Notes on Number Theory and Discrete Mathematics
Vol. 18, 2012, No. 4, 11–39

On the polynomial and maximal solutions to a functional equation arising from multiplication of quantum integers

Lan Nguyen

Department of Mathematics, University of Wisconsin-Parkside
e-mail: nguyenl@uwp.edu

Abstract: We resolve two questions posed by Melvyn Nathanson, Yang Wang, and Alex Borisov concerning solutions with coefficients in $\mathbb{Q}$ of the functional equations arising from multiplication of quantum integers. First, we determine the necessary and sufficient criteria for determining when a rational function solution to these functional equations contains only polynomials. Second, we determine the sets of primes P for which there exist maximal solutions Γ_P to these functional equations with support bases P. We also give an explicit description of these maximal solutions.
Keywords: Diophantine equation, Factorial, Fibonacci, Brocard-Ramanujan.
AMS Classification: 11P99, 11C08.

1 Introduction

First, let us give some background concerning quantum integers and the functional equations arising from multiplication of these integers.

Definition 1.1. A quantum integer is a polynomial in q of the form

$$[n]_q := q^{n-1} + \ldots + q + 1 = \frac{q^n - 1}{q - 1} \tag{1.1}$$

where n is any natural number.

From [3], quantum multiplication, a multiplication operation for quantum integers, is defined by the following rule:

$$[m]_q \star [n]_q := [mn]_q = [m]_q \cdot [n]_{q^m} = [n]_q \cdot [m]_{q^n} \tag{1.2}$$

where $\star$ denotes quantum multiplication and $\cdot$ denotes the usual multiplication of polynomials. Equation (1.2) is just the q-series expansion of the sumset

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

Equation (1.2) provides the motivation for studying sequences of rational functions $\Gamma = \{f_n(q)|n = 1,\ldots,\infty\}$ with coefficients contained in some field of characteristic zero, satisfying the following functional equations:

$$f_m(q)f_n(q^m) \stackrel{(1)}{=} f_n(q)f_m(q^n) \stackrel{(2)}{=} f_{mn}(q) \tag{1.3}$$

for all $m,n \in \mathbb{N}$. We refer to the first equality in the above functional equation as Functional Equation (1) and the second equality as Functional Equation (2). A sequence of polynomials which satisfies Functional Equation (2) automatically satisfies Functional Equation (1) but not vice versa (see [5] for more details).

Definition 1.2. Let $\Gamma = \{f_n(q)|n \in \mathbb{N}\}$ be a sequence of rational functions satisfying Functional Equation (2). Then Γ is said to be generated by quantum integers if there exist ordered pairs of integers $\{u_i,t_i\}_i$ with $i = 1,\ldots,s$ such that $t_\Gamma = \sum_{i=1,\ldots,s} u_i t_i$ and

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

for all n in $\mathbb{N}$.

Let $\Gamma = \{f_n(q)\}$ be a sequence of rational functions 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 $supp\{\Gamma\}$. Let A_P be the set consisting of 1 and all natural numbers whose prime factors come from a set of primes P, then A_P is a multiplicative semigroup which is called a prime multiplicative semigroup associated to P. From [1] and [2], the support of Γ is a multiplicative prime sub-semigroup of $\mathbb{N}$.

Theorem 1.3. *([1]) Let $\Gamma = \{f_n(q)\}$ be a sequence of rational functions satisfying Functional Equation (2). Then $supp\{\Gamma\}$ is of the form A_P for some set of primes P, and Γ is completely determined by the collection of rational functions:*

$$\{f_p(q)|p \in P\}.$$

Definition 1.4. Let P be the collection of primes associated to the support A_P, in the sense of Theorem 1.2, of a sequence of rational functions Γ satisfying Functional Equation (2). Then P is called the support base of Γ.

In the reverse direction, 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:

$$f_n(q) = \begin{cases} [n]_q & \text{if } n \in A_P;\\ 0 & \text{otherwise.}\end{cases}$$

We say that a sequence Γ is nonzero if $supp\{\Gamma\} \neq \emptyset$. If Γ satisfies Functional Equation (2), then Γ is nonzero if and only if $f_1(q) = 1$ (see [3]). We say that Γ is nontrivial if Γ is nonzero and $f_n(q) \neq 1$ for at least one n in the support of Γ.

From [1] and [3], there exists a rational number t_Γ such that:

$$deg(f_n(q)) = t_\Gamma(n-1)$$

for all n in $supp\{\Gamma\}$, where $deg(f_n(q))$ denotes the degree of $f_n(q)$. Consequently, Γ is nontrivial if Γ is nonzero and $P \neq \emptyset$. The rational number t_Γ is not necessarily an integer (see [3] and [5] for an example of such a sequence). In fact, we show in [4] and [5] that t_Γ can only be non integral when the set of primes P associated to the support of Γ has the form $P = \{p\}$ for some prime p.

Definition 1.5. Let $\Gamma := \{f_n(q)|n \in \mathbb{N}\}$ be a sequence of polynomials satisfying Functional Equation (2) and let $P \neq \emptyset$ be its support base. Then Γ is called a maximal solution of Functional Equation (2) if there is no sequence $\Gamma' := \{f'_n(q)|n \in \mathbb{N}\}$ of polynomials satisfying Functional Equation (2) whose support base P' strictly contains P and

$$f_p(q) = f'_p(q)$$

for all $p \in P$. In other words, Γ is a maximal solution if it does not arise from another solution by restriction.

The following result makes it possible to work exclusively with Functional Equation (1) in constructing solutions of Functional Equation (2):

Theorem 1.6. *([3]) Let P be a set of primes. Let $\Gamma' = \{f'_p(q)|p \in P\}$ be a collection of rational functions such that:*

$$f'_{p_1}(q) \cdot f'_{p_2}(q^{p_1}) = f'_{p_2}(q) \cdot f'_{p_1}(q^{p_2})$$

for all $p_i \in P$(i.e, satisfying Functional Equation (1)). Then there exists a unique sequence $\Gamma = \{f_n(q)|n \in \mathbb{N}\}$ of polynomials satisfying Functional Equation (2) such that $f_p(q) = f'_p(q)$ for all primes $p \in P$.

For a sequence Γ of polynomials satisfying Functional Equation (2), the smallest field K which contains all the coefficients of all the polynomials in Γ is called **The Field of Coefficients of** Γ. In this paper, we are only concerned with sequences of polynomials, each of whose field of coefficients K is $\mathbb{Q}$, unless otherwise stated.

Let $\Gamma := \{f_n(q)|n \in \mathbb{N}\}$ be a sequence of rational functions satisfying Functional Equation (2). Suppose that Γ is generated by quantum integers, i.e., there exists a collection of order pairs of integers $\{(u_i, t_i)_i\}$ such that

$$f_n(q) = \prod_i ([n]_{q^{u_i}})^{t_i}$$

for all n in the support of Γ. Let us write $f_n(q)$ as

$$f_n(q) = \frac{\prod_{i,t_i>0}([n]_{q^{u_i}})^{t_i}}{\prod_{i,t_i<0}([n]_{q^{u_i}})^{t_i}}.$$

In [1], Borisov, Nathanson and Wang ask if there are simple criteria for determining when such a sequence of rational functions consists only of polynomials. As they noted, it is sufficient that

$$\prod_{i,t_i<0} ([n]_{q^{u_i}})^{t_i} = 1.$$

However, it is not necessarily so (see [1] for an example).

It is immediate that the field of coefficients of a sequence of rational functions Γ which is generated by quantum integers is necessarily equal to $\mathbb{Q}$. In the reverse direction, if P contains at least two primes, then the following result is known:

Theorem 1.7. *([1]) Let $\Gamma = \{f_n(q)|n \in \mathbb{N}\}$ be a sequence of rational functions with coefficients in $\mathbb{Q}$ that satisfies Functional Equation (2). If the support of Γ is A_P for some collections of primes P containing at least two primes, then there are*

(i) a completely multiplicative arithmetic function $\lambda(n)$ with support A_P,

(ii) a rational number t_0 such that $t_0(n-1)$ is an integer for all n in A_P,

(iii) a finite set R of positive integers and a set $\{t_r\}_{r\in R}$ of integers such that

$$f_n(q) = \lambda(n) q^{t_0(n-1)} \prod_{r\in R} ([n]_{q^r})^{t_r}$$

for all n in the support of Γ.

Similarly, if Γ only contains polynomials, we have the following reduction result:

Proposition 1.8. *([5]) Let $\Gamma = \{f_n(q)|n \in \mathbb{N}\}$ be a nonzero sequence of polynomials satisfying Functional Equation (2) with support A_P for some set of primes P. Then there exists a unique completely multiplicative arithmetic function $\psi(n)$, a rational number t, and a unique sequence $\Sigma = \{g_n(q)\}$ satisfying (2) with the same support A_P 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 $n \in A_P$.

We call the sequence of polynomials Σ in Theorem 1.8 the normalized version of the sequence of polynomials Γ.

The following results provide a link among a general solution of Functional Equation (2), its support base and quantum integers. It also allows us to classify the solutions with field of coefficients of characteristic zero ([4]).

Theorem 1.9. *([5]) Let $\Gamma = \{f_n(q)|n \in \mathbb{N}\}$ be a sequence of polynomials satisfying Functional Equation (2) and whose field of coefficients is of characteristic zero. Suppose $f_n(q)$ is a monic polynomial such that $f_n(0) \neq 0$ for each n in $\mathbb{N}$.*

(1) Field of coefficients is $\mathbb{Q}$: Suppose that $deg(f_p(q)) = t_\Gamma(p-1)$ with $t_\Gamma \geq 1$ for at least two distinct primes p and r, which means that the set P associated to the support A_P of Γ contains p and r and the elements $f_p(q)$ and $f_r(q)$ of Γ are nonconstant polynomials. Then there exist

ordered pairs of integers $\{u_i, t_i\}_i$ *with* $i = 1, \ldots, s$ *such that* $t_\Gamma = \sum_{i=1,\ldots,s} u_i t_i$ *and*

$$f_n(q) = \prod_{i=1}^{s} ([n]_{q^{u_i}})^{t_i} \tag{1.4}$$

for all n *in* $\mathbb{N}$.

(2) Field of coefficients strictly contains $\mathbb{Q}$*: There is no sequence of polynomials* Γ*, with field of coefficients strictly containing* $\mathbb{Q}$*, satisfying Functional Equation* (2) *and the condition* $deg(f_p(q)) = t_\Gamma(p-1)$*, meaning the set* P *associated to the support* A_P *of* Γ *contains all prime numbers and the correspondent elements* $f_p(q)$ *of* Γ *are nonconstant polynomials, with integral* $t_\Gamma \geq 1$ *for all primes* p*. However, if the condition* $deg(f_p(q)) = t_\Gamma(p-1)$ *with integral* $t_\Gamma \geq 1$ *for all primes* p *is not imposed on* Γ*, then there exist sequences* Γ*'s of polynomials with fields of coefficients strictly greater than* $\mathbb{Q}$ *satisfying Functional Equation* (2).

The decomposition of $f_n(q)$ *into a product of quantum integers as above is unique in the sense that if* $\{a_j, b_j\}$ *is another set of integers such that* $t_\Gamma = \sum_{j=1,\ldots,h} a_j b_j$ *and*

$$f_n(q) = \prod_{j=1}^{h} ([n]_{q^{a_j}})^{b_j}$$

for all $n \in supp\{\Gamma\}$*, then for each* u_i *there exists at least one* a_j *such that* $u_i = a_j$*. Moreover, if* $I \subseteq \{1, \ldots, s\}$ *and* $J \subseteq \{1, \ldots, h\}$ *are two collections of indexes such that* $u_i = a_j$ *exactly for all* i *in* I *and* j *in* J *and nowhere else, then*

$$\sum_{i \in I} t_i = \sum_{j \in J} b_j,$$

and the above relation between any such set of integers $\{a_j, b_j\}_j$ *and the set* $\{u_i, t_i\}_i$ *is an equivalence relation.*

Theorem 1.10. *([4]) Let* $\Gamma = \{f_n(q) | n \in \mathbb{N}\}$ *be a sequence of polynomials with field of coefficients of characteristic zero and satisfying Functional Equation* (2)*. Suppose that the set of primes* P *associated to the support of* Γ *contains at least two distinct primes. Then there exists a sequence* $\Gamma' = \{f'_n(q) | n \in \mathbb{N}\}$ *of polynomials satisfying Functional Equation* (2) *with field of coefficients equal to* $\mathbb{Q}$ *and* $supp\{\Gamma\} = supp\{\Gamma'\}$ *such that:*

- $f_n(q)$ *divides* $f'_n(q)$ *in* $\mathbb{C}[q]$ *for all* n *in* $supp\{\Gamma\}$.
- $t_{\Gamma'} - t_\Gamma \in \mathbb{N} \cup \{0\}$.

