On the support base of a functional equation arising from multiplication of quantum integers

Lan Nguyen

Mathematics Department, University of Michigan–Ann Arbor, United States

1. Introduction and background

In this paper, we study the support bases $P$ of solutions $\Gamma$ of the functional equation (discussed in [1]) arising from multiplication of quantum integers. We consider the case where the fields of coefficients of $\Gamma$ are of characteristic zero. It can be seen from [1–4] that quantum integers serve as an important source of generators for the solutions $\Gamma$ above. From [4], it is known that there is no sequence of polynomials, satisfying Functional Equation (2) with support base $P$ containing all primes, which cannot be generated by quantum integers. On the other hand, it is known from [6] that there exist sequences of polynomials satisfying Functional Equation (2) with support base $P$ of finite and infinite cardinality, which cannot be generated by quantum integers. The goal of this paper is to continue the study, begun in [6], of the limitation of quantum integers as generators for solutions of the functional equations above. In particular, we determine explicitly a set of criterions on $P$ that is necessary and sufficient for the existence of a sequence of polynomials, satisfying Functional Equation (2) and having support base $P$, which cannot be generated by quantum integers.
First, let us give some basic background and main results from [1,2,4,5], which are relevant to this paper, 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

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

where $n$ is any natural number.

From [1], multiplication operation for quantum integers, called quantum multiplication, is defined by the following rule:

$$[m]_q \star [n]_q := [mn]_q = [m]_q \cdot [n]_q^n = [n]_q \cdot [m]_q^n$$

where $\star$ denotes quantum multiplication, multiplication operation for quantum integers, and $\cdot$ denotes the usual multiplication of polynomials. It can be verified that Eq. (1.2) is just the $q$-series expansion of the sumset

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

Let $\Gamma = \{f_n(q) \mid n = 1, \ldots, \infty\}$ be a sequence of polynomials in $q$, with coefficients contained in some field of characteristic zero, satisfying the following functional equations:

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

for all $m,n \in \mathbb{N}$. As in [2,4] and others, we refer to the first equality in the above functional equation as Functional Equation (1) and the second equality as Functional Equation (2). A sequence of polynomials which satisfies Functional Equation (2) automatically satisfies Functional Equation (1) but not vice versa (see [4] for more details).

Let $\Gamma = \{f_n(q)\}$ be a sequence of polynomials satisfying Functional Equation (2). The set of integers $n$ in $\mathbb{N}$ where $f_n(q) \neq 0$ is called the **support** of $\Gamma$ and is denoted by $\text{supp}(\Gamma)$. 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 is called a prime multiplicative semigroup associated to $P$. From [1], the support of $\Gamma$ is a multiplicative prime sub-semigroup of $\mathbb{N}$.

**Theorem 1.2.** (See [1].) Let $\Gamma = \{f_n(q)\}$ be a sequence of polynomials satisfying Functional Equation (2). Then $\text{supp}(\Gamma)$ is of the form $A_P$ for some set of primes $P$, and $\Gamma$ is completely determined by the collection of polynomials:

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

**Definition 1.3.** Let $P$ be the collection of primes associated to the support $A_P$, in the sense of Theorem 1.2, of a sequence of polynomials $\Gamma$ satisfying Functional Equation (2). Then $P$ is called the **support base** of $\Gamma$. 
In the reverse direction, if \( P \) is a set of primes in \( \mathbb{N} \) then there is at least one sequence \( \Gamma \) satisfying Functional Equation (2) with \( \text{supp}(\Gamma) = A_P \). One such sequence can be defined as the set of polynomials:

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

Note that the coefficients of \( f_m(q) \) are properly contained in \( \mathbb{Q} \).

We say that a sequence \( \Gamma \) is nonzero if \( \text{supp}(\Gamma) \neq \emptyset \). If \( \Gamma \) satisfies Functional Equation (2), then \( \Gamma \) is nonzero if and only if \( f_1(q) = 1 \) (see [1]).

The degree of each polynomial \( f_n(q) \in \Gamma \) is denoted by \( \text{deg}(f_n(q)) \). From [1], it is known that there exists a rational number \( t_\Gamma \) such that:

\[
    \text{deg}(f_n(q)) = t_\Gamma(n - 1)
\]

for all \( n \) in \( \text{supp}(\Gamma) \). This number \( t_\Gamma \) is not necessarily an integer (see [4] for an example of such a sequence). We show in [2] and [4] that \( t_\Gamma \) can only be non-integral when the set of primes \( P \) associated to the support of \( \Gamma \) has the form \( P = \{p\} \) for some prime \( p \).

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

**Theorem 1.4.** (See [1].) Let \( P \) be a set of primes. Let \( \Gamma' = \{f_p'(q) \mid p \in P\} \) be a collection of polynomials 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 \( \Gamma = \{f_n(q) \mid n \in \mathbb{N}\} \) of polynomials satisfying Functional Equation (2) such that \( f_p(q) = f_p'(q) \) for all primes \( p \in P \).

**Theorem 1.5.** (See [4].) Let \( \Gamma = \{f_n(q) \mid n \in \mathbb{N}\} \) be a nonzero sequence of polynomials satisfying Functional Equation (2) with support \( A_P \) for some set of primes \( P \). Then there exist a unique completely multiplicative arithmetic function \( \psi(n) \), a rational number \( t \), and a unique sequence \( \Sigma = \{g_n(q)\} \) satisfying (2) with the same support \( A_P \) such that:

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

where \( g_n(q) \) is a monic polynomial with \( g_n(0) \neq 0 \) for all \( n \in A_P \).

As a result, in the rest of this paper, unless otherwise stated, all sequences of polynomials which we consider are normalized so that each polynomial is monic and has nonzero constant term.

For a sequence \( \Gamma \) of polynomials satisfying Functional Equation (2), the smallest field \( K \) which contains all the coefficients of all the polynomials in \( \Gamma \) is called the **Field of Coefficients of \( \Gamma \)**. 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 \( \Gamma \) 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 \( \Gamma \) can be viewed as a polynomial in \( \mathbb{C}[q] \). We frequently view polynomials \( f(q) \)'s in \( \Gamma \) as elements of the ring \( \mathbb{C}[q] \) throughout this paper. Thus whenever that is necessary, it is implicitly assumed.
Theorem 1.6. (See [4].) Let \( \Gamma = \{ f_n(q) \mid n \in \mathbb{N} \} \) 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 \( \Gamma \) contains \( p \) and \( r \) and the elements \( f_p(q) \) and \( f_r(q) \) of \( \Gamma \) are nonconstant polynomials. Then there exist ordered pairs of integers \( \{ u_i, t_i \} \) with \( i = 1, \ldots, s \) such that \( t_{\Gamma} = \sum_{i=1}^{s} u_i t_i \) and

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

for all \( n \) in \( \mathbb{N} \).

(2) Field of coefficients strictly contains \( \mathbb{Q} \): There is no sequence of polynomials \( \Gamma' \), with field of coefficients strictly containing \( \mathbb{Q} \), 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 \( \Gamma \) contains all prime numbers and the correspondent elements \( f_p(q) \) of \( \Gamma \) 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 \( t_{\Gamma} = \sum_{j=1}^{h} a_j b_j \) and

\[
  f_n(q) = \prod_{j=1}^{h} \left( [n]_{q^{s_j}} \right)^{b_j}
\]

for all \( n \in \text{supp}(\Gamma) \), 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 \( \{ a_j, b_j \} \) and the set \( \{ u_i, t_i \} \) is an equivalent 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 \( \Gamma \), then there exist sequences \( \Gamma' \)'s of polynomials with fields of coefficients strictly greater than \( \mathbb{Q} \) satisfying Functional Equation (2).

Definition 1.7. Let \( \Gamma = \{ f_n(q) \mid n \in \mathbb{N} \} \) be a sequence of polynomials satisfying Functional Equation (2). Then \( \Gamma \) is said to be generated by quantum integers if there exist ordered pairs of integers \( \{ u_i, t_i \} \) with \( i = 1, \ldots, s \) such that \( t_{\Gamma} = \sum_{i=1}^{s} u_i t_i \) and

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

for all \( n \) in \( \mathbb{N} \).

Let \( \Gamma \) be a nontrivial sequence of polynomials, with coefficients of characteristic zero, which satisfies Functional Equation (2). Let us recall from [4] that if \( f_s(q) \) is an element of \( \Gamma \) where \( s \) is a prime in the support base \( P \) of \( \Gamma \), then all the roots of \( f_s(q) \) are roots of unity of order dividing \( s \). Moreover, there is a product decomposition

\[
  f_s(q) = \prod_{i} f_{u_{s,i}}(q)
\]
where \( f_{u_i,s}(q) \) is the nontrivial factor of \( f_s(q) \) such that its roots are all the roots of \( f_s(q) \) which are roots of unity of order \( u_i \), for some positive integer \( u_i \).

Let \( u \) be any positive integer and \( p \) be any prime number. The polynomial denoted by \( P_{u,p}(q) \) or \( P_{u,p}(q) \) 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 \( P_{u+p}(q) \) or \( P_{u}(q) \) where \( v = u \). For a primitive \( n \)-root of unity \( \alpha \) in \( \mathbb{C} \), which can be written in the form \( \alpha = e^{\frac{2\pi i}{n}} \) for some primitive residue class \( w \) modulo \( n \), we always identify \( \alpha \), 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

\[
u_i \equiv \omega(p_i^{m_i}).\]

We also need to recall from [4] the following definitions since they are used frequently in the subsequent part of our work.

**Definition 1.8.** 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 \( ((\gamma_p, (wp_j))_j) | \gamma_p = 1, \ldots, p-1 \) if \( p \) does not divide \( u \) (resp. by the collection \( \{(wp_j + t((p^*))_j, (wp_j))_j | t = 0, \ldots, p-1 \) if \( p^q \) does not divide \( u \) for some positive integer \( q \geq 1 \) if \( u \) is the irreducible cyclotomic polynomial in \( \mathbb{Q}[q] \)) \( q \) is the nontrivial factor of \( P_{u,p}(q) \) if and only if all the roots of \( P_{u,r}(q) \) represented by the collection \( \{\gamma_r, (wp_j)_j | \gamma_r = 1, \ldots, r-1 \) if \( r \) does not divide \( u \) (resp. by the collection \( \{(wp_j + s(r^h)), (wp_j) | s = 0, \ldots, r-1 \) if \( r^h \) does not divide \( u \) for some positive integer \( h \geq 1 \) if \( r \) is the nontrivial factor of \( P_{u,r}(q) \)) \( q \) 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 \( r \) divides \( u \).

