Uniform Distribution Theory **8** (2013), no.2, 49–120

uniform distribution theory

ON THE CLASSIFICATION OF SOLUTIONS OF A FUNCTIONAL EQUATION ARISING FROM MULTIPLICATION OF QUANTUM INTEGERS

Lan Nguyen

ABSTRACT. We prove an open problem posed by Melvyn Nathanson concerning the solutions of a functional equation arising from multiplication of quantum integers. In this paper we give a complete classification of sequences of polynomials whose coefficients are contained in fields of characteristic zero satisfying the functional equation above.

Communicated by Jean-Paul Allouche

1. Introduction and Background

The aim of this paper is to study the solutions of functional equations arising from multiplication of quantum integers described in [1]. In particular, we seek to classify all sequences of polynomials, with fields of coefficients of characteristic zero, which are solutions of these functional equations. This is Problem 2 stated in [4] and also is one of Nathanson's open problems stated in [1].

Let us give some background and main results from [1] and [4] concerning quantum integers and the functional equation arising from multiplication of these integers.

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

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

where n is any natural number.

2010 Mathematics Subject Classification: 11P99, 11C08.
Keywords: quantum integer; functional equation; q-series; cyclotomic polynomial.

From [1], quantum multiplication 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, multiplication operation for quantum integers, and . denotes the usual multiplication of polynomials. It can be verified that Equation (1.2) is just the q-series expansion of the sumset

$$\{0, 1, \dots, m-1\} + \{0, m, \dots, (n-1)m\} = \{0, 1, \dots, mn-1\}.$$

Equation (1.2) leads Nathanson to the study of sequences of polynomials $\Gamma = \{f_n(q) | n = 1, \dots, \infty\}$, with coefficients contained in some field, satisfying the following functional equations:

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

for all $m, n \in \mathbb{N}$. As in [4], we refer to the first equality in the above functional equation as Functional Equation (1) and the second equality as Functional Equation (2).

Remark 1.2. A sequence of polynomials which satisfies Functional Equation (2) automatically satisfies Functional Equation (1) but not vice versa (see [4] for an example).

Let $\Gamma = \{f_n(q)\}$ be a sequence of polynomials satisfying Functional Equation (2). The set of $n \in \mathbb{N}$ where $f_n(q) \neq 0$ is called the *support* of Γ and denoted by $supp\{\Gamma\}$. If P is a set of rational primes and A_P consists of 1 and all natural numbers such that all their prime factors come from P, then A_P is a multiplicative semigroup which will be called a prime multiplicative semigroup associated to P. From [1], the support of Γ is a multiplicative prime subsemigroup of $\mathbb{N}$.

Theorem 1.3 ([1]). *Let $\Gamma = \{f_n(q)\}$ be a sequence of polynomials 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 polynomials:*

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

As a result, characterizing any sequence Γ satisfying Functional Equation (2) reduces to characterizing the sub-collection of polynomials with prime indexes $p \in P$.

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 $supp\{\Gamma\} = A_P$. One such sequence can be defined as the set of polynomials:

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

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 [1]).

The degree of each polynomial $f_n(q) \in \Gamma$ will be denoted by $deg(f_n(q))$. There exists a rational number t_Γ such that:

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

for all n in $supp\{\Gamma\}$([1]). This number t_Γ is not necessarily an integer (see [4] for an example of such a sequence). We will show in the subsequent part of this paper 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.

For composition and multiplication of sequences of polynomials satisfying Functional Equation (2), the following results are relevant to our work.

Theorem 1.4 ([1]). *Let $\Gamma = \{f_n(q)\}$ be a sequence of polynomials satisfying Functional Equation* (2) *and $g(q)$ be a polynomial such that $g(q^r) = g^r(q)$ for every $r \in supp\{\Gamma\}$. Then the sequence of compositions $\{f_n(g(q))|n \in \mathbb{N}\}$ also satisfies Functional Equation* (2)*.*

In particular, the sequence $\{f_n(q^r)|n \in \mathbb{N}\}$ satisfies Functional Equation (2) if the sequence $\{f_n(q)|n \in \mathbb{N}\}$ does. One important such example is the sequence of polynomials of the form:

$$f_m(q^r) := [m]_{q^r} = (q^r)^{m-1} + \cdots + (q^r) + 1,$$

for each $m \in \mathbb{N}$, which satisfies the Functional Equation (2) since the sequence $\Gamma = \{[m]_q|m \in \mathbb{N}\}$ does.

Theorem 1.5. *If Γ_1, Γ_2 are two nonzero sequences of polynomials satisfying the Functional Equation* (2)*, then the sequence $\Gamma_1 \cdot \Gamma_2$ also satisfies* (2)*. Conversely, if $supp\{\Gamma_1\} = supp\{\Gamma_2\}$ and Γ_1 as well as $\Gamma_1 \cdot \Gamma_2$ satisfying* (2)*, then Γ_2 also satisfies* (2)*. The collection of all solutions of the functional equation* (2) *is an abelian semigroup. Also for every set of primes P, the set of all sequences Γ satisfying* (2) *and having support A_P forms an abelian cancellation semigroup, which will be denoted by Υ_P.*

Remark 1.6. If $\Gamma_1 = \{f_n(q)|n \in \mathbb{N}\}$, $\Gamma_2 = \{g_n(q)|n \in \mathbb{N}\}$ are two nonzero sequences of polynomials satisfying the Functional Equation (2). Then $\Gamma_1 \cdot \Gamma_2$ is defined as the collection $\{f_ng_n(q)|n \in \mathbb{N}\}$ where $f_ng_n(q) = f_n(q)g_n(q)$.

Let P be a set of primes. The next result provides a general way to construct a solution to the Functional Equation (2) with support A_P associated to P:

Theorem 1.7 ([1]). *Let P be a set of primes. Let $\Gamma' = \{f'_p(q)|p \in P\}$ 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* $\Gamma = \{f_n(q)|n \in \mathbb{N}\}$ *satisfying Functional Equation* (2) *such that* $f_p(q) = f'_p(q)$ *for all primes* $p \in P$ *.*

The aim of this paper is to study the solutions of Functional Equations (1) and (2) arising from multiplication of quantum integers and to resolve, for the case where the fields of coefficients of $f_n(q)$'s are of characteristic zero, Nathanson's problems, whose details are stated in [1]. Specifically, this paper seeks to classify all sequences of polynomials satisfying Functional Equation (2). In [6-7], we resolve another problem of Nathanson by classifying all maximal solutions, those which are not restrictions of solutions with strictly larger supports, to Functional Equation (2) with support A_P for some set of primes P.

The classification of solutions in this paper is reduced, by the next result, to the classification of sequences of polynomials whose constant terms are equal to 1:

Theorem 1.8 ([1]). *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:*

$$f_n(q) = \psi(n) q^{t(n-1)} g_n(q)$$

and $g_n(0) = 1$ *for all* $n \in A_P$*.*

As a result, in the rest of this paper, unless otherwise stated, all sequences of polynomials which we consider are assumed to have constant terms 1.

2. Main Objectives and Results

2.1. Main Objectives and Preliminary Remarks

The following series of open problems are posed in Nathanson's paper [1] and also in our first paper on this subject [4]. They are our main objectives.

Problem 1. If $t_\Gamma \geq 2$, then there exist integers t_i, u_i such that $t_\Gamma = \sum_i t_i u_i$ and

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

for all n in the support of Γ.

Problem 2. If P is a set of rational primes. Determine all polynomial sequences $\Gamma = \{f_n(q)|n \in \mathbb{N}\}$ satisfying Functional Equation (2) and with support A_P.

Problem 3. Let $P \subseteq P'$ be two sets of prime numbers, and let $\Gamma = \{f_n(q)|n \in \mathbb{N}\}$ be a sequence of polynomials satisfying Functional Equation (2) with support A_P. Under what condition(s) does there exist a sequence $\Gamma' = \{f'_n(q)|n \in \mathbb{N}\}$ with support $A_{P'}$ such that $f_p(q) = f'_p(q)$ for all $p \in P$?

Problem 4. Let Υ_P be the collection of all solutions $\{\Gamma\}$ to Functional Equation (2) having support A_P. Does every sequence of rational functions having support A_P which satisfies Functional Equation (2) belong to the Grothendieck group $K(\Upsilon_P)$ of Υ_P?

Recall that if Υ is an abelian cancellation 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 $\alpha = \alpha' i$. The group $K(\Upsilon)$ is called the Grothendieck group of Υ.

A solution to Problem 1 is already given in ([4]) in the case where the field of coefficients of Γ is of characteristic zero. A solutions to Problem 2 is one of our main results, again in the case where the fields of coefficients of the sequences of polynomials Γ's are of characteristic zero, given in this paper. Solutions to Problem 3 and 4 are given in [2] and [3] respectively.

First let us discuss briefly the general structure of the subsequent part of this paper. Then we make some remarks concerning some important details needed for the set up of the proofs.

Initially, we intended to include the solution of Problem 2, 3 and 4 in this paper. However, it turns out to be longer than we expected. As a result, we only include the solution to Problem 2 in this paper.

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. We are only concerned with sequences of polynomials whose fields of coefficients K are of characteristic zero. The case of positive characteristic fields of coefficients will be reserved for our future papers. Unless stated otherwise, we always view Γ as a sequence of polynomials with coefficients in a fixed separable closure $\overline{K}$ of K which is embedded in $\mathbb{C}$ via a fixed embedding $\iota : \overline{K} \hookrightarrow \mathbb{C}$. Thus every element $f(q)$ of Γ can be viewed as a polynomial in $\mathbb{C}[q]$. We frequently view the polynomials $f(q)$'s in Γ as elements of the ring $\mathbb{C}[q]$ throughout this paper. Thus whenever that is necessary, it will be assumed.

For the problem treated in this paper, we generally divide the proofs into two parts as far as the fields of coefficients are concerned; one part treats the case where the field of coefficients is $\mathbb{Q}$ and the other part covers the case where $\mathbb{Q}$ is strictly the prime subfield of K.

We also differentiate between the cases where t_Γ is integral and where it is non-integral.

2.2. Main Results

Our main results in this paper is a solution to the Problems 2 in the case where the fields of coefficients of the sequences of polynomials are of characteristic zero. For some of these problems, our results are stronger and more extended than what is conjectured. We will mention them when such situations occur. Again, we only consider sequences of polynomials whose constant terms are equal to 1.

Theorem 2.1. *Let $\Gamma = \{f_n(q)|n \in \mathbb{N}\}$ be a sequence of polynomials satisfying Functional Equation (2) whose field of coefficients is of characteristic zero. Suppose that the set of primes P associated to the support A_P of Γ contains at least two primes. Then there exists a sequence $\Gamma' = \{f'_n(q)|n \in \mathbb{N}\}$ satisfying Functional Equation (2) with field of coefficients $\mathbb{Q}$ such that $f_n(q)$ divides $f'_n(q)$ for all n. Furthermore, $t_{\Gamma'} - t_\Gamma \in \mathbb{N} \cup \{0\}$ and $supp\{\Gamma'\} = supp\{\Gamma\}$. In fact, there is a unique sequence Γ' such that $t_{\Gamma'} - t_\Gamma$ is minimal.*

Let $\Gamma = \{f_n(q)|n \in \mathbb{N}\}$ be a sequence of polynomials satisfying Functional Equation (2) whose field of coefficients is of characteristic zero. Let Γ' be the sequence of polynomials, satisfying Functional Equation (2) with field of coefficients $\mathbb{Q}$ such that $f_n(q)$ divides $f'_n(q)$ for all n and $t_{\Gamma'} - t_\Gamma$ is minimal, which is associated to Γ in the manner of Theorem 2.1. Then we say that Γ' is the sequence over $\mathbb{Q}$ associated to Γ (in the sense of Theorem 2.1).

Corollary 2.2. *Let $\Gamma = \{f_n(q)|n \in \mathbb{N}\}$ be a sequence of polynomials satisfying Functional Equation (2) whose field of coefficients is of characteristic zero. Suppose that the set of primes P associated to the support A_P of Γ contains at least two primes. Then t_Γ is an integer.*

The following result is one of the important consequences of Theorem 2.1, whose proof can be found in [4] where it is given as a conditional result with the condition being the above theorem.

Corollary 2.3. *If Γ is a sequence of polynomials satisfying Functional Equation (2) with field of coefficients of characteristic zero and t_Γ non-integral. Then the set of primes P associated to the support of Γ must have the form $P = \{p\}$ for some prime p.*

Before stating our next theorem, let us recall from [4] the definition of a minimal collection and polynomials of the same form.

Definition 2.4. Let $\{(a_i, b_i)|a_i \geq 1\}_i$ be a collection of finitely many ordered pairs of integers. $\{(a_i, b_i)|a_i \geq 1\}_i$ is called a **minimal** collection if $a_i \neq a_j$ whenever $i \neq j$.

Remark 2.5. For any collection of finitely many ordered pairs of integers

$$\{(a_i, b_i)|a_i \geq 1\}_i,$$

it can be verified that there exists a minimal collection $\{(a'_j, b'_j)\}_j$ satisfying the following conditions:

(1) For each j, $a'_j = a_i$ for some i.

(2) For each j, $b'_j = \sum_{\{i|a_i=a_j\}} b_i$.

This minimal collection is called the **minimal version** of $\{(a_i, b_i)|a_i \geq 1\}_i$. It can also be verified that for each collection of finitely many ordered pairs of integers $\{(a_i, b_i)|a_i \geq 1\}_i$ and its minimal version $\{(a'_j, b'_j)\}_j$, the rational functions $\prod_i([p]_{q^{a_i}})^{b_i}$ and $\prod_i([p]_{q^{a'_j}})^{b'_j}$ are equal.

Definition 2.6. (1) Two collections $\{(a_i, b_i)|a_i \geq 1\}_i$ and $\{(c_j, d_j)|c_j \geq 1\}_j$ of ordered pairs of integers are said to be **equivalent** if they have the same minimal version.

(2) Let $\{(a_i, b_i)|a_i \geq 1\}_i$ and $\{(c_j, d_j)|c_j \geq 1\}_j$ be two minimal collections of ordered pairs of integers. Two rational expressions $\prod_i([p]_{q^{a_i}})^{b_i}$ and $\prod_j([r]_{q^{c_j}})^{d_j}$ are said to be of the **same form** if the following conditions hold:

(1) For each i, $a_i = c_j$ for a unique j and vice versa for each j.

(2) For each i, $b_i = b_j$ whenever $a_i = c_j$.

It can be verified that being equivalent in the sense above is an equivalence relation. For any collection of finitely many ordered pairs of integers $\{(a_i, b_i)|a_i \geq 1\}_i$, we denote its equivalence class by $\|\{(a_i, b_i)|a_i \geq 1\}_i\|$. It can also be verified that each such equivalence class contains exactly one minimal collection.

Definition 2.7. (1) Let Γ_1 and Γ_2 be two sequences of polynomials, satisfying Functional Equation (2) with fields of coefficients of characteristic zero and support A_P for some set of primes P. If there exists a sequence Γ' which is the sequence over $\mathbb{Q}$ associated to Γ_1 and Γ_2 in the sense of Theorem 2.1, then we say that Γ_1 and Γ_2 are linked by Γ' and denoted by $\Gamma_1 \overset{\Gamma'}{\sim} \Gamma_2$.

(2) Let Γ' be a sequence of polynomials, satisfying Functional Equation (2) with fields of coefficients $\mathbb{Q}$ and support A_P for some set of primes P. The collection of all sequences of polynomials satisfying Functional Equation (2), with fields of coefficients of characteristic zero and support A_P, which are linked by Γ' is denoted by $\|\{\Gamma\}\|_{\Gamma'}$.

The relation of being linked by a sequence Γ' over $\mathbb{Q}$ above is an equivalence relation on the collection of all sequences of polynomials satisfying Functional Equation (2) with fields of coefficients of characteristic zero and support A_P. Thus $\|\{\Gamma\}\|_{\Gamma'}$ is an equivalence class for each Γ', and it is immediate that we have a disjoint union:

$$\Upsilon_P = \bigsqcup_{\Gamma'} \|\{\Gamma\}\|_{\Gamma'},$$

where the disjointness comes from the uniqueness of Γ' in Theorem 2.1.

Since all sequences of polynomials satisfying Functional Equation (2) with fields of coefficients of characteristic zero and t_Γ non-integral are characterized in [4], we are only concerned with the cases where $t_\Gamma \geq 1$ integral. In the case where $|P| = 1$ and t_Γ is integral, we classify completely all such sequences. In the case where $|P| \geq 2$, we classify all such sequences up to an equivalence relation whose equivalence classes have finite cardinalities. Our results are summarized in the following theorems.

Let $P = \{p_1, \ldots, p_l\}$ be a collection of distinct primes with $l \geq 1$ which may be finite or infinite.

Theorem 2.8. *Let Γ be a sequence of polynomials satisfying Functional Equation (2) with field of coefficients of characteristic zero and support A_P. Suppose $|P| = 1$ and t_Γ integral. Let $P = \{p\}$ and Υ_P be the collection of all sequences of polynomials satisfying Functional Equation (2) with fields of coefficients of characteristic zero and support $A_{\{p\}}$. Let $\Lambda := \{f(q)\}$ be the collection of all polynomials whose coefficients are contained in fields of characteristic zero and with deg$(f(q)) = t(p-1)$ for some integer t. Then there exists a bijection*

$$\begin{array}{ccc} \Lambda & \longrightarrow & \Upsilon_P, \\ f(q) & \longmapsto & \Gamma_{f(q)}, \end{array}$$

where

$$\Gamma_{f(q)} := \left\{ f_{p^n}(q) | f_1(q) = 1, f_p(q) = f(q), n \in \mathbb{N} \cup \{0\} \right\}$$

and $f_{p^n}(q) := f_p(q) f_{p^{n-1}}(q^p)$ for all $n \geq 0$.

Theorem 2.9. *Let Γ be a sequence of polynomials satisfying Functional Equation (2) with field of coefficients $\mathbb{Q}$ and support A_P. Suppose that $|P| = 2$.*

Let $\Upsilon_{P,\mathbb{Q}}$ be the collection of all sequences of polynomials satisfying Functional Equation (2) *with fields of coefficients* $\mathbb{Q}$ *and support* A_P. *Let* Ω *be the collection of equivalence classes of sets of finitely many ordered pairs of integers* $\|\{(a_i, b_i)\}_i\|$ *defined earlier and also in Theorem 2.1 of [4]. Then there is a bijection between* $\Upsilon_{P,\mathbb{Q}}$ *and* Ω:

$$\begin{array}{ccc} \Upsilon_{P,\mathbb{Q}} & \longrightarrow & \Omega, \\ \Gamma & \longmapsto & \|\{(a_i, b_i)\}_i\|_\Gamma, \end{array}$$

where $\|\{(a_i, b_i)\}_i\|_\Gamma$ *is such that*

$$f_n(q) = \prod_{i \in I} ([n]_{q^{a_i}})^{b_i}$$

for any collection of ordered pairs $\{(a_i, b_i)\}_i$ *in* $\|\{(a_i, b_i)\}_i\|_\Gamma$ *and all* $n \in supp\{\Gamma\}$ *(we may assume that* $\{(a_i, b_i)\}_i$ *is a minimal collection and refer to* $\|\{(a_i, b_i)\}_i\|_\Gamma$ *by this representative collection.*

Theorem 2.10. *Let* Γ *be a sequence of polynomials satisfying Functional Equation* (2) *with field of coefficients of characteristic zero and support* A_P. *Suppose that* $|P| = 2$. *Let* Υ_P *be the collection of all sequences of polynomials satisfying Functional Equation* (2) *with fields of coefficients of characteristic zero and support* A_P. *Let* $\|\Upsilon_P\|$ *denote the collection of all equivalence classes of* Υ_P *with respect to the equivalence relation* $\overset{\Gamma'}{\sim}$ *for each* $\Gamma' \in \Upsilon_{P,\mathbb{Q}}$. *Let* Ω *be as in (a). Then there exists a surjective map*

$$\begin{array}{ccc} \Upsilon_P & \overset{\psi}{\longrightarrow} & \Upsilon_{P,\mathbb{Q}} \cong \Omega, \\ \Gamma & \longmapsto & \Gamma', \end{array}$$

which induces the bijective map

$$\begin{array}{ccc} \|\Upsilon_P\| & \overset{\Psi}{\longrightarrow} & \Omega, \\ \|\{\Gamma\}\| & \longmapsto & \Gamma'_{\|\{\Gamma\}\|}, \end{array}$$

where $\Gamma'_{\|\{\Gamma\}\|}$ *is the sequence of polynomials over* $\mathbb{Q}$ *associated to any sequence* Γ *in* $\|\{\Gamma\}\|$. *Moreover, the cardinality of each fiber* $\|\{\Gamma\}\|_{\Gamma'}$ *of each* $\Gamma' \in \Upsilon_{P,\mathbb{Q}}$ *is finite.*

These Theorems give a solution to Problem 2 described earlier.

3. Proof of Main Results

Let us recall the following theorem, Theorem 2.1 of [4], since it is crucial in our work subsequently.

Theorem 3.1 ([4]). *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.*

(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*

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

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 contained $\mathbb{Q}$, satisfying Functional Equation* (2) *and the condition $deg(f_p(q)) = t_\Gamma(p-1)$ with integral $t_\Gamma \geq 1$ for all primes p. The latter condition means that 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.*

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. 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).

Furthermore, let us also recall some key concepts from [4] which will be used throughout this paper.

Let u be any positive integer and p be any prime number. The polynomial denoted by $P_{u,p}(q)$ or $P_{up}(q)$ is the irreducible cyclotomic polynomial in $\mathbb{Q}[q]$

whose roots are all primitive up-roots of unity. $P_{u,p}(q)$ is sometimes denoted by $P_{up}(q)$ or $P_v(q)$ where $v = up$. For a primitive n-root of unity α in $\mathbb{C}$, which can be written in the form $\alpha = e^{\frac{2\pi i w}{n}}$ for some primitive residue class w modulo n, we always identify α, via the Chinese Remainder Theorem, with the tuples $(u_i)_i$, where $\prod_i (p_i)^{m_i}$ is the prime factorization of n and $u_i \in (\mathbb{Z}/(p_i)^{m_i}\mathbb{Z})^*$ for each i such that $u_i \equiv w \pmod{p_i^{m_i}}$. The readers should see [4] for more details.

Definition 3.2. 1) Let $P_{u,p}(q)$ and $P_{u,r}(q)$ be the cyclotomic polynomials with coefficients in $\mathbb{Q}$ of orders up and ur respectively. Let $F_{u,p}(q)$ and $F_{u,r}(q)$ be two polynomials dividing $P_{u,p}(q)$ and $P_{u,r}(q)$ respectively. If $F_{u,p}(q)$ and $F_{u,r}(q)$ satisfy the condition that for each primitive residue class w modulo u, all the roots of $P_{u,p}(q)$ represented by the collection of tuples $\{(\gamma_p, (w_{p_j})_j) | \gamma_p = 1, \ldots, p-1\}$ if p does not divide u (resp. by the collection $\{(w_p + t(p^l), (w_{p_j})_{j, p_j \neq p}) | t = 0, \ldots \ldots, p-1\}$ if $p^l \| u$ for some positive integer $l \geq 1$) are roots $F_{u,p}(q)$ if and only if all the roots of $P_{u,r}(q)$ represented by the collection $\{\gamma_r, (w_{p_j})_j | \gamma_r = 1, \ldots, r-1\}$ if r does not divide u (resp. by the collection $\{w_r + s(r^h), (w_{p_j})_{j, p_j \neq r} | s = 0, \ldots, r-1\}$ if $r^h \| u$ for some positive integer $h \geq 1$) are roots $F_{u,r}(q)$, then we will say that $F_{u,p}(q)$ and $F_{u,r}(q)$ are **compatible**. For example, $P_{u,p}(q)$ and $P_{u,r}(q)$ are compatible for any positive integer u, primes p and r, a fact which is proven in [4] for the case where pr does not divide u as well as when either p or r dividing u.

2) Two polynomials $f_{u,p}(q)$ and $f_{u,r}(q)$ are said to be **super-compatible** if $f_{u,p}(q) = \prod_i (F^{(i)}_{u,p}(q))^{n_i}$ and $f_{u,r}(q) = \prod_i (F^{(i)}_{u,r}(q))^{n_i}$, where $F^{(i)}_{u,p}(q)$ and $F^{(i)}_{u,r}(q)$ are polynomials which are compatible for all i. In particular, $P_{u,p}(q)^n$ and $P_{u,r}(q)^n$ are super-compatible for any nonnegative integer n. Thus compatibility is a special case of super-compatibility.

Remark 3.3. To understand the rationality of this definition, the readers can consult [4]. The polynomials $F^{(i)}_{u,\Box}(q)$'s in the definition of super-compatible are not unique for any i, where $\Box$ denotes either p or r.

Let p and r be any distinct primes in the support of Γ. Define $f_{u_p,p}(q)$ to be the factor of $f_p(q)$ such that its roots consist of all the roots of $f_p(q)$ with multiplicities which are primitive pu_p-roots of unity. Then $f_p(q) = \prod_{u_{p,j} > u_{p,j+1}} f_{u_{p,j}}(q)$ in the ring $\mathbb{C}[q]$. Similarly, $f_r(q) = \prod_{u_{r,i} > u_{r,i+1}} f_{u_{r,i}}(q)$. We call j (resp. i) or interchangeably $u_{p,j}$ (resp. $u_{r,i}$) the j**-level** (resp. i**-level**) or $u_{p,j}$-level (resp. $u_{r,i}$-level) of $f_p(q)$ (resp. $f_r(q)$) if $f_{u_{p,j}}(q)$ (resp. $f_{u_{r,i}}(q)$) is a nontrivial factor of $f_p(q)$ (resp. $f_r(q)$). Define $V := \{v_{p,r,k} | v_{p,r,k} > v_{p,r,k+1}\} := \{u_{p,j}\}_j \cup \{u_{r,i}\}_i$. We refer to k or $v_{p,r,k}$ as the k**-bi-level** with respect to p and r or the $v_{p,r,k}$-bi--level of $f_p(q)$ and $f_r(q)$. Note that level i of $f_p(q)$ or $f_r(q)$ is not necessarily equal to the bi-level i of $f_p(q)$ and $f_r(q)$. Using V and these product decompositions, we write Functional Equation (1) with respect to $f_p(q)$ and $f_r(q)$ as:

$$\begin{array}{ccc}
f_{v_{p,r,1},p}(q)^{s_{v_{p,1}}} f_{v_{p,r,1},r}(q^p)^{s_{v_{r,1}}} & \stackrel{(1)}{\longleftrightarrow} & f_{v_{p,r,1},r}(q)^{s_{v_{r,1}}} f_{v_{p,r,1},p}(q^r)^{s_{v_{p,1}}} \\
\cdots & \cdots & \cdots \\
f_{v_{p,r,k},p}(q)^{s_{v_{p,k}}} f_{v_{p,r,k},r}(q^p)^{s_{v_{r,k}}} & \stackrel{(k)}{\longleftrightarrow} & f_{v_{p,r,k},r}(q)^{s_{v_{r,k}}} f_{v_{p,r,k},p}(q^r)^{s_{v_{p,k}}} \\
\cdots & \cdots & \cdots \\
f_p(q)f_r(q^p) & = & f_r(q)f_p(q^r),
\end{array}$$

where:

- $s_{p,k} = 1$ if $f_{v_{p,r,k},p}(q)$ nontrivially divides $f_p(q)$ (i.e., $f_{v_{p,r,k},p}(q) = f_{u_i,p}(q)$ for some u_i) and 0 otherwise.
- $s_{r,k} = 1$ if $f_{v_{p,r,k},r}(q)$ nontrivially divides $f_r(q)$ (i.e., $f_{v_{p,r,k},r}(q) = f_{u_i,r}(q)$ for some u_i) and 0 otherwise.
- $\prod_k f_{v_{p,r,k},p}(q)^{s_{v_{p,k}}} f_{v_{p,r,k}}(q^p)^{s_{v_{r,k}}} = f_p(q)f_r(q^p)$.
- $\prod_j f_{v_{p,r,k},r}(q)^{s_{v_{r,k}}} f_{v_{p,r,k}}(q^r)^{s_{v_{p,j}}} = f_r(q)f_p(q^r)$.
- The symbol $\stackrel{(j)}{\longleftrightarrow}$ indicates the functional equation (1) at the bi-level j (notes that the polynomial expressions on the left hand side and the right hand side of $\longleftrightarrow$ at each bi-level are not necessarily equal).

Note that for every level k, where $v_{p,r,k}$ appears in the equation above, either $s_{p,k} = 1$ or $s_{r,k} = 1$.

The above version of Functional Equation (1) will be called the **Expanded Functional Equation** (1) with respect to p and r, denoted by EFE(1). The EFE(1) above is said to be in **reduced form** (rf) if at each level k, where pr does not divide $v_{p,r,k}$, the line

$$f_{v_{p,r,k},p}(q)^{s_{v_{p,k}}} f_{v_{p,r,k},r}(q^p)^{s_{v_{r,k}}} \stackrel{(k)}{\longleftrightarrow} f_{v_{p,r,k},r}(q)^{s_{v_{r,k}}} f_{v_{p,r,k},p}(q^r)^{s_{v_{p,k}}}$$

in EFE (1) is replaced by

(i) $f_{v_{p,r,k},r}(q^p)^{s_{v_{r,k}}} \stackrel{(k)}{\longleftrightarrow} f_{v_{p,r,k},r}(q)^{s_{v_{r,k}}} \frac{f_{v_{p,r,k},p}(q^r)^{s_{v_{p,k}}}}{f_{v_{p,r,k},p}(q)^{s_{v_{p,k}}}}$ if $(r, v_{p,r,k}) = 1$.

(ii) $f_{v_{p,r,k},p}(q)^{s_{v_{p,k}}} \frac{f_{v_{p,r,k},r}(q^p)^{s_{v_{r,k}}}}{f_{v_{p,r,k},r}(q)^{s_{v_{r,k}}}} \stackrel{(k)}{\longleftrightarrow} f_{v_{p,r,k},p}(q^r)^{s_{v_{p,k}}}$ if $(p, v_{p,r,k}) = 1$, or

(iii) $\frac{f_{v_{p,r,k},p}(q^r)^{s_{v_{p,k}}}}{f_{v_{p,r,k},p}(q)^{s_{v_{p,k}}}} \stackrel{(k)}{\longleftrightarrow} \frac{f_{v_{p,r,k},r}(q^p)^{s_{v_{r,k}}}}{f_{v_{p,r,k},r}(q)^{s_{v_{r,k}}}}$ if $(pr, v_{p,r,k}) = 1$.

(iv) The line $f_p(q)f_r(q^p) = f_r(q)f_p(q^r)$ is replaced by $Q_{p,r}(t) = Q_{p,r}(t)$, where $Q_{p,r}(t)$ is the product of all expressions of the left hand columns (or the right hand column) after (i), (ii), (iii) have taken place, i.e.,

$$Q_{p,r}(q) = \frac{f_p(q)f_r(q^p)}{\prod_i f_{v_{p,r,i},r}(q)^{s_{r,i}(1-\delta_{p,i})} f_{v_{p,r,i},p}(q)^{s_{p,i}(1-\delta_{r,i})}}$$

$$= \frac{f_r(q)f_p(q^r)}{\prod_i f_{v_{p,r,i},r}(q)^{s_{r,i}(1-\delta_{p,i})} f_{v_{p,r,i},p}(q)^{s_{p,i}(1-\delta_{r,i})}}.$$

Remark 3.4. (1) The product of all the rational expressions in the left hand column and the product of those in the right hand column of the reduced form of the EFE(1) are equal, and thus can be denoted by the same polynomial $Q_{p,r}(t)$; (2) $Q_{p,r}(t)$ divides $f_{u_1,p}(q)f_{u_1,r}(q^p)$ and thus $f_{u_1,r}(q)f_{u_1,p}(q^r)$; (3) For each line (i), the product of all expressions on both sides of $\longleftrightarrow$ remains equal after *(i)*, *(ii)* or *(iii)* have taken place. It will be shown below that all the rational expressions above are actually polynomials when they occur, and that for each of these rational expressions, its roots are primitive roots of unity of the same order. Also, a reduced form of an EFE(1) is automatically in super reduced form without rearranging if and only if pr does not divide $v_{p,r,i}$ for all levels i.