Even though Theorem 1.9 shows that a solution Γ of Functional Equation (2) with field of coefficient of characteristic zero and support base P containing all primes must be generated by quantum integers, the condition P containing all primes is too rigid to be of used. On the other hand, if the condition P containing all primes is replaced by the condition $|P| = \infty$, then it is not sufficient for such conclusion (see [6]), the next result provides exactly what we need for subsequently parts of this paper.

Theorem 1.11. *([6]) Let P be the support base of a sequence Γ of polynomials satisfying Functional Equation (2) with field of coefficients of characteristic zero. If P contains all but finitely many primes, then Γ is generated by quantum integers.*

2 Main results

Let $\Gamma = \{f_n(q)|n \in \mathbb{N}\}$ be a sequence of rational functions with coefficients in $\mathbb{Q}$ that satisfies Functional Equation (2) and let P be its support base. Then by Theorem 1.7,

$$f_n(q) = \lambda(n)q^{t_0(n-1)} \prod_{r\in R}([n]_{q^r})^{t_r}$$

for some completely multiplicative arithmetic function $\lambda(n)$ with support A_P, a rational number t_0 such that $t_0(n-1)$ is an integer for all n in A_P, a finite set R of positive integers and a set $\{t_r\}_{r\in R}$ of integers. By replacing $f_n(q)$ in Γ by the rational function

$$f'_n(q) = \frac{f_n(q)}{\lambda(n)q^{t_0(n-1)}}$$

for each $n \in A_P$, then it can be verified that the sequence $\Gamma' = \{f'_n(q)|n \in A_P\}$ satisfies Functional Equation (2). As a result, we may assume, from now on, without loss of generality that whenever $\Gamma = \{f_n(q)|n \in \mathbb{N}\}$ is a sequence of rational functions with coefficients in $\mathbb{Q}$ that satisfies Functional Equation (2), then there exists a collection of positive integers R_Γ and some collection of integers $\{t_r\}_{r\in R_\Gamma}$ such that

$$f_n(q) = \prod_{r\in R_\Gamma}([n]_{q^r})^{t_r} = \prod_{r\in R_{+,\Gamma}}([n]_{q^r})^{t_r} \prod_{r\in R_{-,\Gamma}}([n]_{q^r})^{t_r}$$

where $R_{+,\Gamma}$ and $R_{-,\Gamma}$ are subsets of R_Γ such that $t_r > 0$ and $t_r < 0$ when $r \in R_{+,\Gamma}$ and $r \in R_{-,\Gamma}$ respectively and $R_{+,\Gamma} \cup R_{-,\Gamma} = R_\Gamma$, i.e., Γ is generated by quantum integers. If Γ is generated by quantum integers, then we say that Γ is written in *reduced form* if

$$R_{+,\Gamma} \cap R_{-,\Gamma} = \emptyset.$$

By cancelling factors of the form $[n]_{q^r}$, where $r \in R_{+,\Gamma} \cap R_{-,\Gamma}$ if $R_{+,\Gamma} \cap R_{-,\Gamma} \neq \emptyset$, from the numerator and the denominator of $f_n(q)$ for each $f_n(q)$ in Γ, we may assume henceforth that Γ is already in reduced form whenever Γ is generated by quantum integers.

For the question of Borisov, Nathanson and Wang stated before, the answer is trivial if Γ is a zero or a trivial sequence or if $R_{-,\Gamma} = \emptyset$. Otherwise, the answer is contained in the following result:

Theorem 2.1. *Let $\Gamma = \{f_n(q)|n \in \mathbb{N}\}$ be a nonzero sequence of rational functions with coefficients in $\mathbb{Q}$ that satisfies Functional Equation (2) and let $P \neq \emptyset$ be its support base.*

(I) If $P = \{p\}$ for some prime p, then

$$\Gamma = \{f_{p^n}(q)|f_1(q) = 1, n \in \mathbb{N} \cup \{0\}\}$$

with $f_{p^n}(q) = f_p(q) f_{p^{n-1}}(q^p)$ for all $n \geq 1$ where $f_p(q)$ is a rational function, and Γ contains only polynomials if and only if $f_p(q)$ is a polynomial.

(II) If $|P| \geq 2$, then Γ contains only polynomials if and only if the following conditions are satisfied:

(1) (a) Let R_Γ be the collection of positive integers and $\{t_r | r \in R_\Gamma\}$ be the collection of integers such that

$$f_n(q) = \prod_{r \in R_\Gamma} ([n]_{q^r})^{t_r}.$$

Let $R_{+,\Gamma}$ and $R_{-,\Gamma}$ be defined as above. If

$$\frac{\prod_{r \in R_{+,\Gamma}} r^{t_r}}{\prod_{r \in R_{-,\Gamma}} r^{t_r}}$$

is not a (positive) integer, then Γ contains at least one non-polynomial element. The converse does not necessarily hold.

(1) (b) If there exists a positive integer $r \in R_{-,\Gamma}$ satisfying any of the following conditions:

- *r is greater than every element of $R_{+,\Gamma}$;*
- *r is divisible by a prime s which does not divide any element of $R_{+,\Gamma}$, i.e.,*

$$\frac{(\prod_{t \in R_{+,\Gamma}} t)^m}{r}$$

is not an integer for any natural number m,

then Γ does not contain only polynomials. The converse may not necessarily hold.

(2) Let p be a prime in P. For each $r \in R_\Gamma$, let $s_{p,r}$ be the highest power of p dividing r. Define

$$|R_{+,\Gamma}|_p := \{p^{s_{p,r}} \gamma \mid r \in R_{+,\Gamma}; \gamma | \frac{r}{p^{s_{p,r}}}\}$$

and

$$|R_{-,\Gamma}|_p := \{p^{s_{p,r}} \gamma \mid r \in R_{-,\Gamma}; \gamma | \frac{r}{p^{s_{p,r}}}\}$$

where multiplicity is allowed according to the following rules: For each r in R_Γ, $p^{t_{p,r}}\gamma$ appears $|t_r|$ times in $|R_{+,\Gamma}|_p$ (resp. in $|R_{-,\Gamma}|_p$)) if $t_r > 0$ (resp. if $t_r < 0$) for each r (from this point on, we always write $|t_r|$ as t_r, in the context of multiplicity, with the absolute value implicitly understood to avoid the cumbersome of notation and to avoid the confusion with the similar notation in $|R_{-,\Gamma}|_p$ and $|R_{+,\Gamma}|_p$).

If $R_{-,\Gamma} \neq \emptyset$, then Γ contains only polynomials if and only if

$$|R_{-,\Gamma}|_p \subseteq |R_{+,\Gamma}|_p \tag{2.1}$$

for all p in P. Furthermore, the followings also hold:

- *If (1)(b) holds, then* Γ *contains only polynomials if and only if (2.1) holds for all* p *in* P *which divide some* r *in* $R_{+,\Gamma}$.

- *If every prime* p *in* P *does not divide* r *for any* r *in* R_Γ*, i.e., if*

$$(\prod_{p\in P} p, \prod_{r\in R_\Gamma} r) = 1,$$

then Γ *contains only polynomials if and only if (2.1) is satisfied for any* p *in* P.

Our next result concerns maximal solutions of Functional Equation (2). In [2], Nathanson poses, as Problem 6, the following problem:

Problem: Describe the maximal solutions of Functional Equation (2). For what sets of primes P does there exist a maximal solution with support base P?

Our result concerning this problem can be summarized as follows:

Theorem 2.2. *(i) If* $P = \{p\}$ *for some prime* p*, then there always exists infinitely many maximal solutions* Γ *of Functional Equation* (2) *with support base* P*. If* Γ_0 *is a sequence of polynomials, satisfying Functional Equation* (2) *with field of coefficients of characteristic zero and support base* P*, whose normalized version is sequence of the form*

$$\Gamma = \{f_{p^n}(q) | f_1(q) = 1, n \in \mathbb{N}\}$$

with $f_{p^n}(q) = f_p(q) f_{p^{n-1}}(q^p)$ *for all* $n \geq 1$ *where* $f_p(q)$ *is a monic polynomial with nonzero constant term satisfying either of the following conditions:*

1. $f_p(q)$ *possesses at least one root which is not a root of unity.*

2. *If all roots of* $f_p(q)$ *are roots of unity, then* $f_p(q)$ *possesses at least one roots of unity whose order is not divisible by* p.

Then Γ *and thus* Γ_0 *must be a maximal solution. If* Γ *is a normalized version of a maximal solution of Functional Equation* (2) *with support base* $P = \{p\}$ *for some prime* p *and with field of coefficients* $\mathbb{Q}$*, then* Γ *must also be of the form above.*

(ii) Suppose $|P| \geq 2$*, where* $|\cdot|$ *denotes the cardinality of the set* P*. If* P *has finite complement, i.e., there are at most finitely many primes which are not in* P*, then there exists at least one maximal solution with support base* P*. If* Γ *is a maximal solution of Functional Equation* (2) *with support base* P *and if the field of coefficients of* Γ *is* $\mathbb{Q}$*, then* P *has finite complement. If* P *is a set of primes with nonempty finite complement, then a maximal solution has the form*

$$\Gamma = \{f_n(q) = \prod_{r\in R} ([n]_{q^r})^{t_r} = \prod_{r\in R_{-,\Gamma}} ([n]_{q^r})^{t_r} \prod_{r\in R_{+,\Gamma}} ([n]_{q^r})^{t_r} | n \in A_P\}$$

where:

- $R_{-,\Gamma} \neq \emptyset$.
- *For each prime p in the complement of P, $|R_{-,\Gamma}|_p$ is not a subset of $|R_{+,\Gamma}|_p$.*

Furthermore, if there exists one maximal solution with support base P containing at least two primes and with field of coefficients $\mathbb{Q}$, then there are infinitely many such maximal solutions with support base P.

Remark 2.3. The conditions (1) (a) and (b) of (II) of Theorem 2.1 are weaker than condition (2) of Theorem 2.1 since they are necessary but not sufficient for an affirmative conclusion. However, it is simple and effective to check for negative conclusion. In (2) of (II) of Theorem 2.1, for each r in R_Γ, $p^{s_{p,r}}\gamma$ occurs t_r times in $|R_{+,\Gamma}|_p$ (resp. $|R_{-,\Gamma}|_p$) if $t_r > 0$ (resp. if $t_r < 0$) does not mean that the value $m = p^{s_{p,r}}\gamma$ occurs exactly t_r times in $|R_{+,\Gamma}|_p$ (resp. $|R_{-,\Gamma}|_p$). This is because if $s_{p,r_1} = s_{p,r_2}$ for some r_1 and r_2 in R_Γ such that both are in $R_{+,\Gamma}$ (or $R_{-,\Gamma}$), then $p^{s_{p,r_1}}$ occurs t_{r_1} times and $p^{s_{p,r_2}}$ occurs t_{r_2} times, and thus $v = p^{s_{p,r_1}} = p^{s_{p,r_2}}$ ($\gamma = 1$) occurs at least $t_{r_1} + t_{r_2}$ times in $|R_{+,\Gamma}|_p$ (or in $|R_{-,\Gamma}|_p$). In (i) of (II) of Theorem 2.2, Γ is normalized so that $f_p(q)$ does not possess any root equal to zero, i.e., all roots of $f_p(q)$ are nonzero. Hence condition (1) of (i) says that $f_p(q)$ contains at least one non-zero root which is not a root of unity. In a future paper, we will address the lifting of the condition, which we impose on some parts of (i) and (ii) of Theorem 2.2 concerning the fields of coefficients of a maximum solution Γ being $\mathbb{Q}$, in the case where the field of coefficients is of characteristic zero.

We conclude this section with the following:

Problems:

(1) Suppose Γ is a maximal solution of Functional Equation (2) with support base $P = \{p\}$ for some prime p and with field of coefficients different from $\mathbb{Q}$. Must Γ have the form described in (i) of Theorem 2.2?