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

**Remark 1.9.** To understand the motivation for this definition, the readers can consult [4]. The polynomials \( F_{u,p}^{(i)}(q) \)’s in the definition of super-compatible might not be unique for any \( i \), where \( \boxdot \) denotes either \( p \) or \( r \).

Let \( p \) and \( r \) be any distinct primes in the support of \( \Gamma \). Define \( P_{u,p}(q) \) to be the factor of \( P_{p}(q) \) such that its roots consist of all the roots of \( P_{p}(q) \) with multiplicities which are primitive pu-roots of unity. Then \( P_{p}(q) = \prod_{i=0}^{p-1} P_{u,p}(q) \) in the ring \( \mathbb{C}[q] \). Similarly, \( F_{u,p}(q) = \prod_{i=0}^{u-1} F_{u,p,i}(q) \) in the ring \( \mathbb{C}[q] \). We call \( j \) (resp. \( i \) or interchangeably \( u_p,j \) (resp. \( u_p,i \)) the \( j \)-level (resp. \( i \)-level) of \( P_{p}(q) \) (resp. \( F_{u,p}(q) \)) if \( u_{p,j} \) (resp. \( u_{p,i} \)) is a nontrivial factor of \( P_{p}(q) \) (resp. \( F_{u,p}(q) \)). Define \( V_{p,r} := \{v_{p,r,k} | v_{p,r,k} > v_{p,r,k+1} := \{v_{p,r,k} \} \cup \{v_{p,r,k+1} \} \). 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 \( P_{p}(q) \) and \( F_{u,p}(q) \). Note that level \( i \) of \( P_{p}(q) \) or \( F_{u,p}(q) \) is not necessarily equal to the bi-level \( i \) of \( P_{p}(q) \) and \( F_{u,p}(q) \). Using \( V_{p,r} \) and these product decompositions, we write Functional Equation (1) with respect to \( F_{p}(q) \) and \( F_{r}(q) \) as:

\[
\begin{align*}
&f_{v_{p,r,1},p}(q)^{s_{v_{p,r,1},p}} f_{v_{p,r,1},r}(q)^{s_{v_{p,r,1},r}} \overset{(1)}{\rightarrow} f_{v_{p,r,1},p}(q)^{s_{v_{p,r,1},p}} f_{v_{p,r,1},r}(q)^{s_{v_{p,r,1},r}} \\
&\quad \vdots \quad \vdots \\
&f_{v_{p,r,k},p}(q)^{s_{v_{p,r,k},p}} f_{v_{p,r,k},r}(q)^{s_{v_{p,r,k},r}} \overset{(k)}{\rightarrow} f_{v_{p,r,k},p}(q)^{s_{v_{p,r,k},p}} f_{v_{p,r,k},r}(q)^{s_{v_{p,r,k},r}} \\
&\quad \vdots \quad \vdots \\
&f_{p}(q) f_{r}(q^{p^{*}}) = f_{r}(q^{p^{*}}) f_{p}(q^{p^{*}})
\end{align*}
\]
changing the order of the levels, i.e., $v_p$ nontrivially divides $f_p(q)$ (i.e., $f_{v_p,r,k} q = f_{u_i,k} q$ 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.

- $\prod_k f_{v_p,r,k} q^{s_{r,k}} f_{v_p,r,k} r(q) q^{s_{r,k}} = f_p(q) f_r(q^{p}).$

- $\prod_j f_{v_p,r,k} q^{s_{r,k}} f_{v_p,r,k} r(q) q^{s_{r,k}} = f_r(q) f_p(q^{r}).$

- The symbol $\langle \rangle$ indicates Functional Equation (1) at the bi-level $j$ (note that the polynomial expressions on the left-hand side and the right-hand side of $\langle \rangle$ at each bi-level are not necessarily equal).

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

The above version of Functional Equation (1) is 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 if at each bi-level $k$ where $p$ does not divide $v_{p,r,k}$, the line

$$f_{v_p,r,k} q^{s_{r,k}} f_{v_p,r,k} r(q) q^{s_{r,k}} \leftrightarrow f_{v_p,r,k} q^{s_{r,k}} f_{v_p,r,k} r(q) q^{s_{r,k}}$$

in EFE(1) is replaced by

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

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

(iii) $f_{v_p,r,k} q^{s_{r,k}} f_{v_p,r,k} r(q) q^{s_{r,k}} \leftrightarrow f_{v_p,r,k} q^{s_{r,k}} f_{v_p,r,k} r(q) q^{s_{r,k}}$ if $(r, v_{p,r,k}) = 1.$

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

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

Remark 1.10. (1) An EFE(1) with respect to $p$ and $r$ can be transformed into its reduced form by dividing both polynomials $f_p(q) f_r(q^{p})$ and $f_r(q) f_p(q^{r})$ by $\prod_i f_{v_{p,r,i},r}(q) r_{i}(1 - r_{p,i}) f_{v_{p,r,i},p}(q) r_{i}(1 - r_{p,i}).$

(2) 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 $Q_{p,r}(q);$ (3) For each line (i), the product of all expressions on both sides of $\leftrightarrow$ remains equal after (i), (ii) or (iii) have taken place. It is shown in [2] 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.

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 $\leftrightarrow$ can be replaced by $\overset{1}{\leftrightarrow}$ at each bi-level $i \leq k$, then we say that the resulting reduced form is
in $k$-super-reduced form. If $\leftrightarrow$ can be replaced by $\equiv$ at all bi-level $i$, then we say that it is in super-reduced form.

**Definition 1.11.** Let $\square$ denote either $p$ or $r$ and $\triangle$ denote the other. The polynomial $f_{\forall p,r,m,\square}(q) \neq 1$ is said to be directly related to the polynomial $f_{\forall p,r,n,\triangle}(q) \neq 1$ for some $n \neq m$ if $f_{\forall p,r,m,\square}(q) = f_{\forall p,r,n,\triangle}(q)$ and

$$f_{\forall p,r,m,\square}(q) \frac{f_{\forall p,r,l,\triangle}(q)_{\delta_{l,n}}}{f_{\forall p,r,l,\triangle}(q)_{\delta_{l,n}(1-\delta_{l,n})}} \neq f_{\forall p,r,n,\triangle}(q) \frac{f_{\forall p,r,l,\square}(q_{\delta_{l,n}})}{f_{\forall p,r,l,\square}(q_{\delta_{l,n}(1-\delta_{l,n})})}$$

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

$$f_{\forall p,r,m,\square}(q) \frac{f_{\forall p,r,n,\triangle}(q)_{\delta_{l,n}}}{f_{\forall p,r,n,\triangle}(q)_{\delta_{l,n}(1-\delta_{l,n})}} = f_{\forall p,r,n,\triangle}(q_{\delta_{l,n}}) \frac{f_{\forall p,r,l,\square}(q_{\delta_{l,n}})}{f_{\forall p,r,l,\square}(q_{\delta_{l,n}(1-\delta_{l,n})})}.$$

Suppose either $f_{\forall p,r,m,\square}(q)$ or $f_{\forall p,r,n,\triangle}(q)$ is nontrivial such that $\forall p,r,m,\square = \forall p,r,n,\triangle$ and

$$f_{\forall p,r,m,\square}(q) \frac{f_{\forall p,r,l,\triangle}(q)_{\delta_{l,n}}}{f_{\forall p,r,l,\triangle}(q)_{\delta_{l,n}(1-\delta_{l,n})}} = f_{\forall p,r,n,\triangle}(q) \frac{f_{\forall p,r,l,\square}(q_{\delta_{l,n}})}{f_{\forall p,r,l,\square}(q_{\delta_{l,n}(1-\delta_{l,n})})}$$

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

If two (or three in the case of indirect relation) polynomials satisfy one of the related relations above, we refer to the levels, namely $\forall p,r,m$ and $\forall p,r,n$ (and $\forall p,r,l$ 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.

### 2. Main results

Let $P$ be a set of distinct primes. We want to establish the necessary and sufficient criterions on $P$ for determining whether or not there exists a sequence of polynomials satisfying Functional Equation (2) with field of coefficients of characteristic zero and support base $P$.

If $|P| = 1$, then the necessary and sufficient criterions for the existence of a sequence of polynomials satisfying Functional Equation (2) having $P$ as its support base are completely understood (see [4] and [2] for more details). Therefore, we may assume from this point that $P$ contains at least two primes.

From part (1) of Theorem 1.6, if the field of coefficients of a sequence of polynomials satisfying Functional Equation (2) is of characteristic zero, then this sequence is not generated by quantum integers if and only if this field strictly contains $\mathbb{Q}$. Therefore, studying sequences of polynomials satisfying Functional Equation (2) which cannot be generated by quantum integers is equivalent to studying sequences of polynomials satisfying Functional Equation (2) with field of coefficients strictly containing $\mathbb{Q}$.

We know from part (2) of Theorem 1.6 that there is no sequence $\Gamma$ of polynomials satisfying Functional Equation (2) with support base $P$ consisting of all primes and field of coefficients strictly containing $\mathbb{Q}$. Therefore, there is no sequence $\Gamma$ of polynomials satisfying Functional Equation (2) with support base $P$ consisting of all primes, which cannot be generated by quantum integers. On the other hand, the following facts are known about the existence of a sequence of polynomials $\Gamma$.
satisfying Functional Equation (2) with field of coefficients of characteristic zero and support base $P$ where $P$ does not contain all primes.

(a) In the case where the field of coefficients is $\mathbb{Q}$, there exists at least one sequence of polynomials satisfying Functional Equation (2) having $P$ as its support base, namely

$$\Gamma := \{ f_n(q) = [n]_{q} \mid n \in A_P \}. $$

This sequence is in fact the unique sequence of monic polynomials satisfying Functional Equation (2) with support base $P$ such that $\deg(f_n(q)) = n - 1$, or equivalently $\Gamma = 1$, if $P \supseteq \{ 2, p \}$ for some odd prime $p$. Together with Theorem 1.6 part (1), it is necessary and sufficient that $|P| \geq 2$ for the existence of a sequence of polynomials satisfying Functional Equation (2) with field of coefficients equal to $\mathbb{Q}$.

(b) If the fields of coefficients strictly contains $\mathbb{Q}$, then Theorem 2.1 of [6] establishes a set of criterions on $P$ which is sufficient for the existence of a sequence $\Gamma$ of polynomials satisfying Functional Equation (2) with support base $P$.

