Non-singular circulant graphs and digraphs

A. K. Lal[*] A Satyanarayana Reddy[*]

Abstract We give necessary and sufficient conditions for a few classes of known circulant graphs and/or digraphs to be singular. The above graph classes are generalized to (r, s, t)-digraphs for non-negative integers r, s and t, and the digraph $C_n^{i,j,k,l}$, with certain restrictions. We also obtain a necessary and sufficient condition for the digraphs $C_n^{i,j,k,l}$ to be singular. Some necessary conditions are given under which the (r, s, t)-digraphs are singular.

Keywords: Graphs, Digraphs, Circulant matrices, Primitive roots.

1 Introduction and preliminaries

Let $\mathbb{Q}$ denote the set of rational numbers. Then the set of all $n \times n$ matrices with entries from $\mathbb{Q}$ is denoted by $\mathbb{M}_n(\mathbb{Q})$. A matrix $A \in \mathbb{M}_n(\mathbb{Q})$ is said to be symmetric if $A = A^t$, where A^t denotes the transpose of the matrix A and is said to be circulant if $a_{ij} = a_{1,\, j-i+1}$, whenever $2 \le i \le n$ and $1 \le j \le n$, where the subscripts are read modulo n. From the definition, it is clear that if A is circulant then for each $i \ge 2$ the elements of the i-th row are obtained by cyclically shifting the elements of the $(i-1)$-th row one position to the right. So it is sufficient to specify its first row. For example, the identity matrix, denoted I, and the matrix of all 1's, denoted $\mathbf{J}$, are circulant matrices. Let W_n be a circulant matrix of order n with $[0, 1, 0, \ldots, 0]$ as its first row . Then the following result of Davis [4] establishes that every circulant matrix of order n is a polynomial in W_n.

Lemma 1.1. *[4] Let $A \in \mathbb{M}_n(\mathbb{Q})$. Then A is circulant if and only if it is a polynomial over $\mathbb{Q}$ in W_n.*

Let $A \in M_n(\mathbb{Q})$ be a circulant matrix. Then Lemma 1.1 ensures the existence of a polynomial $\gamma_A(x) \in \mathbb{Q}[x]$ such that $A = \gamma_A(W_n)$. We call $\gamma_A(x)$, the representer polynomial of A. For a fixed positive integer n, let ζ_n denote a primitive n-th root of unity. That is, $\zeta_n^n = 1$ and $\zeta_n^k \ne 1$ for $k = 1, 2, \ldots, n-1$. Then the following result about circulant matrices is well known.

Lemma 1.2. *Let $A \in M_n(\mathbb{Q})$ be a circulant matrix with $[a_0, a_1, \ldots, a_{n-1}]$ as its first row. Then*

1. $\gamma_A(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in \mathbb{Q}[x]$.
2. *the eigenvalues of A are given by $\gamma_A(\zeta_n^k)$, for $k = 0, 1, \ldots, n-1$.*

For definitions and results related to linear algebra, algebra and/or graph theory that have been used in this paper but not have been cleared defined or stated, the readers are advised to see any standard textbook on abstract algebra and/or graph theory(for example, see [6] and/or [3]).

[*]Department of Mathematics & Statistics, Indian Institute of Technology Kanpur, Kanpur - 208 016, India. E-Mails: arlal@iitk.ac.in; satya@iitk.ac.in.

Recall that a *directed graph* (in short, digraph) is an ordered pair $X = (V, E)$ that consists of two sets V, the vertex set, and E, the edge set, where V is a non-empty set and $E \subset V \times V$. If $e = (u, v) \in E$ with $u \neq v$ then the edge e is said to be *incident* from u to v. A digraph is called a *graph* if $(u, v) \in E$ whenever $(v, u) \in E$, for any two elements $u, v \in V$. An edge between u and v in the graph X is denoted by $\{u, v\}$. A graph/digraph is said to be finite, if $|V|$ (called the *order* of X) and $|E|$ (called the *size* of X) are finite. All the graphs/digraphs in this paper are finite. The adjacency matrix of a graph/digraph $X = (V, E)$ is a $|V| \times |V|$ matrix, denoted $A(X) = [a_{uv}]$, with $a_{uv} = 1$ if $(u, v) \in E$ and 0, otherwise. Observe that, whenever X is a graph the matrix $A(X)$ is symmetric. For example, if A denotes the adjacency matrix of the cycle graph C_n on n vertices, then A is a circulant matrix and $\gamma_A(x) = x + x^{n-1}$ is its representer polynomial. Therefore, for $r = 0, 1, \ldots, n-1$, the eigenvalues of C_n are given by $\lambda_r = 2\cos(\frac{2\pi r}{n})$. Throughout this paper, we assume that the greatest common divisor, in short gcd, of all the non-zero coefficients of $\gamma_A(x)$ is 1. It is well known that $x^n - 1 = \prod\limits_{d|n} \Phi_d(x)$ (here $a \mid b$ means a 'divides' b), where $\Phi_d(x) = \prod\limits_{\substack{\gcd(k,d)=1\\ 1\le k\le d}} (x - \zeta_d^k) \in \mathbb{Z}[x]$ is called the d-th cyclotomic polynomial. The polynomial $\Phi_n(x)$, for each positive integer n, is a monic irreducible polynomial over $\mathbb{Q}$ and hence the minimal polynomial of ζ_n. Also, $\deg(\Phi_n(x)) = \varphi(n)$, the well known Euler-totient function. Therefore, using the property of minimal polynomials, it follows that if $f(\zeta_n) = 0$ for some $f(x) \in \mathbb{Z}[x]$ then $\Phi_n(x)$ divides $f(x) \in \mathbb{Z}[x]$. Or equivalently, $f(\zeta_n) = 0$ for some $f(x) \in \mathbb{Z}[x]$ if and only if there exists a polynomial $g(x) \in \mathbb{Z}[x]$ such that $f(x) = \Phi_n(x)g(x)$. The next result appears on page 93 in [9].