(2) Suppose Γ is a maximal solution of Functional Equation (2) with support base P containing at least two primes. Suppose that the field of coefficients of Γ is not $\mathbb{Q}$. Must P have finite complement?

(3) If P contains at least two primes and if there exists one maximal solution to Functional Equation (2) with support base P and field of coefficients strictly contains $\mathbb{Q}$, then does that implies there are infinitely many such solutions?

3 Proof of results

Proof. (Proof of Theorem 2.1)

Let $\Gamma = \{f_n(q) | n \in \mathbb{N}\}$ be a nontrivial sequence of rational functions, with field of coefficients $\mathbb{Q}$, which satisfies Functional Equation (2) and let $P \neq \emptyset$ be its support base.

(I) Suppose $P = \{p\}$ for some prime p. Then Γ is nontrivial. The support of Γ, A_P, must have the form $\{p^n | n \in \mathbb{N} \cup \{0\}\}$ for the prime p in P. Since Γ satisfies Functional Equation (2),

$$f_{p^n}(q) = f_p(q) f_{p^{n-1}}(q^p) \tag{3.1}$$

where $f_p(q)$ is the rational function in Γ indexed by p. As a result, each rational function $f_{p^n}(q)$ is determined by $f_p(q)$ by induction. Therefore,

$$\Gamma = \{f_{p^n}(q) | f_0(q) = 1, n \in \mathbb{N} \cup \{0\}\}$$

with $f_{p^n}(q) = f_p(q) f_{p^{n-1}}(q^p)$ for all $n \in A_P$, and Γ contains only polynomials if and only if $f_p(q)$ is a polynomial. Therefore, (I) follows if we prove that (3.1) gives in fact a well-defined formula for $f_{p^n}(q)$ for each $n \in \mathbb{N}$. This follows from the lemma below:

Lemma 3.1. *Let n be any natural number. Let u and v be nonnegative integers such that $u + v = n$. Then*

$$f_{p^n}(q) = f_{p^u}(q) f_{p^v}(q^{p^u}) = f_{p^v}(q) f_{p^u}(q^{p^v}). \tag{3.2}$$

Proof. Without loss of generality, we may assume that $u \geq 1$ and $v \geq 1$ because if either of them is equal to 0, then (3.4) becomes $f_{p^n}(q) = f_{p^n}(q)$. We prove this lemma by induction on n:

(1) For $n = 2$, (3.2) becomes

$$f_{p^2}(q) = f_p(q) f_p(q^p) = f_p(q) f_p(q^p)$$

which holds because of (3.1).

(2) It can be verified from (3.1) and the induction hypothesis that

$$f_{p^n}(q) = f_p(q) f_{p^{n-1}}(q^p) = f_p(q) f_{p^{u-1}}(q^p) f_{p^v}((q^p)^{p^{u-1}}) = f_{p^u}(q) f_{p^v}(q^{p^u}).$$

Similarly,

$$f_{p^n}(q) = f_p(q) f_{p^{n-1}}(q^p) = f_p(q) f_{p^{v-1}}(q^p) f_{p^u}((q^p)^{p^{v-1}}) = f_{p^v}(q) f_{p^u}(q^{p^v}).$$

Therefore,

$$f_{p^n}(q) = f_{p^u}(q) f_{p^v}(q^{p^u}) = f_{p^v}(q) f_{p^u}(q^{p^v})$$

for all nonnegative integers u and v. In particular, the sequence of rational functions

$$\Gamma := \{f_{p^n}(q) | n \in \mathbb{N} \cup \{0\}\}$$

satisfies Functional Equation (2).

□

(II) Suppose $|P| \geq 2$. First we prove (2). Then we show that (2) implies (1).

By the normalization discussed earlier, there exists a collection of positive integers $R = R_{+,\Gamma} \cup R_{-,\Gamma}$ and a collection of positive integers $\{t_r | r \in R\}$ such that

$$f_n(q) = \prod_{r \in R_{+,\Gamma}} ([n]_{q^r})^{t_r} \prod_{r \in R_{-,\Gamma}} ([n]_{q^r})^{t_r}$$

for all n in the support A_P of Γ. If $R_{-,\Gamma} = \emptyset$, then it follows immediately that $f_n(q) \in \mathbb{Q}[q]$ for all n in the support A_P and there is nothing to prove. Hence we may assume that $R_{-,\Gamma} \neq \emptyset$. Let

us consider the collection of rational functions

$$\Gamma_P = \{f_p(q) = \prod_{r \in R_{+,\Gamma}} ([p]_{q^r})^{t_r} \prod_{r \in R_{-,\Gamma}} ([p]_{q^r})^{t_r} \mid p \in P\}.$$

It can be verified from Functional Equation (2) that part (2) of Theorem 2.1 will follow if we can show that $f_p(q)$ is a polynomial for each $p \in P$ if and only if it satisfies the condition described in (2) of (II) of Theorem 2.1.

First let us prove a weaker statement: Γ contains only polynomials if and only if (2.1) holds for all p in P.

$(\Rightarrow)$ Suppose that

$$|R_{-,\Gamma}|_p \subseteq |R_{+,\Gamma}|_p$$

for all p in P.

Lemma 3.2. *Let p be any prime and let r be a positive integers.*

(1) If p does not divide r, then

$$[p]_{q^r} = \prod_{\gamma \in \Sigma_r} P_{p\gamma}(q)$$

where Σ_r is the collection of all distinct divisors of r, and $P_{p\gamma}(q)$ is the irreducible monic cyclotomic polynomial of order $p\gamma$ with coefficients in $\mathbb{Q}$.

(2) If p divides r, then

$$[p]_{q^r} = \prod_{\gamma \in \Sigma_r} P_{p^{z+1}\gamma}(q)$$

where Σ_r is the collection of all distinct divisors of $\frac{r}{p^z}$, p^z is the highest power of p dividing r and $P_{p^{z+1}\gamma}(q)$ is the irreducible monic cyclotomic polynomial of order $p^{z+1}\gamma$ with coefficients in $\mathbb{Q}$.

Proof. (1) Suppose p does not divide r. Let u be a positive integer and let $P_u(q)$ be the cyclotomic polynomial in $\mathbb{Q}[q]$ of order u, i.e., $P_u(q)$ is the irreducible (in $\mathbb{Q}[q]$) monic polynomial in $\mathbb{Q}[q]$ whose roots are all distinct primitive u-roots of unity. Let Σ_r be the collection of all distinct divisors of r . Since

$$[p]_{q^r} = \frac{q^{pr} - 1}{q^r - 1},$$

the roots of $[p]_{q^r}$, viewed as a polynomial in q, are all distinct pr-roots of unity which are not r-roots of unity. Since p does not divide r, the collection of all roots of $[p]_{q^r}$ must consist of all the roots of unity of order $p\gamma$ where γ divides r. As a result,

$$[p]_{q^r} = \prod_{\gamma \in \Sigma_r} P_{p\gamma}(q).$$

(2) Suppose p divides r. Let z be the highest power of p dividing r and let Π_r denote the collection of all distinct divisors of $\frac{r}{p^z}$. Since p divides r, it can be verified using the same argument as in (1) that the collection of all roots of $[p]_{q^r}$ must consist of all the roots of unity of

order $p^{z+1}\gamma$ where γ divides $\frac{r}{p^z}$. Then

$$[p]_{q^r} = \prod_{\gamma \in \Pi_r} P_{p^{z+1}\gamma}(q).$$

□

Let p be any prime in P. It can be verified from (1) and (2) of Lemma 3.2 and the definition of $|R_{+,\Gamma}|_p$ that

$$\prod_{r \in R_{+,\Gamma}} ([p]_{q^r})^{t_r} = \prod_{r \in R_{+,\Gamma}} \prod_{\gamma \in \Pi_r} (P_{p^{z+1}\gamma}(q))^{t_r} = \prod_{\omega \in |R_{+,\Gamma}|_p} P_\omega(q)$$

where Π_r is the collection of all distinct divisors of $\frac{r}{p^z}$. Similarly, it can also be verified that

$$\prod_{r \in R_{-,\Gamma}} ([p]_{q^r})^{t_r} = \prod_{r \in R_{-,\Gamma}} \prod_{\gamma \in \Pi_r} (P_{p^{z+1}\gamma}(q))^{t_r} = \prod_{\omega \in |R_{-,\Gamma}|_p} P_\omega(q).$$

As a result,

$$\begin{aligned} f_p(q) &= \prod_{r \in R_\Gamma} ([p]_{q^r})^{t_r} \\ &= \prod_{r \in R_{+,\Gamma}} ([p]_{q^r})^{t_r} \prod_{r \in R_{-,\Gamma}} ([p]_{q^r})^{t_r} \\ &= \frac{\prod_{\omega \in |R_{+,\Gamma}|_p} P_\omega(q)}{\prod_{\omega \in |R_{-,\Gamma}|_p} P_\omega(q)}. \end{aligned}$$

Hence, $f_p(q)$ is a polynomial since

$$|R_{-,\Gamma}|_p \subseteq |R_{+,\Gamma}|_p$$

for each p in P. Therefore, Γ contains only polynomials.

($\Leftarrow$) Suppose Γ contains only polynomials and $R_{-,\Gamma} \neq \emptyset$. Then $f_p(q)$ is a polynomial for all primes p in P. As above, we have

$$f_p(q) = \frac{\prod_{\omega \in |R_{+,\Gamma}|_p} P_\omega(q)}{\prod_{\omega \in |R_{-,\Gamma}|_p} P_\omega(q)}$$

for all p in P. Since $P_\omega(q)$ is irreducible,

$$|R_{-,\Gamma}|_p \subseteq |R_{+,\Gamma}|_p$$

for each p in P.

Now to see that condition (2) implies (1)(a) and (1)(b), it suffices if we show that the weaker statement above implies (1)(a) and (1)(b).

To prove (1)(b), suppose that there exists an element r in $R_{-,\Gamma}$ such that r is greater than every element of $R_{+,\Gamma}$. Then it can be verified from the definitions of $|R_{-,\Gamma}|_t$ and $|R_{+,\Gamma}|_t$ that r is in $|R_{-,\Gamma}|_t$ but r is not in $|R_{+,\Gamma}|_t$ for every t in P. Similarly, if there exists an element r in $R_{-,\Gamma}$ such that r is divisible by a prime p which does not divide any element of $R_{+,\Gamma}$, then it can be verified that $t^{s_{t,r}}p$, where $s_{t,r}$ is the highest power of t dividing r, is in $|R_{-,\Gamma}|_t$ but not in $|R_{+,\Gamma}|_t$ for every t in P. Therefore, if either of the conditions in (1)(b) occurs, then it can be verified that $|R_{-,\Gamma}|_t$ is not a subset of $|R_{+,\Gamma}|_t$. This contradicts our assumption that condition (2) holds and thus the result follows.

To show that (1)(a) also follows from condition (2), suppose that (2.1) holds for all primes p in P and

$$\frac{\prod_{r\in R_{+,\Gamma}} r^{t_r}}{\prod_{r\in R_{-,\Gamma}} r^{t_r}}$$

is not an integer. Then there exists a prime s with s dividing some element r in $R_{-,\Gamma}$ and a positive integer n such that s^n divides $\prod_{r\in R_{-,\Gamma}} r^{t_r}$ but does not divide $\prod_{r\in R_{+,\Gamma}} r^{t_r}$. Let

$$\Phi_{R_{-,\Gamma}} := \{r_i \in R_{-,\Gamma} \mid s|r_i\}.$$

For each r_i in Φ, let e_i be the highest power of s dividing r_i. Then

$$\prod_{r_i\in\Phi_{R_{-,\Gamma}}} s^{e_i t_{r_i}} = s^n.$$

Note that s must also divide some element r' in $R_{+,\Gamma}$ since (1)(b) holds (see above). Choose a prime p in P such that $p \neq s$ (this can be done since P contains at least two primes by hypothesis). Let

$$\Phi_{R_{+,\Gamma}} := \{r_j \in R_{+,\Gamma} \mid s|r_j\}.$$

For each r_j in $\Phi_{R_{+,\Gamma}}$, let g_i be the highest power of s dividing r_j. Then

$$\prod_{r_j\in\Phi_{R_{+,\Gamma}}} s^{g_j t_{r_j}} = s^m$$

for some integer $m < n$. Let r_i be any element of $\Phi_{R_{-,\Gamma}}$. Let $l_{|R_{-,\Gamma}|_p}$ and $l_{|R_{-,\Gamma}|_p}$ be the multiplicities of $p^{s_{p,r_i}}s^{e_i}$ in $|R_{-,\Gamma}|_p$ and $|R_{+,\Gamma}|_p$ respectively where s_{p,r_i} is the highest power of p dividing r_i. From the hypothesis $|R_{-,\Gamma}|_p \subseteq |R_{+,\Gamma}|_p$, we have:

$$l_{|R_{-,\Gamma}|_p} \leq l_{|R_{+,\Gamma}|_p}.$$

It can be verified that this implies $m \geq n$ (the details are left to the reader), which contradicts our assumption. Thus the result follows. This shows that if Γ contains only polynomials, then it is necessary that conditions (1)(a) and (1)(b) are satisfied.

