Classification of Cubic Tricirculant Nut Graphs

Ivan Damnjanović[a,b] Nino Bašić[c,d,e] Tomaž Pisanski[c,d,e] Arjana Žitnik[e,f]

Submitted: Dec 22, 2023; Accepted: Apr 27, 2024; Published: May 17, 2024

Abstract

A nut graph is a simple graph whose adjacency matrix has the eigenvalue zero with multiplicity one such that its corresponding eigenvector has no zero entries. It is known that there exist no cubic circulant nut graphs. A bicirculant (resp. tricirculant) graph is defined as a graph that admits a cyclic group of automorphisms having two (resp. three) orbits of vertices of equal size. We show that there exist no cubic bicirculant nut graphs and we provide a full classification of cubic tricirculant nut graphs.

Mathematics Subject Classifications: 05C50, 11C08, 12D05

1 Introduction

A *nut graph* is a graph of nullity one whose null space is spanned by a full vector, i.e., a vector with no zero entries. Nut graphs were introduced and studied by Sciriha and Gutman [19–22, 28]. Some of their properties were further investigated in [9, 12, 23, 24]. Moreover, the chemical justification for studying such graphs can be found in [2, 10, 11, 26, 27] and many other results concerning them are to be found in the monograph [25].

The problem of the existence of regular nut graphs on a given number of vertices and a given degree was first considered in [9], where it was solved for degrees up to 11. In [1] the degree was extended to 12 using circulant graphs in a clever way.

In a series of papers [4, 5, 7], Damnjanović and Stevanović completely resolved the problem of existence of circulant nut graphs of given degree and order by establishing the following result.

[a] Faculty of Electronic Engineering, University of Niš, Niš, Serbia (ivan.damnjanovic@elfak.ni.ac.rs).
[b] Diffine LLC, San Diego, California, U.S.A.
[c] FAMNIT, University of Primorska, Koper, Slovenia (nino.basic@famnit.upr.si, pisanski@upr.si).
[d] IAM, University of Primorska, Koper, Slovenia.
[e] Institute of Mathematics, Physics and Mechanics, Ljubljana, Slovenia.
[f] Faculty of Mathematics and Physics, University of Ljubljana, Ljubljana, Slovenia (arjana.zitnik@fmf.uni-lj.si).

Theorem 1 ([5, Theorem 5]). *Let d and n be nonnegative integers. Then there exists a d-regular circulant nut graph of order n if and only if $d > 0$, $4 \mid d$, $2 \mid n$, together with $n \geqslant d + 4$ if $d \equiv_8 4$, and $n \geqslant d + 6$ if $8 \mid d$, as well as $(n, d) \neq (16, 8)$.*

From Theorem 1 it follows that there are no cubic circulant nut graphs and that there exists a quartic circulant nut graph of every even order $n \geqslant 8$. Moreover, the full characterization of quartic circulant nut graphs can be found in [6].

One can generalize the concept of a circulant graph by taking into consideration the so-called *bicirculant* (resp. *tricirculant*) graphs, which are the graphs that admit a cyclic group of automorphisms having two (resp. three) orbits of vertices of equal size [14, 16]. In this paper we show that there exist no cubic bicirculant nut graphs. While there are no cubic circulant and bicirculant graphs, there exist cubic tricirculant graphs. We give a complete classification of these graphs. Below is a more detailed description of our classification. We also note that the quartic bicirculant nut graphs are currently being investigated [17].

For convenience, we will suppose that the vertex set of each tricirculant graph of order $3n$ is given via $X \cup Y \cup Z$, where

$$X = \{x_0, x_1, \ldots, x_{n-1}\}, \qquad Y = \{y_0, y_1, \ldots, y_{n-1}\}, \qquad Z = \{z_0, z_1, \ldots, z_{n-1}\},$$

and that there exists an automorphism which maps x_j to x_{j+1}, y_j to y_{j+1} and z_j to z_{j+1}, for each $j \in \mathbb{Z}_n$. If G is an arbitrary cubic tricirculant graph of order $3n$, it is then clear that n is necessarily even. Moreover, as observed by Potočnik and Toledo [18, Theorem 2.4], it can be shown that if G is connected, then it must be isomorphic to a graph that belongs to at least one of the next four families:

(i) $T_1(n, a, b)$, $0 \leqslant a < b < n$;

(ii) $T_2(n, a, b)$, $0 < a < n$, $0 < b < \frac{n}{2}$;

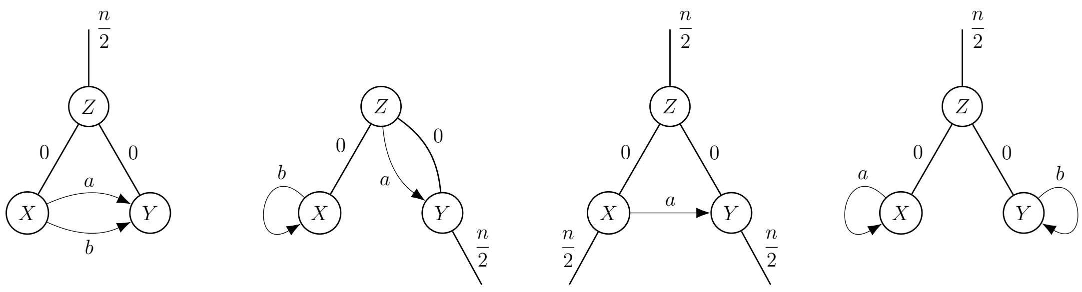
(iii) $T_3(n, a)$, $0 \leqslant a < n$;

(iv) $T_4(n, a, b)$, $0 < a \leqslant b < \frac{n}{2}$;

whose elements can be defined via their edge sets as follows:

$$\begin{aligned}
E(T_1(n, a, b)) &= \{x_j y_{j+a},\, x_j y_{j+b},\, x_j z_j,\, y_j z_j,\, z_j z_{j+\frac{n}{2}} \mid j \in \mathbb{Z}_n\},\\
E(T_2(n, a, b)) &= \{x_j x_{j+b},\, x_j z_j,\, y_j y_{j+\frac{n}{2}},\, y_j z_j,\, y_j z_{j-a} \mid j \in \mathbb{Z}_n\},\\
E(T_3(n, a)) &= \{x_j x_{j+\frac{n}{2}},\, x_j y_{j+a},\, x_j z_j,\, y_j y_{j+\frac{n}{2}},\, y_j z_j,\, z_j z_{j+\frac{n}{2}} \mid j \in \mathbb{Z}_n\},\\
E(T_4(n, a, b)) &= \{x_j x_{j+a},\, x_j z_j,\, y_j y_{j+b},\, y_j z_j,\, z_j z_{j+\frac{n}{2}} \mid j \in \mathbb{Z}_n\}.
\end{aligned}$$

For brevity, if a cubic tricirculant graph is isomorphic to at least one element from the T_j family, we will then say that such a graph is of *type* j, for each $j = 1, 2, 3, 4$. Note that in principle, a cubic tricirculant could be of more than one type. However, every vertex-transitive cubic tricirculant is of type j for exactly one $j \in \{1, 2, 3, 4\}$, with the exception of the triangular prism which is both of type 1 as well as of type 3 [18]. The above definitions can be concisely visualized in the form of Figure 1. Here, we may note that this figure actually formally represents the *voltage graphs* corresponding to the cubic tricirculants [18].



(a) Type 1 (b) Type 2 (c) Type 3 (d) Type 4

Figure 1: Voltage graphs for the cubic tricirculant graphs of types 1, 2, 3 and 4.

Finally, for each $x \in \mathbb{Z}$, $x \neq 0$, let $v_2(x)$ denote the power of two in the prime factorization of $|x|$, i.e., the unique $\beta \in \mathbb{N}_0$ such that $2^\beta \mid x$, but $2^{\beta+1} \nmid x$. We now state our main theorem.

Theorem 2 (Tricirculant cubic nut graph classification)**.** *A tricirculant cubic graph is a nut graph if and only if it is representable as a* $T_1(n, a, b)$, $2 \mid n$, $0 \leqslant a < b < n$ *such that*

(i) $\gcd\left(\frac{n}{2}, a\right) = \gcd\left(\frac{n}{2}, b\right) = 1$;

(ii) $a \not\equiv_2 \frac{n}{2}$ *and* $b \not\equiv_2 \frac{n}{2}$;

(iii) $v_2(b-a) \geqslant v_2(n)$;

or as a $T_4(n, a, b)$, $2 \mid n$, $0 < a \leqslant b < \frac{n}{2}$ *where*

(iv) $\gcd\left(\frac{n}{2}, a, b\right) = 1$;

(v) *if* $4 \nmid n$, *then at least one of* a *and* b *is even;*

(vi) *if* $4 \mid n$, *then* a *and* b *are of different parities;*

(vii) *if* $10 \mid n$, *then at least one of* $a, b, a-b, a+b$ *is divisible by five.*

Remark 3. Condition **(iv)** from Theorem 2 is actually equivalent to $T_4(n, a, b)$ being a connected graph (see, for example, [18, Theorem 2.4]). Moreover, condition **(i)** also implies that $T_1(n, a, b)$ is surely connected.

The rest of the paper will focus on providing the full proof of Theorem 2. Bearing this in mind, its structure shall be organized as follows. Section 2 will serve to preview certain theoretical results to be used throughout the remaining sections. Afterwards, we will use Section 3 to show that no cubic bicirculant graph can be a nut graph and in Section 4 we will take into consideration an arbitrary tricirculant cubic nut graph and demonstrate that it is necessarily of type 1 or of type 4. Afterwards, Section 5 will be used to obtain the precise conditions that a type 1 graph should satisfy in order to be a nut graph. Finally, we shall determine all the type 4 nut graphs in Section 6, thereby completing the proof of Theorem 2.

2 Preliminaries

In this section we review some known theoretical results from various fields of mathematics which will be used later on throughout the remaining sections. First of all, recall that $\eta(G)$ denotes the *nullity* of G, i.e., the nullity of the adjacency matrix of the graph G. Similarly, we will use $\mathcal{N}(A_G)$ to denote the null space of G. We also note that the eigenvectors corresponding to the eigenvalue zero are also called the *kernel vectors* and may be characterized via the following lemma.

Lemma 4. *Let G be a graph and let $u \in \mathbb{R}^{V_G}$ be a nonzero vector. Then u is an eigenvector corresponding to the eigenvalue zero if and only if for every vertex x of G the following holds:*

$$\sum_{y \sim x} u(y) = 0.$$

Proof. Multiply the row of the adjacency matrix of G, corresponding to the vertex x, by the eigenvector u, and the result is obtained. □

Here, we shall call the above condition that a kernel vector must satisfy the *local condition*. We now recall some basic properties of nut graphs, see [28].

Lemma 5. *Every nut graph is connected.*

Lemma 6. *A bipartite graph is not a nut graph.*

Furthermore, we will present the following lemma which forms a connection between the null space vectors of a nut graph and the vertices of a particular orbit of a given graph automorphism. For the proof, see, for example, [3, p. 135].

Lemma 7. *Let G be a nut graph and let $\pi \in \mathrm{Aut}(G)$ be its automorphism. If $u \in \mathcal{N}(A_G)$ and $X = \{x_0, x_1, \ldots, x_{k-1}\} \subseteq V(G)$ represents an orbit of π such that*

$$\pi(x_j) = x_{j+1} \qquad (j = 0, \ldots, k-1),$$

where the addition is done modulo k, then we have that u is constant on X, or the orbit size k is even and

$$u(x_j) = (-1)^j \, u(x_0) \qquad (j = 0, \ldots, k-1).$$

Circulant matrices will also play an important role in our proofs. We note that a circulant matrix $C \in \mathbb{R}^{n\times n}$ is any matrix bearing the form

$$C = \begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_{n-1} \\ c_{n-1} & c_0 & c_1 & \cdots & c_{n-2} \\ c_{n-2} & c_{n-1} & c_0 & \cdots & c_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_1 & c_2 & c_3 & \dots & c_0 \end{bmatrix}.$$

It is well known from elementary linear algebra theory (see, for example, [13, Section 3.1]) that the eigenvalues of a circulant matrix can be evaluated by applying the expression

$$c_0 + c_1\zeta + c_2\zeta^2 + \cdots + c_{n-1}\zeta^{n-1}, \tag{1}$$

as ζ ranges through the n-th roots of unity.