Lemma 1.3. *[9] Let p be a prime number and let n be a positive integer. Then*

$$\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p), & \text{if } p \mid n, \\ \frac{\Phi_n(x^p)}{\Phi_n(x)}, & \text{if } p \nmid n. \end{cases}$$

In particular, $\Phi_{p^k}(x) = 1 + x^{p^{k-1}} + x^{2p^{k-1}} + \cdots + x^{(p-1)p^{k-1}}$ for every positive integer k.

The following result is an application of Lemma 1.2. This result also appears in the work of Geller, Kra, Popescu & Simanca [7].

Lemma 1.4 (Geller, Kra, Popesu & Simanca [7]). *Let $A \in \mathbb{M}_n(\mathbb{Q})$ be a circulant matrix with $\gamma_A(x)$ as its representer polynomial. Then the following statements are equivalent:*

1. *The matrix A is singular.*
2. $\deg(\gcd(\gamma_A(x), x^n - 1)) \geq 1$.

Fix a positive integer n, two distinct integers a and b and let s and t be positive integers with $s + t = n$. Suppose $[\underbrace{a, a, \ldots, a}_{s \text{ times}}, \underbrace{b, b, \ldots, b}_{t \text{ times}}]$ is the first row of a circulant matrix $A \in \mathbb{M}_n(\mathbb{Z})$. Then as a direct corollary of Lemma 1.4, one has the following result.

Corollary 1.5 (Davis [4]). *Let $[\underbrace{a, a, \ldots, a}_{s \text{ times}}, \underbrace{b, b, \ldots, b}_{t \text{ times}}]$ be the first row of the circulant matrix $A \in \mathbb{M}_n(\mathbb{Q})$. Then*

$$\det(A) = \begin{cases} (sa + tb)(a - b)^{n-1}, & \text{if } \gcd(s, n) = 1, \\ 0, & \text{otherwise.} \end{cases}$$

We now state a couple of known results that directly follow from Corollary 1.5.

Lemma 1.6. *The complete graph K_n, for $n \geq 2$, is non-singular.*

Proof. Let A be the adjacency matrix of complete graph K_n. Then $[0, 1, 1, \ldots, 1]$ is the first row of A. Hence the result follows from Corollary 1.5. $\square$

As a second application, we consider a particular class of circulant matrices that appeared in the work of Searle [11]. He considered the circulant matrices that have $[h_0, h_1, \ldots, h_{k-1}, \underbrace{0, \ldots, 0}_{n-k}]$ as its first row, where $h_0 \neq 0$ and $h_{k-1} \neq 0$. The above class of matrices was called a *k-element circulant matrix*. Since we are looking at digraphs, we assume $h_0 = 1 = h_{k-1}$. With an abuse of notation, the circulant matrix with $[\underbrace{1, 1, \ldots, 1}_{k}, \underbrace{0, 0, \ldots, 0}_{n-k}]$ as its first row will be called a *k-element circulant digraph*. With this notation, the second application of Corollary 1.5 is stated below.

Lemma 1.7. *Let X be a k-element circulant digraph on n vertices. Then X is non-singular if and only if* $\gcd(n, k) = 1$.

We now rephrase Lemma 1.4 in terms of cyclotomic polynomials. Let $A \in \mathbb{M}_n(\mathbb{Z})$ be a circulant matrix with $[a_0, a_1, \ldots, a_{n-1}]$ as its first row. Then $\gamma_A(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$ is the representer polynomial of A. Now, suppose that $a_0 = 0$ and let k be the smallest positive integer such that $a_k \neq 0$. Then $\gamma_A(x) = x^k \Gamma_A(x)$, for some polynomial $\Gamma_A(x) \in \mathbb{Z}[x]$. In this case, it follows that the matrix A is non-singular if and only if $\gcd(\Gamma_A(x), x^n - 1) = 1$ as $\gcd(x^k, x^n - 1) = 1$. This observation leads to the next remark.

Remark 1.8. *Let $A \in M_n(\mathbb{Z})$ be a circulant matrix and for each fixed positive integer k consider the matrix $W_n^k A$. Then A is singular (non-singular) if and only if $W_n^k A$ is singular (non-singular). That is, if we want to study singularity/non-singularity of a matrix A then it is enough to study $\Gamma_A(x)$.*

Using Remark 1.8 and Lemma 1.4, the following result is immediate and hence the proof is omitted.

Lemma 1.9. *Let A be a circulant digraph of order n and let $\Gamma_A(x)$ be the polynomial defined above. Then A is singular if and only if $\Phi_d(x) \mid \Gamma_A(x)$, for some divisor $d \neq 1$ of n.*

As an immediate corollary of Lemma 1.9, we have the following result.

