Two families of circulant nut graphs

Ivan Damnjanović[a]

[a]University of Niš, Faculty of Electronic Engineering & Diffine LLC

Abstract. A circulant nut graph is a non-trivial simple graph whose adjacency matrix is a circulant matrix of nullity one such that its non-zero null space vectors have no zero elements. The study of circulant nut graphs was originally initiated by Bašić et al. [Art Discrete Appl. Math. 5(2) (2021) #P2.01], where a conjecture was made regarding the existence of all the possible pairs (n, d) for which there exists a d-regular circulant nut graph of order n. Later on, it was proved by Damnjanović and Stevanović [Linear Algebra Appl. 633 (2022) 127–151] that for each odd $t \geq 3$ such that $t \not\equiv_{10} 1$ and $t \not\equiv_{18} 15$, the $4t$-regular circulant graph of order n with the generator set $\{1, 2, 3, \ldots, 2t + 1\} \setminus \{t\})$ must necessarily be a nut graph for each even $n \geq 4t + 4$. In this paper, we extend these results by constructing two families of circulant nut graphs. The first family comprises the $4t$-regular circulant graphs of order n which correspond to the generator sets $\{1, 2, \ldots, t - 1\} \cup \left\{\frac{n}{4}, \frac{n}{4} + 1\right\} \cup \left\{\frac{n}{2} - (t - 1), \ldots, \frac{n}{2} - 2, \frac{n}{2} - 1\right\}$, for each odd $t \in \mathbb{N}$ and $n \geq 4t + 4$ divisible by four. The second family consists of the $4t$-regular circulant graphs of order n which correspond to the generator sets $\{1, 2, \ldots, t - 1\} \cup \left\{\frac{n+2}{4}, \frac{n+6}{4}\right\} \cup \left\{\frac{n}{2} - (t - 1), \ldots, \frac{n}{2} - 2, \frac{n}{2} - 1\right\}$, for each $t \in \mathbb{N}$ and $n \geq 4t + 6$ such that $n \equiv_4 2$. We prove that all of the graphs which belong to these families are indeed nut graphs, thereby fully resolving the $4t$-regular circulant nut graph order–degree existence problem whenever t is odd and partially solving this problem for even values of t as well.

1. Introduction

In this paper we will consider all graphs to be undirected, finite, simple and non-null. Thus, every graph will have at least one vertex and there shall be no loops or multiple edges. Also, for convenience, we will take that each graph of order n has the vertex set $\{0, 1, 2, \ldots, n - 1\}$.

A graph G is considered to be a circulant graph if its adjacency matrix A has the form

$$A = \begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \cdots & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \ldots & a_0 \end{bmatrix}.$$

Here, we clearly have $a_0 = 0$, as well as $a_j = a_{n-j}$ for all $j = \overline{1, n-1}$. A concise way of describing a circulant graph is by taking into consideration the set of all the values $1 \leq j \leq \frac{n}{2}$ such that $a_j = a_{n-j} = 1$. We shall refer

to this set as the generator set of a circulant graph and we will use $\mathrm{Circ}(n, S)$ to denote the circulant graph of order n whose generator set is S.

A nut graph is a non-trivial graph whose adjacency matrix has nullity one and is such that its non-zero null space vectors have no zero elements, as first described by Sciriha in [6]. Bearing this in mind, a circulant nut graph is simply a nut graph whose adjacency matrix additionally represents a circulant matrix. Bašić et al. [1] initiated the study of these graphs by providing several results, alongside the following two conjectures.

Conjecture 1 (Bašić et al. [1]). *For every even n, $n \geq 16$, there exists a circulant nut graph* $\mathrm{Circ}(n, \{s_1, s_2, s_3, s_4, s_5, s_6\})$ *of degree* 12.

Conjecture 2 (Bašić et al. [1]). *For every d, where $d \equiv_4 0$, and for every even n, $n \geq d + 4$, there exists a circulant nut graph* $\mathrm{Circ}(n, \{s_1, s_2, s_3, \ldots, s_{\frac{d}{2}}\})$ *of degree d.*

Later on, Damnjanović and Stevanović [2, Proposition 8] proved Conjecture 1 by showing that $\mathrm{Circ}(n, \{1, 2, 4, 5, 6, 7\})$ is a 12-regular nut graph for each even $n \geq 16$. In fact, it was shown that for infinitely many odd values of t it is possible to construct similar families of $4t$-regular circulant nut graphs, as demonstrated in the next theorem.

Theorem 1 (Damnjanović and Stevanović [2]). *For each odd $t \geq 3$ such that $t \not\equiv_{10} 1$ and $t \not\equiv_{18} 15$, the circulant graph* $\mathrm{Circ}(n, \{1, 2, 3, \ldots, 2t + 1\} \setminus \{t\})$ *is a nut graph for each even $n \geq 4t + 4$.*

The primary motivation behind this paper is to improve the currently existing results regarding the circulant nut graph order–degree existence problem. In other words, the goal is to answer the question whether there exists a d-regular circulant nut graph of order n, for any such pair $(n, d) \in \mathbb{N}^2$ of integers. As shown by Damnjanović and Stevanović [2, Lemma 6], the order of each circulant nut graph must be even, while its degree must be divisible by four. It is clear that a $4t$-regular circulant nut graph cannot have an order of $4t + 2$, since the adjacency matrix of such a graph would obviously have a nullity greater than one, due to the fact that its first $\frac{n}{2}$ rows would match its following $\frac{n}{2}$ rows, respectively.

Furthermore, if t is even, then the order of a $4t$-regular circulant nut graph cannot be below $4t + 6$, as demonstrated by Damnjanović and Stevanović [2, Lemma 18]. Bearing this in mind, we deduce that for a given $t \in \mathbb{N}$, all the $4t$-regular circulant nut graphs must have an even order n such that

- $n \geq 4t + 4$ if $2 \nmid t$;

- $n \geq 4t + 6$ if $2 \mid t$.

In this paper, we present the following two families of circulant graphs:

$$\mathcal{D}'_{t,n} = \mathrm{Circ}(n, \mathcal{S}'_{t,n}), \quad \text{for each } 2 \nmid t \text{ and } 4 \mid n \text{ such that } n \geq 4t + 4,$$
$$\mathcal{D}''_{t,n} = \mathrm{Circ}(n, \mathcal{S}''_{t,n}), \quad \text{for each } t \in \mathbb{N} \text{ and } n \equiv_4 2 \text{ such that } n \geq 4t + 6,$$

where

$$\mathcal{S}'_{t,n} = \{1, 2, \ldots, t - 1\} \cup \left\{\frac{n}{4}, \frac{n}{4} + 1\right\} \cup \left\{\frac{n}{2} - (t - 1), \ldots, \frac{n}{2} - 2, \frac{n}{2} - 1\right\},$$
$$\mathcal{S}''_{t,n} = \{1, 2, \ldots, t - 1\} \cup \left\{\frac{n+2}{4}, \frac{n+6}{4}\right\} \cup \left\{\frac{n}{2} - (t - 1), \ldots, \frac{n}{2} - 2, \frac{n}{2} - 1\right\}.$$

Subsequently, we prove that all of the graphs which belong to these families are nut graphs, thereby showing that for each odd t, there does exist a $4t$-regular circulant nut graph of order n, for any even $n \geq 4t + 4$. This observation fully resolves the circulant nut graph order–degree existence problem for $4t$-regular graphs whenever t is odd.

When it comes to the even values of t, we get a partial resolution of the existence problem, given the fact that the said constructions do cover the case when $n \equiv_4 2$. However, the case when n is divisible by four is not yet resolved, hence these graphs remain to be further inspected in the future.

The remainder of this paper is structured as follows. In Section 2 we preview certain theoretical facts regarding the circulant matrices, circulant nut graphs and cyclotomic polynomials which are required in order to successfully prove the two main theorems. Subsequently, Section 3 displays a full mathematical proof of the fact that each $\mathcal{D}'_{t,n}$ circulant graph is indeed a nut graph. Afterwards, Section 4 uses a similar strategy in order to prove that every $\mathcal{D}''_{t,n}$ graph must be a circulant nut graph as well. Finally, Section 5 provides a brief conclusion to all the obtained results and discloses a new conjecture to be solved later on.

2. Preliminaries

First of all, it is worth pointing out that the generator sets $\mathcal{S}'_{t,n}$ and $\mathcal{S}''_{t,n}$ are always well defined. It is straightforward to check that

$$1 < 2 < \cdots < t - 1 < \frac{n}{4} < \frac{n}{4} + 1 < \frac{n}{2} - (t-1) < \cdots < \frac{n}{2} - 2 < \frac{n}{2} - 1$$

for each odd $t \geq 3$ and $n \, (\geq 4t + 4)$ that is divisible by four. Similarly, we have

$$1 < 2 < \cdots < t - 1 < \frac{n+2}{4} < \frac{n+6}{4} < \frac{n}{2} - (t-1) < \cdots < \frac{n}{2} - 2 < \frac{n}{2} - 1$$

for every $t \geq 2$ and $n \geq 4t + 6$ such that $n \equiv_4 2$. Finally, for $t = 1$ we have that

$$1 < \frac{n}{4} < \frac{n}{4} + 1 \leq \frac{n}{2} - 1$$

for every $n \geq 4t + 4$ divisible by four, as well as

$$1 < \frac{n+2}{4} < \frac{n+6}{4} \leq \frac{n}{2} - 1$$

for each $n \geq 4t + 6$ such that $n \equiv_4 2$.

It is known from elementary linear algebra theory (see, for example, [4, Section 3.1]) that the circulant matrix

$$A = \begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \cdots & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \ldots & a_0 \end{bmatrix}$$

must have the eigenvalues

$$P(1), P(\omega), P(\omega^2), \ldots, P(\omega^{n-1}),$$

where $\omega = e^{i\frac{2\pi}{n}}$ is an n-th root of unity, and

$$P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}.$$

Starting from the aforementioned result, Damnjanović and Stevanović [2] have managed to give the necessary and sufficient conditions for a circulant graph to be a nut graph in the form of the following lemma.

Lemma 1 (Damnjanović and Stevanović [2]). *Let $G = \mathrm{Circ}(n, S)$ where $n \geq 2$. The graph G is a nut graph if and only if all of the following conditions hold:*

- $2 \mid n$;

- *S consists of t odd and t even integers from $\left\{1, 2, 3, \ldots, \frac{n}{2} - 1\right\}$, for some $t \geq 1$;*

- *$P(\omega^j) \neq 0$ for each $j \in \left\{1, 2, 3, \ldots, \frac{n}{2} - 1\right\}$.*

All of the graphs $\mathcal{D}'_{t,n}$ and $\mathcal{D}''_{t,n}$ clearly satisfy the first condition from Lemma 1. Besides that, it is easy to show that they necessarily satisfy the second condition as well. For $\mathcal{D}'_{t,n}$, it is enough to point out that both $\{1, 2, \ldots, t-1\}$ and $\left\{\frac{n}{2} - (t-1), \ldots, \frac{n}{2} - 2, \frac{n}{2} - 1\right\}$ contain an even number of consecutive integers, due to the fact that $t - 1$ is even. Since $\frac{n}{4}$ and $\frac{n}{4} + 1$ are surely of different parities, it follows that $\mathcal{S}'_{t,n}$ does contain equally many odd and even integers. For $\mathcal{D}''_{t,n}$, it is essential to notice that j and $\frac{n}{2} - j$ must be of different parities, for each $j = \overline{1, t-1}$, due to the fact that $\frac{n}{2}$ is odd. Furthermore, $\frac{n+2}{4}$ and $\frac{n+6}{4}$ are certainly of different parities, hence we obtain that $\mathcal{S}''_{t,n}$ contains equally many odd and even integers, too.

Taking into consideration Lemma 1, it becomes apparent that in order to show that each graph $\mathcal{D}'_{t,n}$ and $\mathcal{D}''_{t,n}$ is a nut graph, it is sufficient to prove that it satisfies the third condition given in the lemma. In other words, it is enough to demonstrate that, for these graphs, the polynomial $P(x) \in \mathbb{Z}[x]$ has no n-th roots of unity among its roots, except potentially -1 or 1.

It is clear that $\omega^{n-j} = \frac{1}{\omega^j}$ for each $j = \overline{1, n-1}$. Bearing this in mind, we quickly obtain that

$$P(\omega^j) = \left(\omega^{js_0} + \frac{1}{\omega^{js_0}}\right) + \left(\omega^{js_1} + \frac{1}{\omega^{js_1}}\right) + \cdots + \left(\omega^{js_{k-1}} + \frac{1}{\omega^{js_{k-1}}}\right) \tag{1}$$

for an arbitrary circulant graph $G = \text{Circ}(n, S)$, where $S = \{s_0, s_1, s_2, \ldots, s_{k-1}\}$, provided all the generator set elements are lower than $\frac{n}{2}$. Formula (1) will be heavily used throughout Sections 3 and 4 while proving the two main theorems of the paper.

Last but not least, it is crucial to point out that the cyclotomic polynomials shall play a key role in demonstrating whether certain polynomials of interest contain the given roots of unity among their roots. The cyclotomic polynomial $\Phi_b(x)$ can be defined for each $b \in \mathbb{N}$ via

$$\Phi_b(x) = \prod_{\zeta} (x - \zeta),$$

where ζ ranges over the primitive b-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, [7]). Hence, an arbitrary polynomial in $\mathbb{Q}[x]$ has a primitive b-th root of unity among its roots if and only if it is divisible by $\Phi_b(x)$.

While inspecting whether certain integer polynomials are divisible by cyclotomic polynomials, we will strongly rely on the following theorem on the divisibility of lacunary polynomials by cyclotomic polynomials.

Theorem 2 (Filaseta and Schinzel [3]). *Let $P(x) \in \mathbb{Z}[x]$ have N nonzero terms and let $\Phi_b(x) \mid P(x)$. Suppose that $p_1, p_2, \ldots, p_k$ are distinct primes such that*

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

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

3. D′(t, n) family of circulant graphs

In this section, we will formulate and provide a full mathematical proof of the first of the two central theorems given in the paper.

Theorem 3. *For each odd $t \in \mathbb{N}$ and $n \geq 4t + 4$ such that $4 \mid n$, the circulant graph $\mathcal{D}'_{t,n}$ must be a $4t$-regular nut graph of order n.*

In order to make the proof more concise, we will need a number of auxiliary lemmas. To start with, let $Q_t(x), R_t(x) \in \mathbb{Z}[x]$ be the following two integer polynomials

$$Q_t(x) = 2x^{2t-1} + x^{t+1} - x^t + x^{t-1} - x^{t-2} - 2,$$
$$R_t(x) = 2x^{2t-1} - x^{t+1} - 3x^t + 3x^{t-1} + x^{t-2} - 2,$$

for each odd $t \geq 3$. It is clear that all of these polynomials must have exactly six non-zero terms, due to the fact that

$$0 < t - 2 < t - 1 < t < t + 1 < 2t - 1$$

for each odd $t \geq 3$. Now, if we let

$$L_t = \{0, t - 2, t - 1, t, t + 1, 2t - 1\}$$

be the set consisting of the powers of these six terms, then it can be shown that this set has one valuable property, as described in the following lemma.

Lemma 2. *For each odd $t \geq 3$ and each prime number $p \geq 5$, the set L_t contains an element whose remainder modulo p is unique within the set.*

Proof. The four integers $t - 2, t - 1, t, t + 1$ are consecutive, hence it is clear that they all have mutually distinct remainders modulo p. Regardless of what their remainders modulo p are, at least two of these integers must have a remainder that is different from the remainders of both 0 and $2t - 1$. □

Lemma 2 proves to be useful while demonstrating one key property of the $Q_t(x)$ and $R_t(x)$ polynomials regarding their divisibility by cyclotomic polynomials. This is shown in the next lemma.

Lemma 3. *For any odd $t \geq 3$, neither $Q_t(x)$ nor $R_t(x)$ can be divisible by a cyclotomic polynomial $\Phi_b(x)$ such that $p^2 \mid b$ for some prime number p.*

Proof. Let $b \in \mathbb{N}$ be such that $p^2 \mid b$ for some prime number p. In this case, $\frac{b}{p}$ is a positive integer divisible by p, hence we get that $\Phi_b(x) = \Phi_{\frac{b}{p}}(x^p)$ (see, for example, [5, p. 160]).

Now, suppose that $\Phi_b(x) \mid Q_t(x)$ for some odd integer $t \geq 3$. It follows that $Q_t(x) = V(x)\,\Phi_b(x)$ for some polynomial $V(x) \in \mathbb{Q}[x]$. Let $Q_t^{(j)}(x)$ be the polynomial composed of all the terms of $Q_t(x)$ whose powers are congruent to j modulo p, for each $j = \overline{0, p - 1}$. Similarly, let $V^{(j)}(x)$ be the polynomial composed of all the terms of $V(x)$ whose powers are congruent to j modulo p, for each $j = \overline{0, p - 1}$. Given the fact that the powers of all the terms of $\Phi_b(x)$ are divisible by p, it swiftly follows that

$$Q_t^{(j)}(x) = V^{(j)}(x)\,\Phi_b(x)$$

must hold for all the $j = \overline{0, p - 1}$. In other words, we necessarily have

$$\Phi_b(x) \mid Q_t^{(j)}(x)$$

for all the $j = \overline{0, p - 1}$. The same reasoning and notation can be applied in the case that we suppose that $\Phi_b(x) \mid R_t(x)$ is true for some odd $t \geq 3$. We will finalize the proof of the lemma by taking into consideration three separate cases depending on the value of the prime number p.

