})} \cdots \frac{\hat{f}(q^{\hat{a}^{e-1}})}{\hat{g}(q^{\hat{a}^{e-1}})}. \quad (84)$$

Define $f_1^*(q) := 1$; $f_n^*(q) := 0$ if n is not in \mathcal{A}^* ;

$$f_n^*(q) := \frac{f^*(q)}{g^*(q)} \frac{f^*(q^{a^*})}{g^*(q^{a^*})} \cdots \frac{f^*(q^{(a^*)^{i_n^*-1}})}{g^*(q^{(a^*)^{i_n^*-1}})}, \quad (85)$$

a polynomial for each n in $\mathcal{A}^* - \{1\}$ having index power i_n^* with respect to a^* , where

$$\frac{f^*(q)}{g^*(q)} := \frac{\hat{f}(q)}{\hat{g}(q)} \frac{\hat{f}(q^{\hat{a}})}{\hat{g}(q^{\hat{a}})} \cdots \frac{\hat{f}(q^{\hat{a}^{e^*-1}})}{\hat{g}(q^{\hat{a}^{e^*-1}})}. \quad (86)$$

Define $\Gamma^* := \{f_n^*(q) \mid n \in \mathbb{N}\}$. Then it is straightforward to check from (86) that Γ^* is a (normalized) polynomial solution to Functional Equation (2) with support \mathcal{A}^* .

Next we check that $f_n(q) = f_n^*(q)$ for each n in \mathcal{A} . For each n in $\mathcal{A} - \{1\}$, it follows from (83)–(86) and $ei_n = e^* i_n^*$ that

$$\begin{aligned} f_n(q) &= \frac{f(q)}{g(q)} \frac{f(q^a)}{g(q^a)} \cdots \frac{f(q^{a^{i_n-1}})}{g(q^{a^{i_n-1}})} \\ &= \left(\frac{\hat{f}(q)}{\hat{g}(q)} \frac{\hat{f}(q^{\hat{a}})}{\hat{g}(q^{\hat{a}})} \cdots \frac{\hat{f}(q^{\hat{a}^{e-1}})}{\hat{g}(q^{\hat{a}^{e-1}})} \right) \cdots \left(\frac{\hat{f}(q^{\hat{a}^e})}{\hat{g}(q^{\hat{a}^e})} \frac{\hat{f}(q^{\hat{a}^{e+1}})}{\hat{g}(q^{\hat{a}^{e+1}})} \cdots \frac{\hat{f}(q^{\hat{a}^{2e-1}})}{\hat{g}(q^{\hat{a}^{2e-1}})} \right) \cdots \\ &\quad \cdots \left(\frac{\hat{f}(q^{\hat{a}^{(i_n-2)e+1}})}{\hat{g}(q^{\hat{a}^{(i_n-2)e+1}})} \frac{\hat{f}(q^{\hat{a}^{(i_n-2)e+2}})}{\hat{g}(q^{\hat{a}^{(i_n-2)e+2}})} \cdots \frac{\hat{f}(q^{\hat{a}^{(i_n-1)e}})}{\hat{g}(q^{\hat{a}^{(i_n-1)e}})} \right) \end{aligned}$$