The main goal of this paper is to prove that the criterions in case (b) above are also the necessary conditions for the existence of such sequences. Our main results can be summarized as follows:

**Theorem 2.1.** Let $P$ be any set of primes. Then there exists a sequence $\Gamma = \{ f_n(q) \mid n \in \text{supp}(\Gamma) \}$ of polynomials satisfying Functional Equation (2) with field of coefficients strictly containing $\mathbb{Q}$ and support base $P$ if and only if at least one of the following conditions is met:

1. $|P| \leq n$ for some natural number $n$.
2. $4 \mid p - 1$ for all odd primes $p$ in $P$.
3. There exists an odd prime $r$ such that $r \mid p - 1$ for all odd primes $p$ in $P$ or there exists a proper nonempty subset $A$ of $(\mathbb{Z}/W\mathbb{Z})^\ast$, for some natural number $W$, with $p.A = A$ for all odd primes $p$ in $P$.
4. There exists a collection of finitely many odd primes $P = \{ r_i \}$ of $P$ such that at least one prime $r_i$ in $P$ divides $p - 1$ for all odd primes $p$ in $P - P$ or there exists a proper nonempty subset $A$ of $(\mathbb{Z}/W\mathbb{Z})^\ast$, for some natural number $W$, with $p.A = A$ for all odd primes $p$ in $P - P$.

**Corollary 2.2.** Let $P$ be the support base of a sequence $\Gamma$ of polynomials satisfying Functional Equation (2) with field of coefficients of characteristic zero. If $P$ contains all but finitely many primes, then $\Gamma$ is generated by quantum integers.

3. Proofs of main results

**Proof of Theorem 2.1.** (1) Let $P$ be a set of primes. Suppose that at least one of the conditions in Theorem 2.1 holds. Let us construct a sequence $\Gamma$ of polynomials, satisfying Functional Equation (2), with field of coefficients strictly containing $\mathbb{Q}$ and with $P$ as its support base. From Theorem 2.1 of [6], it suffices for us to construct such a sequence if at least one of the following conditions holds:

- $2 < |P| < \infty$.
- Condition (4) holds with $|P| > 1$.

(i) Suppose $2 < |P| < \infty$. For this construction, our method is an inductive method which uses the construction in the proof of (1) of Theorem 2.1 of [6] as the starting point and as building blocks.

Let $p$ and $r$ be two primes in $P$ such that $p$ is the smallest prime in $P$ and $r$ is the smallest prime in $P - \{ p \}$. Suppose that there exists a sequence $\Gamma$ of polynomials satisfying Functional Equation (2) with support base $P$ such that $\prod_{w \in P} w$ divides the value $v_{p,r,1}$ of the bi-level 1 of EFE(1) with respect to $p$ and $r$ and that

$$\left( \prod_{w \in P} w, \frac{v_{p,r,1}}{\prod_{w \in P} w} \right) = 1.$$
Then we have:

**Proposition 3.1 (Key Proposition 1).** The reduced form of EFE(1) with respect to \(p\) and \(r\) has the form

\[
\frac{f_{v_{p,r,1},p}(q) f_{v_{p,r,1},p}(q^p)}{f_{v_{p,r,1},p}(q) f_{v_{p,r,1},p}(q^p)} \quad \cdots \quad \frac{f_{v_{p,r,d_1},p}(q^{p_{d_1} r_{d_1}}) f_{v_{p,r,d_1},p}(q^{p_{d_1} r_{d_1}})}{f_{v_{p,r,d_1},p}(q^{p_{d_1} r_{d_1}}) f_{v_{p,r,d_1},p}(q^{p_{d_1} r_{d_1}})} \\
\frac{f_{v_{p,r,1},p}(q^{p_{k_1}}) f_{v_{p,r,1},p}(q^{p_{k_1}})}{f_{v_{p,r,1},p}(q^{p_{k_1}}) f_{v_{p,r,1},p}(q^{p_{k_1}})} \quad \cdots \quad \frac{f_{v_{p,r,d_2},p}(q^{p_{d_2} r_{d_2}}) f_{v_{p,r,d_2},p}(q^{p_{d_2} r_{d_2}})}{f_{v_{p,r,d_2},p}(q^{p_{d_2} r_{d_2}}) f_{v_{p,r,d_2},p}(q^{p_{d_2} r_{d_2}})} \\
\frac{f_{v_{p,r,1},p}(q^{p_{k_2}}) f_{v_{p,r,1},p}(q^{p_{k_2}})}{f_{v_{p,r,1},p}(q^{p_{k_2}}) f_{v_{p,r,1},p}(q^{p_{k_2}})} \quad \cdots \quad \frac{f_{v_{p,r,d_3},p}(q^{p_{d_3} r_{d_3}}) f_{v_{p,r,d_3},p}(q^{p_{d_3} r_{d_3}})}{f_{v_{p,r,d_3},p}(q^{p_{d_3} r_{d_3}}) f_{v_{p,r,d_3},p}(q^{p_{d_3} r_{d_3}})} \\
\frac{f_{v_{p,r,1},p}(q^{p_{k_3}}) f_{v_{p,r,1},p}(q^{p_{k_3}})}{f_{v_{p,r,1},p}(q^{p_{k_3}}) f_{v_{p,r,1},p}(q^{p_{k_3}})} \quad \cdots \quad \frac{f_{v_{p,r,d_4},p}(q^{p_{d_4} r_{d_4}}) f_{v_{p,r,d_4},p}(q^{p_{d_4} r_{d_4}})}{f_{v_{p,r,d_4},p}(q^{p_{d_4} r_{d_4}}) f_{v_{p,r,d_4},p}(q^{p_{d_4} r_{d_4}})} \\
\frac{f_{v_{p,r,1},p}(q^{p_{k_4}}) f_{v_{p,r,1},p}(q^{p_{k_4}})}{f_{v_{p,r,1},p}(q^{p_{k_4}}) f_{v_{p,r,1},p}(q^{p_{k_4}})} \quad \cdots \quad \frac{f_{v_{p,r,d_5},p}(q^{p_{d_5} r_{d_5}}) f_{v_{p,r,d_5},p}(q^{p_{d_5} r_{d_5}})}{f_{v_{p,r,d_5},p}(q^{p_{d_5} r_{d_5}}) f_{v_{p,r,d_5},p}(q^{p_{d_5} r_{d_5}})}
\]

where:

- \(d_1\) (resp. \(k_1\)) is any bi-level of EFE(1) with respect to \(p\) and \(r\) such that \(v_{p,r,1} > v_{p,r,d_i} > \frac{v_{p,r,1}}{p}\) (resp. \(v_{p,r,k_i} = \frac{v_{p,r,1}}{p}\)).

\[Q_{p,r}(q) = Q_{p,r}(q)\]
• $d_2$ (resp. $k_2$) is any bi-level of EFE(1) with respect to $p$ and $r$ such that $v_{p,r,d_2} > v_{p,r,2P}$ (resp. $v_{p,r,k_2} = v_{p,r,1P}$).
• $d_3$ (resp. $k_3$) is any bi-level of EFE(1) with respect to $p$ and $r$ such that $v_{p,r,d_3} > v_{p,r,1P}$ (resp. $v_{p,r,k_3} = v_{p,r,1P}$).
• $d_4$ (resp. $k_4$) is any bi-level of EFE(1) with respect to $p$ and $r$ such that $v_{p,r,d_4} > v_{p,r,1P}$ (resp. $v_{p,r,k_4} = v_{p,r,1P}$).
• $d_5$ is any bi-level of EFE(1) with respect to $p$ and $r$ such that $v_{p,r,d_5} > v_{p,r,5}$.
• All the rational expressions above are polynomials.

Proof. Even though we have $v_{p,r,1} = \prod_{w \in P} w$ with $|P| > 2$ in this proposition instead of $|P| = 2$ as in Key Proposition 1 of [6], the proof is exactly the same (see the proof of Key Proposition 1 of [6] for details). It can be verified that this proposition also holds if $p$ and $r$ are replaced by $s$ and $t$ respectively for any pair of primes $s < t$ in $P$. \qed

From Proposition 3.1, we can construct a sequence of polynomials $\Gamma$ satisfying Functional Equation (2) having support base $P$.

Step 1: We construct $f_p(q)$ and $f_r(q)$ satisfying Functional Equation (1) using the crucial lines of the reduced form of EFE(1) with respect to $p$ and $r$ stated in Proposition 3.1 (see [6] for definition of crucial lines and for the justification of this construction)

$\frac{f_{v_{p,r,1},p}(q)}{f_{v_{p,r,1},p}(q^P)} \overset{(1)}{\longrightarrow} \frac{f_{v_{p,r,1},r}(q)}{f_{v_{p,r,1},r}(q^P)} \frac{f_{v_{p,r,1},p}(q^P)}{f_{v_{p,r,1},r}(q^P)} \frac{f_{v_{p,r,1},p}(q)}{f_{v_{p,r,1},r}(q)} \frac{f_{v_{p,r,1},p}(q^P)}{f_{v_{p,r,1},r}(q^P)} \cdots \cdots \cdots$

as follows:

Let $p_i$ be an odd prime in $P$. For each $p_j \in P$, let $A_{p_j}$ be a nonempty set such that $A_{p_j} = (\mathbb{Z}/p_j\mathbb{Z})^*$ if $p_j \in P - \{p_i\}$ and $A_{p_j} < (\mathbb{Z}/p_j\mathbb{Z})^*$ if $p_j = p_i$. Thus

$A_{\prod_{p_j \in P} p_j} := \prod_{p_j \in P} A_{p_j} < \prod_{p_j \in P} (\mathbb{Z}/p_j\mathbb{Z})^* \cong \left( \mathbb{Z}/\prod_{p_j \in P} p_j \mathbb{Z} \right)^*$. 

Let $v_{p,r,1} = u = \prod_{j \in p} p_j$. Let $1 := k_0$ and $K := \{k_0, k_1, k_2, k_3, k_4\}$. Define

$$f^{(r)}_p(q) = \prod_{i \in K} f_{v_{p,r,i},p}(q)^{s_{p,i}}$$

and

$$f^{(p)}_r(q) = \prod_{i \in K} f_{v_{p,r,i},r}(q)^{s_{r,i}}$$

where:

(0) $s_{p,k_0} = 1$ and $f_{u,p_j}(q)$ is the monic polynomial with nonzero constant term whose roots are primitive $u_{p_j}$-roots of unity represented, via the Chinese Remainder Theorem (see the proof of Key Proposition 1' of [4] for more details), by collection of tuples:

$$A(p_j) := \{(wp_j + t(p_j), (wp_j)_i) \mid 0 \leq t \leq p_j - 1, \ p_i \in P - \{p_j\}, \ wp_j \in A_{p_j}, \ wp_j \in A_{p_j}\}$$

for each $p_j \in P$.

**Remark 3.2.** As in [2] and [4], we use the phrase the collection of roots of a certain polynomial is represented by a collection of tuples to indicate that there is a one-to-one correspondence between the collection of roots of that polynomial and the elements of such a collection of tuples, via Chinese Remainder Theorem.