Case $p \geq 5$. In this case, Lemma 2 dictates that the set L_t must contain an element whose remainder modulo p is unique within that set. In other words, there exists a j, $0 \leq j \leq p - 1$ such that both $Q_t^{(j)}(x)$ and $R_t^{(j)}(x)$

consist of exactly one non-zero term, i.e. have the form $c\,x^a$ for some $c \in \mathbb{Z} \setminus \{0\}$ and $a \in \mathbb{N}_0$. If we suppose that either $\Phi_b(x) \mid Q_t(x)$ or $\Phi_b(x) \mid R_t(x)$, this implies that $\Phi_b(x)$ must necessarily divide a polynomial with the aforementioned form $c\,x^a$, which is clearly impossible.

Case $p = 3$. This case can be quickly resolved by taking into consideration the modular values given in Table 1. We divide the case into three subcases depending on the value of t mod 3.

	$t \equiv_3 0$	$t \equiv_3 1$	$t \equiv_3 2$
0 mod 3	0	0	0
$(t-2)$ mod 3	1	2	0
$(t-1)$ mod 3	2	0	1
t mod 3	0	1	2
$(t+1)$ mod 3	1	2	0
$(2t-1)$ mod 3	2	1	0

Table 1: The elements of the set L_t modulo 3.

Subcase $t \equiv_3 0$. If we suppose that $\Phi_b(x) \mid Q_t(x)$, we get $\Phi_b(x) \mid x^{t+1} - x^{t-2}$. Similarly, $\Phi_b(x) \mid R_t(x)$ would imply $\Phi_b(x) \mid -x^{t+1} + x^{t-2}$. Either way, we obtain

$$\Phi_b(x) \mid x^{t+1} - x^{t-2}$$
$$\implies \quad \Phi_b(x) \mid x^{t-2}\,(x^3 - 1)$$
$$\implies \quad \Phi_b(x) \mid x^3 - 1,$$

which is not possible.

Subcase $t \equiv_3 1$. Regardless of whether we suppose that $\Phi_b(x) \mid Q_t(x)$ holds or $\Phi_b(x) \mid R_t(x)$, we obtain that $\Phi_b(x) \mid x^{t+1} - x^{t-2}$ must be true, which is impossible as we have already demonstrated in the previous subcase.

Subcase $t \equiv_3 2$. Bearing in mind the modular values given in Table 1, we conclude that $\Phi_b(x) \mid Q_t(x)$ or $\Phi_b(x) \mid R_t(x)$ would surely imply that $\Phi_b(x) \mid y^t$, which is not possible.

Case $p = 2$. In this case, we have that the integers $t-2, t, 2t-1$ are odd, while $0, t-1, t+1$ are even. We will resolve this case separately for $Q_t(x)$ and $R_t(x)$, thus yielding two subcases.

Subcase $\Phi_b(x) \mid Q_t(x)$. Suppose that $\Phi_b(x) \mid Q_t(x)$. We now get

$$\Phi_b(x) \mid 2x^{2t-1} - x^t - x^{t-2}, \tag{2}$$
$$\Phi_b(x) \mid x^{t+1} + x^{t-1} - 2. \tag{3}$$

If we take into consideration that $2x^{2t-1} - x^t - x^{t-2} = x^{t-2}\,(2x^{t+1} - x^2 - 1)$, Eq. (2) helps us obtain

$$\Phi_b(x) \mid 2x^{t+1} - x^2 - 1. \tag{4}$$

By subtracting the right-hand sides of Eqs. (3) and (4), we further conclude that

$$\Phi_b(x) \mid (2x^{t+1} - x^2 - 1) - (x^{t+1} + x^{t-1} - 2)$$
$$\implies \quad \Phi_b(x) \mid x^{t+1} - x^{t-1} - x^2 + 1$$
$$\implies \quad \Phi_b(x) \mid (x^{t-1} - 1)(x^2 - 1)$$
$$\implies \quad \Phi_b(x) \mid x^{t-1} - 1. \tag{5}$$

Now, if we subtract the right-hand sides of Eqs. (3) and (5), we get $\Phi_b(x) \mid x^{t+1} - 1$, which directly implies

$$\Phi_b(x) \mid (x^{t+1} - 1) - (x^{t-1} - 1)$$
$$\implies \quad \Phi_b(x) \mid x^{t+1} - x^{t-1}$$
$$\implies \quad \Phi_b(x) \mid x^{t-1}(x^2 - 1)$$
$$\implies \quad \Phi_b(x) \mid x^2 - 1,$$

which is not possible. Hence, $\Phi_b(x) \mid Q_t(x)$ cannot hold, as desired.

Subcase $\Phi_b(x) \mid R_t(x)$. If we suppose that $\Phi_b(x) \mid R_t(x)$, it follows that

$$\Phi_b(x) \mid 2x^{2t-1} - 3x^t + x^{t-2}, \tag{6}$$
$$\Phi_b(x) \mid -x^{t+1} + 3x^{t-1} - 2. \tag{7}$$

Given the fact that $2x^{2t-1} - 3x^t + x^{t-2} = x^{t-2}(2x^{t+1} - 3x^2 + 1)$, Eq. (6) yields

$$\Phi_b(x) \mid 2x^{t+1} - 3x^2 + 1. \tag{8}$$

Now, by subtracting the right-hand sides of Eqs. (7) and (8), we further obtain

$$\Phi_b(x) \mid (2x^{t+1} - 3x^2 + 1) - (-x^{t+1} + 3x^{t-1} - 2)$$
$$\implies \quad \Phi_b(x) \mid 3x^{t+1} - 3x^{t-1} - 3x^2 + 3$$
$$\implies \quad \Phi_b(x) \mid 3(x^{t-1} - 1)(x^2 - 1)$$
$$\implies \quad \Phi_b(x) \mid x^{t-1} - 1. \tag{9}$$

If we take the right-hand side of Eq. (9), multiply it by two, then subtract it from the right-hand side of Eq. (7), we will get another polynomial that is divisible by $\Phi_b(x)$. In other words, we have

$$\Phi_b(x) \mid (-x^{t+1} + 3x^{t-1} - 2) - 2(x^{t-1} - 1)$$
$$\implies \quad \Phi_b(x) \mid -x^{t+1} + x^{t-1}$$
$$\implies \quad \Phi_b(x) \mid x^{t-1}(1 - x^2)$$
$$\implies \quad \Phi_b(x) \mid 1 - x^2,$$

which is not possible. Thus, $\Phi_b(x) \mid R_t(x)$ cannot be true. $\quad \square$

Lemma 3 tells us that the only cyclotomic polynomials $\Phi_b(x)$ that could divide either $Q_t(x)$ or $R_t(x)$ are those where $b \in \mathbb{N}$ is a square-free integer. In fact, for any odd $t \geq 3$, the only cyclotomic polynomials that do divide these polynomials are $\Phi_1(b)$ and $\Phi_2(b)$. This observation will prove to be of the utmost importance while formulating the complete proof of Theorem 3 later on. However, in order to prove this statement, we shall need two more additional lemmas. We begin with the next one.

Lemma 4. *For each odd $t \geq 3$ and each prime number $p \geq 7$, neither $Q_t(x)$ nor $R_t(x)$ can be divisible by the cyclotomic polynomial $\Phi_p(x)$ or the cyclotomic polynomial $\Phi_{2p}(x)$.*

Proof. First of all, it is important to notice that for all prime numbers $p \geq 7$ we have

$$\Phi_p(x) = \sum_{j=0}^{p-1} x^j, \qquad\qquad \Phi_{2p}(x) = \sum_{j=0}^{p-1} (-1)^j x^j.$$

Here, it is clear that $\deg \Phi_p = \deg \Phi_{2p} = p - 1$. We will finish the proof of the lemma by splitting the problem into two separate cases depending on whether we are dealing with $\Phi_p(x)$ or $\Phi_{2p}(x)$.

Case $\Phi_p(x)$. Let $Q_t^{\mathrm{mod}\,p}(x)$ and $R_t^{\mathrm{mod}\,p}(x)$ be the following two polynomials:

$$Q_t^{\mathrm{mod}\,p}(x) = 2x^{(2t-1)\bmod p} + x^{(t+1)\bmod p} - x^{t\bmod p} + x^{(t-1)\bmod p} - x^{(t-2)\bmod p} - 2,$$
$$R_t^{\mathrm{mod}\,p}(x) = 2x^{(2t-1)\bmod p} - x^{(t+1)\bmod p} - 3x^{t\bmod p} + 3x^{(t-1)\bmod p} + x^{(t-2)\bmod p} - 2.$$

Suppose that $\Phi_p(x) \mid Q_t(x)$. In this case, it is clear that $\Phi_p(x) \mid Q_t^{\mathrm{mod}\,p}(x)$ must hold, too. Given the fact that $\deg Q_t^{\mathrm{mod}\,p} \le p - 1 = \deg \Phi_p$, we further get two possibilities:

- $Q_t^{\mathrm{mod}\,p}(x) \equiv 0$;

- $Q_t^{\mathrm{mod}\,p}(x) = c\,\Phi_p(x)$ for some $c \in \mathbb{Q} \setminus \{0\}$.

By virtue of Lemma 2, there must exist a non-zero term in $Q_t(x)$ whose power has a unique remainder modulo p. This directly implies that $Q_t^{\mathrm{mod}\,p}(x) \equiv 0$ cannot hold. On the other hand, $Q_t^{\mathrm{mod}\,p}(x) = c\,\Phi_p(x)$ implies that $Q_t^{\mathrm{mod}\,p}(x)$ and $\Phi_p(x)$ must have the same number of non-zero terms, i.e. $Q_t^{\mathrm{mod}\,p}(x)$ needs to have exactly p non-zero terms. This is clearly impossible due to the fact that $Q_t^{\mathrm{mod}\,p}(x)$ has at most six non-zero terms. We conclude that $\Phi_p(x) \mid Q_t(x)$ cannot be true.

The proof of $\Phi_p(x) \nmid R_t(x)$ is completely analogous to the previously described proof of $\Phi_p(x) \nmid Q_t(x)$. Thus, it will be left out.

Case $\Phi_{2p}(x)$. Let $\overline{Q}_t^{\mathrm{mod}\,p}(x)$ and $\overline{R}_t^{\mathrm{mod}\,p}(x)$ be the following two polynomials:

$$\overline{Q}_t^{\mathrm{mod}\,p}(x) = 2(-1)^{\lfloor \frac{2t-1}{p} \rfloor} x^{(2t-1)\bmod p} + (-1)^{\lfloor \frac{t+1}{p} \rfloor} x^{(t+1)\bmod p} - (-1)^{\lfloor \frac{t}{p} \rfloor} x^{t\bmod p}$$
$$+ (-1)^{\lfloor \frac{t-1}{p} \rfloor} x^{(t-1)\bmod p} - (-1)^{\lfloor \frac{t-2}{p} \rfloor} x^{(t-2)\bmod p} - 2,$$
$$\overline{R}_t^{\mathrm{mod}\,p}(x) = 2(-1)^{\lfloor \frac{2t-1}{p} \rfloor} x^{(2t-1)\bmod p} - (-1)^{\lfloor \frac{t+1}{p} \rfloor} x^{(t+1)\bmod p} - 3(-1)^{\lfloor \frac{t}{p} \rfloor} x^{t\bmod p}$$
$$+ 3(-1)^{\lfloor \frac{t-1}{p} \rfloor} x^{(t-1)\bmod p} + (-1)^{\lfloor \frac{t-2}{p} \rfloor} x^{(t-2)\bmod p} - 2.$$

Since each primitive $2p$-th root of unity gives -1 when raised to the power of p, it becomes evident that $\Phi_{2p}(x) \mid Q_t(x)$ is equivalent to $\Phi_{2p}(x) \mid \overline{Q}_t^{\mathrm{mod}\,p}(x)$. Likewise, $\Phi_{2p}(x) \mid R_t(x)$ will hold if and only if $\Phi_{2p}(x) \mid \overline{R}_t^{\mathrm{mod}\,p}(x)$ does, too.

Now, suppose that $\Phi_{2p}(x) \mid Q_t(x)$. In this case we obtain $\Phi_{2p} \mid \overline{Q}_t^{\mathrm{mod}\,p}(x)$, where $\deg \overline{Q}_t^{\mathrm{mod}\,p} \le p - 1 = \deg \Phi_{2p}$. Like in the previous case, we get two possible options:

- $\overline{Q}_t^{\mathrm{mod}\,p}(x) \equiv 0$;

- $\overline{Q}_t^{\mathrm{mod}\,p}(x) = c\,\Phi_{2p}(x)$ for some $c \in \mathbb{Q} \setminus \{0\}$.

Lemma 2 dictates that there must exist a non-zero term in $Q_t(x)$ whose power has a unique remainder modulo p, which means that it is impossible for $\overline{Q}_t^{\mathrm{mod}\,p}(x) \equiv 0$ to be true. On the other hand, from $\overline{Q}_t^{\mathrm{mod}\,p}(x) = c\,\Phi_{2p}(x)$ we get that $\overline{Q}_t^{\mathrm{mod}\,p}(x)$ must have exactly p non-zero terms. However, this is not possible since it is clear that this polynomial cannot have more than six non-zero terms. It swiftly follows that $\Phi_{2p}(x) \nmid Q_t(x)$.

The proof of $\Phi_{2p}(x) \nmid R_t(x)$ is entirely analogous to the elaborated proof of $\Phi_{2p}(x) \nmid Q_t(x)$. For this reason, we choose to leave it out. $\square$

As the final piece of the puzzle, we will need to show that some concrete cyclotomic polynomials cannot divide $Q_t(x)$ or $R_t(x)$, for each odd integer $t \ge 3$. More precisely, we will turn our interest to the cyclotomic polynomials $\Phi_b(x)$ where b is a square-free integer all of whose prime factors belong to the set $\{2, 3, 5\}$.

Lemma 5. *For each odd $t \geq 3$ and each positive integer $b \in \{3, 5, 6, 10, 15, 30\}$, the cyclotomic polynomial $\Phi_b(x)$ divides neither $Q_t(x)$ nor $R_t(x)$.*

Proof. Similarly as in the proof of Lemma 4, let $Q_t^{\mathrm{mod}\,b}(x)$ and $R_t^{\mathrm{mod}\,b}(x)$ be the next two polynomials:

$$Q_t^{\mathrm{mod}\,b}(x) = 2x^{(2t-1)\,\mathrm{mod}\,b} + x^{(t+1)\,\mathrm{mod}\,b} - x^{t\,\mathrm{mod}\,b} + x^{(t-1)\,\mathrm{mod}\,b} - x^{(t-2)\,\mathrm{mod}\,b} - 2,$$
$$R_t^{\mathrm{mod}\,b}(x) = 2x^{(2t-1)\,\mathrm{mod}\,b} - x^{(t+1)\,\mathrm{mod}\,b} - 3x^{t\,\mathrm{mod}\,b} + 3x^{(t-1)\,\mathrm{mod}\,b} + x^{(t-2)\,\mathrm{mod}\,b} - 2.$$

Here, it is imperative for us to notice that $\Phi_b(x) \mid Q_t(x) \iff \Phi_b(x) \mid Q_t^{\mathrm{mod}\,b}(x)$ and also that $\Phi_b(x) \mid R_t(x) \iff \Phi_b(x) \mid R_t^{\mathrm{mod}\,b}(x)$. However, for a fixed value of $b \in \mathbb{N}$, there exist only finitely many polynomials $Q_t^{\mathrm{mod}\,b}(x)$ and $R_t^{\mathrm{mod}\,b}(x)$, as t ranges over the odd integers greater than or equal to three. This is a direct consequence of the fact that t can only have finitely many remainders modulo b. Hence, if we are able to show that $\Phi_b(x)$ divides none of these concrete polynomials, this is sufficient to prove that $\Phi_b(x)$ divides neither $Q_t(x)$ nor $R_t(x)$.

In order to prove the lemma, it is enough to demonstrate that $\Phi_b(x) \nmid Q_t^{\mathrm{mod}\,b}(x)$ and $\Phi_b(x) \nmid R_t^{\mathrm{mod}\,b}(x)$ for all the $b \in \{3, 5, 6, 10, 15, 30\}$ and for all the possible remainders $t \bmod b$. Doing this is trivial via computer with the help of some symbolic computation software. We disclose the required computational results in the form of two tables which are given in Appendix A and Appendix B. These results clearly indicate that for each $b \in \{3, 5, 6, 10, 15, 30\}$ the remainders $Q_t^{\mathrm{mod}\,b}(x) \bmod \Phi_b(x)$ and $R_t^{\mathrm{mod}\,b}(x) \bmod \Phi_b(x)$ can never be equal to the zero polynomial, regardless of what the value of $t \bmod b$ is, which completes the proof of the lemma. $\square$

It is important to notice that Theorem 2 can very conveniently be used on the polynomials $Q_t(x)$ and $R_t(x)$, given the fact that they only have six non-zero terms. This means that if $\Phi_b(x) \mid Q_t(x)$ and $p \mid b$ for some square-free integer b and some prime number $p \geq 7$, we can immediately deduce that $\Phi_{\frac{b}{p}}(x) \mid Q_t(x)$ is true as well. The same can be said regarding $R_t(x)$. This practically means that if the aforementioned divisibility holds, we can cancel out as many prime factors of b that are not below seven as we want, and the divisibility will still have to hold. Bearing this in mind, we are now able to formulate and prove the following lemma regarding the divisibility of $Q_t(x)$ and $R_t(x)$ by cyclotomic polynomials.