Lemma 3.3. *(1) If each prime t in P does not divide r for any r in R_Γ, then Γ contains only polynomials if and only if (2.1) is satisfied for any t in P.*

(2) If (1)(b) is satisfied and (2.1) holds for at least one prime p in P which divides r for some

$r \in R_{+,\Gamma}$, then (2.1) holds for all primes t which do not divide any r in $R_{+,\Gamma}$, and thus (2.1) holds for all t in P which do not divide r for any r in R_Γ.

Proof. (1) If each prime p in P does not divide r for any r in R_Γ and if Γ contains only polynomials, then (2.1) holds for all primes p in P by the proof above. To prove the other direction, suppose that every prime t in P does not divide r for any r in R_Γ and suppose that (2.1) holds for one prime p in P. To show that Γ contains only polynomials, it is sufficient for us to show that if (2.1) holds for p, then (2.1) holds for all primes t in P in this case. For this, it suffices for us to prove the following statements:

$$|R_{+,\Gamma}|_{p_i} = |R_{+,\Gamma}|_{p_j}$$

and

$$|R_{-,\Gamma}|_{p_i} = |R_{-,\Gamma}|_{p_j}$$

for any primes p_i and p_j in P. By assumption, $s_{t,r} = 0$ for all t in P and all r in R_Γ. In particular, $s_{p,r} = 0$ for all r in R_Γ by above. It follows from the definitions of $|R_{+,\Gamma}|_p$ and $|R_{-,\Gamma}|_p$ that

$$|R_{+,\Gamma}|_p = \{\gamma \mid \gamma | r, r \in R_{+,\Gamma}\} \tag{3.3}$$

and

$$|R_{-,\Gamma}|_p = \{\gamma \mid \gamma | r, r \in R_{-,\Gamma}\} \tag{3.4}$$

with γ appearing t_r times in $|R_{+,\Gamma}|_p$ (resp. in $|R_{-,\Gamma}|_p$) for each r in $R_{+,\Gamma}$ (resp. $R_{-,\Gamma}$) divisible by γ. Since the right hand sides of (3.3) and (3.4) are independent of p, (1) follows.

(2) Suppose (1)(b) holds. Then it follows immediately that if s is prime in P dividing r for some r in $R_{-,\Gamma}$, then s divides r for some prime r in $R_{+,\Gamma}$. Suppose that there exists one prime t in P such that t divides r for some r in $R_{+,\Gamma}$ and

$$|R_{-,\Gamma}|_t \subseteq |R_{+,\Gamma}|_t$$

holds. Let p be any prime such that p does not divide any element r in R_Γ (or equivalently, in $R_{+,\Gamma}$ since (1)(b) holds). Then we need to show:

$$|R_{-,\Gamma}|_p \subseteq |R_{+,\Gamma}|_p.$$

Write

$$|R_{+,\Gamma}|_t := \{t^{s_{t,r}}\gamma \mid r \in R_{+,\Gamma}; \gamma | \frac{r}{t^{s_{t,r}}}\} = \{t^{s_{t,r}}\gamma \mid r \in R^{(1)}_{+,\Gamma}; \gamma | \frac{r}{t^{s_{t,r}}}\} \cup \{\gamma \mid r \in R^{(2)}_{+,\Gamma}; \gamma | r\}$$

and

$$|R_{-,\Gamma}|_t := \{t^{s_{t,r}}\gamma \mid r \in R_{-,\Gamma}; \gamma | \frac{r}{t^{s_{t,r}}}\} = \{t^{s_{t,r}}\gamma \mid r \in R^{(1)}_{-,\Gamma}; \gamma | \frac{r}{t^{s_{t,r}}}\} \cup \{\gamma \mid r \in R^{(2)}_{-,\Gamma}; \gamma | r\}$$

where:

- $t^{s_{t,r}}\gamma$ appears t_r times in $|R_{+,\Gamma}|_t$ (resp. in $|R_{-,\Gamma}|_t$) if $t_r > 0$ (resp. if $t_r < 0$).

- $R^{(1)}_{+,\Gamma}$ (resp. $R^{(1)}_{-,\Gamma}$) consists of all r in $R_{+,\Gamma}$ (resp. in $R_{-,\Gamma}$) which are divisible by t.
- $R^{(2)}_{+,\Gamma}$ (resp. $R^{(2)}_{-,\Gamma}$) consists of all r in $R_{+,\Gamma}$ (resp. in $R_{-,\Gamma}$) which are not divisible by t.

Since the above unions are disjoint as well as

$$\{t^{s_{t,r}}\gamma \mid r \in R^{(1)}_{+,\Gamma}; \gamma|\frac{r}{t^{s_{t,r}}}\} \cap \{\gamma \mid r \in R^{(2)}_{-,\Gamma}; \gamma|r\} = \emptyset,$$

$$\{t^{s_{t,r}}\gamma \mid r \in R^{(1)}_{-,\Gamma}; \gamma|\frac{r}{t^{s_{t,r}}}\} \cap \{\gamma \mid r \in R^{(2)}_{+,\Gamma}; \gamma|r\}$$

and

$$\{t^{s_{t,r}}\gamma \mid r \in R^{(1)}_{-,\Gamma}; \gamma|\frac{r}{t^{s_{t,r}}}\} \cap \{\gamma \mid r \in R^{(2)}_{-,\Gamma}; \gamma|r\} = \emptyset,$$

it follows that

$$\{\gamma \mid r \in R^{(2)}_{+,\Gamma}; \gamma|r\} \supseteq \{\gamma \mid r \in R^{(2)}_{-,\Gamma}; \gamma|r\}$$

and

$$\{t^{s_{t,r}}\gamma \mid r \in R^{(1)}_{+,\Gamma}; \gamma|\frac{r}{t^{s_{t,r}}}\} \supseteq \{t^{s_{t,r}}\gamma \mid r \in R^{(1)}_{-,\Gamma}; \gamma|\frac{r}{t^{s_{t,r}}}\}.$$

We can also write

$$|R_{+,\Gamma}|_p := \{\gamma \mid r \in R_{+,\Gamma}; \gamma|r\} = \{\gamma \mid r \in R^{(1)}_{+,\Gamma}; \gamma|r\} \cup \{\gamma \mid r \in R^{(2)}_{+,\Gamma}; \gamma|r\}$$

and

$$|R_{-,\Gamma}|_p := \{\gamma \mid r \in R_{-,\Gamma}; \gamma|r\} = \{\gamma \mid r \in R^{(1)}_{-,\Gamma}; \gamma|r\} \cup \{\gamma \mid r \in R^{(2)}_{-,\Gamma}; \gamma|r\}$$

since $s_{p,r} = 0$ for all r in R_Γ by assumption. Note that these unions are not necessarily disjoint. It can be verified from above that it suffices for us to prove:

$$\mathcal{U} = \{\gamma \mid r \in R^{(1)}_{+,\Gamma}; \gamma|r\} \cup \{\gamma \mid r \in R^{(2)}_{+,\Gamma}; \gamma|r\} - \{\gamma \mid r \in R^{(2)}_{-,\Gamma}; \gamma|r\}$$

$$\supseteq \{\gamma \mid r \in R^{(1)}_{-,\Gamma}; \gamma|r\} = \mathcal{V}.$$

Let us suppose the contrary. Then there exists an element γ_0 in $\mathcal{V}$ such that γ_0 appears with greater multiplicity in $\mathcal{V}$ than it does in $\mathcal{U}$. It can be verified that γ_0 is of the form $t^w\gamma'$ where $w \in \{0, \ldots, s_{t,r}\}$ and γ' divides $\frac{r}{t^{s_{t,r}}}$ for some r in $R^{(1)}_{-,\Gamma}$ such that $w \leq s_{t,r}$. Let $\mathcal{W}_\mathcal{V}$ (resp. $\mathcal{W}_\mathcal{U}$) denote the collection of all r in $R^{(1)}_{-,\Gamma}$ (resp. in $R^{(1)}_{+,\Gamma}$) such that γ_0 divides r, or equivalently, such that $s_{t,r} \geq w$ and γ' divides $\frac{r}{t^{s_{t,r}}}$.

There are two cases:

(i) $w \in \{1, \ldots, s_{t,r}\}$: It can be verified that the following statements hold:

- γ_0 must occur in $\{\gamma \mid r \in R^{(1)}_{+,\Gamma}; \gamma|r\}$ if γ_0 occurs in $\mathcal{U}$.
- The multiplicity of γ_0 in $\mathcal{V}$ is equal to the its multiplicity in $|R_{-,\Gamma}|_p$.
- The multiplicity of γ_0 in $\mathcal{U}$ is equal to the its multiplicity in $|R_{+,\Gamma}|_p$.

Let m_- denote the multiplicity of $t^w\gamma'$ in $|R_{-,\Gamma}|_p$ and m_+ denote its multiplicity in $|R_{+,\Gamma}|_p$. Then $m_- > m_+$ by assumption. It can be verified that

$$m_- = \sum_{\{r\in R_{-,\Gamma}|s_{t,r}\geq w;\gamma'|\frac{r}{t^{s_{t,r}}}\}} t_r = \sum_{\{r\in R_{-,\Gamma}|r\in\mathcal{W}_\mathcal{V}\}} t_r$$

and

$$m_+ = \sum_{\{r\in R_{+,\Gamma}|s_{t,r}\geq w;\gamma'|\frac{r}{t^{s_{t,r}}}\}} t_r = \sum_{\{r\in R_{+,\Gamma}|r\in\mathcal{W}_\mathcal{U}\}} t_r.$$

Write

$$\mathcal{W}_\mathcal{V} = \bigcup_i \mathcal{W}_\mathcal{V}^{(i)}$$

as a disjoint union where $\mathcal{W}_\mathcal{V}^{(i)} := \{r \in \mathcal{W}_\mathcal{V} \mid s_{t,r} = v_i\}$ for some positive integer v_i, and

$$\mathcal{W}_\mathcal{U} = \bigcup_i \mathcal{W}_\mathcal{U}^{(i)}$$

as a disjoint union where $\mathcal{W}_\mathcal{U}^{(i)} := \{r \in \mathcal{W}_\mathcal{U} \mid s_{t,r} = u_i\}$ for some positive integer u_i. Since $|R_{-,\Gamma}|_t \subseteq |R_{+,\Gamma}|_t$, it can be verified that:

$$\{v_i \mid s_{t,r} = v_i; r \in \mathcal{W}_\mathcal{V}^{(i)}\} \subseteq \{u_i \mid s_{t,r} = u_i; r \in \mathcal{W}_\mathcal{U}^{(i)}\},$$

and

$$\sum_{r\in\mathcal{W}_\mathcal{V}^{(i)}} t_r \leq \sum_{r\in\mathcal{W}_\mathcal{U}^{(i)}} t_r$$

if $v_i = u_i$. Therefore,

$$m_- = \sum_i \sum_{r\in\mathcal{W}_\mathcal{V}^{(i)}} t_r \leq \sum_i \sum_{r\in\mathcal{W}_\mathcal{U}^{(i)}} t_r = m_+$$

which contradicts our assumption.