Corollary 1.10. *Let p be a prime and let k be a positive integer with $p \nmid k$. Also, let X be a k-regular circulant graph/digraph on p^ℓ vertices, for some positive integer ℓ. Then X is non-singular.*

Proof. Using Lemma 1.9, we just need to show that $\Phi_d(x) \nmid \Gamma_A(x)$ for every $d \mid p^\ell, d \neq 1$. Let if possible, $\Gamma_A(x) = \Phi_d(x) g(x)$ for some $g(x) \in \mathbb{Z}[x]$. Using Lemma 1.3, we have $\Phi_d(1) = p$ for every $d \mid p^\ell, d \neq 1$. As $g(x) \in \mathbb{Z}[x], g(1) \in \mathbb{Z}$. Thus, we get

$$k = \Gamma_A(1) = \Phi_d(1) g(1) = p\, g(1).$$

A contradiction to our assumption that $p \nmid k$. Thus the proof of the result is complete. $\square$

The remaining part of this paper consists of two more sections that are mainly concerned with applications of Lemma 1.9. Section 2 gives necessary and sufficient conditions for a few classes of circulant graphs to be non-singular and Section 3 gives possible generalization of the results studied in Section 2.

Before proceeding to Section 2, recall that for a graph $X = (V, E_1)$, the complement graph of X, denoted $X^c = (V, E_2)$, is a graph in which $(u, v) \in E_2$ whenever $(u, v) \notin E_1$ and vice versa, for every $u \neq v \in V$. Note that (u, u) is neither an element of E_1 nor an element of E_2. Also, a graph X is circulant if and only if X^c is circulant and if A is the adjacency matrix of X then the adjacency matrix of X^c is given by $\mathbf{J} - A - I$.

2 Some Singular Circulant Graphs

This section is devoted to finding necessary and sufficient conditions for a few classes of circulant graphs to be singular or not. Before proceeding to these results, we show that the adjacency matrix A of a circulant graph on n vertices is a polynomial in $W_n + W_n^{-1}$, the adjacency matrix of C_n, the cycle graph on n vertices. To do so, we need the following definition.

Definition 2.11. *Let $v_1, v_2, \ldots, v_n$ be the vertices of a connected graph X. If d is the diameter of X then, for $0 \le k \le d$, the k*-th distance matrix *of X, denoted $A_k(X)$, is defined as*

$$(A_k(X))_{rs} = \begin{cases} 1, & \text{if } d(v_r, v_s) = k, \\ 0, & \text{otherwise,} \end{cases}$$

where $d(u, v)$ is the distance between the vertices $u, v \in V$.

For example, $\tau = \lfloor \frac{n}{2} \rfloor$ and consider the cycle graph C_n. Also, let us write A_k to denote the distance matrices $A_k(C_n)$, for $0 \le k \le \tau$. Then, for $1 \le i < \tau$, $A_i = W_n^i + W_n^{n-i}$ and

$$A_\tau = \begin{cases} W_n^\tau, & \text{if } n \text{ is even,} \\ W_n^\tau + W_n^{n-\tau}, & \text{if } n \text{ is odd.} \end{cases} \tag{2.1}$$

The identity

$$(x^k + x^{-k}) = (x + x^{-1})(x^{k-1} + x^{1-k}) - (x^{k-2} + x^{2-k})$$

enables us to readily establish, by mathematical induction, that $x^k + x^{-k}$ is a monic polynomial in $x + x^{-1}$ of degree k with integral coefficients. Also, for n even, $2\tau = n$ and hence $W_n^\tau = \frac{W_n^\tau + W_n^{-\tau}}{2}$. Consequently, A_i's, for $1 \le i \le \tau$, are polynomials of degree $\le i$, in A, the adjacency matrix of C_n, over $\mathbb{Q}$. Now, let B be a symmetric circulant matrix with representer polynomial $\gamma_B(x) = \sum\limits_{i=0}^{n-1} b_i x^i$. Then by definition, $B = \gamma_B(W_n) = \sum\limits_{i=0}^{n-1} b_i W_n^i$ and $B^t = \sum\limits_{i=0}^{n-1} b_i W_n^{n-i}$. But B is symmetric implies that $B = B^t$ and therefore, $b_i = b_{n-i}$, for $1 \le i \le n-1$. Thus, $B = \sum\limits_{i=0}^{\tau} b_i A_i$ and hence we see that the adjacency matrix of any circulant graph is a polynomial in A, the adjacency matrix of C_n, over $\mathbb{Q}$.

For $1 \le i \le \tau$, let us denote the graph with adjacency matrix A_i as C_n^i. Then observe that $C_n^1 = C_n$ is the cycle graph on n vertices. Also, note that the corresponding representer polynomials, for $1 \le i < \tau$, are given by $\gamma_{A_i}(x) = x^i \left(1 + x^{n-2i}\right)$ and $\gamma_{A_\tau}(x) = x^\tau$, if n is even, and $\gamma_{A_\tau}(x) = x^\tau(1 + x)$, if n is odd. The next result uses the above notations and observations to give a necessary and sufficient condition for the graphs C_n^i, for $1 \le i \le \tau$, to be singular.

Lemma 2.12. *Fix a positive integer $n \geq 3$ and let $1 \leq i \leq \tau = \lfloor \frac{n}{2} \rfloor$. Then the graph C_n^i is singular if and only if n is a multiple of 4 and $\gcd(i, \frac{n}{2}) \mid \frac{n}{4}$.*

Proof. Using the discussion above, $\Gamma_{A_i}(x) = 1 + x^{n-2i}$, for $1 \leq i < \tau$ and $\Gamma_{A_\tau}(x) = 1 + x$, if n is odd, and $\Gamma_{A_\tau}(x) = 1$, if n is even. If n is odd then $\zeta_n^k \neq -1$ for any $k, 1 \leq k \leq n-1$. Hence, A_τ is non-singular for all n. So, we need to consider $\Gamma_{A_i}(x) = 1 + x^{n-2i}$, for $1 \leq i < \tau$.