Lemma 6. *For each odd $t \geq 3$, neither $Q_t(x)$ nor $R_t(x)$ can be divisible by a cyclotomic polynomial $\Phi_b(x)$ where $b \geq 3$.*

Proof. The proof will only be given for $Q_t(x)$, given the fact that the proof regarding $R_t(x)$ is completely analogous. Suppose that $\Phi_b(x) \mid Q_t(x)$ for some $b \geq 3$. By virtue of Lemma 3, we know that b needs to be a square-free integer. We now divide the problem into two separate cases, depending on whether b is divisible by either 3 or 5, or not.

Case $3 \nmid b$ and $5 \nmid b$. In this case, it is clear that b has at least one prime factor greater than 5, since $b \notin \{1, 2\}$. If we repeatedly use Theorem 2 in order to cancel out all the prime factors of b that are greater than 5, until exactly one is left, we obtain that

$$\Phi_{b'}(x) \mid Q_t(x)$$

must hold, where b' is square-free, not divisible by 3 or 5, and has exactly one prime factor greater than 5. In other words, we get that either $\Phi_p(x) \mid Q_t(x)$ or $\Phi_{2p} \mid Q_t(x)$ holds, for some prime number $p \geq 7$. However, this is not possible according to Lemma 4.

Case $3 \mid b$ or $5 \mid b$. Here, we can simply use Theorem 2 in order to cancel out all the prime factors of b that are greater than 5, until there are none left. This leads us to

$$\Phi_{b'}(x) \mid Q_t(x),$$

where b' is square-free, divisible by 3 or 5, and has no prime factors outside of the set $\{2, 3, 5\}$. These conditions imply that $b' \in \{3, 5, 6, 10, 15, 30\}$. However, in this case $\Phi_{b'}(x) \mid Q_t(x)$ cannot possibly hold, as a direct consequence of Lemma 5.

Both of the cases have led to a contradiction, which means that $\Phi_b(x) \mid Q_t(x)$ cannot hold for any $b \geq 3$. $\quad\square$

Lemma 6 allows us to finish the proof of Theorem 3. We present the rest of the proof in the remainder of this section.

Proof of Theorem 3. The proof for the case $t = 1$ is fairly straightforward. Due to the fact that $\mathcal{S}'_{1,n} = \left\{\frac{n}{4}, \frac{n}{4} + 1\right\}$, Eq. (1) immediately gives us

$$P(\zeta) = \zeta^{\frac{n}{4}} + \frac{1}{\zeta^{\frac{n}{4}}} + \zeta^{\frac{n}{4}+1} + \frac{1}{\zeta^{\frac{n}{4}+1}}, \tag{10}$$

where ζ is an arbitrary n-th root of unity different from 1 and -1. Now, the condition $P(\zeta) = 0$ becomes equivalent to

$$P(\zeta) = 0$$
$$\iff \quad \zeta^{\frac{n}{4}+1}\left(\zeta^{\frac{n}{4}} + \frac{1}{\zeta^{\frac{n}{4}}} + \zeta^{\frac{n}{4}+1} + \frac{1}{\zeta^{\frac{n}{4}+1}}\right) = 0$$
$$\iff \quad \zeta^{\frac{n}{2}+2} + \zeta^{\frac{n}{2}+1} + \zeta + 1 = 0$$
$$\iff \quad (\zeta + 1)\left(\zeta^{\frac{n}{2}+1} + 1\right) = 0$$
$$\iff \quad \zeta^{\frac{n}{2}+1} + 1 = 0.$$

Since we know that $\zeta^{\frac{n}{2}} \in \{1, -1\}$, we obtain that $\zeta^{\frac{n}{2}+1} + 1$ is equal to $\zeta + 1$ or $-\zeta + 1$. Either way, this value cannot be equal to 0, hence we conclude that $P(\zeta) \neq 0$. Since the value ζ was arbitrarily chosen, we obtain that no n-th root of unity different from 1 and -1 can be a root of $P(x)$. According to Lemma 1, this means that $\mathcal{D}'_{1,n}$ is indeed a circulant nut graph for any $n \geq 8$ divisble by four, as desired.

Now, we turn our attention to the case when $t \geq 3$. In this scenario, Eq. (1) gives us

$$P(\zeta) = \left(\zeta^{\frac{n}{4}} + \frac{1}{\zeta^{\frac{n}{4}}}\right) + \left(\zeta^{\frac{n}{4}+1} + \frac{1}{\zeta^{\frac{n}{4}+1}}\right) + \sum_{j=1}^{t-1}\left(\zeta^j + \frac{1}{\zeta^j}\right) + \sum_{j=\frac{n}{2}-t+1}^{\frac{n}{2}-1}\left(\zeta^j + \frac{1}{\zeta^j}\right),$$

where ζ is an arbitrarily chosen n-th root of unity different from 1 and -1. It is easy to further conclude that

$$P(\zeta) = \left(\zeta^{\frac{n}{4}+1} + \zeta^{\frac{n}{4}} + \frac{1}{\zeta^{\frac{n}{4}}} + \frac{1}{\zeta^{\frac{n}{4}+1}}\right) + \sum_{j=1}^{t-1}\left(\zeta^j + \frac{1}{\zeta^j} + \zeta^{\frac{n}{2}-j} + \frac{1}{\zeta^{\frac{n}{2}-j}}\right). \tag{11}$$

We will finish the proof by showing that $P(\zeta) \neq 0$ must necessarily hold. In order to make the proof more concise, we will divide it into two cases depending on whether $\zeta^{\frac{n}{2}}$ is equal to 1 or -1.

Case $\zeta^{\frac{n}{2}} = -1$. In this case, we have that $\zeta^{\frac{n}{2}-j} = -\frac{1}{\zeta^j}$ and $\frac{1}{\zeta^{\frac{n}{2}-j}} = -\zeta^j$, which quickly implies

$$\zeta^j + \frac{1}{\zeta^j} + \zeta^{\frac{n}{2}-j} + \frac{1}{\zeta^{\frac{n}{2}-j}} = 0$$

for any $j = \overline{1, t-1}$. Thus, Eq. (11) simplifies to the following formula:

$$P(\zeta) = \zeta^{\frac{n}{4}+1} + \zeta^{\frac{n}{4}} + \frac{1}{\zeta^{\frac{n}{4}}} + \frac{1}{\zeta^{\frac{n}{4}+1}}.$$

However, the obtained formula is exactly the same as Eq. (10), which we got while dealing with the case $t = 1$. Hence, an almost absolutely identical proof can be used in order to show that $P(\zeta) \neq 0$.

Case $\zeta^{\frac{n}{2}} = 1$. Here, we obtain that $\zeta^{\frac{n}{2}-j} = \dfrac{1}{\zeta^j}$ and $\dfrac{1}{\zeta^{\frac{n}{2}-j}} = \zeta^j$. This means that

$$\zeta^j + \frac{1}{\zeta^j} + \zeta^{\frac{n}{2}-j} + \frac{1}{\zeta^{\frac{n}{2}-j}} = 2\left(\zeta^j + \frac{1}{\zeta^j}\right)$$

for any $j = \overline{1, t-1}$. According to Eq. (11), the condition $P(\zeta) = 0$ becomes equivalent to

$$P(\zeta) = 0$$

$$\Longleftrightarrow \qquad \left(\zeta^{\frac{n}{4}+1} + \zeta^{\frac{n}{4}} + \frac{1}{\zeta^{\frac{n}{4}}} + \frac{1}{\zeta^{\frac{n}{4}+1}}\right) + 2\sum_{j=1}^{t-1}\left(\zeta^j + \frac{1}{\zeta^j}\right) = 0$$

$$\Longleftrightarrow \qquad \left(\zeta^{\frac{n}{4}+1} + \zeta^{\frac{n}{4}} + \frac{1}{\zeta^{\frac{n}{4}}} + \frac{1}{\zeta^{\frac{n}{4}+1}}\right) - 2 + 2\sum_{j=1-t}^{t-1}\zeta^j = 0$$

$$\Longleftrightarrow \qquad \zeta^{t-1}\left(\left(\zeta^{\frac{n}{4}+1} + \zeta^{\frac{n}{4}} + \frac{1}{\zeta^{\frac{n}{4}}} + \frac{1}{\zeta^{\frac{n}{4}+1}}\right) - 2 + 2\sum_{j=1-t}^{t-1}\zeta^j\right) = 0$$

$$\Longleftrightarrow \qquad \left(\zeta^{t+\frac{n}{4}} + \zeta^{t+\frac{n}{4}-1} + \zeta^{t-\frac{n}{4}-1} + \zeta^{t-\frac{n}{4}-2}\right) - 2\zeta^{t-1} + 2\sum_{j=0}^{2t-2}\zeta^j = 0$$

$$\Longleftrightarrow \qquad (\zeta-1)\left(\zeta^{t+\frac{n}{4}} + \zeta^{t+\frac{n}{4}-1} + \zeta^{t-\frac{n}{4}-1} + \zeta^{t-\frac{n}{4}-2} - 2\zeta^{t-1} + 2\sum_{j=0}^{2t-2}\zeta^j\right) = 0$$

$$\Longleftrightarrow \qquad \zeta^{t+\frac{n}{4}+1} - \zeta^{t+\frac{n}{4}-1} + \zeta^{t-\frac{n}{4}} - \zeta^{t-\frac{n}{4}-2} - 2\zeta^t + 2\zeta^{t-1} + 2\zeta^{2t-1} - 2 = 0. \qquad (12)$$

Now, we will divide the problem into two subcases depending on whether $\zeta^{\frac{n}{4}}$ is equal to 1 or -1.

Subcase $\zeta^{\frac{n}{4}} = 1$. In this subcase, it is easy to see that Eq. (12) further becomes equivalent to

$$\zeta^{t+\frac{n}{4}+1} - \zeta^{t+\frac{n}{4}-1} + \zeta^{t-\frac{n}{4}} - \zeta^{t-\frac{n}{4}-2} - 2\zeta^t + 2\zeta^{t-1} + 2\zeta^{2t-1} - 2 = 0$$

$$\Longleftrightarrow \qquad \zeta^{t+1} - \zeta^{t-1} + \zeta^t - \zeta^{t-2} - 2\zeta^t + 2\zeta^{t-1} + 2\zeta^{2t-1} - 2 = 0$$

$$\Longleftrightarrow \qquad 2\zeta^{2t-1} + \zeta^{t+1} - \zeta^t + \zeta^{t-1} - \zeta^{t-2} - 2 = 0.$$

Thus, if we suppose that $P(\zeta) = 0$, we then get that ζ is a root of the polynomial $Q_t(x)$. However, since $\zeta \neq 1, -1$ and $\zeta^n = 1$, this means that ζ is a primitive b-th root of unity for some $b \geq 3$. This implies that $\Phi_b(x)$ necessarily divides $Q_t(x)$, which is impossible according to Lemma 6, hence $P(\zeta) = 0$ cannot be true.

Subcase $\zeta^{\frac{n}{4}} = -1$. Here, Eq. (12) quickly becomes equivalent to

$$\zeta^{t+\frac{n}{4}+1} - \zeta^{t+\frac{n}{4}-1} + \zeta^{t-\frac{n}{4}} - \zeta^{t-\frac{n}{4}-2} - 2\zeta^t + 2\zeta^{t-1} + 2\zeta^{2t-1} - 2 = 0$$

$$\Longleftrightarrow \qquad -\zeta^{t+1} + \zeta^{t-1} - \zeta^t + \zeta^{t-2} - 2\zeta^t + 2\zeta^{t-1} + 2\zeta^{2t-1} - 2 = 0$$

$$\Longleftrightarrow \qquad 2\zeta^{2t-1} - \zeta^{t+1} - 3\zeta^t + 3\zeta^{t-1} + \zeta^{t-2} - 2 = 0.$$

In a similar fashion, if we suppose that $P(\zeta) = 0$, we conclude that ζ must be a root of the polynomial $R_t(x)$. Due to the fact that $\zeta \neq 1, -1$ and $\zeta^n = 1$, we see that ζ is a primitive b-th root of unity for some $b \geq 3$. Hence, $\Phi_b(x) \mid R_t(x)$ for some $b \geq 3$, which is again impossible by virtue of Lemma 6. Thus, $P(\zeta) \neq 0$. $\qquad\square$

4. D″(t, n) family of circulant graphs

Here, we give the second of the two central theorems disclosed in the paper.

Theorem 4. *For each $t \in \mathbb{N}$ and $n \geq 4t + 6$ such that $n \equiv_4 2$, the circulant graph $\mathcal{D}''_{t,n}$ must be a 4t-regular nut graph of order n.*

The complete proof of Theorem 4 will have a very similar structure as the previously described proof of Theorem 3, albeit with more complexity. Instead of the polynomials $Q_t(x)$ and $R_t(x)$, here we will rely on the integer polynomials $U_t, W_t \in \mathbb{Z}[x]$ that are defined as

$$U_t(x) = 2x^{4t-1} + x^{2t+4} - 2x^{2t+1} + 2x^{2t-1} - x^{2t-4} - 2x,$$
$$W_t(x) = 2x^{4t-1} - x^{2t+4} - 2x^{2t+1} + 2x^{2t-1} + x^{2t-4} - 2x,$$

for all the $t \in \mathbb{N}$, $t \geq 2$. These polynomials are clearly well defined for all the $t \geq 2$ and must have exactly six non-zero terms, due to the fact that

$$1 < 2t - 4 < 2t - 1 < 2t + 1 < 2t + 4 < 4t - 1$$

for each $t \geq 3$, while

$$4t - 1 = 7, \qquad 2t + 4 = 8, \qquad 2t + 1 = 5, \qquad 2t - 1 = 3, \qquad 2t - 4 = 0, \qquad 1 = 1,$$

for $t = 2$. By setting

$$M_t = \{1, 2t - 4, 2t - 1, 2t + 1, 2t + 4, 4t - 1\}$$

for each $t \geq 2$, we can show that the M_t sets have a property that is very similar to the one regarding the L_t sets which was demonstrated earlier in Lemma 2 from Section 3.

Lemma 7. *For each $t \geq 2$ and each prime number $p \geq 7$, the set M_t contains an element whose remainder modulo p is unique within the set.*

Proof. It is easy to notice that the four integers $2t - 4, 2t - 1, 2t + 1, 2t + 4$ necessarily have mutually distinct remainders modulo p. This quickly implies that at least two of them must have a remainder modulo p that is different from the remainders of both 1 and $4t - 1$. □

We will now implement Lemma 7 in order to prove a valuable property of the $U_t(x)$ and $W_t(x)$ polynomials regarding their division by cyclotomic polynomials, as demonstrated in the following lemma.

Lemma 8. *For any $t \geq 2$, neither $U_t(x)$ nor $W_t(x)$ can be divisible by a cyclotomic polynomial $\Phi_b(x)$ such that $p^2 \mid b$ for some prime number $p \geq 3$.*

Proof. This proof will be done in a completely analogous manner as that of Lemma 3. In case $b \in \mathbb{N}$ and $p^2 \mid b$ for some prime number p, we will again use the fact that $\Phi_b(x) = \Phi_{\frac{b}{p}}(x^p)$.

Suppose that $\Phi_b(x) \mid U_t(x)$ for some $t \geq 2$ and $b \in \mathbb{N}$ such that $p^2 \mid b$ for some prime number $p \geq 3$. Let $U_t^{(j)}(x)$ denote the polynomial composed of all the terms of $U_t(x)$ whose powers are congruent to j modulo p, for each $j = \overline{0, p - 1}$. The same logic used in the proof of Lemma 3 allows us to conclude that

$$\Phi_b(x) \mid U_t^{(j)}(x)$$

must hold for all the $j = \overline{0, p - 1}$. It is clear that the same notation and implication can be used regarding the $W_t(x)$ polynomial in case $\Phi_b(x) \mid W_t(x)$ is true. We will now finalize the proof of the lemma by taking into consideration three separate cases depending on the value of the prime number p.

Case $p \geq 7$. In this scenario, Lemma 7 tells us that the set M_t must contain an element whose remainder modulo p is unique within that set. Hence, this case can be proved completely analogously to the case $p \geq 5$ from the proof of Lemma 3.

Case $p = 5$. If $t \equiv_5 2$ or $t \equiv_5 4$, then there exists an element of the set M_t whose remainder modulo 5 is unique with that set, as shown in Table 2. In this subcase, a contradiction can easily be obtained if we suppose that either $\Phi_b(x) \mid U_t(x)$ or $\Phi_b(x) \mid W_t(x)$, by using the same logic as in the $p \geq 7$ case. We resolve the remaining three subcases separately.

	$t \equiv_5 0$	$t \equiv_5 1$	$t \equiv_5 2$	$t \equiv_5 3$	$t \equiv_5 4$
$1 \bmod 5$	1	1	1	1	1
$(2t - 4) \bmod 5$	1	3	0	2	4
$(2t - 1) \bmod 5$	4	1	3	0	2
$(2t + 1) \bmod 5$	1	3	0	2	4
$(2t + 4) \bmod 5$	4	1	3	0	2
$(4t - 1) \bmod 5$	4	3	2	1	0

Table 2: The elements of the set M_t modulo 5.