(ii) $w = 0$: Let us show that the multiplicity of γ_0 in $\mathcal{V}$ is at most its multiplicity in the subset $\{\gamma \mid r \in R_{+,\Gamma}^{(1)}; \gamma|r\}$ of $\mathcal{U}$. Let m_- denote the multiplicity of γ_0 in $\mathcal{V}$, m_+ denote its multiplicity in $\{\gamma \mid r \in R_{+,\Gamma}^{(1)}; \gamma|r\}$ and m represent its multiplicity in $\mathcal{U}$. Hence $m_+ \leq m$. Also, $m_- > m$ by the assumption about γ_0. Let $\mathcal{G}_\mathcal{V}$ (resp. $\mathcal{G}_\mathcal{U}$) denote the collection of r in $R_{-,\Gamma}^{(1)}$ (resp. in $R_{+,\Gamma}^{(1)}$) such that γ_0 divides r, or equivalently, such that $s_{t,r} \geq w$ and γ' divides $\frac{r}{t^{s_{t,r}}}$. It can be verified that

$$m_- = \sum_{\{r\in R_{-,\Gamma}^{(1)}|s_{t,r}\geq w;\gamma'|\frac{r}{t^{s_{t,r}}}\}} t_r = \sum_{\{r\in R_{-,\Gamma}^{(1)}|\gamma'|\frac{r}{t^{s_{t,r}}}\}} t_r = \sum_{\{r\in R_{-,\Gamma}|r\in\mathcal{G}_\mathcal{V}\}} t_r$$

and

$$m_+ = \sum_{\{r\in R_{+,\Gamma}^{(1)}|s_{t,r}\geq w;\gamma'|\frac{r}{t^{s_{t,r}}}\}} t_r = \sum_{\{r\in R_{+,\Gamma}^{(1)}|\gamma'|\frac{r}{t^{s_{t,r}}}\}} t_r = \sum_{\{r\in R_{+,\Gamma}|r\in\mathcal{G}_\mathcal{U}\}} t_r.$$

Similarly as in case (i), write

$$\mathcal{G}_{\mathcal{V}} = \bigcup_i \mathcal{G}_{\mathcal{V}}^{(i)}$$

as a disjoint union where

$$\mathcal{G}_{\mathcal{V}}^{(i)} := \{r \in \mathcal{G}_{\mathcal{V}} \mid s_{t,r} = v_i\}$$

for some positive integer v_i, and

$$\mathcal{G}_{\mathcal{U}} = \bigcup_i \mathcal{G}_{\mathcal{U}}^{(i)}$$

as a disjoint union where

$$\mathcal{G}_{\mathcal{U}}^{(i)} := \{r \in \mathcal{G}_{\mathcal{U}} \mid s_{t,r} = u_i\}$$

for some positive integer u_i. It can be verified from the relation stated earlier, namely

$$\{t^{s_{t,r}}\gamma \mid r \in R_{-,\Gamma}^{(1)}; \gamma|\frac{r}{t^{s_{t,r}}}\} \subseteq \{t^{s_{t,r}}\gamma \mid r \in R_{+,\Gamma}^{(1)}; \gamma|\frac{r}{t^{s_{t,r}}}\},$$

that

$$\{v_i \mid s_{t,r} = v_i; r \in \mathcal{G}_{\mathcal{V}}^{(i)}\} \subseteq \{u_i \mid s_{t,r} = u_i; r \in \mathcal{G}_{\mathcal{U}}^{(i)}\},$$

and

$$\sum_{r \in \mathcal{G}_{\mathcal{V}}^{(i)}} t_r \leq \sum_{r \in \mathcal{G}_{\mathcal{U}}^{(i)}} t_r$$

if $v_i = u_i$. Therefore,

$$m_- = \sum_i \sum_{r \in \mathcal{G}_{\mathcal{V}}^{(i)}} t_r \leq \sum_i \sum_{r \in \mathcal{G}_{\mathcal{U}}^{(i)}} t_r = m_+ \leq m$$

which also contradicts our assumption.

As a result,

$$|R_{-,\Gamma}|_p \subseteq |R_{+,\Gamma}|_p$$

and the proof of Lemma 3.3 is complete.

□

Therefore, if (1)(b) is satisfied and (2.1) holds for all primes t in P which divide some r in $R_{+,\Gamma}$, then (2.1) also holds for all primes t which do not divide any r in $R_{+,\Gamma}$. Therefore, (2.1) holds for all primes p in P, and thus Γ contains only polynomials.

To complete the proof of Theorem 2.1, we need to show that the converses of (1)(a) and (1)(b) do not necessarily hold. That is to show that there exist sequences Γ of rational functions satisfying the hypothesis of Theorem 2.1 such that Γ satisfies either condition (1)(a) or condition (1)(b) of Theorem 2.1 but they contain rational functions which are not polynomials. For this, see examples (1) and (2) below.

□

Some application examples: The following examples illustrate various situations concerning Theorem 2.1.

(1) $\Gamma := \{f_n(q) = \frac{[n]_{q^2}([n]_{q^5})^3}{[n]_{q^3}} \mid n \in A_P\}$ where $P = \{2, 3, 5\}$.
Since

$$\frac{\prod_{r \in R_{+,\Gamma}} r^{t_r}}{\prod_{r \in R_{-,\Gamma}} r^{t_r}} = \frac{2.5^3}{3}$$

is not a positive integer, Γ does not contain only polynomials by condition (1) (a) of Theorem 2.1, a fact which can be verified by direct computation or by noticing that the polynomial which is the numerator of

$$f_3(q) = \frac{[3]_{q^2}([3]_{q^5})^3}{[3]_{q^3}}$$

does not possess any primitive 9-root of unity while the polynomial which is the denominator of $f_3(q)$ does.

(2) $\Gamma := \{f_n(q) = \frac{[n]_{q^2}([n]_{q^3})^3}{[n]_{q^6}} \mid n \in A_P\}$ where $P = \{2, 3, 5\}$. Then

$$\frac{\prod_{r \in R_{+,\Gamma}} r^{t_r}}{\prod_{r \in R_{-,\Gamma}} r^{t_r}} = \frac{2.3^3}{6}$$

is a positive integer. However, since $6 > 2, 3$, Γ does not contain only polynomials by condition 1 (b) of Theorem 2.1. This conclusion can easily be seen to be correct since the polynomial

$$[5]_{q^6} = \frac{q^{30} - 1}{q^6 - 1}$$

possesses at least one primitive 30-roots of unity while the polynomial

$$[5]_{q^2}([5]_{q^3})^3 = \frac{q^{10} - 1}{q^2 - 1}\left(\frac{q^{15} - 1}{q^3 - 1}\right)^3$$

does not.

(3) $\Gamma := \{f_n(q) = \frac{[n]_{q^6}[n]_{q^9}}{[n]_{q^2}([n]_{q^3})^3} \mid n \in A_P\}$ where $P = \{2, 3, 5\}$. Then

$$\frac{\prod_{r \in R_{+,\Gamma}} r^{t_r}}{\prod_{r \in R_{-,\Gamma}} r^{t_r}} = \frac{6.9}{2.3^3} = 1$$

is a positive integer. Moreover, no element in $R_{-,\Gamma}$ is greater than every element of $R_{+,\Gamma}$. To check condition (2), we have

- $R_{+,\Gamma} = \{6, 9\}$ with $t_6 = 1$ and $t_9 = 1$.
- $R_{-,\Gamma} = \{2, 3\}$ with $t_2 = 1$ and $t_3 = 3$.

However,

$$|R_{-,\Gamma}|_3 = \{1, 2, 3.1, 3.1, 3.1\}$$

which is not a subset of

$$|R_{+,\Gamma}|_3 = \{3.1, 3.2, 3^2.1\}.$$

Hence Γ does not contain all polynomials. This can also be seen directly by noting that the numerator of

$$f_3(q) = \frac{[3]_{q^6}[3]_{q^9}}{[3]_{q^2}([3]_{q^3})^3}$$

does not posses any primitive 6-root of unity while the denominator, $[3]_{q^2}([3]_{q^3})^3$, does. This example shows that conditions (1)(a) and (1)(b) are not sufficient for giving an affirmative conclusion to the question whether or not Γ contains only polynomials.

(4) $\Gamma := \{f_n(q) = \frac{([n]_{q^6})^2[n]_{q^{15}}[n]_{q^{21}}}{[n]_{q^2}([n]_{q^3})^3} \mid n \in A_P\}$ for some collection of primes P. Then conditions (1)(a) and (1)(b) are satisfied since

$$\frac{\prod_{r\in R_{+,\Gamma}} r^{t_r}}{\prod_{r\in R_{-,\Gamma}} r^{t_r}} = \frac{6^2.15.21}{2.3^3} = 210$$

is a positive integer and there is no element in $R_{-,\Gamma}$ which is greater than every element of $R_{+,\Gamma}$. Also, there is no element in $R_{-,\Gamma}$ which is divisible by a prime which does not divide any element of $R_{+,\Gamma}$.

(a) Suppose $P = \{2, 3, 5\}$. Then

$$|R_{+,\Gamma}|_2 = \{2.1, 2.3, 2.1, 2.3, 1, 3, 5, 15, 1, 3, 7, 21\}$$

does not contain

$$\{2.1, 1, 3, 1, 3, 1, 3\} = |R_{-,\Gamma}|_2$$

as a subset. Therefore, Γ does not contain only polynomials by condition (2) of Theorem 2.1.

(b) Suppose $P = \{7, 11, 13\}$. Then

$$\begin{aligned}
|R_{+,\Gamma}|_7 &= \{1, 2, 3, 6, 1, 2, 3, 6, 1, 3, 5, 15, 1, 3, 7, 21\} \supseteq \{1, 2, 1, 3, 1, 3, 1, 3\} = |R_{-,\Gamma}|_7.\\
|R_{+,\Gamma}|_{11} &= \{1, 2, 3, 6, 1, 2, 3, 6, 1, 3, 5, 15, 1, 3, 7, 21\} \supseteq \{1, 2, 1, 3, 1, 3, 1, 3\} = |R_{-,\Gamma}|_{11}.\\
|R_{+,\Gamma}|_{13} &= \{1, 2, 3, 6, 1, 2, 3, 6, 1, 3, 5, 15, 1, 3, 7, 21\} \supseteq \{1, 2, 1, 3, 1, 3, 1, 3\} = |R_{-,\Gamma}|_{13}.
\end{aligned}$$

Hence, Γ contains only polynomials by condition (2) of Theorem 2.1. This example demonstrates that the answer to the question whether or not Γ contains only polynomials also depends on its support base P and that $|R_{+,\Gamma}|_p$ and $|R_{-,\Gamma}|_p$ stay the same for every p in P if p does not divide r for any r in R_Γ.

Proof. (Proof of Theorem 2.2)

(i) Suppose that $P = \{p\}$ for some prime p. Let $f(q)$ be a nonzero polynomial with coefficients contained in a field of characteristic zero. It can be verified from the proof of Theorem 2.1 (also see [4] for more details) that there exists a unique sequence of polynomials, satisfying Functional Equation (2), of the form

$$\Gamma = \{f_{p^n}(q) | f_1(q) = 1, n \in \mathbb{N}, f(q) = f_p(q)\}$$

with $f_{p^n}(q) = f_p(q)f_{p^{n-1}}(q^p)$ for all $n \geq 1$. Hence the support base of Γ is P. By normalizing this sequence of polynomials using Theorem 1.8, we may assume that $f_p(q)$ is a monic polynomial

with nonzero constant term (0 is thus not a root of $f_p(q)$).

Lemma 3.4. *Suppose $f_p(q)$ satisfies either of the following conditions of Theorem 2.2:*

1. *$f_p(q)$ possesses at least one root which is not a root of unity.*
2. *If all roots of $f_p(q)$ are roots of unity, then there is at least one root whose order is not divisible by p.*

Then Γ is a maximal solution of Functional Equation (2).

Proof. Suppose that Γ is not a maximal solution. Then there exists a sequence of polynomials

$$\Gamma' := \{f_n^*(q) | n \in \mathbb{N}\}$$

satisfying Functional Equation (2) such that its support base P^* strictly contains P and $f_p^*(q) = f_p(q)$. Hence, P^* contains at least two primes. If the field of coefficients of Γ^* is $\mathbb{Q}$, then there exits a collection of positive integers R_{Γ^*} and a collection of integers $\{t_r \mid r \in R_{\Gamma^*}\}$ such that

$$f_n^* = \prod_{r \in R_{\Gamma^*}} ([n]_{q^r})^{t_r}$$

for all $n \in A_{P^*}$ by Theorem 1.9. In particular,

$$f_p^* = \prod_{r \in R_{\Gamma^*}} ([p]_{q^r})^{t_r}.$$

Consequently, it can be verified that every root of $f_p^*(q) = f_p(q)$ is a root of unity of order divisible by p. Therefore, this contradicts the hypothesis of Lemma 3.4. Hence Γ must be a maximal solution.