CLASSIFICATION OF SOLUTIONS WITH CYCLIC AND SEMI-CYCLIC SUPPORTS

$$\begin{aligned}
 &= \frac{\widehat{f}(q)}{\widehat{g}(q)} \frac{\widehat{f}(q^{\widehat{a}})}{\widehat{g}(q^{\widehat{a}})} \frac{\widehat{f}(q^{\widehat{a}^2})}{\widehat{g}(q^{\widehat{a}^2})} \cdots \frac{\widehat{f}(q^{\widehat{a}^{(i_n-1)e}})}{\widehat{g}(q^{\widehat{a}^{(i_n-1)e}})} \\
 &= \left(\frac{\widehat{f}(q)}{\widehat{g}(q)} \frac{\widehat{f}(q^{\widehat{a}})}{\widehat{g}(q^{\widehat{a}})} \cdots \frac{\widehat{f}(q^{\widehat{a}^{e^*-1}})}{\widehat{g}(q^{\widehat{a}^{e^*-1}})} \right) \cdots \left(\frac{\widehat{f}(q^{\widehat{a}^{e^*}})}{\widehat{g}(q^{\widehat{a}^{e^*}})} \frac{\widehat{f}(q^{\widehat{a}^{e^*+1}})}{\widehat{g}(q^{\widehat{a}^{e^*+1}})} \cdots \frac{\widehat{f}(q^{\widehat{a}^{2e^*-1}})}{\widehat{g}(q^{\widehat{a}^{2e^*-1}})} \right) \cdots \\
 &\quad \cdots \left(\frac{\widehat{f}(q^{\widehat{a}^{(i_n^*-2)e^*+1}})}{\widehat{g}(q^{\widehat{a}^{(i_n^*-2)e^*+1}})} \frac{\widehat{f}(q^{\widehat{a}^{(i_n^*-2)e^*+2}})}{\widehat{g}(q^{\widehat{a}^{(i_n^*-2)e^*+2}})} \cdots \frac{\widehat{f}(q^{\widehat{a}^{(i_n^*-1)e^*}})}{\widehat{g}(q^{\widehat{a}^{(i_n^*-1)e^*}})} \right) \\
 &= \frac{f^*(q)}{f^*(q)} \frac{f^*(q^{a^*})}{g^*(q^{a^*})} \cdots \frac{f^*(q^{(a^*)^{i_n^*-1}})}{g^*(q^{(a^*)^{i_n^*-1}})} = f_n^*(q).
 \end{aligned}$$

Since $f_1(q) = f_1^*(q)$, Corollary 1 follows.

REFERENCES

[1] CHEREDNIK, I.: *On q -analogues of Riemann's zeta*, *Selecta Math. N S.* **7** (2001), 447–491.
 [2] KOBLITZ, N.: *On Carlitz's q -Bernoulli numbers*, *J. Number Theory* **14** (1982), 332–339.
 [3] MOAK, D. S.: *The q -analogue of sterling formula*, *Rocky Mountain J. Math.* **14** (1984), 403–413.
 [4] NATHANSON, M. B.: *A functional equation arising from multiplication of quantum integers*, *J. Number Theory* **103** (2003), no. 2, 214–233.
 [5] NATHANSON, M. B.: *Formal power series arising from multiplication of quantum integers*, *Unusual applications of number theory DIMACS Ser. Discrete Math. Theoret. Comput. Sci.* Vol. 64, (2004) Amer. Math. Soc., Providence, RI, pp.145–157.
 [6] NATHANSON, M. B.: *Linear quantum addition rules*, *Integers* **7** (2007), no. 2, 1–6 (A 27).
 [7] NGUYEN, L.: *On the solutions of a functional equation arising from multiplication of quantum integers*, *J. Number Theory* **130** (2010), no. 6, 1292–1347.
 [8] NGUYEN, L.: *On the classification of solutions of a functional equation arising from multiplication of quantum integers*, *Unif. Distrib. Theory* **8** (2013), no. 2, 49–120.
 [9] NGUYEN, L.: *Nathanson quantum functional equations and the non-prime semi-group support polynomial solutions*, *Semigroup Forum* **93** (2016) no. 3, 459–490.
 [10] NGUYEN, L.: *On symmetries of roots of rational functions and the classification of rational function solutions of functional equations arising from multiplication of quantum integers with prime semigroup supports*, *Aequationes Math.* **92** (2018), 1001–1035, DOI:10.1007/s00010-018-0607-y.

LAN NGUYEN

- [11] NGUYEN, L.: *On the rational function solutions of functional equations arising from multiplication of quantum integers*, **293** Math. Z. (2019), 903–933, DOI:10.1007/s00209-019-02380-z.
- [12] NGUYEN, L.: *Quantum functional equations and extension of non-prime supports for solutions with field of coefficients \mathbb{Q}* , (preprint).
- [13] SATOH, J.: *q -analogue of Riemann's ζ -function and q -Euler numbers*, J. Number Theory **31** (1989), 346–362.

Received August 3, 2020

Accepted December 26, 2020

Lan Nguyen

Department of Mathematics

The University of Wisconsin-Parkside

900 Wood Road

Kenosha, WI 53141

U.S.A.

E-mail: nguyennl@uwp.edu