Finally, we recall the cyclotomic polynomials and provide a theorem on their divisibility which shall play a key role in Section 6. The cyclotomic polynomial $\Phi_f(x)$ can be defined for each $f \in \mathbb{N}$ via

$$\Phi_f(x) = \prod_{\xi}(x - \xi),$$

where ξ ranges over the primitive f-th roots of unity. It is known that these polynomials have integer coefficients and that they are all irreducible in $\mathbb{Q}[x]$ (see, for example, [31]). For this reason, an arbitrary polynomial in $\mathbb{Q}[x]$ has a primitive f-th root of unity among its roots if and only if it is divisible by $\Phi_f(x)$. Besides that, it is worth pointing out that

$$\Phi_f(x) = \Phi_{f/p^{k-1}}(x^{p^{k-1}}) \tag{2}$$

holds whenever $p^k \mid f$ for a given prime number p and some $k \in \mathbb{N}$, $k \geqslant 2$ (see, for example, [15, p. 160]). We end the section by disclosing the following theorem on the divisibility of lacunary polynomials by cyclotomic polynomials.

Theorem 8 (Filaseta and Schinzel [8])**.** *Let $P(x) \in \mathbb{Z}[x]$ have N nonzero terms and let $\Phi_f(x) \mid P(x)$. Suppose that $p_1, p_2, \dots, p_k$ are distinct primes such that*

$$\sum_{j=1}^{k}(p_j - 2) > N - 2.$$

Let e_j be the largest exponent such that $p_j^{e_j} \mid f$. Then for at least one j, $1 \leqslant j \leqslant k$, we have that $\Phi_{f'}(x) \mid P(x)$, where $f' = \dfrac{f}{p_j^{e_j}}$.

3 Nonexistence of cubic bicirculant nut graphs

In this section we show that a cubic bicirculant graph cannot be a nut graph. As demonstrated by Pisanski [16], it is not difficult to establish that each connected cubic bicirculant graph of order $2n$ must be isomorphic to a graph from at least one of the following three families:

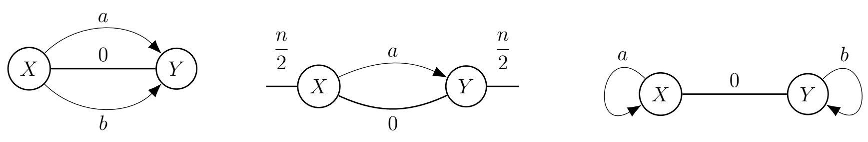
(i) $B_1(n, a, b)$, $0 < a < b < n$;

(ii) $B_2(n, a)$, $0 < a < n$;

(iii) $B_3(n, a, b)$, $0 < a \leqslant b < \frac{n}{2}$;

whose elements have the vertex set $\{x_0, \ldots, x_{n-1}, y_0, \ldots, y_{n-1}\}$ and the edge sets as given below:

$$\begin{aligned} E(B_1(n, a, b)) &= \{x_j y_j,\ x_j y_{j+a},\ x_j y_{j+b} \mid j \in \mathbb{Z}_n\}, \\ E(B_2(n, a)) &= \{x_j x_{j+\frac{n}{2}},\ x_j y_j,\ x_j y_{j+a},\ y_j y_{j+\frac{n}{2}} \mid j \in \mathbb{Z}_n\}, \\ E(B_3(n, a, b)) &= \{x_j y_j,\ x_j x_{j+a},\ y_j y_{j+b} \mid j \in \mathbb{Z}_n\}. \end{aligned}$$



(a) Type 1 (b) Type 2 (c) Type 3

Figure 2: Voltage graphs for the cubic bicirculant graphs of types 1, 2 and 3.

To make matters simple, we will say that a cubic bicirculant graph that is isomorphic to at least one element from the B_j family is of *type* j, for each $j = 1, 2, 3$. This terminology can now be concisely visualized in the form of Figure 2. In the following proposition, we will demonstrate that truly none of these graphs can be nut graphs.

Proposition 9. *There does not exist a cubic bicirculant nut graph.*

Proof. Due to Lemma 5, it is sufficient to restrict ourselves to connected graphs. Let G be a connected cubic bicirculant graph. If G is of type 1, then this graph is necessarily bipartite, hence it cannot be a nut graph, by virtue of Lemma 6. If we suppose that G is of type 2, then applying the local conditions on the vector $u \in \mathcal{N}(A_G)$ promptly gives us

$$u(x_{j+\frac{n}{2}}) + u(y_j) + u(y_{j+a}) = 0 \qquad (j \in \mathbb{Z}_n), \tag{3}$$

$$u(x_j) + u(x_{j-a}) + u(y_{j+\frac{n}{2}}) = 0 \qquad (j \in \mathbb{Z}_n). \tag{4}$$

By virtue of Lemma 7, we see that $u(y_j) = u(y_{j+a})$ or $u(y_j) = -u(y_{j+a})$, which means that Equation (3) leads us to $u(x_{j+\frac{n}{2}}) = 0$ or $u(x_{j+\frac{n}{2}}) = -2u(y_j)$. The former would immediately imply that G is not a nut graph, hence we may assume that the latter holds. Analogously, from Equation (4) we can conclude that $u(y_{j+\frac{n}{2}}) = 0$ or $u(y_{j+\frac{n}{2}}) = -2u(x_j)$. From $u(y_{j+\frac{n}{2}}) = 0$ we again obtain that G is not a nut graph, while the latter quickly yields $u(x_j) = 4u(x_j)$. From here, it promptly follows that $u(x_j) = 0$.

Finally, if we take G to be of type 3, then the local conditions on the vector $u \in \mathcal{N}(A_G)$ dictate

$$u(x_{j+a}) + u(x_{j-a}) + u(y_j) = 0 \qquad (j \in \mathbb{Z}_n), \tag{5}$$

$$u(x_j) + u(y_{j+b}) + u(y_{j-b}) = 0 \qquad (j \in \mathbb{Z}_n). \tag{6}$$

Lemma 7 guarantees that $u(x_{j-a}) = u(x_{j+a})$ and $u(y_{j-b}) = u(y_{j+b})$ must hold, which means that Equations (5) and (6) directly imply $u(y_j) = -2u(x_{j+a})$ and $u(x_j) = -2u(y_{j+b})$, respectively. However, this quickly gives us $u(x_j) = 4u(x_j)$ or $u(x_j) = -4u(x_j)$, hence $u(x_j) = 0$. □

4 Nonexistence of tricirculant nut graphs of types 2 and 3

In this section, we will give a brief demonstration that if a tricirculant cubic graph is a nut graph, then it must necessarily belong to the family comprising the type 1 graphs or the family consisting of the type 4 graphs.

Proposition 10. *A tricirculant cubic graph of type* 2 *or type* 3 *is not a nut graph.*

Proof. Let G be a tricirculant cubic nut graph of type 2, say G is isomorphic to $T_2(n, a, b)$ for appropriate parameters n, a, b, and let $u \in \mathcal{N}(A_G)$. Thus, we may assume that G has the vertex set $\{x_0, \ldots, x_{n-1}, y_0, \ldots, y_{n-1}, z_0, \ldots, z_{n-1}\}$ and that $x_j \sim x_{j+b}, x_{j-b}, z_j$, $y_j \sim y_{j+\frac{n}{2}}, z_j, z_{j-a}$ and $z_j \sim x_j, y_j, y_{j+a}$ for $j \in \mathbb{Z}_n$. Taking everything into consideration, we see that the local conditions for the vector u must bear the form

$$u(x_{j+b}) + u(x_{j-b}) + u(z_j) = 0 \qquad (j \in \mathbb{Z}_n), \tag{7}$$

$$u(y_{j+\frac{n}{2}}) + u(z_j) + u(z_{j-a}) = 0 \qquad (j \in \mathbb{Z}_n), \tag{8}$$

$$u(y_j) + u(y_{j+a}) + u(x_j) = 0 \qquad (j \in \mathbb{Z}_n), \tag{9}$$

where Equations (7), (8), (9) represent the local conditions at vertices x_j, y_j and z_j, respectively.

By applying Lemma 7 multiple times, it is not difficult to reach a contradiction. For starters, given the fact that $j + b \equiv_2 j - b$, Equation (7) immediately tells us that $u(z_j) \in \{2u(x_j), -2u(x_j)\}$. Furthermore, if $u(z_j) = -u(z_{j-a})$ (resp. $u(y_j) = -u(y_{j+a})$), then Equation (8) (resp. (9)) yields $u(y_j) = 0$ (resp. $u(x_j) = 0$), which leads us to $u = \mathbf{0}$. On the other hand, if $u(z_j) = u(z_{j-a})$ and $u(y_j) = u(y_{j+a})$ both hold, then Equation (8) implies $u(y_j) \in \{4u(x_j), -4u(x_j)\}$, while Equation (9) subsequently gives us $u(x_j) \in \{8u(x_j), -8u(x_j)\}$. For this reason, $u(x_j) = 0$ must hold, which promptly implies $u = \mathbf{0}$ once again. Thus, in any case, the zero vector is certainly the only element of $\mathcal{N}(A_G)$, hence $\eta(G) = 0$, which leads to a contradiction.

Now let G be a tricirculant cubic nut graph of type 3, say G is isomorphic to $T_3(n, a)$ for appropriate parameters n, a. Thus, we may assume that G has the vertex set $\{x_0, \ldots, x_{n-1}, y_0, \ldots, y_{n-1}, z_0, \ldots, z_{n-1}\}$ and that $x_j \sim x_{j+\frac{n}{2}}, y_{j+a}, z_j$, $y_j \sim x_{j-a}, y_{j+\frac{n}{2}}, z_j$ and $z_j \sim x_j, y_j, z_{j+\frac{n}{2}}$ for $j \in \mathbb{Z}_n$. Now let us define two vectors $u, v \in \mathbb{R}^{V_G}$ such that

$$\begin{aligned} &u(x_j) = 1, \quad u(y_j) = -1, \quad u(z_j) = 0 \qquad (j \in \mathbb{Z}_n),\\ &v(x_j) = 1, \quad v(y_j) = 0, \quad\ \ v(z_j) = -1 \qquad (j \in \mathbb{Z}_n). \end{aligned}$$

Then we quickly see that these two vectors are linearly independent, while both of them belong to $\mathcal{N}(A_G)$. Hence, $\eta(G) \geqslant 2$, which means that G cannot be a nut graph. □

5 Tricirculant graphs of type 1

In the previous section we have demonstrated that every tricirculant cubic nut graph, if one exists, must be of type 1 or type 4. Our next step in proving Theorem 2 will be to precisely determine all the nut graphs among the tricirculant cubic graphs of type 1. In order to achieve this, we will use the present section to show that the following theorem holds.

Theorem 11. *An arbitrary graph representable as $T_1(n, a, b)$, where n is even and $0 \leqslant a, b < n$, $a \neq b$, is a nut graph if and only if the following conditions hold:*

- **(i)** $\gcd\left(\frac{n}{2}, a\right) = \gcd\left(\frac{n}{2}, b\right) = 1$;
- **(ii)** $a \not\equiv_2 \frac{n}{2}$ *and* $b \not\equiv_2 \frac{n}{2}$;
- **(iii)** $v_2(b-a) \geqslant v_2(n)$.

Before we give the proof of Theorem 11 itself, we will need one auxiliary claim that connects the nut property of $T_1(n, a, b)$ to the root properties of a concrete polynomial. The next lemma demonstrates the aforementioned observation.

Lemma 12. *A graph representable as $T_1(n, a, b)$ is a nut graph if and only if the $\mathbb{Z}[x]$ polynomial*

$$x^{2a+b} + x^{a+2b} + x^a + x^b - x^{\frac{n}{2}+2a} - x^{\frac{n}{2}+2b} - 2x^{\frac{n}{2}+a+b} \tag{10}$$

has no n-th roots of unity among its roots, besides 1.

Proof. Let G be a given graph which is representable as $T_1(n, a, b)$. Thus, we may assume that G has the vertex set $\{x_0, \ldots, x_{n-1}, y_0, \ldots, y_{n-1}, z_0, \ldots, z_{n-1}\}$ and that $x_j \sim y_{j+a}, y_{j+b}, z_j$, $y_j \sim x_{j-a}, x_{j-b}, z_j$ and $z_j \sim x_j, y_j, z_{j+\frac{n}{2}}$ for $j \in \mathbb{Z}_n$.