If the factor(s) appearing in the left hand column and the right hand column of the reduced form of EFE(1) with respect to p and r can be rearranged within their corresponding columns (without changing the order of the levels, i.e., $v_{p,r,i} > v_{p,r,i+1}$ for all bi-levels i occurring in EFE(1)) so that $\overset{(i)}{\longleftrightarrow}$ can be replaced by $\overset{(i)}{=}$ at each bi-level $i \leq k$, then we say that the resulting reduced form is in **k-super reduced form**. If $\overset{(i)}{\longleftrightarrow}$ can be replaced by $\overset{(i)}{=}$ at all bi-level i, then we say that it is in **super reduced form** (see [4] for more details).

3.1. Proof of Theorem 2.1:

Let P be a collection of finitely many primes. Recall from [4] that there exists a sequence of polynomials satisfying Functional Equation (2) and whose field of coefficients is strictly greater than $\mathbb{Q}$ and support is of the form A_P. In fact, we show in [4] that for any finite set P of primes of cardinality at least 2, there exists a sequence of polynomials Γ satisfying Functional Equation (2) with field of coefficients strictly contains $\mathbb{Q}$ such that $\text{supp}\{\Gamma\} = A_P$. Such a sequence constructed in [4] is called a single-level sequence, i.e., there exists a unique positive integer $u > 1$ such that if $f_p(q)$ is an element of Γ, then all roots of $f_p(q)$ are primitive up-roots of unity. It is a special case of what we discuss subsequently in this paper, i.e. multi-level sequences with field of coefficients strictly greater than $\mathbb{Q}$.

Let Γ be a sequence of polynomials satisfying Functional Equation (2) whose field of coefficients is of characteristic zero. To prove Theorem 2.1, we may assume that the field of coefficients of Γ is strictly greater than $\mathbb{Q}$ since otherwise, we may define $\Gamma' := \Gamma$ and the theorem trivially holds. For each $p \in P$, let $\mathcal{J}_p$ be the collection of all levels u_i of $f_p(q)$ such that the coefficients of $f_{u_i,p}(q)$ are not properly contained in $\mathbb{Q}$. Then by our assumption, there exists at least one prime in P, say p_c, such that $\mathcal{J}_{p_c} \neq \emptyset$.

Proposition 3.5 (Key Proposition 1). *Let p be any prime in P. Then $\mathcal{J}_p \neq \emptyset$. Let k be the smallest positive integer such that the coefficients of $f_{v_{p,p_c,k},p_c}(q)$ are not properly contained in $\mathbb{Q}$. Then k is also the smallest positive integer such that the coefficients of $f_{v_{p,p_c,k},p}(q)$ are not properly contained in $\mathbb{Q}$.*

Proof. Let $V := \{v_{p_i,p_j,l}\}$ where $v_{p_i,p_j,l}$ appears in the EFE(1) with respect to any primes p_i and p_j in P. If $\mathcal{U}$ is the set of all distinct prime factors of any element of V, then $\mathcal{U}$ is a finite set by Key Proposition 2 of [4]. From the proof of Key Proposition 2 of [4], there is one case remained to be proved; namely both p and p_c are in $\mathcal{U}$. We employ a similar method as in [4] for this case. Let us assume that p and p_c are in $\mathcal{U}$. For notational convenience, in the rest of this proof, p_c will be denoted by r. Consider the reduced form of EFE(1) with respect to p and $p_c := r$

$$f_{v_{p,r,1},p}(q)^{s_{p,1}\delta_{r,1}} \frac{f_{v_{p,r,1},r}(q^p)^{s_{r,1}}}{f_{v_{p,r,1},r}(q)^{s_{r,1}(1-\delta_{p,1})}} \overset{(1)}{\leftrightarrow} f_{v_{p,r,1},r}(q)^{s_{r,1}\delta_{p,1}} \frac{f_{v_{p,r,1},p}(q^r)^{s_{p,1}}}{f_{v_{p,r,1},p}(q)^{s_{p,1}(1-\delta_{r,1})}}$$

$$\cdots\cdots\cdots$$

$$f_{v_{p,r,k},p}(q)^{s_{p,k}\delta_{r,k}} \frac{f_{v_{p,r,k},r}(q^p)^{s_{r,k}}}{f_{v_{p,r,k},r}(q)^{s_{r,k}(1-\delta_{p,k})}} \overset{(k)}{\leftrightarrow} f_{v_{p,r,k},r}(q)^{s_{r,k}\delta_{p,k}} \frac{f_{v_{p,r,k},p}(q^r)^{s_{p,k}}}{f_{v_{p,r,k},p}(q)^{s_{v_{p,k}}(1-\delta_{r,k})}}$$

$$\cdots\cdots\cdots$$

$$f_p(q)f_r(q^p) = f_r(q)f_p(q^r),$$

where $\delta_{\square,i}$ is 1 if $\square$ divides $v_{p,r,i}$ and $\delta_{\square,i}$ is 0 otherwise, with $\square$ represents either p or r.

If $k = 1$, then this lemma follows from Key Proposition 1 $'$ of [4]. Hence let us assume otherwise. Using the moving factors method in the proof of Key Proposition 2 of [4], we obtain the $(j-1)$-super-reduced form of EFE(1) with respect to p and r for any bi-level j of EFE(1) with respect to p and r. Suppose line (j) of the $(j-1)$-super-reduced form has the form

$$f_{v_{p,r,j},p}(q)^{s_{p,j}\delta_{r,j}} \frac{L(q) f_{v_{p,r,j},r}(q^p)^{s_{r,j}}}{f_{v_{p,r,j},r}(q)^{s_{r,j}(1-\delta_{p,j})}} \overset{(j)}{\longleftrightarrow} f_{v_{p,r,j},r}(q)^{s_{r,j}\delta_{p,j}} \frac{R(q) f_{v_{p,r,j},p}(q^r)^{s_{p,j}}}{f_{v_{p,r,j},p}(q)^{s_{p,j}(1-\delta_{r,j})}},$$

where $L(q) = f_{v_{p,r,m},p}(q)$ and $R(q) = f_{v_{p,r,n},r}(q)$, for some bi-levels m and n such that $m, n \leq (j-1)$ and $v_{p,r,m} = v_{p,r,j}r$ as well as $v_{p,r,n} = v_{p,r,j}p$, which are moved to line (j) by the moving factor process to obtain the $(j-1)$-super-reduced form of EFE(1) with respect to p and r (see the proof of Key Proposition 2 of [4]).

It can be verified that

$$\frac{L(q)f_{v_{p,r,j},r}(q^p)^{s_{r,j}}}{f_{v_{p,r,j},r}(q)^{s_{r,j}(1-\delta_{p,j})}} = \frac{R(q)f_{v_{p,r,j},p}(q^r)^{s_{p,j}}}{f_{v_{p,r,j},p}(q)^{s_{p,j}(1-\delta_{r,j})}}.$$

From now on, we refer to factors such as $L(q)$ and $R(q)$ as the left and right moving factors respectively for short to indicate such factors in the moving factor process employed in the proof of Key Proposition 2 of [4] as well as here.

Lemma 3.6. *The coefficients of the polynomials $L(q)$ and $R(q)$ above are properly contained in $\mathbb{Q}$.*

Proof. If $L(q) = 1$ and $R(q) = 1$, then there is nothing to prove. Hence we may assume that either $L(q) \neq 1$ or $R(q) \neq 1$. Let us consider line (k) of the (k-1)-super-reduced form of EFE(1) with respect to p and r which has the form:

$$f_{v_{p,r,k},p}(q)^{s_{p,k}\delta_{r,1}}\frac{L(q)f_{v_{p,r,k},r}(q^p)}{f_{v_{p,r,k},r}(q)^{(1-\delta_{p,k})}} \overset{(k)}{\longleftrightarrow} f_{v_{p,r,k},r}(q)^{s_{r,k}\delta_{p,k}}\frac{R(q)f_{v_{p,r,k},p}(q^r)^{s_{p,k}}}{f_{v_{p,r,k},p}(q)^{s_{p,k}(1-\delta_{r,k})}},$$

where $s_{r,k} = 1$ holds by definition of k. Thus

$$\frac{L(q)f_{v_{p,r,k},r}(q^p)}{f_{v_{p,r,k},r}(q)^{(1-\delta_{p,k})}} = \frac{R(q)f_{v_{p,r,k},p}(q^r)^{s_{p,k}}}{f_{v_{p,r,k},p}(q)^{s_{p,k}(1-\delta_{r,k})}}.$$

It can be verified from the analysis in [4] that for any bi-level i of EFE(1) with respect to p and r, the coefficients of $f_{v_{p,r,i},\square}(q)$ are contained in $\mathbb{Q}$ if an only if the coefficients of $\frac{f_{v_{p,r,i},\square}(q^{\triangle})}{f_{v_{p,r,i},\square}(q)^{\delta_{\triangle,i}}}$ are contained in $\mathbb{Q}$ (hint: if one is a cyclotomic polynomial, then so is the other).

Claim.

(a) The coefficients of $R(q)$ are properly contained in $\mathbb{Q}$.
(b) The coefficients of $L(q)$ are properly contained in $\mathbb{Q}$.

Proof of claim. (a) If $R(q) = 1$, then there is nothing to prove. Thus let us assume that $R(q) \neq 1$. Therefore, $R(q) = f_{v_{p,r,i},r}(q)$ for some bi-level i such that $v_{p,r,i} = v_{p,r,k}p$ (see the moving factors process in [4]). Hence $v_{p,r,i} > v_{p,r,k}$ and thus $i < k$. By definition of k, the coefficients of $f_{v_{p,r,i},r}(q)$, and thus those of $R(q)$, must be contained in $\mathbb{Q}$ as required.

(b) Again we may assume that $L(q) \neq 1$. Thus $L(q)$ must possess at least one root, say α. Hence it can be deduced that $L(q) = f_{v_{p,r,i},p}(q)$ for some bi-level i such that $\delta_{r,i} = 1$ and $v_{p,r,i} = v_{p,r,k}r$ from the moving factor process in the proof of Key Proposition 2 of [4]. Thus $v_{p,r,i} > v_{p,r,k}$ and $i < k$. If the coefficients of $f_{v_{p,r,i},p}(q)$ are contained in $\mathbb{Q}$, then we are done. Otherwise, the coefficients of $f_{v_{p,r,i},p}(q^r)$ are also not properly contained in $\mathbb{Q}$.

On the other hand, the coefficients of $f_{v_{p,r,i},r}(q)$ and thus those of $f_{v_{p,r,i},r}(q^p)$ are contained in $\mathbb{Q}$. It can be verified that line (i) of the $(i-1)$-super-reduced form of EFE(1) with respect to p and r has the form

$$f_{v_{p,r,i},p}(q)^{s_{p,i}\delta_{r,i}} \frac{L_i(q) f_{v_{p,r,i},r}(q^p)^{s_{r,i}}}{f_{v_{p,r,i},r}(q)^{s_{r,i}(1-\delta_{p,i})}} \overset{(i)}{\longleftrightarrow} f_{v_{p,r,i},r}(q)^{s_{r,i}\delta_{p,i}} \frac{R_i(q) f_{v_{p,r,i},p}(q^r)^{s_{p,i}}}{f_{v_{p,r,i},p}(q)^{s_{p,i}(1-\delta_{r,i})}}$$

with

$$\frac{L_i(q) f_{v_{p,r,i},r}(q^p)^{s_{r,i}}}{f_{v_{p,r,i},r}(q)^{s_{r,i}(1-\delta_{p,i})}} = \frac{R_i(q) f_{v_{p,r,i},p}(q^r)^{s_{p,i}}}{f_{v_{p,r,i},p}(q)^{s_{p,i}(1-\delta_{r,i})}},$$

where $L_i(q)$ and $R_i(q)$ are the left and right moving factors respectively. By the assumption on k, the coefficients of $R_i(q)$ are contained in $\mathbb{Q}$. From the moving factor process, $L_i(q) = f_{v_{p,r,x},p}(q)$ and $R_i(q) = f_{v_{p,r,y},r}(q)$ for some bi-levels $x < i$ and $y < i$ such that $v_{p,r,x} = v_{p,r,i}r$ and $v_{p,r,y} = v_{p,r,i}p$. The argument can then be repeated at bi-level x and so forth obtaining the sequence $i_1 = k > \ldots > i_z$, where either $i_z = 1$ or i_z is the first bi-level of EFE(1) in this sequence, where the coefficients of $L_{i_z}(q)$ are contained in $\mathbb{Q}$ and $s_{i_2,p}\delta_{r,i_2} = \ldots = s_{i_z,p}\delta_{r,i_z} = 1$. By the definition of k and Key Proposition $1'$ of [4], the coefficients of $f_{v_{p,r,1},p}(q)$ are contained in $\mathbb{Q}$ and

$$\frac{f_{v_{p,r,1},r}(q^p)}{f_{v_{p,r,1},r}(q)^{(1-\delta_{p,1})}} = \frac{f_{v_{p,r,1},p}(q^r)}{f_{v_{p,r,1},p}(q)^{(1-\delta_{r,1})}}.$$

Therefore, $L_1(q) = 1$ (whose coefficient is in $\mathbb{Q}$) for $i_z = 1$. Now let us reverse the process. From line (i_z) of the $(i_z - 1)$-super reduced form, the coefficients of $\frac{L_{i_z}(q) f_{v_{p,r,i_z},r}(q^p)^{s_{r,i_z}}}{f_{v_{p,r,i_z},r}(q)^{s_{r,i_z}(1-\delta_{p,i_z})}}$ are contained in $\mathbb{Q}$ by definition of k and i_z. From the definition of k and the moving factor process, we know that the coefficients of $R(i_z(q))$ are also in $\mathbb{Q}$. Therefore, the coefficients of $\frac{f_{v_{p,r,i_z},p}(q^r)}{f_{v_{p,r,i_z},p}(q)^{(1-\delta_{r,i_z})}}$ are in $\mathbb{Q}$. Hence so are the coefficients of $f_{v_{p,r,i_z},p}(q) = L_{i_{z-1}}(q)$. Similar as above, this implies that the coefficients of $f_{v_{p,r,i_{z-1}},p}(q)$ are in $\mathbb{Q}$. By repeating this argument, we must have the coefficients of $L(q) = L_1(q)$ are contained in $\mathbb{Q}$. The claim is thus proved. □

Since

$$\frac{L(q) f_{v_{p,r,k},r}(q^p)}{f_{v_{p,r,k},r}(q)^{(1-\delta_{p,k})}} = \frac{R(q) f_{v_{p,r,k},p}(q^r)^{s_{p,k}}}{f_{v_{p,r,k},p}(q)^{s_{p,k}(1-\delta_{r,k})}},$$

and the coefficients of $\frac{f_{v_{p,r,k},r}(q^p)}{f_{v_{p,r,k},r}(q)^{(1-\delta_{p,k})}}$ are not contained in $\mathbb{Q}$, neither do the coefficients of $\frac{f_{v_{p,r,k},p}(q^r)^{s_{p,k}}}{f_{v_{p,r,k},p}(q)^{s_{p,k}(1-\delta_{r,k})}}$ by the above claim. Therefore, the coefficients of $f_{v_{p,r,k},p}(q)$ are also not contained in $\mathbb{Q}$. Furthermore, this also implies that $s_{p,k} = 1$ ($s_{r,k} = 1$ by the assumption on $r = p_c$).

$\square$

(1) Single-level sequences: Let $P = \{p_i\}$ be a collection of finitely (or infinitely) many primes such that $p_i - 1$ is divisible by some positive integer $u > 1$ for all i. For example $P = \{7, 13\}$ and $u = 6$. Let $P_{u,p_i}(q)$ be the cyclotomic polynomial with coefficients in $\mathbb{Q}$ of order up_i. Then its roots are represented by the collection of tuples $\{(w_{p_i}, u^*)|1 \le w_{p_i} \le p_i - 1; u^* \in (\mathbb{Z}/u\mathbb{Z})^*\}$ (see [4]). Let A be any nonempty subset of $(\mathbb{Z}/u\mathbb{Z})^*$. Then the collection of polynomials $P'_{u,p_i}(q)$ dividing $P_{u,p_i}(q)$, whose roots are represented by the collection $\{(w_{p_i}, w^*)|1 \le w_{p_i} \le p_i - 1; w^* \in A\}$ satisfies Functional Equation (1) by Key Proposition 1 in [4]. By Theorem 1.7, the collection $\{(P'_{u,p_i}(q))^n|p_i \in P\}$ determines a unique non-trivial sequence $\Gamma_{A,n}$ of polynomials satisfying Functional Equation (2). If A is a nonempty proper subset of $(\mathbb{Z}/u\mathbb{Z})^*$, then the field of coefficients of $\Gamma_{A,n}$ is strictly greater than $\mathbb{Q}$ for each $n \in \mathbb{N}$. For each $n \in \mathbb{N}$, the collection $\{(P_{u,p_i}(q))^n|p_i \in P\}$ is a nontrivial sequence of polynomials satisfying Functional Equation (1) with field of coefficients $\mathbb{Q}$. For each $n \in \mathbb{N}$, let $\Gamma'_{A,n}$ be the sequence of polynomials, satisfying Functional Equation (2), induced by the sequence $\{(P_{u,p_i}(q))^n|p_i \in P\}$ in the manner of Theorem 1.7. It can be verified that $\Gamma'_{A,n}$ satisfies the desired requirements of Theorem 2.1 with $\mathbb{N} \cup \{0\} \ni t_{\Gamma'_{A,n}} - t_{\Gamma_{A,n}}$ minimal. It can be verified from [4] that all sequences Γ of polynomials satisfying the hypothesis of Theorem 2.1, which are single-level, must be of the form $\Gamma = \prod_{A_i,n_i} \Gamma_{A_i,n_i}$ for some collection of finitely many ordered pairs $I = \{(A_i, n_i)\}$, i.e., $f_n(q) = \prod_i f_{A_i,n_i}(q)$ with $f_{A_i,n_i}(q) \in \Gamma_{A_i,n_i}$ for all $f_n(q) \in \Gamma$. Suppose that $A_i \cup A_j \subseteq (\mathbb{Z}/u\mathbb{Z})^*$ with $n_i \le n_j$ for some i, j. Then we can replace Γ_{A_i,n_i} and Γ_{A_j,n_j} by $\Gamma_{A'_i,n'_i}$ and $\Gamma_{A'_j,n'_j}$ in the above product, where

- $A'_i = A_i \cup' A_j$ with $n'_i = n_i$, and
- $A'_j = A_j$ with $n'_j = n_j - n_i$

with $\cup'$ denoting the union which takes into account multiplicity (e.g. $\{1\} \cup' \{1, 2\} = \{1, 1, 2\}$), since it can be verified that $\Gamma_{A_i,n_i}\Gamma_{A_j,n_j} = \Gamma_{A'_i,n'_i}\Gamma_{A'_j,n'_j}$. By iterating this process, we may assume that $\Gamma = \prod_{A_i,n_i} \Gamma_{A_i,n_i}$ where $A_i \cup A_j$ is not a subset of $(\mathbb{Z}/u\mathbb{Z})^*$ for any $i \ne j$. Then the corresponding sequence $\Gamma' = \prod_{A_i,n_i} \Gamma'_{A_i,n_i}$ satisfies the requirements of Theorem 2.1 and thus is the associated sequence to Γ over $\mathbb{Q}$. Therefore Theorem 2.1 is proven for this case.

(2) Multi-level sequences: First let us show the existence of a multi-level sequence of polynomials Γ satisfying Functional Equation (2) whose field of coefficients strictly contains $\mathbb{Q}$. Suppose that $P = \{p_j|j = 1, \ldots, t\}$ is a set of primes.

Let $u_1 > 1$ and $u_2 > 1$ be two distinct positive integers such that u_1 and u_2 divide $p_i - 1$ for every prime p_i in P. For example take $P = \{7, 13\}$, $u_1 = 3$ and $u_2 = 6$. Let $\mathcal{U}_1$ and $\mathcal{U}_2$ be subsets of $(\mathbb{Z}/u_1\mathbb{Z})^*$ and $(\mathbb{Z}/u_2\mathbb{Z})^*$ respectively. Let Γ_1 and Γ_2 as well as Γ'_1 and Γ'_2 be the sequences of polynomials obtained as in (1) with u being replaced by u_1 and u_2 respectively. Let $\Gamma := \prod_{1\leq i\leq 2}\Gamma_i$ and $\Gamma' := \prod_{1\leq i\leq 2}\Gamma'_i$ be the associated sequence to Γ over $\mathbb{Q}$. Then Γ and Γ' are the sequences of polynomials whose supports are of the form A_P, where $P = \{p_j | j = 1, \ldots, t\}$, satisfying the requirements of Theorem 2.1 and having two levels. This is the simplest kind of multi-level sequences. In fact, it can be seen from [4] and the subsequent parts of this paper that more general multi-level sequences of polynomials, with support of the form A_P for some set of primes P, whose fields of coefficients are of characteristic zero.

Suppose $\Gamma = \{f_n(q) | n \in \mathbb{N}\}$ is a sequence of polynomials satisfying Functional Equation (2) with field of coefficients of characteristic zero and support of the form A_P for some set of prime P. Since it would be trivial otherwise, we may assume without loss of generality that the field of coefficients of Γ strictly contains $\mathbb{Q}$.

Now we begin the construction of the sequence of polynomials

$$\Gamma' := \{f'_n(q) | n \in \mathbb{N}\},$$

with support being of the form A_P and satisfying Functional Equation (2), associated to Γ such that $f_{p_j}(q)$ divides $f'_{p_j}(q)$ for each $p_j \in P$, the field of coefficients of Γ' is $\mathbb{Q}$ and $\mathbb{N} \ni t_{\Gamma'} - t_\Gamma$ minimal. Let p be any prime in P. As in [4], we can write:

$$f_p(q) = \prod_i f_{u_i,p}(q),$$

where $f_{u_i,p}(q)$ is the nontrivial factor of $f_p(q)$ whose roots are all roots of $f_p(q)$ which are primitive u_ip-roots of unity for some positive integer u_i. By our assumption on the field of coefficients of Γ, we see from the introduction that Γ is not a constant sequence. Thus there exists at least one prime $p_l \in P$ such that $f_{p_l}(q)$ is not a constant polynomial, which in turns means that $f_{u_{i_{p_l}},p_l}(q)$ is nontrivial for some positive integer $u_{i_{p_l}}$. By [4], this implies that for each $p_j \in P$, there exists some integer $u_{i_{p_j}}$ such that $f_{u_{i_{p_j}},p_j}$ is nontrivial. Thus without loss of generality, we may assume that each factor $f_{u_i,p_j}(q)$ appearing in the product $f_{p_j}(q) = \prod_i f_{u_i,p_j}(q)$ is nontrivial for each $p_j \in P$.

For each i, let n_i be the smallest positive integer such that $f_{u_i,p}(q)$ divides $(P_{u_i,p}(q))^{n_i}$, where $P_{u_i,p}(q)$ is the cyclotomic polynomial, with coefficients contained in $\mathbb{Q}$, of order u_ip.

Construction Algorithm: This algorithm is designed to construct a sequence of polynomials $\Gamma^* = \{f^*_{p_j}(q)|p_j \in P\}$ whose coefficients are contained in $\mathbb{Q}$, satisfying Functional Equation (1), of minimal degree such that $f_{p_j}(q)$ divides $f^*_{p_j}(q)$ for each $p_j \in P$. This is equivalent to constructing a sequence of polynomials of the form $\prod_i([p_j]_{q^{a_i}})^{b_i}$ satisfying Functional Equation (1), of minimal degree such that $f_{p_j}(q)$ divides $\prod_i([p_j]_{q^{a_i}})^{b_i}$ for each $p_j \in P$ by Theorem 2.1 of [4].

Step 1: For each $p_j \in P$, define $f^*_{p_j}(q) := \prod_i(P_{u_i,p_j}(q))^{n_{ij}}$ where n_{ij} is the smallest positive integer such that $f_{u_i,p_j}(q)$ divides $(P_{u_i,p_j}(q))^{n_{ij}}$. Then the coefficients of $f^*_{p_j}(q) := \prod_i(P_{u_i,p_j}(q))^{n_{ij}}$ are contained in $\mathbb{Q}$. If the sequence $\Gamma^* = \{f^*_{p_j}(q)|p_j \in P\}$ satisfies Functional Equation (1), then the algorithm stops since there exists a unique sequence of polynomials $\Gamma' = \{f'_n(q)|n \in \mathbb{N}\}$ with support of the form A_P where $f'_{p_j}(q) = f^*_{p_j}(q)$ satisfying Functional Equation (2) by Theorem 1.7. Furthermore, the sequence Γ' also satisfies requirement of Theorem 2.1 concerning the minimality of $t_{\Gamma'} - t_\Gamma$ since $f'_{p_j}(q)$ has coefficients contained in $\mathbb{Q}$ if and only if $f'_{u_i,p_j}(q)$ does for all i (see [4]) which in terns implies that $f'_{u_i,p_j}(q)$ must be a power of $P_{u_i,p_j}(q)$ for each i (also see [4]). Otherwise we proceed to Step 2.

Step 2: By Theorem 2.1 of [4], $f^*_{p_j}(q) = \prod_i([p]_{q^{a_{ij}}})^{b_{ij}}$ for some collection of finitely many ordered pairs of integers $\{(a_{ij}, b_{ij})|a_{ij} \geq 1\}_i$ for each $p_j \in P$. Since we are going to build the sequence Γ' of polynomials satisfying Functional Equation (1) in a series of successive steps, we denote $f^*_{p_j}(q) = \prod_i([p]_{q^{a_{ij}}})^{b_{ij}}$ by $f^{(0)}_{p_j}(q) = \prod_i([p]_{q^{a^{(0)}_{ij}}})^{b^{(0)}_{ij}}$ for each $p_j \in P$. By assumption, $\Gamma^* = \{f^*_{p_j}(q)|p_j \in P\}$ does not satisfy Functional Equation (1). By Theorem 2.1 of [4], there must exist two primes, say p_1 and p_2 in P (re-indexing P if necessary), such that $f^{(0)}_{p_1}(q) = \prod_i([p_1]_{q^{a^{(0)}_{i1}}})^{b^{(0)}_{i1}}$ and $f^{(0)}_{p_2}(q) = \prod_i([p_2]_{q^{a^{(0)}_{i2}}})^{b^{(0)}_{i2}}$ does not have the same form, where $\Psi^{(0)}_1 = \{(a^{(0)}_{i1}, b^{(0)}_{i1})|a^{(0)}_{i1} \geq 1\}_i$ and $\Psi^{(0)}_2 = \{(a^{(0)}_{i2}, b^{(0)}_{i2})|a^{(0)}_{i2} \geq 1\}_i$ are minimal collections. By re-indexing, we may assume that $a_{i1} > a_{(i+1)1}$ and $a_{i2} > a_{(i+1)2}$ for each i. Hence there exists at least one index l where (1) either $a^{(0)}_{l1} \neq a^{(0)}_{i2}$ or $a^{(0)}_{l2} \neq a^{(0)}_{i1}$ for all i, or (2) there exists an index i such that $a^{(0)}_{l1} = a^{(0)}_{i2}$ but $b^{(0)}_{l1} \neq b^{(0)}_{i2}$ or $a^{(0)}_{l2} = a^{(0)}_{i1}$ but $b^{(0)}_{l2} \neq b^{(0)}_{i1}$. Note that the index i in (2) is unique, if it exists, by the minimality of the collections Ψ_1, Ψ_2. Since (1) can be viewed as a special case of (2), we include (1) in (2) and treat only case (2). Let A be the maximal collection of indexes l where $a^{(0)}_{l1} = a^{(0)}_{i2}$ but $b^{(0)}_{l1} \neq b^{(0)}_{i2}$ or $a^{(0)}_{l2} = a^{(0)}_{i1}$ but $b^{(0)}_{l2} \neq b^{(0)}_{i1}$ for some i. For each $l \in A$, we denote such i by i_l since it is unique by the minimality of the collections Ψ_1, Ψ_2. A can be partitioned into four disjoint sub-collections:

(i) $A_1 \subseteq A$ consisting of indexes l such that $a_{l1}^{(0)} = a_{i_l 2}^{(0)}$ and $b_{l1}^{(0)} > b_{i_l 2}^{(0)}$ for some i_l with $b_{l1}^{(0)} \geq 0$, and $A_1' \subseteq A$ consisting of indexes l such that $a_{l1}^{(0)} = a_{i_l 2}^{(0)}$ and $b_{l1}^{(0)} > b_{i_l 2}^{(0)}$ for some i_l with $b_{l1}^{(0)} < 0$.

(ii) $A_2 \subseteq A$ consisting of indexes l such that $a_{l2}^{(0)} = a_{i_l 1}^{(0)}$ and $b_{l2}^{(0)} > b_{i1}^{(0)}$ for some i_l with $b_{l2}^{(0)} \geq 0$, and $A_2' \subseteq A$ consisting of indexes l such that $a_{l2}^{(0)} = a_{i_l 1}^{(0)}$ and $b_{l2}^{(0)} > b_{i_l 1}^{(0)}$ for some i_l with $b_{l2}^{(0)} < 0$.

Let A_2^* be the maximal subset of A_2' such that

$$\frac{\prod_{l \in A_1} ([p_2]_{q^{a_{l1}^{(0)}}})^{b_{l1}^{(0)} - b_{i_l 2}^{(0)}}}{\prod_{l \in A_2^*} ([p_2]_{q^{a_{l2}^{(0)}}})^{e_l}}$$

is a polynomial for some $e_l \in \{1, \ldots, b_{l2}^{(0)} - b_{i_l 1}^{(0)}\}$ for each $l \in A_2^*$. Note that A_2^* could be empty and in such a case, $\prod_{l \in A_2^*} ([p_2]_{q^{a_{l1}^{(0)}}})^{e_l}$ is defined to be 1.

Define

$$E_1(q) := \frac{\prod_{l \in A_1} ([p_2]_{q^{a_{l1}^{(0)}}})^{b_{l1}^{(0)} - b_{i_l 2}^{(0)}}}{\prod_{l \in A_2^*} ([p_2]_{q^{a_{l1}^{(0)}}})^{m_l^{(0)}}},$$

where $m_l^{(0)}$ is the greatest integer in $\{1, \ldots, b_{l2}^{(0)} - b_{i_l 1}^{(0)}\}$ such that

$$\frac{\prod_{l \in A_1} ([p_2]_{q^{a_{l1}^{(0)}}})^{b_{l1}^{(0)} - b_{i_l 2}^{(0)}}}{\prod_{l \in A_2^*} ([p_2]_{q^{a_{l1}^{(0)}}})^{m_l^{(0)}}}$$

is an integer for each $l \in A_2^*$. Similarly, let A_1^* be the maximal subset of A_1' such that

$$\frac{\prod_{l \in A_2} ([p_1]_{q^{a_{l2}^{(0)}}})^{b_{l2}^{(0)} - b_{i_l 1}^{(0)}}}{\prod_{l \in A_1^*} ([p_1]_{q^{a_{l2}^{(0)}}})^{e_l}}$$

is a polynomial for some $e_l \in \{1, \ldots, b_{l2}^{(0)} - b_{i_l 1}^{(0)}\}$ for each $l \in A_1^*$. Note that A_1^* could be empty.