In this case, A_i is singular if and only if $\Gamma_{A_i}(\zeta_n^k) = 0$, for some $k, 1 \leq k \leq n-1$. That is, we need $\left(\zeta_n^k\right)^{n-2i} = -1$. Or equivalently, we need $2ki \equiv \frac{n}{2} \pmod{n}$. That is, $ki \equiv \frac{n}{4} \pmod{\frac{n}{2}}$. Therefore, it follows that 4 divides n and $\gcd(i, \frac{n}{2}) \mid \frac{n}{4}$. ∎

Remark 2.13. *We can rewrite the condition in Lemma 2.12 as follows:*
The graph C_n^i is singular if and only if the following conditions are satisfied:

1. *n is a multiple of 4, and*

2. *if s is the largest positive integer such that 2^s divides n then i is an odd multiple of 2^t for some t, $0 \leq t \leq s-2$.*

As an immediate consequence of Lemma 2.12, we have the following corollary.

Corollary 2.14. *Let C_n be the cycle graph on n vertices. Then C_n is singular if and only if $4 \mid n$.*

The next result gives a necessary and sufficient condition for the complement graph $(C_n^i)^c$ of C_n^i to be singular.

Lemma 2.15. *Fix a positive integer $n \geq 4$. Then the graph*

1. *$(C_n^\tau)^c$ is singular if and only if n is even or $n \equiv 3 \pmod{6}$.*

2. *$(C_n^i)^c$, for $1 \leq i < \tau$, is singular if and only if $3 \mid n$ and $\gcd(i, n) \mid \frac{n}{3}$.*

Proof. Let n be even. Then, using definition of complement of a graph, the adjacency matrix of $(C_n^\tau)^c$, say A, is given by $\mathbf{J} - A_\tau - I$. Hence, $\gamma_A(x) = 1 + x + \cdots + x^{n-1} - 1 - \gamma_{A_\tau}(x)$ is the representer polynomial of $(C_n^\tau)^c$. Thus,

$$\gamma_A(x) = \frac{x^n - 1}{x - 1} - (1 + x^\tau)$$

and hence $\gamma_A(\zeta_n) = 0$ (n is even). Thus, the graph $(C_n^\tau)^c$ is singular, whenever n is even. For n odd, it can be checked that

$$\gamma_A(x) = \frac{x^n - 1}{x - 1} - (1 + x^\tau + x^{\tau+1}).$$

Consequently, $(C_n^\tau)^c$ is singular if and only if $\gamma_A(\zeta_n^k) = 0$, for some $k, 1 \leq k \leq n-1$. Or equivalently, $1 + (\zeta_n^k)^\tau + (\zeta_n^k)^{\tau+1} = 0$, for some $k, 1 \leq k \leq n-1$. This is equivalent to the statement that $\zeta_n^{k\tau}$ is a primitive 3-rd root of unity. Thus, $k\tau \equiv \frac{n}{3} \pmod{n}$, or equivalently, $\gcd(\tau, n) \mid \frac{n}{3}$. Thus, $n \equiv 3 \pmod{6}$ and in this case, $\gcd(\tau, n)$ indeed divides $\frac{n}{3}$.

Now assume that $1 \leq i < \tau$. In this case, if A is the adjacency matrix of $(C_n^i)^c$, then $A = \mathbf{J} - A_i - I$. Consequently, its representer polynomial is $\gamma_A(x) = \frac{x^n-1}{x-1} - (1 + x^i + x^{n-i})$. Thus, $(C_n^i)^c$ is singular if and only if $\gamma_A(\zeta_n^k) = 0$, for some $k, 1 \leq k \leq n-1$. Or equivalently, $1 + \zeta_n^{ki} + \zeta_n^{-ki} = 0$, for some k, $1 \leq k \leq n-1$. That is, ζ_n^{ki} is a primitive 3-rd root of unity. Thus, using the argument similar to one in the first part, one has $(C_n^i)^c$ is singular if and only if $3 \mid n$ and $\gcd(i, n) \mid \frac{n}{3}$. ∎

As an immediate consequence of Lemma 2.15, we have the following corollary.

Corollary 2.16. *Fix a positive integer n and let C_n^c be the complement graph of the cycle graph C_n. Then the complement graph C_n^c is singular if and only if $3 \mid n$.*

We now obtain necessary and sufficient conditions for non-singularity of circulant graphs that were studied by Ruivivar [10]. In [10], the author studied two classes of graphs. For the sake of notational clarity, his notations have been slightly modified. Fix a positive integer $n \geq 3$ and let $1 \leq r < \tau = \lfloor \frac{n}{2} \rfloor$. The first class of circulant graphs, denoted $C_n^{(r)}$, has the same vertex set as the vertex set of the cycle C_n and $\{x, y\}$ is an edge whenever the length of the smallest path from x to y in C_n is at most r. He called these graphs the r-th power graph of the cycle graph C_n. Note that $C_n^{(\tau)}$ is the complete graph. The second class of graphs, denoted $C(2n, r)$ is a graph on $2n$ vertices and its adjacency matrix is the sum of the adjacency matrices of $C_{2n}^{(r)}$ and C_{2n}^{n}, where $1 \leq r < n$. The next result appears as Theorem 2.2 of [10]. We give a separate proof for the sake of completeness.