From the local conditions for x_j, y_j, z_j, respectively, it is clear that $\mathcal{N}(A_G)$ represents the solution set to the system of equations

$$u(z_j) + u(y_{j+a}) + u(y_{j+b}) = 0 \qquad (j \in \mathbb{Z}_n), \tag{11}$$

$$u(z_j) + u(x_{j-a}) + u(x_{j-b}) = 0 \qquad (j \in \mathbb{Z}_n), \tag{12}$$

$$u(x_j) + u(y_j) + u(z_{j+\frac{n}{2}}) = 0 \qquad (j \in \mathbb{Z}_n) \tag{13}$$

in $u \in \mathbb{R}^{V_G}$. Suppose that a fixed vector $u \in \mathbb{R}^{V_G}$ is indeed a solution vector to the aforementioned system. From Equation (13) we quickly see that

$$u(z_j) = -u(x_{j+\frac{n}{2}}) - u(y_{j+\frac{n}{2}}) \tag{14}$$

holds for each $j \in \mathbb{Z}_n$. By plugging in Equation (14) into Equation (11), we further obtain

$$-u(x_{j+\frac{n}{2}}) - u(y_{j+\frac{n}{2}}) + u(y_{j+a}) + u(y_{j+b}) = 0,$$

which means that

$$u(x_j) = u(y_{j+\frac{n}{2}+a}) + u(y_{j+\frac{n}{2}+b}) - u(y_j) \tag{15}$$

is true for each $j \in \mathbb{Z}_n$. It is now possible to plug in Equations (14) and (15) into Equation (12) in order to get

$$\begin{aligned}\big(- u(y_{j+a}) - u(y_{j+b}) + u(y_{j+\frac{n}{2}}) - u(y_{j+\frac{n}{2}})\big) \\ + \big(u(y_{j+\frac{n}{2}}) + u(y_{j+\frac{n}{2}+b-a}) - u(y_{j-a})\big) \\ + \big(u(y_{j+\frac{n}{2}+a-b}) + u(y_{j+\frac{n}{2}}) - u(y_{j-b})\big) = 0,\end{aligned}$$

i.e.,

$$\begin{aligned}-u(y_{j+a}) - u(y_{j+b}) - u(y_{j-a}) - u(y_{j-b}) \\ + u(y_{j+\frac{n}{2}+b-a}) + u(y_{j+\frac{n}{2}+a-b}) + 2u(y_{j+\frac{n}{2}}) = 0,\end{aligned} \tag{16}$$

for each $j \in \mathbb{Z}_n$.

Now, Equation (16) can be thought of as a system of equations in $u \in \mathbb{R}^Y$ and it is not difficult to establish that a vector u represents its solution if and only if

$$\begin{bmatrix} u(y_0) & u(y_1) & \cdots & u(y_{n-1}) \end{bmatrix}^\intercal$$

is a null space vector of the corresponding circulant matrix $C \in \mathbb{R}^{n\times n}$. By implementing Equation (1), we see that the eigenvalues of C are obtained by the expression

$$- \zeta^a - \zeta^b - \zeta^{-a} - \zeta^{-b} + \zeta^{\frac{n}{2}+b-a} + \zeta^{\frac{n}{2}+a-b} + 2\zeta^{\frac{n}{2}}, \tag{17}$$

as ζ ranges through the n-th roots of unity. We will now prove that the graph G is a nut graph if and only if C is of nullity one.

First of all, it is clear that the scenario $\eta(C) = 0$ is certainly not possible due to the fact that plugging in $\zeta = 1$ into Equation (17) yields the value zero. If $\eta(C) \geqslant 2$, then there exist two linearly independent solutions to Equation (16). However, if we apply Equations (14) and (15) to these solutions, we further obtain two linearly independent solution vectors to the starting system determined by Equations (11), (12) and (13). Thus, we have $\eta(G) \geqslant 2$, which means that G is not a nut graph. On the other hand, if $\eta(C) = 1$, it becomes sufficient to notice that the solution set of Equation (16) contains the vectors $u \in \mathbb{R}^Y$ such that $u(y_j)$ is constant for each $j \in \mathbb{Z}_n$. The condition $\eta(C) = 1$ guarantees that these vectors are actually the only solutions to Equation (16). By implementing Equations (15) and (14), it can be swiftly seen that if $u \in \mathcal{N}(A_G)$, then this vector must be of the form

$$u(x_j) = \beta, \qquad u(y_j) = \beta, \qquad u(z_j) = -2\beta \qquad (j \in \mathbb{Z}_n),$$

for some $\beta \in \mathbb{R}$. The converse is also trivial to check, which immediately tells us that $\eta(G) = 1$ and that $\mathcal{N}(A_G)$ contains a full vector. Hence, G is a nut graph.

We have proved that G is a nut graph if and only if Equation (17) becomes zero for only a single value of $\zeta \in \mathbb{C}$ among the n-th roots of unity. Since $\zeta = 1$ necessarily yields the value zero, it is clear that this condition is equivalent to Equation (17) being nonzero for each $\zeta \in \mathbb{C}$, $\zeta^n = 1$, $\zeta \neq 1$. For each such ζ, it is sufficient to notice that

$$-\zeta^a - \zeta^b - \zeta^{-a} - \zeta^{-b} + \zeta^{\frac{n}{2}+b-a} + \zeta^{\frac{n}{2}+a-b} + 2\zeta^{\frac{n}{2}} = 0$$

if and only if

$$-\zeta^{a+b}\left(-\zeta^{a}-\zeta^{b}-\zeta^{-a}-\zeta^{-b}+\zeta^{\frac{n}{2}+b-a}+\zeta^{\frac{n}{2}+a-b}+2\zeta^{\frac{n}{2}}\right)=0$$

if and only if

$$\zeta^{2a+b}+\zeta^{a+2b}+\zeta^{a}+\zeta^{b}-\zeta^{\frac{n}{2}+2a}-\zeta^{\frac{n}{2}+2b}-2\zeta^{\frac{n}{2}+a+b}=0,$$

in order to complete the proof of the lemma. □

We are now in position to apply the auxiliary Lemma 12 in order to give a relatively short proof of Theorem 11.

Proof of Theorem 11. Let G be a graph representable as $T_1(n, a, b)$. By virtue of Lemma 12, we see that G is a nut graph if and only if the polynomial given in Equation (10) contains only the root 1 among all the n-th roots of unity. However, for any $x \in \mathbb{C}$, $x^n = 1$, it is possible to notice that

$$\begin{aligned} x^{2a+b}+x^{a+2b}+x^{a}+x^{b}-x^{\frac{n}{2}+2a}-x^{\frac{n}{2}+2b}-2x^{\frac{n}{2}+a+b} &= \\ &= x^{a}\,(x^{b-a}+1)(x^{\frac{n}{2}+a}-1)(x^{\frac{n}{2}+b}-1). \end{aligned}$$

From here, it is easy to see that G is a nut graph if and only if the equation $x^{b-a} = -1$ has no solutions in $x \in \mathbb{C}$, $x^n = 1$, while the equations $x^{\frac{n}{2}+a} = 1$ and $x^{\frac{n}{2}+b} = 1$ each have a single solution in $x \in \mathbb{C}$, $x^n = 1$, namely the value 1.

If we put $x = e^{\frac{2t\pi}{n}i}$ for a uniquely defined $t \in \mathbb{N}_0$, $0 \leqslant t < n$, the equation $x^{b-a} = -1$ in $x \in \mathbb{C}$, $x^n = 1$ becomes equivalent to the equation

$$t(b-a) \equiv_n \frac{n}{2} \tag{18}$$

in $t \in \mathbb{N}_0$, $0 \leqslant t < n$. Thus, the two equations will have the same number of solutions. However, Equation (18) represents a linear congruence equation, which means that it contains a solution if and only if $\gcd(n, b-a) \mid \frac{n}{2}$ (see, for example, [29, p. 170, Theorem 5.14]). Furthermore, it is simple to see that $\gcd(n, b-a) \mid \frac{n}{2}$ is equivalent to $v_2(b-a) < v_2(n)$. Thus, the starting equation has no solutions if and only if $v_2(b-a) \geqslant v_2(n)$.

In an analogous fashion, we may analyze the remaining two equations and discover that they both necessarily contain a solution. Moreover, the equation $x^{\frac{n}{2}+a} = 1$ has $\gcd(n, \frac{n}{2}+a)$ distinct solutions in total, while the number of solutions of $x^{\frac{n}{2}+b} = 1$ is equal to $\gcd(n, \frac{n}{2}+b)$. Taking everything into consideration, we conclude that G is a nut graph if and only if the following conditions hold:

- $\gcd(n, \frac{n}{2}+a) = 1$;
- $\gcd(n, \frac{n}{2}+b) = 1$;
- $v_2(b-a) \geqslant v_2(n)$.

We will now show that $\gcd(n, \frac{n}{2}+a) = 1$ is equivalent to the conjunction of $\gcd(\frac{n}{2}, a) = 1$ and $a \not\equiv_2 \frac{n}{2}$. First of all, it is not difficult to realize that $\gcd(\frac{n}{2}, a) \mid \gcd(n, \frac{n}{2} + a)$, hence if $\gcd(\frac{n}{2}, a) > 1$, then $\gcd(n, \frac{n}{2} + a) > 1$ as well. Besides that, if $a \equiv_2 \frac{n}{2}$, then n and $\frac{n}{2} + a$ are both surely even, which means that $\gcd(n, \frac{n}{2} + a) \geqslant 2$. These observations show that $\gcd\left(n, \frac{n}{2} + a\right) = 1$ implies that $\gcd\left(\frac{n}{2}, a\right) = 1$ and $a \not\equiv_2 \frac{n}{2}$.

Now, suppose that $\gcd(\frac{n}{2}, a) = 1$ and $a \not\equiv_2 \frac{n}{2}$ do both hold. If we put $\beta = \gcd(n, \frac{n}{2}+a)$, it is clear that $\beta \mid n$ and $\beta \mid n + 2a$, which directly implies that $\beta \mid 2a$ as well, hence $\beta \mid \gcd(n, 2a)$. Thus, we obtain $\beta \mid 2\gcd(\frac{n}{2}, a)$, which is only possible if $\beta \in \{1, 2\}$. Bearing in mind that $a \not\equiv_2 \frac{n}{2}$, it is clear that $\frac{n}{2} + a$ is odd, which implies $\beta \neq 2$, hence $\gcd(n, \frac{n}{2} + a) = 1$, as desired.

Thus, we have demonstrated that $\gcd(n, \frac{n}{2} + a) = 1$ is true if and only if $\gcd(\frac{n}{2}, a) = 1$ and $a \not\equiv_2 \frac{n}{2}$, and it is analogous to prove that $\gcd(n, \frac{n}{2} + b) = 1$ is equivalent to the conjunction of $\gcd(\frac{n}{2}, b) = 1$ and $b \not\equiv_2 \frac{n}{2}$. From here, we quickly conclude that G being a nut graph is indeed equivalent to the conjunction of conditions **(i)**, **(ii)** and **(iii)**. □

Remark 13. For any $t \in \mathbb{N}$ such that $\gcd(n, t) = 1$, it is not difficult to show that $T_1(n, a, b)$, $0 \leqslant a, b < n$, $a \neq b$ is surely isomorphic to $T_1(n, ta \bmod n, tb \bmod n)$. Bearing this in mind, we may impose n, a, b parameter conditions precisely required for $T_1(n, a, b)$ to be a nut graph which are stricter than those given in Theorem 11. If $4 \mid n$, then a tricirculant graph of type 1 is a nut graph if and only if it is representable as $T_1(n, 1, b)$ where $3 \leqslant b < n$, $\gcd(n, b) = 1$ and $v_2(b - 1) \geqslant v_2(n)$. Similarly, if $4 \nmid n$, then a tricirculant graph of type 1 is a nut graph if and only if it is representable as $T_1(n, 2, b)$ where $4 \leqslant b < n$ and $\gcd(n, b) = 2$.