Define

$$E_2(q) := \frac{\prod_{l \in A_2} ([p_1]_{q^{a_{l2}^{(0)}}})^{b_{l2}^{(0)} - b_{i_l 1}^{(0)}}}{\prod_{l \in A_1^*} ([p_1]_{q^{a_{l2}^{(0)}}})^{m_l^{(0)}}},$$

where $m_l^{(0)}$ is the greatest integer in $\{1, \ldots, b_{l2}^{(0)} - b_{i_l 1}^{(0)}\}$ such that

$$\frac{\prod_{l \in A_1} ([p_1]_{q^{a_{l2}^{(0)}}})^{b_{l2}^{(0)} - b_{i_l 1}^{(0)}}}{\prod_{l \in A_2^*} ([p_1]_{q^{a_{l2}^{(0)}}})^{m_l^{(0)}}}$$

is an integer for each $l \in A_1^*$.

Next let us multiply the polynomial $f_{p_2}^{(0)}(q) = \prod_i ([p_2]_{q^{a_{i2}^{(0)}}})^{b_{i2}^{(0)}}$ by the polynomial $E_1(q)$ and $f_{p_1}^{(0)}(q) = \prod_i ([p_1]_{q^{a_{i1}^{(0)}}})^{b_{i1}^{(0)}}$ by the polynomial $E_2(q)$ and denote the results by $f_{p_2}^{(1)}(q)$ and $f_{p_1}^{(1)}(q)$ respectively. Let

$$\Psi_1^{(1)} := \{(a_{i1}^{(1)}, b_{i1}^{(1)}) | a_{i1}^{(1)} > a_{(i+1)1}^{(1)}\}_i$$

and

$$\Psi_2^{(1)} := \{(a_{i2}^{(1)}, b_{i2}^{(1)}) | a_{i2}^{(1)} > a_{(i+1)2}^{(1)}\}_i,$$

where $f_{p_1}^{(1)}(q) = \prod_i ([p_1]_{q^{a_{i1}^{(1)}}})^{b_{i1}^{(1)}}$ and $f_{p_2}^{(1)}(q) = \prod_i ([p_2]_{q^{a_{i2}^{(1)}}})^{b_{i2}^{(1)}}$. Again we re-index so that $a_{i1} > a_{(i+1)1}$ and $a_{i2} > a_{(i+1)2}$ for all i. Note that at this point, if $a_{l1}^{(1)} = a_{i_l 2}^{(1)}$ with either $b_{l1}^{(1)}$ or $b_{i_l 2}^{(1)}$ being nonnegative, then $b_{l1}^{(1)} = b_{i_l 2}^{(1)}$. This is a direct consequence of the minimality of the collections Ψ_1 and Ψ_2 as well as the disjointness of the subsets A_i and A_i' for $i = 1, 2$.

Let B_1 be the collection of indexes l, where $a_{l1}^{(1)} = a_{i_l 2}^{(1)}$ and $b_{i1}^{(1)} < b_{l2}^{(1)} < 0$. Let B_2 be the collection of indexes l, where $a_{l2}^{(1)} = a_{i_l 1}^{(1)}$ and $b_{l2}^{(1)} < b_{l1}^{(1)} < 0$. Note that B_1 and B_2 can be empty. Define

$$F_1(q) = \prod_{i \in B_1} ([p_2]_{q^{a_{l1}^{(1)}}})^{b_{l2}^{(1)} - b_{l1}^{(1)}}$$

and

$$F_2(q) = \prod_{i \in B_2} ([p_1]_{q^{a_{l2}^{(1)}}})^{b_{l1}^{(1)} - b_{l2}^{(1)}}.$$

If B_1 or B_2 are empty, then we let $F_1(q) := 1$ or $F_2(q) := 1$ respectively. Let $f_{p_1}^{(2)}(q) = F_2(q) f_{p_1}^{(1)}(q)$ and $f_{p_2}^{(2)}(q) = F_1(q) f_{p_2}^{(1)}(q)$. If $|P| = 2$, then the algorithm stops. Otherwise go to Step 3.

Note that if we can show that $f_{p_1}^{(2)}(q)$ and $f_{p_2}^{(2)}(q)$ satisfy Functional Equation (1), then they induce a sequence Γ', by Theorem 1.7, satisfying Functional Equation (2). We show later that in such case, Γ' has all the requirements of Theorem 2.1. Thus if $|P| = 2$, we are done.

Remark 3.7. Step 2 is in fact a necessary step in some cases (it is not difficult to construct, using the work of [4], a sequence where Step 1 alone is not sufficient for our purpose; we leave it to the readers).

Step 3. Let p_3 be another prime in P distinct from p_1 and p_2. At this step we already have $f^{(2)}(q)$ and $f^{(2)}_{p_2}(q)$ from Step 2. Let us denote them by $f^{(2_{p_1},_{p_2})}_{p_1}(q)$ and $f^{(2_{p_1},_{p_2})}_{p_2}(q)$ respectively. Let us apply the process of Step 2 to the polynomials $f^{(2_{p_1},_{p_2})}_{p_1}(q)$ and $f^{(0)}_{p_3}(q)$. Let $f^{(2_{p_1},_{p_3})}_{p_1}(q)$ and $f^{(2_{p_1},_{p_3})}_{p_3}(q)$ denote the resulting polynomials. Let $G(q)$ denote the polynomial obtained as a result of Step 2 such that $f^{(2_{p_1},_{p_3})}_{p_1}(q) = G(q)f^{(2_{p_1},_{p_2})}_{p_1}(q)$. By Theorem 2.1 of [4], $G(q) = \prod_i([p_1]_{q^{c_{i1}}})^{d_{i1}}$ for some minimal collection of ordered pairs of integers $\{(c_{i1}, d_{i1})|c_{i1} \geq 1\}_i$. Let $f^{(2_{p_1},_{p_3})}_{p_2}(q) := \prod_i([p_2]_{q^{c_{i1}}})^{d_{i1}} f^{(2_{p_1},_{p_2})}_{p_2}(q)$.

Next we repeat Step 3 for each successive prime in P to obtain a sequence of polynomials $\{f^{(2_{p_1},_{p_z})}_{p_i}(q)|1 \leq i \leq z\}$ for $1 < z \leq |P|$ where $|P|$ is either finite or infinite. It will be shown subsequently that each such sequence satisfies all the required properties and thus induces uniquely a sequence Γ_z of polynomials, with the same field of coefficients and support A_{P_z} where $P_z = \{p_1, \ldots, p_z\}$, satisfying Functional Equation (2) in the manner of Theorem 1.7.

Proposition 3.8. *(Key Proposition 2)*

Let $z \in \{2, \ldots, |P|\}$ be a positive integer. Let $\Gamma^{\partial}_z := \{f^{(2_{p_1},_{p_z})}_{p_i}(q)|1 \leq i \leq z\}$ be the sequence of polynomials resulting from Step 3 above. Then

(i) The polynomials in Γ^{∂}_z, which have coefficients in $\mathbb{Q}$, satisfy Functional Equation (1). There exists an integer, denoted by $t_{\Gamma^{\partial}_z}$, such that

$$deg(f^{(2_{p_1},_{p_z})}_{p_i}(q)) = t_{\Gamma^{\partial}_z}(p_i - 1)$$

for $1 \leq i \leq z$.

(ii) Let Γ'_z be the sequence of polynomials satisfying Functional Equation (2) induced by Γ^{∂}_z using Theorem 1.7. Then for any $z > 1$, Γ'_z satisfies Theorem 2.1, with Γ replaced by Γ_z which is obtained from Γ by restricting the set of primes P to $P_z = \{p_1, \ldots, p_z\}$, except possibly the condition $t_{\Gamma'_z} - t_{\Gamma_z}$ being an integer where $t_{\Gamma'_z}$ and t_{Γ_z} are the rational numbers such that $deg(f^{(2_{p_1},_{p_z})}_{p_j}(q)) = t_{\Gamma'_z}(p_j - 1)$ for each $1 \leq j \leq z$ and $deg(f_{p_j}(q)) = t_{\Gamma_z}(p_j - 1)$ respectively. For each $z > 1$, $t_{\Gamma'_z}$ is an integer.

Remark 3.9. The existence of the integer $t_{\Gamma'_z}$ above is guaranteed by [1] once one can show that the sequence $\Gamma^{\partial}_z = \{f^{(2_{p_1},_{p_z})}_{p_i}(q)|1 \leq i \leq z\}$ satisfies Functional

Equation (1). The condition $t_{\Gamma'_z} - t_{\Gamma_z}$ being an integer also holds and we prove that in the subsequent propositions.

P r o o f. (i) Firstly it is immediate from the construction above that the coefficients of each polynomial in $\Gamma_z^{\partial} = \{f_{p_i}^{(2_{p_1},p_z)}(q)|1 \le i \le z\}$ are contained in $\mathbb{Q}$ since each $f_{p_i}^{(2_{p_1},p_z)}(q)$ is formed by multiplying $f_{p_i}^*(q)$ with polynomials of the form $\prod_t([p_i]_{a_t})^{b_t}$, where a_t and b_t are integers for each t. Therefore by Theorem 2.1 of [4] and the properties of quantum integers described briefly in the introduction, they satisfy Functional Equation (1) if and only if they have the same form. Secondly, it can be verified directly that the process in Step 1 and 2, which uses [4], constructs two polynomials $f_{p_1}^{(2_{p_1},p_2)}(q)$ and $f_{p_2}^{(2_{p_1},p_2)}(q)$ having the same form from two polynomials $f_{p_1}^{(0)}(q)$ and $f_{p_2}^{(0)}(q)$ which may not be of the same form. Thus $f_{p_1}^{(2_{p_1},p_2)}(q)$ and $f_{p_2}^{(2_{p_1},p_2)}(q)$ must satisfy Functional Equation (1). The process being performed in Step 3 is an extension of that of Step 2, in which it constructs successively a collection of polynomials $\{f_{p_i}^{(2_{p_1},p_z)}(q)|1 \le i \le z\}$ having the same form from a smaller collection of polynomials of the same form $\{f_{p_i}^{(2_{p_1},p_{z-1})}(q)|1 < i \le z-1\}$ for each $z > 2$. By similar reason as above, this new collection Γ_z^{∂} of polynomials also satisfies Functional Equation (1). As a result, it induces a sequence Γ'_z with the same support, having Γ_z^{∂} as a subsequence and whose elements satisfy Functional Equation (2) by Theorem 1.7. Thus there exists a minimal collection $\{(a_t, b_t)|a_t \ge 1\}_t$ such that $f_{p_i}^{(2_{p_1},p_z)}(q)$ has the form $\prod_t([p_i]_{q^{a_t}})^{b_t}$ for each $1 \le i \le z$. As a result, $\deg(f_{p_i}^{(2_{p_1},p_z)}(q)) = t(p_i - 1)$ for some integer t, which we denote by $t_{\Gamma_z^{\partial}}$.

(ii) For each $p_j \in P_z$, the polynomial $f_{p_j}^{(2_{p_j},p_z)}(q)$ is a product of $f_{p_j}^*(q)$ of Γ_z^* with some nonzero polynomials. Therefore, $supp\{\Gamma'_z\} = supp\{\Gamma_z\} = A_{P_z}$ (see [1] for the last equality). It remains to be proved that Γ'_z is the unique sequence of polynomials satisfying Functional Equation (2) whose elements are of minimal degree such that $f_n(q)$ divides $f'_n(q)$ for each n in $supp\{\Gamma_z\} = supp\{\Gamma'_z\}$. It is sufficient for to us to show that $\Gamma_z^{\partial} = \{f_{p_i}^{(2_{p_1},p_t)}(q)|1 \le i \le z\}$ is the unique sequence of polynomials with minimal degree such that $f_{p_i}(q)$ divides $f_{p_j}^{(2_{p_1},p_z)}(q)$ for each $1 \le i \le z$ and for all $z > 1$. It is immediate from the construction that for each $1 \le i \le z$, $f_{p_i}(q)$ divides $f_{p_i}^{(2_{p_1},p_z)}(q)$ since $f_{p_i}^{(2_{p_1},p_z)}(q)$ is obtained from $f_{p_i}(q)$ by multiplying to $f_{p_i}(q)$ some polynomial. For each $p_i \in P$, $f_{p_i}(q) = \prod_j f_{u_t,p_i}(q)$ has coefficients in $\mathbb{Q}$ if and only if the coefficients of $f_{u_t,p_i}(q)$ are contained in $\mathbb{Q}$ for each t. Thus by construction, $f_{p_i}^*(q)$ is the polynomials with minimal degree having coefficients contained in $\mathbb{Q}$ such that $f_{p_i}(q)$ divides $f_{p_i}^*(q)$ for each p_i in P. By basic field theory, if $T(q)$ is any polynomial in $\mathbb{Q}[q]$ divisible by $f_{p_i}(q)$, then $T(q)$ must be divisible by $f^*_{p_i}(q)$. Therefore, if the sequence $\{f^*_{p_i}(q)|p_i \in P_z\}$ satisfies Functional Equation (1), then it satisfies (ii). Now let us suppose $\{f^*_{p_i}(q)|p_i \in P_z\}$ does not satisfy (i). By [4] and by re-indexing as above, we may assume that $f^*_{p_1}(q) := \prod_i([p_1]_{q^{a_i}})^{b_i}$ and $f^*_{p_2}(q) := \prod_i([p_2]_{q^{c_j}})^{d_j}$, not of the same form, where $\{(a_i, b_i)|a_i \geq 1\}_i$ and $\{(c_j, d_j)|c_j \geq 1\}_j$ are two minimal collections of ordered pairs of integers. By Theorem 2.1 of [4], if $T_{p_1}(q)$ and $T_{p_2}(q)$ are two polynomials in $\mathbb{Q}[q]$ satisfying Functional Equation (1) which are divisible by $f^*_{p_1}(q)$ and $f^*_{p_2}(q)$ respectively, then they must be of the same form and there must exist a minimal collections $\{(u_i, v_i)|u_i \geq 1\}_i$ such that $T_{p_1}(q) = \prod_i([p_1]_{q^{u_i}})^{v_i}$ and $T_{p_2}(q) := \prod_i([p_2]_{q^{u_i}})^{v_i}$, which are divisible by $f^*_{p_1}(q) := \prod_i([p_1]_{q^{a_i}})^{b_i}$ and $f^*_{p_2}(q) := \prod_i([p_2]_{q^{c_j}})^{d_j}$. It can be verified directly from the process of Step 2 that the polynomials obtained there, namely $T_{p_1}(q) := f_{p_1}^{(2_{p_1,p_2})}(q)$ and $T_{p_2}(q) := f_{p_2}^{(2_{p_1,p_2})}(q)$, are the unique polynomials of minimal degree having such properties, because they are built by multiplying $f^*_{p_1}(q)$ and $f^*_{p_2}(q)$ with the polynomials $E_1(q)$, $E_2(q)$, $B_1(q)$ and $B_2(q)$ which are uniquely determined by $f_{p_1}(q)$ and $f_{p_2}(q)$ and which are of minimal possible degree having the required properties. Step 3 is just Step 2 apply successively and the polynomial $G_{p_1,p_j}(q)$ is uniquely determined by $f_{p_1}^{(2_{p_1,p_j})}(q)$ and $f_{p_1}^{(2_{p_1,p_j})}(q)$ and is of minimal degree, a fact which immediate from the construction. Therefore the same argument as above also holds. Thus $t_{\Gamma'} - t_\Gamma$ is minimal. Thus the result follows.

□

If P contains finitely many primes, then this algorithm ends in finitely many steps. If P contains all primes, then we have shown in [4] that there is no sequence satisfying Functional Equation (2) with field of coefficients of characteristic zero strictly greater than $\mathbb{Q}$ and thus there is nothing to prove. In the case where P contains infinitely many primes but not necessarily all primes, our results concerning the existence of a sequence of polynomials satisfying Functional Equation (2) with field of coefficients strictly greater than $\mathbb{Q}$ whose support is of the form A_P is affirmative and can be found in [5] which is in preparation. As a result of the existence of such a sequence, it could mean that we may have to apply Step 3 infinitely many times, one for each prime. Thus this shows that there is a possibility that no sequence Γ' with the required properties. However the next result resolves this problem.

Proposition 3.10. *Suppose that there exists a sequence Γ of polynomials satisfying the hypothesis of Theorem 2.1 with field of coefficients strictly containing $\mathbb{Q}$, and the set of primes P associated to the support of Γ containing infinitely many primes but not necessarily all primes. Then there exists a positive integer g such* *that the polynomial* $f_{p_1}^{(2_{p_1},p_z)}(q)$ *in* $\{f_{p_i}^{(2_{p_1},p_z)}(q)|1 \leq i \leq z\}$ *at the end of Step 3 is unchanged for all* $z \geq g$.

P r o o f. For each $p_j \in P$, write $f_{p_j}(q) = f_{u_{ij},p_j}(q)$ as above. By [4], u_{1j} is constant for all j. Since $u_{ij} \leq u_{1j}$ for all i and j, the collection $\mathcal{U} := \{r_l\}$ consisting of all distinct prime factors of u_{ij} for any u_{ij} can only contain finitely many elements. This also implies that the collection $\{u_{ij}|p_j \in P\}$ of distinct levels of Γ has finite cardinality. Therefore the result follows.

□

Thus this algorithm produces a sequence of polynomials $\Gamma'=\{f'_{p_j}(q)|p_j\in P\}$ satisfying Functional Equation (1), whose field of coefficients $\mathbb{Q}$ and such that $f_{p_j}(q)$ divides $f'_{p_j}(q)$ for each $p_j \in P$. By Theorem 1.7, this induces the sequence $\Gamma' = \{f'_n(q)|n \in A_P\}$ of polynomials satisfying Functional Equation (2) whose support is the support A_P of Γ (see the introduction) and whose field of coefficients is $\mathbb{Q}$ such that $f_n(q)$ divides $f'_n(q)$ for all n in A_P. The minimality of $t_{\Gamma'} - t_\Gamma$ and the uniqueness of such Γ' follow immediately from the minimality of $t_{\Gamma'_z} - t_{\Gamma_z}$ and the uniqueness of Γ_z for all $z > 1$ (we leave the details to the interested readers). Therefore, it remains to be shown that $t_{\Gamma'} - t_\Gamma$ is a nonnegative integer. We prove this by induction on the number of levels of $f_{p_j}(q)$ for any $p_j \in P$, i.e the number of u_i's such that the factors $f_{u_i,p_j}(q)$ of $f_{p_j}(q)$ are nontrivial polynomials. Let p be the smallest prime in P. Let r be any other prime in P. It is sufficient for us to prove that $\deg(f_p(q)) = t(p-1)$ for some nonnegative integer t. This is sufficient since $\deg(f_r) = t(p_j - 1)$ for any $p_j \in P$ by [1] (or see the introduction above). Unless stated otherwise, the prime p in the rest of the proof of Theorem 2.1 has this minimal property.

Definition 3.11. Let $f(q)$ be a nonconstant polynomial with field of coefficients of characteristic zero and whose roots are primitive a-roots of unity for some positive integer a. If n is the smallest positive integer such that $f(q)$ divides $P_a(q)$, the cyclotomic polynomial of order a with coefficients in $\mathbb{Q}$, then n is called the **least power** of $f(q)$.

Proposition 3.12. *(Key Proposition 3)*

Let Γ *be a sequence of polynomials satisfying Functional Equation* (2) *such that:*

- *The field of coefficients of* Γ *strictly contains* $\mathbb{Q}$.
- *Support*$\{\Gamma\} = A_P$, *where* $P = \{p, r\}$ *with* p *and* r *being two distinct primes.*

Let k be the integer in Key Proposition 1. Then $\frac{P_{v_{p,r,k},p}(q)^{n_{kp}}}{f_{v_{p,r,k},p}(q)}$ *and* $\frac{P_{v_{p,r,k},r}(q)^{n_{kr}}}{f_{v_{p,r,k},r}(q)}$ *are super-compatible, where n_{kp} and n_{kr} are the least powers of the polynomials $f_{v_{p,r,k},p}(q)$ and $f_{v_{p,r,k},r}(q)$ respectively.*

Proof. From the definition of k, the assumption that the field of coefficients of Γ strictly contains $\mathbb{Q}$ and Key Proposition 1, $s_{p,k} = s_{r,k} = 1$ and the EFE(1) of the polynomials $f_p(q)$ and $f_r(q)$ in Γ has the form:

$$\begin{array}{ccc}
f^{s_{p,1}\delta_{r,1}}_{v_{p,r,1},p}(q)\frac{f_{v_{p,r,1},r}(q^p)^{s_{r,1}}}{f_{v_{p,r,1},r}(q)^{s_{r,1}(1-\delta_{p,1})}} & \overset{(1)}{\leftrightarrow} & f^{s_{r,1}\delta_{p,1}}_{v_{p,r,1},r}(q)\frac{f_{v_{p,r,1},p}(q^r)^{s_{p,1}}}{f_{v_{p,r,1},p}(q)^{s_{p,1}(1-\delta_{r,1})}} \\
\cdots & \cdots & \cdots \\
f^{\delta_{r,k}}_{v_{p,r,k},p}(q)\frac{f_{v_{p,r,k},r}(q^p)}{f_{v_{p,r,k},r}(q)^{(1-\delta_{p,k})}} & \overset{(k)}{\leftrightarrow} & f^{\delta_{p,k}}_{v_{p,r,k},r}(q)\frac{f_{v_{p,r,k},p}(q^r)}{f_{v_{p,r,k},p}(q)^{(1-\delta_{r,k})}} \\
\cdots & \cdots & \cdots \\
f_p(q)f_r(q^p) & = & f_r(q)f_p(q^r).
\end{array}$$

Then it can be verified that line (k) of the $(k-1)$ super-reduced form of EFE(1) above has the form

$$f_{v_{p,r,k},p}(q)^{\delta_{r,k}}\frac{L(q)f_{v_{p,r,k},r}(q^p)}{f_{v_{p,r,k},r}(q)^{(1-\delta_{p,k})}} \overset{(k)}{\longleftrightarrow} f_{v_{p,r,k},r}(q)^{\delta_{p,k}}\frac{R(q)f_{v_{p,r,k},p}(q^r)}{f_{v_{p,r,k},p}(q)^{(1-\delta_{r,k})}},$$

where

$$\frac{L(q)f_{v_{p,r,k},r}(q^p)}{f_{v_{p,r,k},r}(q)^{s_{r,k}(1-\delta_{p,k})}} = \frac{R(q)f_{v_{p,r,k},p}(q^r)}{f_{v_{p,r,k},p}(q)^{(1-\delta_{r,k})}}$$

and $L(q)$ and $R(q)$ are the left and right moving factors respectively defined earlier. By definition of k, both $L(q)$ and $R(q)$ must have the form $P_{v_{p,r,k}p,r}(q)^{n_{L(q)}}$ and $P_{v_{p,r,k}r,p}(q)^{n_{R(q)}}$ respectively for some integers $n_{L(q)}$ and $n_{R(q)}$ which are not necessarily equal and where $P_{v_{p,r,k}p,r}(q) = P_{v_{p,r,k}r,p}(q)$ is the cyclotomic polynomial of order $v_{p,r,k}rp$ in $\mathbb{Q}[q]$. Let m_L and m_R be the maximal integers such that $P_{v_{p,r,k}p,r}(q)^{m_L}$ and $P_{v_{p,r,k}r,p}(q)^{m_R}$ divide $\frac{f_{v_{p,r,k},r}(q^p)^{s_{r,k}}}{f_{v_{p,r,k},r}(q)^{(1-\delta_{p,k})}}$ and $\frac{f_{v_{p,r,k},p}(q^r)}{f_{v_{p,r,k},p}(q)^{(1-\delta_{r,k})}}$ respectively. Then $n_{L(q)} + m_L = n_{R(q)} + m_R$ (see [4]). Thus if we divide both sides of line (k) of the $(k-1)$ super-reduced form above by $P_{v_{p,r,k}p,r}(q)^{n_{L(q)}+m_L}$ (which is equal to $P_{v_{p,r,k}r,rp}(q)^{n_{R(q)}+m_R}$ since $P_{v_{p,r,k}p,r}(q) = P_{v_{p,r,k}r,p}(q)$), we obtain

$$f_{v_{p,r,k},p}(q)^{s_{p,k}\delta_{r,k}}\frac{f'_{v_{p,r,k},r}(q^p)}{f'_{v_{p,r,k},r}(q)^{(1-\delta_{p,k})}} \overset{(k)}{\longleftrightarrow} f_{v_{p,r,k},r}(q)^{\delta_{p,k}}\frac{f'_{v_{p,r,k},p}(q^r)^{s_{p,k}}}{f'_{v_{p,r,k},p}(q)^{(1-\delta_{r,k})}}$$

with

$$\frac{f'_{v_{p,r,k},r}(q^p)}{f'_{v_{p,r,k},r}(q)^{(1-\delta_{p,k})}} = \frac{f'_{v_{p,r,k},p}(q^r)}{f'_{v_{p,r,k},p}(q)^{(1-\delta_{r,k})}},$$

where $\frac{f'_{v_{p,r,k},r}(q^p)}{f'_{v_{p,r,k},r}(q)^{(1-\delta_{p,k})}}$ and $\frac{f'_{v_{p,r,k},p}(q^r)}{f'_{v_{p,r,k},p}(q)^{(1-\delta_{r,k})}}$ are polynomials dividing the polynomials $\frac{f_{v_{p,r,k},r}(q^p)}{f_{v_{p,r,k},r}(q)^{(1-\delta_{p,k})}}$ and $\frac{f_{v_{p,r,k},p}(q^r)}{f_{v_{p,r,k},p}(q)^{(1-\delta_{r,k})}}$ respectively which are maximal with respect to the property that 0 is the highest power of $P_{v_{p,r,k}r,p}(q) = P_{v_{p,r,k}p,r}(q)$ dividing $\frac{f'_{v_{p,r,k},r}(q^p)}{f'_{v_{p,r,k},r}(q)^{(1-\delta_{p,k})}}$ and $\frac{f'_{v_{p,r,k},p}(q^r)}{f'_{v_{p,r,k},p}(q)^{(1-\delta_{r,k})}}$. As a result, a similar argument as in Key Proposition 1′ of [4] implies that the polynomials $f'_{v_{p,r,k},p}(q)$ and $f'_{v_{p,r,k},r}(q)$ are super-compatible. It is immediate that this is equivalent to the desired result.

□

Let □ denotes either p or r and △ denotes the other. From now on, we call the polynomials $f'_{v_{p,r,k},\triangle}(q)$ defined above the **non-rational factor** of the polynomial $f_{v_{p,r,k},\triangle}(q)$. Hence if k is the bi-level defined in Key Proposition 1, then Key Proposition 3 shows that even though $f_{v_{p,r,k},p}(q)$ and $f_{v_{p,r,k},r}(q)$ may not be super-compatible, their non-rational factors (nontrivial for Γ satisfying hypothesis of Key Proposition 3) are.

Proposition 3.13. *(Key Proposition 4)*

Let P be a set of primes with at least two primes. Let $\Gamma = \{f_n(q)|n \in \mathbb{N}\}$ be a sequence of polynomials satisfying Functional Equation (2) *with field of coefficients strictly containing $\mathbb{Q}$ and whose support is A_P [see the introduction]. For each $p_j \in P$, let $f^*_{p_j}(q) = \prod_i (P_{u_i,p_j}(q))^{n_{ij}}$ as before where n_{ij} is the smallest positive integer such that $f_{u_i,p_j}(q)$, the polynomial whose roots are all roots of $f_{p_j}(q)$ which are primitive $u_i p_j$-roots of unity, divides $(P_{u_i,p_j}(q))^{n_{ij}}$. Then for each $p_j \in P$, deg$(f^*_{p_j}(q)) = t_{p_j}(p_j - 1)$ for some integer t_{p_j}.*

P r o o f. Let p be as above ($p < p_j$ for any other primes $p_j \in P$) and r be any other prime in P. To prove this lemma, it can be verified that it is sufficient if we prove it for the case $P = \{p, r\}$. Furthermore, it is also sufficient if we can show that $\deg(f_p(q)) = t(p-1)$ for some integer t. This is because there exists a rational number t_Γ such that $\deg(f_{p_j}(q)) = t_\Gamma(p_j - 1)$ for all $p_j \in P$ by [1], which means that $t = t_\Gamma$ and thus $\deg f_r(q) = t(r-1)$ as well. We prove this proposition by induction on the number of levels of $f_p(q)$. The case where $f_p(q)$ has one level is demonstrated in (a). Let us consider the reduced form of EFE(1) with respect to p and r

$$f_{v_{p,r,1},p}(q)^{s_{p,1}\delta_{r,1}} \frac{f_{v_{p,r,1},r}(q^p)^{s_{r,1}}}{f_{v_{p,r,1},r}(q)^{s_{r,1}(1-\delta_{p,1})}} \overset{(1)}{\leftrightarrow} f_{v_{p,r,1},r}(q)^{s_{r,1}\delta_{p,1}} \frac{f_{v_{p,r,1},p}(q^r)^{s_{p,1}}}{f_{v_{p,r,1},p}(q)^{s_{p,1}(1-\delta_{r,1})}}$$

. . . .

$$f_{v_{p,r,k},p}(q)^{s_{p,k}\delta_{r,k}} \frac{f_{v_{p,r,k},r}(q^p)^{s_{r,k}}}{f_{v_{p,r,k},r}(q)^{s_{r,k}(1-\delta_{p,k})}} \overset{(k)}{\leftrightarrow} f_{v_{p,r,k},r}(q)^{s_{r,k}\delta_{p,k}} \frac{f_{v_{p,r,k},p}(q^r)^{s_{p,k}}}{f_{v_{p,r,k},p}(q)^{s_{p,k}(1-\delta_{r,k})}}$$
$$\cdots\cdots\cdots$$
$$Q_{p,r}(q) = Q_{p,r}(q)$$

where

$$Q_{p,r}(q) = \frac{f_p(q)f_r(q^p)}{\prod_i f_{v_{p,r,i},r}(q)^{s_{r,i}(1-\delta_{p,i})} f_{v_{p,r,i},p}(q)^{s_{p,i}(1-\delta_{r,i})}}$$
$$= \frac{f_r(q)f_p(q^r)}{\prod_i f_{v_{p,r,i},r}(q)^{s_{r,i}(1-\delta_{p,i})} f_{v_{p,r,i},p}(q)^{s_{p,i}(1-\delta_{r,i})}}$$

as in [4]. It is immediate from the definition of EFE(1) that either $f_{v_{p,r,i},p}(q)$ or $f_{v_{p,r,i},r}(q)$ is different from 1 for any bi-level i, i.e., either $s_{p,i} = 1$ or $s_{r,i} = 1$ for any bi-level i appearing in the EFE(1).

Definition 3.14. A **period** $\mathcal{P}_i$ of EFF(1) with respect to primes p and r and with initial level i is the minimal collection of bi-levels $\{i = i_1, \ldots, i_l\}$ such that $\prod_{j=1}^{j=l} f_{v_{p,r,i_j},p}(q)$ and $\prod_{j=1}^{j=l} f_{v_{p,r,i_j},r}(q)$ satisfy Functional Equation (1).