If the field of coefficients of Γ^* strictly contains $\mathbb{Q}$, then there exists a sequence of polynomials Γ', with $\mathbb{Q}$ as its field of coefficients and support A_{P^*}, satisfying Functional Equation (2) such that $f_n^*(q)$ divides $f_n'(q)$ for all n in A_{P^*}, by Theorem 1.10. Then again by Theorem 1.9,

$$f_n' = \prod_{r \in R_{\Gamma'}} ([n]_{q^r})^{t_r}$$

for all $n \in A_{P'}$ for some collection of positive integers $R_{\Gamma'}$ and some collection of integers $\{t_r \mid r \in R_{\Gamma'}\}$ since the field of coefficients of Γ' is $\mathbb{Q}$. Since $f_p(q)$ divides $f_p^*(q)$ which in turn divides $f_p'(q)$ in $\mathbb{C}[q]$, it can be deduced that every root of $f_p(q)$ must also be a root of unity of order divisible by p, which contradicts the hypothesis. Therefore, Γ must be a maximal solution. □

Next let us suppose that Γ is a maximal solution of Functional Equation (2) with support base $P = \{p\}$ for some prime p and with field of coefficients $\mathbb{Q}$. Hence $f_p(q)$, the polynomial in Γ indexed by p, must be nonzero. We need to show that Γ has the form and satisfies the properties prescribed in Theorem 2.2. As above, it can be verified that Γ must have the form

$$\Gamma = \{f_{p^n}(q) | f_1(q) = 1, n \in \mathbb{N}\}$$

with $f_{p^n}(q) = f_p(q)f_{p^{n-1}}(q^p)$ for all $n \geq 1$. By Theorem 1.8,

$$f_p(q) = \psi(p)q^{t_\Gamma(p-1)}g_p(q)$$

where:

- $g_p(q)$ is a monic polynomial with nonzero constant term and the sequence of polynomials $\{g_n(q) \mid n \in A_P\}$ satisfies Functional Equation (2).
- ψ is a completely multiplicative arithmetic function with support A_P.

Lemma 3.5. *$g_p(q)$ must be a nonconstant polynomial.*

Proof. Suppose $g_p(q)$ is a constant polynomial, i.e. $g_p(q) = 1$ since it is monic. Let r be any prime distinct from p. Define:

$$f_r(q) = \psi(r)q^{t_\Gamma(r-1)}g_r(q)$$

where:

- $g_r(q) = 1$.
- $\psi(r) = 1$, $\psi(r^m) := (\psi(r))^m$ and $\psi(p^n r^m) := \psi(p^n)\psi(r^m)$ for any nonnegative integers m and n.

Then ψ is a completely multiplicative arithmetic function on the domain of the form $A_{P'} := \{p^n r^m \mid n, m \in \mathbb{N} \cup \{0\}\}$ which is a prime semigroup generated by $P' = \{p, r\}$. It can be verified that the sequences of polynomials

$$\{g_n(q) \mid n \in A_{P'}\}$$

and

$$\Gamma' := \{f_n(q) \mid n \in A_{P'}\}$$

satisfy Functional Equation (2) such that Γ is the restriction of Γ' to the domain A_P. Hence, Γ is not a maximal solution to Functional Equation (2), which contradicts our assumption. Therefore, $g_p(q)$ must be a nonconstant polynomial. □

By Theorem 1.8, we may assume that Γ is its own normalized version, i.e., each polynomial $f_n(q)$ is a monic polynomial with nonzero constant term for all n in the support of Γ. By Lemma 3.5, $f_p(q)$ is a nonconstant polynomial and thus possesses at least one root. Suppose that every root of $f_p(q)$ is a root of unity of order divisible by p. Let Υ be the collection of all roots of $f_p(q)$ and let α be an arbitrary element of Υ. Then its minimal polynomial over $\mathbb{Q}$ is $P_{u_\alpha p}(q)$ for some positive u_α, where $P_{u_\alpha p}(q)$ is the cyclotomic polynomials with coefficients in $\mathbb{Q}$ and of order up. From the proof of Part (I) of [5], we know that

$$P_{u_\alpha p}(q) = \prod_{r \in R_{u_\alpha p}} ([p]_{q^r})^{t_r}$$

for some collection of positive integers R and some collection of integers $\{t_r \mid r \in R\}$. Hence,

$$f_p(q) = \prod_{\alpha\in\Upsilon}(P_{u_\alpha p}(q))^{n_\alpha} = \prod_{\alpha\in\Upsilon}(\prod_{r\in R_{u_\alpha p}}([p]_{q^r})^{t_r})^{n_\alpha} = \prod_{r\in R}([p]_{q^r})^{s_r}$$

for some collection of positive integers R and some collection of integers $\{s_r \mid r \in R\}$. Let t be a prime distinct from p such that t does not divide r for any r in R. Then it can be verified from the proof of Theorem 2.1 above that

$$f_t(q) := \prod_{r\in R}([t]_{q^r})^{s_r}$$

is a polynomial. It can be verified that $f_p(q)$ and $f_t(q)$ satisfy Functional Equation (1). Therefore, they determine a unique sequence of polynomials Γ', satisfying Functional Equation (2) with support base $P' = \{p, t\}$, which contains both $f_p(q)$ and $f_t(q)$ by Theorem 1.6. Hence, Γ is the restriction of Γ' to A_P and thus cannot be a maximal solution. This contradicts our assumption. Thus the result follows. □

(ii) Suppose P contains at least two primes and let A_P be the prime semigroup generated by P. Suppose further that P has finite complement and let $P_\circ$ be its complement, i.e, $P_\circ$ is the collection of all primes which are not in P. If $P_\circ = \emptyset$, i.e, P contains all primes, then it follows immediately that

$$\Gamma := \{([n]_q)^s \mid n \in \mathbb{N}\}$$

is a maximal solution with support base P for each nonnegative integer s. We may assume henceforth without loss of generality that $P_\circ \neq \emptyset$. Let

$$u = \prod_{p_i\in P_\circ} p_i.$$

Define

$$\Gamma := \{f_n(q) \mid f_n(q) = \frac{[n]_{q^u}}{[n]_q}; n \in A_P\}.$$

Lemma 3.6. Γ *contains only polynomials and*

$$\frac{[p_i]_{q^u}}{[p_i]_q}$$

is not a polynomial for any prime p_i *in* $P_\circ$.

Proof. We have $R_{+,\Gamma} = \{u\}$, $R_{-,\Gamma} = \{1\}$ and $t_u = 1 = t_1$. Let p be any prime in $P - P_\circ$. Since p does not divide u by construction, it can be verified that $|R_{+,\Gamma}|_p$ is exactly the collection of all distinct divisors of u each appears with multiplicity 1, and $|R_{1,\Gamma}|_p = \{1\}$. Hence,

$$|R_{+,\Gamma}|_p \supseteq |R_{1,\Gamma}|_p. \tag{3.5}$$

Since p is an arbitrary prime in $P - P_\circ$, (3.5) holds for all p in $P - P_\circ$. Therefore, Γ contains only polynomials by Theorem 2.1.

Let p_i be any prime in $P_\circ$. Then

$$|R_{+,\Gamma}|_p = \{p_i\gamma \mid \gamma|\frac{u}{p_i}\}$$

where $p_i\gamma$ appears with multiplicity 1 since $t_u = 1$. Since $t_1 = 1$,

$$|R_{-,\Gamma}|_p = \{1\}$$

where 1 appears with multiplicity 1. Hence, $|R_{+,\Gamma}|_{p_i}$ does not contain $|R_{-,\Gamma}|_{p_i}$ for each prime p_i in $P_\circ$. Therefore, it can be verified from Theorem 2.1 that

$$\frac{[p_i]_{q^u}}{[p_i]_q}$$

is not a polynomial for any prime p_i in $P_\circ$.

□

It follows immediately from Lemma 3.6 that Γ is a maximal solution with support base P. Suppose

$$\Gamma := \{f_n(q) \mid n \in A_P\}$$

is a maximal solution of Functional Equation (2) with support base P containing at least two primes and with field of coefficients $\mathbb{Q}$. By Theorem 1.9, there exists a collection of positive integers R_Γ and a collection of integers $\{t_r \mid r \in R_\Gamma\}$ such that

$$f_n(q) = \prod_{r\in R_\Gamma} ([n]_{q^r})^{t_r} = \prod_{r\in R_{+,\Gamma}} ([n]_{q^r})^{t_r} \prod_{r\in R_{-,\Gamma}} ([n]_{q^r})^{t_r}$$

for all n in A_P where $R_{+,\Gamma}$ and $R_{-,\Gamma}$ are defined as before.

Lemma 3.7. *P must have finite complement.*

Proof. Since Γ is a maximal solution, it contains only polynomials by definition. Hence,

$$|R_{+,\Gamma}|_t \supseteq |R_{-,\Gamma}|_t$$

for all primes t in P by Theorem 2.1. Hence condition (1)(b) holds. Let p be any prime such that p does not divide r for any r in R_Γ, then it follows from Lemma 3.3 that

$$|R_{+,\Gamma}|_p \supseteq |R_{-,\Gamma}|_p.$$

Let T be the set containing all such primes p. By Theorem 2.1, this is equivalent to

$$f_p(q) = \prod_{r\in R_\Gamma} ([p]_{q^r})^{t_r} = \prod_{r\in R_{+,\Gamma}} ([p]_{q^r})^{t_r} \prod_{r\in R_{-,\Gamma}} ([p_i]_{q^r})^{t_r}$$

is a polynomial for all primes p in T. Since R_Γ contains only finite many elements, it follows that T contains all but finitely many primes. As a result, P must contain T as a subset for otherwise Γ would not be a maximal solution. In other words, P contains all but finitely many primes.

To complete the proof of Theorem 2.2, we need to prove the following lemmas:

Lemma 3.8. *Let P be a set of primes with nonempty finite complement. Then every maximal solution to Functional Equation (2) with support base P must have the form*

$$\Gamma = \{f_n(q) = \prod_{r\in R}([n]_{q^r})^{t_r} = \prod_{r\in R_{-,\Gamma}}([n]_{q^r})^{t_r} \prod_{r\in R_{+,\Gamma}}([n]_{q^r})^{t_r} | n \in A_P\}$$

where:

- $R_{-,\Gamma} \neq \emptyset$.
- *For each prime p in the complement of P, $|R_{-,\Gamma}|_p$ is not a subset of $|R_{+,\Gamma}|_p$.*

Proof. From above, we know that there exists at least one maximal solution with support base P. Let Γ be one such maximal solution with support base P and field of coefficients of characteristic zero. By Theorem 1.11, Γ is generated by quantum integers. Thus there exists a collection of positive integers R_Γ and a collection of integers $\{t_r \mid r \in R_\Gamma\}$ such that

$$\Gamma = \{f_n(q) = \prod_{r\in R}([n]_{q^r})^{t_r} = \prod_{r\in R_{-,\Gamma}}([n]_{q^r})^{t_r} \prod_{r\in R_{+,\Gamma}}([n]_{q^r})^{t_r} | n \in A_P\}.$$

Suppose $R_{-,\Gamma} = \emptyset$. Since the complement of P is nonempty, there exists at least one prime, say p, in the complement of P. Then

$$f_p(q) := \prod_{r\in R}([p]_{q^r})^{t_r} = \prod_{r\in R_{-,\Gamma}}([p]_{q^r})^{t_r} \prod_{r\in R_{+,\Gamma}}([p]_{q^r})^{t_r} = \prod_{r\in R_{+,\Gamma}}([p]_{q^r})^{t_r}$$

is a polynomial. It can be verified that $f_p(q)$ and $f_r(q)$ satisfy Functional Equation (1) for any prime r in P. By Theorem 1.6, the sequence of polynomials

$$\Sigma = \{f_s(q) \mid s \in P \cup \{p\}\}$$

induces a unique sequence of polynomials Γ' satisfying Functional Equation (2) with support base $P' = P \cup \{p\}$, which contains Σ as a subsequence. It can also be verified that Γ arises from Γ' by restriction of domain to A_P. This contradicts the fact that Γ is a maximal solution. Hence $R_{-,\Gamma} \neq \emptyset$.