(1) $s_{p,k_1} = 1$ and

$$f_{v_{p,r,k_1},p}(q) = f^{r_{p,r,k_0}}_{p}(q)$$

is the monic polynomial who roots are primitive $v_{p,r,k_0}$-roots of unity represented by the collection of tuples

$$\{(wp, (wp)_1) \mid p_i \in P - \{p\}, \ wp_i \in B_{p_i} = A_{p_i}^*, \ wp \in B_p = A_p^*\},$$

where $A_{p_i}^* = (\mathbb{Z}/p_i\mathbb{Z})^* = A_{p_i}$ for each $p_i \in P - \{p\}$ and $A_{p_i}^* = (\mathbb{Z}/p_i\mathbb{Z})^* = A_{p_i}$.

(1) $s_{r,k_1} = 1$ and

$$f_{v_{p,r,k_1},r}(q) = f^{r_{p,r,k_0}}_{p}(q)$$

where $P^{r_{p,r,k_0}}_{p,r}(q)$ is the cyclotomic polynomial with coefficients in $\mathbb{Q}$ and order $\frac{v_{p,r,k_0}}{p}r$.

(2) $s_{p,k_2} = s_{r,k_2} = 0$, i.e.,

$$f_{v_{p,r,k_2},r}(q) = f^{r_{p,r,k_0}}_{p}(q) = f^{r_{p,r,k_0}}_{r}(q) = f_{v_{p,r,k_2},p}(q) \quad (3)$$

(3) $s_{p,k_3} = 1$ and

$$f_{v_{p,r,k_3},p}(q) = f^{r_{p,r,k_0}}_{p}(q) = P^{r_{p,r,k_0}}_{r,p}(q)$$

where $P^{r_{p,r,k_0}}_{r,p}(q)$ is the cyclotomic polynomial with coefficients in $\mathbb{Q}$ and order $\frac{v_{p,r,k_0}}{r}p$. 
(3r) $s_{r,k_3} = 1$ and

$$f_{v_{p,r,k_3^*}}(q) = f_{v_{p,r,k_0}}(q)$$

is the monic polynomial whose roots are primitive $v_{p,r,k_0}$-roots of unity represented by the collection of tuples

$$\left\{ (w_r, (w_{p_i})) \mid p_i \in P - \{r\}, \ w_{p_i} \in B_{p_i} = A_{p_i}^*, \ w_r \in B_r = A_r^* \right\},$$

where $A_{p_i}^* = (\mathbb{Z}/p_i \mathbb{Z})^* = A_{p_i}$ for each $p_i \in P - \{p_r\}$ and $A_{p_i}^* = (\mathbb{Z}/p_i \mathbb{Z})^* - A_{p_i}$.

(4) $s_{p,k_4} = s_{r,k_4} = 0$, i.e.,

$$f_{v_{p,r,k_4}}(p) = f_{v_{p,r,k_0}}(p) = 1 = f_{v_{p,r,k_0}}(q) = f_{v_{p,r,k_4}}(q).$$

**Proposition 3.3 (Key Proposition 2).** $f_{v_r}(q)$ and $f_{v_r}(p)$ satisfy Functional Equation (1).

**Proof.** See the proof of Theorem 2.1 of [6]. $\Box$

By indexing $P$, we write $P = \{p_1, \ldots, p_{|P|}\}$. For each natural number $n$ in $[2, \ldots, |P|]$, let $P_n$ be the set $\{p^{(1)}, \ldots, p^{(|P|)}\}$, the collection of all distinct subsets of $P$ with cardinality $n$. For each $P^{(i)}$, define

$$|P^{(i)}| := \prod_{p_j \in P^{(i)}} p_j.$$

**Step 2:** We generalize Step 1 to the case where $|P| > 2$. Let $s$ be any prime in $P$. Define

$$f_s(q) := f_{u,s}(q) \prod_{p^{(i)} \in P_1} f_{u_{|P^{(i)}|}, s}(q) \cdots \prod_{p^{(i)} \in P_{n-1}} f_{u_{|P^{(i-1)}|}, s}(q),$$

where:

- $f_{u,s}(q)$ is the monic polynomial whose roots are primitive $us$-roots of unity represented by the collection of tuples

$$A(s) := \{(w_s, (w_{p_j})_j) \mid p_j \in P - \{s\}, \ w_{p_j} \in A_{p_j}, \ w_s \in A_s\}.$$

- $f_{u_{|P^{(i)}|}, s}(q)$ is the monic polynomial whose roots are primitive $u_{|P^{(i)}|}$-roots of unity represented by the collection of tuples

$$\left\{ (w_s, (w_{p_j})_j) \mid p_j \in P - \{s\}, \ w_{p_j} \in B_{p_j}, \ w_s \in B_s \right\},$$

where $B_{p_j} = A_{p_j}^*$ for each $p_j \in P - \{s\}$ and $B_s = A_s^*$, if $i = 1$ and $s \in P^{(i)}$.

- $f_{u_{|P^{(i-1)}|}, s}(q) = P_{u_{|P^{(i-1)}|}, s}(q)$, where $P_{u_{|P^{(i-1)}|}, s}(q)$ is the cyclotomic polynomial of order $u_{|P^{(i-1)}|}$ with coefficients in $\mathbb{Q}$, if $i = 1$ and $s$ is not in $P^{(i)}$. 
Lemma 3.5. There exists a set of natural numbers $U$ such that

$$
\prod_{P^{(i)} \in P_1, P^{(i)} \neq [p]} f_{u \mid P^{(i)}}, p(q) \cdots \prod_{P^{(i)} \in P_{n-1}} f_{u \mid P^{(i)}}, p(q) = \prod_{u_i \in U} \left( f_{u_i, p}(q) f_{u_i \mid P}, p(q) f_{u_i \mid P}, p(q) \right),
$$

$$
\prod_{P^{(i)} \in P_1, P^{(i)} \neq [r]} f_{u \mid P^{(i)}}, r(q) \cdots \prod_{P^{(i)} \in P_{n-1}} f_{u \mid P^{(i)}}, r(q) = \prod_{u_i \in U} \left( f_{u_i, r}(q) f_{u_i \mid P}, r(q) f_{u_i \mid P}, r(q) \right),
$$

where $gcd(pr, u_i) = pr$ for each $u_i \in U$. 

Proposition 3.4 (Key Proposition 3). Let $\Sigma_P := \{f_s(q) \mid s \in P\}$ where $f_s(q)$ is the polynomial defined in Step 2 for each prime $s$ in $P$. Then $\Gamma_P$ satisfies Functional Equation (1). 

Proof. Our method for proving this proposition is to use Key Proposition 2. Let $p$ and $r$ be any two primes in $P$ and let $f_p(q)$ and $f_r(q)$ be the polynomials in $\Sigma_P$ corresponding to $p$ and $r$. Then

$$
f_p(q) = f_{u \mid P}, p(q) \prod_{P^{(i)} \in P_1} f_{u \mid P^{(i)}}, p(q) \cdots \prod_{P^{(i)} \in P_{n-1}} f_{u \mid P^{(i)}}, p(q)
$$

and

$$
f_r(q) = f_{u \mid P}, r(q) \prod_{P^{(i)} \in P_1} f_{u \mid P^{(i)}}, r(q) \cdots \prod_{P^{(i)} \in P_{n-1}} f_{u \mid P^{(i)}}, r(q)
$$

By Key Proposition 2, $f_{u \mid P}, p(q) f_{u \mid P}, p(q) f_{u \mid P}, r(q)$ and $f_{u \mid P}, r(q) f_{u \mid P}, r(q) f_{u \mid P}, r(q)$ satisfy Functional Equation (1). Therefore, it suffices for us to prove that

$$
\frac{f_p(q)}{f_{u \mid P}, p(q) f_{u \mid P}, r(q) f_{u \mid P}, r(q)} = \prod_{P^{(i)} \in P_1, P^{(i)} \neq [p], P^{(i)} \neq [r]} f_{u \mid P^{(i)}}, p(q) \cdots \prod_{P^{(i)} \in P_{n-1}} f_{u \mid P^{(i)}}, p(q)
$$

and

$$
\frac{f_r(q)}{f_{u \mid P}, p(q) f_{u \mid P}, r(q) f_{u \mid P}, r(q)} = \prod_{P^{(i)} \in P_1, P^{(i)} \neq [r], P^{(i)} \neq [p]} f_{u \mid P^{(i)}}, r(q) \cdots \prod_{P^{(i)} \in P_{n-1}} f_{u \mid P^{(i)}}, r(q)
$$

satisfy Functional Equation (1).
**Proof.** Let \( p^{(i)} \) be an arbitrary element of \( P_1 \) such that \( P^{(i)} \neq \{p\} \) and \( \{r\} \). Then

\[
 f_{\frac{u}{p^{(i)}}} \cdot p(q) = f_{\frac{u}{p^{(i)}}} \cdot p(q)
\]

and

\[
 f_{\frac{u}{p^{(i)}}} \cdot r(q) = f_{\frac{u}{p^{(i)}}} \cdot r(q)
\]

for some prime \( s \). Then it can be verified that there exists a unique element \( P^{(j, s)} \) in \( P_2 \) such that \( P^{(j, s)} = \{s, p\} \) and a unique element \( P^{(j, r)} \) in \( P_2 \) such that \( P^{(j, r)} = \{s, r\} \). Then

\[
 f_{\frac{u}{p^{(j, s)}}} \cdot p(q) = f_{\frac{u}{p^{(j, s)}}} \cdot p(q) = f_{\frac{u}{p^{(j, s)}}} \cdot p(q),
\]

\[
 f_{\frac{u}{p^{(j, r)}}} \cdot p(q) = f_{\frac{u}{p^{(j, r)}}} \cdot p(q) = f_{\frac{u}{p^{(j, r)}}} \cdot p(q),
\]

\[
 f_{\frac{u}{p^{(j, s)}}} \cdot r(q) = f_{\frac{u}{p^{(j, s)}}} \cdot r(q) = f_{\frac{u}{p^{(j, s)}}} \cdot r(q),
\]

\[
 f_{\frac{u}{p^{(j, r)}}} \cdot r(q) = f_{\frac{u}{p^{(j, r)}}} \cdot r(q) = f_{\frac{u}{p^{(j, r)}}} \cdot r(q).
\]

Let \( u_i := \frac{u}{s} \). It can be verified by direct computation using the definition in Step 2 that

\[
 f_{u_i} \cdot p(q) f_{u_i} \cdot p(q) f_{u_i} \cdot p(q)
\]

and

\[
 f_{u_i} \cdot r(q) f_{u_i} \cdot r(q) f_{u_i} \cdot r(q)
\]

satisfy Functional Equation (1). Therefore,

\[
 \prod_{p^{(i)} \in P_1, \ p^{(i)} \neq \{p\} \neq \{r\}} f_{\frac{u}{p^{(i)}}} \cdot p(q) \prod_{p^{(i, s)} \in P_2} f_{\frac{u}{p^{(i, s)}}} \cdot p(q) \prod_{p^{(i, r)} \in P_2} f_{\frac{u}{p^{(i, r)}}} \cdot r(q)
\]

and

\[
 \prod_{p^{(i)} \in P_1, \ p^{(i)} \neq \{p\} \neq \{r\}} f_{\frac{u}{p^{(i)}}} \cdot p(q) \prod_{p^{(i, s)} \in P_2} f_{\frac{u}{p^{(i, s)}}} \cdot r(q) \prod_{p^{(i, r)} \in P_2} f_{\frac{u}{p^{(i, r)}}} \cdot r(q)
\]

satisfy Functional Equation (1) as well.