Theorem 2.17 (Ruivivar [10])**.** *Let $n \geq 3$ and let $1 \leq r < \lfloor \frac{n}{2} \rfloor$. Then the graph $C_n^{(r)}$ is singular if and only if one of the following conditions hold:*

1. $\gcd(n, r) > 1$
2. $\gcd(n, r) = 1$, *n is even and* $\gcd(r + 1, n)$ *divides* $\frac{n}{2}$.

Proof. Let A be the adjacency matrix of the graph $C_n^{(r)}$. Then, by definition, the first row of A equals $[0, \underbrace{1, 1, \ldots, 1}_{r}\ \underbrace{0, 0, \ldots, 0}_{n-2r-1}\ \underbrace{1, 1, \ldots, 1}_{r}]$ and $\gamma_A(x) = x\Gamma_A(x)$, where

$$\Gamma_A(x) = [1 + x + \cdots + x^{r-1}] + x^{n-r-1}[1 + x + \cdots + x^{r-1}] = \frac{x^r - 1}{x - 1}(1 + x^{n-r-1}).$$

Therefore, $C_n^{(r)}$ is singular if and only if $\Gamma_A(\zeta_n^d) = 0$, for some $d, 1 \leq d \leq n - 1$. Or equivalently either $(\zeta_n^d)^r - 1 = 0$ or $1 + (\zeta_n^d)^{n-r-1} = 0$.

If $(\zeta_n^d)^r - 1 = 0$ then $\gcd(r, n) > 1$ is the required condition as $1 \leq d \leq n-1$. If $\gcd(r, n) = 1$ then we need $1 + (\zeta_n^d)^{n-r-1} = 0$. This implies that $d(r + 1) \equiv \frac{n}{2} \pmod{n}$. Which in turn gives the required result.

Thus, the proof of the theorem is complete. □

The following result can be seen as a corollary to Lemma 1.7. But an idea of the proof is given for completeness.

Corollary 2.18. *Let $n \geq 3$ and let $1 \leq r < \lfloor \frac{n}{2} \rfloor$. Then the graph $(C_n^{(r)})^c$ is non-singular if and only if* $\gcd(n, 2r + 1) = 1$.

Proof. Let A be the adjacency matrix of $(C_n^{(r)})^c$. Then $[\underbrace{0, 0, \ldots, 0}_{r+1}\ \underbrace{1, \ldots, 1}_{n-2r-1}\ \underbrace{0, 0, \ldots, 0}_{r}]$ is the first row of A. Thus, using Remark 1.8, A is singular if and only if the circulant matrix with $[\underbrace{1, 1, \ldots, 1}_{n-2r-1}\ \underbrace{0, 0, \ldots, 0}_{2r+1}]$ as its first row is singular. Thus, using Lemma 1.7, A is singular if and only if $\gcd(2r + 1, n) > 1$. Hence, the required result follows. □

Before proceeding with the next result that gives a necessary and sufficient condition for the graph $C(2n, r)$ to be singular, we state a result that appears as Proposition 1 in Kurshan & Odlyzko [8]

Lemma 2.19 (Kurshan & Odlyzko [8]). *Let m and n be positive integers with $m \neq n$ and let ζ_n be a primitive n-root of unity. Then there exists a unit $u \in \mathbb{Z}[\zeta_n]$ dependent on m, n and ζ_n such that*

$$\Phi_m(\zeta_n) = \begin{cases} pu, & \text{if } \frac{m}{n} = p^{\alpha}, \quad p \text{ a prime}, \quad \alpha > 0; \\ (1-\zeta_{p^{\alpha}})u, & \text{if } \frac{m}{n} = p^{-\alpha}, \quad p \text{ a prime}, \quad \alpha > 0; \quad p \nmid m; \\ (1-\zeta_{p^{\alpha}+1})^{p-1}u, & \text{if } \frac{m}{n} = p^{-\alpha}, \quad p \text{ a prime}, \quad \alpha > 0; \quad p \mid m; \\ u, & \text{otherwise.} \end{cases}$$

Theorem 2.20. *Let n and r be positive integers such that the circulant graph $C(2n, r)$ is well defined. Then the circulant graph $C(2n, r)$ is singular if and only if $\gcd(n, 2r+1) \geq 3$.*

Proof. Let A be the adjacency matrix of the graph $C(2n, r)$. Then observe that the first row of A equals $[0, \underbrace{1, 1, \ldots, 1}_{r}, \underbrace{0, 0, \ldots, 0}_{n-r-1}, 1, \underbrace{0, 0, \ldots, 0}_{n-r-1}, \underbrace{1, 1, \ldots, 1}_{r}]$. Consequently,

$$\gamma_A(x) = x + x^2 + \cdots + x^r + x^n + x^{2n-r} + \cdots + x^{2n-1} = x\Gamma_A(x)$$

and

$$\begin{aligned} (x-1)\Gamma_A(x) &= x^r - 1 + x^{n-1}(x-1) + x^{2n-r-1}(x^r - 1) \\ &= x^r(1 - x^{2n-2r-1}) + (x^n - 1) - (x^{n-1} - x^{2n-1}) \\ &= (x^n - 1)(x^{n-1} + 1) - x^r(x^{2n-2r-1} - 1). \end{aligned}$$

Now, let us assume that $\gcd(n, 2r+1) = d \geq 3$. Then $(\zeta_{2n}^{2n/d} - 1)\Gamma_A(\zeta_{2n}^{2n/d}) = 0$ as

$$\left(\zeta_{2n}^{2n/d}\right)^n = \left(\zeta_{2n}^{2n}\right)^{n/d} = 1 = \left(\zeta_{2n}^{2n}\right)^{(2r+1)/d} = \left(\zeta_{2n}^{2n/d}\right)^{2r+1} = \left(\zeta_{2n}^{2n/d}\right)^{2n-2r-1}.$$

Hence, the circulant graph $C(2n, r)$ is singular.