Subcase $t \equiv_5 0$. If we suppose that $\Phi_b \mid U_t(x)$, then we get

$$\Phi_b(x) \mid -2x^{2t+1} - x^{2t-4} - 2x,$$
$$\Phi_b(x) \mid 2x^{4t-1} + x^{2t+4} + 2x^{2t-1}.$$

Since $t \geq 5$, we quickly obtain

$$\Phi_b(x) \mid -2x^{2t+1} - x^{2t-4} - 2x$$
$$\implies \Phi_b(x) \mid -x(2x^{2t} + x^{2t-5} + 2)$$
$$\implies \Phi_b(x) \mid 2x^{2t} + x^{2t-5} + 2, \tag{13}$$

as well as

$$\Phi_b(x) \mid 2x^{4t-1} + x^{2t+4} + 2x^{2t-1}$$
$$\implies \Phi_b(x) \mid x^{2t-1}(2x^{2t} + x^5 + 2)$$
$$\implies \Phi_b(x) \mid 2x^{2t} + x^5 + 2. \tag{14}$$

Furthermore, if we subtract the right-hand sides of Eqs. (13) and (14), this leads us to

$$\Phi_b(x) \mid (2x^{2t} + x^{2t-5} + 2) - (2x^{2t} + x^5 + 2)$$
$$\implies \Phi_b(x) \mid x^{2t-5} - x^5$$
$$\implies \Phi_b(x) \mid x^5(x^{2t-10} - 1)$$
$$\implies \Phi_b(x) \mid x^{2t-10} - 1.$$

Now, Eq. (14) helps us obtain

$$\Phi_b(x) \mid 2x^{2t} + x^5 + 2$$
$$\implies \Phi_b(x) \mid 2x^{2t} + x^5 + 2 - 2x^{10}(x^{2t-10} - 1)$$
$$\implies \Phi_b(x) \mid 2x^{10} + x^5 + 2.$$

However, none of the roots of the polynomial $2x^{10} + x^5 + 2$ are actually roots of unity, as demonstrated in Appendix E, hence we obtain a contradiction.

Similarly, if we suppose that $\Phi_b(x) \mid W_t(x)$, then we get

$$\Phi_b(x) \mid -2x^{2t+1} + x^{2t-4} - 2x,$$
$$\Phi_b(x) \mid 2x^{4t-1} - x^{2t+4} + 2x^{2t-1}.$$

Due to $t \geq 5$, we have

$$\Phi_b(x) \mid -2x^{2t+1} + x^{2t-4} - 2x$$
$$\implies \Phi_b(x) \mid -x\,(2x^{2t} - x^{2t-5} + 2)$$
$$\implies \Phi_b(x) \mid 2x^{2t} - x^{2t-5} + 2 \tag{15}$$

and

$$\Phi_b(x) \mid 2x^{4t-1} - x^{2t+4} + 2x^{2t-1}$$
$$\implies \Phi_b(x) \mid x^{2t-1}(2x^{2t} - x^5 + 2)$$
$$\implies \Phi_b(x) \mid 2x^{2t} - x^5 + 2. \tag{16}$$

By subtracting the right-hand sides of Eqs. (15) and (16), it follows that

$$\Phi_b(x) \mid (2x^{2t} - x^{2t-5} + 2) - (2x^{2t} - x^5 + 2)$$
$$\implies \Phi_b(x) \mid -x^{2t-5} + x^5$$
$$\implies \Phi_b(x) \mid -x^5\,(x^{2t-10} - 1)$$
$$\implies \Phi_b(x) \mid x^{2t-10} - 1.$$

Hence, Eq. (16) is now able to give us

$$\Phi_b(x) \mid 2x^{2t} - x^5 + 2$$
$$\implies \Phi_b(x) \mid 2x^{2t} - x^5 + 2 - 2x^{10}\,(x^{2t-10} - 1)$$
$$\implies \Phi_b(x) \mid 2x^{10} - x^5 + 2.$$

However, similarly as with $U_t(x)$, none of the roots of $2x^{10} - x^5 + 2$ are roots of unity, as shown in Appendix E, which leads to a contradiction.

Subcase $t \equiv_5 1$. If we suppose that $\Phi_b \mid U_t(x)$, we immediately get

$$\Phi_b(x) \mid x^{2t+4} + 2x^{2t-1} - 2x,$$
$$\Phi_b(x) \mid 2x^{4t-1} - 2x^{2t+1} - x^{2t-4}.$$

It is easy to see that

$$\Phi_b(x) \mid x^{2t+4} + 2x^{2t-1} - 2x$$
$$\implies \Phi_b(x) \mid x\,(x^{2t+3} + 2x^{2t-2} - 2)$$
$$\implies \Phi_b(x) \mid x^{2t+3} + 2x^{2t-2} - 2, \tag{17}$$

as well as

$$\Phi_b(x) \mid 2x^{4t-1} - 2x^{2t+1} - x^{2t-4}$$
$$\implies \Phi_b(x) \mid x^{2t-4}\,(2x^{2t+3} - 2x^5 - 1)$$
$$\implies \Phi_b(x) \mid 2x^{2t+3} - 2x^5 - 1. \tag{18}$$

By using Eqs. (17) and (18) together, we further obtain

$$\Phi_b(x) \mid 2(x^{2t+3} + 2x^{2t-2} - 2) - (2x^{2t+3} - 2x^5 - 1)$$
$$\implies \quad \Phi_b(x) \mid 4x^{2t-2} + 2x^5 - 3. \tag{19}$$

Now, by using Eqs. (18) and (19) together, we see that

$$\Phi_b(x) \mid 2(2x^{2t+3} - 2x^5 - 1) - x^5(4x^{2t-2} + 2x^5 - 3)$$
$$\implies \quad \Phi_b(x) \mid -2x^{10} - x^5 - 2,$$

which is not possible since the polynomial $2x^{10} + x^5 + 2$ has no roots of unity among its roots, as discussed earlier.

In a similar fashion, if we suppose that $\Phi_b \mid W_t(x)$, this gives us

$$\Phi_b(x) \mid -x^{2t+4} + 2x^{2t-1} - 2x,$$
$$\Phi_b(x) \mid 2x^{4t-1} - 2x^{2t+1} + x^{2t-4},$$

from which we swiftly obtain

$$\Phi_b(x) \mid -x^{2t+4} + 2x^{2t-1} - 2x$$
$$\implies \quad \Phi_b(x) \mid -x(x^{2t+3} - 2x^{2t-2} + 2)$$
$$\implies \quad \Phi_b(x) \mid x^{2t+3} - 2x^{2t-2} + 2 \tag{20}$$

and

$$\Phi_b(x) \mid 2x^{4t-1} - 2x^{2t+1} + x^{2t-4}$$
$$\implies \quad \Phi_b(x) \mid x^{2t-4}(2x^{2t+3} - 2x^5 + 1)$$
$$\implies \quad \Phi_b(x) \mid 2x^{2t+3} - 2x^5 + 1. \tag{21}$$

If we use Eqs. (20) and (21) together, we conclude that

$$\Phi_b(x) \mid (2x^{2t+3} - 2x^5 + 1) - 2(x^{2t+3} - 2x^{2t-2} + 2)$$
$$\implies \quad \Phi_b(x) \mid 4x^{2t-2} - 2x^5 - 3. \tag{22}$$

Furthermore, by using Eqs. (21) and (22) together, we get

$$\Phi_b(x) \mid x^5(4x^{2t-2} - 2x^5 - 3) - 2(2x^{2t+3} - 2x^5 + 1)$$
$$\implies \quad \Phi_b(x) \mid -2x^{10} + x^5 - 2,$$

which is impossible given the fact that the polynomial $2x^{10} - x^5 + 2$ has no roots of unity among its roots, as we have already discussed.

Subcase $t \equiv_5 3$. If we suppose that $\Phi_b(x) \mid U_t(x)$, we obtain

$$\Phi_b(x) \mid x^{2t+4} + 2x^{2t-1},$$
$$\Phi_b(x) \mid -2x^{2t+1} - x^{2t-4},$$

which directly gives us

$$\Phi_b(x) \mid x^{2t+4} + 2x^{2t-1}$$
$$\implies \quad \Phi_b(x) \mid x^{2t-1}(x^5 + 2)$$
$$\implies \quad \Phi_b(x) \mid x^5 + 2 \tag{23}$$

and

$$\Phi_b(x) \mid -2x^{2t+1} - x^{2t-4}$$
$$\implies \Phi_b(x) \mid -x^{2t-4}(2x^5 + 1)$$
$$\implies \Phi_b(x) \mid 2x^5 + 1. \tag{24}$$

By combining Eqs. (23) and (24), we reach

$$\Phi_b(x) \mid 2(x^5 + 2) - (2x^5 + 1)$$
$$\implies \Phi_b(x) \mid 3,$$

thus yielding a contradiction.

On the other hand, if we suppose that $\Phi_b(x) \mid W_t(x)$, this gives us

$$\Phi_b(x) \mid -x^{2t+4} + 2x^{2t-1},$$
$$\Phi_b(x) \mid -2x^{2t+1} + x^{2t-4},$$

which further implies

$$\Phi_b(x) \mid -x^{2t+4} + 2x^{2t-1}$$
$$\implies \Phi_b(x) \mid -x^{2t-1}(x^5 - 2)$$
$$\implies \Phi_b(x) \mid x^5 - 2, \tag{25}$$

as well as

$$\Phi_b(x) \mid -2x^{2t+1} + x^{2t-4}$$
$$\implies \Phi_b(x) \mid -x^{2t-4}(2x^5 - 1)$$
$$\implies \Phi_b(x) \mid 2x^5 - 1. \tag{26}$$

By combining Eqs. (25) and (26), we conclude that

$$\Phi_b(x) \mid 2(x^5 - 2) - (2x^5 - 1)$$
$$\implies \Phi_b(x) \mid -3,$$

which is not possible.

Case $p = 3$. This case can be resolved by taking into consideration the modular values given in Table 3. Thus, we divide the case into three subcases depending on the value of $t \bmod 3$.

	$t \equiv_3 0$	$t \equiv_3 1$	$t \equiv_3 2$
1 mod 3	1	1	1
$(2t - 4)$ mod 3	2	1	0
$(2t - 1)$ mod 3	2	1	0
$(2t + 1)$ mod 3	1	0	2
$(2t + 4)$ mod 3	1	0	2
$(4t - 1)$ mod 3	2	0	1

Table 3: The elements of the set M_t modulo 3.

Subcase $t \equiv_3 0$. In this subcase, if we suppose that $\Phi_b(x) \mid U_t(x)$, we then have

$$\Phi_b(x) \mid x^{2t+4} - 2x^{2t+1} - 2x,$$
$$\Phi_b(x) \mid 2x^{4t-1} + 2x^{2t-1} - x^{2t-4},$$

which immediately gives

$$\Phi_b(x) \mid x^{2t+4} - 2x^{2t+1} - 2x$$
$$\implies \Phi_b(x) \mid x\,(x^{2t+3} - 2x^{2t} - 2)$$
$$\implies \Phi_b(x) \mid x^{2t+3} - 2x^{2t} - 2 \qquad (27)$$

and

$$\Phi_b(x) \mid 2x^{4t-1} + 2x^{2t-1} - x^{2t-4}$$
$$\implies \Phi_b(x) \mid x^{2t-4}\,(2x^{2t+3} + 2x^3 - 1)$$
$$\implies \Phi_b(x) \mid 2x^{2t+3} + 2x^3 - 1. \qquad (28)$$

By using Eqs. (27) and (28) together, we obtain

$$\Phi_b(x) \mid (2x^{2t+3} + 2x^3 - 1) - 2(x^{2t+3} - 2x^{2t} - 2)$$
$$\implies \Phi_b(x) \mid 4x^{2t} + 2x^3 + 3. \qquad (29)$$

Now, by using Eqs. (28) and (29), we get

$$\Phi_b(x) \mid 2(2x^{2t+3} + 2x^3 - 1) - x^3\,(4x^{2t} + 2x^3 + 3)$$
$$\implies \Phi_b(x) \mid -2x^6 + x^3 - 2.$$

However, none of the roots of the polynomial $2x^6 - x^3 + 2$ are actually roots of unity, as shown in Appendix E, which leads us to a contradiction.

Similarly, if we suppose that $\Phi_b(x) \mid W_t(x)$, we obtain

$$\Phi_b(x) \mid -x^{2t+4} - 2x^{2t+1} - 2x,$$
$$\Phi_b(x) \mid 2x^{4t-1} + 2x^{2t-1} + x^{2t-4},$$

which quickly leads us to

$$\Phi_b(x) \mid -x^{2t+4} - 2x^{2t+1} - 2x$$
$$\implies \Phi_b(x) \mid -x\,(x^{2t+3} + 2x^{2t} + 2)$$
$$\implies \Phi_b(x) \mid x^{2t+3} + 2x^{2t} + 2 \qquad (30)$$

and

$$\Phi_b(x) \mid 2x^{4t-1} + 2x^{2t-1} + x^{2t-4}$$
$$\implies \Phi_b(x) \mid x^{2t-4}\,(2x^{2t+3} + 2x^3 + 1)$$
$$\implies \Phi_b(x) \mid 2x^{2t+3} + 2x^3 + 1. \qquad (31)$$

If we use Eqs. (30) and (31) together, we conclude that

$$\Phi_b(x) \mid 2(x^{2t+3} + 2x^{2t} + 2) - (2x^{2t+3} + 2x^3 + 1)$$
$$\implies \Phi_b(x) \mid 4x^{2t} - 2x^3 + 3. \qquad (32)$$

Furthermore, by combining Eqs. (31) and (32), we reach

$$\Phi_b(x) \mid 2(2x^{2t+3} + 2x^3 + 1) - x^3\,(4x^{2t} - 2x^3 + 3)$$
$$\implies \Phi_b(x) \mid 2x^6 + x^3 + 2,$$

which leads to a contradiction, given the fact that the polynomial $2x^6 + x^3 + 2$ has no root which represents a root of unity, as demonstrated in Appendix E.

Subcase $t \equiv_3 1$. In this scenario, supposing that $\Phi_b(x) \mid U_t(x)$ is true leads to

$$\Phi_b(x) \mid 2x^{2t-1} - x^{2t-4} - 2x,$$
$$\Phi_b(x) \mid 2x^{4t-1} + x^{2t+4} - 2x^{2t+1}.$$

Given the fact that $t \geq 4$, we swiftly get

$$\Phi_b(x) \mid 2x^{2t-1} - x^{2t-4} - 2x$$
$$\implies \quad \Phi_b(x) \mid x \, (2x^{2t-2} - x^{2t-5} - 2)$$
$$\implies \quad \Phi_b(x) \mid 2x^{2t-2} - x^{2t-5} - 2, \tag{33}$$

as well as

$$\Phi_b(x) \mid 2x^{4t-1} + x^{2t+4} - 2x^{2t+1}$$
$$\implies \quad \Phi_b(x) \mid x^{2t+1} \, (2x^{2t-2} + x^3 - 2)$$
$$\implies \quad \Phi_b(x) \mid 2x^{2t-2} + x^3 - 2. \tag{34}$$

Furthermore, subtracting the right-hand sides of Eqs. (33) and (34) helps us obtain

$$\Phi_b(x) \mid (2x^{2t-2} + x^3 - 2) - (2x^{2t-2} - x^{2t-5} - 2)$$
$$\implies \quad \Phi_b(x) \mid x^{2t-5} + x^3$$
$$\implies \quad \Phi_b(x) \mid x^3 \, (x^{2t-8} + 1)$$
$$\implies \quad \Phi_b(x) \mid x^{2t-8} + 1. \tag{35}$$

Now, by combining Eqs. (34) and (35), we conclude that

$$\Phi_b(x) \mid (2x^{2t-2} + x^3 - 2) - 2x^6 \, (x^{2t-8} + 1)$$
$$\implies \quad \Phi_b(x) \mid -2x^6 + x^3 - 2,$$

thus yielding a contradiction due to the fact that the polynomial $2x^6 - x^3 + 2$ has no roots of unity among its roots, as discussed earlier.

In a similar fashion, supposing that $\Phi_b(x) \mid W_t(x)$ gives us

$$\Phi_b(x) \mid 2x^{2t-1} + x^{2t-4} - 2x,$$
$$\Phi_b(x) \mid 2x^{4t-1} - x^{2t+4} - 2x^{2t+1}.$$

Since $t \geq 4$, this immediately leads us to

$$\Phi_b(x) \mid 2x^{2t-1} + x^{2t-4} - 2x$$
$$\implies \quad \Phi_b(x) \mid x \, (2x^{2t-2} + x^{2t-5} - 2)$$
$$\implies \quad \Phi_b(x) \mid 2x^{2t-2} + x^{2t-5} - 2, \tag{36}$$

as well as

$$\Phi_b(x) \mid 2x^{4t-1} - x^{2t+4} - 2x^{2t+1}$$
$$\implies \quad \Phi_b(x) \mid x^{2t+1} \, (2x^{2t-2} - x^3 - 2)$$
$$\implies \quad \Phi_b(x) \mid 2x^{2t-2} - x^3 - 2. \tag{37}$$

We can now subtract the right-hand sides of Eqs. (36) and (37) in order to obtain

$$\Phi_b(x) \mid (2x^{2t-2} + x^{2t-5} - 2) - (2x^{2t-2} - x^3 - 2)$$
$$\implies \quad \Phi_b(x) \mid x^{2t-5} + x^3$$
$$\implies \quad \Phi_b(x) \mid x^3(x^{2t-8} + 1)$$
$$\implies \quad \Phi_b(x) \mid x^{2t-8} + 1. \tag{38}$$

Furthermore, combining Eqs. (37) and (38) gives us

$$\Phi_b(x) \mid (2x^{2t-2} - x^3 - 2) - 2x^6(x^{2t-8} + 1)$$
$$\implies \quad \Phi_b(x) \mid -2x^6 - x^3 - 2,$$

which is impossible since the polynomial $2x^6 + x^3 + 2$ has no roots of unity among its roots, as we have already discussed.