Remark 3.15. It is immediate that every bi-levels of EFE(1) belongs to some period.

It is also sufficient if we can show that $\deg(\prod_{j\in\mathcal{P}_1} f_{v_{p,r,j},p}(q)) = t(p-1)$ for some integer t since we can replace $f_p(q)$ and $f_r(q)$ by $\frac{f_p(q)}{\prod_{j\in\mathcal{P}_1} f_{v_{p,r,j},p}(q)}$ and $\frac{f_r(q)}{\prod_{j\in\mathcal{P}_1} f_{v_{p,r,j},r}(q)}$ respectively and the proposition follows by induction. As a result, we may assume without loss of generality that $EFE(1)$ with respect to p and r has only one period, namely $\mathcal{P}_1$.

To prove this proposition, it is immediate that we only need to be concerned with the non-rational factors $f'_{v_{p,r,i},\Box}(q)$ of $f_{v_{p,r,i},\Box}(q)$ (instead of the whole factor $f_{v_{p,r,i},\Box}(q)$) at each bi-level i of EFE(1). Hence for the rest of the proof of this proposition, we make the following notational convention:

- Two polynomials are said to be super-compatible if their nonrational factors are (it is straightforward to verify that the nonrational factors of two super-compatible polynomials of the form we are considering are super-compatible but the converse is not true).
- Unless otherwise stated, all the equalities concerning the polynomials of the forms $f_{v_{p,r,i},\Box}(q)^{s_{\Box,i}}$ or $\frac{f_{v_{p,r,i},\Box}(q^{\triangle})^{s_{\Box,i}}}{f_{v_{p,r,i},\Box}(q)^{s_{\Box,i}(1-\delta_{\triangle,i})}}$ in the proof of this proposition should be understood as equalities modulo the polynomials $P_{v_{p,r,i},\Box}(q)$ or $P_{v_{p,r,i}\triangle,\Box}(q)$ respectively (i.e. we are only concerned with equalities of the various nonrational factors).

- $s_{\square,i} = 0$ means that $f'_{v_{p,r,i},\square}(q)^{s_{\square,i}} = 1$ but not necessarily $f_{v_{p,r,i},\square}(q)^{s_{\square,i}} = 1$ for any bi-level i occurring in EFE(1) with respect to p and r.
- $f_{v_{p,r,i},\square}(q)^{s_{\square,i}}$ denotes the $f'_{v_{p,r,i},\square}(q)^{s_{\square,i}}$, its nonrational factor (to reduce the cumbersome notation) unless otherwise stated.

Let k be the integer in Key Proposition 1. From Key Proposition 1, $s_{p,k} = 1 = s_{r,k}$. Together with the definition of k, this implies that the polynomials $f_{v_{p,r,k},p}(q)$ and $f_{v_{p,r,k},r}(q)$ are nontrivial in the new notational convention. It can be verified from the proof of Key Proposition 1 that the moving factors $L(q)$ and $R(q)$ can be written as $L(q) = L_k(q) = P_{v_{p,r,k}r,p}(q)^{n_k} = \frac{P_{v_{p,r,k},r}(q^p)^{n_k}}{P_{v_{p,r,k},r}(q)^{n_k(1-\delta_{p,k})}}$ and $R(q) = R_k(q) = P_{v_{p,r,k}p,r}(q)^{m_k} = \frac{P_{v_{p,r,k},p}(q^r)^{m_k}}{P_{v_{p,r,k},p}(q)^{m_k(1-\delta_{r,k})}}$ respectively for some nonnegative integers n_k and m_k such that

$$\frac{P_{v_{p,r,k},r}(q^p)^{n_k}}{P_{v_{p,r,k},r}(q)^{n_k(1-\delta_{p,k})}}\frac{f_{v_{p,r,k},r}(q^p)}{f_{v_{p,r,k},r}(q^p)^{(1-\delta_{p,k})}} = \frac{L(q)f_{v_{p,r,k},r}(q^p)}{f_{v_{p,r,k},r}(q^p)^{(1-\delta_{p,k})}} =$$

$$\frac{R(q)f_{v_{p,r,k},p}(q^r)}{f_{v_{p,r,k},p}(q^r)^{(1-\delta_{r,k})}} = \frac{P_{v_{p,r,k},p}(q^r)^{m_k}}{P_{v_{p,r,k},p}(q)^{m_k(1-\delta_{r,k})}}\frac{f_{v_{p,r,k},p}(q^r)}{f_{v_{p,r,k},p}(q^r)^{(1-\delta_{r,k})}}.$$

Hence the polynomials $P_{v_{p,r,k},r}(q)^{n_k} f_{v_{p,r,k},r}(q)$ and $P_{v_{p,r,k},p}(q)^{m_k} f_{v_{p,r,k},p}(q)$- the polynomials $f_{v_{p,r,k},p}(q)$ and $f_{v_{p,r,k},r}(q)$ denote the original polynomials (not their nonrational factors)- are super-compatible in the original sense by the analysis of [4]. Hence their nonrational factors, which are equal to the nonrational factors of $f_{v_{p,r,k},p}(q)$ and $f_{v_{p,r,k},r}(q)$ respectively since non-rational factors of $f_{v_{p,r,i},p}(q)$ and $f_{v_{p,r,i},r}(q)$ are trivial for all $i < k$, are super-compatible. As a result, $f_{v_{p,r,k},p}(q)$ and $f_{v_{p,r,k},r}(q)$ are also super-compatible in the sense of the convention above. Since we only need to use for our proof the fact that the nonrational factors of $f_{v_{p,r,k},p}(q)$ and $f_{v_{p,r,k},p}(q)$ are super-compatible together with the above notational conventions, we may assume without loss of generality that $k = 1$.

Definition 3.16. If a line (j), for some j, of a reduced form of EFE(1) is unchanged after the moving-factor process is applied to it to obtain the (l)-super-reduced form for some $l \geq j$, we say that line (j) is an **independent line**.

If $\delta_{p,1} = 0 = \delta_{r,1}$, then line (1) of the reduced form of EFE(1) with respect to p and r has the form

$$\frac{f_{v_{p,r,1},r}(q^p)}{f_{v_{p,r,1},r}(q)} \overset{(1)}{=} \frac{f_{v_{p,r,1},p}(q^r)}{f_{v_{p,r,1},p}(q)}.$$

Therefore, it remains unchanged in the the moving-factor process, a process which produces the super-reduced form from the reduced form of EFE(1) with respect to p and r (see [4]). Thus (1) is an independent line.

By the super-compatibility of $f_{v_{p,r,1},p}(q)$ and $f_{v_{p,r,1},r}(q)$ together with the assumption $\delta_{p,1} = 0 = \delta_{r,1}$, we have

$$deg(f_{v_{p,r,1},p}(q)) = t(p-1)$$

and

$$deg(f_{v_{p,r,1},r}(q)) = t(r-1)$$

for some positive integer t (see [4]). Thus we may replace $f_p(q)$ and $f_r(q)$ by $\frac{f_p(q)}{f_{v_{p,r,1},p}(q)}$ and $\frac{f_r(q)}{f_{v_{p,r,1},r}(q)}$ respectively and the proposition follows by induction. Furthermore, if there is an index j such that line (j) of the reduced form of EFE(1) above takes the form

$$\frac{f_{v_{p,r,j},r}(q^p)}{f_{v_{p,r,j},r}(q)} \overset{(j)}{=} \frac{f_{v_{p,r,j},p}(q^r)}{f_{v_{p,r,j},p}(q)},$$

then it is an independent line as well as $f_{v_{p,r,1},p}(q)$ and $f_{v_{p,r,1},r}(q)$ are compatible and $\delta_{p,j} = 0 = \delta_{r,j}$. Therefore we may replace $f_p(q)$ and $f_r(q)$ by $\frac{f_p(q)}{f_{v_{p,r,j},p}(q)}$ and $\frac{f_r(q)}{f_{v_{p,r,j},r}(q)}$ respectively and the proposition follows by induction.

Note that if line (j) of EFE(1) with respect to p and r is an independent line, then $f_{v_{p,r,j},p}(q)$ and $f_{v_{p,r,j},r}(q)$ themselves induce single-level sequences as in (1) which have already been characterized. As a result, we may assume henceforth without loss of generality that there is no independent line in EFE(1) with respect to p and r.

Definition 3.17. Let $\Box$ denote either p or r and $\triangle$ denote the other. The polynomial $f_{v_{p,r,m},\Box}(q) \neq 1$ is said to be **directly related** to the polynomial $f_{v_{p,r,n},\triangle}(q) \neq 1$ for some $n \neq m$ if $f_{v_{p,r,m},\Box}(q) = f_{v_{p,r,n},\triangle}(q)$ and

$$f_{v_{p,r,m},\Box}(q)\frac{f_{v_{p,r,l},\triangle}(q^{\Box})^{s_{\triangle,l}}}{f_{v_{p,r,l},\triangle}(q)^{s_{\triangle,l}(1-\delta_{\Box,l})}} \neq f_{v_{p,r,n},\triangle}(q)\frac{f_{v_{p,r,l},\Box}(q^{\triangle})^{s_{\Box,l}}}{f_{v_{p,r,l},\Box}(q^{\triangle})^{s_{\Box,l}(1-\delta_{\triangle,l})}}$$

for for all $l > m, n$ such that $v_{p,r,m}\Box = v_{p,r,l}\triangle\Box$. The polynomial $f_{v_{p,r,m},\Box}(q) \neq 1$ is said to **semi-directly related** to $f_{v_{p,r,n},\Box}(q) \neq 1$ (or vice versa) if

$$f_{v_{p,r,m},\Box}(q)\frac{f_{v_{p,r,n},\triangle}(q^{\Box})^{s_{\triangle,n}}}{f_{v_{p,r,n},\triangle}(q)^{s_{\triangle,n}(1-\delta_{\Box,n})}} = \frac{f_{v_{p,r,n},\Box}(q^{\triangle})}{f_{v_{p,r,n},\Box}(q^{\triangle})^{\delta_{\triangle,n}}}.$$

Suppose either $f_{v_{p,r,m},\Box}(q)$ or $f_{v_{p,r,n},\triangle}(q)$ is nontrivial such that

$$v_{p,r,m}\Box = v_{p,r,n}\triangle$$

and

$$f_{v_{p,r,m},\square}(q)\frac{f_{v_{p,r,l},\triangle}(q^{\square})^{s_{\triangle,l}}}{f_{v_{p,r,l},\triangle}(q)^{s_{\triangle,l}(1-\delta_{\square,l})}} = f_{v_{p,r,n},\triangle}(q)\frac{f_{v_{p,r,l},\square}(q^{\triangle})^{s_{\square,l}}}{f_{v_{p,r,l},\square}(q^{\triangle})^{s_{\square,l}(1-\delta_{\triangle,l})}}$$

for some bi-levels $l > n, m$. Then $f_{v_{p,r,m},\square}(q)$ is said to be **indirectly related** to the order pair of polynomials $(f_{v_{p,r,n},\triangle}(q), f_{v_{p,r,l},\square}(q))$ (or $f_{v_{p,r,n},\triangle}(q)$ is **indirectly related** to the ordered pair $(f_{v_{p,r,m},\square}(q), f_{v_{p,r,l},\square}(q))$).

If two (or three in the case of indirect relation) polynomials satisfy one of the related relations above, we refer to the levels, namely $v_{p,r,m}$ and $v_{p,r,n}$ (and $v_{p,r,l}$ if applicable), of the polynomials involved as the **related levels** or as being **related**. Similarly, we also refer to these polynomials or the lines of EFE(1) containing the polynomials involved in such relations as being related polynomials or related lines respectively.

From the definition above, we would like to make the following observations (their verifications are straightforward and thus left to the readers):

- Let m and n be two related levels. If $s \neq p, r$ is a prime dividing $v_{p,r,m}$, then s also divides $v_{p,r,n}$ and vice versa.
- Since $p < r$ by assumption, if $\square = r$ in the definition above, then $f_{v_{p,r,m},r}(q)$ can be neither indirectly (of either types) nor directly related to polynomials of higher levels because $v_{p,r,m} > v_{p,r,n}$ if $m < n$ which means that $v_{p,r,m}r > v_{p,r,n}r > v_{p,r,n}p$ if $m < n$. If $f_{v_{p,r,m},\square}(q)$ is directly related to $f_{v_{p,r,n},\triangle}(q)$ for some bi-level n, then if $\deg(f_{v_{p,r,m},\square}(q)) = t(\square - 1)$ for some integer t, then so is $\deg(f_{v_{p,r,n},\triangle}(q))$.

Definition 3.18. Let l be a bi-level of EFE(1) with respect to p and r. Let $\mathcal{R} = \{i\}$ be a collection of distinct bi-levels of EFE(1) with respect to p and r. Then $\mathcal{R}$ is called a **chain** (containing l) if it satisfies the following conditions:

(1) $l \in \mathcal{R}$.

(2) $\mathcal{R} = \{i_j | 0 \leq j \leq n-1, i_j < i_{j+1}\}$ (after some rearrangement if necessary) with $i_v = l$ for some $v \in \{0, \dots, n-1\}$ and for each $j \in \{0, \dots, n-2\}$, $v_{p,r,i_j} = p^d v_{p,r,i_{j+1}}$ for some integer d.

(3) n is maximal with respect to (1) and (2).

(4) $\mathcal{R} \neq \emptyset$.

Remark 3.19. Condition (3) means that $\mathcal{R}$ is a chain if it is nonempty, satisfying conditions (1) and (2) and which cannot be enlarged.

First we need to show, for any given bi-level l of EFE(1) with respect to p and r, the existence of a chain of EFE(1) with respect to p and r containing l.

Then to prove Theorem 2.1, it is sufficient for us at this point to verify the following:

- Every bi-level of EFE(1) with respect to p and r belongs to at least one chain.
- If $\mathcal{R} = \{i_j | 0 \leq j \leq n-1\}$ is a chain, then $\sum_{i_j \in \mathcal{R}} deg(f_{v_{p,r,i_j},p}(q)) = t(p-1)$ for some integer t.
- If R $:= \{\mathcal{R}\}$ is the collection of all chains of EFE(1) with respect to p and r, then

$$\prod_{i_{j,\mathcal{R}} \in \mathcal{R} \in \mathrm{R}} f_{p,r,i_{j,\mathcal{R}}}(q) = f_p(q).$$

We partition the rest of the proof of this proposition into the following series of lemmas:

Lemma 3.20. *Let l be a bi-level of EFE(1) with respect to p and r. Then there exists an integer $n \geq 1$ and collection of bi-levels $\mathcal{C} = \{i_j | j = 0, \ldots, b-1, j_0 = l, p^0 \| v_{p,r,j_{b-1}}\}$ such that j_i related to j_{i+1} for $i = 0, \ldots, n-2$ if $n \geq 2$.*

Proof. Let l be a bi-level of EFE(1) with respect to p and r such that $f_{v_{p,r,l},p}(q)$ is nontrivial. If p does not divide $v_{p,r,l}$, then we may take $n = 1$ and $\mathcal{C} := \{l\}$ satisfies the requirement of this lemma. Let us suppose otherwise, i.e. p divides $v_{p,r,l}$, say $p^{\alpha} \| v_{p,r,l}$ for some positive integer $\alpha \geq 1$. Let $\mathcal{C}_1 := \{l\}$. As a result of our assumption, line (l) of the reduced form of EFE(1) takes the form

$$f_{v_{p,r,l},p}(q)^{\delta_{r,l}} f_{v_{p,r,l},r}(q^p)^{s_{r,l}} = f_{v_{p,r,l},r}(q)^{s_{r,l}} \frac{f_{v_{p,r,l},p}(q^r)^{\delta_{r,l}}}{f_{v_{p,r,l},p}(q)^{(1-\delta_{r,l})}}.$$

There are two cases to consider: (i) $s_{r,l} = 1$ and (ii) $s_{r,l} = 0$.

If (i) occurs, then line (l) of the reduced form of EFE(1) has the form

$$f_{v_{p,r,l},p}(q)^{\delta_{r,l}} f_{v_{p,r,l},r}(q^p) = f_{v_{p,r,l},r}(q) \frac{f_{v_{p,r,l},p}(q^r)^{\delta_{r,l}}}{f_{v_{p,r,l},p}(q)^{(1-\delta_{r,l})}}.$$

It can be deduced from EFE(1) that either $f_{v_{p,r,l},r}(q)$ is indirectly related to an ordered pair $(f_{v_{p,r,m},p}(q), f_{v_{p,r,n},p}(q))$ for some bi-levels $m < l < n$ such that

- either $f_{v_{p,r,m},p}(q) \neq 1$ or
- $f_{v_{p,r,n},r}(q) \neq 1$ (note that $f_{v_{p,r,n},p}(q)$ may be trivial)

or $f_{v_{p,r,l},r}(q)$ is semi-directly related to $f_{v_{p,r,n},r}(q) \neq 1$ for some bi-level $n > l$. It can be verified that when the former occurs, then we can define $\mathcal{C}_2$ to be either $\{l, m\}$ or $\{l, m\}$ respectively. Note that $p^{\alpha-1} \| v_{p,r,m} = \frac{v_{p,r,l} r}{p}$ and $p^{\alpha-1} \| v_{p,r,n} = \frac{v_{p,r,l}}{p}$. If the latter occurs, then we let $\mathcal{C}_2$ be $\{l, m\}$. Again note that $p^{\alpha-1} \| v_{p,r,n} = \frac{v_{p,r,l}}{p}$.

If (ii) occurs, then it can be verified from EFE(1) that either there exist bi-levels $m < n < l$ such that $(f_{v_{p,r,m},p}(q), f_{v_{p,r,l},p}(q))$ is indirectly related to $f_{v_{p,r,n},r}(q)$ with $f_{v_{p,r,m},p}(q) \neq 1$ or $f_{v_{p,r,l},p}(q)$ is semi-directly related to $f_{v_{p,r,m},p}(q) \neq 1$ for some bi-level $m < l$. In either case, we have $p^{\alpha-1} \| v_{p,r,m}$.

A finite number of iterations of the above argument (the details of which are left to the readers) allow us obtain a collection $\mathcal{C} = \{j_i | i = 0, \dots, n-1\}$ of n bi-levels (for some integer $n \geq 2$) such that $j_0 = l$, j_i is related to j_{i+1} for $0 \leq i \leq n-2$ and with $p^0 \| v_{p,r,j_{n-1}}$. A similar argument also applies in the case, where $f_{v_{p,r,l},p}(q) = 1$ (hence $f_{v_{p,r,l},r}(q) \neq 1$). Thus the result follows.

□

Two bi-level u and u' of EFE(1) are said to be **connected** if there exists a sequence of bi-levels $\{i_j | 0 \leq j \leq n-1, i_0 = u, i_{n-1} = u'\}$ such that i_j is related to i_{j+1} for $0 \leq j \leq n-2$. In this terminology, l and i_{b-1} in the above lemma are connected.

Lemma 3.21. *If m and n are bi-levels of EFE(1), then there exists a sequence of bi-levels $\{i_j | 0 \leq j \leq n-1, m = i_0, n = i_{n-1}\}$ for some integer n such that i_j is related to i_{j+1} for $0 \leq j \leq n-2$.*

Proof. Let $\mathcal{L} := \{i_j\}$ be the collection of bi-levels of EFE(1) with respect to p and r such that $p^0 \| v_{p,r,i_j}$ for all $i_j \in \mathcal{L}$. For each $i_j \in \mathcal{L}$, let $|i_j|$ be the collection of all bi-levels l of EFE(1) such that l and i_j are connected. From Lemma 3.21, it can be verified that this induces an equivalence relation over the collection of all bi-levels occurring in EFE(1) with respect to p and r whose equivalence classes are $\{|i_j| | i_j \in \mathcal{L}\}$. For each $i_j \in \mathcal{L}$, we refer to $|i_j|$ as the equivalence class of i_j with respect to this equivalent relation. If i_s and i_t are two bi-levels in $\mathcal{L}$ such that $l \in |i_s|$ and $l' \in |i_t|$ are related, then we also say that $|i_s|$ and $|i_t|$ are **connected**. Let m and n be bi-levels of EFE(1), then there exist i_a and i_b in $\mathcal{L}$ such that $m \in |i_a|$ and $n \in |i_b|$ by Lemma 3.21. If $i_a = i_b$, then the result follows. Let us suppose otherwise. If there exists bi-levels $m' \in i_a$ and $n' \in i_b$ such that m' is related to n', then there exists a sequence of bi-levels

$$m, \dots, i_a, \dots, m', \dots, n', \dots, i_b, \dots, n$$

such that any two consecutive bi-levels are related. Hence m and n are connected (hence the terminology for $|i_s|$ and $|i_t|$ being connected). Now let $\mathcal{L}_a$ be a subset of $\mathcal{L}$ maximal with respect to the following properties

- $i_a \in \mathcal{L}_1$.
- If $i_c \neq i_a$ is any element of $\mathcal{L}_1$, then there exists a sequence of elements of $\mathcal{L}_1$ of the form

$$i_c, \dots, i_a$$

such that the equivalence classes of any two consecutive elements in this sequence are connected.

Let $\mathcal{L}_2$ be defined similarly as $\mathcal{L}_1$ with i_a replaced by i_b. If $\mathcal{L}_1 \cap \mathcal{L}_2 \neq \emptyset$, say $i_w \in \mathcal{L}_1 \cap \mathcal{L}_2$, then we have a sequence of elements of $\mathcal{L}$:

$$i_a, \ldots, i_w, \ldots, i_b,$$

where the equivalence classes of any two consecutive bi-levels are connected. By applying a similar argument as above to each pair of consecutive bi-levels of this sequence, it can be deduced that m and n are connected as desired. Let us suppose that $\mathcal{L}_1 \cap \mathcal{L}_2 = \emptyset$. However, it can be deduced directly from the definition of related relations that i_a and i_b must then belong to two distinct periods (we leave the details to the readers). This contradicts the assumption that EFE(1) with respect to p and r has exactly one period. Thus the result follows.

□

Lemma 3.22. (1) *Let* P *be the collection of all primes, distinct from* p *and* r*, dividing* $v_{p,r,i}$ *for any bi-levels* i *occurring in EFE*(1) *with respect to* p *and* r*. Then* $\prod_{s\in \mathrm{P}} s$ *divides all such* $v_{p,r,i}$*.*

(2) *Let* l *be any bi-level occurring in a chain* $\mathcal{R}$ *of EFE*(1) *with respect to* p *and* r*. Let* P *be defined as above. Then the prime factorization of* $v_{p,r,l}$ *has the form* $\prod_{s\in \mathrm{P}} s^{\pi_s} p^{\lambda} r^{\mu}$ *for some nonnegative integers* λ*,* μ *and some collection of positive integers* $\{\pi_s | s \in \mathrm{P}\}$*.*

Proof. (1) If $\mathrm{P} = \emptyset$, then this is trivial. Let us assume otherwise. Let m and n be any two bi-levels of EFE(1) with respect to p . From Lemma 3.22, there is a positive integer n and a sequence of bi-levels $\{i_j | 0 \le j \le n-1 | i_0 = m, i_{n-1} = n\}$ of EFE(1) such that i_j is related to i_{j+1} for $0 \le j \le n-2$. It can be verified directly from the definitions of related relations that if m and n are related bi-levels, then $v_{p,r,m} = p^x r^y v_{p,r,n}$ for some integers (not necessarily nonnegative) x and y. Hence if s is any prime distinct from p and r such that $s^{\beta} \| v_{p,r,m}$ for some positive integer β, then $s^{\beta} \| v_{p,r,n}$ and vice versa. As m and n are arbitrary, it follows that if s is a prime distinct from p and r such that $s^{\beta} \| v_{p,r,l}$ for some bi-level l of EFE(1), then $s^{\beta} \| v_{p,r,i}$ for all bi-levels i occurring in EFE(1). As a result, if P denotes the collections of all such primes s, then $\prod_{s\in \mathrm{P}} s^{\beta_s}$ divides $v_{p,r,i}$ for any bi-level i of EFE(1) with respect to p and r.

(2) This part follows immediately from (1).

□

From our definition of a chain, if $\mathcal{R}$ is a nonempty chain and if $r^{\gamma} \| v_{p,r,l}$ for any l in $\mathcal{R}$, then it can be deduced that $r^{\gamma} \| v_{p,r,i}$ for all i in $\mathcal{R}$. Hence we may denote a chain $\mathcal{R}$ as $\mathcal{R}_{(\gamma)}$ if $r^{\gamma} \| v_{p,r,i}$ for any $i \in \mathcal{R}$ when we need to emphasize that aspect of $\mathcal{R}$.

Lemma 3.23. (i) *There exists a unique chain $\mathcal{R}$ of EFE(1) with respect to p and r of the form $\mathcal{R}_{(\alpha)}$ with α maximal.*

(ii) *Let $\mathcal{R}_{(\alpha)}$*

$$deg\Big(\prod_{j\in\mathcal{R}_{(\alpha)}} f_{v_{p,r,j},p}(q)\Big) = \sum_{j\in\mathcal{R}_{(\alpha)}} deg\big(f_{v_{p,r,j},p}(q)\big) = t(p-1)$$

for some integer t.

Proof. (i) Let P be the collection of all primes distinct from p and r dividing any bi-level of EFE(1) with respect to p and r. By Lemma 3.23, if l is a bi-level of EFE(1) with respect to p and r, then the prime factorization of $v_{p,r,l}$ has the form $\prod_{s\in \mathrm{P}} s^{\pi_s} p^{\nu} r^{\gamma}$ for some nonnegative integers ν, γ and some collection of positive integers $\{\pi_s | s \in \mathrm{P}\}$. Let $\mathcal{R}_{(\alpha)} := \{i_j | r^{\alpha} \| v_{p,r,i_j}\}$ be the collection of all bi-levels of EFE(1) with respect to p and r such that

$$\alpha = \max_{r^{\gamma}\|v_{p,r,i}} \{\gamma\}, \quad \lambda_{(\alpha)} = \max_{p^{\nu}\|v_{p,r,i}, i\in\mathcal{R}_{(\alpha)}} \{\nu\},$$

where i ranges over all bi-levels of EFE(1) with respect to p and r.

Claim. $\mathcal{R} = \mathcal{R}_{(\alpha)}$ is a nonempty chain of EFE(1) with respect to p and r.

Proof of claim. By the definition of α, there exist at least one bi-level i such that $r^{\alpha} \| v_{p,r,i}$. Thus $\mathcal{R}_{(\alpha)} \neq \emptyset$. Let $n \geq 1$ be the cardinality of $\mathcal{R}_{(\alpha)}$. By rearrangement if necessary, we write $\mathcal{R}_{(\alpha)} = \{i_j | 0 \leq j \leq n-1\}$ so that $i_j < i_{j+1}$ (hence $v_{p,r,i_j} > v_{p,r,i_{j+1}}$) for $0 \leq j \leq n-2$. For each $i_j \in \mathcal{R}_{(\alpha)}$, let $\prod_{s\in \mathrm{P}} s^{\pi_s} p^{\lambda_j} r^{\alpha}$ be the prime factorization of v_{p,r,i_j} where λ_j is a nonnegative integer in $\{0, \ldots, \lambda_{(\alpha)}\}$, $\{\pi_s\}$ is some collection of positive integers, and P is the collection of all primes distinct from p and r dividing any bi-level of EFE(1) with respect to p and r. Thus

$$\lambda_{(\alpha)} = \lambda_0 > \cdots > \lambda_{n-1} \geq 0.$$

Let us consider line (i_0) of EFE(1) with respect to p and r:

$$f_{v_{p,r,i_0},p}^{s_{p,i_0}\delta_{r,i_0}}(q) \frac{f_{v_{p,r,i_0},r}(q^p)^{s_{r,i_0}}}{f_{v_{p,r,i_0},r}(q)^{s_{r,i_0}(1-\delta_{p,i_0})}} \overset{(i_0)}{\longleftrightarrow} f_{v_{p,r,i_0},r}^{s_{r,i_0}\delta_{p,i_0}}(q) \frac{f_{v_{p,r,i_0},p}(q^r)^{s_{p,i_0}}}{f_{v_{p,r,i_0},p}(q)^{s_{p,i_0}(1-\delta_{r,i_0})}}.$$

Subclaim. Line (i_0) of EFE(1) with respect to p and r must have the form

$$f_{v_{p,r,i_0},p}(q)^{\delta_{r,i_0}} \frac{f_{v_{p,r,i_0},r}(q^p)}{f_{v_{p,r,i_0},r}(q)^{(1-\delta_{p,i_0})}} \overset{(i_0)}{\longleftrightarrow} f_{v_{p,r,i_0},r}(q)^{\delta_{p,i_0}} \frac{f_{v_{p,r,i_0},p}(q^r)}{f_{v_{p,r,i_0},p}(q)^{(1-\delta_{r,i_0})}},$$

or equivalently, $s_{p,i_0} = 1 = s_{r,i_0}$.

Proof of subclaim. (a) Suppose $s_{p,i_0} = 1$. Then line (i_0) of EFE(1) has the form

$$f_{v_{p,r,i_0},p}(q)^{\delta_{r,i_0}} \frac{f_{v_{p,r,i_0},r}(q^p)^{s_{r,i_0}}}{f_{v_{p,r,i_0},r}(q)^{s_{r,i_0}(1-\delta_{p,i_0})}} \overset{(i_0)}{\leftrightarrow} f_{v_{p,r,i_0},r}(q)^{s_{r,i_0}\delta_{p,i_0}} \frac{f_{v_{p,r,i_0},p}(q^r)}{f_{v_{p,r,i_0},p}(q)^{(1-\delta_{r,i_0})}}.$$

Suppose that $s_{r,i_0} = 0$, then it can be verified that one of the following three possibilities must occur:

(i) There exists a bi-level $l < i_0$ such that $s_{p,l} = 1$ and $f_{v_{p,r,l},p}(q)$ is semi-directly related to $f_{v_{p,r,i_0},p}(q)$. If this was the case, then $v_{p,r,l} = v_{p,r,i_0}r$. Therefore, $r^{\alpha+1} \| v_{p,r,l}$ which contradicts the maximality of α. Thus this case cannot occur.

(ii) There exists a bi-level $l < i_0$ such that $s_{r,l} = 1$ and $f_{v_{p,r,l},r}(q)$ is semi-directly related to $f_{v_{p,r,i_0},r}(q)$. However, this cannot occur since $s_{r,i_0} = 0$ (see the definition of semi-related relation earlier).

(iii) There exist bi-levels $w < l < i_0$ such that either $s_{p,w} = 1$ or $s_{r,l} = 1$ and $f_{v_{p,r,w},p}(q)$ is indirectly related to the ordered pair $(f_{v_{p,r,l},r}(q), f_{v_{p,r,i_0},p}(q))$. A combination of the argument in (i) and (ii) above produces a contradiction.

Therefore, we have $s_{r,i_0} = 1$.

(b) Suppose that $s_{r,i_0} = 1$. Then line (i_0) of EFE(1) has the form

$$f^{s_{p,i_0}\delta_{r,i_0}}_{v_{p,r,i_0},p}(q) \frac{f_{v_{p,r,i_0},r}(q^p)}{f_{v_{p,r,i_0},r}(q)^{(1-\delta_{p,i_0})}} \overset{(i_0)}{\leftrightarrow} f^{\delta_{p,i_0}}_{v_{p,r,i_0},r}(q) \frac{f_{v_{p,r,i_0},p}(q^r)^{s_{p,i_0}}}{f_{v_{p,r,i_0},p}(q)^{s_{p,i_0}(1-\delta_{r,i_0})}}.$$

If $s_{p,i_0} = 0$, then again one of the following possibilities must occur:

(i) There exists a bi-level $l < i_0$ such that $s_{p,l} = 1$ and $f_{v_{p,r,l},p}(q)$ is semi-directly related to $f_{v_{p,r,i_0},p}(q)$. However, this cannot occurs since $s_{r,i_0} = 0$ (see definition of semi-related relation).