If there is some prime p in the complement of P such that

$$|R_{-,\Gamma}|_p \subseteq |R_{+,\Gamma}|_p,$$

then it can be verified from the proof of Theorem 2.1 that

$$f_p(q) := \prod_{r\in R_\Gamma}([p]_{q^r})^{t_r} = \prod_{r\in R_{-,\Gamma}}([p]_{q^r})^{t_r} \prod_{r\in R_{+,\Gamma}}([p]_{q^r})^{t_r}$$

is a polynomial. By a similar argument as above, it can also be verified that Γ is not a maximal solution which contradicts the assumption. Therefore, the result follows.

□

Let P be a collection of primes containing at least two primes. Suppose that there exists a sequence of polynomials Γ which is a maximal solution to Functional Equation (2) with support base P and with field of coefficients $\mathbb{Q}$. We want to show that there are infinitely many such sequences. If P contains all primes, then this is proven above. Thus we may assume henceforth without loss of generality that P has nonempty complement. By the proof above, P has finite complement and there exists a collection of positive integers R_Γ and a collection of integers $\{t_r \mid r \in R\}$ such that for all n in A_P,

$$f_n(q) = \prod_{r \in R_\Gamma} ([n]_{q^r})^{t_r} = \prod_{r \in R_{+,\Gamma}} ([n]_{q^r})^{t_r} \prod_{r \in R_{-,\Gamma}} ([n]_{q^r})^{t_r}$$

with $R_{-,\Gamma} \neq \emptyset$ and $|R_{-,\Gamma}|_p \subseteq |R_{+,\Gamma}|_p$ for all p in P.

Lemma 3.9. *Each sequence of polynomials of the form*

$$\Gamma' := \{f'_n(q) = \prod_{r \in \mathcal{S}_{\Gamma'}} ([n]_{q^r})^{s_r} = \prod_{r \in \mathcal{S}_{+,\Gamma'}} ([n]_{q^r})^{s_r} \prod_{r \in \mathcal{S}_{-,\Gamma'}} ([n]_{q^r})^{s_r} \mid n \in A_P\}$$

is a maximal solution of Functional Equation (2) *with support base* P *and field of coefficients* $\mathbb{Q}$ *where:*

- $\mathcal{S}_{\Gamma'} := \mathcal{S}_{+,\Gamma'} \cup \mathcal{S}_{-,\Gamma'}$*;*
- $\mathcal{S}_{+,\Gamma'} := R_{+,\Gamma} \cup \mathcal{C}$*;*
- $\mathcal{C}$ *is either the empty set or a set of the form* $\{r\}$ *where* r *is a positive integer such that* w *does not divide* r *for any* w *in the complement of* P*;*
- $\mathcal{S}_{-,\Gamma'} = R_{-,\Gamma}$*,*

such that $s_r \geq t_r$ *is a positive integer for each* r *in* $R_{+,\Gamma}$ *and* $s_r = l$ *for some positive integer* l *if* $r \in \mathcal{C}$*.*

Proof. The only nontrivial part is that Γ' is a maximal solution. First let us verify that Γ' is a solution of Functional Equation (2) for any set $\mathcal{S}_{\Gamma'}$ of the form given in the statement of Lemma 3.9. By carrying out a direct verification using (1.2) and Theorem 6 of [3], it can be verified that Γ' satisfies Functional Equation (2). Next, let us verify that for any set $\mathcal{S}_{\Gamma'}$ of that form, the corresponding sequence of rational functions Γ' contains only polynomials. If s is any prime in P, then

$$\prod_{r \in \mathcal{R}_{+,\Gamma}} ([s]_{q^r})^{t_r} \prod_{r \in R_{-,\Gamma}} ([s]_{q^r})^{t_r}$$

is a polynomial by definition of Γ, or equivalently, $|R_{-,\Gamma}|_s$ is a subset of $|R_{+,\Gamma}|_s$. Therefore, it follows immediately from the definitions of $\mathcal{S}_{+,\Gamma'}$ and $\mathcal{S}_{-,\Gamma'}$ that

$$f'_s(q) = \prod_{r \in \mathcal{S}_{+,\Gamma'}} ([s]_{q^r})^{t_r} \prod_{r \in \mathcal{S}_{-,\Gamma}} ([s]_{q^r})^{t_r} = \prod_{r \in \mathcal{S}_{+,\Gamma'}} ([s]_{q^r})^{t_r} \prod_{r \in R_{-,\Gamma}} ([s]_{q^r})^{t_r} \tag{3.6}$$

must also be a polynomial. Since Γ' contains only polynomials if and only if $f'_s(q)$ is a polynomial for each prime s in P, it follows that Γ' contains only polynomials. Finally, let us show that a set $\mathcal{S}_{\Gamma'}$ of such form can be constructed so that Γ' is maximal. It can be deduced from the definition of $\mathcal{S}_{+,\Gamma}$ and $\mathcal{S}_{-,\Gamma'}$ that

$$|\mathcal{S}_{-,\Gamma'}|_s = |R_{-,\Gamma}|_s \subseteq |R_{+,\Gamma}|_s \subseteq |\mathcal{S}_{+,\Gamma'}|_s \tag{3.7}$$

where $|\mathcal{S}_{+,\Gamma}|_s$ and $|\mathcal{S}_{-,\Gamma}|_s$ are defined in a similar fashion as $|R_{+,\Gamma}|_s$ and $|R_{-,\Gamma}|_s$ respectively. Note that $|\mathcal{S}_{-,\Gamma'}|_t = |R_{-,\Gamma}|_t$ for all primes t (not just the primes in P). Note also that a prime t in the complement of P divides an element r' in $S_{+,\Gamma'}$ if and only if t divides some element r in $R_{+,\Gamma}$. Thus we may replace $|\mathcal{S}_{-,\Gamma'}|_t$ by $|R_{-,\Gamma}|_t$ for any prime t from now on. By the same argument as before, $|R_{-,\Gamma}|_t$ being a subset of $|\mathcal{S}_{+,\Gamma}|_t$ is equivalent to the fact that (3.6) is a polynomial for each prime t (with t replacing s). In particular, (3.7) holds for each prime s in P. Let p be a prime not in P. Then

$$\prod_{r\in\mathcal{R}_{+,\Gamma}} ([p]_{q^r})^{t_r} \prod_{r\in R_{-,\Gamma}} ([p]_{q^r})^{t_r}$$

is not a polynomial since Γ is maximal. Therefore, $|R_{-,\Gamma}|_p$ is not a subset of $|R_{+,\Gamma}|_p$. Since Γ contains only polynomials, condition (1)(b) of Theorem 2.1 is satisfied. Therefore, p must divide some r in $R_{+,\Gamma}$ by Lemma 3.3. Write:

$$|\mathcal{S}_{+,\Gamma'}|_p := \{p^{s_{p,r}}\gamma \mid r \in \mathcal{S}_{+,\Gamma'}; \gamma|\frac{r}{p^{s_{p,r}}}\} = \{p^{s_{p,r}}\gamma \mid r \in \mathcal{S}^{(1)}_{+,\Gamma'}; \gamma|\frac{r}{p^{s_{p,r}}}\} \cup \{\gamma \mid r \in \mathcal{S}^{(2)}_{+,\Gamma'}; \gamma|r\}; \tag{3.8}$$

$$|R_{+,\Gamma}|_p := \{p^{s_{p,r}}\gamma \mid r \in R_{+,\Gamma}; \gamma|\frac{r}{p^{s_{p,r}}}\} = \{p^{s_{p,r}}\gamma \mid r \in R^{(1)}_{+,\Gamma}; \gamma|\frac{r}{p^{s_{p,r}}}\} \cup \{\gamma \mid r \in R^{(2)}_{+,\Gamma}; \gamma|r\}; \tag{3.9}$$

$$|R_{-,\Gamma}|_p := \{p^{s_{p,r}}\gamma \mid r \in R_{-,\Gamma}; \gamma|\frac{r}{p^{s_{p,r}}}\} = \{p^{s_{p,r}}\gamma \mid r \in R^{(1)}_{-,\Gamma}; \gamma|\frac{r}{p^{s_{p,r}}}\} \cup \{\gamma \mid r \in R^{(2)}_{-,\Gamma}; \gamma|r\} \tag{3.10}$$

where:

- $p^{s_{p,r}}\gamma$ appears t_r times in $|R_{+,\Gamma}|_p$ (resp. in $|R_{-,\Gamma}|_p$) if $t_r > 0$ (resp. if $t_r < 0$).
- $s_{p,r} \geq 1$ for at least one r in $R_{+,\Gamma}$.
- $\mathcal{S}^{(1)}_{+,\Gamma'}$, $R^{(1)}_{+,\Gamma}$ and $R^{(1)}_{-,\Gamma}$ consist of all r in $\mathcal{S}_{+,\Gamma}$, $R_{+,\Gamma}$ and in $R_{-,\Gamma}$ correspondingly which are divisible by p.
- $\mathcal{S}^{(2)}_{+,\Gamma'}$, $R^{(2)}_{+,\Gamma}$ and $R^{(2)}_{-,\Gamma}$ consist of all r in $\mathcal{S}_{+,\Gamma}$, $R_{+,\Gamma}$ and in $R_{-,\Gamma}$ correspondingly which are not divisible by p.

Note that $R^{(1)}_{+,\Gamma} \neq \emptyset$. If $R^{(2)}_{-,\Gamma} \neq \emptyset$, then define $\mathcal{C} := \emptyset$. Otherwise, let $\mathcal{C} := \{r\}$ for some positive integer r such that w does not divide r for any prime w in the complement of P. As a result, $\mathcal{S}^{(2)}_{+,\Gamma'} \neq \emptyset$ since p does not divide the element r in $\mathcal{C}$ by construction.

As the unions in (3.8), (3.9) and (3.10) are disjoint, it can be verified from the definition of $\mathcal{S}_{+,\Gamma'}$ that

$$\{p^{s_{p,r}}\gamma \mid r \in R^{(1)}_{+,\Gamma}; \gamma|\frac{r}{p^{s_{p,r}}}\} \subseteq \{p^{s_{p,r}}\gamma \mid r \in \mathcal{S}^{(1)}_{+,\Gamma'}; \gamma|\frac{r}{p^{s_{p,r}}}\}$$

and

$$\{\gamma \mid r \in R^{(2)}_{+,\Gamma}; \gamma|r\} \subseteq \{\gamma \mid r \in \mathcal{S}^{(2)}_{+,\Gamma'}; \gamma|r\}.$$

Moreover, it can be verified from our construction that if α appears in $\{p^{s_{p,r}}\gamma \mid r \in \mathcal{S}^{(1)}_{+,\Gamma}; \gamma|\frac{r}{p^{s_{p,r}}}\}$ (resp. in $\{\gamma \mid r \in \mathcal{S}^{(2)}_{+,\Gamma}; \gamma|r\}$) with multiplicity $m > 0$ (resp. $n > 0$), then α must appear in $\{p^{s_{p,r}}\gamma \mid r \in R^{(1)}_{+,\Gamma}; \gamma|\frac{r}{p^{s_{p,r}}}\}$ (resp. in $\{\gamma \mid r \in R^{(2)}_{+,\Gamma}; \gamma|r\}$) with multiplicity u (resp. v) such that $m \geq u > 0$ and $n \geq v > 0$. Hence if there exists an element λ in

$$\{p^{s_{p,r}}\gamma \mid r \in R^{(1)}_{-,\Gamma}; \gamma|\frac{r}{p^{s_{p,r}}}\}$$

which does not appear in

$$\{p^{s_{p,r}}\gamma \mid r \in R^{(1)}_{+,\Gamma}; \gamma|\frac{r}{p^{s_{p,r}}}\},$$

then λ does not appear in

$$\{p^{s_{p,r}}\gamma \mid r \in \mathcal{S}^{(1)}_{+,\Gamma}; \gamma|\frac{r}{p^{s_{p,r}}}\}.$$