Subcase $t \equiv_3 2$. In this subcase, if we suppose that $\Phi_b(x) \mid U_t(x)$, then we directly obtain

$$\Phi_b(x) \mid x^{2t+4} - 2x^{2t+1},$$
$$\Phi_b(x) \mid 2x^{2t-1} - x^{2t-4},$$

which leads us to

$$\Phi_b(x) \mid x^{2t+4} - 2x^{2t+1}$$
$$\implies \quad \Phi_b(x) \mid x^{2t+1}(x^3 - 2)$$
$$\implies \quad \Phi_b(x) \mid x^3 - 2 \tag{39}$$

and

$$\Phi_b(x) \mid 2x^{2t-1} - x^{2t-4}$$
$$\implies \quad \Phi_b(x) \mid x^{2t-4}(2x^3 - 1)$$
$$\implies \quad \Phi_b(x) \mid 2x^3 - 1. \tag{40}$$

By using Eqs. (39) and (40) together, we reach

$$\Phi_b(x) \mid (2x^3 - 1) - 2(x^3 - 2)$$
$$\implies \quad \Phi_b(x) \mid 3,$$

thus yielding a contradiction.

Similarly, if we suppose that $\Phi_b(x) \mid W_t(x)$, we obtain

$$\Phi_b(x) \mid -x^{2t+4} - 2x^{2t+1},$$
$$\Phi_b(x) \mid 2x^{2t-1} + x^{2t-4},$$

which further gives

$$\Phi_b(x) \mid -x^{2t+4} - 2x^{2t+1}$$
$$\implies \quad \Phi_b(x) \mid -x^{2t+1}(x^3 + 2)$$
$$\implies \quad \Phi_b(x) \mid x^3 + 2, \tag{41}$$

as well as

$$\Phi_b(x) \mid 2x^{2t-1} + x^{2t-4}$$
$$\implies \quad \Phi_b(x) \mid x^{2t-4}(2x^3 + 1)$$
$$\implies \quad \Phi_b(x) \mid 2x^3 + 1. \tag{42}$$

By combining Eqs. (41) and (42), we get

$$\Phi_b(x) \mid (2x^3 + 1) - 2(x^3 + 2)$$
$$\implies \quad \Phi_b(x) \mid -3,$$

which is clearly not possible. $\square$

It is clear that the formulation of Lemma 8 is very similar to that of the previously proven Lemma 3 from Section 3. The key difference is that Lemma 8 does not cover the case for $p = 2$. In fact, it can be shown that this property does not hold for the $U_t(x)$ and $W_t(x)$ polynomials, i.e. it is possible that they are divisible by a cyclotomic polynomial $\Phi_b(x)$ such that $4 \mid b$. However, although the condition $4 \mid b$ can hold, it can be shown that the only way for this to happen is if $b \in \{4, 8\}$, as demonstrated in the following lemma.

Lemma 9. *For any $t \geq 2$, if $U_t(x)$ or $W_t(x)$ are divisible by some cyclotomic polynomial $\Phi_b(x)$ such that $4 \mid b$, then $b = 4$ or $b = 8$.*

Proof. Suppose that $4 \mid b$. Given the fact that $2 \mid \frac{b}{2}$, it is clear that $\Phi_b(x) = \Phi_{\frac{b}{2}}(x^2)$ (see, for example, [5, p. 160]). By using the same logic as in the proofs of Lemmas 3 and 8, we obtain that $\Phi_b(x) \mid U_t(x)$ would imply

$$\Phi_b(x) \mid U_t^{(j)}(x)$$

for each $j = \overline{0,1}$, where $U_t^{(j)}(x)$ represents the polynomial composed of the terms of $U_t(x)$ whose powers are congruent to j modulo 2. The same conclusion and notation can be applied to $W_t(x)$ as well.

Since all the values $1, 2t - 1, 2t + 1, 4t - 1$ are odd, while $2t + 4$ and $2t - 4$ are even, we conclude that $\Phi_b \mid U_t(x)$ would immediately imply

$$\Phi_b(x) \mid x^{2t+4} - x^{2t-4},$$

while $\Phi_b \mid W_t(x)$ would give

$$\Phi_b(x) \mid -x^{2t+4} + x^{2t-4}.$$

Either way, we would reach

$$\Phi_b(x) \mid x^{2t+4} - x^{2t-4}$$
$$\implies \quad \Phi_b(x) \mid x^{2t-4}(x^8 - 1)$$
$$\implies \quad \Phi_b(x) \mid x^8 - 1.$$

This practically means that each primitive b-th root of unity must be an eighth root of unity, i.e. $b \mid 8$. This is only possible if $b = 4$ or $b = 8$. $\square$

A direct consequence of Lemmas 8 and 9 is that if the cyclotomic polynomial $\Phi_b(x)$ divides $U_t(x)$ or $W_t(x)$, then the integer $b \in \mathbb{N}$ needs to either be square-free, or be equal to 4 or 8. In fact, for any $t \geq 2$, the only cyclotomic polynomials that could divide $U_t(x)$ or $W_t(x)$ are actually $\Phi_1(x), \Phi_2(x), \Phi_4(x), \Phi_8(x)$. This observation forms the central part of the proof of Theorem 4. However, in order to prove this claim, we will be in need of two more auxiliary lemmas that hold a great resemblance to the previously proven Lemmas 4 and 5 from Section 3.

Lemma 10. *For each $t \geq 2$ and each prime number $p \geq 7$, neither $U_t(x)$ nor $W_t(x)$ can be divisible by the cyclotomic polynomial $\Phi_p(x)$ or the cyclotomic polynomial $\Phi_{2p}(x)$.*

Proof. The proof can be done in an entirely analogous manner as the proof of Lemma 4 from Section 3, the only difference being that Lemma 7 is used to conclude that there exists an element of the set M_t that has a unique remainder within that set, instead of Lemma 2. Thus, we choose to leave the proof out. $\square$

Lemma 11. *For each $t \geq 2$ and each positive integer $b \in \{3, 5, 6, 10, 15, 30\}$, the cyclotomic polynomial $\Phi_b(x)$ divides neither $U_t(x)$ nor $W_t(x)$.*

Proof. The proof can be done by using an absolutely identical mechanism as the proof of Lemma 5 from Section 3. We disclose the necessary computational results in Appendix C and Appendix D. $\square$

We shall now formulate and prove the central lemma regarding the divisibility of the $U_t(x)$ and $W_t(x)$ polynomials by cyclotomic polynomials. Given the fact that these polynomials also have six non-zero terms, like the $Q_t(x)$ and $R_t(x)$ polynomials from Section 3, using Theorem 2 becomes very convenient once again. The same prime number cancellation mechanism can be implemented for each prime number $p \geq 7$ that divides b whenever $\Phi_b(x)$ divides either $U_t(x)$ or $W_t(x)$, as it was elaborated in Section 3. Bearing this in mind, we give the following lemma.

Lemma 12. *For each $t \geq 2$, neither $U_t(x)$ nor $W_t(x)$ can be divisible by a cyclotomic polynomial $\Phi_b(x)$ such that $b \notin \{1, 2, 4, 8\}$.*

Proof. The proof will only be given for $U_t(x)$, given the fact that the proof regarding $W_t(x)$ is completely analogous. Suppose that $\Phi_b(x) \mid U_t(x)$, for some $b \in \mathbb{N}$ such that $b \notin \{1, 2, 4, 8\}$. Since b is not equal to 4 or 8, Lemmas 8 and 9 tell us that b must be a square-free integer. We now divide the problem into two separate cases, depending on whether b is divisible by either 3 or 5, or not.

Case $3 \nmid b$ and $5 \nmid b$. This case is proved completely analogously to the corresponding case from the proof of Lemma 6 from Section 3. The only small difference is that Lemma 10 is used instead of Lemma 4.

Case $3 \mid b$ or $5 \mid b$. This case is also proved entirely analogously to the corresponding case from the proof of Lemma 6. As expected, the only minor difference is that Lemma 11 is used instead of Lemma 5. $\square$

Taking into consideration all the results obtained in the previously disclosed lemmas, we are finally able to complete the proof of Theorem 4. Thus, we present the rest of the proof.

Proof of Theorem 4. The case $t = 1$ is trivial to prove. Here, we simply have $S''_{1,n} = \left\{ \frac{n+2}{4}, \frac{n+6}{4} \right\}$, hence Eq. (1) directly gives us

$$P(\zeta) = \zeta^{\frac{n+2}{4}} + \frac{1}{\zeta^{\frac{n+2}{4}}} + \zeta^{\frac{n+6}{4}} + \frac{1}{\zeta^{\frac{n+6}{4}}}, \tag{43}$$

where ζ is an arbitrary n-th root of unity different from 1 and -1. The condition $P(\zeta) = 0$ is clearly equivalent to

$$P(\zeta) = 0$$
$$\iff \zeta^{\frac{n+6}{4}} \left(\zeta^{\frac{n+2}{4}} + \frac{1}{\zeta^{\frac{n+2}{4}}} + \zeta^{\frac{n+6}{4}} + \frac{1}{\zeta^{\frac{n+6}{4}}} \right) = 0$$
$$\iff \zeta^{\frac{n}{2}+3} + \zeta^{\frac{n}{2}+2} + \zeta + 1 = 0$$
$$\iff (\zeta + 1)\left(\zeta^{\frac{n}{2}+2} + 1 \right) = 0$$
$$\iff \zeta^{\frac{n}{2}+2} + 1 = 0.$$

Due to the fact that $\zeta^{\frac{n}{2}} \in \{1, -1\}$, it is obvious that $\zeta^{\frac{n}{2}+2}$ is equal to either $\zeta^2 + 1$ or $-\zeta^2 + 1$. However, both of these expressions cannot be equal to zero. If $\zeta^2 + 1$ were to equal zero, then we would have that $\zeta \in \{i, -i\}$, which is impossible due to the fact that $n \equiv_4 2$, hence both i and $-i$ are not n-th roots of unity. On the other hand, $-\zeta^2 + 1 \neq 0$ purely because ζ was chosen in such a way that it is distinct from both 1 and -1. Thus, we get that $P(\zeta) \neq 0$ for any n-th root of unity different from 1 and -1. By virtue of Lemma 1, we conclude that $\mathcal{D}''_{1,n}$ truly is a circulant nut graph for any $n \geq 10$ such that $n \equiv_4 2$.

In the remainder of the proof, we will suppose that $t \geq 2$. Eq. (1) now gives us

$$P(\zeta) = \left(\zeta^{\frac{n+2}{4}} + \frac{1}{\zeta^{\frac{n+2}{4}}} \right) + \left(\zeta^{\frac{n+6}{4}} + \frac{1}{\zeta^{\frac{n+6}{4}}} \right) + \sum_{j=1}^{t-1} \left(\zeta^j + \frac{1}{\zeta^j} \right) + \sum_{j=\frac{n}{2}-t+1}^{\frac{n}{2}-1} \left(\zeta^j + \frac{1}{\zeta^j} \right),$$

where ζ is an arbitrarily chosen n-th root of unity different from 1 and -1. It is not difficult to further obtain

$$P(\zeta) = \left(\zeta^{\frac{n+6}{4}} + \zeta^{\frac{n+2}{4}} + \frac{1}{\zeta^{\frac{n+2}{4}}} + \frac{1}{\zeta^{\frac{n+6}{4}}} \right) + \sum_{j=1}^{t-1} \left(\zeta^j + \frac{1}{\zeta^j} + \zeta^{\frac{n}{2}-j} + \frac{1}{\zeta^{\frac{n}{2}-j}} \right). \tag{44}$$

We will finalize the proof by demonstrating that $P(\zeta) \neq 0$ must be true. We will divide this proof into two cases in the same way as it was done while proving Theorem 3.

Case $\zeta^{\frac{n}{2}} = -1$. In this case, it is straightforward to notice that $\zeta^{\frac{n}{2}-j} = -\frac{1}{\zeta^j}$ and $\frac{1}{\zeta^{\frac{n}{2}-j}} = -\zeta^j$, which directly leads us to

$$\zeta^j + \frac{1}{\zeta^j} + \zeta^{\frac{n}{2}-j} + \frac{1}{\zeta^{\frac{n}{2}-j}} = 0$$

for any $j = \overline{1, t-1}$. Hence, it is convenient to simplify Eq. (44) in order to get

$$P(\zeta) = \zeta^{\frac{n+6}{4}} + \zeta^{\frac{n+2}{4}} + \frac{1}{\zeta^{\frac{n+2}{4}}} + \frac{1}{\zeta^{\frac{n+6}{4}}}.$$

However, this formula is identical to Eq. (43) which we had to deal with while solving the case $t = 1$. An almost absolutely identical proof can be used in order to show that $P(\zeta) \neq 0$ must hold, as desired, hence we choose to leave it out.

Case $\zeta^{\frac{n}{2}} = 1$. It is easy to see that $\zeta^{\frac{n}{2}-j} = \frac{1}{\zeta^j}$ and $\frac{1}{\zeta^{\frac{n}{2}-j}} = \zeta^j$. This implies

$$\zeta^j + \frac{1}{\zeta^j} + \zeta^{\frac{n}{2}-j} + \frac{1}{\zeta^{\frac{n}{2}-j}} = 2\left(\zeta^j + \frac{1}{\zeta^j} \right)$$

for any $j = \overline{1, t-1}$. According to Eq. (44), the equality $P(\zeta) = 0$ becomes equivalent to

$$P(\zeta) = 0$$

$$\Longleftrightarrow \qquad \left(\zeta^{\frac{n+6}{4}} + \zeta^{\frac{n+2}{4}} + \frac{1}{\zeta^{\frac{n+2}{4}}} + \frac{1}{\zeta^{\frac{n+6}{4}}} \right) + 2\sum_{j=1}^{t-1} \left(\zeta^j + \frac{1}{\zeta^j} \right) = 0$$

$$\Longleftrightarrow \qquad \left(\zeta^{\frac{n+6}{4}} + \zeta^{\frac{n+2}{4}} + \frac{1}{\zeta^{\frac{n+2}{4}}} + \frac{1}{\zeta^{\frac{n+6}{4}}} \right) - 2 + 2\sum_{j=1-t}^{t-1} \zeta^j = 0$$

$$\iff \qquad \zeta^{t-1}\left(\left(\zeta^{\frac{n+6}{4}} + \zeta^{\frac{n+2}{4}} + \frac{1}{\zeta^{\frac{n+2}{4}}} + \frac{1}{\zeta^{\frac{n+6}{4}}}\right) - 2 + 2\sum_{j=1-t}^{t-1} \zeta^j\right) = 0$$

$$\iff \qquad \left(\zeta^{t+\frac{n+2}{4}} + \zeta^{t+\frac{n-2}{4}} + \zeta^{t-\frac{n+6}{4}} + \zeta^{t-\frac{n+10}{4}}\right) - 2\zeta^{t-1} + 2\sum_{j=0}^{2t-2} \zeta^j = 0$$

$$\iff \qquad (\zeta - 1)\left(\zeta^{t+\frac{n+2}{4}} + \zeta^{t+\frac{n-2}{4}} + \zeta^{t-\frac{n+6}{4}} + \zeta^{t-\frac{n+10}{4}} - 2\zeta^{t-1} + 2\sum_{j=0}^{2t-2} \zeta^j\right) = 0$$

$$\iff \qquad \zeta^{t+\frac{n+6}{4}} - \zeta^{t+\frac{n-2}{4}} + \zeta^{t-\frac{n+2}{4}} - \zeta^{t-\frac{n+10}{4}} - 2\zeta^t + 2\zeta^{t-1} + 2\zeta^{2t-1} - 2 = 0$$

$$\iff \qquad 2\zeta^{2t-1} + \zeta^{t+\frac{n+6}{4}} - \zeta^{t+\frac{n-2}{4}} - 2\zeta^t + 2\zeta^{t-1} + \zeta^{t-\frac{n+2}{4}} - \zeta^{t-\frac{n+10}{4}} - 2 = 0.$$

Now, if we define ψ to be one of the two possible square roots of ζ, i.e. a complex number such that $\psi^2 = \zeta$, then it is easy to see that the condition $P(\zeta) = 0$ becomes equivalent to

$$2\psi^{4t-2} + \psi^{2t+3+\frac{n}{2}} - \psi^{2t-1+\frac{n}{2}} - 2\psi^{2t} + 2\psi^{2t-2} + \psi^{2t-1-\frac{n}{2}} - \psi^{2t-5-\frac{n}{2}} - 2 = 0. \qquad (45)$$

Taking into consideration that the condition $\zeta^{\frac{n}{2}} = 1$ translates to $\psi^n = 1$, it becomes clear that in order to prove that $P(\zeta) \neq 0$ for any n-th root of unity ζ such that $\zeta \neq 1, -1$ and $\zeta^{\frac{n}{2}} = 1$, it is enough to show that Eq. (45) does not hold for any n-th root of unity ψ such that $\psi \notin \{1, -1, i, -i\}$. Since i and $-i$ are not n-th roots of unity to begin with, due to $n \equiv_4 2$, it suffices to prove that Eq. (45) is not satisfied for any n-th root of unity, besides potentially 1 and -1.