Conversely, let us assume that the graph $C(2n, r)$ is singular. This implies that there exists an eigenvalue of $C(2n, r)$ that equals zero. That is, there exists a k, $1 \leq k \leq 2n-1$, such that $\gamma_A(\zeta_{2n}^k) = 0$. We will now show that if $\gcd(n, 2r+1) = 1$ then the expression $(x-1)\Gamma_A(x)$ evaluated at $x = \zeta_{2n}^k$ can never equal zero, for any k, $1 \leq k \leq 2n-1$, and this will complete the proof of the result.

We need to consider two cases depending on whether k is odd or k is even. Let k be even, say $k = 2m$, for some m, $1 \leq m < n$. Then evaluating $(x-1)\Gamma_A(x)$ at $x = \zeta_{2n}^{2m}$ and using $\gcd(n, 2r+1) = 1$ leads to

$$\begin{aligned} &\left[\left(\zeta_{2n}^{2m}\right)^n - 1\right]\left[\left(\zeta_{2n}^{2m}\right)^{(n-1)} + 1\right] - \left(\zeta_{2n}^{2m}\right)^r \left[\left(\zeta_{2n}^{2m}\right)^{2n-2r-1} - 1\right] \\ &= -\left(\zeta_{2n}^{2m}\right)^r \left[\left(\zeta_{2n}^{2m}\right)^{-(2r+1)} - 1\right] \neq 0. \end{aligned}$$

Now, let k be odd, say $k = 2m+1$, for some m, $0 \le m \le n-1$. Then evaluating $(x-1)\Gamma_A(x)$ at $x = \zeta_{2n}^{2m+1}$ leads to

$$\begin{aligned}
&\left[\left(\zeta_{2n}^{2m+1}\right)^n - 1\right]\left[\left(\zeta_{2n}^{2m+1}\right)^{(n-1)} + 1\right] - \left(\zeta_{2n}^{2m+1}\right)^r\left[\left(\zeta_{2n}^{2m+1}\right)^{2n-2r-1} - 1\right] \\
&\qquad = -2\left[-\zeta_{2n}^{-(2m+1)} + 1\right] - \zeta_{2n}^{-(2m+1)(r+1)}\left[1 - \zeta_{2n}^{(2m+1)(2r+1)}\right] \\
&\qquad = -\frac{\zeta_{2n}^{2m+1} - 1}{\zeta_{2n}^{(2m+1)(r+1)}}\left[-2\zeta_{2n}^{(2m+1)r} + \frac{\zeta_{2n}^{(2m+1)(2r+1)} - 1}{\zeta_{2n}^{(2m+1)} - 1}\right] \\
&\qquad = -\frac{\zeta_{2n}^{2m+1} - 1}{\zeta_{2n}^{(2m+1)(r+1)}}\left[-2\zeta_{2n}^{(2m+1)r} + \prod_{\ell|(2r+1),\ell\neq 1} \Phi_\ell(\zeta_{2n}^{2m+1})\right]
\end{aligned} \tag{2.2}$$

Note that, ζ_{2n}^{2m+1} is a d-th primitive root of unity, for some d dividing $2n$. As $\gcd(2r+1, 2n) = 1$, $\gcd(2r+1, d) = 1$. Thus, using Lemma 2.19, we get $\prod\limits_{\ell|(2r+1),\ell\neq 1} \Phi_\ell(\zeta_{2n}^{2m+1})$ is a unit in $\mathbb{Z}[\zeta_d]$. That is, $\left|\prod\limits_{\ell|(2r+1),\ell\neq 1} \Phi_\ell(\zeta_{2n}^{2m+1})\right| = 1$. Hence, in Equation (2.2), the term in the parenthesis cannot be zero. Thus, we have proved the result for the odd case as well.

Thus, the proof of the result is complete. $\square$

Remark 2.21. *We would like to mention here that the necessary part of Theorem 2.20 was stated and proved by Ruivivar (see Theorem 2.1 in [10]).*

We will now try to understand the complement graph $C(2n, r)^c$ of $C(2n, r)$.

Lemma 2.22. *Let n and r be positive integers such that the circulant graph $C(2n, r)$ is well defined. Then $C(2n, r)^c$ is non-singular if and only if the following conditions hold:*

1. *n and r have the same parity,*
2. *$\gcd(n, r+1) = 1$, and*
3. *the highest power of 2 dividing n is strictly smaller than the highest power of 2 dividing $n - r$.*

Proof. Let A be the adjacency matrix of $C(2n, r)^c$. Then $[\underbrace{0, 0, \ldots, 0}_{r+1}\ \underbrace{1, 1, \ldots, 1}_{n-r-1}\ 0\ \underbrace{1, 1, \ldots, 1}_{n-r-1}\ \underbrace{0, 0, \ldots, 0}_{r}]$ is the first row of A. Note that

$$\Gamma_A(x) = (1 + x^{n-r})\frac{x^{n-r-1} - 1}{x - 1}.$$

Now, let us assume that the graph $C(2n, r)^c$ is non-singular. This means that $\Gamma_A(\zeta_{2n}^k) \neq 0$, for any $k = 1, 2, \ldots, 2n-1$.