To prove the lemma, it suffices now to prove that

\[
 \prod_{p^{(i)} \in P_2, \ p^{(i)} \neq \{p, s\} \neq \{r\}} f_{\frac{u}{p^{(i)}}} \cdot p(q) \prod_{p^{(i)} \in P_2, \ p^{(i)} \neq \{p, r\} \neq \{s\}} f_{\frac{u}{p^{(i)}}} \cdot r(q)
\]

and

\[
 \prod_{p^{(i)} \in P_2, \ p^{(i)} \neq \{p, s\} \neq \{r\}} f_{\frac{u}{p^{(i)}}} \cdot r(q) \prod_{p^{(i)} \in P_2, \ p^{(i)} \neq \{p, r\} \neq \{s\}} f_{\frac{u}{p^{(i)}}} \cdot r(q)
\]
satisfy Functional Equation (1). For each \( P^{(i)} \) in \( P_2 \) such that \( P^{(i)} \neq P^{(i,p)} \) and \( P^{(i)} \neq P^{(i,r)} \), define

\[
 u_i := \frac{u}{|P^{(i)}|}.
\]

Then the same argument as above can be applied. By repeating this argument, the result follows. \( \Box \)

Therefore \( f_p(q) \) and \( f_r(q) \) satisfy Functional Equation (1) and Key Proposition 3 follows. \( \Box \)

Therefore \( \Sigma_P \) induces a unique sequence of polynomials \( \Gamma \) satisfying Functional Equation (2) which contains \( \Sigma_P \) as a subsequence by Theorem 1.4. It is straightforward to verify that \( \Gamma \) has all the required properties.

(ii) Suppose that condition (4) of Theorem 2.1 holds with \(|P| > 1\). Let us construct a sequence of polynomials \( \Gamma \) satisfying Functional Equation (2) with field of coefficients strictly containing \( \mathbb{Q} \) and with \( P \) as its support base.

Define:

\[
 u := \prod_{s \in P} s.
\]

Let us apply the construction of part (i) above to each prime \( s \) in \( P \) with \( u = \prod_{s \in P} s \) replacing \( u = \prod_{s \in P} s \) and \( P \) replacing \( P \). Therefore, we obtain a sequence of polynomials

\[
 \Sigma_1 := \{ f_s(q) \mid s \in P \}
\]

satisfying Functional Equation (1) by Key Proposition 3.

Let us fix a prime \( z \) in \( P \) and let \( f_z(q) \) be the corresponding polynomial in \( \Sigma_1 \). It can be verified from its construction that \( f_z(q) \) has the following product decomposition:

\[
 f_z(q) = \prod_i f_{u_{z,i}, z}(q)
\]

where \( f_{u_{z,i}, w}(q) \) is the factor of \( f_w(q) \) whose roots are all the roots of \( f_z(q) \) which are primitive \( u_{z,i} \)-roots of unity for some positive integer \( u_{z,i} \). It can also be verified from the construction of \( f_z(q) \) that \( f_{u_{z,i}, z}(q) \) divides \( P_{u_{z,i}, z}(q) \) or \( (P_{u_{z,i}, z}(q))^2 \) for each \( i \), where \( P_{u_{z,i}, z}(q) \) is the cyclotomic polynomial of order \( u_{z,i} \) and has coefficients in \( \mathbb{Q} \).

For each prime \( p \) in \( P - P \), define:

\[
 f_p(q) := f_{u_{z,1}, p}(q) \prod_{i > 1} f_{u_{z,i}, p}(q)
\]

where:

- \( f_{u_{z,1}, p}(q) \) is the monic polynomial whose roots are represented by the collection of tuples of integers

\[
 \{(w_p, (w_{p_i})_i) \mid p_i \in P, w_{p_i} \in A_{p_i}, w_p \in (\mathbb{Z}/p\mathbb{Z})^*\}.
\]
• For each $i > 1$, define

$$f_{u_{z,i},p}(q) = \begin{cases} P_{u_{z,i},p}(q) & \text{if } z \text{ does not divide } u_{z,i}, \\ (P_{u_{z,i},p}(q))^2 & \text{otherwise}, \end{cases}$$

where $P_{u_{z,i},p}(q)$ is the cyclotomic polynomial of order $u_{z,i}$ and with coefficients contained in $\mathbb{Q}$.

It follows immediately from the construction above that the coefficients of $f_p(q)$ are not properly contained in $\mathbb{Q}$ for each prime $p \in P - P$.

Let

$$\Sigma_2 := \{ f_s(q) \mid s \in P - P \}.$$

**Proposition 3.6 (Key Proposition 4).** Let

$$\Sigma = \Sigma_1 \cup \Sigma_2.$$

Then $\Sigma$ satisfies Functional Equation (1).

**Proof.** Let $f_p(q)$ be a polynomial $\Sigma_1$. Let $f_r(q)$ and $f_t(q)$ be polynomials in $\Sigma_2$. From Key Proposition 2, it suffices for us to prove:

(i) $f_r(q)$ and $f_t(q)$ satisfy Functional Equation (1).
(ii) $f_p(q)$ and $f_r(q)$ satisfy Functional Equation (1).

(i) Let $u = \prod_{s \in P} s$ and let $z$ be the fixed prime in $P$ chosen above. Then $u = u_{z,1}$. Since $f_r(q)$ and $f_t(q)$ are polynomials in $\Sigma_2$, $r$ and $t$ are two primes in $P - P$. Hence

$$f_t(q) = f_{u_{z,1},t}(q) \prod_{i > 1} f_{u_{z,i},t}(q)$$

and

$$f_r(q) = f_{u_{z,1},r}(q) \prod_{i > 1} f_{u_{z,i},r}(q)$$

by definition. Since condition (4) holds, it can be verified that either $r \equiv t \equiv 1 \pmod{p_i}$, where $p_i$ is the only prime in $P$ with $A_{p_i}$ a nonempty proper subset of $(\mathbb{Z}/p_i\mathbb{Z})^*$, or there exists a nonempty proper subset $A$ of $(\mathbb{Z}/u\mathbb{Z})^*$ such that $rA = tA = A$. Therefore, $f_{u_{z,1},r}(q^i)$ and $f_{u_{z,1},t}(q^i)$ are polynomials by Key Proposition 1' of [4] since $rt$ is relatively prime to $u$ by construction. Moreover, it can be verified from the construction above that

$$\frac{f_{u_{z,i},r}(q^i)}{f_{u_{z,i},t}(q^i)} = \frac{f_{u_{z,1},t}(q^i)}{f_{u_{z,1},r}(q^i)}$$

is a polynomial. Thus

$$f_{u_{z,i},t}(q) f_{u_{z,i},r}(q) = f_{u_{z,i},r}(q) f_{u_{z,i},t}(q).$$
Furthermore, it can also be verified from our construction that

\[ \frac{f_{u_{z,i},r}(q^p)}{f_{u_{z,i},r}(q)} = \frac{f_{u_{z,i},r}(q^r)}{f_{u_{z,i},r}(q)} , \]

or equivalently,

\[ f_{u_{z,i},p}(q) f_{u_{z,i},r}(q^p) = f_{u_{z,i},r}(q) f_{u_{z,i},p}(q^r) \]

for each \( i > 1 \) since

\[ f_{u_{z,i},\Box}(q) = \begin{cases} P_{u_{z,i},\Box}(q) & \text{if } z \text{ divide } u_{z,i}, \\ (P_{u_{z,i},\Box}(q))^2 & \text{otherwise}, \end{cases} \]

where \( \Box \) denotes either \( p \) or \( r \). Putting together these equations, we obtain the EFE(1) with respect to \( p \) and \( r \). Hence \( f_p(q) \) and \( f_r(q) \) satisfy Functional Equation (1).

(ii) Let \( z \) be the fixed prime above. By (i), \( f_z(q) \) and \( f_p(q) \) satisfy Functional Equation (1). Thus we may consider EFE(1) with respect to \( p \) and \( z \)

\[ f_{v_{p,z,i},p}(q) s_{v_{p,z,i}} f_{v_{p,z,i},z}(q) s_{v_{p,z,i}} \xrightarrow{(1)} f_{v_{p,z,i},z}(q) s_{v_{p,z,i}} f_{v_{p,z,i},p}(q) s_{v_{p,z,i}} \]

\[ \vdots \quad \vdots \]

\[ f_{v_{p,z,i},p}(q) s_{v_{p,z,i}} f_{v_{p,z,i},z}(q) s_{v_{p,z,i}} \xleftarrow{(i)} f_{v_{p,z,i},z}(q) s_{v_{p,z,i}} f_{v_{p,z,i},p}(q) s_{v_{p,z,i}} \]

\[ \vdots \quad \vdots \]

\[ f_p(q) f_z(q^p) = f_z(q) f_p(q^z). \]

It can be verified from our construction that \( s_{\Box,i} = 1 \) for all bi-levels \( i \), where \( \Box \) denotes either \( p \) or \( z \). Hence \( v_{p,z,i} = u_{z,i} \), and thus

\[ f_{v_{p,z,i},z}(q) = f_{u_{z,i},z}(q) \]

for each \( i \), where \( i \) represents a bi-level of EFE(1) with respect to \( p \) and \( z \) on the left-hand side while \( i \) represents a level of \( f_z(q) \) on the right-hand side. For each line

\[ f_{v_{p,z,i},p}(q) f_{v_{p,z,i},z}(q^p) \xleftarrow{(i)} f_{v_{p,z,i},z}(q) f_{v_{p,z,i},p}(q^z) \]

of EFE(1) with respect to \( p \) and \( z \), we replace it by the line

\[ f_{v_{p,z,i},p}(q) f_{v_{p,z,i},r}(q^p) \xleftarrow{(i)} f_{v_{p,z,i},r}(q) f_{v_{p,z,i},p}(q^r) \]

where \( f_{v_{p,z,i},r}(q) = f_{u_{z,i},r}(q) \). We also replace line

\[ f_p(q) f_z(q^p) = f_z(q) f_p(q^z) \]

of EFE(1) with respect to \( p \) and \( z \) by the line

\[ f_p(q) f_r(q^p) = f_r(q) f_p(q^r). \]
Then it is straightforward to verify that the result is the EFE (1) with respect to $p$ and $r$. That is, $f_p(q)$ and $f_r(q)$ satisfy Functional Equation (1). □

Now suppose $P$ contains 2. Then

$$u = 2 \prod_{s \in P} s = \prod_{s \in P' := P \cup \{2\}} s.$$ 

Note that $\prod_{s \in P} s$ divides $p - 1$ for each odd prime $p$ in $P - P$ if and only if $2 \prod_{s \in P} s$ divides $p - 1$ for each odd prime $p$ in $P - P$. It can be verified that the same construction as above with $P'$ replacing $P$ also works.