(ii) There exists a bi-level $l < i_0$ such that $s_{r,l} = 1$ and $f_{v_{p,r,l},r}(q)$ is semi-directly related to $f_{v_{p,r,i_0},r}(q)$. If this is the case, then $v_{p,r,l} = v_{p,r,i_0}p$. Hence $p^{\lambda_0+1} | v_{p,r,l}$ which means l is not in $\mathcal{R}_{(\alpha)}$. Therefore, if γ is such that $r^{\gamma} \| v_{p,r,l}$, then $\gamma \neq \alpha$. This is a contradiction. Thus this case cannot occur.

(iii) There exist bi-levels $w < l < i_0$ such that either $s_{p,w} = 1$ or $s_{r,l} = 1$ and $f_{v_{p,r,w},p}(q)$ is indirectly related to the ordered pair $(f_{v_{p,r,l},r}(q), f_{v_{p,r,i_0},p}(q))$. Then a combination of the argument in (i) and (ii) above also produces a contradiction.

Thus $s_{p,i_0} = 1$ as well and the subclaim is proven.

□

If $\delta_{p,i_0} = 0$, i.e. $\lambda_0 = 0$, then it is a straightforward verification from the definition of a chain shows that $\mathcal{R}_{(\alpha)} := \{i_0\}$ is a chain. Thus let us suppose that $\delta_{p,i_0} = 1$, i.e. $\lambda_0 = 1$ or equivalently p divides v_{p,r,i_0}. Hence line (i_0) has the form

$$f_{v_{p,r,i_0},p}(q)^{\delta_{r,i_0}} f_{v_{p,r,i_0},r}(q^p) \overset{(i_0)}{\longleftrightarrow} f_{v_{p,r,i_0},r}(q) \frac{f_{v_{p,r,i_0},p}(q^r)}{f_{v_{p,r,i_0},p}(q)^{(1-\delta_{r,i_0})}}.$$

Thus it can be verified from EFE(1) and an earlier remark that there must exist a bi-level $l \geq i_0$ such that line (l) of EFE(1) has the form

$$f_{v_{p,r,l},p}(q)^{s_{p,l}\delta_{r,l}} \frac{f_{v_{p,r,l},r}(q^p)}{f_{v_{p,r,l},r}(q)^{(1-\delta_{p,l})}} \overset{(l)}{\longleftrightarrow} f_{v_{p,r,l},r}(q)^{\delta_{p,l}} \frac{f_{v_{p,r,l},p}(q^r)^{s_{p,l}}}{f_{v_{p,r,l},p}(q)^{(1-\delta_{r,l})}}$$

such that $f_{v_{p,r,i_0},r}(q)$ is semi-related to the polynomial $f_{v_{p,r,l},r}(q)$. Hence $v_{p,r,l} = \frac{v_{p,r,i_0}}{p}$. As $r^\alpha \| v_{p,r,i_0}$, we also have $r^\alpha \| v_{p,r,l}$. Thus $l \in \mathcal{R}_{(\alpha)}$ by definition. Moreover, it is immediate, from the equality $v_{p,r,l} = \frac{v_{p,r,i_0}}{p}$, that $p^{\lambda_0 - 1} \| v_{p,r,l}$. Hence $l = i_1$. If $\delta_{p,l} (= \delta_{p,i_1}) = 0$ (i.e. $\lambda_0 = 1$), then it can be verified that $\mathcal{R}_{(\alpha)} := \{i_0, i_1\}$ is a chain. If $\delta_{p,l} (= \delta_{p,i_1}) = 1$, then there are two possibilities:

(1) There exists bi-levels $g < i_1 < h$ such that $f_{v_{p,r,i_1},r}(q)$ is indirectly-related to the ordered pair of polynomials $(f_{v_{p,r,g},p}(q), f_{v_{p,r,h},p}(q))$, or

(2) There exists bi-level a h such that $f_{v_{p,r,i_1},r}(q)$ semi-directly related to the polynomial $f_{v_{p,r,h},r}(q)$.

If (1) occurs, then $v_{p,r,g}p = v_{p,r,i_1}r$. Thus $r^{\alpha+1} \| v_{p,r,g}$ which contradicts the maximality of α. Therefore (2) must be the case and the proof of the subclaim is complete.

As a result, there exists a bi-level h of EFE(1) such that $f_{v_{p,r,i_1},r}(q)$ is semi-directly related to the polynomial $f_{v_{p,r,h},r}(q)$. Line (h) of EFE(1) must then have the form

$$f_{v_{p,r,h},p}(q)^{s_{p,h}\delta_{r,h}} \frac{f_{v_{p,r,h},r}(q^p)}{f_{v_{p,r,h},r}(q)^{(1-\delta_{p,h})}} \overset{(h)}{\longleftrightarrow} f_{v_{p,r,h},r}(q)^{\delta_{p,h}} \frac{f_{v_{p,r,h},p}(q^r)^{s_{p,l}}}{f_{v_{p,r,h},p}(q)^{(1-\delta_{r,h})}}.$$

By the same argument as above, we have $p^{\lambda_0 - 2} \| v_{p,r,h}$, and thus $h = i_2$. The argument above can be iterated and can only stop when we reach the bi-level z where $p^0 \| v_{p,r,z} = \frac{v_{p,r,1}}{p^{\lambda_0}}$. Line (z) must then have the form

$$f_{v_{p,r,z},p}(q)^{s_{p,z}\delta_{r,z}} \frac{f_{v_{p,r,z},r}(q^p)}{f_{v_{p,r,z},r}(q)} \overset{(z)}{\longleftrightarrow} \frac{f_{v_{p,r,z},p}(q^r)^{s_{p,l}}}{f_{v_{p,r,z},p}(q)^{(1-\delta_{r,z})}}.$$

This also implies that $z = i_{n-1}$ and $\lambda_{(\alpha)} = n - 1$. A straightforward direct verification shows that $\mathcal{R}_{(\alpha)} := \{i_j | 0 \leq j \leq n-1\}$ satisfies all the conditions of a chain. The claim is thus established.

□

The uniqueness of the chain $\mathcal{R} = \mathcal{R}_{(\alpha)}$ above is immediate from its construction.

(ii) For this part, we divide the proof into four cases:

Case 1: $\lambda_{(\alpha)} = 0$.
Case 2: $\lambda_{(\alpha)} = 1$.
Case 3: $\lambda_{(\alpha)} = 2$.
Case 4: $\lambda_{(\alpha)} \geq 3$.

Case 1. Suppose $\lambda_{(\alpha)} = 0$ (i.e. $v_{p,r,i_0} = (\prod_{s\in \mathrm{P}} s^{\pi_s})r^{\alpha}$). Then p does not divide v_{p,r,i_0}. Together with part (1), we have then $\mathcal{R} = \{i_0\}$ and line (i_0) of EFE(1) with respect to p and r has the form

$$f_{v_{p,r,i_0},p}(q)\frac{f_{v_{p,r,i_0},r}(q^p)}{f_{v_{p,r,i_0},r}(q)} \overset{(i_0)}{\longleftrightarrow} \frac{f_{v_{p,r,i_0},p}(q^r)}{f_{v_{p,r,i_0},p}(q)^{(1-\delta_{r,i_0})}}$$

(since $s_{p,i_0} = s_{r,i_0} = 1$).

Claim.

$$\frac{f_{v_{p,r,i_0},r}(q^p)}{f_{v_{p,r,i_0},r}(q)} = \frac{f_{v_{p,r,i_0},p}(q^r)}{f_{v_{p,r,i_0},p}(q)^{(1-\delta_{r,i_0})}}.$$

P r o o f o f C l a i m. Let us suppose

$$\frac{f_{v_{p,r,i_0},r}(q^p)}{f_{v_{p,r,i_0},r}(q)} \neq \frac{f_{v_{p,r,i_0},p}(q^r)}{f_{v_{p,r,i_0},p}(q)^{(1-\delta_{r,i_0})}}.$$

Then it can be verified that one of the following three possibilities must occur:

(i) There exists a bi-level $l < i_0$ such that $s_{p,l} = 1$ and $f_{v_{p,r,l},p}(q)$ is semi-directly related to $f_{v_{p,r,i_0},p}(q)$. If this is the case, then $v_{p,r,l} = v_{p,r,i_0}r$. Therefore, $p^{\alpha+1}\|v_{p,r,l}$ which contradicts the maximality of α. Thus this case cannot occur.

(ii) There exists a bi-level $l < i_0$ such that $s_{r,l} = 1$ and $f_{v_{p,r,l},r}(q)$ is semi-directly related to $f_{v_{p,r,i_0},r}(q)$. Hence $v_{p,r,l} = v_{p,r,i_0}p$ and we have $r^{\alpha}\|v_{p,r,l}$. Thus $l \in \mathcal{R}_{(\alpha)}$ which contradicts the fact that $\mathcal{R}_{(\alpha)} = \{i_0\}$ (note that $v_{p,r,l} = v_{p,r,i_0}p$ implies that $p^{\lambda_{(\alpha)}+1}|v_{p,r,l}$ which means that l can not be in $\mathcal{R}_{(\alpha)}$ by definition of $\lambda_{(\alpha)}$, is independent of that fact that we know $\mathcal{R}_{(\alpha)} = \{i_0\}$ in this case).

(iii) There exist bi-levels $w < l < i_0$ such that either $s_{p,w} = 1$ or $s_{r,l} = 1$ and $f_{v_{p,r,w},p}(q)$ is indirectly related to the ordered pair $(f_{v_{p,r,l},r}(q), f_{v_{p,r,i_0},p}(q))$. A combination of the argument in (i) and (ii) above produces a contradiction.

Therefore, we must have

$$\frac{f_{v_{p,r,i_0},r}(q^p)}{f_{v_{p,r,i_0},r}(q)} = \frac{f_{v_{p,r,i_0},p}(q^r)}{f_{v_{p,r,i_0},p}(q)^{(1-\delta_{r,i_0})}}.$$

□

As a result of the analysis in [4] and the above claim, the collection of all roots of $f_{v_{p,r,1},p}(q)$, with multiplicities, can be represented by the following collection of tuples of integers

$$\bigcup_{\{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,1},p}(q)} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,1},i}}\mathbb{Z})^*\}} \big((\mathbb{Z}/p\mathbb{Z})^* \times (\alpha_{p_i})_i\big),$$

where

- $\prod_i (p_i)^{e_{v_{p,r,1},i}}$ is the prime factorization of $v_{p,r,1}$,
- $(\alpha_{p_i})_i$'s are not necessarily distinct (see [4]) and $((\mathbb{Z}/p\mathbb{Z})^* \times (\alpha_{p_i})_i) := \{(\alpha_p, (\alpha_{p_i})_i) | \alpha_p \in (\mathbb{Z}/p\mathbb{Z})^*\}$,
- $\mathcal{B}_{f_{v_{p,r,1},p}(q)} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,1},i}}\mathbb{Z})^*$ means that the set $\mathcal{B}_{f_{v_{p,r,1},p}(q)}$ is a set of tuples determined by $f_{v_{p,r,1},p}(q)$ each of whose elements is an element of $\prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,1},i}}\mathbb{Z})^*$ but the set $\mathcal{B}_{f_{v_{p,r,1},p}(q)}$ is not necessarily a subset of the set $\prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,1},i}}\mathbb{Z})^*$ (repetition may occur).

Since $|((\mathbb{Z}/p\mathbb{Z})^*, (\alpha_{p_i})_i)| = p - 1$ for each $(\alpha_{p_i})_i$, $\deg(f_{v_{p,r,1},p}(q)) = t(p-1)$ for some integer t (see [4] for more details). Thus the proposition is proven in this case.

Case 2. Suppose that $\lambda_{(\alpha)} = 1$. Then $\mathcal{R} := \mathcal{R}_{(\alpha)} = \{i_j | 0 \leq j \leq n-1\}$ where $n = \lambda_{(\alpha)} + 1 = 2$ (thus $n - 2 = 0$). A similar argument as in the above claim (the details are left to the readers) also shows that

$$\frac{f_{v_{p,r,i_{n-2}},r}(q^p)}{f_{v_{p,r,i_{n-2}},r}(q)} = \frac{f_{v_{p,r,i_{n-2}},p}(q^r)}{f_{v_{p,r,i_{n-2}},p}(q)^{(1-\delta_{r,i_{n-2}})}}.$$

As a result, we have

$$\prod_{1\leq j\leq 2} \frac{f_{v_{p,r,i_{n-j}},p}(q^r)^{s_{p,i_{n-j}}}}{f_{v_{p,r,i_{n-j}},p}(q)^{s_{p,i_{n-j}}(1-\delta_{r,i_{n-j}})}} =$$

$$= f_{v_{p,r,i_{n-2}},r}(q^p) \frac{f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}.$$

Moreover, it can be verified directly from EFE(1) that

$$\frac{f_{v_{p,r,i_{n-1}},r}(q^p)^{s_{r,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},r}(q)^{s_{r,i_{n-1}}(1-\delta_{p,i_{n-1}})}} =$$

$$f_{v_{p,r,i_{n-2}},r}(q)^{s_{r,i_{n-2}}(\delta_{p,i_{n-2}})} \frac{f_{v_{p,r,i_{n-1}},p}(q^p)^{s_{r,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{r,i_{n-1}}(1-\delta_{p,i_{n-1}})}}.$$

By part (i), line (i_{n-1}) of EFE(1) with respect to p and r has the form

$$f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}\delta_{r,i_{n-1}}} \frac{f_{v_{p,r,i_{n-1}},r}(q^p)}{f_{v_{p,r,i_{n-1}},r}(q)} \overset{(i_{n-1})}{\longleftrightarrow} \frac{f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}.$$

From our analysis in [4], all roots, with multiplicities, of $\frac{f_{v_{p,r,i_{n-1}},r}(q^p)}{f_{v_{p,r,i_{n-1}},r}(q)}$ can be represented by the collection of tuples of integers of the form

$$\bigcup_{\{(\alpha_{p_i})_i \in \mathcal{B}_{\frac{f_{v_{p,r,i_{n-1}},r}(q^p)}{f_{v_{p,r,i_{n-1}},r}(q)}} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}r,i}}\mathbb{Z})^*\}} \big((\mathbb{Z}/p\mathbb{Z})^* \times (\alpha_{p_i})_i\big)$$

where $\prod_i (p_i)^{e_{v_{p,r,i_{n-1}}r,i}}$ is the prime factorization of $v_{p,r,i_{n-1}}r$ and $\mathcal{B}_{\frac{f_{v_{p,r,i_{n-1}},r}(q^p)}{f_{v_{p,r,i_{n-1}},r}(q)}}$ is a set determined by $\frac{f_{v_{p,r,i_{n-1}},r}(q^p)}{f_{v_{p,r,i_{n-1}},r}(q)}$ each of whose elements is an element of $\prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}r,i}}\mathbb{Z})^*$ but not necessarily distinct. As a result,

$$deg\left(\frac{f_{v_{p,r,i_{n-1}},r}(q^p)}{f_{v_{p,r,i_{n-1}},r}(q)}\right) = t(p-1)$$

for some nonnegative integer t. From part (i), we have $v_{p,r,i_{n-1}}p = v_{p,r,i_{n-2}}$ as well as $s_{r,i_{n-2}} = 1$. Therefore, we have

$$\frac{f_{v_{p,r,i_{n-1}},r}(q^p)}{f_{v_{p,r,i_{n-1}},r}(q)} = f_{v_{p,r,i_{n-2}},r}(q) \frac{f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}$$

which means that all roots of $f_{v_{p,r,i_{n-2}},r}(q)\frac{f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}$ can be represented, with multiplicities, by the same collection as well. If all the roots of $\frac{f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}$ can be represented, with multiplicity (different from the previous), by the collection of tuples of the form

$$\bigcup_{\{(\alpha_{p_i})_i \in \mathcal{B}_{\frac{f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,1},i}r}\mathbb{Z})^*\}} \big((\mathbb{Z}/p\mathbb{Z})^* \times (\alpha_{p_i})_i\big)$$

with $\mathcal{B}_{\frac{f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}}$ is a set uniquely determined by the polynomial $\frac{f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}$ each of whose elements is an element of the set $\prod_i(\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}r,i}}\mathbb{Z})^*$, where $\prod_i p_i^{e_{v_{p,r,i_{n-1}},i}r}$ is the prime factorization of $v_{p,r,i_{n-1}}r$. $\mathcal{B}_{\frac{f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}}$ is defined to be the empty set if $s_{p,i_{n-1}} = 0$. Hence $\deg\big(\frac{f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}\big) = t(p-1)$ with

$$t = \left|\mathcal{B}_{\frac{f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}}\right|$$

an integer. From our analysis in [4], each root of $\frac{f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}$ is a primitive r-root of a root of $f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}}$. Therefore it can be verified that all roots of $f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}}$ must also be representable by a collection of tuples of the form

$$\bigcup_{\{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}}} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}},i}}\mathbb{Z})^*\}} \big((\mathbb{Z}/p\mathbb{Z})^* \times (\alpha_{p_i})_i\big),$$

where $v_{p,r,i_{n-1}} = \prod_i (p_i)^{e_{p,r,i_{n-1}},i}$ and the set $\mathcal{B}_{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}}}$ is determined by $f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}}$ in the above fashion. Thus we have $\deg(f_{v_{p,r,i_{n-1}},p}(q)) = b(p-1)$, where $b = |\mathcal{B}_{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}}}|$. As a result, roots of $f_{v_{p,r,i_{n-2}},r}(q)$ are representable as the collection of tuples

$$\bigcup_{\{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q)} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}r,i}}\mathbb{Z})^*\}} \big((\mathbb{Z}/p\mathbb{Z})^* \times (\alpha_{p_i})_i\big),$$

where $\mathcal{B}_{f_{v_{p,r,i_{n-1}},r}(q)}$ is the set of tuples determined by $\prod_i p_i^{e_{v_{p,r,i_{n-1}}r,i}}$, the prime factorization of $v_{p,r,i_{n-1}}r$ as above, and the polynomial $f_{v_{p,r,i_{n-2}},r}(q)$. This, together with the analysis in [4] applying to the case where p divides $v_{p,r,i_{n-2}}$, implies that the set of roots of $f_{v_{p,r,i_{n-2}},r}(q^p)$ is representable as the collection of tuples of the form

$$\bigcup_{\{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q)} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}r,i}}\mathbb{Z})^*\}} \Big(\big((\mathbb{Z}/p\mathbb{Z})^* + z(p) \big)_{\{0 \le z \le p-1\}} \times (\alpha_{p_i})_i \Big).$$

As a result, we have $\deg(f_{v_{p,r,i_{n-2}},r}(q^p)) = (tp)(p-1)$ where $t = |\mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q)}|$ since $|((\mathbb{Z}/p\mathbb{Z})^* + z(p))_{\{0 \le z \le p-1\}}| = p(p-1)$. From part (i), it can be deduced that

$$f_{v_{p,r,i_{n-2}},r}(q^p) = f_{v_{p,r,i_{n-2}},r}(q) \frac{f_{v_{p,r,i_{n-2}},p}(q^r)^{s_{p,i_{n-2}}}}{f_{v_{p,r,i_{n-2}},p}(q)^{s_{p,i_{n-2}}(1-\delta_{r,i_{n-2}})}}.$$

Therefore the same argument as above applies at this bi-level, namely i_{n-2}, and can then be iterated.

On the other hand, if the set of roots of $\frac{f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}$ cannot be represented by the collection of tuples

$$\bigcup_{\{(\alpha_{p_i})_i \in \mathcal{B} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}r,i}}\mathbb{Z})^*\}} \big((\mathbb{Z}/p\mathbb{Z})^* \times (\alpha_{p_i})_i \big)$$

for any set $\mathcal{B} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}r,i}}\mathbb{Z})^*$, then it can be verified that the following holds:

- The collection of all roots of $\frac{f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}$, with multiplicities, must be represented by the collection of tuples of the form

$$\bigcup_{\{(\alpha_{p_i})_i \in \mathcal{B}_{\frac{f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}r,i}}\mathbb{Z})^*\}} \big(\mathcal{A}_{(\alpha_{p_i})_i} \times (\alpha_{p_i})_i \big),$$

  where the set $\mathcal{B}_{\frac{f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}}$ is determined by the polynomial $\frac{f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}$ and $\mathcal{A}_{(\alpha_{p_i})_i}$ is a subset of $\{1, \ldots, p-1\}$ for each $(\alpha_{p_i})_i$.

- The collection of all roots of $f_{v_{p,r,i_{n-2}},r}(q)$, with multiplicities, must be represented by the collection of tuples

$$\bigcup_{\{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q)} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}^{r,i}}}\mathbb{Z})^*\}} \big((\mathcal{A}'_{(\alpha_{p_i})_i}) \times (\alpha_{p_i})_i\big),$$

  where $\mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q)}$ is determined by $f_{v_{p,r,i_{n-2}},r}(q)$ and $\mathcal{A}'_{(\alpha_{p_i})_i}$ is some subset of $\{1,\ldots,p-1\}$ for each $(\alpha'_{p_i})_i$.
- For each $(\alpha_{p_i})_i \in \mathcal{B}_{\frac{f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}} \bigcap \mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q)}$, $\mathcal{A}_{(\alpha_{p_i})_i} \cup A'_{(\alpha_{p_i})_i} = (\mathbb{Z}/p\mathbb{Z})^*$.
- Either $\mathcal{A}_{(\alpha_{p_i})_i}$ or $A'_{(\alpha_{p_i})_i}$ must be $(\mathbb{Z}/p\mathbb{Z})^*$ if $(\alpha_{p_i})_i$ is in

$$\Big(\mathcal{B}_{\frac{f_{v_{p,r,h},p}(q^r)^{s_{p,h}}}{f_{v_{p,r,h},p}(q)^{s_{p,h}(1-\delta_{r,h})}}} \cup \mathcal{B}_{f_{v_{p,r,l},r}(q)}\Big) - \Big(\mathcal{B}_{\frac{f_{v_{p,r,h},p}(q^r)^{s_{p,h}}}{f_{v_{p,r,h},p}(q)^{s_{p,h}(1-\delta_{r,h})}}} \cap \mathcal{B}_{f_{v_{p,r,l},r}(q)}\Big).$$

- Either $\mathcal{A}_{(\alpha_{p_i})_i}$ or $A'_{(\alpha_{p_i})_i}$ must be a proper subset of $(\mathbb{Z}/p\mathbb{Z})^*$ for at least one $(\alpha_{p_i})_i$ such that $(\alpha_{p_i})_i \in (\mathcal{B}_{\frac{f_{v_{p,r,h},p}(q^r)^{s_{p,h}}}{f_{v_{p,r,h},p}(q)^{s_{p,h}(1-\delta_{r,h})}}} \cap \mathcal{B}_{f_{v_{p,r,l},r}(q)})$.

By a similar analysis to that found in [4], it can be deduced that all roots of $f_{v_{p,r,i_{n-2}},r}(q^p)$, with multiplicities, must be representable by the collection of tuples

$$\bigcup_{\{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q)} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}^{r,i}}}\mathbb{Z})^*\}} \Big(\big(\mathcal{A}'_{(\alpha_{p_i})_i} + z(p)\big)_{\{0 \le z \le p-1\}} \times (\alpha_{p_i})_i\Big),$$

where the sets $\mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q)}$ and $\mathcal{A}'_{(\alpha_{p_i})_i}$ are defined above and $z(p)_{\{0 \le z \le p-1\}} := \{0, p, 2p, \ldots, (p-1)p\}$.

If $\mathcal{R}_{(\alpha)} = \{i_j | 0 \le j \le 1\}$ (i.e. $n = 2$ and $\lambda_0 = 1$), then $i_0 = i_{n-2}$ in this case. Hence

$$f_{v_{p,r,i_{n-2}},r}(q^p) = \frac{f_{v_{p,r,i_{n-2}},p}(q^r)^{s_{p,i_{n-2}}}}{f_{v_{p,r,i_{n-2}},p}(q)^{s_{p,i_{n-2}}(1-\delta_{r,i_{n-2}})}},$$

which means that $\frac{f_{v_{p,r,i_{n-2}},p}(q^r)^{s_{p,i_{n-2}}}}{f_{v_{p,r,i_{n-2}},p}(q)^{s_{p,i_{n-2}}(1-\delta_{r,i_{n-2}})}} = \frac{f_{v_{p,r,i_{n-2}},p}(q^r)}{f_{v_{p,r,i_{n-2}},p}(q)^{(1-\delta_{r,i_{n-2}})}}$ and that all roots of $\frac{f_{v_{p,r,i_{n-2}},p}(q^r)}{f_{v_{p,r,i_{n-2}},p}(q)^{(1-\delta_{r,i_{n-2}})}}$ must also correspond to the collection of tuples

$$\bigcup_{\{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q^p)} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}r,i}}\mathbb{Z})^*\}} \big((\mathcal{A}'_{(\alpha_{p_i})_i} + z(p))_{\{0\leq z\leq p-1\}} \times (\alpha_{p_i})_i\big).$$

Now let us show that in such case,

$$deg(f_{v_{p,r,i_{n-2}},p}(q)) + deg\big(f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}}\big) = t(p-1)$$

for some integer t. Let us rewrite the above union of tuples of integers as

$$\bigcup_{\{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q)} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}r,i}}\mathbb{Z})^*\}} \big((\mathcal{A}'_{(\alpha_{p_i})_i} + z(p))_{\{0\leq z\leq p-1\}} \times (\alpha_{p_i})_i\big) =$$

$$\Big(\bigcup_{\{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q)} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}r,i}}\mathbb{Z})^*\}} \big((\mathcal{A}'_{(\alpha_{p_i})_i} + z(p))_{\{1\leq z\leq p-1\}} \times (\alpha_{p_i})_i\big)\Big)$$

$$\bigcup\Big(\bigcup_{\{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q)} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}r,i}}\mathbb{Z})^*\}} \big((\mathcal{A}'_{(\alpha_{p_i})_i}) \times (\alpha_{p_i})_i\big)\Big).$$

It can be observed that

$$\Big(\bigcup_{\{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q)} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}r,i}}\mathbb{Z})^*\}} \big((\mathcal{A}'_{(\alpha_{p_i})_i}) \times (\alpha_{p_i})_i\big)\Big)$$

$$\bigcup\Big(\bigcup_{\{(\alpha_{p_i})_i \in \mathcal{B}_{\frac{f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}r,i}}\mathbb{Z})^*\}} \big(\mathcal{A}_{(\alpha_{p_i})_i} \times (\alpha_{p_i})_i\big)\Big)$$

$$= \bigcup_{\{(\alpha_{p_i})_i \in (\mathcal{B}_{\frac{f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}} \cup \mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q)})\}} \big((\mathbb{Z}/p\mathbb{Z})^* \times (\alpha_{p_i})_i\big).$$

As a result, we obtain

$$\Big|\bigcup_{\{(\alpha_{p_i})_i \in (\mathcal{B}_{\frac{f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}} \cup \mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q)})\}} \big((\mathbb{Z}/p\mathbb{Z})^* \times (\alpha_{p_i})_i\big)\Big| =$$

$$= t_{\mathcal{B}_{\frac{f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}} \cup \mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q)}}(p-1).$$

where

$$t_{\mathcal{B}_{\frac{f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}} \cup \mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q^p)}} =$$

$$\left|\mathcal{B}_{\frac{f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}} \cup \mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q^p)}\right|$$

is an integer. Furthermore, we also have

$$\left|\bigcup_{\{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q)} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}}{}^{r,i}}\mathbb{Z})^*\}} \left((\mathcal{A}'_{(\alpha_{p_i})_i} + z(p))_{\{1\le z\le p-1\}} \times (\alpha_{p_i})_i\right)\right| =$$

$$= t_{\mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q^p)}}(p-1),$$

where

$$t_{\mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q)}} = \sum_{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q)}} |\mathcal{A}'_{(\alpha_{p_i})_i}|$$

is an integer.