We now divide the case into two subcases, depending on whether $\psi^{\frac{n}{2}}$ is equal to 1 or -1.

Subcase $\psi^{\frac{n}{2}} = 1$. Here, it is straightforward to deduce that Eq. (45) is equivalent to

$$2\psi^{4t-2} + \psi^{2t+3} - \psi^{2t-1} - 2\psi^{2t} + 2\psi^{2t-2} + \psi^{2t-1} - \psi^{2t-5} - 2 = 0$$

$$\iff \qquad 2\psi^{4t-2} + \psi^{2t+3} - 2\psi^{2t} + 2\psi^{2t-2} - \psi^{2t-5} - 2 = 0$$

$$\iff \qquad 2\psi^{4t-1} + \psi^{2t+4} - 2\psi^{2t+1} + 2\psi^{2t-1} - \psi^{2t-4} - 2\psi = 0.$$

Now, suppose that Eq. (45) does hold for some n-th root of unity ψ different from 1 and -1. It is clear that ψ must be a primitive b-th root of unity for some $b \neq 1, 2$, since $\psi \neq 1, -1$. Also, due to the fact that $b \mid n$ and $n \equiv_4 2$, we conclude that $b \neq 4, 8$. However, Eq. (45) directly implies that ψ is a root of the polynomial $U_t(x)$. Hence, we get that $U_t(x)$ is divisible by a cyclotomic polynomial $\Phi_b(x)$ such that $b \neq 1, 2, 4, 8$, which is not possible according to Lemma 12, thus yielding a contradiction.

Subcase $\psi^{\frac{n}{2}} = -1$. In this subcase, Eq. (45) quickly becomes equivalent to

$$2\psi^{4t-2} - \psi^{2t+3} + \psi^{2t-1} - 2\psi^{2t} + 2\psi^{2t-2} - \psi^{2t-1} + \psi^{2t-5} - 2 = 0$$

$$\iff \qquad 2\psi^{4t-2} - \psi^{2t+3} - 2\psi^{2t} + 2\psi^{2t-2} + \psi^{2t-5} - 2 = 0$$

$$\iff \qquad 2\psi^{4t-1} - \psi^{2t+4} - 2\psi^{2t+1} + 2\psi^{2t-1} + \psi^{2t-4} - 2\psi = 0.$$

If we suppose that Eq. (45) is true for some n-th root of unity ψ different from 1 and -1, we can use the same logic implemented in the previous subcase in order to immediately obtain that ψ has to be a primitive b-th root of unity for some $b \notin \{1, 2, 4, 8\}$. However, Eq. (45) implies that ψ is a root of the polynomial $W_t(x)$, which further means that this polynomial has to be divisible by a cyclotomic polynomial $\Phi_b(x)$ such that $b \notin \{1, 2, 4, 8\}$. By virtue of Lemma 12, this is impossible, which completes the proof. $\square$

5. Conclusion

In conclusion, Theorems 3 and 4 provide a construction for any $4t$-regular circulant nut graph of order n, whenever

- t is odd and $n \geq 4t + 4$;

- t is even and $n \geq 4t + 6$ and $n \equiv_4 2$.

For the odd values of t, these two theorems provide a way to construct a $4t$-regular circulant nut graph of every possible order, thereby fully resolving the circulant nut graph order–degree existence problem. On the other hand, for the even values of t, Theorem 12 shows that there exists a $4t$-regular circulant nut graph of each order $n \geq 4t + 6$ such that $n \equiv_4 2$, without covering the case when $4 \mid n$.

Damnjanović and Stevanović [2, Proposition 19] have shown that an interesting irregularity exists for the case $t = 2$. Moreover, there does not exist an 8-regular circulant nut graph of order 16. In fact, the set of all the values n such that there exists an 8-regular circulant nut graph of order n is given by the expression $\{14\} \cup \{18, 20, 22, 24, 26, \ldots\}$.

Despite the irregularity that occurs for $t = 2$, the experimental results obtained in [2] dictate that for each even integer t such that $4 \leq t \leq 1300$ there does exist a $4t$-regular circulant nut graph of order n for each even $n \geq 4t + 6$. Bearing this in mind, we end the paper with the following conjecture.

Conjecture 3. *For each even $t \geq 4$ and each $n \geq 4t + 8$ divisible by four, there exists a $4t$-regular circulant nut graph of order n.*

References

[1] N. Bašić, M. Knor, R. Škrekovski, On 12-regular nut graphs, The Art of Discrete and Applied Mathematics 5(2) (2021) #P2.01.
[2] I. Damnjanović, D. Stevanović, On circulant nut graphs, Linear Algebra and its Applications 633 (2022) 127–151.
[3] M. Filaseta, A. Schinzel, On testing the divisibility of lacunary polynomials by cyclotomic polynomials, Mathematics of Computation 73(246) (2003) 957–965.
[4] R. M. Gray, Toeplitz and circulant matrices: A review, Foundations and Trends in Communications and Information Theory 2(3) (2006) 155–239.
[5] T. Nagell, Introduction to Number Theory, Wiley, New York, 1951.
[6] I. Sciriha, On the construction of graphs of nullity one, Discrete Mathematics 181(1–3) (1998) 193–211.
[7] Cyclotomic polynomials, Encyclopedia of Mathematics, encyclopediaofmath.org/index.php?title=Cyclotomic_polynomials.

Appendix A. $Q_t^{\bmod b}(x) \bmod \Phi_b(x)$ table

$t \bmod 3$	$Q_t^{\bmod 3}(x)$	$Q_t^{\bmod 3}(x) \bmod \Phi_3(x)$
0	$-3 + 3x^2$	$-6 - 3x$
1	$-1 + x$	$-1 + x$
2	$x - x^2$	$1 + 2x$

$t \bmod 5$	$Q_t^{\bmod 5}(x)$	$Q_t^{\bmod 5}(x) \bmod \Phi_5(x)$
0	$-3 + x - x^3 + 3x^4$	$-6 - 2x - 3x^2 - 4x^3$
1	$-1 + x + x^2 - x^4$	$2x + 2x^2 + x^3$
2	$-3 + x - x^2 + 3x^3$	$-3 + x - x^2 + 3x^3$
3	$-x + x^2 - x^3 + x^4$	$-1 - 2x - 2x^3$
4	$-1 + x^2 + x^3 - x^4$	$x + 2x^2 + 2x^3$

$t \bmod 6$	$Q_t^{\bmod 6}(x)$	$Q_t^{\bmod 6}(x) \bmod \Phi_6(x)$
0	$-3 + x - x^4 + 3x^5$	$-x$
1	$-1 + x + x^2 - x^5$	$-3 + 3x$
2	$-3 + x - x^2 + 3x^3$	-5
3	$-2 - x + x^2 - x^3 + x^4 + 2x^5$	$-3x$
4	$-2 + 2x - x^2 + x^3 - x^4 + x^5$	$-1 + x$
5	$-1 + x^3 + x^4 - x^5$	-3

$t \bmod 10$	$Q_t^{\bmod 10}(x)$	$Q_t^{\bmod 10}(x) \bmod \Phi_{10}(x)$
0	$-3 + x - x^8 + 3x^9$	$-2x + 3x^2 - 2x^3$
1	$-1 + x + x^2 - x^9$	$-2 + 2x + x^3$
2	$-3 + x - x^2 + 3x^3$	$-3 + x - x^2 + 3x^3$
3	$-2 - x + x^2 - x^3 + x^4 + 2x^5$	-5

4	$-2 - x^2 + x^3 - x^4 + x^5 + 2x^7$	$-2 - x - 2x^2$
5	$-2 - x^3 + x^4 - x^5 + x^6 + 2x^9$	$-2x + x^2 - 2x^3$
6	$-2 + 2x - x^4 + x^5 - x^6 + x^7$	$-2 + 2x - x^3$
7	$-2 + 2x^3 - x^5 + x^6 - x^7 + x^8$	$-1 - x + x^2 + x^3$
8	$-2 + 2x^5 - x^6 + x^7 - x^8 + x^9$	-3
9	$-1 + x^7 + x^8 - x^9$	$-2 + x - 2x^2$

$t \bmod 15$	$Q_t^{\bmod 15}(x)$	$Q_t^{\bmod 15}(x) \bmod \Phi_{15}(x)$
0	$-3 + x - x^{13} + 3x^{14}$	$-1 + 2x - 3x^2 + 3x^3 - 2x^4 - x^5 + 3x^6 - 2x^7$
1	$-1 + x + x^2 - x^{14}$	$-2 + x + 2x^2 - x^3 + x^4 - x^6 + x^7$
2	$-3 + x - x^2 + 3x^3$	$-3 + x - x^2 + 3x^3$
3	$-2 - x + x^2 - x^3 + x^4 + 2x^5$	$-2 - x + x^2 - x^3 + x^4 + 2x^5$
4	$-2 - x^2 + x^3 - x^4 + x^5 + 2x^7$	$-2 - x^2 + x^3 - x^4 + x^5 + 2x^7$
5	$-2 - x^3 + x^4 - x^5 + x^6 + 2x^9$	$-4 + 2x^2 - 3x^3 + x^4 - x^5 - x^6 + 2x^7$
6	$-2 - x^4 + x^5 - x^6 + x^7 + 2x^{11}$	$-2 - 2x - x^4 + x^5 - 3x^6 + x^7$
7	$-2 - x^5 + x^6 - x^7 + x^8 + 2x^{13}$	$-1 - x - x^3 - x^4 + x^6 - 2x^7$
8	$-x^6 + x^7 - x^8 + x^9$	$-x - x^2 - x^4 + x^5 - 2x^6 + x^7$
9	$-2 + 2x^2 - x^7 + x^8 - x^9 + x^{10}$	$-3 + x + x^2 + x^4 - 2x^5 + x^6 - x^7$
10	$-2 + 2x^4 - x^8 + x^9 - x^{10} + x^{11}$	$-1 - 2x + x^2 + x^4 + 2x^5 - 2x^6$
11	$-2 + 2x^6 - x^9 + x^{10} - x^{11} + x^{12}$	$-2 + x - 2x^2 + x^3 - x^5 + 4x^6 - 2x^7$
12	$-2 + 2x^8 - x^{10} + x^{11} - x^{12} + x^{13}$	$-2 + x^2 - 2x^3 + x^4 - x^6 + 2x^7$
13	$-2 + 2x^{10} - x^{11} + x^{12} - x^{13} + x^{14}$	$-4 + 2x - 2x^2 + x^3 - 3x^5 + 2x^6 - x^7$
14	$-1 + x^{12} + x^{13} - x^{14}$	$-1 - x - x^3 + x^5 - x^6 - x^7$

$t \bmod 30$	$Q_t^{\bmod 30}(x)$	$Q_t^{\bmod 30}(x) \bmod \Phi_{30}(x)$
0	$-3 + x - x^{28} + 3x^{29}$	$-7 + 3x^2 + 3x^3 + 4x^4 + x^5 - 3x^6 - 4x^7$
1	$-1 + x + x^2 - x^{29}$	$x - x^3 - x^4 + x^6 + x^7$
2	$-3 + x - x^2 + 3x^3$	$-3 + x - x^2 + 3x^3$
3	$-2 - x + x^2 - x^3 + x^4 + 2x^5$	$-2 - x + x^2 - x^3 + x^4 + 2x^5$
4	$-2 - x^2 + x^3 - x^4 + x^5 + 2x^7$	$-2 - x^2 + x^3 - x^4 + x^5 + 2x^7$
5	$-2 - x^3 + x^4 - x^5 + x^6 + 2x^9$	$-2x^2 - 3x^3 + x^4 - x^5 + 3x^6 + 2x^7$
6	$-2 - x^4 + x^5 - x^6 + x^7 + 2x^{11}$	$-2 - 2x - x^4 + x^5 + x^6 + x^7$
7	$-2 - x^5 + x^6 - x^7 + x^8 + 2x^{13}$	$-5 - 3x + x^3 + 3x^4 + 2x^5 + x^6 - 4x^7$
8	$-2 - x^6 + x^7 - x^8 + x^9 + 2x^{15}$	$-2 + x - x^2 - 2x^3 - x^4 - x^5 + 3x^7$
9	$-2 - x^7 + x^8 - x^9 + x^{10} + 2x^{17}$	$-5 - x - x^2 + 2x^3 + x^4 + 2x^5 - x^6 - 3x^7$
10	$-2 - x^8 + x^9 - x^{10} + x^{11} + 2x^{19}$	$1 - x^2 - 2x^3 - 3x^4 - 2x^5 + 2x^6 + 2x^7$
11	$-2 - x^9 + x^{10} - x^{11} + x^{12} + 2x^{21}$	$-4 + x + x^3 + x^5 - 4x^6$
12	$-2 - x^{10} + x^{11} - x^{12} + x^{13} + 2x^{23}$	$x^2 - x^3 - x^4 - 2x^5 + x^6$
13	$-2 - x^{11} + x^{12} - x^{13} + x^{14} + 2x^{25}$	$2 + 2x - 2x^2 - x^3 - 2x^4 - 3x^5 + 3x^7$
14	$-2 - x^{12} + x^{13} - x^{14} + x^{15} + 2x^{27}$	$-5 - x + 4x^2 + x^3 + 2x^4 + x^5 - x^6 - 5x^7$
15	$-2 - x^{13} + x^{14} - x^{15} + x^{16} + 2x^{29}$	$-1 + x^2 + x^3 - x^5 - x^6$
16	$-2 + 2x - x^{14} + x^{15} - x^{16} + x^{17}$	$-4 + 3x + x^3 + x^4 - x^6 - x^7$
17	$-2 + 2x^3 - x^{15} + x^{16} - x^{17} + x^{18}$	$-1 - x + x^2 + x^3$
18	$-2 + 2x^5 - x^{16} + x^{17} - x^{18} + x^{19}$	$-2 + x - x^2 + x^3 - x^4 + 2x^5$
19	$-2 + 2x^7 - x^{17} + x^{18} - x^{19} + x^{20}$	$-2 + x^2 - x^3 + x^4 - x^5 + 2x^7$
20	$-2 + 2x^9 - x^{18} + x^{19} - x^{20} + x^{21}$	$-2x^2 - x^3 - x^4 + x^5 + x^6 + 2x^7$
21	$-2 + 2x^{11} - x^{19} + x^{20} - x^{21} + x^{22}$	$-2 - 2x + x^4 - x^5 + 3x^6 - x^7$
22	$-2 + 2x^{13} - x^{20} + x^{21} - x^{22} + x^{23}$	$-3 - x - x^3 + x^4 + 2x^5 - x^6$
23	$-2 + 2x^{15} - x^{21} + x^{22} - x^{23} + x^{24}$	$-6 - x + x^2 + 2x^3 + x^4 + x^5 - 3x^7$
24	$-2 + 2x^{17} - x^{22} + x^{23} - x^{24} + x^{25}$	$1 + x - 3x^2 - 2x^3 - x^4 - 2x^5 + x^6 + 3x^7$
25	$-2 + 2x^{19} - x^{23} + x^{24} - x^{25} + x^{26}$	$-5 + x^2 + 2x^3 - x^4 + 2x^5 - x^6 - 2x^7$
26	$-2 + 2x^{21} - x^{24} + x^{25} - x^{26} + x^{27}$	$-x - x^3 - x^5$
27	$-2 + 2x^{23} - x^{25} + x^{26} - x^{27} + x^{28}$	$4x - x^2 - 2x^3 - 3x^4 - 2x^5 - x^6 + 4x^7$
28	$-2 + 2x^{25} - x^{26} + x^{27} - x^{28} + x^{29}$	$-2 - 2x + 2x^2 + x^3 + 2x^4 - x^5 - 3x^7$
29	$-1 + x^{27} + x^{28} - x^{29}$	$1 + x - x^3 - 2x^4 - x^5 + x^6 + x^7$

Appendix B. $R_t^{\bmod b}(x) \bmod \Phi_b(x)$ table

$t \bmod 3$	$R_t^{\bmod 3}(x)$	$R_t^{\bmod 3}(x) \bmod \Phi_3(x)$
0	$-5 + 5x^2$	$-10 - 5x$
1	$1 - x$	$1 - x$
2	$3x - 3x^2$	$3 + 6x$

$t \bmod 5$	$R_t^{\bmod 5}(x)$	$R_t^{\bmod 5}(x) \bmod \Phi_5(x)$
0	$-5 - x + x^3 + 5x^4$	$-10 - 6x - 5x^2 - 4x^3$
1	$1 - x - x^2 + x^4$	$-2x - 2x^2 - x^3$
2	$-1 + 3x - 3x^2 + x^3$	$-1 + 3x - 3x^2 + x^3$
3	$x + 3x^2 - 3x^3 - x^4$	$1 + 2x + 4x^2 - 2x^3$