(II) Let us prove the only if direction. Let $P$ be a set of primes. Suppose that $\Gamma := \{f_n(q) \mid n \in \mathbb{N}\}$ is a sequence of polynomials satisfying Functional Equation (2) with support base $P$ and field of coefficients strictly containing $\mathbb{Q}$. Let us assume the following:

- $|P| = \infty$.
- 4 does not divide $s - 1$ for all odd prime $s$ in $P$.
- There is no odd prime $r$ such that $r$ divides $s - 1$ for all odd primes $s$ in $P$ and there is no proper nonempty subset $A$ of $\mathbb{Z}/W\mathbb{Z}$, for some natural number $W$, with $sA = A$ for all odd primes $s$ in $P$.

To prove (II) of Theorem 2.1, we need to show that there exists a collection of odd primes $P = \{r_i\}$ of $P$ such that either at least one $r_i$ in $P$ divides $p - 1$ for all odd primes $p$ in $P - P$ or there exists a nonempty proper subset $A$ of $\mathbb{Z}/W\mathbb{Z}$, for some natural number $W$, with $pA = A$ for all odd primes $p$ in $P - P$.

Since the field of coefficients of $\Gamma$ strictly contains $\mathbb{Q}$, it can be verified using the same method as in the proof of Key Proposition 3 of [4] that the coefficients of each polynomial $f_s(q)$ in $\Gamma$ are not properly contained in $\mathbb{Q}$ if $s$ is in $P$. In particular, if $s$ is a prime in $P$ and

$$f_s(q) = \prod_i f_{u_{s,i},s}(q)$$

is its product decomposition as in the introduction, then there exists a level $i$ of $f_s(q)$ such that the coefficients of $f_{u_{s,i},s}(q)$ are not properly contained in $\mathbb{Q}$. Let $i_s$ be the smallest such level for each prime $s$ in $P$.

Let $p_1$ and $p_2$ be two primes in $P$. Let $f_{p_1}(q)$ and $f_{p_2}(q)$ be the corresponding polynomials in $\Gamma$ with product decompositions

$$f_{p_1}(q) = \prod_i f_{u_{p_1,i},p_1}(q)$$

and

$$f_{p_1}(q) = \prod_j f_{u_{p_2,j},p_2}(q).$$

Let

$$V_{p_1, p_2} := \{v_{p_1, p_2, l} \mid v_{p_1, p_2, l} > v_{p_1, p_2, l+1}\} = \{u_{p_1, i_l} \cup \{u_{p_2, j}\}_j$$
and

\[ V := \bigcup_{p_n, p_m \in \mathcal{P}} V_{p_n, p_m}. \]

Let \( \mathcal{U} \) be the collection of all prime factors of all elements of \( V \). By Key Proposition 3 of [4],

\[ |\mathcal{U}| < \infty. \]

Therefore, there exist infinitely many primes in \( \mathcal{P} \) which are not in \( \mathcal{U} \). Let \( p \) be a prime in \( \mathcal{P} \) such that \( p \) is greater than all primes in \( \mathcal{U} \) and let \( r \) be any prime in \( \mathcal{P} \). Let us consider EFE(1) with respect to \( p \) and \( r \),

\[
\frac{f_{v, p, r, p}(q)^{\delta_{v, p, r}} f_{v, p, r, r}(q^{p})^{-1}}{f_{v, p, r, r}(q)} \xrightarrow{f_{v, p, r, p}(q^{p})} \frac{f_{v, p, r, p}(q)^{\delta_{v, p, r}} f_{v, p, r, r}(q^{p})^{-1}}{f_{v, p, r, r}(q)}.
\]

By Key Proposition 3 of [4], there exists a bi-level \( k_{p, r} \) of EFE(1) with respect to \( p \) and \( r \) such that \( v_{p, r, k_{p, r}} = u_{p, i_p} = u_{r, i_r} \) and \( u_{p, k_{p, r}} \) and \( u_{r, k_{p, r}} \) are the values of the bi-level \( k_{p, r} \) and the level \( i_{p, r} \) respectively, where \( \square \) denotes either \( p \) or \( r \). Hence \( s_{p, k_{p, r}} = s_{r, k_{p, r}} = 1 \). Since \( p \) is not in \( \mathcal{U} \), \( p \) does not divide \( v_{p, r, k_{p, r}} \) and thus \( \delta_{p, k_{p, r}} = 0 \). As a result, line \((k_{p, r})\) of the reduced form of EFE(1) with respect to \( p \) and \( r \) has the form

\[
\frac{f_{v, p, r, k_{p, r}, p}(q^{p})}{f_{v, p, r, k_{p, r}, r}(q)} \xrightarrow{f_{v, p, r, k_{p, r}, r}(q)} \frac{f_{v, p, r, k_{p, r}, p}(q^{p})}{f_{v, p, r, k_{p, r}, r}(q)}.
\]

where \( \delta_{r, k_{p, r}} = 1 \) if \( r \) divides \( v_{p, r, k_{p, r}} \) and \( \delta_{r, k_{p, r}} = 0 \) otherwise. By part (i) of Key Proposition 1’ of [4],

\[
\frac{f_{v, p, r, k_{p, r}, p}(q^{p})}{f_{v, p, r, k_{p, r}, r}(q)}
\]

is a polynomial. Let \( v_{p, r, k_{p, r}} = \prod_{i} t_{i}^{n_{i}} \) be the prime factorization of \( v_{p, r, k_{p, r}} \). Since the coefficients of \( f_{v, p, r, k_{p, r}, r}(q) = f_{u, v}(q) \) are not properly contained in \( \mathbb{Q} \) by definition of \( i_{p, r} \), Key Propositions 1 and 1’ of [4] imply that either \( p \equiv 1 \) (mod \( p_{p, r, k_{p, r}} \)) and thus every prime factor \( r_{i} \) of \( v_{p, r, k_{p, r}} \) divides \( p - 1 \) or there exists a nonempty proper subset \( \mathcal{A} \) of \( \mathbb{Z}/v_{p, r, k_{p, r}, r}(\mathbb{Z})^{*} \) such that \( p, \mathcal{A} = \mathcal{A} \).

**Remark 3.7.** Key Proposition 1 of [2] (a version of Key Proposition 3 of [4] which does not require that \( p \) is not in \( \mathcal{U} \)) guarantees that there exists a natural number \( L \) such that \( L = v_{s, t, k_{s, t}} = u_{s, i_s} = u_{t, i_t} \) for all primes \( s \) and \( t \) in \( \mathcal{P} \). Hence \( s_{s, k_{s, t}} = s_{t, k_{s, t}} = 1 \) for all primes \( s \) and \( t \) in \( \mathcal{P} \) as well. Consequently, the argument for \( p \) above applies to every prime \( t \) in \( \mathcal{P} \), which does not divide \( L \).

**Proposition 3.8** (Key Proposition 5). Let \( p \) and \( r \) be two primes in \( \mathcal{P} \) with \( p < r \). Suppose \( (pr, L) = 1 \). Then line \((k_{p, r})\) of the \((k_{p, r} - 1)\)-super-reduced form of EFE(1) with respect to \( p \) and \( r \) has the form

\[
\frac{f_{v, p, r, k_{p, r}, p}(q^{p})^{k_{p, r}}}{f_{v, p, r, k_{p, r}, r}(q)} \xrightarrow{f_{v, p, r, k_{p, r}, r}(q)} \frac{f_{v, p, r, k_{p, r}, p}(q^{p})^{k_{p, r}}}{f_{v, p, r, k_{p, r}, r}(q)}.
\]
Proof. Since \((pr, L) = 1\), \(\delta_{p,kp,r} = \delta_{r,kp,r} = 0\). In addition, we also know that \(s_{p,kp,r} = s_{r,kp,r} = 1\) by Key Proposition 1 of [4]. Thus line \((k_{p,r})\) of the reduced form of EFE(1) with respect to \(p\) and \(r\) has the form

\[
\frac{f_{v_{p,r,kp,r},r}(q^p)}{f_{v_{p,r,kp,r},r}(q)} \rightarrow \frac{f_{v_{p,r,kp,r},p}(q^r)}{f_{v_{p,r,kp,r},p}(q)}.
\]

It can be verified that there are three possibilities:

- \(f_{v_{p,r,kp,r},r}(q)\) is semi-directly related to \(f_{v_{p,r,kp,lp},p}(q)\) for some bi-level \(lp < kp,r\). If this occurs, then it can be verified that \(v_{p,r,kp,r} = v_{p,r,lp}\) and line \((k_{p,r})\) of the \(kp,r\)-super-reduced form of EFE(1) with respect to \(p\) and \(r\) has the form

\[
\frac{f_{v_{p,r,kp,r},r}(q^p)}{f_{v_{p,r,kp,r},r}(q)} \rightarrow \frac{f_{v_{p,r,kp,lp},p}(q^r)}{f_{v_{p,r,kp,lp},p}(q)}.
\]

- \(f_{v_{p,r,kp,r},p}(q)\) is semi-directly related to \(f_{v_{p,r,lr},r}(q)\) for some bi-level \(lr < kp,r\). If this case occurs, then it can be verified that \(v_{p,r,kp,r} = v_{p,r,lr}\) and line \((k_{p,r})\) of the \(kp,r\)-super-reduced form of EFE(1) with respect to \(p\) and \(r\) has the form

\[
\frac{f_{v_{p,r,kp,r},r}(q^p)}{f_{v_{p,r,kp,r},r}(q)} \rightarrow \frac{f_{v_{p,r,lr},r}(q)}{f_{v_{p,r,lr},r}(q)}.
\]

- There exist bi-levels \(lp < kp,r\) and \(lr < kp,r\) such that \(f_{v_{p,r,lp},p}(q)\) is indirectly related to an ordered pair of polynomials

\[
(f_{v_{p,r,lp},r}(q), f_{v_{p,r,kp,lp},p}(q)).
\]

If this case occurs, then it can be verified that \(v_{p,r,kp,r} = v_{p,r,lp}\), \(v_{p,r,kp,lp} = v_{p,r,lp}\) and line \((k_{p,r})\) of the \(kp,r\)-super-reduced form of EFE(1) with respect to \(p\) and \(r\) has the form

\[
\frac{f_{v_{p,r,lp},p}(q^p)}{f_{v_{p,r,lp},p}(q)} \rightarrow \frac{f_{v_{p,r,lp},r}(q^r)}{f_{v_{p,r,lp},r}(q)}.
\]

Therefore, the result follows. \(\square\)

Let \(p\) and \(r\) be two primes in \(P\) not dividing \(L\). It can be verified from line \((k_{p,r})\) of the \((k_{p,r} - 1)\)-super-reduced form of EFE(1) with respect to \(p\) and \(r\) as described in Key Proposition 1 that

\[
f_{v_{p,lr},r}(q)^{f_{p,lp}} f_{v_{p,r,kp,lr},r}(q^p) f_{v_{p,r,kp,lr},p}(q^r) = f_{v_{p,r,lr},r}(q)^{t_{lr}} f_{v_{p,r,lr},p}(q^r).
\]
since \( f_{v_{p,r},lp,p}(q)^{lp,p} \) is the factor of \( f_p(q)f_r(q^p) \) where \( \tau_p(q) \) whose roots are all the roots of \( f_p(q)f_r(q^p) \) which are primitive \( L_{pr} \)-roots of unity.