Since all roots of the polynomial

$$\frac{f_{v_{p,r,i_{n-2}},p}(q^r)}{f_{v_{p,r,i_{n-2}},p}(q)^{(1-\delta_{r,i_{n-2}})}} \frac{f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}$$

can be represented as

$$\bigcup_{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q)} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}}{}^{r,i}}\mathbb{Z})^*} \left((\mathcal{A}'_{(\alpha_{p_i})_i} + z(p))_{\{0\le z\le p-1\}} \times (\alpha_{p_i})_i\right)$$

$$\bigcup_{(\alpha_{p_i})_i \in \mathcal{B}_{\frac{f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}}} \bigcup_{\preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}}{}^{r,i}}\mathbb{Z})^*} \left(\mathcal{A}_{(\alpha_{p_i})_i} \times (\alpha_{p_i})_i\right)$$

$$= \bigcup_{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q)} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}}{}^{r,i}}\mathbb{Z})^*} \left((\mathcal{A}'_{(\alpha_{p_i})_i} + z(p))_{\{1\le z\le p-1\}} \times (\alpha_{p_i})_i\right)$$

$$\bigcup_{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-2}}},r(q)} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}}{}^{r,i}}\mathbb{Z})^*} \bigcup ((\mathcal{A}'_{(\alpha_{p_i})_i}) \times (\alpha_{p_i})_i)$$

$$\bigcup_{(\alpha_{p_i})_i \in \mathcal{B}_{\frac{f_{v_{p,r,i_{n-1}}},p(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}}},p(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}}{}^{r,i}}\mathbb{Z})^*} \bigcup (\mathcal{A}_{(\alpha_{p_i})_i} \times (\alpha_{p_i})_i)$$

$$= \bigcup_{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-2}}},r(q)} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}}{}^{r,i}}\mathbb{Z})^*} ((\mathcal{A}'_{(\alpha_{p_i})_i} + z(p))_{\{1 \le z \le p-1\}} \times (\alpha_{p_i})_i)$$

$$\bigcup_{(\alpha_{p_i})_i \in (\mathcal{B}_{\frac{f_{v_{p,r,i_{n-1}}},p(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}}},p(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}} \cup \mathcal{B}_{f_{v_{p,r,i_{n-2}}},r(q)})} \bigcup ((\mathbb{Z}/p\mathbb{Z})^* \times (\alpha_{p_i})_i).$$

As a result, the cardinality of the set of roots of the polynomial

$$\frac{f_{v_{p,r,i_{n-2}}},p(q^r)}{f_{v_{p,r,i_{n-2}}},p(q)^{(1-\delta_{r,i_{n-2}})}} \frac{f_{v_{p,r,i_{n-1}}},p(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}}},p(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}$$

is

$$t_{\mathcal{B}_{\frac{f_{v_{p,r,i_{n-1}}},p(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}}},p(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}} \cup \mathcal{B}_{f_{v_{p,r,i_{n-2}}},r(q)}}(p-1) + t_{\mathcal{B}_{f_{v_{p,r,i_{n-2}}},r(q^p)}}(p-1) =$$

$$= \big(t_{\mathcal{B}_{\frac{f_{v_{p,r,i_{n-1}}},p(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}}},p(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}} \cup \mathcal{B}_{f_{v_{p,r,i_{n-2}}},r(q)}} + t_{\mathcal{B}_{f_{v_{p,r,i_{n-2}}},r(q)}}\big)(p-1) =$$

$$= deg\Big(\frac{f_{v_{p,r,i_{n-2}}},p(q^r)^{s_{p,i_{n-2}}}}{f_{v_{p,r,i_{n-2}}},p(q)^{s_{p,i_{n-2}}(1-\delta_{r,i_{n-2}})}}\Big) + deg\Big(\frac{f_{v_{p,r,i_{n-1}}},p(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}}},p(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}\Big).$$

Let us show that $deg(f_{v_{p,r,i_{n-2}}},p(q)) + deg(f_{v_{p,r,i_{n-1}}},p(q)^{s_{p,i_{n-1}}}) = t(p-1)$ for some integer t. Let $v_{p,r,i_{n-1}} = \prod_i p_i^{e_{p,r,i_{n-1},i}}$ and $v_{p,r,i_{n-2}} = \prod_i p_i^{e_{p,r,i_{n-2},i}}$ be the prime factorizations of $v_{p,r,i_{n-1}}$ and $v_{p,r,i_{n-2}}$ respectively. From part (i), $e_{p,r,i_{n-1},i} = e_{p,r,i_{n-2},i}$ for all i except when $p_i = p$, in which case $e_{p,r,i_{n-1},i} + 1 = e_{p,r,i_{n-2},i}$. From [4], it can be verified that the set of roots of $f_{v_{p,r,i_{n-2}}},p(q^r)$ can be represented as the following union of collections of tuples

$$\Big(\bigcup_{\{(\alpha_{p_i})_i \in \mathcal{D}_{f_{v_{p,r,i_{n-2}}},p(q)} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-2}}}{}^{,i}}\mathbb{Z})^*\}} ((\alpha_{p_i})_i \times (\mathbb{Z}/r\mathbb{Z})^*)\Big) \bigcup$$

$$\Big(\bigcup_{\{(\alpha_{p_i})_i\in\mathcal{D}^*_{f_{v_{p,r,i_{n-2}}},p(q)}\preceq\prod_i(\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-2}},i}}\mathbb{Z})^*\}}(\alpha_{p_i})_i\Big),$$

and that the set of all roots of $\dfrac{f_{v_{p,r,i_{n-2}},p}(q^r)}{f_{v_{p,r,i_{n-2}},p}(q)^{(1-\delta_{r,i_{n-2}})}}$ corresponds to

$$\bigcup_{\{(\alpha_{p_i})_i\in\mathcal{D}_{f_{v_{p,r,i_{n-2}},p}(q)}\preceq\prod_i(\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-2}},i}}\mathbb{Z})^*\}}\big((\alpha_{p_i})_i\times(\mathbb{Z}/r\mathbb{Z})^*\big),$$

where the set $\mathcal{D}_{f_{v_{p,r,i_{n-2}},p}(q)}$ is determined by $f_{v_{p,r,i_{n-2}},p}(q)$, each of whose elements is an element of $\prod_i(\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-2}},i}}\mathbb{Z})^*$, and $\mathcal{B}^*_{f_{v_{p,r,i_{n-2}},p}(q)}$ is defined as follows:

$$\begin{cases}\mathcal{D}^*_{f_{v_{p,r,i_{n-2}},p}(q)}:=\mathcal{D}_{f_{v_{p,r,i_{n-2}},p}(q)} & \text{if } \delta_{r,i_{n-2}}=0,\\ \mathcal{D}^*_{f_{v_{p,r,i_{n-2}},p}(q)}:=\emptyset & \text{otherwise.}\end{cases}$$

These unions can be rewritten as

$$\Big(\bigcup_{\{(\alpha_{p_i})'_i\in\mathcal{D}'_{f_{v_{p,r,i_{n-2}},p}(q)}\preceq\prod'_i(\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-2}},i}}\mathbb{Z})^*\}}\big((\alpha_{p_i})'_i\times\mathcal{A}_{((\alpha_{p_i})'_i,i_{n-2})}\times(\mathbb{Z}/r\mathbb{Z})^*\big)\Big)\bigcup$$

$$\Big(\bigcup_{\{(\alpha_{p_i})'_i\in\mathcal{D}^{*,\prime}_{f_{v_{p,r,i_{n-2}},p}(q)}\preceq\prod'_i(\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-2}},i}}\mathbb{Z})^*\}}\big((\alpha_{p_i})'_i\times\mathcal{A}_{((\alpha_{p_i})'_i,i_{n-2})}\big)\Big)$$

and

$$\bigcup_{\{(\alpha_{p_i})'_i\in\mathcal{D}'_{f_{v_{p,r,i_{n-2}},p}(q)}\preceq\prod'_i(\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-2}},i}}\mathbb{Z})^*\}}\big((\alpha_{p_i})'_i\times\mathcal{A}_{((\alpha_{p_i})'_i,i_{n-2})}\times(\mathbb{Z}/r\mathbb{Z})^*\big)$$

respectively, where

- $\prod'_i(\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-2}},i}}\mathbb{Z})^*$ is equal to $\prod_i(\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-2}},i}}\mathbb{Z})^*$ with the $p_i=p$ omitted.
- $(\alpha_{p_i})'_i$ is $(\alpha_{p_i})_i$ but with the component $\alpha_{p_i=p}$ omitted.
- $(\alpha_{p_i})'_i\in\mathcal{D}'_{f_{v_{p,r,i_{n-2}},p}(q)}$ if and only if $(\alpha_{p_i})_i\in\mathcal{D}_{f_{v_{p,r,i_{n-2}},p}(q)}$.
- $\mathcal{A}_{((\alpha_{p_i})'_i,i_{n-2})}\subseteq(\mathbb{Z}/p^2\mathbb{Z})^*$ (since $p\|v_{p,r,i_{n-2}}$) ,
- $\mathcal{D}^{*,\prime}_{f_{v_{p,r,i_{n-2}},p}(q)}$ is defined similarly as $\mathcal{D}^*_{f_{v_{p,r,i_{n-2}},p}(q)}$ but with $\mathcal{D}'_{f_{v_{p,r,i_{n-2}},p}(q)}$ replacing $\mathcal{D}_{f_{v_{p,r,i_{n-2}},p}(q)}$.

By similar reasoning, the set of all roots of $f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}$ is representable as

$$\Big(\bigcup_{\{(\alpha_{p_i})_i\in\mathcal{D}_{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}}}\preceq\prod_i(\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}},i}}\mathbb{Z})^*\}}\big((\alpha_{p_i})_i\times(\mathbb{Z}/r\mathbb{Z})^*\big)\Big)\bigcup$$

$$\big(\bigcup_{\{(\alpha_{p_i})_i\in\mathcal{D}^*_{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}}}\preceq\prod_i(\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}},i}}\mathbb{Z})^*\}}(\alpha_{p_i})_i\big)$$

and the set of roots of $\frac{f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}$ corresponds to the set

$$\Big(\bigcup_{\{(\alpha_{p_i})_i\in\mathcal{D}_{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}}}\preceq\prod_i(\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}},i}}\mathbb{Z})^*\}}\big((\alpha_{p_i})_i\times(\mathbb{Z}/r\mathbb{Z})^*\big)\Big),$$

where $\mathcal{D}_{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}}}$ is the set of tuples, which is defined to be the empty set if $s_{p,i_{n-1}}=0$, determined by $f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}}$, each of whose elements is an element of $\prod_i(\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}},i}}\mathbb{Z})^*$ while

$$\mathcal{D}^*_{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}}}:=\mathcal{D}_{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}}}$$

if $\delta_{r,i_{n-1}}=0$ and is the empty set otherwise. This union can also be rewritten as

$$\bigcup_{(\alpha_{p_i})'_i\in\mathcal{D}'_{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}}}\preceq\prod'_i(\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}},i}}\mathbb{Z})^*}\big((\alpha_{p_i})'_i\times\mathcal{A}_{((\alpha_{p_i})'_i,i_{n-1})}\times(\mathbb{Z}/r\mathbb{Z})^*\big)$$

$$\bigcup\bigcup_{(\alpha_{p_i})'_i\in\mathcal{D}^{*,\prime}_{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}}}\preceq\prod'_i(\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}},i}}\mathbb{Z})^*}\big((\alpha_{p_i})'_i\times\mathcal{A}_{((\alpha_{p_i})'_i,i_{n-1})}\big)$$

and

$$\bigcup_{(\alpha_{p_i})'_i\in\mathcal{D}'_{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}}}\preceq\prod'_i(\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}},i}}\mathbb{Z})^*}\big((\alpha_{p_i})'_i\times\mathcal{A}_{((\alpha_{p_i})'_i,i_{n-2})}\times(\mathbb{Z}/r\mathbb{Z})^*\big),$$

respectively, where

- $\prod_i'(\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}},i}}\mathbb{Z})^*$ is $\prod_i'(\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}},i}}\mathbb{Z})^*$ with the component corresponding to the prime $p_i = p$ omitted (hence $\prod_i'(\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}},i}}\mathbb{Z})^* = \prod_i'(\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-2}},i}}\mathbb{Z})^*$).
- $(\alpha_{p_i})_i'$ is $(\alpha_{p_i})_i$ with the component $\alpha_{p_w=p}$ omitted.
- $(\alpha_{p_i})_i' \in \mathcal{D}'_{f_{v_{p,r,h}},p(q)^{s_{p,h}}}$ if and only if $(\alpha_{p_i})_i \in \mathcal{D}_{f_{v_{p,r,h}},p(q)^{s_{p,h}}}$.
- If $s_{p,i_{n-1}} = 0$, then $\mathcal{D}'_{f_{v_{p,r,i_{n-1}}},p(q)^{s_{p,i_{n-1}}}} = \emptyset$.

By construction, we have the following tautological bijections of sets:

(1) $\big(\mathcal{D}'_{f_{v_{p,r,i_{n-2}}},p(q)} \times (\mathbb{Z}/r\mathbb{Z})^*\big) \longleftrightarrow \mathcal{B}_{\frac{f_{v_{p,r,i_{n-2}}},p(q^r)}{f_{v_{p,r,i_{n-2}}},p(q)^{(1-\delta_{r,i_{n-2}})}}}$.

(2) $\big(\mathcal{D}'_{f_{v_{p,r,i_{n-1}}},p(q)^{s_{p,i_{n-1}}}} \times (\mathbb{Z}/r\mathbb{Z})^*\big) \longleftrightarrow \mathcal{B}_{\frac{f_{v_{p,r,i_{n-1}}},p(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}}},p(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}}$.

(3) $\big(\mathcal{D}^{*,\prime}_{f_{v_{p,r,i_{n-2}}},p(q)} \times (\mathbb{Z}/r\mathbb{Z})^*\big) \longleftrightarrow \mathcal{B}_{f_{v_{p,r,i_{n-2}}},p(q)}$.

(4) $\big(\mathcal{D}^{*,\prime}_{f_{v_{p,r,i_{n-1}}},p(q)^{s_{p,i_{n-1}}}} \times (\mathbb{Z}/r\mathbb{Z})^*\big) \longleftrightarrow \mathcal{B}_{f_{v_{p,r,i_{n-1}}},p(q)^{s_{p,i_{n-1}}}}$.

Remark 3.24. The bijections agree on all the relevant overlap of domains.

For each $((\alpha_{p_i})_i', \tau)$ in

$$\big(\mathcal{D}'_{f_{v_{p,r,i_{n-2}}},p(q)} \times (\mathbb{Z}/r\mathbb{Z})^*\big) \cup \big(\mathcal{D}'_{f_{v_{p,r,i_{n-1}}},p(q)^{s_{p,i_{n-1}}}} \times (\mathbb{Z}/r\mathbb{Z})^*\big),$$

let $(\alpha_{p_i})_i$ be its image in $\mathcal{B}_{f_{v_{p,r,i_{n-2}}},p(q)} \cup \mathcal{B}_{\frac{f_{v_{p,r,i_{n-1}}},p(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}}},p(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}}$ under the bijections in (1) or (2). Then it can be verified that for any $\tau \in (\mathbb{Z}/r\mathbb{Z})^*$

$$|\mathcal{A}_{((\alpha_{p_i})_i', i_{n-12})}| + |\mathcal{A}_{((\alpha_{p_i})_i', i_{n-1})}| = |\mathcal{A}_{(\alpha_{p_i})_i}| + \Big|\Big(\cup_{0\le z\le p-1}\big(\mathcal{A}'_{(\alpha_{p_i})_i} + z(p)\big)\Big)\Big| =$$
$$= (|\mathcal{A}_{(\alpha_{p_i})_i}| + |\mathcal{A}'_{(\alpha_{p_i})_i}|) + \sum_{1\le z\le p-1} |(\mathcal{A}'_{(\alpha_{p_i})_i} + z(p)| = t(p-1)$$

for some integer t. Therefore, we have

$$\sum_{\{(\alpha_{p_i})_i' \in \mathcal{D}^{*,\prime}_{f_{v_{p,r,i_{n-2}}},p(q)} \preceq \prod_i'(\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-2}},i}}\mathbb{Z})^*\}} |\mathcal{A}_{((\alpha_{p_i})_i', i_{n-2})}| +$$
$$+ \sum_{\{(\alpha_{p_i})_i' \in \mathcal{D}^{*,\prime}_{f_{v_{p,r,i_{n-1}}},p(q)^{s_{p,i_{n-1}}}} \preceq \prod_i'(\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}},i}}\mathbb{Z})^*\}} |\mathcal{A}_{((\alpha_{p_i})_i', i_{n-2})}| =$$

$$= s(p-1) = deg\big(f_{v_{p,r,i_{n-2}},p}(q)\big) + deg\big(f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}}\big) =$$

$$= deg\big(f_{v_{p,r,i_{n-2}},p}(q) f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}}\big)$$

for some integer s as desired.

Case 3: Let $\lambda_{(\alpha)} = 2$. It can be verified from part (i) that in this case $\mathcal{R}_{(2)} = \{i_j | 0 \leq j \leq n-1\} = \{i_0, i_1, i_2\}$, where $n = \lambda_{(\alpha)} + 1 = 3$. It can then be verified from EFE(1) that

$$f_{v_{p,r,i_0},r}(q^p) = f_{v_{p,r,i_{n-3}},r}(q^p) = \frac{f_{v_{p,r,i_{n-3}},p}(q^r)^{s_{p,i_{n-3}}}}{f_{v_{p,r,i_{n-3}},p}(q)^{s_{p,i_{n-3}}(1-\delta_{r,i_{n-3}})}} =$$

$$\frac{f_{v_{p,r,i_0},p}(q^r)}{f_{v_{p,r,i_0},p}(q)^{(1-\delta_{r,i_0})}}.$$

As a result, we have

$$\prod_{1 \leq j \leq 3} \frac{f_{v_{p,r,i_{n-j}},p}(q^r)^{s_{p,i_{n-j}}}}{f_{v_{p,r,i_{n-j}},p}(q)^{s_{p,i_{n-j}}(1-\delta_{r,i_{n-j}})}} =$$

$$= f_{v_{p,r,i_{n-3}},r}(q^p) \prod_{1 \leq j \leq 2} \frac{f_{v_{p,r,i_{n-j}},p}(q^r)^{s_{p,i_{n-j}}}}{f_{v_{p,r,i_{n-j}},p}(q)^{s_{p,i_{n-j}}(1-\delta_{r,i_{n-j}})}}.$$

Similar to Case 2, it can be verified directly from EFE(1) that

$$\frac{f_{v_{p,r,i_{n-j}},r}(q^p)^{s_{r,i_{n-j}}}}{f_{v_{p,r,i_{n-j}},r}(q)^{s_{r,i_{n-j}}(1-\delta_{p,i_{n-j}})}} = f_{v_{p,r,i_{n-(j+1)}},r}(q)^{s_{r,i_{n-(j+1)}}(\delta_{p,i_{n-(j+1)}})}.$$

$$\cdot \frac{f_{v_{p,r,i_{n-j}},p}(q^p)^{s_{r,i_{n-j}}}}{f_{v_{p,r,i_{n-j}},p}(q)^{s_{r,i_{n-j}}(1-\delta_{p,i_{n-j}})}}$$

for $1 \leq j \leq 2$.

For this case, we proceed using what is known in Case 2. What makes Case 3 different from Case 2 is that we have

$$f_{v_{p,r,i_{n-2}},r}(q^p) = f_{v_{p,r,i_{n-3}},r}(q) \frac{f_{v_{p,r,i_{n-2}},p}(q^r)^{s_{p,i_{n-2}}}}{f_{v_{p,r,i_{n-2}},p}(q)^{s_{p,i_{n-2}}(1-\delta_{r,i_{n-2}})}}$$

instead of

$$f_{v_{p,r,i_{n-2}},r}(q^p) = \frac{f_{v_{p,r,i_{n-2}},p}(q^r)^{s_{p,i_{n-2}}}}{f_{v_{p,r,i_{n-2}},p}(q)^{s_{p,i_{n-2}}(1-\delta_{r,i_{n-2}})}}$$

as in Case 2.

From Case 2, we know that

$$\frac{f_{v_{p,r,i_{n-1}},r}(q^p)}{f_{v_{p,r,i_{n-1}},r}(q)} = f_{v_{p,r,i_{n-2}},r}(q)\frac{f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}}$$

and that the collections of all roots of $f_{v_{p,r,i_{n-1}},r}(q)$ and $\frac{f_{v_{p,r,i_{n-1}},r}(q^p)}{f_{v_{p,r,i_{n-1}},r}(q)}$, with multiplicities, are represented by the collections of tuples

$$\bigcup_{\{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-1}},r}(q)} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}r,i}}\mathbb{Z})^*\}} (\alpha_{p_i})_i$$

and

$$\bigcup_{\{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-1}},r}(q)} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}r,i}}\mathbb{Z})^*\}} \big((\mathbb{Z}/p\mathbb{Z})^* \times (\alpha_{p_i})_i\big),$$

respectively, where the set $\mathcal{B}_{f_{v_{p,r,i_{n-1}},r}(q)}$ was defined earlier. Thus the collection of all roots of

$$f_{v_{p,r,i_{n-2}},r}(q)\frac{f_{v_{p,r,i_{n-1}},p}(q^r)^{s_{p,i_{n-1}}}}{f_{v_{p,r,i_{n-1}},p}(q)^{s_{p,i_{n-1}}(1-\delta_{r,i_{n-1}})}},$$

with multiplicities, is represented by the latter collection. For the latter collection of tuples, we have

$$\Big|\bigcup_{\{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-1}},r}(q)} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}r,i}}\mathbb{Z})^*\}} \big((\mathbb{Z}/p\mathbb{Z})^* \times (\alpha_{p_i})_i\big)\Big| =$$

$$= \Big(\sum_{\{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-1}},r}(q)} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}r,i}}\mathbb{Z})^*\}} 1\Big)(p-1) = |\mathcal{B}_{f_{v_{p,r,i_{n-1}},r}(q)}|(p-1).$$

We also know that the sets of all roots of $f_{v_{p,r,i_{n-2}},r}(q)$ and $f_{v_{p,r,i_{n-2}},r}(q^p)$, with multiplicities, are represented by the collections of tuples

$$\bigcup_{\{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q)} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}r,i}}\mathbb{Z})^*\}} \big(\mathcal{A}'_{(\alpha_{p_i})_i} \times (\alpha_{p_i})_i\big)$$

and

$$\bigcup_{\{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q)} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}r,i}}\mathbb{Z})^*\}} \Big(\big(\mathcal{A}'_{(\alpha_{p_i})_i} + z(p)\big)_{\{0\le z\le p-1\}} \times (\alpha_{p_i})_i\Big),$$

respectively, where the sets $\mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q)}$ and $\mathcal{A}'_{(\alpha_{p_i})_i}$ are defined earlier and where $z(p)_{\{0\le z\le p-1\}} := \{0, p, 2p, \dots, (p-1)p\}$. Thus the collection of all roots of

$$f_{v_{p,r,i_{n-3}},r}(q)\frac{f_{v_{p,r,i_{n-2}},p}(q^r)^{s_{p,i_{n-2}}}}{f_{v_{p,r,i_{n-2}},p}(q)^{s_{p,i_{n-2}}(1-\delta_{r,i_{n-2}})}},$$

with multiplicities, is represented by the latter collection. The latter collection of tuples can be be rewritten as

$$\bigcup_{\{(\alpha_{p_i})_i\in\mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q)}\preceq\prod_i(\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}r,i}}\mathbb{Z})^*\}}\Big(\big(\mathcal{A}'_{(\alpha_{p_i})_i}+z(p)\big)_{\{1\le z\le p-1\}}\times(\alpha_{p_i})_i\Big)$$

$$\bigcup\Bigg(\bigcup_{\{(\alpha_{p_i})_i\in\mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q)}\preceq\prod_i(\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}r,i}}\mathbb{Z})^*\}}\big(\mathcal{A}'_{(\alpha_{p_i})_i}\times(\alpha_{p_i})_i\big)\Bigg),$$

where

$$\Bigg(\bigcup_{\{(\alpha_{p_i})_i\in\mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q)}\preceq\prod_i(\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}r,i}}\mathbb{Z})^*\}}\big(\mathcal{A}'_{(\alpha_{p_i})_i}\times(\alpha_{p_i})_i\big)\Bigg)$$

can be identified with the collection of all roots of $f_{v_{p,r,i_{n-2}},r}(q)$, with multiplicities, in the obvious way and

$$\left|\bigcup_{\{(\alpha_{p_i})_i\in\mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q)}\preceq\prod_i(\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}r,i}}\mathbb{Z})^*\}}\Big(\big(\mathcal{A}'_{(\alpha_{p_i})_i}+z(p)\big)_{\{1\le z\le p-1\}}\times(\alpha_{p_i})_i\Big)\right| =$$

$$=\Bigg(\sum_{\{(\alpha_{p_i})_i\in\mathcal{B}_{f_{v_{p,r,i_{n-2}},r}(q)}\preceq\prod_i(\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}r,i}}\mathbb{Z})^*\}}|\mathcal{A}'_{(\alpha_{p_i})_i}|\Bigg)(p-1).$$

As $p^2\|v_{p,r,i_{n-3}}$, the collection of roots of $f_{v_{p,r,i_{n-3}},r}(q)$, with multiplicities, can be represented as the collection of tuples of the form

$$\bigcup_{\{(\alpha_{p_i})_i\in\mathcal{B}_{f_{v_{p,r,i_{n-3}},r}(q)}\preceq\prod_i(\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}r,i}}\mathbb{Z})^*\}}\big(\mathcal{A}_{((\alpha_{p_i})_i,i_{n-3})}\times(\alpha_{p_i})_i\big),$$

where

- $\mathcal{B}_{f_{v_{p,r,i_{n-3}},r}(q)}$ is a set determined by the polynomials $f_{v_{p,r,i_{n-3}},r}(q)$, each of whose elements is an element of the set $\prod_i(\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}r,i}}\mathbb{Z})^*$.
- $\mathcal{A}_{((\alpha_{p_i})_i,i_{n-3})}$ is some subset of $(\mathbb{Z}/p^2\mathbb{Z})^*$.

Therefore the collection of roots, with multiplicities, of $f_{v_{p,r,i_{n-3}},r}(q^p)$ (thus also of the polynomial $\frac{f_{v_{p,r,i_{n-3}},p}(q^r)^{s_{p,i_{n-3}}}}{f_{v_{p,r,i_{n-3}},p}(q)^{s_{p,i_{n-3}}(1-\delta_{r,i_{n-3}})}}$ by the above) is represented as the collection of tuples of the form

$$\bigcup_{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-3}},r(q)}} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}}{}^{r,i}}\mathbb{Z})^*} \left(\mathcal{A}_{((\alpha_{p_i})_i,i_{n-3})} + z(p^2)\right)_{\{0\leq z\leq p-1\}} \times (\alpha_{p_i})_i$$

which can be rewritten as

$$\bigcup_{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-3}},r(q)}} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}}{}^{r,i}}\mathbb{Z})^*} \left(\mathcal{A}_{((\alpha_{p_i})_i,i_{n-3})} + z(p^2)\right)_{\{1\leq z\leq p-1\}} \times (\alpha_{p_i})_i$$

$$\bigcup \bigcup_{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-3}},r(q)}} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}}{}^{r,i}}\mathbb{Z})^*} \left(\mathcal{A}_{((\alpha_{p_i})_i,i_{n-3})} \times (\alpha_{p_i})_i\right),$$

where

$$\left(\bigcup_{\{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-3}},r(q)}} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}}{}^{r,i}}\mathbb{Z})^*\}} \left(\mathcal{A}_{((\alpha_{p_i})_i,i_{n-3})} \times (\alpha_{p_i})_i\right)\right)$$

can be identified with the collection of all roots of $f_{v_{p,r,i_{n-3}},r}(q)$, with multiplicities, in the obvious way and

$$\left|\bigcup_{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-3}},r(q)}} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}}{}^{r,i}}\mathbb{Z})^*} \left(\mathcal{A}_{((\alpha_{p_i})_i,i_{n-3})} + z(p^2)\right)_{\{1\leq z\leq p-1\}} \times (\alpha_{p_i})_i\right|$$

$$= \left(\sum_{\{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-3}},r(q)}} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}}{}^{r,i}}\mathbb{Z})^*\}} \left|\mathcal{A}_{((\alpha_{p_i})_i,i_{n-3})}\right|\right)(p-1).$$

Assembling all this information, it can be verified that the collection of roots, with multiplicities, of

$$\prod_{1\leq j\leq 3} \frac{f_{v_{p,r,i_{n-j}},p}(q^r)^{s_{p,i_{n-j}}}}{f_{v_{p,r,i_{n-j}},p}(q)^{s_{p,i_{n-j}}(1-\delta_{r,i_{n-j}})}}$$

can be represented as the collection of tuples of the form

$$\bigcup_{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-1}}},r(q)} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}}{}^{r,i}}\mathbb{Z})^*} ((\mathbb{Z}/p\mathbb{Z})^* \times (\alpha_{p_i})_i) \bigcup'$$

$$\bigcup_{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-2}}},r(q)} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}}{}^{r,i}}\mathbb{Z})^*} \big(\mathcal{A}'_{(\alpha_{p_i})_i} + z(p)\big)_{\{1 \le z \le p-1\}} \times (\alpha_{p_i})_i \bigcup'$$

$$\bigcup_{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-3}}},r(q)} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}}{}^{r,i}}\mathbb{Z})^*} \big(\mathcal{A}_{((\alpha_{p_i})_i, i_{n-3})} + z(p^2)\big)_{\{1 \le z \le p-1\}} \times (\alpha_{p_i})_i,$$

where $\bigcup'$ denotes the union which takes into account multiplicities. Therefore it can be verified that the cardinality of the set of roots, with multiplicities, of the polynomials $\prod_{1 \le j \le 3} \frac{f_{v_{p,r,i_{n-j}}},p(q^r)^{s_{p,i_{n-j}}}}{f_{v_{p,r,i_{n-j}}},p(q)^{s_{p,i_{n-j}}(1-\delta_{r,i_{n-j}})}}$ is

$$|\mathcal{B}_{f_{v_{p,r,i_{n-1}}},r(q)}|((p-1)+$$

$$+ \sum_{\{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-2}}},r(q)} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}}{}^{r,i}}\mathbb{Z})^*\}} |\mathcal{A}'_{(\alpha_{p_i})_i}|(p-1)+$$

$$+ \sum_{\{(\alpha_{p_i})_i \in \mathcal{B}_{f_{v_{p,r,i_{n-3}}},r(q)} \preceq \prod_i (\mathbb{Z}/p_i^{e_{v_{p,r,i_{n-1}}}{}^{r,i}}\mathbb{Z})^*\}} |\mathcal{A}_{((\alpha_{p_i})_i, i_{n-3})}|(p-1) = t(p-1)$$

for some integer t. Thus

$$deg\Big(\prod_{1 \le j \le 3} \frac{f_{v_{p,r,i_{n-j}}},p(q^r)^{s_{p,i_{n-j}}}}{f_{v_{p,r,i_{n-j}}},p(q)^{s_{p,i_{n-j}}(1-\delta_{r,i_{n-j}})}}\Big) =$$

$$= \sum_{1 \le j \le 3} deg\Big(\frac{f_{v_{p,r,i_{n-j}}},p(q^r)^{s_{p,i_{n-j}}}}{f_{v_{p,r,i_{n-j}}},p(q)^{s_{p,i_{n-j}}(1-\delta_{r,i_{n-j}})}}\Big) = t(p-1).$$

By employing the same method as in Case 2, we also arrive at

$$deg\Big(\prod_{1 \le j \le 3} f_{v_{p,r,i_{n-j}}},p(q)^{s_{p,i_{n-j}}}\Big) = \sum_{1 \le j \le 3} deg\Big(f_{v_{p,r,i_{n-j}}},p(q)^{s_{p,i_{n-j}}}\Big) = s(p-1)$$

for some integer s as desired.

Remark 3.25. We leave the last verification to the interested readers using the method explained in Case 2. The hint for this is to note that the factor $(p-1)$ comes from the cardinality of the p-components of various collections of tuples and thus is independent of the changes in r-component which comes from taking r-roots.

Case 4: Let $\lambda_{(\alpha)} \geq 3$. Then it can be verified that $\mathcal{R}_{(\alpha)} = \{i_j | 0 \leq j \leq n-1\}$ for $n = \lambda_{(\alpha)} + 1$, where α is the maximal power of r dividing $v_{p,r,i}$ for any bi-levels i occurring in EFE(1) with respect to p and r. By a similar argument as in Case 3, it can be verified from EFE(1) with respect to p and r that

$$f_{v_{p,r,i_0},r}(q^p) = f_{v_{p,r,i_{n-(\lambda_{(\alpha)}+1)}},r}(q^p) =$$

$$\frac{f_{v_{p,r,i_{n-(\lambda_{(\alpha)}+1)}},p}(q^r) s_{p,i_{n-(\lambda_{(\alpha)}+1)}}}{f_{v_{p,r,i_{n-(\lambda_{(\alpha)}+1)}},p}(q)^{s_{p,i_{n-(\lambda_{(\alpha)}+1)}}(1-\delta_{r,i_{n-(\lambda_{(\alpha)}+1)}})}} = \frac{f_{v_{p,r,i_0},p}(q^r)}{f_{v_{p,r,i_0},p}(q)^{(1-\delta_{r,i_0})}},$$

$$\prod_{1 \leq j \leq \lambda_0+1} \frac{f_{v_{p,r,i_{n-j}},p}(q^r)^{s_{p,i_{n-j}}}}{f_{v_{p,r,i_{n-j}},p}(q)^{s_{p,i_{n-j}}(1-\delta_{r,i_{n-j}})}} =$$

$$= f_{v_{p,r,i_{n-(\lambda_0+1)}},r}(q^p) \prod_{1 \leq j \leq \lambda_0} \frac{f_{v_{p,r,i_{n-j}},p}(q^r)^{s_{p,i_{n-j}}}}{f_{v_{p,r,i_{n-j}},p}(q)^{s_{p,i_{n-j}}(1-\delta_{r,i_{n-j}})}}$$

and

$$\frac{f_{v_{p,r,i_{n-j}},r}(q^p)^{s_{r,i_{n-j}}}}{f_{v_{p,r,i_{n-j}},r}(q)^{s_{r,i_{n-j}}(1-\delta_{p,i_{n-j}})}} = f_{v_{p,r,i_{n-(j+1)}},r}(q)^{s_{r,i_{n-(j+1)}}(\delta_{p,i_{n-(j+1)}})}.$$

$$\cdot \frac{f_{v_{p,r,i_{n-j}},p}(q^p)^{s_{r,i_{n-j}}}}{f_{v_{p,r,i_{n-j}},p}(q)^{s_{r,i_{n-j}}(1-\delta_{p,i_{n-j}})}}$$

for $1 \leq j \leq \lambda_{(\alpha)}$.