4	$-3 + 3x^2 + 3x^3 - 3x^4$	$3x + 6x^2 + 6x^3$
$t \bmod 6$	$R_t^{\bmod 6}(x)$	$R_t^{\bmod 6}(x) \bmod \Phi_6(x)$
0	$-5 - x + x^4 + 5x^5$	$-7x$
1	$1 - x - x^2 + x^5$	$3 - 3x$
2	$-1 + 3x - 3x^2 + x^3$	1
3	$-2 + x + 3x^2 - 3x^3 - x^4 + 2x^5$	$3x$
4	$-2 + 2x + x^2 + 3x^3 - 3x^4 - x^5$	$-7 + 7x$
5	$-3 + 3x^3 + 3x^4 - 3x^5$	-9
$t \bmod 10$	$R_t^{\bmod 10}(x)$	$R_t^{\bmod 10}(x) \bmod \Phi_{10}(x)$
0	$-5 - x + x^8 + 5x^9$	$-6x + 5x^2 - 6x^3$
1	$1 - x - x^2 + x^9$	$2 - 2x - x^3$
2	$-1 + 3x - 3x^2 + x^3$	$-1 + 3x - 3x^2 + x^3$
3	$-2 + x + 3x^2 - 3x^3 - x^4 + 2x^5$	$-3 + 4x^2 - 4x^3$
4	$-2 + x^2 + 3x^3 - 3x^4 - x^5 + 2x^7$	$2 - 3x + 2x^2$
5	$-2 + x^3 + 3x^4 - 3x^5 - x^6 + 2x^9$	$2x - x^2 + 2x^3$
6	$-2 + 2x + x^4 + 3x^5 - 3x^6 - x^7$	$-6 + 6x + x^3$
7	$-2 + 2x^3 + x^5 + 3x^6 - 3x^7 - x^8$	$-3 - 3x + 3x^2 + 3x^3$
8	$-2 + 2x^5 + x^6 + 3x^7 - 3x^8 - x^9$	$-5 - 4x^2 + 4x^3$
9	$-3 + 3x^7 + 3x^8 - 3x^9$	$-6 + 3x - 6x^2$
$t \bmod 15$	$R_t^{\bmod 15}(x)$	$R_t^{\bmod 15}(x) \bmod \Phi_{15}(x)$
0	$-5 - x + x^{13} + 5x^{14}$	$1 - 2x - 5x^2 + 5x^3 - 6x^4 + x^5 + 5x^6 - 6x^7$
1	$1 - x - x^2 + x^{14}$	$2 - x - 2x^2 + x^3 - x^4 + x^6 - x^7$
2	$-1 + 3x - 3x^2 + x^3$	$-1 + 3x - 3x^2 + x^3$
3	$-2 + x + 3x^2 - 3x^3 - x^4 + 2x^5$	$-2 + x + 3x^2 - 3x^3 - x^4 + 2x^5$
4	$-2 + x^2 + 3x^3 - 3x^4 - x^5 + 2x^7$	$-2 + x^2 + 3x^3 - 3x^4 - x^5 + 2x^7$
5	$-2 + x^3 + 3x^4 - 3x^5 - x^6 + 2x^9$	$-4 + 2x^2 - x^3 + 3x^4 - 3x^5 - 3x^6 + 2x^7$
6	$-2 + x^4 + 3x^5 - 3x^6 - x^7 + 2x^{11}$	$-2 - 2x + x^4 + 3x^5 - 5x^6 - x^7$
7	$-2 + x^5 + 3x^6 - 3x^7 - x^8 + 2x^{13}$	$1 - 3x + x^3 - 3x^4 + 4x^5 + 3x^6 - 6x^7$
8	$x^6 + 3x^7 - 3x^8 - x^9$	$4 - 3x - x^2 + 4x^3 - 3x^4 + 3x^5 + 2x^6 - x^7$
9	$-2 + 2x^2 + x^7 + 3x^8 - 3x^9 - x^{10}$	$-1 + 3x - x^2 + 3x^4 - 2x^5 + 3x^6 + x^7$
10	$-2 + 2x^4 + x^8 + 3x^9 - 3x^{10} - x^{11}$	$-3 + 2x + 2x^2 - 4x^3 + 3x^4 + 2x^5 - 2x^6 + 4x^7$
11	$-2 + 2x^6 + x^9 + 3x^{10} - 3x^{11} - x^{12}$	$-6 + 3x + 2x^2 - x^3 - 3x^5 + 4x^6 + 2x^7$
12	$-2 + 2x^8 + x^{10} + 3x^{11} - 3x^{12} - x^{13}$	$-6 + 3x^2 - 2x^3 + 3x^4 - 4x^5 - 3x^6 + 6x^7$
13	$-2 + 2x^{10} + x^{11} + 3x^{12} - 3x^{13} - x^{14}$	$-8 + 2x - 2x^2 - x^3 + 4x^4 - 5x^5 - 2x^6 + x^7$
14	$-3 + 3x^{12} + 3x^{13} - 3x^{14}$	$-3 - 3x - 3x^3 + 3x^5 - 3x^6 - 3x^7$
$t \bmod 30$	$R_t^{\bmod 30}(x)$	$R_t^{\bmod 30}(x) \bmod \Phi_{30}(x)$
0	$-5 - x + x^{28} + 5x^{29}$	$-9 + 5x^2 + 5x^3 + 4x^4 - x^5 - 5x^6 - 4x^7$
1	$1 - x - x^2 + x^{29}$	$-x + x^3 + x^4 - x^6 - x^7$
2	$-1 + 3x - 3x^2 + x^3$	$-1 + 3x - 3x^2 + x^3$
3	$-2 + x + 3x^2 - 3x^3 - x^4 + 2x^5$	$-2 + x + 3x^2 - 3x^3 - x^4 + 2x^5$
4	$-2 + x^2 + 3x^3 - 3x^4 - x^5 + 2x^7$	$-2 + x^2 + 3x^3 - 3x^4 - x^5 + 2x^7$
5	$-2 + x^3 + 3x^4 - 3x^5 - x^6 + 2x^9$	$-2x^2 - x^3 + 3x^4 - 3x^5 + x^6 + 2x^7$
6	$-2 + x^4 + 3x^5 - 3x^6 - x^7 + 2x^{11}$	$-2 - 2x + x^4 + 3x^5 - x^6 - x^7$
7	$-2 + x^5 + 3x^6 - 3x^7 - x^8 + 2x^{13}$	$-3 - x - x^3 + x^4 + 2x^5 + 3x^6 - 4x^7$
8	$-2 + x^6 + 3x^7 - 3x^8 - x^9 + 2x^{15}$	$-2 + 3x + x^2 - 2x^3 - 3x^4 - 3x^5 + 5x^7$
9	$-2 + x^7 + 3x^8 - 3x^9 - x^{10} + 2x^{17}$	$-7 - 3x + x^2 + 6x^3 + 3x^4 + 2x^5 - 3x^6 - 5x^7$
10	$-2 + x^8 + 3x^9 - 3x^{10} - x^{11} + 2x^{19}$	$3 - 3x^2 - 2x^3 - x^4 - 2x^5 + 2x^6 + 2x^7$
11	$-2 + x^9 + 3x^{10} - 3x^{11} - x^{12} + 2x^{21}$	$-4 + 3x - x^3 + 3x^5 - 4x^6$
12	$-2 + x^{10} + 3x^{11} - 3x^{12} - x^{13} + 2x^{23}$	$3x^2 - 2x^3 - 3x^4 - 2x^5 + 3x^6$
13	$-2 + x^{11} + 3x^{12} - 3x^{13} - x^{14} + 2x^{25}$	$2 + 2x - 2x^2 + x^3 - 2x^4 - 5x^5 + 5x^7$
14	$-2 + x^{12} + 3x^{13} - 3x^{14} - x^{15} + 2x^{27}$	$-7 - 3x + 4x^2 + 3x^4 + 6x^4 + 3x^5 - 3x^6 - 7x^7$
15	$-2 + x^{13} + 3x^{14} - 3x^{15} - x^{16} + 2x^{29}$	$1 - x^2 - x^3 + x^5 + x^6$
16	$-2 + 2x + x^{14} + 3x^{15} - 3x^{16} - x^{17}$	$-4 + 5x - x^3 - x^4 + x^6 + x^7$
17	$-2 + 2x^3 + x^{15} + 3x^{16} - 3x^{17} - x^{18}$	$-3 - 3x + 3x^2 + 3x^3$
18	$-2 + 2x^5 + x^{16} + 3x^{17} - 3x^{18} - x^{19}$	$-2 - x - 3x^2 + 3x^3 + x^4 + 2x^5$
19	$-2 + 2x^7 + x^{17} + 3x^{18} - 3x^{19} - x^{20}$	$-2 - x^2 - 3x^3 + 3x^4 + x^5 + 2x^7$
20	$-2 + 2x^9 + x^{18} + 3x^{19} - 3x^{20} - x^{21}$	$-2x^2 - 3x^3 - 3x^4 + 3x^5 + 3x^6 + 2x^7$
21	$-2 + 2x^{11} + x^{19} + 3x^{20} - 3x^{21} - x^{22}$	$-2 - 2x - x^4 - 3x^5 + 5x^6 + x^7$
22	$-2 + 2x^{13} + x^{20} + 3x^{21} - 3x^{22} - x^{23}$	$-5 - 3x + x^3 + 3x^4 + 2x^5 - 3x^6$
23	$-2 + 2x^{15} + x^{21} + 3x^{22} - 3x^{23} - x^{24}$	$-6 - 3x - x^2 + 2x^3 + 3x^4 + 3x^5 - 5x^7$
24	$-2 + 2x^{17} + x^{22} + 3x^{23} - 3x^{24} - x^{25}$	$3 + 3x - 5x^2 - 6x^3 - 3x^4 - 2x^5 + 3x^6 + 5x^7$
25	$-2 + 2x^{19} + x^{23} + 3x^{24} - 3x^{25} - x^{26}$	$-7 + 3x^2 + 2x^3 - 3x^4 + 2x^5 - 2x^6 - 2x^7$
26	$-2 + 2x^{21} + x^{24} + 3x^{25} - 3x^{26} - x^{27}$	$-3x + x^3 - 3x^5$
27	$-2 + 2x^{23} + x^{25} + 3x^{26} - 3x^{27} - x^{28}$	$4x - 3x^2 - 2x^3 - x^4 - 2x^5 - 3x^6 + 4x^7$
28	$-2 + 2x^{25} + x^{26} + 3x^{27} - 3x^{28} - x^{29}$	$-2 - 2x + 2x^2 - x^3 + 2x^4 + x^5 - 5x^7$
29	$-3 + 3x^{27} + 3x^{28} - 3x^{29}$	$3 + 3x - 3x^3 - 6x^4 - 3x^5 + 3x^6 + 3x^7$

Appendix C. $U_t^{\text{mod } b}(x) \bmod \Phi_b(x)$ table

$t \bmod 3$	$U_t^{\text{mod } 3}(x)$	$U_t^{\text{mod } 3}(x) \bmod \Phi_3(x)$
0	$-3x + 3x^2$	$-3 - 6x$
1	$1 - x$	$1 - x$
2	$1 - x^2$	$2 + x$

$t \bmod 5$	$U_t^{\text{mod } 5}(x)$	$U_t^{\text{mod } 5}(x) \bmod \Phi_5(x)$
0	$-5x + 5x^4$	$-5 - 10x - 5x^2 - 5x^3$
1	$x - x^3$	$x - x^3$
2	$-3 - 2x + 2x^2 + 3x^3$	$-3 - 2x + 2x^2 + 3x^3$
3	$3 - 3x^2$	$3 - 3x^2$
4	$2 - 2x + 3x^2 - 3x^4$	$5 + x + 6x^2 + 3x^3$

$t \bmod 6$	$U_t^{\text{mod } 6}(x)$	$U_t^{\text{mod } 6}(x) \bmod \Phi_6(x)$
0	$-4x - x^2 + x^4 + 4x^5$	$5 - 10x$
1	$1 - x^4$	$1 + x$
2	$-1 + x^2 + 2x^3 - 2x^5$	$-6 + 3x$
3	$-4x - x^2 + x^4 + 4x^5$	$5 - 10x$
4	$1 - x^4$	$1 + x$
5	$-1 + x^2 + 2x^3 - 2x^5$	$-6 + 3x$

$t \bmod 10$	$U_t^{\text{mod } 10}(x)$	$U_t^{\text{mod } 10}(x) \bmod \Phi_{10}(x)$
0	$-4x + x^4 - x^6 + 4x^9$	$3 - 6x + 3x^2 - 3x^3$
1	$x^6 - x^8$	$-x + x^3$
2	$-1 - 2x + 2x^3 - 2x^5 + 2x^7 + x^8$	$1 - 2x - 2x^2 + x^3$
3	$1 - x^2 + 2x^5 - 2x^7$	$-1 + x^2$
4	$-2x + x^2 - x^4 + 2x^5 + 2x^7 - 2x^9$	$-3 - x - 2x^2 + x^3$
5	$-4x + x^4 - x^6 + 4x^9$	$3 - 6x + 3x^2 - 3x^3$
6	$x^6 - x^8$	$-x + x^3$
7	$-1 - 2x + 2x^3 - 2x^5 + 2x^7 + x^8$	$1 - 2x - 2x^2 + x^3$
8	$1 - x^2 + 2x^5 - 2x^7$	$-1 + x^2$
9	$-2x + x^2 - x^4 + 2x^5 + 2x^7 - 2x^9$	$-3 - x - 2x^2 + x^3$

$t \bmod 15$	$U_t^{\text{mod } 15}(x)$	$U_t^{\text{mod } 15}(x) \bmod \Phi_{15}(x)$
0	$-4x + x^4 - x^{11} + 4x^{14}$	$4 - 3x - 4x^2 + 4x^3 - 3x^4 + 5x^6 - 4x^7$
1	$x^6 - x^{13}$	$-1 + x + x^4 - x^5 + x^6 + x^7$
2	$-1 - 2x + 2x^3 - 2x^5 + 2x^7 + x^8$	$-2 - x + x^3 + x^4 - 3x^5 + 3x^7$
3	$-2x - x^2 + 2x^5 - 2x^7 + x^{10} + 2x^{11}$	$-1 - 4x - x^2 + x^5 - 2x^6 - 2x^7$
4	$2 - 2x - x^4 + 2x^7 - 2x^9 + x^{12}$	$4 - 2x - 3x^2 + 2x^3 - x^4 + 2x^6 - x^7$
5	$-2x + 2x^4 - x^6 + 2x^9 - 2x^{11} + x^{14}$	$-1 + x^2 - x^3 + x^4 + x^7$
6	$-x + x^8 + 2x^{11} - 2x^{13}$	$-3 - x^3 + 3x^4 - 3x^5 - 2x^6 + 3x^7$
7	$-2 - 2x + x^3 - x^{10} + 2x^{12} + 2x^{13}$	$1 - 4x - 2x^2 + x^3 - 2x^4 + 3x^5 - 4x^7$
8	$2 - 2x^2 + x^5 - x^{12}$	$2 - x^2 + x^5 + x^7$
9	$-2x + 2x^2 - 2x^4 + 2x^5 + x^7 - x^{14}$	$-1 - 2x + 3x^2 - x^3 - x^4 + 2x^5 - x^6 + 2x^7$
10	$-3x + 2x^4 - 2x^6 + 3x^9$	$-3 - 3x + 3x^2 - 3x^3 + 2x^4 - 5x^6 + 3x^7$
11	$-2x - x^3 + 2x^6 - 2x^8 + x^{11} + 2x^{13}$	$4 - 7x + x^3 - 4x^4 + 4x^5 + x^6 - 4x^7$
12	$-2x + 2x^2 - x^5 + 2x^8 - 2x^{10} + x^{13}$	$1 - x + 2x^2 - 2x^3 + x^4 + x^7$
13	$1 - 2x + 2x^6 - x^7 + 2x^{10} - 2x^{12}$	$-1 - 2x + 2x^2 - 2x^5 + 2x^6 + x^7$
14	$-2x + x^2 - x^9 + 2x^{10} + 2x^{12} - 2x^{14}$	$-3 - 2x - x^3 + 2x^4 - 2x^5 - x^6 - x^7$

$t \bmod 30$	$U_t^{\text{mod } 30}(x)$	$U_t^{\text{mod } 30}(x) \bmod \Phi_{30}(x)$
0	$-4x + x^4 - x^{26} + 4x^{29}$	$-4 - 5x + 4x^2 + 4x^3 + 5x^4 - 3x^6 - 4x^7$
1	$x^6 - x^{28}$	$-1 - x + x^4 + x^5 + x^6 - x^7$
2	$-1 - 2x + 2x^3 - 2x^5 + 2x^7 + x^8$	$-2 - 3x + 3x^3 + x^4 - x^5 + x^7$
3	$-2x - x^2 + 2x^5 - 2x^7 + x^{10} + 2x^{11}$	$-1 - 4x - x^2 + 3x^5 + 2x^6 - 2x^7$
4	$-2x - x^4 + 2x^7 - 2x^9 + x^{12} + 2x^{15}$	$-4 - 2x + 2x^2 + 2x^3 - x^4 - 2x^6 + x^7$
5	$-2x - x^6 + 2x^9 - 2x^{11} + x^{14} + 2x^{19}$	$3 - 3x^2 - 3x^3 - 3x^4 + 3x^7$
6	$-2x - x^8 + 2x^{11} - 2x^{13} + x^{16} + 2x^{23}$	$5 - 3x^3 - 5x^4 - 5x^5 + 2x^6 + 5x^7$
7	$-2x - x^{10} + 2x^{13} - 2x^{15} + x^{18} + 2x^{27}$	$1 - 4x + 2x^2 - x^3 + 2x^4 + x^5 - 4x^7$
8	$-x^{12} + 2x^{15} - 2x^{17} + x^{20}$	$-2 + 3x^2 - x^5 - x^7$
9	$-2x + 2x^5 - x^{14} + 2x^{17} - 2x^{19} + x^{22}$	$-1 - 2x - x^2 + x^3 + 3x^4 + 2x^5 - x^6 - 2x^7$
10	$-2x + 2x^9 - x^{16} + 2x^{19} - 2x^{21} + x^{24}$	$1 - x - x^2 - x^3 - 2x^4 + 3x^6 + x^7$
11	$-2x + 2x^{13} - x^{18} + 2x^{21} - 2x^{23} + x^{26}$	$-4 - 5x + 3x^3 + 4x^4 + 4x^5 - 3x^6 - 4x^7$
12	$-2x + 2x^{17} - x^{20} + 2x^{23} - 2x^{25} + x^{28}$	$1 + x - 2x^2 - 2x^3 - 3x^4 + 3x^7$
13	$1 - 2x + 2x^{21} - x^{22} + 2x^{25} - 2x^{27}$	$3 - 2x - 2x^2 - 2x^5 - 2x^6 + 3x^7$
14	$-2x + x^2 - x^{24} + 2x^{25} + 2x^{27} - 2x^{29}$	$5 - 2x - 3x^3 - 2x^4 - 2x^5 + 3x^6 + x^7$
15	$-4x + x^4 - x^{26} + 4x^{29}$	$-4 - 5x + 4x^2 + 4x^3 + 5x^4 - 3x^6 - 4x^7$
16	$x^6 - x^{28}$	$-1 - x + x^4 + x^5 + x^6 - x^7$