By [4] and the definition of \( k_{p,r} \), there exists an integer \( n_{v_{p,r},i,\Box} \) such that

\[
f_{v_{p,r},i,\Box}(q) = (P_{v_{p,r},i,\Box}(q))^{n_{v_{p,r},i,\Box}}
\]

for each bi-level \( i < k_{p,r} \), where \( P_{v_{p,r},i,\Box}(q) \) is the cyclotomic polynomial of order \( v_{p,r,i,\Box} \) with coefficients in \( \mathbb{Q} \), and \( \Box \) denotes either \( p \) or \( r \). In addition, it can be verified that

\[
P_{v_{p,r},i,\Box}(q) = \begin{cases} 
\frac{P_{v_{p,r},i,\Box}(q)}{\Delta} & \text{if } \Box \text{ divides } \frac{v_{p,r,i}}{\Delta}, \\
\frac{P_{v_{p,r},i,\Box}(q)}{\Delta} & \text{otherwise,}
\end{cases}
\]

where \( \Delta \) denotes \( r \) if \( \Box = p \) and vice versa and \( \frac{P_{v_{p,r},i,\Box}}{\Delta} \) is the cyclotomic polynomials of order \( \frac{v_{p,r,i}}{\Delta} \) with coefficients in \( \mathbb{Q} \) (see [4] for more details). Therefore,

\[
f_{v_{p,r},lp,p}(q)^{lp,p} = (P_{v_{p,r},lp,p}(q)^{lp,p})^{n_{v_{p,r},lp,p}}
\]

where

\[
(P_{v_{p,r},lp,p}(q)^{lp,p})^{n_{v_{p,r},lp,p}} = \begin{cases} 
(P_{v_{p,r},lp,p}(q)^{lp,p})^{n_{v_{p,r},lp,p}} & \text{if } p \text{ divides } \frac{v_{p,r,lp}}{r}, \\
(P_{v_{p,r,lp,p},pr}(q)^{lp,p})^{n_{v_{p,r,lp,p}}} & \text{otherwise,}
\end{cases}
\]

and

\[
f_{v_{p,r},lr,r}(q)^{lr,r} = (P_{v_{p,r,lr,r}}(q)^{lr,r})^{n_{v_{p,r,lr,r}}}
\]

where

\[
(P_{v_{p,r,lr,r}}(q)^{lr,r})^{n_{v_{p,r,lr,r}}} = \begin{cases} 
(P_{v_{p,r,lr,r}}(q)^{lr,r})^{n_{v_{p,r,lr,r}}} & \text{if } r \text{ divides } \frac{v_{p,r,lr}}{p}, \\
(P_{v_{p,r,lr,r}}(q)^{lr,r})^{n_{v_{p,r,lr,r}}} & \text{otherwise.}
\end{cases}
\]

Since \( pr \) is relatively prime to \( v_{p,r,k_{p,r}} = L \) by assumption and

\[
v_{p,r,k_{p,r}} = \frac{v_{p,r,lp}}{r} = \frac{v_{p,r,lp}}{p},
\]

we have

\[
f_{v_{p,r},lp,p}(q)^{lp,p} = \frac{P_{v_{p,r,lp,p},pr}(q)^{lp,p}}{(P_{v_{p,r,lp,p},pr}(q)^{lp,p})^{n_{v_{p,r,lp,p}}} (P_{v_{p,r,lp,p},pr}(q)^{lp,p})^{n_{v_{p,r,lp,p}}}}
\]
Remark 3.10. (the details are left to the readers) with and thus every prime factor such that \( f_{vp} \) replacing \( f_{vp} \) and \( f_{vp} \) replacing \( f_{vp} \). This follows from the same argument as in the proof of part (3) of Key Proposition 1. Therefore,}

\[
\frac{(P_{vp,r,kp,r}'(q)^{f_{r,kp,r}})^{n_{r,kp,r}} f_{v_{p,r,kp,r}}(q)}{(P_{vp,r,kp,r}'(q)^{f_{r,kp,r}})^{n_{r,kp,r}} f_{v_{p,r,kp,r}}(q)} = \frac{(P_{vp,r,kp,r}'(q)^{f_{r,kp,r}})^{n_{r,kp,r}} f_{v_{p,r,kp,r}}(q)}{(P_{vp,r,kp,r}'(q)^{f_{r,kp,r}})^{n_{r,kp,r}} f_{v_{p,r,kp,r}}(q)}.
\]

**Proposition 3.9 (Key Proposition 6).**

\[
(P_{vp,r,kp,r}'(q)^{f_{r,kp,r}})^{n_{r,kp,r}} f_{v_{p,r,kp,r}}(q)
\]

and

\[
(P_{vp,r,kp,r}'(q)^{f_{r,kp,r}})^{n_{r,kp,r}} f_{v_{p,r,kp,r}}(q)
\]

are super-compatible.

**Proof.** This follows from the same argument as in the proof of part (3) of Key Proposition 1′ of [4] (the details are left to the readers) with

\[
(P_{vp,r,kp,r}'(q)^{f_{r,kp,r}})^{n_{r,kp,r}} f_{v_{p,r,kp,r}}(q)
\]

and

\[
(P_{vp,r,kp,r}'(q)^{f_{r,kp,r}})^{n_{r,kp,r}} f_{v_{p,r,kp,r}}(q)
\]

replacing \( f_{v_{p,r,1}}(q) \) and \( f_{v_{p,r,1}}(q) \) respectively. □

Let \( \mathcal{P}_0 \) be the collection of all prime factors of \( v_{p,r,kp,r} = L \). There are two cases to consider:

1. \( \mathcal{P}_0 \cap P = \emptyset \).
2. \( \mathcal{P}_0 \cap P \neq \emptyset \).

Suppose (1) occurs. Then \( t \) does not divide \( L \) for all primes \( t \) in \( P \). By using the same argument immediately above Remark 3.7 applied to \( p \), with \( t \) replacing \( p \), and Remark 3.7, either \( t \equiv 1 \mod L \) and thus every prime factor \( r_i \) of \( L \) divides \( t - 1 \) for all primes \( t \) in \( P \) or there exists nonempty proper subset \( \mathcal{A} \) of \((\mathbb{Z}/L\mathbb{Z})^*\) such that \( t.A = \mathcal{A} \) for all primes \( t \) in \( P \) and thus for all odd primes \( t \) in \( P \).

**Remark 3.10.** Note that we also have either \( t \equiv 1 \mod L \) and thus every prime factor \( r_i \) of \( L \) divides \( t - 1 \) for each odd prime \( t \) in \( P - (\mathcal{P}_0 \cap P) \) or there exists a nonempty proper subset \( \mathcal{A} \) of \((\mathbb{Z}/L\mathbb{Z})^*\) such that \( t.A = \mathcal{A} \) for each odd prime \( t \) in \( P - (\mathcal{P}_0 \cap P) \) by the same argument above.
Let $p$ and $r$ be two primes not dividing $L$ and let

$$L = \prod_{i} 2^{\epsilon_i} r_i^{n_i}$$

be the prime factorization of $L$ where $\epsilon$ is a nonnegative integer. Then the super-compatibility of

$$(P_{v_{p,r,k_p,r},r}(q))^{t_{p,r}} (P_{v_{p,r,k_p,r}}(q))^{r_{p,r}} f_{v_{p,r,k_p,r},r}(q)$$

and

$$(P_{v_{p,r,k_p,r},p}(q))^{t_{p,r}} (P_{v_{p,r,k_p,r}}(q))^{r_{p,r}} f_{v_{p,r,k_p,r},p}(q)$$

implies that $L > 1$ by the same argument as in Key Proposition 5 of [4], with $(P_{v_{p,r,k_p,r},r}(q))^{t_{p,r}} (P_{v_{p,r,k_p,r}}(q))^{r_{p,r}} f_{v_{p,r,k_p,r},r}(q)$ and $(P_{v_{p,r,k_p,r},p}(q))^{t_{p,r}} (P_{v_{p,r,k_p,r}}(q))^{r_{p,r}} f_{v_{p,r,k_p,r},p}(q)$ replacing $f_{v_{p,r,k_p,r},r}(q)$ and $f_{v_{p,r,k_p,r},r}(q)$. If $n_i > 0$ for at least one $i$ in the factorization of $L$, then it can be verified from Key Propositions 1 and 1' of [4] that either there exists at least one such odd prime, say $r_i$ with $n_i > 0$, such that $r_i$ divides $t - 1$ for all odd primes $t$ in $P$ or there exists a nonempty proper subset $A$ of $(\mathbb{Z}/L\mathbb{Z})^*$ such that $tA = A$ for each prime $t$ and thus for each odd prime $t$ in $P$, which contradicts our assumption. Thus $n_i = 0$ for all $i$. If $\epsilon > 1$, then Key Propositions 1 and 1' of [4] imply that either 4 divides $t - 1$ for all odd primes $t$ in $P$ or there exists a nonempty proper subset $A$ of $(\mathbb{Z}/4\mathbb{Z})^*$ with $tA = A$ for all primes $t$ and thus for all odd primes $t$ in $P$. This also contradicts our assumption. Hence $\epsilon \leq 1$.