6 Tricirculant graphs of type 4

In this final section, we shall determine all the nut graphs among the cubic tricirculant graphs of type 4, thereby completing the proof of Theorem 2. The aforementioned result is disclosed within the following theorem.

Theorem 14. *An arbitrary graph representable as $T_4(n, a, b)$ where n is even and $1 \leqslant a, b < \frac{n}{2}$, is a nut graph if and only if the following conditions hold:*

(i) $\gcd\left(\frac{n}{2}, a, b\right) = 1$*;*

(ii) *if $4 \nmid n$, then at least one of a and b is even;*

(iii) *if $4 \mid n$, then a and b are of different parities;*

(iv) *if $10 \mid n$, then at least one of $a, b, a - b, a + b$ is divisible by five.*

We will now demonstrate how the problem of testing whether a $T_4(n, a, b)$ graph is a nut graph can be transformed to a number theory problem, in a similar manner as it was done in Lemma 12. The corresponding result is given in the next lemma.

Lemma 15. *A graph representable as $T_4(n,a,b)$ is a nut graph if and only if the $\mathbb{Z}[x]$ polynomial*

$$x^{2a+b} + x^{a+2b} + x^a + x^b - x^{\frac{n}{2}+2a+2b} - x^{\frac{n}{2}+2a} - x^{\frac{n}{2}+2b} - x^{\frac{n}{2}} \tag{19}$$

has no n-th roots of unity among its roots, besides 1.

Proof. Let G be a given graph that is representable as $T_4(n,a,b)$. The very definition of the type 4 graphs dictates that $\mathcal{N}(A_G)$ represents the solution set to the system of equations

$$u(x_j) + u(y_j) + u(z_{j+\frac{n}{2}}) = 0 \qquad (j \in \mathbb{Z}_n), \tag{20}$$

$$u(z_j) + u(y_{j+b}) + u(y_{j-b}) = 0 \qquad (j \in \mathbb{Z}_n), \tag{21}$$

$$u(z_j) + u(x_{j+a}) + u(x_{j-a}) = 0 \qquad (j \in \mathbb{Z}_n) \tag{22}$$

in $u \in \mathbb{R}^{V_G}$. If we suppose that some vector $u \in \mathbb{R}^{V_G}$ is a solution vector to the given system, Equation (20) lets us immediately obtain that

$$u(z_j) = -u(x_{j+\frac{n}{2}}) - u(y_{j+\frac{n}{2}}) \tag{23}$$

is true for each $j \in \mathbb{Z}_n$. Furthermore, we can plug in Equation (23) into Equation (21) in order to get

$$-u(x_{j+\frac{n}{2}}) - u(y_{j+\frac{n}{2}}) + u(y_{j+b}) + u(y_{j-b}) = 0,$$

i.e.,

$$u(x_j) = u(y_{j+\frac{n}{2}+b}) + u(y_{j+\frac{n}{2}-b}) - u(y_j) \tag{24}$$

for each $j \in \mathbb{Z}_n$. Now, by plugging in Equations (23) and (24) into Equation (22), we may conclude that

$$\begin{aligned}\big(-u(y_{j+b}) - u(y_{j-b}) + u(y_{j+\frac{n}{2}}) - u(y_{j+\frac{n}{2}})\big)&\\ + \big(u(y_{j+\frac{n}{2}+b+a}) + u(y_{j+\frac{n}{2}-b+a}) - u(y_{j+a})\big)&\\ + \big(u(y_{j+\frac{n}{2}+b-a}) + u(y_{j+\frac{n}{2}-b-a}) - u(y_{j-a})\big) &= 0,\end{aligned}$$

which immediately gives

$$\begin{aligned}-u(y_{j+a}) - u(y_{j+b}) - u(y_{j-a}) - u(y_{j-b}) + u(y_{j+\frac{n}{2}+a+b})&\\ + u(y_{j+\frac{n}{2}+a-b}) + u(y_{j+\frac{n}{2}-a+b}) + u(y_{j+\frac{n}{2}-a-b}) &= 0,\end{aligned} \tag{25}$$

for each $j \in \mathbb{Z}_n$.

By thinking of Equation (25) as a system of equations in $u \in \mathbb{R}^Y$, we are now able to implement the same circulant matrix null space strategy from Lemma 12. In other words, by using an analogous proof method which we choose to leave out for the sake of brevity, we may conclude that the graph G is a nut graph if and only if the expression

$$-\zeta^a - \zeta^b - \zeta^{-a} - \zeta^{-b} + \zeta^{\frac{n}{2}+a+b} + \zeta^{\frac{n}{2}+a-b} + \zeta^{\frac{n}{2}-a+b} + \zeta^{\frac{n}{2}-a-b} \tag{26}$$

yields zero only for a single value of $\zeta \in \mathbb{C}$, $\zeta^n = 1$. Given the fact that Equation (26) surely gives zero when we plug in $\zeta = 1$, the said condition must be equivalent to Equation (26) not giving zero for any other n-th root of unity. However, for each $\zeta \in \mathbb{C}$, $\zeta^n = 1$, we have

$$-\zeta^a - \zeta^b - \zeta^{-a} - \zeta^{-b} + \zeta^{\frac{n}{2}+a+b} + \zeta^{\frac{n}{2}+a-b} + \zeta^{\frac{n}{2}-a+b} + \zeta^{\frac{n}{2}-a-b} = 0$$

if and only if

$$-\zeta^{a+b}\left(-\zeta^a - \zeta^b - \zeta^{-a} - \zeta^{-b} + \zeta^{\frac{n}{2}+a+b} + \zeta^{\frac{n}{2}+a-b} + \zeta^{\frac{n}{2}-a+b} + \zeta^{\frac{n}{2}-a-b}\right) = 0$$

if and only if

$$\zeta^{2a+b} + \zeta^{a+2b} + \zeta^a + \zeta^b - \zeta^{\frac{n}{2}+2a+2b} - \zeta^{\frac{n}{2}+2a} - \zeta^{\frac{n}{2}+2b} - \zeta^{\frac{n}{2}} = 0,$$

which promptly leads us to the desired lemma statement. □

Unfortunately, the Equation (19) polynomial does not adhere to a factorization analogous to the one applied on the Equation (10) polynomial during the proof of Theorem 11. For this reason, we shall use an entirely different strategy in order to complete the proof of Theorem 14. To begin, we define the following two auxiliary polynomials

$$\begin{aligned} Q_{a,b}(x) &= x^{2a+b} + x^{a+2b} + x^a + x^b - x^{2a+2b} - x^{2a} - x^{2b} - 1, \\ R_{a,b}(x) &= x^{2a+b} + x^{a+2b} + x^a + x^b + x^{2a+2b} + x^{2a} + x^{2b} + 1, \end{aligned}$$

for each $a, b \in \mathbb{N}$. It now becomes convenient to disclose the following brief reformulation of the polynomial problem obtained as a result of Lemma 15.

Lemma 16. *A graph representable as $T_4(n, a, b)$ is a nut graph if and only if the following two conditions hold:*

(i) $\Phi_f(x) \nmid Q_{a,b}(x)$ *for every* $f \in \mathbb{N}$, $f \geqslant 2$ *such that* $f \mid \frac{n}{2}$*;*

(ii) $\Phi_f(x) \nmid R_{a,b}(x)$ *for every* $f \in \mathbb{N}$ *such that* $f \mid n$ *and* $2 \nmid \frac{n}{f}$.

Proof. Let G be a given graph that is representable as $T_4(n, a, b)$. By virtue of Lemma 15, it can be immediately seen that G is a nut graph if and only if the following two conditions hold:

- $Q_{a,b}(x)$ does not contain a root ζ among all the n-th roots of unity such that $\zeta^{\frac{n}{2}} = 1$, besides 1;
- $R_{a,b}(x)$ does not contain a root ζ among all the n-th roots of unity such that $\zeta^{\frac{n}{2}} = -1$.

A complex number $\zeta \in \mathbb{C}$ is an n-th root of unity and satisfies $\zeta^{\frac{n}{2}} = 1$ if and only if it is an f-th primitive root of unity for some $f \in \mathbb{N}$ such that $f \mid \frac{n}{2}$. From here, it is not difficult to realize that $Q_{a,b}(x)$ does not contain a root among all such n-th roots of unity, besides 1, if and only if it is not divisible by any cyclotomic polynomial $\Phi_f(x)$ where $f \geqslant 2$ and $f \mid \frac{n}{2}$. In a similar fashion, it can be noticed that some $\zeta \in \mathbb{C}$ is an n-th root of unity and satisfies $\zeta^{\frac{n}{2}} = -1$ if and only if this number is an f-th primitive root of unity for some $f \in \mathbb{N}$ such that $f \mid n$ and $2 \nmid \frac{n}{f}$. However, this means that $R_{a,b}(x)$ does not contain such a root if and only if it is not divisible by any polynomial $\Phi_f(x)$ where $f \mid n$ and $2 \nmid \frac{n}{f}$. □

It is worth pointing out that, for any $f \in \mathbb{N}$, $\Phi_f(x)$ divides a given polynomial $V(x) \in \mathbb{Q}[x]$ if and only if it divides any other polynomial which can be obtained from $V(x)$ by adding or subtracting any multiple of f from the powers of its terms. Bearing this in mind, our next step in proving Theorem 14 will be to demonstrate the validity of the easier underlying implication of the required equivalence. In other words, we will show that each graph not satisfying the stated conditions is certainly not a nut graph. This result is given in the next lemma.

Lemma 17. *A graph representable as $T_4(n, a, b)$ which does not satisfy the conditions stated in Theorem 14 is surely not a nut graph.*

Proof. Let G be a given graph which is representable as $T_4(n, a, b)$ and suppose that this graph does not satisfy all four conditions disclosed in Theorem 14. In order to make the proof more concise, we will split it into four cases depending on which of the four conditions is not satisfied. In all the cases, we shall demonstrate that G cannot be a nut graph.

Case 1: $\gcd(\frac{n}{2}, a, b) = 1$ does not hold. Let $\beta = \gcd(\frac{n}{2}, a, b) \geqslant 2$. Given the fact that both a and b are divisible by β, it is straightforward to notice that $Q_{a,b}(x)$ must contain each β-th root of unity among its roots, hence $\Phi_\beta(x) \mid Q_{a,b}(x)$. However, since $\beta \geqslant 2$ and $\beta \mid \frac{n}{2}$, condition **(i)** from Lemma 16 dictates that G cannot be a nut graph, as desired.

Case 2: $4 \nmid n \implies 2 \mid ab$ does not hold. Suppose that $4 \nmid n$, while $2 \nmid a$ and $2 \nmid b$. It is obvious that $2 \mid n$ and $\frac{n}{2}$ is odd. Also, it can be swiftly noticed that -1 must be a root of $R_{a,b}(x)$, which means that $\Phi_2(x) \mid R_{a,b}(x)$. Thus, condition **(ii)** from Lemma 16 fails, which implies that the graph G cannot be a nut graph.

Case 3: $4 \mid n \implies a \not\equiv_2 b$ does not hold. Now, suppose that $4 \mid n$, while a and b are of the same parity. If a and b are both even, then it is easy to see that -1 is a root of $Q_{a,b}(x)$. Thus, $\Phi_2(x) \mid Q_{a,b}(x)$ must hold, while $2 \mid \frac{n}{2}$. By implementing condition **(i)** from Lemma 16, we get that G is not a nut graph, as desired.

If a and b are both odd, then it becomes convenient to split the problem into two further subcases depending on whether $8 \mid n$ or $n \equiv_8 4$. If $n \equiv_8 4$, then $4 \mid n$ and $2 \nmid \frac{n}{4}$, together with

$$R_{a,b}(i) = i^{2a+b} + i^{a+2b} + i^a + i^b + i^{2a+2b} + i^{2a} + i^{2b} + 1 = (i^{a+b} + 1)(i^a + i^b).$$

If $a \equiv_4 b$, then $i^{a+b} + 1 = 0$, and if $a \not\equiv_4 b$, then $i^a + i^b = 0$. Either way, we conclude that $R_{a,b}(i) = 0$, which further implies $\Phi_4(x) \mid R_{a,b}(x)$. According to condition **(ii)** from Lemma 16, the graph G is not a nut graph. Finally, if $8 \mid n$, we may observe that $Q_{a,b}(i) = 0$ by using the same computational strategy as done in the previous subcase. This directly gives $\Phi_4(x) \mid Q_{a,b}(x)$. Bearing in mind that $4 \mid \frac{n}{2}$, condition **(i)** from Lemma 16 tells us that G is not a nut graph.