17	$-1 - 2x + 2x^3 - 2x^5 + 2x^7 + x^8$	$-2 - 3x + 3x^3 + x^4 - x^5 + x^7$
18	$-2x - x^2 + 2x^5 - 2x^7 + x^{10} + 2x^{11}$	$-1 - 4x - x^2 + 3x^5 + 2x^6 - 2x^7$
19	$-2x - x^4 + 2x^7 - 2x^9 + x^{12} + 2x^{15}$	$-4 - 2x + x^2 + 2x^3 - x^4 - 2x^6 + x^7$
20	$-2x - x^6 + 2x^9 - 2x^{11} + x^{14} + 2x^{19}$	$3 - 3x^2 - 3x^3 - 3x^4 + 3x^7$
21	$-2x - x^8 + 2x^{11} - 2x^{13} + x^{16} + 2x^{23}$	$5 - 3x^3 - 5x^4 - 5x^5 + 2x^6 + 5x^7$
22	$-2x - x^{10} + 2x^{13} - 2x^{15} + x^{18} + 2x^{27}$	$1 - 4x + 2x^2 - x^3 + 2x^4 + x^5 - 4x^7$
23	$-x^{12} + 2x^{15} - 2x^{17} + x^{20}$	$-2 + 3x^2 - x^5 - x^7$
24	$-2x + 2x^5 - x^{14} + 2x^{17} - 2x^{19} + x^{22}$	$-1 - 2x - x^2 + x^3 + 3x^4 + 2x^5 - x^6 - 2x^7$
25	$-2x + 2x^9 - x^{16} + 2x^{19} - 2x^{21} + x^{24}$	$1 - x - x^2 - x^3 - 2x^4 + 3x^6 + x^7$
26	$-2x + 2x^{13} - x^{18} + 2x^{21} - 2x^{23} + x^{26}$	$-4 - 5x + 3x^3 + 4x^4 + 4x^5 - 3x^6 - 4x^7$
27	$-2x + 2x^{17} - x^{20} + 2x^{23} - 2x^{25} + x^{28}$	$1 + x - 2x^2 - 2x^3 - 3x^4 + 3x^7$
28	$1 - 2x + 2x^{21} - x^{22} + 2x^{25} - 2x^{27}$	$3 - 2x - 2x^2 - 2x^5 - 2x^6 + 3x^7$
29	$-2x + x^2 - x^{24} + 2x^{25} + 2x^{27} - 2x^{29}$	$5 - 2x - 3x^3 - 2x^4 - 2x^5 + 3x^6 + x^7$

Appendix D. $W_t^{\bmod b}(x) \bmod \Phi_b(x)$ table

$t \bmod 3$	$W_t^{\bmod 3}(x)$	$W_t^{\bmod 3}(x) \bmod \Phi_3(x)$
0	$-5x + 5x^2$	$-5 - 10x$
1	$-1 + x$	$-1 + x$
2	$3 - 3x^2$	$6 + 3x$

$t \bmod 5$	$W_t^{\bmod 5}(x)$	$W_t^{\bmod 5}(x) \bmod \Phi_5(x)$
0	$-3x + 3x^4$	$-3 - 6x - 3x^2 - 3x^3$
1	$-x + x^3$	$-x + x^3$
2	$-1 - 2x + 2x^2 + x^3$	$-1 - 2x + 2x^2 + x^3$
3	$1 - x^2$	$1 - x^2$
4	$2 - 2x + x^2 - x^4$	$3 - x + 2x^2 + x^3$

$t \bmod 6$	$W_t^{\bmod 6}(x)$	$W_t^{\bmod 6}(x) \bmod \Phi_6(x)$
0	$-4x + x^2 - x^4 + 4x^5$	$3 - 6x$
1	$-1 + x^4$	$-1 - x$
2	$1 - x^2 + 2x^3 - 2x^5$	$-2 + x$
3	$-4x + x^2 - x^4 + 4x^5$	$3 - 6x$
4	$-1 + x^4$	$-1 - x$
5	$1 - x^2 + 2x^3 - 2x^5$	$-2 + x$

$t \bmod 10$	$W_t^{\bmod 10}(x)$	$W_t^{\bmod 10}(x) \bmod \Phi_{10}(x)$
0	$-4x - x^4 + x^6 + 4x^9$	$5 - 10x + 5x^2 - 5x^3$
1	$-x^6 + x^8$	$x - x^3$
2	$1 - 2x + 2x^3 - 2x^5 + 2x^7 - x^8$	$3 - 2x - 2x^2 + 3x^3$
3	$-1 + x^2 + 2x^5 - 2x^7$	$-3 + 3x^2$
4	$-2x - x^2 + x^4 + 2x^5 + 2x^7 - 2x^9$	$-5 + x - 6x^2 + 3x^3$
5	$-4x - x^4 + x^6 + 4x^9$	$5 - 10x + 5x^2 - 5x^3$
6	$-x^6 + x^8$	$x - x^3$
7	$1 - 2x + 2x^3 - 2x^5 + 2x^7 - x^8$	$3 - 2x - 2x^2 + 3x^3$
8	$-1 + x^2 + 2x^5 - 2x^7$	$-3 + 3x^2$
9	$-2x - x^2 + x^4 + 2x^5 + 2x^7 - 2x^9$	$-5 + x - 6x^2 + 3x^3$

$t \bmod 15$	$W_t^{\bmod 15}(x)$	$W_t^{\bmod 15}(x) \bmod \Phi_{15}(x)$
0	$-4x - x^4 + x^{11} + 4x^{14}$	$4 - 5x - 4x^2 + 4x^3 - 5x^4 + 3x^6 - 4x^7$
1	$-x^6 + x^{13}$	$1 - x - x^4 + x^5 - x^6 - x^7$
2	$1 - 2x + 2x^3 - 2x^5 + 2x^7 - x^8$	$2 - 3x + 3x^3 - x^4 - x^5 + x^7$
3	$-2x + x^2 + 2x^5 - 2x^7 - x^{10} + 2x^{11}$	$1 - 4x + x^2 + 3x^5 - 2x^6 - 2x^7$
4	$2 - 2x + x^4 + 2x^7 - 2x^9 - x^{12}$	$4 - 2x - x^2 + 2x^3 + x^4 + 2x^6 + x^7$
5	$-2x + 2x^4 + x^6 + 2x^9 - 2x^{11} - x^{14}$	$-3 + 3x^2 - 3x^3 + 3x^4 + 3x^7$
6	$-3x + 3x^8 + 2x^{11} - 2x^{13}$	$-5 - 3x^3 + 5x^4 - 5x^5 - 2x^6 + 5x^7$
7	$-2 - 2x - x^3 + x^{10} + 2x^{12} + 2x^{13}$	$-1 - 4x - 2x^2 - x^3 - 2x^4 + x^5 - 4x^7$
8	$2 - 2x^2 - x^5 + x^{12}$	$2 - 3x^2 - x^5 - x^7$
9	$-2x + 2x^2 - 2x^4 + 2x^5 - x^7 + x^{14}$	$1 - 2x + x^2 + x^3 - 3x^4 + 2x^5 + x^6 - 2x^7$
10	$-x + 2x^4 - 2x^6 + x^9$	$-1 - x + x^2 - x^3 + 2x^4 - 3x^6 + x^7$
11	$-2x + x^3 + 2x^6 - 2x^8 - x^{11} + 2x^{13}$	$4 - 5x + 3x^3 - 4x^4 + 4x^5 + 3x^6 - 4x^7$
12	$-2x + 2x^2 + x^5 + 2x^8 - 2x^{10} - x^{13}$	$-1 + x + 2x^2 - 2x^3 + 3x^4 + 3x^7$
13	$-1 - 2x + 2x^6 + x^7 + 2x^{10} - 2x^{12}$	$-3 - 2x + 2x^2 - 2x^5 + 2x^6 + 3x^7$
14	$-2x - x^2 + x^9 + 2x^{10} + 2x^{12} - 2x^{14}$	$-5 - 2x - 3x^3 + 2x^4 - 2x^5 - 3x^6 + x^7$

$t \bmod 30$	$W_t^{\bmod 30}(x)$	$W_t^{\bmod 30}(x) \bmod \Phi_{30}(x)$
0	$-4x - x^4 + x^{26} + 4x^{29}$	$-4 - 3x + 4x^2 + 4x^3 + 3x^4 - 5x^6 - 4x^7$

1	$-x^6 + x^{28}$	$1 + x - x^4 - x^5 - x^6 + x^7$
2	$1 - 2x + 2x^3 - 2x^5 + 2x^7 - x^8$	$2 - x + x^3 - x^4 - 3x^5 + 3x^7$
3	$-2x + x^2 + 2x^5 - 2x^7 - x^{10} + 2x^{11}$	$1 - 4x + x^2 + x^5 + 2x^6 - 2x^7$
4	$-2x + x^4 + 2x^7 - 2x^9 - x^{12} + 2x^{15}$	$-4 - 2x + 3x^2 + 2x^3 + x^4 - 2x^6 - x^7$
5	$-2x + x^6 + 2x^9 - 2x^{11} - x^{14} + 2x^{19}$	$1 - x^2 - x^3 - x^4 + x^7$
6	$-2x + x^8 + 2x^{11} - 2x^{13} - x^{16} + 2x^{23}$	$3 - x^3 - 3x^4 - 3x^5 + 2x^6 + 3x^7$
7	$-2x + x^{10} + 2x^{13} - 2x^{15} - x^{18} + 2x^{27}$	$-1 - 4x + 2x^2 + x^3 + 2x^4 + 3x^5 - 4x^7$
8	$x^{12} + 2x^{15} - 2x^{17} - x^{20}$	$-2 + x^2 + x^5 + x^7$
9	$-2x + 2x^5 + x^{14} + 2x^{17} - 2x^{19} - x^{22}$	$1 - 2x - 3x^2 - x^3 + x^4 + 2x^5 + x^6 + 2x^7$
10	$-2x + 2x^9 + x^{16} + 2x^{19} - 2x^{21} - x^{24}$	$3 - 3x - 3x^2 - 3x^3 - 2x^4 + 5x^6 + 3x^7$
11	$-2x + 2x^{13} + x^{18} + 2x^{21} - 2x^{23} - x^{26}$	$-4 - 7x + x^3 + 4x^4 + 4x^5 - x^6 - 4x^7$
12	$-2x + 2x^{17} + x^{20} + 2x^{23} - 2x^{25} - x^{28}$	$-1 - x - 2x^2 - 2x^3 - x^4 + x^7$
13	$-1 - 2x + 2x^{21} + x^{22} + 2x^{25} - 2x^{27}$	$1 - 2x - 2x^2 - 2x^5 - 2x^6 + x^7$
14	$-2x - x^2 + x^{24} + 2x^{25} + 2x^{27} - 2x^{29}$	$3 - 2x - x^3 - 2x^4 - 2x^5 + x^6 - x^7$
15	$-4x - x^4 + x^{26} + 4x^{29}$	$-4 - 3x + 4x^2 + 4x^3 + 3x^4 - 5x^6 - 4x^7$
16	$-x^6 + x^{28}$	$1 + x - x^4 - x^5 - x^6 + x^7$
17	$1 - 2x + 2x^3 - 2x^5 + 2x^7 - x^8$	$2 - x + x^3 - x^4 - 3x^5 + 3x^7$
18	$-2x + x^2 + 2x^5 - 2x^7 - x^{10} + 2x^{11}$	$1 - 4x + x^2 + x^5 + 2x^6 - 2x^7$
19	$-2x + x^4 + 2x^7 - 2x^9 - x^{12} + 2x^{15}$	$-4 - 2x + 3x^2 + 2x^3 + x^4 - 2x^6 - x^7$
20	$-2x + x^6 + 2x^9 - 2x^{11} - x^{14} + 2x^{19}$	$1 - x^2 - x^3 - x^4 + x^7$
21	$-2x + x^8 + 2x^{11} - 2x^{13} - x^{16} + 2x^{23}$	$3 - x^3 - 3x^4 - 3x^5 + 2x^6 + 3x^7$
22	$-2x + x^{10} + 2x^{13} - 2x^{15} - x^{18} + 2x^{27}$	$-1 - 4x + 2x^2 + x^3 + 2x^4 + 3x^5 - 4x^7$
23	$x^{12} + 2x^{15} - 2x^{17} - x^{20}$	$-2 + x^2 + x^5 + x^7$
24	$-2x + 2x^5 + x^{14} + 2x^{17} - 2x^{19} - x^{22}$	$1 - 2x - 3x^2 - x^3 + x^4 + 2x^5 + x^6 + 2x^7$
25	$-2x + 2x^9 + x^{16} + 2x^{19} - 2x^{21} - x^{24}$	$3 - 3x - 3x^2 - 3x^3 - 2x^4 + 5x^6 + 3x^7$
26	$-2x + 2x^{13} + x^{18} + 2x^{21} - 2x^{23} - x^{26}$	$-4 - 7x + x^3 + 4x^4 + 4x^5 - x^6 - 4x^7$
27	$-2x + 2x^{17} + x^{20} + 2x^{23} - 2x^{25} - x^{28}$	$-1 - x - 2x^2 - 2x^3 - x^4 + x^7$
28	$-1 - 2x + 2x^{21} + x^{22} + 2x^{25} - 2x^{27}$	$1 - 2x - 2x^2 - 2x^5 - 2x^6 + x^7$
29	$-2x - x^2 + x^{24} + 2x^{25} + 2x^{27} - 2x^{29}$	$3 - 2x - x^3 - 2x^4 - 2x^5 + x^6 - x^7$

Appendix E. Roots of certain polynomials

In this appendix section, we will prove that some required polynomials truly do not possess any root that is a root of unity as well, as claimed multiple times throughout Section 4. The polynomials of interest shall be the four following ones:

$$Z_1(x) = 2x^{10} + x^5 + 2, \qquad Z_2(x) = 2x^{10} - x^5 + 2, \qquad Z_3(x) = 2x^6 + x^3 + 2, \qquad Z_4(x) = 2x^6 - x^3 + 2.$$

First and foremost, let us define the next two additional polynomials:

$$Z'(x) = 2x^2 + x + 2, \qquad\qquad\qquad Z''(x) = 2x^2 - x + 2.$$

It is clear that the roots of $Z_1(x)$ are actually the fifth roots of the roots of $Z'(x)$, while the roots of $Z_2(x)$ are the fifth roots of the roots of $Z''(x)$. Similarly, the roots of $Z_3(x)$ represent the third roots of the roots of $Z'(x)$, while the roots of $Z_4(x)$ represent the third roots of the roots of $Z''(x)$. Thus, in order to prove that neither of the four polynomials $Z_1(x), Z_2(x), Z_3(x), Z_4(x)$ contains a root that is a root of unity, it is sufficient to show that neither of the two polynomials $Z'(x), Z''(x)$ has such a root.

Now, if the polynomial $Z'(x)$ were to have a root that is a root of unity, then this root would surely represent a primitive b-th root of unity for some $b \in \mathbb{N}$, which would imply that $\Phi_b(x) \mid Z'(x)$ must hold. However, it is simple to show that the polynomial $Z'(x)$ is not divisible by any cyclotomic polynomial. The same logic can be applied to the $Z''(x)$ polynomial.

It is clear that neither $Z'(x)$ nor $Z''(x)$ can be divisible by a cyclotomic polynomial whose degree is greater than two. However, given the fact that $\deg \Phi_b = \varphi(b)$ for each $b \in \mathbb{N}$, where φ represents Euler's totient function, it is easy to deduce that only five cyclotomic polynomials have a degree that is not greater than two:

$$\Phi_1(x) = x - 1,$$
$$\Phi_2(x) = x + 1,$$
$$\Phi_3(x) = x^2 + x + 1,$$
$$\Phi_4(x) = x^2 + 1,$$

$$\Phi_6(x) = x^2 - x + 1.$$

It is trivial to check that neither $Z'(x)$ nor $Z''(x)$ is divisible by any of these five polynomials, which completes the proof.　□