The only possibility therefore is $L = 2$. There are two cases to consider when $L = 2$: (i) $k_{p,r} = 1$; (ii) $k_{p,r} > 1$.

If (i) occurs, then $f_{v_{p,r,k_p,r},p}(q)$ and $f_{v_{p,r,k_p,r},r}(q)$ are super-compatible by Key Proposition 1' of [4]. As a result, by using the same argument as in the conclusion of the proof of Theorem 2.1 of [4], it can be verified that this is impossible since the coefficients of $f_{v_{p,r,k_p,r},p}(q)$ and $f_{v_{p,r,k_p,r},r}(q)$ are not properly contained in $\mathbb{Q}$.

Let us suppose that (ii) occurs. Pick two primes $p$ and $r$ not in $\mathcal{U}$ such that $p < r$. Then it follows from the definition of $\mathcal{U}$ that $(pr, L) = 1$. Then

$$(P_{v_{p,r,k_p,r},r}(q))^{t_{p,r}} (P_{v_{p,r,k_p,r}}(q))^{r_{p,r}} f_{v_{p,r,k_p,r},r}(q)$$

and

$$(P_{v_{p,r,k_p,r},p}(q))^{t_{p,r}} (P_{v_{p,r,k_p,r}}(q))^{r_{p,r}} f_{v_{p,r,k_p,r},p}(q)$$

are super-compatible by Key Proposition 6. Since the coefficients of $f_{v_{p,r,k_p,r},r}(q)$ and $f_{v_{p,r,k_p,r},p}(q)$ are not properly contained in $\mathbb{Q}$, the coefficients of

$$(P_{v_{p,r,k_p,r},r}(q))^{t_{p,r}} (P_{v_{p,r,k_p,r}}(q))^{r_{p,r}} f_{v_{p,r,k_p,r},r}(q)$$

and

$$(P_{v_{p,r,k_p,r},p}(q))^{t_{p,r}} (P_{v_{p,r,k_p,r}}(q))^{r_{p,r}} f_{v_{p,r,k_p,r},p}(q)$$

are not properly contained in $\mathbb{Q}$ either.
As \( v_{p,r,k,p,r} = L = 2 \), there exists a subset \( \mathcal{L}_2 \) of \( ((\mathbb{Z}/2\mathbb{Z})^*)^T \), for some positive integer \( T \), such that roots of

\[
(P_{v_{p,r,k,p,r},p}(q)^{t_{r,l,r}})^{n_{v_{p,r,k,p,r},p}} f_{v_{p,r,k,p,r},p}(q) = (P_{2,p}(q)^{t_{r,l,r}})^{n_{v_{p,r,k,p,r},p}} f_{2,p}(q)
\]

and

\[
(P_{v_{p,r,k,p,r},r}(q)^{t_{p,l,p}})^{n_{v_{p,r,k,p,r},r}} f_{v_{p,r,k,p,r},r}(q) = (P_{2,r}(q)^{t_{p,l,p}})^{n_{v_{p,r,k,p,r},r}} f_{2,r}(q)
\]

are represented by the collection of tuples

\[
\bigcup_{\alpha \in \mathcal{L}_2} \{\alpha\} \times (\mathbb{Z}/p\mathbb{Z})^*
\]

and

\[
\bigcup_{\alpha \in \mathcal{L}_2} \{\alpha\} \times (\mathbb{Z}/r\mathbb{Z})^*
\]

respectively.

Since \((\mathbb{Z}/2\mathbb{Z})^* = \{1\}\),

\[
\mathcal{L}_2 = (\mathbb{Z}/2\mathbb{Z})^* T'
\]

for some integer \( T' \leq T \). It can be verified that the monic polynomial whose roots are primitive \( 2p \)-roots of unity and the monic polynomial whose roots are primitive \( 2r \)-roots of unity represented by the collection of tuples

\[
\bigcup_{\alpha \in (\mathbb{Z}/2\mathbb{Z})^*} \{\alpha\} \times (\mathbb{Z}/p\mathbb{Z})^*
\]

and

\[
\bigcup_{\alpha \in (\mathbb{Z}/2\mathbb{Z})^*} \{\alpha\} \times (\mathbb{Z}/r\mathbb{Z})^*
\]

respectively are the cyclotomic polynomial, with coefficients in \( \mathbb{Q} \) of order \( 2p \), \( P_{2p}(q) \) and the cyclotomic polynomial, with coefficients in \( \mathbb{Q} \) of order \( 2r \), \( P_{2r}(q) \). As a result,

\[
(P_{v_{p,r,k,p,r},p}(q)^{t_{r,l,r}})^{n_{v_{p,r,k,p,r},p}} f_{v_{p,r,k,p,r},p}(q) = (P_{2,p}(q)^{t_{r,l,r}})^{n_{v_{p,r,k,p,r},p}} f_{2,p}(q)^{T'}
\]

and

\[
(P_{v_{p,r,k,p,r},r}(q)^{t_{p,l,p}})^{n_{v_{p,r,k,p,r},r}} f_{v_{p,r,k,p,r},r}(q) = (P_{2,r}(q)^{t_{p,l,p}})^{n_{v_{p,r,k,p,r},r}} f_{2,r}(q)^{T'}.
\]

Hence their coefficients are properly contained in \( \mathbb{Q} \). This is a contradiction and thus case (ii) cannot occur either. Therefore,

\[
\mathcal{P}_0 \cap \mathcal{P} \neq \emptyset.
\]
It also follows from above that $L > 2$, and thus $L$ is divisible by at least one odd prime. Then it follows that either at least one of these prime divisors of $L$, say $r_i$, divides $s - 1$ for all odd primes $s$ in $P - (P_0 \cap P)$ or there exists a nonempty proper subset $A$ of $(\mathbb{Z}/L\mathbb{Z})^*$ such that $sA = A$ for all primes $s$ in $P - (P_0 \cap P)$ and thus for all odd primes $s$ in $P - (P_0 \cap P)$ by Remark 3.10.

If $P_0 \cap P = \{2\}$, then either there exists at least one odd prime $r_i$ in $P_0$ such that $r_i$ divides $s - 1$ for each odd prime $s$ in $P$ or there exists a nonempty proper subset $A$ of $(\mathbb{Z}/L\mathbb{Z})^*$ such that $sA = A$ for each odd prime $s$ in $P$ which contradicts our assumption made earlier. Therefore, $P_0 \cap P$ contains at least one odd prime.

Define

$$\mathcal{P} := \begin{cases} P_0 \cap P & \text{if } P \text{ does not contain 2}, \\ P_0 \cap (P - \{2\}) & \text{otherwise.} \end{cases}$$

Then $\mathcal{P}$ is a nonempty set of odd primes such that either at least one prime $r_i$ in $\mathcal{P}$ divides $s - 1$ for each odd prime $s$ in $P - \mathcal{P}$ or there exists a nonempty proper subset $A$ of $(\mathbb{Z}/L\mathbb{Z})^*$ such that $sA = A$ for each odd prime $s$ in $P - \mathcal{P}$ by Remark 3.10. The proof of Theorem 2.1 is thus complete. □

**Proof of Corollary 2.2.** Let $\Gamma$ be a sequence of polynomials satisfying Functional Equation (2) with support base $P$ and field of coefficients of characteristic zero. Suppose that $P$ has finite complement, i.e. all but a finite number of primes are in $P$. Suppose that $\Gamma$ is not generated by quantum integers. Then the field of coefficients of $\Gamma$ strictly contains $\mathbb{Q}$ by Theorem 2.1 of [4]. Therefore, $P$ must satisfy at least one of the criterions of Theorem 2.1, namely criterions (2), (3), and (4) since $|P| = \infty$.

If $P$ satisfies criterion (2) of Theorem 2.1, let define

$$\Sigma_1 := \{4k + 1 \mid k \in \mathbb{N}\}$$

and

$$\Sigma_2 := \{4k + 3 \mid k \in \mathbb{N}\}.$$ 

Then

$$\Sigma_1 \cap \Sigma_2 = \emptyset.$$ 

Moreover, each of the sequences $\Sigma_1$ and $\Sigma_2$ contains infinitely many primes by Dirichlet’s Theorem concerning primes in Arithmetic Progression. Since $P$ contains all but finitely many primes,

$$|P \cap \Sigma_i| = \infty$$

for $i = 1, 2$. In particular, there exists a prime, say $w$, such that $w \in P \cap \Sigma_2$. This contradicts criterion (2) of Theorem 2.1.

If $P$ satisfies criterion (3) of Theorem 2.1 and if $r$ divides $p - 1$ for all primes $p$ in $P$, then define

$$\Upsilon_1 := \{rk + 1 \mid k \in \mathbb{N}\}$$

and

$$\Upsilon_2 := \{rk + r - 1 \mid k \in \mathbb{N}\},$$

where $r$ is the odd prime mention in the statement of criterion (3). By applying the same argument as in the case where $P$ satisfies criterion (2) of Theorem 2.1, the result follows. If $r$ does not necessarily
divide \( p - 1 \) for all odd primes \( p \) in \( P \) while there exists a nonempty proper subset \( \mathcal{A} \) of \((\mathbb{Z}/W\mathbb{Z})^*\), for some natural number \( W \), such that \( p_\mathcal{A} = \mathcal{A} \) for all odd primes \( p \) in \( P \), then it can be verified from [4] that \( p_\mathcal{A} = \mathcal{A} \) for all primes \( p \) which is impossible by [4].

Finally, suppose \( P \) satisfies criterion (4) for some sub-collection of odd primes \( \mathcal{P} \) of \( P \). Let us define the following collections of natural numbers

\[
\Lambda_1 := \{ r_1 \ldots r_n k + 1 \mid k \in \mathbb{N}, \ r_i \in \mathcal{P} \}
\]

and

\[
\Lambda_2 := \{ r_1 \ldots r_n k + r_1 \ldots r_n - 1 \mid k \in \mathbb{N}, \ r_i \in \mathcal{P} \}
\]

if at least one \( r_i \) divides \( p - 1 \) for all odd primes \( p \) in \( P - \mathcal{P} \). Then the same argument as in the two previous cases also holds. If no \( r_i \) divides \( p - 1 \) for all odd primes \( p \) in \( P - \mathcal{P} \) while there exists a nonempty proper subset \( \mathcal{A} \) of \((\mathbb{Z}/W\mathbb{Z})^*\), for some natural number \( W \), such that \( p_\mathcal{A} = \mathcal{A} \) for all odd primes \( p \) in \( P - \mathcal{P} \), then [4] implies that \( p_\mathcal{A} = \mathcal{A} \) for all primes \( p \) which is impossible by [4]. Therefore, \( \Gamma \) must be generated by quantum integers. \( \square \)

References