Note that if n and r have opposite parity then $\gcd(2n, n-r-1) = d \ge 2$ and hence $\Gamma_A(\zeta_{2n}^{2n/d}) = 0$. Also, if n and r have the same parity and $\gcd(n, r+1) = d > 2$ then $n - r - 1$ is odd and $\gcd(2n, n-r-1) = \gcd(n, n-r-1) = \gcd(n, r+1) = d$. Hence, in this case again, $\Gamma_A(\zeta_{2n}^{2n/d}) = 0$.

Now, the only case that we need to check is the following:
n and r have the same parity, $\gcd(n, r+1) = 1$ and the highest power of 2 dividing n is greater than or equal to the highest power of 2 dividing $n - r$.

As n and r have the same parity and $\gcd(n, r+1) = 1$, we get $\gcd(2n, n-r-1) = 1$ and thus

$$(\zeta_{2n}^k)^{n-r-1} - 1 \neq 0, \quad \text{for any} \quad k = 1, 2, \ldots, 2n-1.$$

Thus, we need to check for the condition on k so that $1 + (\zeta_{2n}^k)^{n-r} = 0$. This is true if and only if $\gcd(2n, n-r) \mid n$, or equivalently, the highest power of 2 dividing n is greater than or equal to the highest power of 2 dividing $n - r$.

Thus, we have the required result. $\square$

Remark 2.23. *Observe that using Lemma 2.22, the graph $C(2n, r)^c$ is non-singular, whenever n and r are both odd and $\gcd(n, r+1) = 1$. Such numbers can be easily computed. For example, a class of such graphs can be obtained by choosing two positive integers s and t with $s > t$ and defining $n = 2^s - 2^t + 1$ and $r = 2^t - 1$.*

3 Generalizations

In this section, we look at a few classes of graphs/digraphs, which are generalizations of the graphs that appear in Section 2. We first start with a class of circulant digraphs.

Consider a circulant matrix A whose first row contains r and s consecutive 1's separated by t consecutive 0's, where each of r, s and t are non-negative integers. That is, the vector $[\underbrace{1, 1, \ldots, 1}_{r}, \underbrace{0, 0, \ldots, 0}_{t}, \underbrace{1, 1, \ldots, 1}_{s}, \underbrace{0, 0, \ldots, 0}_{n-(r+t+s)}]$ is the first row of A. If $s = 0$, then it is an r-element circulant digraph studied in Lemma 1.7. These circulant digraphs will be called an (r, s, t)-element circulant digraph. The next result gives a few conditions under which the (r, s, t)-element circulant digraph is singular.

Lemma 3.24. *Let X be an (r, s, t)-element circulant digraph on n vertices. Then the graph X is singular if*

1. *$\gcd(n, s, r) > 1$, or*
2. *$\gcd(n, s) = 1$ and one of the following condition holds:*
   (a) *there exists $d \geq 2$ such that $d \mid t$ and $s = \ell r$, for some positive integer $\ell \equiv -1 \pmod{d}$.*
   (b) *n is even, there exists an even integer d such that $(r + t)$ is an odd multiple of $\frac{d}{2}$ and $s = \ell r$, for some positive integer $\ell \equiv 1 \pmod{d}$.*

Proof. **Proof of Part 1:** Observe that the representer polynomial of the (r, s, t)-element circulant digraph is given by

$$\begin{aligned} \gamma_A(x) &= 1 + x + \cdots + x^{r-1} + x^{r+t} + \cdots + x^{r+s+t-1} \\ &= \frac{x^r - 1}{x - 1} + x^{r+t}\frac{x^s - 1}{x - 1}. \end{aligned}$$

Or equivalently,

$$(x - 1)\gamma_A(x) = (x^r - 1) + x^{r+t}(x^s - 1). \tag{3.3}$$

Let $\gcd(n, r, s) = k > 1$. Then it can be easily checked that $\zeta_n^{n/k}$ is a root of Equation (3.3). Thus, X is singular. This completes the proof of the first part.

Proof of Part 2.2a: Let us assume that $\gcd(n, s) = 1$. Also, let us assume that there exists a positive integer $d \geq 2$ such that $d \mid t$ and $s = \ell r$, for some positive integer $\ell \equiv -1 \pmod{d}$. So, there exists $\beta \in \mathbb{Z}$ such that $\ell = \beta d - 1$. In this case, using Equation (3.3), we get

$$\begin{aligned}
(\zeta_n^{(n/d)} - 1)\gamma_A(\zeta_n^{(n/d)}) &= (\zeta_n^{(rn/d)} - 1)\left(1 + \zeta_n^{(r+t)n/d}\frac{\zeta_n^{\ell(rn/d)} - 1}{\zeta_n^{(rn/d)} - 1}\right) \\
&= (\zeta_n^{rn/d} - 1)\left(1 + \zeta_n^{(r+t)n/d}\frac{\zeta_n^{-(rn/d)} - 1}{\zeta_n^{(rn/d)} - 1}\right) \\
&= (\zeta_n^{rn/d} - 1)\left(1 - \zeta_n^{(tn/d)}\right).
\end{aligned}$$

As $d \mid t$, $\gamma_A(\zeta_n^{n/d}) = 0$. That is, we get the required result in this case as well.