Case 4: $10 \mid n \implies 5 \mid ab(a-b)(a+b)$ does not hold. Finally, suppose that $10 \mid n$ and that $5 \nmid ab(a-b)(a+b)$. It is not difficult to establish that the latter condition is equivalent to the disjuction of $a \bmod 5 \in \{1,4\} \wedge b \bmod 5 \in \{2,3\}$ and $b \bmod 5 \in \{1,4\} \wedge a \bmod 5 \in \{2,3\}$. Given the fact that $5 \mid \frac{n}{2}$, Lemma 16 claims that in order to show that G is not a nut graph, it is sufficient to prove that $\Phi_5(x) \mid Q_{a,b}(x)$, and this is exactly what we shall do. Since $Q_{a,b}(x) = Q_{b,a}(x)$, we may assume that $a \bmod 5 \in \{1,4\}$ and $b \bmod 5 \in \{2,3\}$, without loss of generality. From here, it is straightforward to notice that either $b \equiv_5 2a$ or $b \equiv_5 3a$.

If we have $b \equiv_5 2a$, then by plugging in the said modular equality we swiftly notice that

$$\begin{aligned} & \Phi_5(x) \mid Q_{a,b}(x) \\ \iff\quad & \Phi_5(x) \mid x^{4a} + x^{5a} + x^{a} + x^{2a} - x^{6a} - x^{2a} - x^{4a} - 1 \\ \iff\quad & \Phi_5(x) \mid x^{4a} + 1 + x^{a} + x^{2a} - x^{a} - x^{2a} - x^{4a} - 1 \\ \iff\quad & \Phi_5(x) \mid 0, \end{aligned}$$

hence $\Phi_5(x) \mid Q_{a,b}(x)$ is indeed true. Similarly, if $b \equiv_5 3a$, then by using the same strategy we obtain

$$\begin{aligned} & \Phi_5(x) \mid Q_{a,b}(x) \\ \iff\quad & \Phi_5(x) \mid x^{5a} + x^{7a} + x^{a} + x^{3a} - x^{8a} - x^{2a} - x^{6a} - 1 \\ \iff\quad & \Phi_5(x) \mid 1 + x^{2a} + x^{a} + x^{3a} - x^{3a} - x^{2a} - x^{a} - 1 \\ \iff\quad & \Phi_5(x) \mid 0, \end{aligned}$$

which directly implies $\Phi_5(x) \mid Q_{a,b}(x)$ once again. □

Before we proceed with the proof of Theorem 14, we will need another short auxiliary folklore lemma.

Lemma 18. *Let $V(x), W(x) \in \mathbb{Q}[x]$, $W(x) \not\equiv 0$ be two polynomials such that $W(x) \mid V(x)$ and the powers of all the nonzero terms of $W(x)$ are divisible by some $\beta \in \mathbb{N}$. For any $j \in \{0, \ldots, \beta-1\}$, if we use $V^{(\beta,j)}(x)$ to denote the polynomial composed of all the terms of $V(x)$ whose powers are congruent to j modulo β, we then have $W(x) \mid V^{(\beta,j)}(x)$.*

Proof. Since $W(x) \mid V(x)$, we may write $V(x) = W(x)\,U(x)$ for some polynomial $U(x) \in \mathbb{Q}[x]$. For each $j \in \{0, \ldots, \beta-1\}$, let $U^{(\beta,j)}(x)$ denote the polynomial comprising all the terms of $U(x)$ whose powers are congruent to j modulo β. It now becomes simple to notice that $V^{(\beta,j)}(x) = W(x)\,U^{(\beta,j)}(x)$ must be true for each $j \in \{0, \ldots, \beta-1\}$. The lemma statement follows directly from here. □

We shall now extensively implement Lemma 18 in order to obtain a series of auxiliary lemmas regarding the divisibility of $Q_{a,b}(x)$ and $R_{a,b}(x)$ by polynomials whose nonzero terms have powers divisible by a common prime.

Lemma 19. *If a given $W(x) \in \mathbb{Q}[x]$ has at least two nonzero terms and all of its nonzero terms have powers divisible by a prime number $p \geqslant 7$, then $W(x) \mid Q_{a,b}(x)$ and $W(x) \mid R_{a,b}(x)$ both imply $p \mid a, b$.*

Proof. First of all, if all the numbers $2a + b, a + 2b, a, b, 2a + 2b, 2a, 2b$ are not divisible by p, we then obtain

$$Q_{a,b}^{(p,0)}(x) = -1, \quad R_{a,b}^{(p,0)}(x) = 1.$$

From here we have that $W(x) \nmid Q_{a,b}^{(p,0)}(x), R_{a,b}^{(p,0)}(x)$, hence $W(x) \nmid Q_{a,b}(x), R_{a,b}(x)$, by virtue of Lemma 18. Thus, there is nothing left to discuss in this scenario. We will now suppose that at least one number from $2a + b, a + 2b, a, b, 2a + 2b, 2a, 2b$ is divisible by p. In order to make the proof easier to follow, we shall split the problem into seven corresponding cases.

Case 1: $p \mid 2a + b$. Here, we have that $b \equiv_p -2a$, which implies

$$\begin{array}{cccc} 2a + b \equiv_p 0, & a + 2b \equiv_p -3a, & a \equiv_p a, & b \equiv_p -2a, \\ 2a + 2b \equiv_p -2a, & 2a \equiv_p 2a, & 2b \equiv_p -4a, & 0 \equiv_p 0. \end{array}$$

It is now easy to see that we obtain two further possibilities:

- a has a unique remainder modulo p within the set $\{2a+b, a+2b, a, b, 2a+2b, 2a, 2b, 0\}$;
- at least one number from the set $\{a, 3a, 4a, 5a\}$ is divisible by p.

In the former scenario, Lemma 18 dictates that $W(x) \mid Q_{a,b}(x)$ or $W(x) \mid R_{a,b}(x)$ would both imply $W(x) \mid x^a$, which is not possible. Thus, $W(x) \nmid Q_{a,b}(x), R_{a,b}(x)$ and the lemma statement holds. In the latter scenario, it is not difficult to conclude that each subcase leads to $p \mid a$. From here, it immediately follows that $p \mid a, b$, as desired.

Case 2: $p \mid a + 2b$. This case can be proved in an entirely analogous manner as case 1.

Case 3: $p \mid a$. In this case, we get $a \equiv_p 0$, which means that

$$\begin{array}{cccc} 2a + b \equiv_p b, & a + 2b \equiv_p 2b, & a \equiv_p 0, & b \equiv_p b, \\ 2a + 2b \equiv_p 2b, & 2a \equiv_p 0, & 2b \equiv_p 2b, & 0 \equiv_p 0. \end{array}$$

We now get two further possibilities:

- $p \mid b$ or $p \mid 2b$;
- the numbers $\{2a + b, a + 2b, a, b, 2a + 2b, 2a, 2b, 0\}$ can be partitioned as $\{\{2a + b, b\}, \{a + 2b, 2a + 2b, 2b\}, \{a, 2a, 0\}\}$ according to their remainder modulo p.

In the former scenario, we certainly have that $p \mid a, b$, hence there is nothing more to discuss. In the later scenario, Lemma 18 allows us to swiftly conclude that $W(x) \mid Q_{a,b}(x)$ implies

$$W(x) \mid x^{2a+b} + x^b, \tag{27}$$
$$W(x) \mid x^{a+2b} - x^{2a+2b} - x^{2b}, \tag{28}$$

which is not possible due to the fact that Equations (27) and (28) together give

$$\begin{aligned} & W(x) \mid (x^{a+2b} - x^{2a+2b} - x^{2b}) + x^b \left(x^{2a+b} + x^b\right) \\ \implies \quad & W(x) \mid x^{a+2b}. \end{aligned}$$

In a similar fashion, $W(x) \mid R_{a,b}(x)$ would lead to

$$W(x) \mid x^{2a+b} + x^b, \tag{29}$$
$$W(x) \mid x^{a+2b} + x^{2a+2b} + x^{2b}, \tag{30}$$

However, this is again impossible since Equations (29) and (30) imply

$$\begin{aligned} & W(x) \mid (x^{a+2b} + x^{2a+2b} + x^{2b}) - x^b \left(x^{2a+b} + x^b\right) \\ \implies \quad & W(x) \mid x^{a+2b}. \end{aligned}$$

Case 4: $p \mid b$. This case can be proved in an entirely analogous manner as case 3.

Case 5: $p \mid 2a+2b$. The condition $p \mid 2a+2b$ gets down to $b \equiv_p -a$, which immediately leads to

$$\begin{array}{cccc} 2a+b \equiv_p a, & a+2b \equiv_p -a, & a \equiv_p a, & b \equiv_p -a, \\ 2a+2b \equiv_p 0, & 2a \equiv_p 2a, & 2b \equiv_p -2a, & 0 \equiv_p 0. \end{array}$$

From here, we reach two further possibilities:

- $2a$ has a unique remainder modulo p within the set $\{2a+b, a+2b, a, b, 2a+2b, 2a, 2b, 0\}$;
- at least one number from the set $\{a, 2a, 3a, 4a\}$ is divisible by p;

In the former scenario, Lemma 18 states that $W(x) \mid Q_{a,b}(x)$ or $W(x) \mid R_{a,b}(x)$ would both imply $W(x) \mid x^{2a}$, which is clearly impossible. For this reason, we obtain $W(x) \nmid Q_{a,b}(x), R_{a,b}(x)$ as desired. In the latter scenario, it can be quickly noticed that $p \mid a$ must be true. This leads to $p \mid a, b$, which completes the proof.

Case 6: $p \mid 2a$. The condition $p \mid 2a$ directly gives us $a \equiv_p 0$, which means that this case actually coincides with case 3.

Case 7: $p \mid 2b$. This case can be proved in an entirely analogous manner as case 6. □

Lemma 20. *If $W(x) \in \mathbb{Q}[x]$ is a polynomial with at least two nonzero terms such that all of its nonzero terms have powers divisible by five, then $W(x) \mid Q_{a,b}(x)$ and $W(x) \mid R_{a,b}(x)$ both imply $5 \mid a, b$ or $5 \nmid a, b, a+b, a-b$.*

Proof. To begin, if $5 \mid a, b$, then the lemma statement certainly holds and there is nothing more to discuss. Due to the fact that $Q_{a,b}(x) = Q_{b,a}(x)$, as well as $R_{a,b}(x) = R_{b,a}(x)$, we can assume, without loss of generality, that $5 \nmid b$. Now, it is not difficult to notice that a must satisfy precisely one of the following five modular equalies: $a \equiv_5 0$, $a \equiv_5 b$, $a \equiv_5 2b$, $a \equiv_5 3b$, $a \equiv_5 4b$. We shall use this observation to complete the proof by splitting the problem into five corresponding cases.

	$a \equiv_5 0$	$a \equiv_5 b$	$a \equiv_5 2b$	$a \equiv_5 3b$	$a \equiv_5 4b$
$2a+b \equiv_5$	b	$3b$	0	$2b$	$4b$
$a+2b \equiv_5$	$2b$	$3b$	$4b$	0	b
$a \equiv_5$	0	b	$2b$	$3b$	$4b$
$b \equiv_5$	b	b	b	b	b
$2a+2b \equiv_5$	$2b$	$4b$	b	$3b$	0
$2a \equiv_5$	0	$2b$	$4b$	b	$3b$
$2b \equiv_5$	$2b$	$2b$	$2b$	$2b$	$2b$
$0 \equiv_5$	0	0	0	0	0

Table 1: The powers of the $Q_{a,b}(x)$ and $R_{a,b}(x)$ nonzero terms modulo five.

Case 1: $a \equiv_5 0$. In this scenario, Table 1 and Lemma 18 together dictate that $W(x) \mid Q_{a,b}(x)$ implies

$$W(x) \mid x^{2a+b} + x^b,$$
$$W(x) \mid x^{a+2b} - x^{2a+2b} - x^{2b},$$
$$W(x) \mid x^a - x^{2a} - 1,$$

while $W(x) \mid R_{a,b}(x)$ implies

$$W(x) \mid x^{2a+b} + x^b,$$
$$W(x) \mid x^{a+2b} + x^{2a+2b} + x^{2b},$$
$$W(x) \mid x^a + x^{2a} + 1.$$

From here onwards, the proof can be completed by using the same strategy used in case 3 in the proof of Lemma 19.