The rest of the proof is just iterations of the same argument as in Case 3 until reaching the bi-level $i_{n-(\lambda_{(\alpha)}+1)} = i_0$. The interested readers can carry out the details.

The proof of part (ii) and thus of this lemma is complete.

□

Lemma 3.26. *Let α be the maximal power of r dividing any bi-levels of EFE(1) with respect to p and r defined earlier. For each $t \in \{0, \ldots, \alpha\}$, let $\mathcal{R}_{(\alpha-t)} = \{i_j\}$ denote the collection of all bi-levels of EFE(1) with respect to p and r which consists of all bi-levels i_j occurring in EFE(1) such that the prime factorization of v_{p,r,i_j} has the form $\prod_{s \in \mathrm{P}} s^{\pi_s} p^{\lambda_j} r^{\alpha-t}$, where λ_j is some nonnegative integer and $\{\pi_s\}_{s \in \mathrm{P}}$ is some collection of positive integers depending on i_j. Then*

(1) $\mathcal{R}_{(\alpha-t)}$ *is a chain for each* $t \in \{0, \ldots, \alpha\}$.

(2) *If* $0 \leq t_1 \neq t_2 \leq \alpha$, *then*

$$\mathcal{R}_{(\alpha-t_1)} \bigcap \mathcal{R}_{(\alpha-t_2)} = \emptyset.$$

Proof. (1) If $t = 0$, then $\mathcal{R}_{(\alpha-0)} = \mathcal{R}_{(\alpha)}$ is a chain by an earlier lemma, Lemma 3.24. Let $t \in \{1, \ldots, \alpha\}$.

Claim. $\mathcal{R}_{(\alpha-t)} \neq \emptyset$ for each $t \in \{1, \ldots, \alpha\}$.

Proof of claim. As shown earlier, $\mathcal{R}_{(\alpha)} \neq \emptyset$. Thus $\mathcal{R}_{(\alpha)} = \{i_j | 0 \leq j \leq n-1, i_j > i_{j+1}\}$ for some positive integer n. Moreover, we have also shown earlier that $s_{p,i_0} = 1 = s_{r,i_0}$. Thus the reduced form of EFE(1) must contain the line

$$f^{\delta_{r,i_0}}_{v_{p,r,i_0},p}(q)\frac{f_{v_{p,r,i_0},r}(q^p)}{f_{v_{p,r,i_0},r}(q)^{(1-\delta_{p,i_0})}} \overset{(i_0)}{\longleftrightarrow} f^{\delta_{p,i_0}}_{v_{p,r,i_0},r}(q)\frac{f_{v_{p,r,i_0},p}(q^r)}{f_{v_{p,r,i_0},p}(q)^{(1-\delta_{r,i_0})}}.$$

If $\delta_{r,i_0} = 0$, i.e., r does not divide v_{p,r,i_0} or equivalently $\alpha = 0$. Thus $\emptyset \neq \mathcal{R}_{(\alpha)} = \mathcal{R}_{(0)}$ and both parts of this lemma follow immediately (part (2) is trivially true in this case). As a result, we may assume that $\delta_{r,i_0} = 1$ which means that $\alpha \geq 1$. Then line (i_0) has the form

$$f_{v_{p,r,i_0},p}(q)\frac{f_{v_{p,r,i_0},r}(q^p)}{f_{v_{p,r,i_0},r}(q)^{(1-\delta_{p,i_0})}} \overset{(i_0)}{\longleftrightarrow} f_{v_{p,r,i_0},r}(q)^{\delta_{p,i_0}} f_{v_{p,r,i_0},p}(q^r).$$

As a result, at least one of the following must be true:

(i) There exists a bi-level l of EFE(1) such that $f_{v_{p,r,i_0},p}(q)$ is semi-directly related to $f_{v_{p,r,l},p}(q)$.

(ii) There exist bi-levels $i_0 < g < l$ of EFE(1) such that $f_{v_{p,r,i_0},p}(q)$ is indirectly related to the ordered pair $(f_{v_{p,r,g},r}(q), f_{v_{p,r,l},p}(q))$.

If (i) occurs, then it can be verified from EFE(1) that $s_{p,l} = 1$ (see definition of semi-related relation) and $v_{p,r,l}r = v_{p,r,i_0}$. Hence $p^{\alpha-1} \| v_{p,r,l} = \frac{v_{p,r,i_0}}{r}$. As a result, l must be in $\mathcal{R}_{(\alpha-1)}$, which means that $\mathcal{R}_{(\alpha-1)} \neq \emptyset$. If (ii) occurs, then it can be verified directly from EFE(1), using the definition of indirectly-related relation, that either $s_{p,l} = 1$ or if $s_{p,l} = 0$, then $s_{r,g}\delta_{p,g} = 1$. This means that either $v_{p,r,l} = \frac{v_{p,r,i_0}}{r}$ or $v_{p,r,g} = \frac{v_{p,r,i_0}p}{r}$, respectively. Hence either $r^{\alpha-1} \| v_{p,r,g}$ or $r^{\alpha-1} \| v_{p,r,l}$. Therefore either g or l is in $\mathcal{R}_{(\alpha-1)}$, which means that $\mathcal{R}_{(\alpha-1)} \neq \emptyset$.

Therefore, $\mathcal{R}_{(\alpha-1)} \neq \emptyset$. If $\alpha = 1$, then part (1) is done. Thus let us suppose that $\alpha > 1$. Let l be the smallest bi-level in $\mathcal{R}_{(\alpha-1)}$. If $s_{p,l}\delta_{r,l} = 1$, then the above argument for the case of $\mathcal{R}_{(\alpha)}$ can be repeated and we have $\mathcal{R}_{(\alpha-2)} \neq \emptyset$. Otherwise, we must have either $\delta_{r,l} = 0$ or $s_{r,l} = 1$. If $\delta_{r,l} = 0$, then r does not divide $v_{p,r,l}$ or equivalently $\alpha - 1 = 0$ and we are done. Otherwise, $\alpha \geq 2$ and $s_{r,l} = 1$. Then line (l) of the reduced form of EFE(1) must have the form

$$f^{s_{p,l}\delta_{r,l}}_{v_{p,r,l},p}(q)\frac{f_{v_{p,r,l},r}(q^p)}{f_{v_{p,r,l},r}(q)^{(1-\delta_{p,l})}} \overset{(i_0)}{\longleftrightarrow} f^{\delta_{p,l}}_{v_{p,r,l},r}(q)\frac{f_{v_{p,r,l},p}(q^r)^{s_{p,l}}}{f_{v_{p,r,l},p}(q)^{s_{p,l}(1-\delta_{r,l})}}.$$

As a result, at least one of the following must hold:

(a) There exists a bi-level $g < l$ such that $s_{r,g} = 1$ and $f_{v_{p,r,g},r}(q)$ is semi-related to $f_{v_{p,r,l},r}(q)$. Thus $v_{p,r,l}p = v_{p,r,g}$.

(b) There exist bi-levels $w < g < l$ such that $s_{r,g} = 1$ and $f_{v_{p,r,g},r}(q)$ is indirectly related to the ordered pair $(f_{v_{p,r,w},p}(q), f_{v_{p,r,l},r}(q))$.

In both cases, we have $v_{p,r,l}p = v_{p,r,g}$. Hence $r^{(\alpha-2)} \| v_{p,r,g}$ which means that $g \in \mathcal{R}_{(\alpha-2)}$, contradicting the minimality of l. Thus $s_{r,l} = 0$. Therefore $\mathcal{R}_{(\alpha-2)} \neq \emptyset$. This argument can be iterated and we have $\mathcal{R}_{(\alpha-t)} \neq \emptyset$ for all $t \in \{1, \dots, \alpha\}$.

□

The rest of the verification showing that $\mathcal{R}_{(\alpha-t)}$ is a chain for each $t \in \{1, \dots, \alpha\}$ is immediate from their definition given in the lemma.

Remark 3.27. Though it is not necessary for our proof of Theorem 2.1, it is true that $s_{p,i_j} = 1$ for at least one i_j in each $\mathcal{R}_{(\alpha-t)}$, where $0 \leq t \leq \alpha$ (the same method found in the proof above can be used to prove this).

(2) This also follows immediately from the definition of $\mathcal{R}_{(\alpha-t)}$.

□

As a result of our work up to this point, Theorem 2.1 follows from the next lemma.

Lemma 3.28. *Let* R *be the collection of all bi-levels of EFE*(1) *with respect to* p *and* r. *Then*

$$\mathrm{R} = \bigsqcup_t \mathcal{R}_{(\alpha-t)},$$

where α *is the maximal power of* r *dividing any bi-level of EFE*(1) *and* $\bigsqcup$ *denotes a disjoint union.*

Proof. Let i be any bi-level of EFE(1) with respect to p and r. Then it has been proven earlier that the prime factorization of $v_{p,r,i}$ has the form $\prod_{s\in \mathrm{P}} s^{\pi_s} p^{\lambda_j} r^{\alpha-t}$, where $0 \leq \lambda_j \leq \lambda$ and $t \in \{0, \dots, \alpha\}$. Then $i \in \mathcal{R}_{(\alpha-t)}$ by definition of $\mathcal{R}_{(\alpha-t)}$. Thus the result follows immediately from the previous lemma.

□

Lemma 3.29. *For each $\beta \in \{1, \ldots, \alpha - 1\}$, let $\mathcal{R}_{(\beta)}$ be the corresponding chain of EFE(1) with respect to p and r defined earlier. Then*

$$\sum_{i \in \mathcal{R}_\beta} deg\big(f_{v_{p,r,i},p}(q)^{s_{p,j}}\big) = d_{(\beta)}(p-1)$$

for some integer $d_{(\beta)}$.

P r o o f. Let α and $\lambda_{(\alpha)}$ be as before and $\lambda_{(\alpha-1)}$ be defined similarly with $\alpha - 1$ replacing α. From Lemma 3.24, we have

$$deg\left(\prod_{1 \leq j \leq \lambda_{(\alpha)}} f_{v_{p,r,i_{n_{(\beta)}-j}},p}(q)^{s_{p,i_{n_{(\beta)}-j}}}\right) = t(p-1)$$

for some integer t. In the rest of the proof of this lemma, we denote $n_{(\alpha-1)}$ denotes the number n in $\mathcal{R}_{(\alpha-1)} = \{i_j | 0 \leq j \leq n-1\}$. Thus $n_{(\alpha-1)} = \lambda_{(\alpha-1)} + 1$. Contrary to the case of $\mathcal{R}_{(\alpha)}$, it can be verified from EFE(1) that in the case of $\mathcal{R}_{(\alpha-1)}$, the following equalities **need not** hold

$$f_{v_{p,r,i_0},r}(q^p) = f_{v_{p,r,i_{n_{(\alpha-1)}-(\lambda_{(\alpha-1)}+1)}},r}(q^p) =$$

$$= \frac{f_{v_{p,r,i_{n_{(\alpha-1)}-(\lambda_{(\alpha-1)}+1)}},p}(q^r) s_{p,i_{n-(\lambda_{(\alpha-1)}+1)}}}{f_{v_{p,r,i_{n_{(\alpha-1)}-(\lambda_{(\alpha-1)}+1)}},p}(q)^{s_{p,i_{n_{(\alpha-1)}-(\lambda_{(\alpha-1)}+1)}}(1-\delta_{r,i_{n_{(\alpha-1)}-(\lambda_{(\alpha-1)}+1)}})}} =$$

$$= \frac{f_{v_{p,r,i_0},p}(q^r)}{f_{v_{p,r,i_0},p}(q)^{(1-\delta_{r,i_0})}},$$

$$\prod_{1 \leq j \leq \lambda_0 + 1} \frac{f_{v_{p,r,i_{n-j}},p}(q^r)^{s_{p,i_{n-j}}}}{f_{v_{p,r,i_{n-j}},p}(q)^{s_{p,i_{n-j}}(1-\delta_{r,i_{n-j}})}} =$$

$$= f_{v_{p,r,i_{n-(\lambda_0+1)}},r}(q^p) \prod_{1 \leq j \leq \lambda_0} \frac{f_{v_{p,r,i_{n-j}},p}(q^r)^{s_{p,i_{n-j}}}}{f_{v_{p,r,i_{n-j}},p}(q)^{s_{p,i_{n-j}}(1-\delta_{r,i_{n-j}})}}$$

and

$$\frac{f_{v_{p,r,i_{n-j}},r}(q^p)^{s_{r,i_{n-j}}}}{f_{v_{p,r,i_{n-j}},r}(q)^{s_{r,i_{n-j}}(1-\delta_{p,i_{n-j}})}} = f_{v_{p,r,i_{n-(j+1)}},r}(q)^{s_{r,i_{n-(j+1)}}(\delta_{p,i_{n-(j+1)}})}.$$

$$\cdot \frac{f_{v_{p,r,i_{n-j}},p}(q^p)^{s_{r,i_{n-j}}}}{f_{v_{p,r,i_{n-j}},p}(q)^{s_{r,i_{n-j}}(1-\delta_{p,i_{n-j}})}}$$

for $1 \leq j \leq \lambda_{(\alpha-1)}$. Therefore, some modifications to the previous method is needed.

Let us consider all lines (i) of the reduced form of EFE(1), where $i \in \mathcal{R}_{(\alpha-1)} = \{i_j | 0 \leq j \leq n_{(\alpha-1)} - 1; i_j < i_{j+1}\}$ for some positive integer $n_{(\alpha-1)}$:

$$\cdots$$

$$f_{v_{p,r,i_0},p}^{s_{p,i_0}\delta_{r,i_0}}(q)\frac{f_{v_{p,r,i_0},r}^{s_{r,i_0}}(q^p)}{f_{v_{p,r,i_0},r}^{s_{r,i_0}(1-\delta_{p,i_0})}(q)} \overset{(i_0)}{\longleftrightarrow}$$

$$f_{v_{p,r,i_0},r}^{s_{r,i_0}\delta_{p,i_0}}(q)\frac{f_{v_{p,r,i_0},p}^{s_{p,i_0}}(q^r)}{f_{v_{p,r,i_0},p}^{s_{p,i_0}(1-\delta_{r,i_0})}(q)}$$

$$\cdots$$

$$f_{v_{p,r,i_{n_{(\alpha-1)}-1}},p}^{s_{p,i_{n_{(\alpha-1)}-1}}\delta_{r,i_0}}(q)\frac{f_{v_{p,r,i_{n_{(\alpha-1)}-1}},r}^{s_{r,i_{n_{(\alpha-1)}-1}}}(q^p)}{f_{v_{p,r,i_{n-1}},r}^{s_{r,i_{n_{(\alpha-1)}-1}}(1-\delta_{p,i_{n_{(\alpha-1)}-1}})}(q)} \overset{(i_{n_{(\alpha-1)}-1})}{\longleftrightarrow}$$

$$f_{v_{p,r,i_{n_{(\alpha-1)}-1}},r}^{s_{r,i_{n_{(\alpha-1)}-1}}\delta_{p,i_{n_{(\alpha-1)}-1}}}(q)\frac{f_{v_{p,r,i_{n_{(\alpha-1)}-1}},p}^{s_{p,i_{n_{(\alpha-1)}-1}}}(q^r)}{f_{v_{p,r,i_{n_{(\alpha-1)}-1}},p}^{s_{p,i_{n_{(\alpha-1)}-1}}(1-\delta_{r,i_{n_{(\alpha-1)}-1}})}(q)}$$

$$\cdots$$

It can be verified that if $s_{p,i_j}\delta_{p,i_j} = 1$ for some $i_j \in \mathcal{R}_{(\alpha)}$, then $f_{v_{p,r,i_j},p}(q)$ is either directly related to $f_{v_{p,r,g},r}(q)$ or semi-related to $f_{v_{p,r,l},p}(q)$, or indirectly related to the ordered pair $(f_{v_{p,r,g},r}(q), f_{v_{p,r,l},p}(q))$, where g and l are bi-levels in $\mathcal{R}_{(\alpha-1)}$ (note that they can not be directly related). As a result, we have

$$\left(\prod_{i_j\in\mathcal{R}_{(\alpha)}} f_{v_{p,r,i_j},p}(q)^{s_{p,i_j}\delta_{p,i_j}}\right)\Bigg|\left(\prod_{i_j\in\mathcal{R}_{(\alpha-1)}} f_{v_{p,r,i_j},r}(q)^{s_{r,i_j}\delta_{p,i_j}}\frac{f_{v_{p,r,i_j},p}^{s_{s,i_j}}(q^r)}{f_{v_{p,r,i_j},p}^{s_{s,i_j}(1-\delta_{r,i_j})}(q)}\right).$$

Then the collection of lines (i_j), where $i_j \in \mathcal{R}_{(\alpha-1)}$ in the EFE(1) can be written as

$$\cdots$$

$$f_{v_{p,r,i_0},p}^{s_{p,i_0}\delta_{r,i_0}}(q)\frac{F_{v_{p,r,i_0},r}^{s_{r,i_0}}(q^p)}{F_{v_{p,r,i_0},r}^{s_{r,i_0}(1-\delta_{p,i_0})}(q)}H_{v_{p,r,i_0},r}^{s_{r,i_0}}(q) \overset{(i_0)}{\longleftrightarrow}$$

$$F_{v_{p,r,i_0},r}^{s_{r,i_0}\delta_{p,i_0}}(q)G_{v_{p,r,i_0},r}^{s_{r,i_0}\delta_{p,i_0}}(q)\frac{F_{v_{p,r,i_0}r,p}^{s_{p,i_0}}(q)}{f_{v_{p,r,i_0},p}^{s_{p,i_0}(1-\delta_{r,i_0})}(q)}G_{v_{p,r,i_0},p}^{s_{p,i_0}}(q)$$

$$\cdots$$

$$f_{v_{p,r,i_j},p}^{s_{p,i_j}\delta_{r,i_j}}(q)\frac{F_{v_{p,r,i_j},r}^{s_{r,i_j}}(q^p)}{F_{v_{p,r,i_j},r}^{s_{r,i_j}(1-\delta_{p,i_j})}(q)}H_{v_{p,r,i_j},r}^{s_{r,i_j}}(q) \overset{(i_j)}{\longleftrightarrow}$$

$$F^{s_{r,i_j}\delta_{p,i_j}}_{v_{p,r,i_j},r}(q)G^{s_{r,i_j}\delta_{p,i_j}}_{v_{p,r,i_j},r}(q)\frac{F^{s_{p,i_j}}_{v_{p,r,i_j}r,p}(q)}{f^{s_{p,i_j}(1-\delta_{r,i_j})}_{v_{p,r,i_j},p}(q)}G^{s_{p,i_j}}_{v_{p,r,i_j},p}(q)$$

$$\cdots$$

$$f^{s_{p,i_{n_{(\alpha-1)}-1}}\delta_{r,i_{n_{(\alpha-1)}-1}}}_{v_{p,r,i_{n_{(\alpha-1)}-1}},p}(q)\frac{F^{s_{r,i_{n_{(\alpha-1)}-1}}}_{v_{p,r,i_{n_{(\alpha-1)}-1}},r}(q^p)}{F^{s_{r,i_{n_{(\alpha-1)}-1}}(1-\delta_{p,i_{n_{(\alpha-1)}-1}})}_{v_{p,r,i_{n_{(\alpha-1)}-1}},r}(q)}H^{s_{r,i_{n_{(\alpha-1)}-1}}}_{v_{p,r,i_{n_{(\alpha-1)}-1}},r}(q)$$

$$\overset{(i_{n_{(\alpha-1)}-1})}{\longleftrightarrow}$$

$$F^{s_{r,i_{n_{(\alpha-1)}-1}}\delta_{p,i_{n_{(\alpha-1)}-1}}}_{v_{p,r,i_{n_{(\alpha-1)}-1}},r}(q)G^{s_{r,i_{n_{(\alpha-1)}-1}}\delta_{p,i_{n_{(\alpha-1)}-1}}}_{v_{p,r,i_{n_{(\alpha-1)}-1}},r}(q)\frac{F^{s_{p,i_{n_{(\alpha-1)}-1}}}_{v_{p,r,i_{n_{(\alpha-1)}-1}}r,p}(q)}{f^{s_{p,i_{n-1}}(1-\delta_{r,i_{n_{(\alpha-1)}-1}})}_{v_{p,r,i_{n_{(\alpha-1)}-1}},p}(q)}$$

$$G^{s_{p,i_{n_{(\alpha-1)}-1}}}_{v_{p,r,i_{n_{(\alpha-1)}-1}},p}(q)$$

$$\cdots$$

where $i_0 \geq i_j \geq i_{n_{(\alpha-1)}-1} \in \mathcal{R}_{(\alpha-1)}$ and for all such i_j:

- $F^{s_{r,i_j}\delta_{p,i_j}}_{v_{p,r,i_j},r}(q)G^{s_{r,i_j}\delta_{p,i_j}}_{v_{p,r,i_j},r}(q) = f^{s_{r,i_j}\delta_{p,i_j}}_{v_{p,r,i_j},r}(q)$ such that:

$$\left(f^{s_{r,i_j}\delta_{p,i_j}}_{v_{p,r,i_j},r}(q), \prod_{i_j\in\mathcal{R}_{(\alpha)}} f_{v_{p,r,i_j},p}(q)^{s_{p,i_j}\delta_{p,i_j}}\right) = G^{s_{r,i_j}\delta_{p,i_j}}_{v_{p,r,i_j},r}(q)$$

  with $(*,*)$ denoting the greatest common divisor operator in $\mathbb{C}[q]$.

- $\frac{F^{s_{p,i_j}}_{v_{p,r,i_j}r,p}(q)}{f^{s_{p,i_j}(1-\delta_{r,i_j})}_{v_{p,r,i_j},p}(q)}G^{s_{p,i_j}}_{v_{p,r,i_j},p}(q) = \frac{f^{s_{p,i_j}}_{v_{p,r,i_j},p}(q^r)}{f^{s_{p,i_j}(1-\delta_{r,i_j})}_{v_{p,r,i_j},p}(q)}$ such that :

$$\left(\frac{f^{s_{p,i_j}}_{v_{p,r,i_j},p}(q^r)}{f^{s_{p,i_j}(1-\delta_{r,i_j})}_{v_{p,r,i_j},p}(q)}, \prod_{i_j\in\mathcal{R}_{(\alpha)}} f_{v_{p,r,i_j},p}(q)^{s_{p,i_j}\delta_{p,i_j}}\right) = G^{s_{p,i_j}}_{v_{p,r,i_j},p}(q)$$

- $\frac{F^{s_{r,i_j}}_{v_{p,r,i_j},r}(q^p)}{F^{s_{r,i_j}(1-\delta_{p,i_j})}_{v_{p,r,i_j},r}(q)}H^{s_{r,i_j}}_{v_{p,r,i_j},r}(q) = \frac{f^{s_{r,i_j}}_{v_{p,r,i_j},r}(q^p)}{f^{s_{r,i_j}(1-\delta_{p,i_j})}_{v_{p,r,i_j},r}(q)}$ such that:

$$\left(\frac{F^{s_{r,i_j}}_{v_{p,r,i_j},r}(q^p)}{f^{s_{r,i_j}(1-\delta_{p,i_j})}_{v_{p,r,i_j},r}(q)}, \prod_{i_j\in\mathcal{R}_{(\alpha)}} f_{v_{p,r,i_j},p}(q)^{s_{p,i_j}\delta_{p,i_j}}\right) = H^{s_{r,i_j}}_{v_{p,r,i_j},r}(q)$$

  and

$$H^{s_{r,i_j}}_{v_{p,r,i_j},r}(q) = \frac{G^{s_{r,i_j}}_{v_{p,r,i_j},r}(q^p)}{G^{s_{r,i_j}(1-\delta_{p,i_j})}_{v_{p,r,i_j},r}(q)}.$$

As a result, it can be verified from above that

$$\frac{F^{s_{r,i_0}}_{v_{p,r,i_0},r}(q^p)}{F^{s_{r,i_0}(1-\delta_{p,i_0})}_{v_{p,r,i_0},r}(q)} H^{s_{r,i_0}}_{v_{p,r,i_0},r}(q) =$$

$$\frac{F^{s_{r,i_{n_{\alpha-1}-(\lambda_{(\alpha-1)}+1)}}}_{v_{p,r,i_{n_{\alpha-1}-(\lambda_{(\alpha-1)}+1)}},r}(q^p)}{F^{s_{r,i_0}(1-\delta_{p,i_0})}_{v_{p,r,i_0},r}(q)} H^{s_{r,i_{n_{\alpha-1}-(\lambda_{(\alpha-1)}+1)}}}_{v_{p,r,i_{n_{\alpha-1}-(\lambda_{(\alpha-1)}+1)}},r}(q) =$$

$$\frac{F^{s_{p,i_{n_{\alpha-1}-(\lambda_{(\alpha-1)}+1)}}}_{v_{p,r,i_{n_{\alpha-1}-(\lambda_{(\alpha-1)}+1)}}r,p}(q)}{f^{s_{p,i_{n_{\alpha-1}-(\lambda_{(\alpha-1)}+1)}}(1-\delta_{r,i_{n_{\alpha-1}-(\lambda_{(\alpha-1)}+1)}})}_{v_{p,r,i_{n_{\alpha-1}-(\lambda_{(\alpha-1)}+1)}},p}(q)} = \frac{F^{s_{p,i_0}}_{v_{p,r,i_0}r,p}(q)}{f^{s_{p,i_0}(1-\delta_{r,i_0})}_{v_{p,r,i_0},p}(q)},$$

$$\frac{F^{s_{r,i_{j+1}}}_{v_{p,r,i_{j+1}},r}(q^p)}{F^{s_{r,i_{j+1}}(1-\delta_{p,i_{j+1}})}_{v_{p,r,i_{j+1}},r}(q)} H^{s_{r,i_{j+1}}}_{v_{p,r,i_{j+1}},r}(q) = F^{s_{r,i_j}\delta_{p,i_j}}_{v_{p,r,i_j},r}(q) \frac{F^{s_{p,i_{j+1}}}_{v_{p,r,i_{j+1}}r,p}(q)}{f^{s_{p,i_{j+1}}(1-\delta_{r,i_{j+1}})}_{v_{p,r,i_{j+1}},p}(q)}$$

for $0 \leq j \leq n_{(\alpha-1)} - 2$ and

$$\prod_{0\leq j\leq n_{(\alpha-1)}-1} \frac{f^{s_{r,i_j}}_{v_{p,r,i_j},r}(q^p)}{f^{s_{r,i_j}(1-\delta_{p,i_j})}_{v_{p,r,i_j},r}(q)} = \prod_{0\leq j\leq n_{(\alpha-1)}-1} \frac{F^{s_{p,i_j}}_{v_{p,r,i_j}r,p}(q)}{f^{s_{p,i_j}(1-\delta_{r,i_j})}_{v_{p,r,i_j},p}(q)} G^{s_{p,i_j}}_{v_{p,r,i_j},p}(q)$$

$$= \frac{F^{s_{r,i_0}}_{v_{p,r,i_0},r}(q^p)}{F^{s_{r,i_0}(1-\delta_{p,i_0})}_{v_{p,r,i_0},r}(q)} H^{s_{r,i_0}}_{v_{p,r,i_0},r}(q) G^{s_{p,i_0}}_{v_{p,r,i_0},p}(q)$$

$$\prod_{1\leq j\leq n_{(\alpha-1)}-1} \frac{F^{s_{p,i_j}}_{v_{p,r,i_j}r,p}(q)}{f^{s_{p,i_j}(1-\delta_{r,i_j})}_{v_{p,r,i_j},p}(q)} G^{s_{p,i_j}}_{v_{p,r,i_j},p}(q).$$

Furthermore, we also have

$$\prod_{i_j\in\mathcal{R}_{(\alpha)}} f_{v_{p,r,i_j},p}(q)^{s_{p,i_j}\delta_{p,i_j}} = \prod_{i_j\in\mathcal{R}_{(\alpha-1)}} G^{s_{r,i_j}\delta_{p,i_j}}_{v_{p,r,i_j},r}(q) G^{s_{p,i_j}}_{v_{p,r,i_j},p}(q).$$

Hence

$$t(p-1) = deg\left(\prod_{i_j\in\mathcal{R}_{(\alpha)}} f_{v_{p,r,i_j},p}(q)^{s_{p,i_j}\delta_{p,i_j}}\right) =$$

$$deg\left(\prod_{i_j\in\mathcal{R}_{(\alpha-1)}} G^{s_{r,i_j}\delta_{p,i_j}}_{v_{p,r,i_j},r}(q) G^{s_{p,i_j}}_{v_{p,r,i_j},p}(q)\right)$$

for some integer t.

Claim. $\deg(\prod_{i_j\in\mathcal{R}_{(\alpha-1)}} f^{s_{p,i_j}}_{v_{p,r,i_j},p}(q)) = w(p-1)$ for some integer w.