Since P has finite complement, there exists a prime z in P such that z does not divide r for any r in $R_{\Gamma'}$. Then

$$|\mathcal{S}_{+,\Gamma}|_z = \{\gamma \mid r \in \mathcal{S}_{+,\Gamma}; \gamma|r\} = \{p^{w_r}\gamma \mid r \in \mathcal{S}^{(1)}_{+,\Gamma}; \gamma|\frac{r}{p^{s_{p,r}}}\} \cup \{\gamma \mid r \in \mathcal{S}^{(2)}_{+,\Gamma}; \gamma|r\}; \tag{3.11}$$

$$|R_{+,\Gamma}|_z = \{\gamma \mid r \in R_{+,\Gamma}; \gamma|r\} = \{p^{w_r}\gamma \mid r \in R^{(1)}_{+,\Gamma}; \gamma|\frac{r}{p^{s_{p,r}}}\} \cup \{\gamma \mid r \in R^{(2)}_{+,\Gamma}; \gamma|r\}; \tag{3.12}$$

$$|R_{-,\Gamma}|_z = \{\gamma \mid r \in R_{-,\Gamma}; \gamma|r\} = \{p^{w_r}\gamma \mid r \in R^{(1)}_{-,\Gamma}; \gamma|\frac{r}{p^{s_{p,r}}}\} \cup \{\gamma \mid r \in R^{(2)}_{-,\Gamma}; \gamma|r\}, \tag{3.13}$$

where $0 \leq w_r \leq s_{p,r}$ for each r, since $s_{z,r} = 0$ for all r in $\mathcal{S}_{\Gamma'}$. Note that the unions in (3.11) (3.12) and (3.13) are not necessarily disjoint. Since z is in P, (3.7) implies that if γ_0 satisfies either of the following properties: (i) $\gamma_0|r$ for some r in $R^{(2)}_{-,\Gamma}$; or (ii) $\gamma_0|\frac{r}{p^{s_{p,r}}}$ for some r in $R^{(1)}_{-,\Gamma}$, then

$$0 < m_{1,\gamma_0} + n_{1,\gamma_0} \leq m_{2,\gamma_0} + n_{2,\gamma_0} \leq m_{3,\gamma_0} + n_{3,\gamma_0},$$

where:

- m_{1,γ_0}, m_{2,γ_0} and m_{3,γ_0} are the multiplicities of γ_0 in $\{\gamma \mid r \in R^{(2)}_{-,\Gamma}; \gamma|r\}$, $\{\gamma \mid r \in R^{(2)}_{+,\Gamma}; \gamma|r\}$ and $\{\gamma \mid r \in \mathcal{S}^{(2)}_{+,\Gamma}; \gamma|r\}$ correspondingly.

- n_{1,γ_0}, n_{2,γ_0}, and n_{3,γ_0} are the multiplicities of γ_0 in $\{p^w\gamma \mid 0 \leq w \leq s_{p,r}; r \in R^{(1)}_{-,\Gamma}; \gamma|\frac{r}{p^{s_{p,r}}}\}$, $\{p^w\gamma \mid r \in R^{(1)}_{+,\Gamma}; \gamma|\frac{r}{p^{s_{p,r}}}; 0 \leq w \leq s_{p,r}\}$, and $\{p^w\gamma \mid r \in \mathcal{S}^{(1)}_{+,\Gamma}; \gamma|\frac{r}{p^{s_{p,r}}}; 0 \leq w \leq s_{p,r}\}$ correspondingly.

- $m_{1,\gamma_0} + n_{1,\gamma_0}$, $m_{2,\gamma_0} + n_{2,\gamma_0}$, and $m_{3,\gamma_0} + n_{3,\gamma_0}$ are the multiplicities of γ_0 in $|R_{-,\Gamma}|_z$, $|R_{+,\Gamma}|_z$, and $|\mathcal{S}_{+,\Gamma}|_z$ correspondingly.

Note that m_{i,γ_0}'s and n_{i,γ_0}'s may be zero. It can be verified that such a γ_0 also appears in $|R_{-,\Gamma}|_p$ and m_{1,γ_0}, m_{2,γ_0} and m_{3,γ_0} are also the multiplicities of γ_0 in the sets $\{\gamma \mid r \in R^{(2)}_{-,\Gamma}; \gamma|r\}$, $\{\gamma \mid r \in R^{(2)}_{+,\Gamma}; \gamma|r\}$, and $\{\gamma \mid r \in \mathcal{S}^{(2)}_{+,\Gamma}; \gamma|r\}$ of the equations (3.10), (3.9) and (3.8) correspondingly.

If $m_{1,\gamma_0} > m_{2,\gamma_0}$ for one such γ_0, then $R^{(2)}_{-,\Gamma} \neq \emptyset$ and thus $\mathcal{C} = \emptyset$ and $\{\gamma \mid r \in R^{(2)}_{-,\Gamma}; \gamma|r\}$ is not a subset of $\{\gamma \mid r \in R^{(2)}_{+,\Gamma}; \gamma|r\}$. Define:

$$\Gamma' := \{f'_n(q) = \prod_{r\in\mathcal{S}_{\Gamma'}} ([n]_{q^r})^{s_r} = \prod_{r\in\mathcal{S}_{+,\Gamma'}} ([n]_{q^r})^{s_r} \prod_{r\in\mathcal{S}_{-,\Gamma'}} ([n]_{q^r})^{s_r} \mid n \in A_P\} \tag{3.14}$$

with $s_r > t_r$ for each r in $R^{(1)}_{+,\Gamma}$ and $s_r = t_r$ for each r in $R^{(2)}_{+,\Gamma}$. Then $\Gamma' \neq \Gamma$ since $R^{(1)}_{+,\Gamma} \neq \emptyset$. It can be verified that

$$\{\gamma \mid r \in \mathcal{S}^{(2)}_{+,\Gamma'}; \gamma|r\} = \{\gamma \mid r \in R^{(2)}_{+,\Gamma}; \gamma|r\}, \tag{3.15}$$

where the set on the left hand side of (3.15) is the set that appears in (3.8) and the set of the right hand side of (3.15) is the set that appears in (3.9) (and (3.12)), as well as

$$\{p^{s_{p,r}}\gamma \mid r \in \mathcal{S}^{(1)}_{+,\Gamma'}; \gamma|\frac{r}{p^{s_{p,r}}}\} \cap \{\gamma \mid r \in R^{(2)}_{-,\Gamma}; \gamma|r\} = \emptyset, \tag{3.16}$$

where the set on the left hand side of $\cap$ in (3.16) is the set appears that in (3.8) and the set of the right hand side of $\cap$ in (3.16) is the set that appears in (3.10) (and (3.13)). As a result, $|R_{-,\Gamma}|_p = |\mathcal{S}_{-,\Gamma}|_p$ is not a subset of $|\mathcal{S}_{+,\Gamma'}|_p$, and thus it follows from Theorem 2.1 that

$$f'_p(q) = \prod_{r\in\mathcal{S}_{\Gamma'}} ([p]_{q^r})^{s_r} = \prod_{r\in\mathcal{S}_{+,\Gamma'}} ([p]_{q^r})^{s_r} \prod_{r\in\mathcal{S}_{-,\Gamma'}} ([p]_{q^r})^{s_r}$$

is not a polynomial. Therefore, Γ' is a maximal solution with support base P. Since there are infinitely many distinct sequences of polynomials Γ' of the form defined in (3.14), there are infinitely many maximal solution with support base P and coefficients in $\mathbb{Q}$ as required.

If $m_{1,\gamma_0} \leq m_{2,\gamma_0}$ for all such γ_0, then

$$\{\gamma \mid r \in R^{(2)}_{-,\Gamma}; \gamma|r\} \subseteq \{\gamma \mid r \in R^{(2)}_{+,\Gamma}; \gamma|r\} \subseteq \{\gamma \mid r \in \mathcal{S}^{(2)}_{+,\Gamma'}; \gamma|r\}. \tag{3.17}$$

By construction, $\mathcal{S}^{(2)}_{+,\Gamma'} \neq \emptyset$ whether or not $R^{(2)}_{-,\Gamma}$ is empty.

Since

$$\{p^{s_{p,r}}\gamma \mid r \in R^{(1)}_{-,\Gamma}; \gamma|\frac{r}{p^{s_{p,r}}}\} \cap \{\gamma \mid r \in \mathcal{S}^{(2)}_{+,\Gamma'}; \gamma|r\} = \emptyset,$$

$$|R_{-,\Gamma}|_p \subseteq |\mathcal{S}_{+,\Gamma'}|_p$$

if and only if

$$\{p^{s_{p,r}}\gamma \mid r \in R^{(1)}_{-,\Gamma}; \gamma|\frac{r}{p^{s_{p,r}}}\} \subseteq \{p^{s_{p,r}}\gamma \mid r \in \mathcal{S}^{(1)}_{+,\Gamma'}; \gamma|\frac{r}{p^{s_{p,r}}}\}. \tag{3.18}$$

That is, $f'_p(q)$ is a polynomial if and only if (3.18) holds. By the maximality of Γ and (3.17),

$$\{p^{s_{p,r}}\gamma \mid r \in R^{(1)}_{-,\Gamma}; \gamma|\frac{r}{p^{s_{p,r}}}\}$$

is not a subset of $\{p^{s_{p,r}}\gamma \mid r \in R^{(1)}_{+,\Gamma}; \gamma|\frac{r}{p^{s_{p,r}}}\}$, i.e.,

$$\{p^{s_{p,r}}\gamma \mid r \in R^{(1)}_{-,\Gamma}; \gamma|\frac{r}{p^{s_{p,r}}}\} \cap \{p^{s_{p,r}}\gamma \mid r \in R^{(1)}_{+,\Gamma}; \gamma|\frac{r}{p^{s_{p,r}}}\} \neq \{p^{s_{p,r}}\gamma \mid r \in R^{(1)}_{-,\Gamma}; \gamma|\frac{r}{p^{s_{p,r}}}\}. \tag{3.19}$$

Define:

$$\Gamma' := \{f'_n(q) = \prod_{r \in \mathcal{S}_{\Gamma'}} ([n]_{q^r})^{s_r} = \prod_{r \in \mathcal{S}_{+,\Gamma'}} ([n]_{q^r})^{s_r} \prod_{r \in \mathcal{S}_{-,\Gamma'}} ([n]_{q^r})^{s_r} \mid n \in A_P\} \tag{3.20}$$

with $s_r = t_r$ for each r in $\mathcal{S}^{(1)}_{+,\Gamma}$ and $s_r > t_r$ for each r in $\mathcal{S}^{(2)}_{+,\Gamma}$. Together with (3.19), it follows that (3.18) does not hold. Therefore, the polynomial in Γ' defined in (3.20) which is indexed by p,

$$f'_p(q) = \prod_{r \in \mathcal{S}_{\Gamma'}} ([p]_{q^r})^{s_r} = \prod_{r \in \mathcal{S}_{+,\Gamma'}} ([p]_{q^r})^{s_r} \prod_{r \in \mathcal{S}_{-,\Gamma'}} ([p]_{q^r})^{s_r}$$

is not a polynomial. Therefore, the sequence of polynomials Γ' defined in (3.20) is a maximal solution.

If $R^{(2)}_{+,\Gamma} \neq \emptyset$, then it follows immediately from the construction in (3.20) that $\Gamma' \neq \Gamma$. If $R^{(2)}_{+,\Gamma} = \emptyset$, then $\Gamma' \neq \Gamma$ since

$$f'_n(q) = f_n(q)([n]_{q^r})^l$$

for each n in A_P where r is in $\mathcal{C}$ and $s_r = l$ by construction. In the former case, there are infinitely many choices for s_r such that $s_r > t_r$ for each r in $R^{(2)}_{+,\Gamma}$. In the latter case, there are infinitely many choices for the integer l. Thus the proof of Lemma 3.9 is complete. □

The proof of Theorem 2.2 is therefore complete. □

References

[1] Borisov, A., Nathanson, M. B., Wang, Y., Quantum Integers and Cyclotomy, *Journal of Number Theory*, Vol. 109, 2004, No. 1, 120–135.

[2] Nathanson, M. B. Formal Power Series Arising From Multiplication of Quantum Integers, *DIMACs Series in Discrete Mathematics and Theoretical Computer Science*, Vol. 64, 2004, 145–157.

[3] Nathanson, M. B., A Functional Equation Arising From Multiplication of Quantum Integers, *Journal of Number Theory*, Vol. 103, 2003, No. 2, 214–233.

[4] Nguyen, L., On the Classification of Solutions of a Functional Equation Arising from Multiplication of Quantum Integers, *Uniform Distribution Theory Journal* (accepted).

[5] Nguyen, L., On the Solutions of a Functional Equation Arising from Multiplication of Quantum Integers, *Journal of Number Theory*, Vol. 130, 2010, No. 6, 1292–1347.

[6] Nguyen, L., On the Support Base of a Functional Equation Arising from Multiplication of Quantum Integers, *Journal of Number Theory*, Volume 130, 2010, No. 6, 1348–1373.