Case 2: $a \equiv_5 b$. In this case, Table 1 states that the element 0 has a unique remainder modulo five within the set $\{2a+b, a+2b, a, b, 2a+2b, 2a, 2b, 0\}$. For this reason, $W(x) \mid Q_{a,b}(x)$ and $W(x) \mid R_{a,b}(x)$ would both imply $W(x) \mid 1$, by virtue of Lemma 18. Thus, neither $W(x) \mid Q_{a,b}(x)$ nor $W(x) \mid R_{a,b}(x)$ can be true.

Case 3: $a \equiv_5 2b$. Here, it is easy to check that $5 \nmid a, b, a+b, a-b$ and there is nothing more to discuss.

Case 4: $a \equiv_5 3b$. In this situation, it is straightforward to notice that once again $5 \nmid a, b, a+b, a-b$, which means that the lemma statement does hold.

Case 5: $a \equiv_5 4b$. Here, Table 1 tells us that the element $2a$ has a unique remainder modulo five within the set $\{2a+b, a+2b, a, b, 2a+2b, 2a, 2b, 0\}$. The rest of the proof can now be carried out analogously as it was done in case 2. □

Lemma 21. *If $W(x) \in \mathbb{Q}[x]$ is a polynomial with at least two nonzero terms such that all of its nonzero terms have powers divisible by three, then $W(x) \mid Q_{a,b}(x)$ and $W(x) \mid R_{a,b}(x)$ both imply $3 \mid a, b$.*

Proof. For starters, if $3 \mid a, b$, then the lemma statement holds and there is nothing left to prove. Given the fact that $Q_{a,b}(x) = Q_{b,a}(x)$ and $R_{a,b}(x) = R_{b,a}(x)$, we may assume, without loss of generality, that $3 \nmid b$. It is easy to establish that either $a \equiv_3 0$ or $a \equiv_3 b$ or $a \equiv_3 2b$ must hold. For this reason, it becomes convenient to split the problem into the three corresponding cases that arise from this observation.

	$a \equiv_3 0$	$a \equiv_3 b$	$a \equiv_3 2b$
$2a+b \equiv_3$	b	0	$2b$
$a+2b \equiv_3$	$2b$	0	b
$a \equiv_3$	0	b	$2b$
$b \equiv_3$	b	b	b
$2a+2b \equiv_3$	$2b$	b	0
$2a \equiv_3$	0	$2b$	b
$2b \equiv_3$	$2b$	$2b$	$2b$
$0 \equiv_3$	0	0	0

Table 2: The powers of the $Q_{a,b}(x)$ and $R_{a,b}(x)$ nonzero terms modulo three.

Case 1: $a \equiv_3 0$. In this case, Table 2 and Lemma 18 tell us that $W(x) \mid Q_{a,b}(x)$ implies

$$\begin{aligned} &W(x) \mid x^{2a+b} + x^b, \\ &W(x) \mid x^{a+2b} - x^{2a+2b} - x^{2b}, \\ &W(x) \mid x^a - x^{2a} - 1, \end{aligned}$$

while $W(x) \mid R_{a,b}(x)$ implies

$$\begin{aligned} &W(x) \mid x^{2a+b} + x^b, \\ &W(x) \mid x^{a+2b} + x^{2a+2b} + x^{2b}, \\ &W(x) \mid x^a + x^{2a} + 1. \end{aligned}$$

It is now evident that the given case can be resolved in the same manner as case 3 from Lemma 19.

Case 2: $a \equiv_3 b$. If we suppose that $W(x) \mid Q_{a,b}(x)$, then Table 2 and Lemma 18 yield

$$\begin{aligned} &W(x) \mid x^{2a+b} + x^{a+2b} - 1, \\ &W(x) \mid x^a + x^b - x^{2a+2b}, \\ &W(x) \mid x^{2a} + x^{2b}, \end{aligned}$$

which promptly leads us to

$$\begin{aligned} &W(x) \mid (x^b - x^a)(x^a + x^b)^2\,(x^{2a+b} + x^{a+2b} - 1) \\ &\qquad + (x^{2b} - x^{2a})(x^a + x^b - x^{2a+2b}) \\ &\qquad + x^{a+b}(x^{2a} - x^{2b} + x^{a+b})(x^{2a} + x^{2b}) \\ \implies \quad &W(x) \mid 2x^{2a+4b}, \end{aligned}$$

which is impossible. Thus, $W(x) \nmid Q_{a,b}(x)$. In a similar fashion, if we suppose that $W(x) \mid R_{a,b}(x)$, it follows that

$$\begin{aligned} &W(x) \mid x^{2a+b} + x^{a+2b} + 1, \\ &W(x) \mid x^a + x^b + x^{2a+2b}, \\ &W(x) \mid x^{2a} + x^{2b}. \end{aligned}$$

Subsequently, we may obtain

$$\begin{aligned} &W(x) \mid (x^a - x^b)(x^a + x^b)^2\,(x^{2a+b} + x^{a+2b} + 1) \\ &\qquad + (x^{2b} - x^{2a})(x^a + x^b + x^{2a+2b}) \\ &\qquad + x^{a+b}(x^{2b} - x^{2a} + x^{a+b})(x^{2a} + x^{2b}) \\ \implies \quad &W(x) \mid 2x^{4a+2b}, \end{aligned}$$

which is again not possible, hence $W(x) \nmid R_{a,b}(x)$.

Case 3: $a \equiv_3 2b$. If we suppose that $W(x) \mid Q_{a,b}(x)$, then Table 2 and Lemma 18 dictate that

$$\begin{aligned} &W(x) \mid x^{2a+b} + x^a - x^{2b}, \\ &W(x) \mid x^{a+2b} + x^b - x^{2a}, \\ &W(x) \mid x^{2a+2b} + 1. \end{aligned}$$

However, in this scenario we may conclude that

$$\begin{aligned} &W(x) \mid (-1 - x^{12b} + x^{a+7b})(x^{2a+b} + x^a - x^{2b}) \\ &\qquad + (-x^b + x^{a+2b} + x^{a+11b} - x^{2a+6b})(x^{a+2b} + x^b - x^{2a}) \\ &\qquad + (x^a + x^{a+9b} - x^{2a+4b})(x^{2a+2b} + 1) \\ \implies \quad &W(x) \mid x^{14b}, \end{aligned}$$

which is obviously impossible. Similarly, if we suppose that $W(x) \mid R_{a,b}(x)$, we immediately get

$$\begin{aligned} W(x) &\mid x^{2a+b} + x^a + x^{2b}, \\ W(x) &\mid x^{a+2b} + x^b + x^{2a}, \\ W(x) &\mid x^{2a+2b} + 1, \end{aligned}$$

which promptly implies

$$\begin{aligned} & W(x) \mid (1 + x^{12b} - x^{a+7b})(x^{2a+b} + x^a + x^{2b}) \\ & \qquad + (-x^b + x^{a+2b} - x^{a+11b} + x^{2a+6b})(x^{a+2b} + x^b + x^{2a}) \\ & \qquad + (-x^a + x^{a+9b} - x^{2a+4b})(x^{2a+2b} + 1) \\ \implies \quad & W(x) \mid x^{14b}, \end{aligned}$$

which is again not possible. □

Lemma 22. *If a given polynomial $W(x) \in \mathbb{Q}[x]$ has at least two nonzero terms and all of its nonzero terms have powers divisible by four, then $W(x) \mid Q_{a,b}(x)$ and $W(x) \mid R_{a,b}(x)$ both imply $2 \mid a, b$.*

Proof. If $2 \mid a, b$, then the lemma statement holds and there is nothing left to prove. Given the fact that $Q_{a,b}(x) = Q_{b,a}(x)$ and $R_{a,b}(x) = R_{b,a}(x)$, we may assume, without loss of generality, that a is odd. Depending on the value of $b \bmod 4$, we can divide the problem into four corresponding cases and solve each of them separately.

	$b \equiv_4 2$	$b \equiv_4 0$	$b \equiv_4 a$	$b \equiv_4 a+2$
$2a+b \equiv_4$	0	2	$a+2$	a
$a+2b \equiv_4$	a	a	$a+2$	$a+2$
$a \equiv_4$	a	a	a	a
$b \equiv_4$	2	0	a	$a+2$
$2a+2b \equiv_4$	2	2	0	0
$2a \equiv_4$	2	2	2	2
$2b \equiv_4$	0	0	2	2
$0 \equiv_4$	0	0	0	0

Table 3: The powers of the $Q_{a,b}(x)$ and $R_{a,b}(x)$ nonzero terms modulo four, provided a is odd.

Case 1: $b \equiv_4 2$. In this case, Table 3 and Lemma 18 tell us that $W(x) \mid Q_{a,b}(x)$ implies

$$W(x) \mid x^b - x^{2a+2b} - x^{2a}, \tag{31}$$

$$W(x) \mid x^{a+2b} + x^a. \tag{32}$$

However, by combining Equations (31) and (32), we get

$$\begin{aligned} & W(x) \mid (x^b - x^{2a+2b} - x^{2a}) + x^a\,(x^{a+2b} + x^a) \\ \implies \quad & W(x) \mid x^b, \end{aligned}$$

which is not possible. Similarly, $W(x) \mid R_{a,b}(x)$ implies

$$W(x) \mid x^b + x^{2a+2b} + x^{2a}, \tag{33}$$

$$W(x) \mid x^{a+2b} + x^a, \tag{34}$$

which can also be shown to be impossible by combining Equation (33) and (34)

$$\begin{aligned} & W(x) \mid (x^b + x^{2a+2b} + x^{2a}) - x^a\,(x^{a+2b} + x^a) \\ \implies \quad & W(x) \mid x^b. \end{aligned}$$

Case 2: $b \equiv_4 0$. Here, Table 3 and Lemma 18 dictate that $W(x) \mid Q_{a,b}(x)$ implies

$$\begin{aligned} & W(x) \mid x^{a+2b} + x^a, \\ & W(x) \mid x^{2a+b} - x^{2a+2b} - x^{2a}, \end{aligned}$$

while $W(x) \mid R_{a,b}(x)$ implies

$$\begin{aligned} & W(x) \mid x^{a+2b} + x^a, \\ & W(x) \mid x^{2a+b} + x^{2a+2b} + x^{2a}. \end{aligned}$$

This case can now be resolved in an entirely analogous manner as case 3 in the proof of Lemma 19.

Case 3: Case $b \equiv_4 a$. Here, Table 3 and Lemma 18 dictate that $W(x) \mid Q_{a,b}(x)$ and $W(x) \mid R_{a,b}(x)$ would both have to imply

$$W(x) \mid x^a + x^b, \tag{35}$$

$$W(x) \mid x^{2a} + x^{2b}. \tag{36}$$

By combining Equations (35) and (36) we could obtain

$$\begin{aligned} & W(x) \mid (x^{2a} + x^{2b}) + (x^a - x^b)(x^a + x^b) \\ \implies \quad & W(x) \mid 2x^{2a}, \end{aligned}$$

which is not possible, as desired.

Case 4: $b \equiv_4 a + 2$. In this situation, from Table 3 and Lemma 18 we can easily see that both $W(x) \mid Q_{a,b}(x)$ and $W(x) \mid R_{a,b}(x)$ would surely imply

$$W(x) \mid x^{2a+b} + x^a, \tag{37}$$

$$W(x) \mid x^{2a+2b} + 1. \tag{38}$$

However, if we combined Equations (37) and (38), we would get

$$\begin{aligned} & W(x) \mid (x^{a+b}-1)(x^{2a+b}+x^a)+x^a\,(x^{2a+2b}+1) \\ \implies \quad & W(x) \mid 2x^{3a+2b}, \end{aligned}$$

which is impossible once again. □

It is worth pointing out that the polynomials $Q_{a,b}(x)$ and $R_{a,b}(x)$ have at most eight nonzero terms. For this reason, it becomes convenient to implement Theorem 8 while inspecting their divisibility by cyclotomic polynomials. For example, if $\Phi_f(x) \mid Q_{a,b}(x)$ for some $f \in \mathbb{N}$, we may cancel out each prime factor of f which is greater than seven in order to obtain another integer $f' \in \mathbb{N}$ which satisfies $\Phi_{f'}(x) \mid Q_{a,b}(x)$. The same conclusion can be made regarding the $R_{a,b}(x)$ polynomials. The proof of Theorem 14 will heavily rely on this observation. Before we proceed with the main part of the proof, we shall need one more auxiliary lemma regarding the divisibility of $Q_{a,b}(x)$ and $R_{a,b}(x)$ by certain cyclotomic polynomials.