Proof of claim. Let $v_{p,r,i_{n_{(\alpha-1)-1}}}r = p^{m_{i_{n_{(\alpha-1)-1}}}} \prod_i p_i^{e_{p,r,i_{n_{(\alpha-1)-1}}r,i}}$ be the prime factorization of $v_{p,r,i_{n_{(\alpha-1)-1}}}$ (note that $m_{i_{n_{(\alpha)-1}}} = 0$ but $m_{i_{n_{(\alpha-t)-1}}}$ may be positive for $t \in \{1, \ldots, \alpha\}$). By the analysis in [4], the collection of all roots of the polynomial $G^{s_{r,i_{n_{(\alpha-1)-1}}}\delta_{p,i_{n_{(\alpha-1)-1}}}}_{v_{p,r,i_{n_{(\alpha-1)-1}}},r}(q)$ can be represented by the collection of tuples of the form

$$\bigcup_{(\alpha_i)_i \in \mathcal{B}_{G^{s_{r,i_{n_{(\alpha-1)-1}}}\delta_{p,i_{n_{(\alpha-1)-1}}}}_{v_{p,r,i_{n_{(\alpha-1)-1}}},r}(q)} \preceq (\mathbb{Z}/p_i^{e_{p,r,i_{n_{(\alpha-1)-1}}r,i}}\mathbb{Z})^*} \mathcal{A}_{((\alpha_i)_i, i_{n_{(\alpha-1)-1}})} \times (\alpha_i)_i$$

where $\mathcal{B}_{G^{s_{r,i_{n_{(\alpha-1)-1}}}\delta_{p,i_{n_{(\alpha-1)-1}}}}_{v_{p,r,i_{n_{(\alpha-1)-1}}},r}(q)}$ is a collection of tuples determined by the polynomial $G^{s_{r,i_{n_{(\alpha-1)-1}}}\delta_{p,i_{n_{(\alpha-1)-1}}}}_{v_{p,r,i_{n_{(\alpha-1)-1}}},r}(q)$ and $\mathcal{A}_{((\alpha_i)_i, i_{n_{(\alpha-1)-1}})} \subseteq (\mathbb{Z}/p^{m_{i_{n_{(\alpha-1)-1}}}}\mathbb{Z})^*$. Therefore, the collection of all roots of $H^{s_{r,i_j}}_{v_{p,r,i_j},r}(q)$ is representable as the set of tuples of the form

$$\bigcup_{(\alpha_i)_i \in \mathcal{B}_{G^{s_{r,i_{n_{(\alpha-1)-1}}}\delta_{p,i_{n_{(\alpha-1)-1}}}}_{v_{p,r,i_{n_{(\alpha-1)-1}}},r}(q)} \preceq (\mathbb{Z}/p_i^{e_{p,r,i_{n_{(\alpha-1)-1}}r,i}}\mathbb{Z})^*} \mathbf{A}_{((\alpha_i)_i, i_{n_{(\alpha-1)-1}})}$$

where

$$\mathbf{A}_{((\alpha_i)_i, i_{n_{(\alpha-1)-1}})} = \left(\mathcal{A}_{((\alpha_i)_i, i_{n_{(\alpha-1)-1}})} + z(p^{m_{i_{n_{(\alpha-1)-1}}}})\right)_{\{0 \le z \le p-1\}} \times (\alpha_i)_i$$

which can be rewritten as

$$\left(\bigcup_{(\alpha_i)_i \in \mathcal{B}_{G^{s_{r,i_{n_{(\alpha-1)-1}}}\delta_{p,i_{n_{(\alpha-1)-1}}}}_{v_{p,r,i_{n_{(\alpha-1)-1}}},r}(q)} \preceq (\mathbb{Z}/p_i^{e_{p,r,i_{n_{(\alpha-1)-1}}r,i}}\mathbb{Z})^*} \mathbf{A}_{((\alpha_i)_i, i_{n_{(\alpha-1)-1}}),1}\right) \bigcup$$

$$\left(\bigcup_{(\alpha_i)_i \in \mathcal{B}_{G^{s_{r,i_{n_{(\alpha-1)-1}}}\delta_{p,i_{n_{(\alpha-1)-1}}}}_{v_{p,r,i_{n_{(\alpha-1)-1}}},r}(q)} \preceq (\mathbb{Z}/p_i^{e_{p,r,i_{n_{(\alpha-1)-1}}r,i}}\mathbb{Z})^*} \mathbf{A}_{((\alpha_i)_i, i_{n_{(\alpha-1)-1}}),2}\right)$$

where

$$\mathbf{A}_{((\alpha_i)_i, i_{n_{(\alpha-1)-1}}),1} = \left(\mathcal{A}_{((\alpha_i)_i, i_{n_{(\alpha-1)-1}})} + z(p^{m_{i_{n_{(\alpha-1)-1}}}})\right)_{\{1 \le z \le p-1\}} \times (\alpha_i)_i$$

and

$$\mathbf{A}_{((\alpha_i)_i, i_{n_{(\alpha-1)}-1}),2} = \mathcal{A}_{((\alpha_i)_i, i_{n_{(\alpha-1)}-1})} \times (\alpha_i)_i$$

where

$$\left| \bigcup_{(\alpha_i)_i \in \mathcal{B}_{G^{s_{r,i_{n_{(\alpha-1)}-1}} \delta_{p,i_{n_{(\alpha-1)}-1}}}_{v_{p,r,i_{n_{(\alpha-1)}-1}},r}(q)} \preceq (\mathbb{Z}/p_i^{e_{p,r,i_{n_{(\alpha-1)}-1}}{}^{r,i}}\mathbb{Z})^*} \mathbf{A}_{((\alpha_i)_i, i_{n_{(\alpha-1)}-1}),1} \right| =$$

$$= s(p-1)$$

for some integer s and the collection

$$\bigcup_{(\alpha_i)_i \in \mathcal{B}_{G^{s_{r,i_{n_{(\alpha-1)}-1}} \delta_{p,i_{n_{(\alpha-1)}-1}}}_{v_{p,r,i_{n_{(\alpha-1)}-1}},r}(q)} \preceq (\mathbb{Z}/p_i^{e_{p,r,i_{n_{(\alpha-1)}-1}}{}^{r,i}}\mathbb{Z})^*} \mathbf{A}_{((\alpha_i)_i, i_{n_{(\alpha-1)}-1}),2}$$

can be identified in the obvious way with the collection of tuples representing the collection of all roots of $G^{s_{r,i_{n_{(\alpha-1)}-1}} \delta_{p,i_{n-1}}}_{v_{p,r,i_{n-1}},r}(q)$ given above. By a similar argument, it can also be verified that, for each j such that $1_0 \leq i_j \leq i_{n_{(\alpha-1)}-1} \in \mathcal{R}_{(\alpha-1)}$, the collection of tuples of the form

$$\bigcup_{(\alpha_i)_i \in \mathcal{B}_{G^{s_{r,i_j} \delta_{p,i_j}}_{v_{p,r,i_j},r}(q)} \preceq (\mathbb{Z}/p_i^{e_{p,r,i_{n_{(\alpha-1)}-1}}{}^{r,i}}\mathbb{Z})^*} \mathcal{A}_{((\alpha_i)_i, i_j)} \times (\alpha_i)_i$$

where $\mathcal{B}_{G^{s_{r,i_j} \delta_{p,i_j}}_{v_{p,r,i_j},r}(q)}$ is a collection of tuples which is determined by the polynomial $G^{s_{r,i_j} \delta_{p,i_j}}_{v_{p,r,i_j},r}(q)$ and $\mathcal{A}_{((\alpha_i)_i, i_j)} \subseteq (\mathbb{Z}/p^{m_{i_j}}\mathbb{Z})^*$ where $p^{m_{i_j}} \| v_{p,r,i_j}$. Therefore, the collection of all roots of $H^{s_{r,i_j}}_{v_{p,r,i_j},r}(q)$ is representable as the set of tuples of the form

$$\bigcup_{(\alpha_i)_i \in \mathcal{B}_{G^{s_{r,i_j} \delta_{p,i_j}}_{v_{p,r,i_j},r}(q)} \preceq (\mathbb{Z}/p_i^{e_{p,r,i_{n_{(\alpha-1)}-1}}{}^{r,i}}\mathbb{Z})^*} \mathbf{A}_{((\alpha_i)_i, i_j)}$$

where

$$\mathbf{A}_{((\alpha_i)_i, i_j)} = \left(\mathcal{A}_{((\alpha_i)_i, i_j)} + z(p^{m_{i_j}})\right)_{\{0 \leq z \leq p-1\}} \times (\alpha_i)_i,$$

which can be rewritten as

$$\left(\bigcup_{(\alpha_i)_i \in \mathcal{B}_{G^{s_{r,i_j} \delta_{p,i_j}}_{v_{p,r,i_j},r}(q)} \preceq (\mathbb{Z}/p_i^{e_{p,r,i_{n_{(\alpha-1)}-1}}{}^{r,i}}\mathbb{Z})^*} \mathbf{A}_{((\alpha_i)_i, i_j),1} \right) \bigcup$$

$$\left(\bigcup_{(\alpha_i)_i \in \mathcal{B}_{G^{s_{r,i_j}\delta_{p,i_j}}_{v_{p,r,i_j},r}(q)} \preceq (\mathbb{Z}/p_i^{e_{p,r,i_{n_{(\alpha-1)}-1}}{}^{r,i}}\mathbb{Z})^*} \mathbf{A}_{((\alpha_i)_i,i_j),2} \right)$$

where

$$\mathbf{A}_{((\alpha_i)_i,i_j),1} = \left(\mathcal{A}_{((\alpha_i)_i,i_j)} + z(p^{m_{i_j}})\right)_{\{1 \le z \le p-1\}} \times (\alpha_i)_i$$

and

$$\mathbf{A}_{((\alpha_i)_i,i_j),2} = \mathcal{A}_{((\alpha_i)_i,i_j)} \times (\alpha_i)_i$$

where

$$\left| \bigcup_{(\alpha_i)_i \in \mathcal{B}_{G^{s_{r,i_j}\delta_{p,i_j}}_{v_{p,r,i_j},r}(q)} \preceq (\mathbb{Z}/p_i^{e_{p,r,i_{n_{(\alpha-1)}-1}}{}^{r,i}}\mathbb{Z})^*} \mathbf{A}_{((\alpha_i)_i,i_j),1} \right| = t(p-1)$$

for some integer t and the collection

$$\bigcup_{(\alpha_i)_i \in \mathcal{B}_{G^{s_{r,i_j}\delta_{p,i_j}}_{v_{p,r,i_j},r}(q)} \preceq (\mathbb{Z}/p_i^{e_{p,r,i_{n_{(\alpha-1)}-1}}{}^{r,i}}\mathbb{Z})^*} \mathbf{A}_{((\alpha_i)_i,i_j),2}$$

can be identified in the obvious way with the collection of tuples representing the collection of all roots of $G^{s_{r,i_j}\delta_{p,i_j}}_{v_{p,r,i_j},r}(q)$ given above.

Let us remark that it can be verified that we must have

$$F^{s_{r,i_{n_{(\alpha-1)}-1}}\delta_{p,i_{n_{(\alpha-1)}-1}}}_{v_{p,r,i_{n_{(\alpha-1)}-1}},r}(q) = 1$$

in this case. Therefore, there are two possibilities:

- $\delta_{p,i_{n_{(\alpha-1)}-1}} = 0$, i.e. p does not divide $v_{p,r,i_{n_{(\alpha-1)}-1}}$.
- $f^{s_{r,i_{n_{(\alpha-1)}-1}}\delta_{p,i_{n_{(\alpha-1)}-1}}}_{v_{p,r,i_{n_{(\alpha-1)}-1}},r}(q) = G^{s_{r,i_{n_{(\alpha-1)}-1}}\delta_{p,i_{n_{(\alpha-1)}-1}}}_{v_{p,r,i_{n_{(\alpha-1)}-1}},r}(q)$.

The difference between this case (as well as all the cases where $\mathcal{R}_{(\alpha-t)}$ for $t \ge 1$) and the case of $\mathcal{R}_{(\alpha)}$ is that the latter possibility may occur, which means that p may divide $i_{n_{\alpha-1}-1}$. If the first case occurs, then we must have

$$G^{s_{r,i_{n_{(\alpha-1)}-1}}\delta_{p,i_{n_{(\alpha-1)}-1}}}_{v_{p,r,i_{n_{(\alpha-1)}-1}},r}(q) = 1,$$

and hence we may proceed as in the case of $\mathcal{R}_{(\alpha)}$. It can be verified from above that there must exist at least one $i_j \in \mathcal{R}_{(\alpha-1)}$ such that

$$G^{s_{r,i_j}\delta_{p,i_j}}_{v_{p,r,i_j},r}(q) \ne 1.$$

However, the modification of the lines $i_j \in \mathcal{R}_{(\alpha-1)}$ in EFE(1) with respect to p and r given earlier together with the above identification provides exactly what is needed for the method to work (the readers should verify this). If the second case occurs, then the above identification also allows us to use the same method as in the case of $\mathcal{R}_{(\alpha)}$ (note that the above identification should be taken into account throughout the process).

By applying the above modification of the method employed in the case of $\mathcal{R}_{(\alpha)}$ to this case, $\mathcal{R}_{(\alpha-1)}$, we have

$$deg\left(\prod_{i_j\in\mathcal{R}_{(\alpha-1)}} f_{v_{p,r,i_j},p}(q^r)^{s_{p,i_j}\delta_{r,i_j}}\right) = \sum_{i_j\in\mathcal{R}_{(\alpha-1)}} deg\left(f_{v_{p,r,i_j},p}(q^r)^{s_{p,i_j}\delta_{r,i_j}}\right) =$$
$$= t(p-1)$$

for some integer t. Also using the method in the case of $\mathcal{R}_{(\alpha)}$, we have from the above that

$$deg\left(\prod_{i_j\in\mathcal{R}_{(\alpha-1)}} f_{v_{p,r,i_j},p}(q)^{s_{p,i_j}\delta_{r,i_j}}\right) = \sum_{i_j\in\mathcal{R}_{(\alpha-1)}} deg\left(f_{v_{p,r,i_j},p}(q)^{s_{p,i_j}\delta_{r,i_j}}\right) = s(p-1)$$

for some integer s as desired. □

By using the known fact from above that

$$\sum_{i_j\in\mathcal{R}_{(\alpha-1)}} deg(f_{v_{p,r,i_j},p}(q)^{s_{p,i_j}\delta_{r,i_j}}) = s(p-1)$$

for some integer s, the same method applies to the case of $\mathcal{R}_{(\alpha-2)}$ giving

$$deg(\prod_{i_j\in\mathcal{R}_{(\alpha-2)}} f_{v_{p,r,i_j},p}(q)^{s_{p,i_j}\delta_{r,i_j}}) = \sum_{i_j\in\mathcal{R}_{(\alpha-2)}} deg(f_{v_{p,r,i_j},p}(q)^{s_{p,i_j}\delta_{r,i_j}}) = v(p-1)$$

for some integer v. This method can then be iterated for each successive $t \in \{0, \ldots, \alpha\}$. Therefore for each $t \in \{0, \ldots, \alpha\}$, we have

$$\sum_{i_j\in\mathcal{R}_{(\alpha-t)}} deg(f_{v_{p,r,i_j},p}(q)^{s_{p,i_j}\delta_{r,i_j}}) = d_{(t)}(p-1)$$

for some integer $d_{(t)}$. Thus the claim is established and the proof of the lemma is complete.

□

By combining all the above lemmas, we have the proof of Key Proposition 4.
□

The following proposition completes the proof of Theorem 2.1:

Proposition 3.30. *Let Γ be a sequence of polynomials satisfying the hypothesis of Theorem 2.1. Let P be the set of primes associated to the support of Γ. Let $\Gamma^{\partial}_{|P|} := \{f_{p_i}^{(2_{p_1,p_{|P|}})} | 1 \leq i \leq |P|\}$ be the sequence of polynomials generated by the algorithm constructed earlier where*

- *$i \leq |P|$ is replaced by $i < |P|$ if $|P| = \infty$, and*
- *If $|P| = \infty$ and if $l \geq g$, then $f_{p_l}^{(2_{p_1,p_{|P|}})}(q)$ is defined to be $f_{p_g}^{(2_{p_1,p_g})}(q)$ but with p_l replacing p_g where g is the integer defined in Proposition 3.10.*

Then

(1) If $|P| = \infty$, then $\underset{z\to\infty}{lim}\, \Gamma^{\partial}_z = \Gamma^{\partial}_{|P|}$ where the limit is defined as follows: $\underset{z\to\infty}{lim}\, \Gamma^{\partial}_z = \Gamma^{\partial}_{|P|}$ if for any positive integer n, there exist a sequence of integer $z = g = z_1 < z_2 \ldots < z_n$ such that $\Gamma^{\partial}_{z_1} \subseteq \ldots \subseteq \Gamma^{\partial}_{z_n} \subseteq \Gamma^{\partial}_{|P|}$ where g is the integer mentioned in above.

(2) Key Proposition 2 holds if Γ^{∂}_z is replaced by $\Gamma^{\partial}_{|P|}$.

(3) The sequence $\Gamma^{\partial}_{|P|}$ satisfies Functional Equation (1) and induces the required sequence Γ' of Theorem 2.1. Moreover, Γ' is the unique such sequence with $t_{\Gamma'} - t_{\Gamma}$ minimal.

Proof. If $|P|$ is finite, then most of this corollary is just Key Proposition 2 and Key Proposition 4. The only thing left is Γ' is unique if $t_{\Gamma'} - t_{\Gamma}$ is minimal. However, this is immediate from our construction of the sequence Γ'.

Let us assume $|P| = \infty$. By Proposition 3.10, there exists an integer g such that $f_{p_1}^{(2_{p_1,p_z})}(q)$ is the same for all $z \geq g$. Let $\Gamma^{\partial}_g = \{f_{p_i}^{(2_{p_1,p_g})}(q) | 1 \leq i \leq g\}$, which satisfies Functional Equation (1) by construction, and $\Gamma'_g = \{f'_n(q) | n \in A_{P_g}\}$ be the sequence defined in Key Proposition 2 satisfying Functional Equation (2) which is induced by Γ^{∂}_g and has Γ^{∂}_g as a subsequence. By Theorem 2.1 of [4], there exists a unique minimal collection $\{(a_j, b_j) | a_j \geq 1\}$ such that $f'_n(q) = \prod_j ([n]_{q^{a_j}})^{b_j}$ for all n in $supp\{\Gamma'_g\} = A_{P_g}$. Hence $f_{p_1}^{(2_{p_1,p_g})}(q) = \prod_j ([p_1]_{q^{a_j}})^{b_j}$. By our algorithm, this implies that $f_{p_i}^{(2_{p_1,p_g})}(q) = \prod_j ([p_i]_{q^{a_j}})^{b_j}$ for all $1 \leq i \leq g$. As $f_{p_1}^{(2_{p_1,p_g})}(q) = f_{p_1}^{(2_{p_1,p_z})}(q)$ for all $z \geq g$, we also have

$$f_{p_i}^{(2_{p_1,p_z})}(q) = \prod_j ([p_i]_{q^{a_j}})^{b_j}$$

for all $1 \leq i \leq z$ by our algorithm. Therefore,

$$f_{p_i}^{(2_{p_1,p_{|P|}})}(q) = \prod_j ([p_i]_{q^{a_j}})^{b_j} \quad \text{for } 1 \leq i \leq |P|$$

and thus

$$\Gamma^{\partial}_{|P|} = \left\{ \prod_i ([p_i]_{q^{a_j}})^{b_j} | p_i \in P \right\}$$

is well-defined and Γ^{∂}_{g} is a subsequence of Γ^{∂}_{z} for all $z \geq g$ which in turn is a . The rest of (1) and (2) is straight forward and is left to the interested readers. By Theorem 1.7, $\Gamma^{\partial}_{|P|}$ induces a sequence Γ' having $\Gamma^{\partial}_{|P|}$ as a subsequence and satisfying Functional Equation (2). Therefore $supp\{\Gamma^{\partial}_{|P|}\} = supp\{\Gamma'\}$. It is immediate from our construction that $t_{\Gamma'} - t_{\Gamma}$ is minimal and Γ' is the only such sequence. Thus the result follows.

□

Proof of Corollary 2.2. By construction, Γ' is a sequence of polynomials satisfying Functional Equation (2) with field of coefficients $\mathbb{Q}$ and support A_P where $|P| \geq 2$. By Theorem 2.1 of [4], there exists a minimal collection of finitely many ordered pairs of integers $\{(a_i, b_i)\}_i$ such that $f_n(q) = \prod_i ([n]_{q^{a_i}})^{b_i}$ for each n in the support of Γ'. Hence $\deg(f_n(q)) = t(n-1)$ where $t = \sum_i a_i b_i$. On the other hand, there exists a rational number $t_{\Gamma'}$ such that $\deg(f_n(q)) = t_{\Gamma}(n-1)$ for all n in the support of Γ' by [1]. Thus $t = t_{\Gamma'}$ is an integer. Since $t_{\Gamma'} - t_{\Gamma}$ is an integer by Theorem 2.1, t_{Γ} must also be an integer.

□

Corollary 2.3 shows that the collection of all the sequences of polynomials Γ satisfying Functional Equation (2) with field of coefficients of characteristic zero and t_{Γ} non-integral is strictly contained in the collection of all sequences of polynomials satisfying Functional Equation (2) with fields of coefficients of characteristic zero and support of the form A_P, where $P = \{p\}$ for some prime p. The former is classified completely:

Theorem 3.31 ([4]). (a) *If the parameter t_{Γ} of a sequence of polynomials $\Gamma = \{f_n(q)|n \in \mathbb{N}\}$, satisfying Functional Equation (2) and with field of coefficients of characteristic zero, is non-integral, then the set of primes P associated to the support A_P of Γ contains exactly one prime.*

(b) *If $\Gamma = \{f_n(q)|n \in \mathbb{N}\}$ is a sequence of polynomials satisfying Functional Equation (2), whose field of coefficients is of characteristic zero and t_{Γ} non-integral, then Γ is completely determined by the polynomial $f_p(q)$, where p is the prime in the support of Γ. In the opposite direction, for each triple $(f(q), p, t)$,* *where p is a prime,* $f(q)$ *is any polynomial with coefficients in the field of characteristic zero, constant term equal to* 1 *and degree td where d is any divisor of* $p-1$ *such that* $(t, \frac{p-1}{d}) = 1$*, there exists a unique sequence of polynomials* $\Gamma = \{f_{p^n}(q) | n \in \mathbb{N}; f_{p^0}(q) = 1, f_{p^1}(q) = f(q), t_\Gamma \in \mathbb{Q} - \mathbb{Z})\}$*, with the same field of coefficients, which satisfies Functional Equation* (2)*.*

Therefore it constitutes an essential part of a solution to Problem 2 stated in [4].

For completeness, we now sketch briefly the proof of Corollary 2.3:

Proof of Corollary 2.3. It is proved in [4] as a conditional result pending Theorem 2.1 above, which is Theorem 2.3 in [4]. Since Theorem 2.1 is established in earlier part of this paper, the proof of Corollary 2.3 is therefore complete. Please see [4] for more details of the argument.

□

To give a complete solution to Problem 2 described in the introduction for the case where the fields of coefficients are of characteristic zero, we need to extend our classification to all sequences satisfying Functional Equation (2) with fields of coefficients of characteristic zero, support of the form A_P where P is a given collection of primes, and $t_\Gamma \geq 1$ integral. What remains to be proven are the following cases: (1) $|P| = 1$ with t_Γ integral, and (2) $|P| \geq 2$ (which automatically means t_Γ integral by Corollary 2.2).

Proof of Theorem 2.8. Let $P = \{p\}$ and Υ_P be the collection of all sequences Γ of polynomials satisfying Functional Equation (2) with fields of coefficients of characteristic zero, support $A_{\{p\}}$ and t_Γ integral. Let $\Lambda := \{f(q)\}$ be the collection of all polynomials whose coefficients are contained in fields of characteristic zero and with $\deg(f(q)) = t(p-1)$ for some integer t. We need to show that the map

$$\begin{array}{ccc} \Lambda & \xrightarrow{\Psi} & \Upsilon_P \\ f(q) & \longmapsto & \Gamma_{f(q)}, \end{array}$$

where

$$\Gamma_{f(q)} := \left\{ f_{p^n}(q) | f_1(q) = 1, f_p(q) = f(q), n \in \mathbb{N} \cup \{0\} \right\}$$

and $f_{p^n}(q) := f_p(q) f_{p^{n-1}}(q^p)$ for all $n \geq 0$, is well-defined and bijective. Let $f(q)$ be any polynomial with coefficients in a field of characteristic zero.

Suppose we define $f(q) := f_p(q)$ and for each $n \in \mathbb{N}$, let $f_{p^n}(q)$ be defined by the recursive relation

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

Then it determines a unique sequence Γ of polynomials satisfying Functional Equation (2) with field of coefficients of characteristic zero, support $A_{P=\{p\}}$ and $f_p(q) = f(q)$ by [4] (particularly the proof of Theorem 2.5 there). We denote this sequence by $\Gamma_{f(q)}$. If $\deg(f(q)) = t(p-1)$ for some integer t, then $\Gamma_{f(q)}$ is an element of Υ_P. Thus Ψ is well-defined. Let Γ be any sequence in Υ_P. Let $f_p(q)$ be the polynomial in Γ corresponding to p. Then it can be verified that

$$\Psi(f_p(q)) = \Gamma_{f_p(q)} = \Gamma.$$

Thus Ψ is surjective. For injectivity, suppose there exist two polynomials $f_1(q)$ and $f_2(q)$ in Λ such that $\Gamma_{f_1(q)} = \Gamma_{f_2(q)}$. Then $t_{\Gamma_1} = t_{\Gamma_2}$. Hence $f_1(q) = f_2(q)$ since

$$deg\big(f_1(q)\big) = t_{\Gamma_1}(p-1) = t_{\Gamma_2}(p-1) = deg\big(f_2(q)\big).$$

Therefore the result follows.

□

P r o o f o f T h e o r e m 2.9. Let $P = \{p_1, \ldots, p_l\}$ be a collection of distinct primes with $l \geq 2$ which may be finite or infinite. Let $\Gamma = \{f_n(q) | n \in A_P\}$ be a sequence of polynomials satisfying the hypothesis of Theorem 2.1 with field of coefficients equal to $\mathbb{Q}$. Let $\Upsilon_{P,\mathbb{Q}}$ be the collection of all sequences of polynomials satisfying Functional Equation (2) with fields of coefficients $\mathbb{Q}$ and support A_P. Let Ω be the collection of equivalence classes of sets of finitely many ordered pairs of integers $\|\{(a_i, b_i)\}_i\|$ defined earlier. Let Γ be an element of $\Upsilon_{P,\mathbb{Q}}$. By Theorem 2.1 of [4], which is recalled at the beginning, there exists a unique minimal collection of finitely many ordered pairs of integers $\{(a_i, b_i)\}_i$ such that

$$f_n(q) = \prod_i ([n]_{q^{a_i}})^{b_i}$$

for all n in the support of Γ. Let $\|\{(a_i, b_i)\}_i\|$ be the equivalence class of $\{(a_i, b_i)\}_i$ in Ω. Then $f_n(q) = \prod_i ([n]_{q^{a_i}})^{b_i}$ for any $\{(a_i, b_i)\}_i \in \|\{(a_i, b_i)\}_i\|$. As $\|\{(a_i, b_i)\}_i\|$ is uniquely defined by Γ, we denoted it by $\|\{(a_i, b_i)\}_i\|_\Gamma$. Thus we have an injective map

$$\begin{array}{ccc} \Upsilon_{P,\mathbb{Q}} & \overset{\psi_1}{\hookrightarrow} & \Omega \\ \Gamma & \mapsto & \|\{(a_i, b_i)\}_i\|_\Gamma. \end{array}$$

On the other hand, for each equivalence class $\|\{(a_i,b_i)\}_i\| \in \Omega$, let us define a sequence of polynomials

$$\Gamma_{\|\{(a_i,b_i)\}_i\|} := \left\{ \prod_i ([n]_{q^{a_i}})^{b_i} | n \in supp\{\Gamma\} \right\},$$

where $\{(a_i,b_i)\}_i$ is any element of $\|\{(a_i,b_i)\}_i\|$ which we may assume to be the unique minimal collection in $\|\{(a_i,b_i)\}_i\|$. Then $\Gamma_{\|\{(a_i,b_i)\}_i\|}$ is a well-defined sequence of polynomials satisfying the hypothesis of Theorem 2.1 with field of coefficients equal to $\mathbb{Q}$ by the properties of quantum integers listed in the introduction and Theorem 2.1 of [4]. This gives an injective map

$$\begin{array}{ccc} \Omega & \overset{\psi_2}{\hookrightarrow} & \Upsilon_{P,\mathbb{Q}} \\ \|\{(a_i,b_i)\}_i\| & \mapsto & \Gamma_{\|\{(a_i,b_i)\}_i\|}. \end{array}$$

such that $\psi_2 \circ \psi_1$ is an identity map on $\Upsilon_{P,\mathbb{Q}}$. Therefore there exists a well-defined bijective map

$$\begin{array}{ccc} \Upsilon_{P,\mathbb{Q}} & \overset{\psi}{\longrightarrow} & \Omega \\ \Gamma & \longmapsto & \|\{(a_i,b_i)\}_i\|_\Gamma \end{array}$$

between $\Upsilon_{P,\mathbb{Q}}$ and Ω. Thus we have the complete classification of all sequences of polynomials satisfying Functional Equation (2) with fields of coefficients $\mathbb{Q}$ and support A_P for the given set of primes P. □

P r o o f o f T h e o r e m 2.10. Let $P = \{p_1, \ldots, p_l\}$ be a collection of distinct primes with $l \geq 2$ which may be finite or infinite. Let Υ_P be the collection of all sequences of polynomials satisfying Functional Equation (2) with fields of coefficients of characteristic zero and support A_P. Let Γ be an element of Υ_P. By Theorem 2.1 above, there exists a unique sequence $\Gamma' \in \Upsilon_{P,\mathbb{Q}}$ such that Γ' is the sequence over $\mathbb{Q}$ associated to Γ. Since $\Upsilon_{P,\mathbb{Q}} \subseteq \Upsilon_P$, we have a surjective map

$$\begin{array}{ccc} \Upsilon_P & \overset{\phi}{\longrightarrow} & \Upsilon_{P,\mathbb{Q}} \\ \Gamma & \longmapsto & \Gamma'. \end{array}$$

Thus we have a surjective map

$$\begin{array}{ccc} \Upsilon_P & \overset{\psi\circ\phi}{\longrightarrow} & \Omega \\ \Gamma & \longmapsto & |\{(a_i,b_i)\}_i\|_{\Gamma'}. \end{array}$$

For any $\Gamma' \in \Upsilon_{P,\mathbb{Q}}$, let $\|\{\Gamma\}\|_{\Gamma'}$ be the collection of all elements Γ of Υ_P such that Γ' is the sequence over $\mathbb{Q}$ associated to them, i.e. the fiber of ϕ above Γ'.

Let $\|\Upsilon_P\|$ denote the collection of all equivalence classes of Υ_P with respect to the relation $\overset{\Gamma'}{\sim}$. Therefore, we have a bijective map

$$\begin{array}{ccc} \|\Upsilon_P\| & \xrightarrow{\Phi} & \Omega, \\ \|\{\Gamma\}\|_{\Gamma'} & \longmapsto & |\{(a_i, b_i)\}_i\|_{\Gamma'} \end{array}$$

Therefore this gives us a classification of Υ_P up to the equivalence relation $\overset{\Gamma'}{\sim}$.

Let Γ' be an element of $\Upsilon_{P,\mathbb{Q}}$. Let Γ be any sequence of polynomials in $\|\{\Gamma\}\|_{\Gamma'}$. Let p be any prime in P and $f_p(q)$ and f'_p be the corresponding polynomials in Γ and Γ' respectively. As before, $f_p(q)$ can be written in the form

$$f_p(q) = \prod_{i \in I} f_{u_i,p}(q)$$

where $f_{u_i,p}(q)$ is the nontrivial factor of $f_p(q)$ whose roots are all the roots of $f_p(q)$ which are primitive $u_i p$-roots of unity and I is some finite set of indexes . By construction, $f_{u_i,p}(q)$ divides $f'_{u_i,p}(q)$ where $f'_{u_i,p}(q)$ is the nontrivial factor of $f'_p(q)$ whose roots are all the roots of $f'_p(q)$ which are primitive $u_i p$-roots of unity. Thus there are a finite number of possibilities for $f_{u_i,p}(q)$. Since I is a finite set, it is immediate that $\|\{\Gamma\}\|_{\Gamma'}$ has finite cardinality. □

Acknowledgement. The author would like to thank Melvyn Nathanson for posing this problem and the referee for several helpful suggestions in organizing this paper.

REFERENCES

[1] Nathanson, M. B.: *A Functional Equation Arising From Multiplication of Quantum Integers*, J. Number Theory **103** (2003), no. 2, 214-233.

[2] Nguyen, L.: *Extensions of supports of the solutions of a functional equation arising from multiplication of quantum integers* (submitted).

[3] Nguyen, L.: *On the Grothendieck group associated to the cllection of all solutions of a functional equation arising from multiplication of quantum integers with a given support*, (to appear in the Proceeding of Combinatorics and Additive Number Theory (2011)).

[4] Nguyen, L.: *On the Solutions of a Functional Equation Arising from Multiplication of Quantum Integers*, J. Number Theory **130** (2010), no. 6, 1292–1347.

[5] Nguyen, L.: *On the Support Base of a Functional Equation Arising from Multiplication of Quantum Integers*, J. Number Theory **130** (2010), no. 6, 1348–1373.

[6] Nguyen, L.: *A Complete Description of Maximal Solutions of Functional Equations Arising from Multiplication of Quantum Integers*, Int. J. Number Theory **7**(2011), no. 1, 09–56.
[7] Nguyen, L.: *On the Polynomial and Maximal Solutions to a Functional Equation Arising from Multiplication of Quantum Integers*, Notes on Number Theory and Discrete Math. **18** (2012), no. 4, 11–39.

Received December 16, 2011
Accepted September 13, 2012

Lan Nguyen
Department of Mathematics
University of Wisconsin-Parkside
Wisconsin
USA
E-mail: nguyenl@uwp.edu