Proof of Part 2.2b: Let us assume that $\gcd(n, s) = 1$, $n = 2m$. Also, let us assume that there exists an even positive integer d such that $r + t$ is an odd multiple of $\frac{d}{2}$ and $s = \ell r$, for some positive integer $\ell \equiv 1 \pmod{d}$. Then there exists $\beta \in \mathbb{Z}$ such that $\ell = \beta d + 1$. In this case, using Equation (3.3), we get

$$\begin{aligned}
(\zeta_n^{(n/d)} - 1)\gamma_A(\zeta_n^{(n/d)}) &= (\zeta_n^{(rn/d)} - 1)\left(1 + \zeta_n^{(r+t)n/d}\frac{\zeta_n^{\ell(rn/d)} - 1}{\zeta_n^{(rn/d)} - 1}\right) \\
&= (\zeta_n^{rn/d} - 1)\left(1 + \zeta_n^{(r+t)n/d}\frac{\zeta_n^{(rn/d)} - 1}{\zeta_n^{(rn/d)} - 1}\right) \\
&= (\zeta_n^{rn/d} - 1)\left(1 + \zeta_n^{(r+t)n/d)}\right).
\end{aligned}$$

Thus, under the given conditions, the corresponding digraph X is singular.

Hence, the proof of the lemma is complete. $\square$

Thus, the above result gives conditions under which the generalized (r, s, t)- digraphs, for non-negative values of r, s and t, are singular. We will now define another class of circulant digraphs and obtain conditions under which the circulant digraphs are singular. These graphs are also a generalization of the graphs studied in Lemma 1.7.

Let i, j, k and ℓ be non-negative integers such that $j > \ell$ and $kj + i + \ell < n$. Consider a class of circulant digraphs, denoted $C_n^{i,j,k,\ell}$, that has $\gamma_{A(C_n^{i,j,k,\ell})}(x) = \sum\limits_{t=0}^{k}\sum\limits_{s=i}^{i+\ell} x^{s+tj}$ as its representer polynomial. Then

$$\begin{aligned}
\gamma_{A(C_n^{i,j,k,\ell})}(x) &= x^i(1 + x + \cdots + x^\ell)(1 + x^j + x^{2j} + \cdots + x^{kj}) \\
&= x^i\frac{x^{\ell+1} - 1}{x - 1} \cdot \frac{x^{(k+1)j} - 1}{x^j - 1} \\
&= x^i \prod_{s \mid \ell+1, s \neq 1} \Phi_s(x) \cdot \prod_{t \mid (k+1)j, t \nmid j} \Phi_t(x). \qquad (3.4)
\end{aligned}$$

Hence, we have the following theorem which we state without proof.

Theorem 3.25. *Let i, j, k and ℓ be non-negative integers with $j > \ell$ and $kj + i + \ell < n$. Then the circulant digraph $C_n^{i,j,k,\ell}$, defined above, is singular if and only if either* $\gcd(\ell + 1, n) \geq 2$ *or* $\gcd(k + 1, \frac{n}{\gcd(n,j)}) \geq 2$.

Remark 3.26. *Note that we can vary the non-negative integers i, j, k and ℓ to define quite a few class of circulant digraphs. For example, it can be seen that the graphs $G(r, t)$ that are given by Doob [5] are a particular case of the above class. Also, it can be easily verified that Theorem 3.25 is a generalization of Lemma 1.7.*

Conclusion

In the first section, we have obtained necessary and sufficient conditions for a few known classes of circulant graphs/digraphs to be singular. We found these necessary and sufficient conditions by using Lemma 1.9. The graphs/digraphs that were studied in Section 2 have been generalized to (r, s, t)-circulant digraphs for non-negative integers r, s and t, and the circulant digraph $C_n^{i,j,k,l}$, under certain restrictions. A necessary and sufficient condition for the digraphs $C_n^{i,j,k,l}$ to be singular is also obtained. Some necessary conditions are given under which the (r, s, t)-circulant digraphs are singular.

It will be nice to obtain necessary and sufficient conditions for the generalized (r, s, t)-digraphs to be singular.

References

[1] Tom M. Apostol. "Introduction to Analytic Number theory," *Springer-Verlag*, New York, 1976.

[2] N. Biggs. "Algebraic Graph Theory," Cambridge Tracts in Mathematics, 67, Cambridge Univ. Press, New York and London, 1974.

[3] J. A. Bondy and U. S. R. Murty. *Graph Theory with Applications*. The Macmillan Press Ltd., London, 1976.

[4] Philip J. Davis. "Circulant matrices," A Wiley-interscience publications, 1979.

[5] Michael Doob. 'Circulant graphs with $\det(-A(G)) = -\deg(G)$: codeterminants with K_n,' Linear algebra and its applications, 340: 87 - 96, 2002.

[6] David S. Dummit and Richard M. Foote. "Abstract Algebra," Second Edition, John Wiley and Sons, 1999.

[7] D. Geller, I. Kra, S. Popescu and S. Simanca. 'On circulant matrices,' (http://www.math.sunysb.edu/˜sorin/eprints/circulant.pdf).

[8] R. P. Kurshan and A. M. Odlyzko. 'Values of cyclotomic polynomials at roots of unity,' Math. Scand. 49, 15 - 35, 1981.

[9] Victor V. Prasolov. "Polynomials," Springer, 2001.

[10] Leonor Aquino-Ruivivar. 'Singular and Nonsingular Circulant Graphs,' Journal of Research in Science, Computing and Engineering (JRSCE), Vol. 3, No. 3, 2006.

[11] S. R. Searle. 'On Inverting Circulant Matrices,' Linear algebra and its applications, 25: 77 - 89, 1979.