Lemma 23. *For each prime $p \geqslant 11$, $\Phi_p(x) \mid Q_{a,b}(x)$ and $\Phi_p(x) \mid R_{a,b}(x)$ both imply $p \mid a, b$.*

Proof. Let us define $Q_{a,b}^{\bmod p}(x)$ and $R_{a,b}^{\bmod p}(x)$ as the polynomials obtained from $Q_{a,b}(x)$ and $R_{a,b}(x)$, respectively, by replacing the power of each nonzero term by its remainder modulo p. It is straightforward to see that $\Phi_p(x) \mid Q_{a,b}(x)$ holds if and only if $\Phi_p(x) \mid Q_{a,b}^{\bmod p}(x)$ does. Also, $\Phi_p(x) \mid R_{a,b}(x)$ is surely equivalent to $\Phi_p(x) \mid R_{a,b}^{\bmod p}(x)$.

We shall demonstrate the lemma statement only for the $Q_{a,b}(x)$ polynomial, given the fact that the proof regarding the $R_{a,b}(x)$ polynomial can be carried out in an entirely analogous manner. Suppose that $\Phi_p(x) \mid Q_{a,b}(x)$. Bearing in mind that

$$\Phi_p(x) = \sum_{j=0}^{p-1} x^j,$$

it is easy to see that $\deg \Phi_p(x) = p-1$. However, since $\deg Q_{a,b}^{\bmod p}(x) \leqslant p-1$, the divisibility $\Phi_p(x) \mid Q_{a,b}^{\bmod p}(x)$ directly implies that one of the following two possibilities must be true:

- $Q_{a,b}^{\bmod p}(x) = \beta\,\Phi_p(x)$ for some $\beta \in \mathbb{Q} \setminus \{0\}$;
- $Q_{a,b}^{\bmod p}(x) \equiv 0$.

In the first scenario, $Q_{a,b}^{\bmod p}(x)$ would need to have exactly $p \geqslant 11$ nonzero terms, which is obviously not possible. Thus, $Q_{a,b}^{\bmod p}(x) \equiv 0$ surely holds. It is now convenient to perform a remainder modulo p analysis identical to the one done throughout the proof of Lemma 19. Bearing in mind all the cases disclosed in the aforementioned lemma, we may conclude that at least one of the following four statements must be true:

- $p \mid a, b$;
- there exists an element from the set $\{2a + b, a + 2b, a, b, 2a + 2b, 2a, 2b, 0\}$ whose remainder modulo p is unique within that set;
- the numbers $\{2a + b, a + 2b, a, b, 2a + 2b, 2a, 2b, 0\}$ can be partitioned as $\{\{2a + b, b\}, \{a + 2b, 2a + 2b, 2b\}, \{a, 2a, 0\}\}$ according to their remainder modulo p.
- the numbers $\{2a + b, a + 2b, a, b, 2a + 2b, 2a, 2b, 0\}$ can be partitioned as $\{\{a + 2b, a\}, \{2a + b, 2a + 2b, 2a\}, \{b, 2b, 0\}\}$ according to their remainder modulo p.

If $p \mid a, b$, then there is nothing left to discuss, since the lemma statement directly holds. If the set $\{2a+b, a+2b, a, b, 2a+2b, 2a, 2b, 0\}$ contains an element whose remainder modulo p is unique within the set, it is easy to see that $Q_{a,b}^{\bmod p}(x) \equiv 0$ leads to a contradiction. The last two scenarios can be resolved in an analogous manner, so we will only deal with the third.

Suppose that the elements of the set $\{2a + b, a + 2b, a, b, 2a + 2b, 2a, 2b, 0\}$ can be partitioned as $\{\{2a + b, b\}, \{a + 2b, 2a + 2b, 2b\}, \{a, 2a, 0\}\}$ according to their remainder modulo p. From here, the condition $Q_{a,b}^{\bmod p}(x) \equiv 0$ immediately implies

$$x^{a \bmod p} - x^{2a \bmod p} - 1 \equiv 0,$$

which is clearly impossible. □

We are now finally able to put all the pieces of the puzzle together and finalize the proof of Theorem 14.

Proof of Theorem 14. Let G be an arbitrarily chosen graph which is representable as $T_4(n, a, b)$. According to Lemma 17, if G does not satisfy the four conditions given in the theorem, then this graph is certainly not a nut graph. Thus, in order to complete the proof, it is sufficent to suppose that G is not a nut graph, then prove that it fails to satisfy at least one of the four stated conditions. However, if we suppose that the graph G is not a nut graph, then Lemma 16 states that there must exist an $f \in \mathbb{N}$, $f \geqslant 2$ such that $f \mid \frac{n}{2}$ and $\Phi_f(x) \mid Q_{a,b}(x)$, or an $f \in \mathbb{N}$ such that $f \mid n$, $2 \nmid \frac{n}{f}$ and $\Phi_f(x) \mid R_{a,b}(x)$. It now becomes convenient to split the problem into two cases depending on whether $Q_{a,b}(x)$ or $R_{a,b}(x)$ is divisible by the corresponding cyclotomic polynomial.

Case 1: $\Phi_f(x) \mid Q_{a,b}(x)$. If $p^2 \mid f$ holds for any prime number $p \in \mathbb{N}$, we then have that $\Phi_f(x) = \Phi_{f/p}(x^p)$, which implies that all the nonzero terms of $\Phi_f(x)$ possess powers divisible by p. Thus, if $p^2 \mid f$ for any prime $p \geqslant 7$ or $p = 3$, we can implement Lemma 19 or Lemma 21 in order to obtain that $p \mid a, b$. However, it is now straightforward to see that $p \mid a, b, \frac{n}{2}$, hence $\gcd(\frac{n}{2}, a, b) \neq 1$, which means that condition **(i)** from Theorem 14 is not satisfied.

If we have that $5^2 \mid f$, we may apply Lemma 20 to obtain that $5 \mid a, b$ or $5 \nmid a, b, a - b, a + b$. If $5 \mid a, b$, it is then clear that condition **(i)** from Theorem 14 fails to hold. If $5 \nmid a, b, a - b, a + b$, it is enough to notice that $10 \mid n$ to conclude that condition **(iv)** from Theorem 14 is not satisfied. Also, if $8 \mid f$, it is then convenient to use Lemma 22 to reach $2 \mid a, b$. However, this further gives that condition **(i)** from Theorem 14 fails to hold once again.

Taking everything into consideration, we may assume that $\Phi_f(x) \mid Q_{a,b}(x)$ where $f \in \mathbb{N}$ is such that:

- $f \geqslant 2$ and $f \mid \frac{n}{2}$;
- $8 \nmid f$ and $p^2 \nmid f$ for every prime $p \geqslant 3$.

We now divide the problem into two subcases depending on whether f contains a prime factor from the set $\{2, 3, 5, 7\}$.

Subcase 1.1: $2, 3, 5, 7 \nmid f$. In this subcase, it is obvious that f must be representable as a product of one or more distinct prime numbers greater than seven. By applying Theorem 8, we may cancel out all the prime factors of f, one by one, until there is exactly one left. This allows us to conclude that $\Phi_p(x) \mid Q_{a,b}(x)$ for some prime $p \geqslant 11$ such that $p \mid f$, hence $p \mid \frac{n}{2}$. By implementing Lemma 23, it becomes easy to see that $p \mid a, b$. However, this means that condition **(i)** from Theorem 14 does not hold.

Subcase 1.2: $\neg(2, 3, 5, 7 \nmid f)$. Here, we have that f contains at least one prime factor not greater than seven. We are now able to use Theorem 8 in order to cancel out all the prime factors of f greater than seven. Furthermore, if the obtained integer is simultaneously divisible by five and seven, we can implement Theorem 8 once more and cancel out one of them, given the fact that $(5-2)+(7-2) > (8-2)$. Bearing everything in mind, we get that $\Phi_{f'}(x) \mid Q_{a,b}(x)$ must hold for some integer $f' \in \mathbb{N}$ such that:

- $f' \geqslant 2$, $f' \mid \frac{n}{2}$ and f' contains no prime factor greater than seven;
- $8 \nmid f'$ and $p^2 \nmid f'$ for each prime $p \in \{3, 5, 7\}$;
- f' is not divisible by both five and seven.

It is not difficult to check that such an integer f' would necessarily have to belong to the set

$$\{2, 3, 4, 5, 6, 7, 10, 12, 14, 15, 20, 21, 28, 30, 42, 60, 84\}.$$

Furthermore, let us define $Q_{a,b}^{\bmod f'}(x)$ as the polynomial obtained from $Q_{a,b}(x)$ by replacing the power of each nonzero term by its remainder modulo f'. It is clear that $\Phi_{f'}(x) \mid Q_{a,b}(x)$ is equivalent to $\Phi_{f'}(x) \mid Q_{a,b}^{\bmod f'}(x)$. We now observe that for a fixed $f' \in \mathbb{N}$ one can determine a finite set

$$\Psi \subseteq \{0, 1, \dots, n-1\} \times \{0, 1, \dots, n-1\},$$

such that $\Phi_{f'}(x) \mid Q_{a,b}^{\bmod f'}(x)$ holds if and only if $(a \bmod p, b \bmod p) \in \Psi$. Given the fact that there are only 17 possible values for f', it is quite convenient to use a computer in order to determine all the modular conditions under which $\Phi_{f'}(x) \mid Q_{a,b}(x)$ is true for each feasible f'. The corresponding computational results are given in Appendix A. By examining the said results, it is not difficult to establish that at least one of the following statements has to be true:

- there exists a prime number $p \in \mathbb{N}$ such that $p \mid a, b, f'$;
- $f' = 4$ and a and b are both odd;
- $f' = 5$ and $5 \nmid a, b, a+b, a-b$.

If $p \mid a, b, f'$, we then clearly have $\gcd(\frac{n}{2}, a, b) \neq 1$, which implies that condition **(i)** given in Theorem 14 does not hold. Similarly, if $f' = 4$ and $2 \nmid a, b$, it can be immediately seen that $4 \mid \frac{n}{2}$, hence condition **(iii)** is not satisfied. Finally, if $f' = 5$ and $5 \nmid a, b, a+b, a-b$, then $5 \mid \frac{n}{2}$, which means that condition **(iv)** from Theorem 14 does not hold, as desired.

Case 2: $\Phi_f(x) \mid R_{a,b}(x)$. In this case, we can apply the same initial discussion once again in order to show that we may asume that $\Phi_f(x) \mid R_{a,b}(x)$ holds for some integer $f \in \mathbb{N}$ such that:

- $f \mid n$ and $2 \nmid \frac{n}{f}$;
- $8 \nmid f$ and $p^2 \nmid f$ for every prime $p \geqslant 3$.

It is now convenient to divide the problem into two subcases in the same manner as it was done in the previous case.

Subcase 2.1: $2, 3, 5, 7 \nmid f$. This subcase can be resolved in an entirely analogous manner as subcase 1.1. For this reason, we choose to omit the proof details.

Subcase 2.2: $\neg(2, 3, 5, 7 \nmid f)$. In this subcase, we can implement Theorem 8 in an identical manner as done so in subcase 1.2. This allows us to reach that $\Phi_{f'}(x) \mid R_{a,b}(x)$ must be true for some integer $f' \in \mathbb{N}$ such that:

- $f' \mid n$, $2 \nmid \frac{n}{f'}$ and f' contains no prime factor greater than seven;
- $8 \nmid f'$ and $p^2 \nmid f'$ for each prime $p \in \{3, 5, 7\}$;
- f' is not divisible by both five and seven.

Taking into account that $f' \neq 1$, this means that f' once again certainly belongs to the set

$$\{2, 3, 4, 5, 6, 7, 10, 12, 14, 15, 20, 21, 28, 30, 42, 60, 84\}.$$

By defining $R_{a,b}^{\bmod p}(x)$ in an analogous manner as $Q_{a,b}^{\bmod p}(x)$ was defined in case 1, it becomes possible to inspect the precise modular conditions that a and b have to satisfy in order for $\Phi_{f'} \mid R_{a,b}(x)$ to be true for a given value of f'. Of course, the aforementioned examination can be easily performed via computer. The corresponding computational results are disclosed in Appendix B and by analyzing the obtained results it is possible to conclude that f' is surely even. Moreover, at least one of the following statements is certainly true:

- there exists a prime number $p \in \mathbb{N}$ such that $p \mid a, b, \frac{f'}{2}$;

- $f' = 2$ and a and b are both odd;
- $f' = 4$ and a and b are both odd;
- $f' = 10$ and $5 \nmid a, b, a-b, a+b$.

If there exists a prime p such that $p \mid a, b, \frac{f'}{2}$, it is evident that $\gcd(\frac{n}{2}, a, b) \neq 1$, hence condition **(i)** from Theorem 14 is not satisfied. Furthermore, if $f' = 2$ and $2 \nmid a, b$, then it is easy to see that $n \equiv_4 2$, which means that condition **(ii)** fails to hold. Similarly, if $f' = 4$ and $2 \nmid a, b$, then we get $4 \mid n$, which implies that condition **(iii)** is not satisfied. Finally, if $f' = 10$ and $5 \nmid a, b, a-b, a+b$, it is straightforward to deduce that condition **(iv)** from Theorem 14 fails to hold. □

Remark 24. In an analogous manner as done so in Section 5, it is possible to demonstrate that $T_4(n, a, b)$ is always isomorphic to

$$T_4\left(n, \min(ta \bmod n, n - ta \bmod n), \min(tb \bmod n, n - tb \bmod n)\right)$$

whenever $\gcd(n, t) = 1$. From here, it follows that if $4 \mid n$, then a tricirculant graph of type 4 is a nut graph if and only if it is representable as $T_4(n, a, b)$ where $1 \leqslant a, b < \frac{n}{2}$, $\gcd(a, b) = 1$, $a \not\equiv_2 b$, and $5 \mid ab(a-b)(a+b)$ provided $10 \mid n$.

Acknowledgements

I. Damnjanović is grateful to the University of Primorska, University of Ljubljana, Inštitut za matematiko, fiziko in mehaniko and Diffine LLC for all the support given throughout the duration of the research. T. Pisanski gratefully acknowledges the support provided by the Mathematical Institute of the Serbian Academy of Sciences and Arts. This work is supported in part by the Slovenian Research Agency (research program P1-0294 and research projects N1-0140, J1-2481, J1-3002 and J1-4351).

References

[1] N. Bašić, M. Knor and R. Škrekovski. On 12-regular nut graphs. *Art Discrete Appl. Math.*, 5(2): #P2.01, 2022.

[2] K. Coolsaet, P.W. Fowler and J. Goedgebeur. Generation and properties of nut graphs. *MATCH Commun. Math. Comput. Chem.*, 80: 423–444, 2018.

[3] D.M. Cvetković, M. Doob and H. Sachs. *Spectra of graphs: Theory and applications*, Leipzig: J. A. Barth Verlag, 1995.

[4] I. Damnjanović. Two families of circulant nut graphs. *Filomat*, 37(24): 8331–8360, 2023.

[5] I. Damnjanović. Complete resolution of the circulant nut graph order–degree existence problem. *Ars Math. Contemp.*, 2023.

[6] I. Damnjanović. On the nullities of quartic circulant graphs and their extremal null spaces. arXiv:2212.12959, 2022.

[7] I. Damnjanović and D. Stevanović. On circulant nut graphs. *Linear Algebra Appl.*, 633: 127–151, 2022.

[8] M. Filaseta and A. Schinzel. On testing the divisibility of lacunary polynomials by cyclotomic polynomials. *Math. Comput.*, 73(246): 957–965, 2003.

[9] P.W. Fowler, J.B. Gauci, J. Goedgebeur, T. Pisanski and I. Sciriha. Existence of regular nut graphs for degree at most 11. *Discuss. Math. Graph Theory*, 40: 533–557, 2020.

[10] P.W. Fowler, B.T. Pickup, T.Z. Todorova, M. Borg and I. Sciriha. Omni-conducting and omni-insulating molecules. *J. Chem. Phys.*, 140(5): 054115, 2014.

[11] P.W. Fowler, T. Pisanski and N. Bašić. Charting the space of chemical nut graphs. *MATCH Commun. Math. Comput. Chem.*, 86(3): 519–538, 2021.

[12] J.B. Gauci, T. Pisanski and I. Sciriha. Existence of regular nut graphs and the Fowler construction. *Appl. Anal. Discrete Math.*, 2023.

[13] R.M. Gray. Toeplitz and circulant matrices: A review. *Found. Trends Commun. Inf.* Theory, 2: 155–239, 2006. https://ee.stanford.edu/~gray/CIT006-journal.pdf.

[14] I. Kovács, K. Kutnar, D. Marušič and S. Wilson. Classification of cubic symmetric tricirculants. *Electron. J. Combin.*, 19(2): P24, 2012.

[15] T. Nagell. *Introduction to Number Theory*, Wiley, New York, 1951.

[16] T. Pisanski. A classification of cubic bicirculants. *Discrete Math.*, 307(3–5): 567–578, 2007.

[17] T. Pisanski and A. Žitnik. Classification of quartic bicirculant nut graphs, manuscript.

[18] P. Potočnik and M. Toledo. Classification of cubic vertex-transitive tricirculants. *Ars Math. Contemp.*, 18: 1–31, 2020.

[19] I. Sciriha. On the coefficient of λ in the characteristic polynomial of singular graphs. *Util. Math.*, 52: 97–111, 1997.

[20] I. Sciriha. On singular line graphs of trees. *Congr. Numerantium*, 135: 73–91, 1998.

[21] I. Sciriha. On the construction of graphs of nullity one. *Discrete Math.*, 181(1–3): 193–211, 1998.

[22] I. Sciriha. The two classes of singular line graphs of trees. *Rend. Semin. Mat. Messina, Ser. II*, 20(5): 167–180, 1999.

[23] I. Sciriha. A characterization of singular graphs. *Electron. J. Linear Algebra*, 16: 451–462, 2007.

[24] I. Sciriha. Coalesced and embedded nut graphs in singular graphs. *Ars Math. Contemp.*, 1: 20–31, 2008.

[25] I. Sciriha and A. Farrugia. *From nut graphs to molecular structure and conductivity*, Mathematical chemistry monographs, No. 23, University of Kragujevac, Kragujevac, 2021.

[26] I. Sciriha and P.W. Fowler. Nonbonding orbitals in fullerenes: Nuts and cores in singular polyhedral graphs. *J. Chem. Inf. Model.*, 47(5): 1763–1775, 2007.

[27] I. Sciriha and P.W. Fowler. On nut and core singular fullerenes. *Discrete Math.*, 308(2–3): 267–276, 2008.

[28] I. Sciriha and I. Gutman. Nut graphs: maximally extending cores. *Util. Math.*, 54: 257–272, 1998.

[29] J. Tattersall. *Elementary number theory in nine chapters*, Cambridge University Press, New York, 1999.

[30] D.B. West. *Introduction to Graph Theory*, second edition, Prentice Hall, 2000.

[31] Cyclotomic polynomials, Encyclopedia of Mathematics, Springer Verlag GmbH, European Mathematical Society. https://encyclopediaofmath.org/index.php?title=Cyclotomic_polynomials.

A Inspection for $\Phi_f(x) \mid Q_{a,b}(x)$

In this appendix section, we disclose the computational results that describe all the possible modular conditions that $a, b \in \mathbb{N}$ have to adhere to in order for $\Phi_f(x) \mid Q_{a,b}(x)$ to be true, for certain values of $f \in \mathbb{N}$. The given results can be generated, for example, by using the following Wolfram Mathematica command:

```
MatrixForm[
 Table[{f,
   MatrixForm[
    Select[Flatten[Table[{a, b}, {a, 0, f - 1}, {b, 0, f - 1}], 1],
     Length[CoefficientRules[
         PolynomialRemainder[
          x^(2 #[[1]] + #[[2]]) + x^(#[[1]] + 2 #[[2]]) + x^#[[1]] +
           x^#[[2]] - x^(2 #[[1]] + 2 #[[2]]) - x^(2 #[[1]]) -
           x^(2 #[[2]]) - 1, Cyclotomic[f, x], x]]] == 0 &]]}, {f, {2,
     3, 4, 5, 6, 7, 10, 12, 14, 15, 20, 21, 28, 30, 42, 60, 84}}]]
```

f	$a \bmod f$	$b \bmod f$
2	0	0
3	0	0
4	0	0
	1	1
	1	3
	3	1
	3	3
5	0	0
	1	2
	1	3
	2	1
	2	4
	3	1
	3	4
	4	2
	4	3
6	0	0
7	0	0
10	0	0
	2	4
	2	6
	4	2
	4	8
	6	2
	6	8
	8	4
	8	6
12	0	0
	3	3
	3	9
	9	3
	9	9

f	$a \bmod f$	$b \bmod f$
14	0	0
15	0	0
	3	6
	3	9
	6	3
	6	12
	9	3
	9	12
	12	6
	12	9
20	0	0
	4	8
	4	12
	5	5
	5	15
	8	4
	8	16
	12	4
	12	16
	15	5
	15	15
	16	8
	16	12
21	0	0
28	0	0
	7	7
	7	21
	21	7
	21	21

f	$a \bmod f$	$b \bmod f$
30	0	0
	6	12
	6	18
	12	6
	12	24
	18	6
	18	24
	24	12
	24	18
42	0	0
60	0	0
	12	24
	12	36
	15	15
	15	45
	24	12
	24	48
	36	12
	36	48
	45	15
	45	45
	48	24
	48	36
84	0	0
	21	21
	21	63
	63	21
	63	63

B Inspection for $\Phi_f(x) \mid R_{a,b}(x)$

In this appendix section, we give the computational results that describe all the possible modular conditions that $a, b \in \mathbb{N}$ have to satisfy in order for $\Phi_f(x) \mid R_{a,b}(x)$ to hold, for concrete values of $f \in \mathbb{N}$. The said results can be quickly obtained, for example, by using the following Wolfram Mathematica command:

```
MatrixForm[
 Table[{f,
   MatrixForm[
    Select[Flatten[Table[{a, b}, {a, 0, f - 1}, {b, 0, f - 1}], 1],
     Length[CoefficientRules[
         PolynomialRemainder[
          x^(2 #[[1]] + #[[2]]) + x^(#[[1]] + 2 #[[2]]) + x^#[[1]] +
           x^#[[2]] + x^(2 #[[1]] + 2 #[[2]]) + x^(2 #[[1]]) +
           x^(2 #[[2]]) + 1, Cyclotomic[f, x], x]]] == 0 &]]}, {f, {2,
     3, 4, 5, 6, 7, 10, 12, 14, 15, 20, 21, 28, 30, 42, 60, 84}}]]
```

f	$a \bmod f$	$b \bmod f$
2	1	1
3		
4	1	1
	1	3
	2	2
	3	1
	3	3
5		
6	3	3
7		
10	1	3
	1	7
	3	1
	3	9
	5	5
	7	1
	7	9
	9	3
	9	7
12	3	3
	3	9
	6	6
	9	3
	9	9

f	$a \bmod f$	$b \bmod f$
14	7	7
15		
20	2	6
	2	14
	5	5
	5	15
	6	2
	6	18
	10	10
	14	2
	14	18
	15	5
	15	15
	18	6
	18	14
21		
28	7	7
	7	21
	14	14
	21	7
	21	21

f	$a \bmod f$	$b \bmod f$
30	3	9
	3	21
	9	3
	9	27
	15	15
	21	3
	21	27
	27	9
	27	21
42	21	21
60	6	18
	6	42
	15	15
	15	45
	18	6
	18	54
	30	30
	42	6
	42	54
	45	15
	45	45
	54	18
	54	42
84	21	21
	21	63
	42	42
	63	21
	63	63